Acronis

acronis.com

網路保護

24.07

使用指南

版本：2024/8/7

目錄

開始使用 Cyber Protection

啟用帳戶

當系統管理員為您建立帳戶後，系統會傳送一封電子郵件到您的電子郵件位址。此郵件包含以下資訊：

- **您的登入。**這是您用來登入的使用者名稱。您的登入也會顯示在帳戶啟用頁面上。
- **啟用帳戶**按鈕。按一下該按鈕，然後設定帳戶的密碼。請確保密碼長度至少 9 個字元。如需有關密碼的詳細資訊，請參閱 "密碼需求" (第 19 頁)。

如果系統管理員已啟用雙重驗證機制，則系統會提示您為帳戶設定該機制。如需有關該機制的詳細資訊，請參閱 "雙重驗證機制" (第 19 頁)。

密碼需求

使用者帳戶的密碼必須至少包含 9 個字元。還會檢查密碼的複雜性，並將其歸入下列其中一個類別：

- 弱式
- 中
- 強式

您不能儲存弱式密碼，即使它可能包含 9 個以上字元。與使用者名稱、登入名稱、使用者電子郵件或使用者帳戶所屬之租用戶的名稱重複的密碼一律被視為弱式密碼。大多數常用密碼也被視為弱式密碼。

若要強化密碼，請新增更多字元。並非必須使用不同類型的字元(例如數字、大小寫字母及特殊字元)，但這樣做會強化密碼，也會縮短其長度。

雙重驗證機制

雙重驗證機制 (2FA) 提供額外的保護，使未經授權者無法存取您的帳戶。設定 2FA 時，您必須輸入密碼 (第一要素) 和一次性代碼 (第二要素)，才能登入 Cyber Protect 主控台。一次性代碼是由必須安裝在您的行動電話或您所屬的其他裝置上的特殊應用程式所產生。即使有人發現您的登入和密碼，如果沒有您第二要素裝置的存取權，他們將無法登入您的帳戶。

若要為您的帳戶設定雙重驗證機制

如果系統管理員已為您的組織啟用 2FA，您必須為您的帳戶設定 2FA。如果系統管理員在登入 Cyber Protect 主控台時啟用 2FA，則您必須在目前的工作階段過期時對其進行設定。

必要條件

- 系統管理員已為您的組織啟用雙重驗證機制。

若要為您的帳戶設定雙重驗證機制

1. 在行動裝置上安裝驗證器應用程式。

   驗證器應用程式的範例：

   - Twilio Authy
   - Microsoft Authenticator
   - Google Authenticator
2. 使用驗證器應用程式掃描 QR 碼，然後在 **[設定雙重驗證機制]** 視窗中，輸入驗證器應用程式上顯示的 6 位數代碼。
3. 按 **[下一步]**。

   如果您遺失 2FA 裝置或解除安裝驗證器應用程式，則會顯示如何還原您帳戶存取權的指示。
4. 儲存或列印 PDF 檔案。

   注意事項

   請務必將 PDF 檔案儲存在安全位置，或列印出來以供進一步參考。這是還原存取權的最佳方式。
5. 返回 Cyber Protect 主控台登入頁面，然後輸入所產生的代碼。

   一次性代碼的有效期限為 30 秒。如果您等待超過 30 秒，請使用下一個產生的代碼。

下次登入時，您可以選擇 **[信任此瀏覽器...]** 核取方塊。在此情況下，當您在這部電腦上使用此瀏覽器進行後續登入時，就不需要驗證碼。

注意事項

建議您清除此核取方塊。否則，您將失去您帳戶對 2FA 的存取權。

若要在新裝置上還原雙重驗證機制 (2FA)

如果您可以存取先前設定的行動版驗證應用程式

1. 在新裝置上安裝驗證器應用程式。
2. 使用您在裝置上設定 2FA 時所儲存的 PDF 檔案。此檔案包含 32 位數驗證碼，您必須在驗證器應用程式中輸入這個驗證碼，才能將驗證器應用程式再次連結到您的 Acronis 帳戶。

   重要事項

   如果驗證碼沒有作用，請在驗證器的行動版應用程式中確認其與您裝置同步的時間。

   如果您在設定期間沒有儲存 PDF 檔案：

a. 按一下 **[重設 2FA]**，然後輸入顯示在行動版驗證器應用程式中的一次性密碼。
b. 依照畫面上的說明操作。

如果您無法存取先前設定的行動版驗證器應用程式

1. 拿一個新的行動裝置。
2. 使用已儲存的 PDF 檔案連結新裝置 (此檔案的預設名稱為 `cyberprotect-2fa-backupcode.pdf`)。
3. 從備份還原對您帳戶的存取權。請確認您的行動版應用程式支援備份。
4. 從另一個行動裝置 (如果受到應用程式支援) 使用相同的帳戶開啟應用程式。

隱私設定

隱私設定可協助您表明您是否同意收集、使用和披露您的個人資訊。

根據您要使用 Cyber Protect Cloud 所在的國家/地區以及為您提供服務的 Cyber Protect Cloud 資料中心而定，在最初啟動 Cyber Protect Cloud 時，可能會要求您確認您是否同意在 Cyber Protect Cloud 中使用 Google Analytics (分析)。

Google Analytics (分析) 可透過收集化名資料，協助我們更瞭解使用者行為並提升 Cyber Protect Cloud 中的使用者體驗。

如果您在最初啟動 Cyber Protect Cloud 時已啟用或拒絕啟用 Google Analytics (分析)，之後可以隨時改變您的決定。

若要啟用或停用 Google Analytics (分析)

1. 在 Cyber Protect 主控台中，按一下 **[管理帳戶]**。
2. 按一下右上角的帳戶圖示。
3. 選擇 **[我的隱私設定]**。**[我的隱私設定]** 視窗隨即顯示。
4. 在 **[Google Analytics (分析) 資料收集]** 區段中，按一下下列其中一個按鈕：
   - **[開啟]** 表示啟用 Google Analytics (分析)
   - **[關閉]** 表示停用 Google Analytics (分析)

在 **[如何刪除 Cookie]** 區段中，您可以直接在瀏覽器中控制並管理 Cookie。

注意事項
如果沒有看到 [Google Analytics (分析)] 區段，表示您的國家/地區未使用 Google Analytics (分析)。

在試用期最初顯示的 **[產品內上線和互動式說明]** 區段中，您可以停止或繼續接收程式未來的改進功能和新功能的相關資訊。預設啟用此功能，但您可以切換到 **[關閉]** 來停用此功能。

存取 Cyber Protection 服務

啟用帳戶之後，即可登入 Cyber Protect 主控台或透過管理入口網站 Cyber Protection 存取服務。

登入 Cyber Protect 主控台

1. 請移至 Cyber Protection 服務登入頁面。
2. 輸入登入，然後按一下 **[下一步]**。
3. 輸入您的密碼，然後按一下 **[下一步]**。
4. [如果您使用多 Cyber Protect Cloud 服務] 按一下 **[網路保護]**。
   僅能存取 Cyber Protection 服務的使用者，請直接登入 Cyber Protect 主控台。
   如果 **[資安防護]** 不是您唯一可存取的服務，您可使用右上角的  圖示，在服務之間進行切換。系統管理員也可以使用此圖示切換到管理入口網站。

啟用的工作階段，Cyber Protect 主控台的逾時期間為 24 小時，閒置工作階段則為 1 小時。

您可以按一下右上角的帳戶圖示，以變更 Web 介面的語言。

透過管理入口網站存取 Cyber Protect 主控台

1. 在管理入口網站，前往 **[監控]** > **[使用情形]**。
2. 在 **[Cyber Protect]**，選取 **[保護]**，然後按一下 **[管理服務]**。
   或者，在 **[用戶端]**，選取客戶，然後按一下 **[管理服務]**。

最後系統會將您重新導向至 Cyber Protect 主控台。

重要事項
如果客戶位於**自助服務**管理模式下，則您無法為其管理服務。只有客戶系統管理員可以將客戶模式變更為 **[由服務提供者管理]**，然後就可以管理服務。

重設密碼

1. 請移至 Cyber Protection 服務登入頁面。
2. 輸入登入，然後按一下 **[下一步]**。
3. 按一下 **[忘記密碼?]**
4. 按一下 **[傳送]**，確認您需要進一步的指示。
5. 依照您收到的電子郵件中的指示進行。
6. 設定您的新密碼。

軟體需求

支援的網頁瀏覽器

Cyber Protect 主控台使用 TLS 1.2 通訊協定並支援以下網頁瀏覽器：

- Google Chrome 29 或更新版本
- Mozilla Firefox 23 或更新版本
- Opera 16 或更新版本
- Microsoft Edge 25 或更新版本
- 在 macOS 與 iOS 作業系統中執行的 Safari 8 或更新版本

在其他網頁瀏覽器 (包括在其他作業系統中執行的 Safari 瀏覽器) 中，使用者介面可能會顯示不正確，或是部分功能無法正常使用。

支援的作業系統和環境

下列資訊適用於備份與復原。如需有關作業系統支援的保護功能的詳細資料，請參閱 "作業系統支援的保護功能" (第 42 頁)。

Windows 用代理程式

此代理程式包含用於支援一組不同作業系統的 [防毒和防惡意軟體防護] 及 [URL 篩選] 的元件。請參閱 "支援防毒和防惡意軟體防護的作業系統" (第 729 頁)。

注意事項
以下支援的作業系統清單適用於備份與復原。

- Windows XP Professional SP1 (x64)、SP2 (x64)、SP3 (x86)
- Windows Server 2003 SP1/2003 R2 以及更新版本 - Standard 與 Enterprise 版 (x86、x64)
- Windows Small Business Server 2003/2003 R2
- Windows Server 2008、Windows Server 2008 SP2* – Standard、Enterprise、Datacenter、Foundation 和 Web 版本 (x86、x64)
- Windows Small Business Server 2008, Windows Small Business Server 2008 SP2*
- Windows 7 – 所有版本

  注意事項
  若要搭配 Windows 7 使用 Cyber Protection，您必須安裝以下 Microsoft 更新，然後再安裝保護代理程式：
  - Windows 7 Extended Security Updates (ESU)
  - KB4474419
  - KB4490628

  有關所需更新的詳細資訊，請參閱本知識庫文章。

- Windows Server 2008 R2* – Standard、Enterprise、Datacenter、Foundation 和 Web 版本
- Windows Home Server 2011*
- Windows MultiPoint Server 2010*/2011*/2012
- Windows Small Business Server 2011* – 所有版本
- Windows 8/8.1 – 所有版本(x86、x64) ，但 Windows RT 版除外
- Windows Server 2012/2012 R2 – 所有版本
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 – Home、Pro、Education、Enterprise、IoT Enterprise 以及 LTSC (前身為 LTSB) 版
- Windows Server 2016 – 所有安裝選項，Nano Server 除外
- Windows Server 2019 – 所有安裝選項，Nano Server 除外
- Windows 11 – 所有版本
- Windows Server 2022 – 所有安裝選項，Nano Server 除外

注意事項
* 若要搭配此版本的 Windows 使用 Cyber Protection，必須在安裝保護代理程式之前，先安裝 Microsoft 的 SHA2 程式碼簽署支援更新 (KB4474419)。

如需有關與 SHA2 程式碼簽署支援更新相關的資訊，請參閱這篇知識庫文章。

SQL 用代理程式、Active Directory 用代理程式、Exchange 用代理程式 (適用於資料庫備份及應用程式感知備份)

每一個代理程式可安裝於執行任何上述所列之作業系統的電腦，以及個別應用程式的支援版本。

資料洩漏防禦用代理程式

裝置控制

- Microsoft Windows 7 Service Pack 1 和更新版本
- Microsoft Windows Server 2008 R2 和更新版本
- macOS 10.15 (Catalina)
- macOS 11.2.3 (Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)

注意事項
適用於 macOS 的資料洩漏防禦用代理程式僅支援 x64 處理器。不支援 Apple Silicon ARM 型處理器。

資料洩漏防禦

- Microsoft Windows 7 Service Pack 1 和更新版本
- Microsoft Windows Server 2008 R2 和更新版本

注意事項
資料洩漏防禦用代理程式可能安裝在不支援的 macOS 系統上，因為它是 Mac 用代理程式的完整部分。在此情況下，Cyber Protect 主控台將會指出資料洩漏防禦用代理程式已安裝在電腦上，但是裝置控制和資料洩漏防禦功能將無法運作。裝置控制功能僅適用於資料洩漏防禦用代理程式支援的 macOS 系統。

Advanced Data Loss Prevention 用代理程式

- Microsoft Windows 7 Service Pack 1 和更新版本
- Microsoft Windows Server 2008 R2 和更新版本

File Sync & Share 用代理程式

如需支援的作業系統清單，請參閱 Cyber Files Cloud 使用指南。

Exchange 用代理程式 (適用於信箱備份)

- Windows Server 2008 - Standard、Enterprise、Datacenter、Foundation 和 Web 版本 (x86、x64)
- Windows Small Business Server 2008
- Windows 7 – 所有版本
- Windows Server 2008 R2 – Standard、Enterprise、Datacenter、Foundation 和 Web 版本
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – 所有版本
- Windows 8/8.1 – 所有版本(x86、x64) , 但 Windows RT 版除外

- Windows Server 2012/2012 R2 – 所有版本
- Windows Storage Server 2008/2008 R2/2012/2012 R2
- Windows 10 – Home、Pro、Education 和 Enterprise 版本
- Windows Server 2016 – 所有安裝選項，Nano Server 除外
- Windows Server 2019 – 所有安裝選項，Nano Server 除外
- Windows 11 – 所有版本
- Windows Server 2022 – 所有安裝選項，Nano Server 除外

Microsoft 365 用代理程式

- Windows Server 2008 – Standard、Enterprise、Datacenter、Foundation 和 Web 版本 (僅限 x64)
- Windows Small Business Server 2008
- Windows Server 2008 R2 – Standard、Enterprise、Datacenter、Foundation 和 Web 版本
- Windows Home Server 2011
- Windows Small Business Server 2011 – 所有版本
- Windows 8/8.1 – 所有版本(僅限 x64) , 但 Windows RT 版除外
- Windows Server 2012/2012 R2 – 所有版本
- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016 (僅限 x64)
- Windows 10 – Home、Pro、Education 和 Enterprise 版本 (僅限 x64)
- Windows Server 2016 – 所有安裝選項，Nano Server 除外 (僅限 x64)
- Windows Server 2019 – 所有安裝選項，Nano Server 除外 (僅限 x64)
- Windows 11 – 所有版本
- Windows Server 2022 – 所有安裝選項，Nano Server 除外

適用於 Oracle 的代理程式

- Windows Server 2008R2 - Standard、Enterprise、Datacenter 和 Web 版本 (x86、x64)
- Windows Server 2012R2 - Standard、Enterprise、Datacenter 和 Web 版本 (x86、x64)
- Linux – Linux 用代理程式支援的任何核心和發行版本 (列在下面)

MySQL/MariaDB 用代理程式

- Linux – Linux 用代理程式支援的任何核心和發行版本 (列在下面)

Linux 用代理程式

此代理程式包含用於支援一組不同作業系統的 [防毒和防惡意軟體防護] 及 [URL 篩選] 的元件。請參閱 "支援防毒和防惡意軟體防護的作業系統" (第 729 頁)。

注意事項
以下支援的作業系統清單適用於備份與復原。

Cyber Protect Cloud 支援使用下列元件的 x86 和 x86_64 Linux 發行版：

- 核心版本 2.6.9 到 6.6

  支援的核心版本會根據 www.kernel.org 的發行版本列出。部分發行版 (如 Red Hat Enterprise Linux) 會將新功能回移至舊核心版本。即使其版本在支援的範圍內，可能還是不支援這類發行版專用的核心版本。
- GNU C 程式庫 (glibc) 2.3.4 或更新版本

下列發行版已經過特別測試。但是，即使您的 Linux 發行版或核心版本未列於下方，但基於 Linux 作業系統的特性，仍可能在所有必要的情況下正確運作。如果您在使用 Cyber Protect Cloud 時遇到發行版和核心版本的組合問題，請聯絡支援團隊進行進一步調查。

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- 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
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 37, 38
- SUSE Linux Enterprise Server 10, 11, 12, 15

  重要事項
  SUSE Linux Enterprise Server 12 和 SUSE Linux Enterprise Server 15 不支援使用 Btrfs 的設定。

- 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* – Unbreakable Enterprise Kernel 和 Red Hat Compatible Kernel

  注意事項
  在啟用安全開機的 Oracle Linux 8.6 和更新版本上安裝保護代理程式需要手動簽署核心模組。如需有關如何簽署核心模組的詳細資訊，請參閱這篇知識庫文章。

- CloudLinux 5.x, 6.x, 7.x, 8.x*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.x*,9.0*, 9.1*, 9.2*, 9.3*
- Rocky Linux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- ALT Linux 7.0

* 從 8.4 版開始，只支援 4.18 到 5.19 的核心

Mac 用代理程式

此代理程式包含用於支援一組不同作業系統的 [防毒和防惡意軟體防護] 及 [URL 篩選] 的元件。請參閱 "支援防毒和防惡意軟體防護的作業系統" (第 729 頁)。

注意事項
以下支援的作業系統清單適用於備份與復原。

支援 x64 和 ARM 架構 (用於 Apple Slicon 處理器，例如 Apple M1 和 M2)。

注意事項
您無法將 Intel Mac 的磁碟層級備份復原至使用 Apple 晶片處理器的 Mac，反之亦然。您可以復原檔案和資料夾。

- 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

重要事項
從 C23.07 版開始，Cyber Protect Cloud 不支援下列作業系統：OS X Yosemite 10.10、OS X El Capitan 10.11 和 macOS Sierra 10.12。

強烈建議您將作業系統升級到支援的版本以確保相容性，而且才能夠使用 Cyber Protect Cloud 的完整功能。

VMware 用代理程式 (虛擬裝置)

此代理程式採虛擬裝置的形式提供，在 ESXi 主機上執行。

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

VMware 用代理程式 (Windows)

針對上列 Windows 用代理程式適用之任何作業系統，此代理程式採 Windows 應用程式的形式提供，但以下情形例外：

- 不支援 32 位元的作業系統。
- 不支援 Windows XP、Windows Server 2003/2003 R2 和 Windows Small Business Server 2003/2003 R2。

Hyper-V 用代理程式

- 擁有 Hyper-V 角色的 Windows Server 2008 (僅限 x64)，包括 Server Core 安裝模式
- 擁有 Hyper-V 角色的 Windows Server 2008 R2，包括 Server Core 安裝模式
- Microsoft Hyper-V Server 2008/2008 R2
- 擁有 Hyper-V 角色的 Windows Server 2012/2012 R2，包括 Server Core 安裝模式
- Microsoft Hyper-V Server 2012/2012 R2
- 帶 Hyper-V 的 Windows 8、8.1(僅限 x64)
- 帶 Hyper-V 的 Windows 10 – Pro，Education 和 Enterprise 版本
- 帶 Hyper-V 的 Windows 11 – Pro，Education 和 Enterprise 版本

- 擁有 Hyper-V 角色的 Windows Server 2016 – 所有安裝選項，Nano Server 除外
- Microsoft Hyper-V Server 2016
- 擁有 Hyper-V 角色的 Windows Server 2019 – 所有安裝選項，Nano Server 除外
- Microsoft Hyper-V Server 2019
- Windows Server 2022 – 所有安裝選項，Nano Server 除外

Virtuozzo 用代理程式

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

Virtuozzo Hybrid Infrastructure 用代理程式

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

Scale Computing HC3 用代理程式

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

oVirt 用代理程式

Red Hat Virtualization 4.2, 4.3, 4.4, 4.5

Synology 用代理程式

DiskStation Manager 6.2.x、7.x

Synology 用代理程式僅支援配備 x86_64 處理器的 NAS 裝置。不支援 ARM 處理器。請參閱 Synology 知識中心。

Cyber Protect Monitor

- Windows 7 和更新版本
- Windows Server 2008 R2 和更新版本
- Mac 用代理程式支援的所有 macOS 版本

支援的 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 版本也受到支援。

注意事項
僅在 NFTS、REFS 和 FAT32 檔案系統上執行的資料庫才支援 Microsoft SQL 備份。不支援 ExFat。

支援的 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、累計 Update 1 (CU1) 及更新版本。
- Microsoft Exchange Server 2010 – 所有版本、所有服務套件。從 Service Pack 1 (SP1) 開始，支援從資料庫備份進行信箱備份和細微復原。
- Microsoft Exchange Server 2007 – 所有版本、所有服務套件。並不支援從資料庫備份進行信箱備份和細微復原。

支援的 Microsoft SharePoint 版本

Cyber Protection 支援下列 Microsoft SharePoint 版本：

- 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*

*若要搭配使用 SharePoint Explorer 與這些版本，您需要 SharePoint 復原伺服器陣列來附加資料庫。

您要從中擷取資料的備份或資料庫，必須源自於已安裝 SharePoint Explorer 的相同 SharePoint 版本。

受支援的 Oracle 資料庫版本

- Oracle Database 11g 版，所有版本
- Oracle Database 12c 版，所有版本
- Oracle Database 19c 版，所有版本
- Oracle Database 21c 版，所有版本

僅支援單個執行個體組態。

支援的 SAP HANA 版本

HANA 2.0 SPS 03 已安裝在實體機器或 VMware ESXi 虛擬機器上所執行的 RHEL 7.6 中。

SAP HANA 不支援使用存放區快照復原多租用戶資料庫容器，因此這個解決方案支援只有一個租用戶資料庫的 SAP HANA 容器。

支援的 MySQL 版本

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

支援的 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

支援的虛擬化平台

下表概述各種虛擬化平台的支援情況。

如需有關代理程式型備份和無代理程式備份間差異的詳細資訊，請參閱 "代理程式型和無代理程式備份" (第 56 頁)。

注意事項
如果您使用以下未列出的虛擬化平台或版本，**代理程式型備份 (從客體作業系統內部備份)** 方法應該仍然可以在所有所需案例中正常運作。如果代理程式型備份發生問題，請聯絡支援團隊進行進一步調查。

VMware

平台	無代理程式備份 (Hypervisor 層級備份)	代理程式型備份 (從客體作業系統內進行備份)
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*	支援 **[裝置]** > **[新增]** > **[虛擬化主機]** > **[VMware ESXi]** > **[Windows 中安裝用代理程式]** 或 **[裝置]** > **[新增]** > **[虛擬化主機]**	支援 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**

平台	無代理程式備份 (Hypervisor 層級備份)	代理程式型備份 (從客體作業系統內進行備份)
VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	> **[VMware ESXi]** > **[虛擬裝置 (OVF)]**	
VMware vSphere Hypervisor (免費版 ESXi)**	不支援	支援 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**
VMware Server (VMware Virtual server) VMware Workstation VMware ACE VMware Player	不支援	支援 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**

* 在這些版本中，vSphere 5.0 及更新版本支援虛擬磁碟 HotAdd 傳輸。在版本 4.1 中，備份的執行速度較慢。

** vSphere Hypervisor 不支援在 Hypervisor 層級備份，因為此產品將對遠端命令列介面 (RCLI) 的存取限制為唯讀模式。在 vSphere Hypervisor 評估期內 (您尚未輸入序號前)，代理程式可正常運作。一旦您輸入序號，代理程式就會停止運作。

注意事項
Cyber Protect Cloud 正式支援受支援的主要 vSphere 版本內的任何更新。

例如，除非另有說明，否則 vSphere 8.0 支援包括對此版本內任何更新的支援。亦即，除了最初發佈的 vSphere 8.0，也支援 vSphere 8.0 Update 1。

支援特定 VMware vSphere 版本表示也支援對應版本的 vSAN。例如，支援 vSphere 8.0 表示也支援 vSAN 8.0。

限制

- **容錯機器**
  只有當 VMware vSphere 6.0 及更新版本啟用容錯時，VMware 用代理程式方能備份容錯機器。從較早的 vSphere 版本升級後，即可停用及啟用每台電腦的容錯。如果您使用較早的 vSphere 版本，請在客體作業系統中安裝代理程式。
- **獨立磁碟與 RDM**
  VMware 用代理程式不會備份實體相容性模式的原生裝置對應 (RDM) 磁碟或獨立磁碟。代理程式會跳過這些磁碟，並將警告寫入記錄。您可以從保護計劃中排除獨立磁碟與處於實體相容模

式的 RDM，以避免觸發警告。若您要備份這些磁碟或磁碟上面的資料，請在客體作業系統中安裝代理程式。

- **客體內 iSCSI 連線**
  VMware 用代理程式不會備份可在客體作業系統內運作的 iSCSI 啟動器所連線的 LUN 磁碟區。ESXi Hypervisor 不會察覺這種磁碟區，因此這些磁碟區不會包含在 Hypervisor 層級的快照中，而且會從備份中省略，但不會出現任何警告。如果您要備份這些磁碟區或這些磁碟區上的資料，請在客體作業系統中安裝代理程式。
- **加密虛擬機器** (VMware vSphere 6.5 提供)
  - 加密虛擬機器在解密狀態下備份。如果加密對您很重要，請在建立保護計劃時啟用備份加密。
  - 復原後的虛擬機器始終為解密狀態。完成復原後，可手動啟用加密。
  - 如果您要備份加密虛擬機器，建議您也對執行 VMware 用代理程式的虛擬機器加密。否則，對加密電腦的操作可能會慢於預期。使用 vSphere Web Client 對代理程式的電腦套用 **VM 加密原則**。
  - 即使您為代理程式設定了 SAN 傳輸模式，加密虛擬機器仍會透過 LAN 進行備份。由於 VMware 不支援採用 SAN 傳輸備份加密虛擬磁碟，所以代理程式會回復至 NBD 傳輸。
- **安全開機**
  - VMware 虛擬機器：(在 VMware vSphere 6.5 中推出) 虛擬機器復原為新的虛擬機器後，會停用**安全開機**。完成復原後，可手動啟用此選項。此限制適用於 VMware。
  - Hyper-V 虛擬機器：針對所有第 2 代虛擬機器，[安全開機] 會在機器復原到新的虛擬機器或現有的虛擬機器之後遭到停用。
- VMware vSphere 7.0 或更新版本不支援 **ESXi 設定備份**。
- **執行個體 UUID 為空白的虛擬機器不會出現在 Cyber Protect 主控台中**
  執行個體 `UUID` vSphere 屬性 (`vc.uuid`) 為空白的 VMware 虛擬機器不會列在 Cyber Protect 主控台中。如需有關如何解決此問題的詳細資訊，請參閱本知識庫文章。
- **保護代理程式的網路設定**
  如果保護代理程式無法將 vCenter 中註冊的 ESXi 主機的名稱解析為 IP 位址，即使可以解析 vCenter 主機名稱，VMware 虛擬機器的備份也可能會失敗。系統會顯示以下錯誤：「您無法存取此檔案。」
  若要解決此問題，請透過設定 DNS 或修改 `/etc/hosts` 檔案來編輯保護代理程式的網路設定。若要驗證修復情況，請在具有保護代理程式的電腦上，執行以下命令：

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

- **具有邏輯磁碟區的電腦支援的操作**
  支援使用邏輯磁碟區備份和復原工作負載，例如 Windows 中的 LDM (動態磁碟) 和 Linux 中的 LVM，但具備以下限制。如需有關這些限制的詳細資訊，請參閱 "支援的邏輯磁碟區操作" (第 52 頁)。

Microsoft

Hyper-V 虛擬機器 (在超融合叢集上執行，具有 Storage Spaces Direct (S2D)) 受到支援。Storage Spaces Direct 也受到支援作為備份儲存空間。

平台	無代理程式備份 (Hypervisor 層級備份)	代理程式型備份 (從客體作業系統內進行備份)
帶 Hyper-V 的 Windows Server 2008 (x64) 帶 Hyper-V 的 Windows Server 2008 R2 Microsoft Hyper-V Server 2008/2008 R2 帶 Hyper-V 的 Windows Server 2012/2012 R2 Microsoft Hyper-V Server 2012/2012 R2 帶 Hyper-V 的 Windows 8, 8.1 (x64) 帶 Hyper-V 的 Windows 10 帶 Hyper-V 的 Windows 11 Windows Server 2016 with Hyper-V – 所有安裝選項，Nano Server 除外 Microsoft Hyper-V Server 2016 Windows Server 2019 與 Hyper-V – 所有安裝選項，Nano Server 除外 Microsoft Hyper-V Server 2019 Windows Server 2022 with Hyper-V – 所有安裝選項，Nano Server 除外	支援 **[裝置]** > **[新增]** > **[虛擬化主機]** > **[Hyper-V]**	支援 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**
Microsoft Virtual PC 2004, 2007 Windows Virtual PC	不支援	支援 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**
Microsoft Virtual Server 2005	不支援	支援 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**

注意事項

支援在具有儲存空間直接存取 (S2D) 的超融合叢集上執行的 Hyper-V 虛擬機器。也支援儲存空間直接存取作為備份儲存空間。

限制

- **傳遞磁碟**

  Hyper-V 用代理程式不會備份傳遞磁碟。在備份期間，代理程式會跳過這些磁碟，並將警告寫入記錄。您可以從保護計劃中排除傳遞磁碟，以避免觸發警告。若您要備份這些磁碟或磁碟上面的資料，請在客體作業系統中安裝代理程式。

- **Hyper-V 客體叢集**

  Hyper-V 用代理程式不支援備份 Windows Server 容錯移轉叢集節點的 Hyper-V 虛擬機器。主機層級的 VSS 快照甚至可以暫時中斷外接式仲裁磁碟與叢集的連線。如果您要備份這些電腦，請在客體作業系統中安裝代理程式。

- **客體內 iSCSI 連線**

  Hyper-V 用代理程式不會備份可在客體作業系統內運作的 iSCSI 啟動器所連線的 LUN 磁碟區。Hyper-V Hypervisor 不會察覺這種磁碟區，因此這些磁碟區不會包含在 Hypervisor 層級的快照中，而且會從備份中省略，但不會出現任何警告。如果您要備份這些磁碟區或這些磁碟區上的資料，請在客體作業系統中安裝代理程式。

- **帶有 & 符號的 VHD/VHDX 檔案名稱**

  在執行 Windows Server 2016 或更新版本的 Hyper-V 主機上，如果其 VHD/VHDX 檔案的名稱包含 & 符號，則您無法備份原本使用 Hyper-V 2012 R2 或更舊版本建立的舊版虛擬機器 (5.0 版)。

  若要能夠備份此類電腦，請在 Hyper-V Manager 中，從虛擬機器卸離對應的虛擬磁碟、移除 & 符號來編輯 VHD/VHDX 檔案名稱，然後將磁碟附加回虛擬機器。

- **與 Microsoft WMI 子系統的相依性**

  Hyper-V 虛擬機器的無代理程式備份相依於 Microsoft WMI 子系統，特別是在 `Msvm_VirtualSystemManagementService` 類別。如果 WMI 查詢失敗，備份也將失敗。如需有關 `Msvm_VirtualSystemManagementService` 類別的詳細資訊，請參閱 Microsoft 文件。

- **具有 PMEM 磁碟的虛擬機器**

  不支援備份具有持續性記憶體 (PMEM) 磁碟的 Hyper-V 虛擬機器。

- **跨平台復原**

  如果 Hyper-V 用代理程式將另一個代理程式建立的備份復原為新的 Hyper-V 虛擬機器，則產生的電腦為第一代。

- **安全開機**

  為確保復原的第 2 代 Hyper-V 虛擬機器能夠開機，會停用 [安全開機]。您可以使用 Hyper-V 管理工具，手動重新啟用 [安全開機]。如需有關 [安全開機] 和第 2 代虛擬機器的詳細資訊，請參閱 Microsoft 文件。

- **Linux 虛擬機器的當機一致備份**

  基於 Microsoft 的限制 (無法為 Linux 虛擬機器建立實際運作檢查點)，在 Hyper-V 2019 主機上執行的 Linux 虛擬機器的備份會容錯移轉到當機一致快照。為避免在備份期間出現警告，請在保護計劃中停用 [虛擬機器的 VSS]備份選項。

- **正在從備份執行虛擬機器**
  如果備份與為裝載的 VM 磁碟所選擇的路徑位於相同的磁碟區上，則從 Hyper-V 主機上的備份執行虛擬機器將會失敗。若要解決此問題，請為裝載的 VM 磁碟的路徑選擇不同的磁碟區。此空間將僅用於已裝載的虛擬機器內部產生的變更，而且將不會佔用虛擬磁碟的整個大小。
- **具有邏輯磁碟區的電腦支援的操作**
  支援使用邏輯磁碟區備份和復原工作負載，例如 Windows 中的 LDM (動態磁碟) 和 Linux 中的 LVM，但具備以下限制。如需有關這些限制的詳細資訊，請參閱 "支援的邏輯磁碟區操作" (第 52 頁)。

Scale Computing

平台	無代理程式備份 (Hypervisor 層級備份)	代理程式型備份 (從客體作業系統內進行備份)
Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3	支援 **[裝置]** > **[新增]** > **[虛擬化主機]** > **[Scale Computing HC3]**	支援 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**

限制

具有邏輯磁碟區的電腦支援的操作

支援使用邏輯磁碟區備份和復原工作負載，例如 Windows 中的 LDM (動態磁碟) 和 Linux 中的 LVM，但具備以下限制。如需有關這些限制的詳細資訊，請參閱 "支援的邏輯磁碟區操作" (第 52 頁)。

Citrix

平台	無代理程式備份 (Hypervisor 層級備份)	代理程式型備份 (從客體作業系統內進行備份)
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	不支援	僅支援完全虛擬化 (亦即 HVM) 的客體。不支援半虛擬化 (亦即 PV) 的客體。 **[裝置]** > **[新增]** > **[虛擬化主機]** > **[Citrix XenServer]** > **[Windows]** 或 **[Linux]**

Red Hat 和 Linux

平台	無代理程式備份 (Hypervisor 層級備份)	代理程式型備份 (從客體作業系統內進行備份)
Red Hat Enterprise Virtualization	不支援	支援

平台	無代理程式備份 (Hypervisor 層級備份)	代理程式型備份 (從客體作業系統內進行備份)
(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		**[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**
Red Hat Virtualization (受 oVirt 管理) 4.2、4.3、4.4、4.5	支援 **[裝置]** > **[新增]** > **[虛擬化主機]** > **[Red Hat Virtualization (oVirt)]**	支援 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**
核心虛擬機器 (KVM)	不支援	支援 **[裝置]** > **[新增]** > **[KVM]** > **[Windows]** 或 **[Linux]**
由 Red Hat Enterprise Linux 7.6、7.7 或 CentOS 7.6、7.7 上執行的 oVirt 4.3 所管理的核心虛擬機器 (KVM)	支援 **[裝置]** > **[新增]** > **[虛擬化主機]** > **[Red Hat Virtualization (oVirt)]**	支援 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**
由 Red Hat Enterprise Linux 8.x 或 CentOS Stream 8.x 上執行的 oVirt 4.4 所管理的核心虛擬機器 (KVM)	支援 **[裝置]** > **[新增]** > **[虛擬化主機]** > **[Red Hat Virtualization (oVirt)]**	支援 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**
由 Red Hat Enterprise Linux 8.x 或 CentOS Stream 8.x 上執行的 oVirt 4.5 所管理的核心虛擬機器 (KVM)	支援 **[裝置]** > **[新增]** > **[虛擬化主機]** > **[Red Hat Virtualization (oVirt)]**	支援 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**

限制

具有邏輯磁碟區的電腦支援的操作

支援使用邏輯磁碟區備份和復原工作負載，例如 Windows 中的 LDM (動態磁碟) 和 Linux 中的 LVM，但具備以下限制。如需有關這些限制的詳細資訊，請參閱 "支援的邏輯磁碟區操作" (第 52 頁)。

Parallels

平台	無代理程式備份 (Hypervisor 層級備份)	代理程式型備份 (從客體作業系統內進行備份)
Parallels Workstation	不支援	支援 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**
Parallels Server 4 Bare Metal	不支援	支援 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**

Oracle

平台	無代理程式備份 (Hypervisor 層級備份)	代理程式型備份 (從客體作業系統內進行備份)
Oracle Virtualization Manager (以 oVirt 為基礎)* 4.3	支援 **[裝置]** > **[新增]** > **[虛擬化主機]** > **[Red Hat Virtualization (oVirt)]**	支援 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**
Oracle VM Server 3.0, 3.3, 3.4	不支援	僅支援完全虛擬化 (亦即 HVM) 的客體。不支援半虛擬化 (亦即 PV) 的客體。 **[裝置]** > **[新增]** > **[虛擬化主機]** > **[Oracle]** > **[Windows]** 或 **[Linux]**
Oracle VM VirtualBox 4.x	不支援	支援 **[裝置]** > **[新增]** > **[虛擬化主機]** > **[Oracle]** > **[Windows]** 或 **[Linux]**

*Oracle Virtualization Manager 受到 oVirt 用代理程式的支援。

限制

具有邏輯磁碟區的電腦支援的操作

支援使用邏輯磁碟區備份和復原工作負載，例如 Windows 中的 LDM (動態磁碟) 和 Linux 中的 LVM，但具備以下限制。如需有關這些限制的詳細資訊，請參閱 "支援的邏輯磁碟區操作" (第 52 頁)。

Nutanix

平台	無代理程式備份 (Hypervisor 層級備份)	代理程式型備份 (從客體作業系統內進行備份)
Nutanix Acropolis Hypervisor (AHV) 20160925.x 到 20180425.x	不支援	支援 **[裝置]** > **[新增]** > **[虛擬化主機]** > **[Nutanix AHV]** > **[Windows]** 或 **[Linux]**

Virtuozzo

平台	無代理程式備份 (Hypervisor 層級備份)	代理程式型備份 (從客體作業系統內進行備份)
Virtuozzo 6.0.10, 6.0.11, 6.0.12	支援 **[裝置]** > **[新增]** > **[虛擬化主機]** > **[Virtuozzo]**	僅支援虛擬機器。不支援容器。 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**
Virtuozzo 7.0.13, 7.0.14	僅支援 Ploop 容器。不支援虛擬機器。 **[裝置]** > **[新增]** > **[虛擬化主機]** > **[Virtuozzo]**	僅支援虛擬機器。不支援容器。 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**
Virtuozzo Hybrid Server 7.5	支援 **[裝置]** > **[新增]** > **[虛擬化主機]** > **[Virtuozzo]**	僅支援虛擬機器。不支援容器。 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**

限制

具有邏輯磁碟區的電腦支援的操作

支援使用邏輯磁碟區備份和復原工作負載，例如 Windows 中的 LDM (動態磁碟) 和 Linux 中的 LVM，但具備以下限制。如需有關這些限制的詳細資訊，請參閱 "支援的邏輯磁碟區操作" (第 52 頁)。

Virtuozzo Hybrid Infrastructure

平台	無代理程式備份 (Hypervisor 層級備份)	代理程式型備份 (從客體作業系統內進行備份)
Virtuozzo Hybrid Infrastructure 3.5, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0	支援 **[裝置]** > **[新增]** > **[虛擬化主機]** > **[Virtuozzo Hybrid Infrastructure]**	支援 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**

限制

- **使用外接式 iSCSI 儲存裝置上的磁碟對 VM 進行無代理程式備份**
  如果 VM 磁碟置於外接式 iSCSI 磁碟區 (附掛到 VHI 叢集) 上，則您無法從 Virtuozzo Hybrid Infrastructure 備份 VM。
- **具有邏輯磁碟區的電腦支援的操作**
  支援使用邏輯磁碟區備份和復原工作負載，例如 Windows 中的 LDM (動態磁碟) 和 Linux 中的 LVM，但具備以下限制。如需有關這些限制的詳細資訊，請參閱 "支援的邏輯磁碟區操作" (第 52 頁)。

Amazon

平台	無代理程式備份 (Hypervisor 層級備份)	代理程式型備份 (從客體作業系統內進行備份)
Amazon EC2 執行個體	不支援	支援 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**

Microsoft Azure

平台	無代理程式備份 (Hypervisor 層級備份)	代理程式型備份 (從客體作業系統內進行備份)
Azure 虛擬機器	支援 **[裝置]** > **[新增]** > **[Microsoft Azure 虛擬機器]**	支援 **[裝置]** > **[新增]** > **[工作站]** 或 **[伺服器]** > **[Windows]** 或 **[Linux]**

與加密軟體的相容性

透過*檔案層級*加密軟體加密的資料無備份和復原限制。

*磁碟層級*加密軟體會即時加密資料。這就是備份中包含的資料並未加密的原因。磁碟層級加密軟體經常會修改系統區域:開機記錄、磁碟分割表或檔案系統表。這些因素會影響磁碟層級的備份和復原,以及已復原系統開機和存取 Secure Zone 的能力。

您可對採用以下磁碟層級加密軟體加密的資料進行備份:

- Microsoft BitLocker 磁碟加密
- McAfee 端點加密
- PGP Whole Disk Encryption

若要確保可靠的磁碟層級復原,請遵循一般規則和特定軟體的建議。

一般安裝規則

強烈建議您先安裝加密軟體,再安裝保護代理程式。

使用 Secure Zone 的方法

Secure Zone 不得以磁碟層級加密的方式加密。使用 Secure Zone 的唯一方法如下:

1. 安裝加密軟體,然後安裝代理程式。
2. 建立 Secure Zone。
3. 加密磁碟或其磁碟區時,排除 Secure Zone。

一般備份規則

您可以在作業系統中執行磁碟層級備份。

軟體特定的復原程序

Microsoft BitLocker 磁碟機加密

復原由 BitLocker 加密的系統:

1. 從可開機媒體開機。
2. 復原系統。復原後的資料將會解密。
3. 將已復原的系統重新開機。
4. 開啟 BitLocker。

如果您只需要復原多重磁碟分割磁碟的其中一個磁碟分割,請在作業系統中進行。在可開機媒體下復原可能會使得 Windows 偵測不到復原的磁碟分割。

McAfee 端點加密和 PGP 全磁碟機加密

您只能使用可開機媒體復原加密的系統磁碟分割。

如果復原後的系統無法開機,請依照下列 Microsoft 知識庫文章的說明,重新建立主開機記錄:
https://support.microsoft.com/kb/2622803

與 Dell EMC Data Domain 儲存空間的相容性

您可以將 Dell EMC Data Domain 裝置用作備份儲存空間。

對於此儲存，建議您使用定期建立完整備份的備份配置，例如 **[一律完整]**。若要深入瞭解可用的備份配置，請參閱 "備份配置" (第 371 頁)。

保留鎖定

支援保留鎖定 (治理模式)。如果在 Data Domain 儲存空間上啟用保留鎖定，您必須將 AR_RETENTION_LOCK_SUPPORT 環境變數新增至具有使用此儲存空間作為備份目的地之保護代理程式的電腦上。如需詳細資訊，請參閱 "新增 AR_RETENTION_LOCK_SUPPORT 變數" (第 41 頁)。

注意事項
Mac 用代理程式不支援啟用保留鎖定的 Dell EMC Data Domain 儲存空間。

如果在 Data Domain 儲存空間上啟用了保留鎖定，則保護計劃中的保留規則不會刪除儲存空間上的備份。系統將不會顯示任何錯誤。當保留鎖定到期並再次套用保留規則時，備份將遭到刪除。

根據保護計劃的設定，保留規則會在備份之前或之後套用到存檔。

新增 AR_RETENTION_LOCK_SUPPORT 變數

如果在 Data Domain 儲存空間上啟用保留鎖定，您必須將 AR_RETENTION_LOCK_SUPPORT 環境變數新增至具有使用此儲存空間作為備份目的地之保護代理程式的電腦上。

若要新增 AR_RETENTION_LOCK_SUPPORT 環境變數

在 Windows 中

1. 以系統管理員身分，登入具有保護代理程式的電腦。
2. 在 **[控制台]** 中，前往 **[系統及安全性]** > **[系統]** > **[進階系統設定]**。
3. 在 **[進階]** 索引標籤上，按一下 **[環境變數]**。
4. 在 **[系統變數]** 面板中，按一下 **[新增]**。
5. 在 **[新增系統變數]** 視窗中新增變數，如下所示：
   - 變數名稱：AR_RETENTION_LOCK_SUPPORT
   - 變數值：1
6. 按一下 **[確定]**。
7. 在 **[環境變數]** 視窗中，按一下 **[確定]**。
8. 重新啟動機器。

在 Linux 中

1. 以系統管理員身分，登入具有保護代理程式的電腦。
2. 前往 /sbin 目錄，然後開啟 acronis_mms 檔案進行編輯。
3. 在 export LD_LIBRARY_PATH 行上方，新增下行：

```
export AR_RETENTION_LOCK_SUPPORT=1
```

4. 儲存 acronis_mms 檔案。
5. 重新啟動機器。

在虛擬裝置中

1. 以系統管理員的身分，登入虛擬裝置。
2. 前往 /bin 目錄，然後開啟 autostart 檔案進行編輯。
3. 在 export LD_LIBRARY_PATH 行下方，新增下行：

```
export AR_RETENTION_LOCK_SUPPORT=1
```

4. 儲存 autostart 檔案。
5. 重新啟動虛擬裝置。

作業系統支援的保護功能

本主題包含 Cyber Protect Cloud 保護功能的相關資訊。其不會列出備份和復原功能。

只有已安裝保護代理程式的電腦才支援保護功能。這些功能不適用於在無代理程式模式下 (例如，Hyper-V 用代理程式、VMware 用代理程式、Virtuozzo Hybrid Infrastructure 用代理程式、Scale Computing 用代理程式或 oVirt 用代理程式) 備份的虛擬機器。

部分功能可能需要額外的授權，端視適用的授權模型而定。

支援的作業系統和版本

Windows

除非針對特定功能集另有說明，否則支援以下 Windows 版本：

- Windows 7 Service Pack 1 和更新版本
- Windows Server 2008 R2 Service Pack 1 和更新版本

注意事項
若是 Windows 7，您必須先安裝以下 Microsoft 更新，然後再安裝保護代理程式。

- Windows 7 Extended Security Updates (ESU)
- KB4474419
- KB4490628

有關所需更新的詳細資訊，請參閱本知識庫文章。

Linux

支援的 Linux 發行版及其版本取決於功能集，而且顯示在每個表格的底部。

macOS

支援的 macOS 版本取決於功能集，而且顯示在每個表格的底部。

功能集	Windows	Linux	macOS
預設保護計劃			
遠端工作者	是	否	否
辦公室工作者 (第三方防毒軟體)	是	否	否
辦公室工作者 (Cyber Protect 防毒軟體)	是	否	否
Cyber Protect Essentials (僅適用於 Cyber Protect Essentials 版本)	是	否	否
請參閱 "支援的作業系統和版本" (第 42 頁) 中支援的 Windows 版本。			

功能集	Windows	Linux	macOS
鑑識備份			
收集記憶體傾印	是	否	否
執行中程序的快照	是	否	否
公證本機映像鑑識備份	是	否	否
公證雲端映像鑑識備份	是	否	否
請參閱 "支援的作業系統和版本" (第 42 頁) 中支援的 Windows 版本。			

功能	Windows	Linux	macOS
連續資料保護 (CDP)			
針對檔案與資料夾進行 CDP	是	否	否
針對已變更的檔案，透過應用程式追蹤進行 CDP	是	否	否
請參閱 "支援的作業系統和版本" (第 42 頁) 中支援的 Windows 版本。			

功能集	Windows	Linux	macOS
自動探索和遠端安裝			
網路型探索	是	否	否
Active Directory 型探索	是	否	否
範本型探索 (從檔案匯入電腦)	是	否	否

功能集	Windows	Linux	macOS
自動探索和遠端安裝			
手動新增裝置	是	否	否
請參閱 "支援的作業系統和版本" (第 42 頁) 中支援的 Windows 版本。			

功能集	Windows	Linux	macOS
Active Protection			
程序插入偵測	是	否	否
從本機快取自動復原受影響的檔案	是	是	是
Acronis 備份檔案的自我防衛	是	否	否
Acronis 軟體的自我防衛	是	否	是 (僅限 Active Protection 和防惡意程式碼元件)
受信任/遭到封鎖的程序管理	是	否	是
程序/資料夾排除	是	是	是
根據程序行為 (基於 AI) 進行勒索軟體偵測	是	是	是
根據程序行為進行加密採礦程序偵測	是	否	否
外接磁碟機保護 (HDD、快閃磁碟機、SD 卡)	是	否	是
網路資料夾保護	是	是	是
伺服器端保護	是	否	否
Zoom、Cisco Webex、Citrix Workspace 和 Microsoft Teams 保護	是	否	否
如需有關支援的作業系統及其版本的詳細資訊，請參閱 "支援防毒和防惡意軟體防護的作業系統" (第 729 頁)。			

功能集	Windows	Linux	macOS
防毒和反惡意程式碼保護			
完全整合的 Active Protection 功能	是	否	否

功能集	Windows	Linux	macOS
防毒和反惡意程式碼保護			
即時反惡意軟體防護	是	是，含進階防惡意軟體套件	是，含進階防惡意軟體套件
包含本機特徵比對偵測的進階即時反惡意程式碼保護	是	是	是
針對可攜式可執行檔進行靜態分析	是	否	是*
按需反惡意程式碼掃描	是	是**	是
網路資料夾保護	是	是	否
伺服器端保護	是	否	否
掃描存檔檔案	是	否	是
掃描卸除式磁碟機	是	否	是
僅掃描新的和已變更的檔案	是	否	是
檔案/資料夾排除	是	是	是***
程序排除	是	否	是
行為分析引擎	是	否	是
漏洞利用防禦	是	否	否
隔離	是	是	是
隔離區自動清理	是	是	是
URL 篩選 (http/https)	是	否	否
全公司的白名單	是	否	是
防火牆管理****	是	否	否
Microsoft Defender 防毒軟體管理*****	是	否	否
Microsoft Security Essentials 管理	是	否	否
透過 Windows Security Center 註冊並管理防毒和反惡意程式碼保護	是	否	否
如需有關支援的作業系統及其版本的詳細資訊，請參閱 "支援防毒和防惡意軟體防護的作業系統" (第 729 頁)。			

* 只有在 macOS 上的排程掃描才支援針對可攜式可執行檔進行靜態分析。

** Linux 上的按需掃描不支援開始條件。

*** 只有在 macOS 上指定即時保護或排程掃描將不會掃描的檔案和資料夾時，才支援檔案/資料夾排除。

**** Windows 8 和更新版本支援防火牆管理。不支援 Windows Server。

***** Windows 8.1 和更新版本支援 Microsoft Defender 防毒軟體管理。

功能集	Windows	Linux	macOS
弱點評估			
作業系統及其原生應用程式的弱點評估	是	是******	是
適用於協力廠商應用程式的弱點評估	是	否	是
如需有關支援的作業系統及其版本的詳細資訊，請參閱 "支援的 Microsoft 和第三方產品" (第 869 頁)、"支援的 Linux 產品" (第 871 頁) 和 "支援的 Apple 和協力廠商產品" (第 871 頁)。			

****** 弱點評估取決於是否提供特定發行版的官方安全公告，例如 https://lists.centos.org/pipermail/centos-announce、https://lists.centos.org/pipermail/centos-cr-announce 等等。

功能集	Windows	Linux	macOS
修補程式管理			
修補程式自動核准	是	否	否
修補程式自動安裝	是	否	否
修補程式測試	是	否	否
修補程式手動安裝	是	否	否
修補程式排程	是	否	否
故障移轉修補：安裝修補程式作為保護計劃一部分之前備份電腦	是	否	否
如果備份正在執行，則取消電腦重新開機	是	否	否
請參閱 "支援的作業系統和版本" (第 42 頁) 中支援的 Windows 版本。			

功能	Windows	Linux	macOS
資料保護圖			
可調整的重要檔案定義	是	否	否

功能	Windows	Linux	macOS
資料保護圖			
掃描電腦以尋找未受保護的檔案	是	否	否
未受保護的位置概觀	是	否	否
能夠從資料保護圖桌面小工具啟動保護動作 (**[保護所有檔案]** 動作)	是	否	否
請參閱 "支援的作業系統和版本" (第 42 頁) 中支援的 Windows 版本。			

功能集	Windows	Linux	macOS
磁碟健全狀況			
基於 AI 的 HDD 和 SSD 健全狀況控制	是	否	否
請參閱 "支援的作業系統和版本" (第 42 頁) 中支援的 Windows 版本。			

功能	Windows	Linux	macOS
以 Acronis 網路保護營運中心 (CPOC) 警示為基礎的智慧型保護計劃			
威脅摘要	是	否	否
修復精靈	是	否	否
請參閱 "支援的作業系統和版本" (第 42 頁) 中支援的 Windows 版本。			

功能集	Windows	Linux	macOS
備份掃描			
映像備份的反惡意程式碼掃描是備份計劃的一部分	是	否	否
掃描雲端的映像備份中是否有惡意程式碼	是	否	否
加密備份的惡意程式碼掃描	是	否	否
請參閱 "支援的作業系統和版本" (第 42 頁) 中支援的 Windows 版本。			

功能集	Windows	Linux	macOS
安全復原			
在復原過程中, 使用防毒和反惡意程式碼保進行反惡意程式碼掃描	是	否	否
加密備份的安全復原	是	否	否
請參閱 "支援的作業系統和版本" (第 42 頁) 中支援的 Windows 版本。			

功能集	Windows	Linux	macOS
遠端桌面連線			
透過 NEAR 連線	是	是	是
透過 RDP 連線	是	否	否
透過 [Apple 畫面共用] 連線	否	否	是
透過 Web 用戶端連線	是	否	否
透過 快速協助 連線	是	是	是
遠端協助	是	是	是
檔案傳輸	是	是	是
螢幕擷取畫面傳輸	是	是	是
如需有關支援的作業系統及其版本的詳細資訊，請參閱 "支援的平台" (第 901 頁)。			

功能集	Windows	Linux	macOS
#CyberFit 分數			
#CyberFit 分數狀態	是	否	否
#CyberFit 分數獨立工具	是	否	否
#CyberFit 分數建議	是	否	否
請參閱 "支援的作業系統和版本" (第 42 頁) 中支援的 Windows 版本。			

功能集	Windows	Linux	macOS
資料洩漏防禦			
裝置控制	是	否	在配備執行 macOS 10.15 和更新版本或 macOS 11.2.3 或更新版本的 Intel 處理器的 Mac 上支援。 在 ARM 型

功能集	Windows	Linux	macOS
資料洩漏防禦			
			Apple Silicon 處理器 (例如 Apple M1/M2) 上不支援。
Advanced Data Loss Prevention	是	否	否
請參閱 "支援的作業系統和版本" (第 42 頁) 中支援的 Windows 版本。			

功能集	Windows	Linux	macOS
管理選項			
宣傳 Cyber Protect 版本的追加銷售案例	是	是	是
網頁型集中式與遠端管理主控台	是	是	是
支援的作業系統和版本:不受限於平台。			

功能集	Windows	Linux	macOS
保護選項			
遠端抹除	是	否	否
支援 Windows 10 和更新版本。			

功能集	Windows	Linux	macOS
Cyber Protect Monitor			
Cyber Protect 應用程式	是	否	是
Zoom 的保護狀態	是	否	否
Cisco Webex 的保護狀態	是	否	否
Citrix Workspace 的保護狀態	是	否	否
Microsoft Teams 的保護狀態	是	否	否
請參閱 "支援的作業系統和版本" (第 42 頁) 中支援的 Windows 版本。 在 macOS 上, 您可以安裝 Mac 用代理程式的所有版本都支援 Cyber Protect Monitor。如需詳細資訊, 請參閱 "Mac 用代理程式" (第 26 頁)。			

功能集	Windows	Linux	macOS
軟體清查			
軟體清查掃描	是	否	是
軟體清查監視	是	否	是
請參閱 "支援的作業系統和版本" (第 42 頁) 中支援的 Windows 版本。 在 macOS 上，10.13.x – 13.x 版支援軟體清查。			

功能集	Windows	Linux	macOS
硬體清查			
硬體清查掃描	是	否	是
硬體清查監視	是	否	是
請參閱 "支援的作業系統和版本" (第 42 頁) 中支援的 Windows 版本。 在 macOS 上，10.13.x – 13.x 版支援硬體清查。			

支援的檔案系統

保護代理程式能夠備份可從安裝代理程式所在的作業系統存取的任何檔案系統。例如，如果 Windows 中安裝了對應的磁碟機，Windows 用代理程式便可以備份及復原 ext4 檔案系統。

下表摘述可以備份和復原的檔案系統 (可開機媒體僅支援復原)。限制適用於代理程式和可開機媒體。

檔案系統	支援			限制
	代理程式	Windows 和 Linux 可開機媒體	Mac 可開機媒體	
FAT16/32	所有代理程式	+	+	無限制
NTFS	所有代理程式	+	+	
ext2/ext3/ext4	所有代理程式	+	-	
HFS+	Mac 用代理程式	-	+	

檔案系統	支援			限制
	代理程式	Windows 和 Linux 可開機媒體	Mac 可開機媒體	
APFS	Mac 用代理程式	-	+	• 支援從 Mac OS High Sierra 10.13 開始 • 復原至非原始電腦或裸機時，應手動重新建立磁碟組態。
JFS	Linux 用代理程式	+	-	• 不支援檔案篩選 (包含/排除) • 無法啟用快速增量/差異備份
ReiserFS3	Linux 用代理程式	+	-	
ReiserFS4	Linux 用代理程式	+	-	• 不支援檔案篩選 (包含/排除) • 無法啟用快速增量/差異備份 • 復原期間無法調整磁碟區大小
ReFS	所有代理程式	+	+	• 不支援檔案篩選 (包含/排除) • 無法啟用快速增量/差異備份 • 復原期間無法調整磁碟區大小 • 在從 ReFS 備份復原檔案期間，只會復原內容。不會復原存取控制清單 (ACL) 和替代串流。疏鬆檔案會當作一般檔案復原。
XFS	所有代理程式	+	+	• 不支援檔案篩選 (包含/排除) • 無法啟用快速增量/差異備份 • 復原期間無法調整磁碟區大小 • XFS 檔案系統不支援快速增量備份模式。XFS 磁碟區至雲端的增量備份與差異備份，可能會比使用快速增量模式的可比 ext4 備份慢上許多。
Linux swap	Linux 用代理程式	+	-	無限制
exFAT	所有代理程式	+ 如果備份是*儲存在* exFAT	+	• 僅支援磁碟/磁碟區備份 • 不支援檔案篩選 (包含/排除) • 個別檔案無法從備份中復原

檔案系統	支援			限制
	代理程式	Windows 和 Linux 可開機媒體	Mac 可開機媒體	
		上，則可開機媒體無法用於復原。		

在備份具有無法識別或不支援檔案系統 (例如 Btrfs) 的磁碟機時，軟體會自動切換至「逐一磁區」模式。以下任何檔案系統均可進行逐一磁區備份：

- 基於區塊的檔案系統
- 橫跨單一磁碟的檔案系統
- 具有標準 MBR/GPT 磁碟分割配置的檔案系統

如果檔案系統不符合這些要求，備份便會失敗。

重複資料刪除

在 Windows Server 2012 和更新版本中，您可以為 NTFS 磁碟區啟用重複資料刪除功能。重複資料刪除會將磁碟區檔案的重複片段只儲存一次，來減少磁碟區上已使用的空間。

您可以於磁碟層級備份和復原已啟用重複資料刪除的磁碟區，不受任何限制。支援檔案層級備份，但在使用 Acronis VSS Provider 時除外。若要從磁碟備份復原檔案，請從備份執行虛擬機器，或在執行 Windows Server 2012 或更新版本的電腦上掛載備份，然後從已掛載磁碟區中複製檔案。

Windows Server 的 [重複資料刪除] 功能與 Acronis Backup 的 [重複資料刪除] 功能無關。

支援的邏輯磁碟區操作

支援使用邏輯磁碟區備份和復原工作負載，例如 Windows 中的 LDM (動態磁碟) 和 Linux 中的 LVM，但具備以下限制。

備份

代理程式型備份是由安裝在工作負載上的保護代理程式或可開機媒體所建立的備份。

無代理程式備份僅適用於虛擬機器。無代理備份是由可以備份和復原環境中所有虛擬機器的代理程式，在 Hypervisor 層級上執行的。受保護的虛擬機器上未安裝個別的代理程式。

如需有關代理程式型備份和無代理程式備份間差異的詳細資訊，請參閱 "代理程式型和無代理程式備份" (第 56 頁)。

代理程式型備份	無代理程式備份
• 邏輯磁碟區是逐磁碟區備份的。 • 支援檔案篩選 (包含/排除)。	• 在磁碟上偵測到邏輯磁碟區時，磁碟將以逐一磁區 (RAW) 模式備份。系統不會分析磁碟的磁碟分

代理程式型備份	無代理程式備份
	割結構，也不會另外儲存磁碟區映像。 • 無法透過直接選擇或使用原則規則來選擇個別 LDM 或 LVM 磁碟區作為備份來源。保護計劃的 **[備份內容]** 區段僅能使用 **[整部電腦]**。 • 不支援檔案篩選 (包含/排除)。已設定的任何包含項目或排除項目都將遭到忽略。

復原

代理程式型復原是由安裝在工作負載上的代理程式或可開機媒體所執行的復原。

無代理程式復原僅支援虛擬機器作為目標。無代理程式復原是由可以備份和復原環境中所有虛擬機器的代理程式在 Hypervisor 層級上執行的。您不必手動建立在其中復原備份的目標電腦。

	來自代理程式型備份	來自無代理程式備份
代理程式型復原	• 可以使用按磁碟區復原。 • 可以使用檔案和資料夾復原。	• 無法使用按磁碟區復原。 • 可以使用檔案和資料夾復原。
無代理程式復原	• 不支援電腦遷移 (P2V、V2P 和 V2V)。若要從代理程式型備份復原資料，請使用可開機媒體。 • 不支援 **[以 VM 的身分執行]** 操作。 • 可以使用檔案和資料夾復原。	• 無法使用按磁碟區復原。 • 可以使用整部電腦復原。 • 可以使用檔案和資料夾復原。 • 支援 **[以 VM 的身分執行]** 操作。若要將虛擬機器設為可開機，您可能需要變更開機順序。如需詳細資訊，請參閱本知識庫文章。 • 支援轉換為以下類型的虛擬機器： ◦ VMware ESXi ◦ Microsoft Hyper-V ◦ Scale Computing HC3

安裝並部署 Cyber Protection 代理程式

在您開始之前

準備

步驟 1

選擇代理程式，視您要備份的內容而定。如需有關可能選擇的詳細資訊，請參閱我需要哪種代理程式？

步驟 2

請確認您的硬碟上有足夠的可用空間，才能安裝代理程式。如需有關所需空間的詳細資訊，請參閱 "代理程式的系統需求" (第 60 頁)。

步驟 3

下載安裝程式。若要尋找下載連結，請按一下 **[所有裝置]** > **[新增]**。

[新增裝置] 頁面會針對 Windows 中安裝的每個代理程式提供 Web 安裝程式。Web 安裝程式是一個小型的可執行檔，它會從網際網路下載主要的安裝程式，並將其儲存為暫存檔。安裝完成後會立即將檔案刪除。

若要在本機儲存安裝程式，請使用 **[新增裝置]** 頁面底部的連結，下載包含在 Windows 中安裝之所有代理程式的套件。提供 32 位元和 64 位元套件。這些套件可讓您自訂要安裝的元件清單。這些套件也可讓您進行自動安裝，例如透過群組原則。此進階案例詳述於 "透過群組原則部署保護代理程式" (第 120 頁) 中。

若要下載 Microsoft 365 用代理程式的安裝程式，請按一下右上角的帳戶圖示，然後按一下 **[下載]** > **[Microsoft 365 用代理程式]**。

Linux 和 macOS 中的安裝是從一般安裝程式執行。

所有安裝程式都需要網際網路連線，才能在 Cyber Protection 服務中登錄電腦。如果沒有網際網路連線，安裝將無法成功執行。

步驟 4

Cyber Protect 功能需要使用 Microsoft Visual C++ 2017 可轉散發套件。請確認已在電腦上安裝該可轉散發套件，或在安裝代理程式前加以安裝。安裝 Microsoft Visual C++ 後，可能需要重新啟動。您可以在以下網址找到 Microsoft Visual C++ 可轉散發套件：https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows。

步驟 5

請確認您的防火牆及網路安全性系統的其他元件 (例如 Proxy 伺服器) 允許透過下列 TCP 連接埠的輸出連線。

- 連接埠 **443** 和 **8443**

  這些連接埠用於存取 Cyber Protect 主控台、註冊代理程式、下載憑證、使用者授權，以及從雲端儲存空間下載檔案。
- 範圍 **7770 – 7800** 的連接埠

  代理程式使用這些連接埠與管理伺服器進行通訊。
- 連接埠 **44445** 和 **55556**

  代理程式使用這些連接埠在備份和復原期間進行資料傳輸。

如果您的網路中已啟用 Proxy 伺服器，請參閱 "設定 Proxy 伺服器設定" (第 66 頁)，瞭解您是否需要在每部執行保護代理程式的電腦上進行這些設定。

從雲端管理代理程式所需的最低網際網路連線速度為每秒 1 Mbit (請不要與備份至雲端可接受的資料傳輸速率混淆)。如果您使用的是低頻寬的連線技術 (如 ADSL)，請考慮此情況。

需要有 TCP 連接埠才能備份和複寫 VMware 虛擬機器

- 連接埠 **443**

  VMware 用代理程式 (Windows 和虛擬裝置) 會連線到 ESXi 主機/vCenter 伺服器上的這個連接埠以執行 VM 管理作業，例如，在備份、復原和 VM 複寫作業期間，於 vSphere 上建立、更新與刪除 VM。
- 連接埠 **902**

  VMware 用代理程式 (Windows 和虛擬裝置) 會連線到 ESXi 主機上的這個連接埠建立 NFC 連線，以便在備份、復原和 VM 複寫作業期間，讀取/寫入 VM 磁碟上的資料。
- 連接埠 **2029**

  VMware 用代理程式 (虛擬裝置) 會在此連接埠監聽代理程式上託管的 NFS 伺服器的傳入要求。您必須透過此連接埠連線，才能從備份 (立即還原) 執行虛擬機器。
- 連接埠 **3333**

  如果 VMware 用代理程式 (虛擬裝置) 在 VM 複寫目標的 ESXi 主機/叢集上執行，則 VM 複寫流量不會直接進入連接埠 **902** 上的 ESXi 主機。但是，該流量會從來源 VMware 用代理程式進入位於目標 ESXi 主機/叢集之 VMware 用代理程式 (虛擬裝置) 上的 TCP 連接埠 **3333**。

  從原始 VM 磁碟讀取資料的 VMware 用代理程式可以在其他任何地方，而且可以是任何類型：虛擬裝置或 Windows。

  負責在目標 VMwar 用代理程式 (虛擬裝置) 上接受 VM 複寫資料的服務稱為「複本磁碟伺服器」。此服務負責 WAN 最佳化技術 (例如，在 VM 複寫期間的流量壓縮和重複資料刪除)，包括複本植入 (請參閱植入初始複本)。在目標 ESXi 主機上沒有執行任何 VMware 用代理程式 (虛擬裝置) 時，無法使用此服務此服務，因此不支援複本植入案例。

Downloader 元件所需的連接埠

Downloader 元件負責將更新提供給電腦，並將其分配給其他 Downloader 執行個體。它可以代理程式模式下執行，在此模式下，其電腦能夠變成 Downloader 代理程式。Downloader 代理程式會從網際網路下載更新，並作為將更新分配給其他電腦的來源。Downloader 需要使用下列連接埠才能運作。

- TCP 和 UDP (傳入) 連接埠 **6888**
  由 BitTorrent 通訊協定用於 torrent 點對點更新。
- UDP 連接埠 **6771**
  當作本機對等探索連接埠使用。也參與點對點更新。
- TCP 連接埠 **18018**
  用於不同模式下運作的 Updater 之間的通訊：Updater 和 UpdaterAgent。
- TCP 連接埠 **18019**
  本機連接埠，用於 Updater 和保護代理程式之間的通訊。

步驟 6

在您打算安裝保護代理程式的電腦上，確認下列本機連接埠未由其他處理程序使用中。

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

注意事項
您不必在防火牆中開放這些連接埠。

變更保護代理程式所使用的連接埠

保護代理程式所需的部分連接埠可能由環境中的其他應用程式使用中。為避免發生衝突，您可以修改下列檔案，變更保護代理程式所使用的預設連接埠。

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

代理程式型和無代理程式備份

代理程式型備份需要在每部受保護的機器上安裝保護代理程式。所有實體機器和虛擬機器都支援代理程式型備份。如需有關所需代理程式以及安裝位置的詳細資訊，請參閱 "我需要哪種代理程式？ "(第 57 頁)

部分虛擬化平台支援無代理程式備份，而且不適用於實體機器。無代理程式備份僅需要一個保護代理程式，該代理程式必須已安裝在虛擬環境中的專用電腦上。此代理程式會備份此環境中的其他所有虛擬機器。如需有關每個虛擬化平台支援之備份類型的詳細資訊，請參閱 "支援的虛擬化平台" (第 30 頁)。

部分虛擬化平台可以使用虛擬裝置。虛擬裝置 (VA) 是隨附保護代理程式的一種現成虛擬機器。虛擬裝置可使用 Hypervisor 專用格式，例如 .ovf、.ova，或 .qcow。

我需要哪種備份類型？

如果您需要以下功能，建議您使用代理程式型備份：

- 其他保護功能，例如，防毒和防惡意軟體、修補程式管理或遠端桌面連線。如需有關這些功能的詳細資訊，請參閱 "作業系統支援的保護功能" (第 42 頁)。
- 在租用戶層級區分虛擬機器。例如，因為您希望租用戶中的使用者僅能存取自己的備份。
- 您可以復原到客體作業系統的檔案層級備份。

如果您需要以下功能，建議您使用無代理程式備份：

- 僅備份，而不需要其他任何保護功能。
- 簡化管理 — 只要安裝並設定一個代理程式，就可以備份多部虛擬機器。
- 資源使用量最少 — 相較於在您的環境中的每部虛擬機器上安裝多個代理程式，一個專用代理程式使用的 CPU 和 RAM 較少。
- 特定的備份設定，例如，不透過 LAN 的備份。如需有關此功能的詳細資訊，請參閱 "VMware 用代理程式 - 不透過 LAN 備份" (第 616 頁)。
- 設定開銷更少。無論客體作業系統為何，專用代理程式都會備份 Hypervisor 層級的虛擬機器。

我需要哪種代理程式？

選擇代理程式，視您要備份的內容而定。下表摘要說明可協助您做出決定的資訊。

在 Windows 中，Exchange 用代理程式、SQL 用代理程式、Active Directory 用代理程式，以及 Oracle 用代理程式要求同時安裝 Windows 用代理程式。因此，例如，如果您安裝 SQL 用代理程式，您也將可以備份已安裝代理程式的整部電腦。

建議您在安裝 VMware 用代理程式 (Windows) 和 Hyper-V 用代理程式時，也安裝 Windows 用代理程式。

在 Linux 中，Oracle 用代理程式、MySQL/MariaDB 用代理程式和 Virtuozzo 用代理程式需要也安裝 Linux 用代理程式 (64 位元)。這些代理程式會與 Linux (64 位元) 用代理程式安裝檔案一起搭售。

您要備份什麼內容？	要安裝哪一個代理程式？	要安裝在哪裡？
實體機器		
執行 Windows 的實體機器	Windows 用代理程式	在將進行備份的機器上。
執行 Linux 的實體機器	Linux 用代理程式	
執行 macOS 的實體機器	Mac 用代理程式	
資料庫		

SQL 資料庫	SQL 用代理程式	在執行 Microsoft SQL Server 的電腦上。
MySQL 資料庫	MySQL/MariaDB 用代理程式 (與 Linux (64 位元) 用代理程式安裝檔案一起搭售)	在執行 MySQL Server 的電腦上。
MariaDB 資料庫	MySQL/MariaDB 用代理程式 (與 Linux (64 位元) 用代理程式安裝檔案一起搭售)	在執行 MariaDB Server 的電腦上。
Exchange 資料庫	Exchange 用代理程式	在執行 Microsoft Exchange Server 信箱角色的電腦上。*
Oracle 資料庫	適用於 Oracle 的代理程式 (在 Linux 中，與 Linux (64 位元) 用代理程式安裝檔案一起搭售)	在執行 Oracle 資料庫的電腦上。
雲端對雲端工作負載		
Microsoft 365 信箱 (雲端代理程式和本機代理程式)	雲端代理程式 (不需要安裝)	此功能適用於在資料中心部署的雲端代理程式。如需詳細資訊，請參閱 "使用雲端 Microsoft 365 用代理程式" (第 550 頁)。
	Office 365 用代理程式	在已連線至網際網路的 Windows 電腦上。如需詳細資訊，請參閱 "使用本機安裝的 Office 365 用代理程式" (第 546 頁)。
Microsoft 365 OneDrive 檔案和 SharePoint Online 網站	雲端代理程式 (不需要安裝)	此功能適用於在資料中心部署的雲端代理程式。如需詳

		細資訊，請參閱 "使用雲端 Microsoft 365 用代理程式" (第 550 頁)。
Google Workspace Gmail 信箱、Google 雲端硬碟檔案和共用磁碟機檔案	雲端代理程式 (不需要安裝)	此功能適用於在資料中心部署的雲端代理程式。如需詳細資訊，請參閱 "保護 Google Workspace 資料" (第 577 頁)。
Active Directory		
執行 Active Directory 網域服務的電腦	Active Directory 用代理程式	在網域控制站上。
虛擬機器		
VMware ESXi 虛擬機器	VMware 用代理程式 (Windows)	在可經由網路存取 vCenter Server 和虛擬機器儲存空間的 Windows 電腦上。**
	VMware 用代理程式 (虛擬裝置)	在 ESXi 主機上。
Hyper-V 虛擬機器	Hyper-V 用代理程式	在 Hyper-V 主機上。
Scale Computing HC3 虛擬機器	Scale Computing HC3 用代理程式 (虛擬裝置)	在 Scale Computing HC3 主機上。
Red Hat Virtualization 虛擬機器 (受 oVirt 管理)	oVirt 用代理程式 (虛擬裝置)	在 Red Hat Virtualization 主機上。
Virtuozzo 虛擬機器和容器***	Virtuozzo 用代理程式 (與 Linux (64 位元) 用代理程式安裝檔案一起搭售)	在 Virtuozzo 主機上。
Virtuozzo Hybrid Infrastructure 虛擬機器	Virtuozzo Hybrid Infrastructure 用代理程式 (虛擬裝置)	在 Virtuozzo Hybrid Infrastructure 主機上。

裝載於 Amazon EC2 主機上的虛擬機器	與實體機器相同 ****	在將進行備份的機器上。
裝載於 Windows Azure 主機上的虛擬機器		
Citrix XenServer 虛擬機器		
Red Hat Virtualization (RHV/RHEV), not managed by oVirt		
不是由 oVirt 管理的核心虛擬機器 (KVM)		
不是由 oVirt 管理的 Oracle 虛擬機器		
Nutanix AHV 虛擬機器		
由 oVirt 管理的 Red Hat Virtualization (RHV/RHEV)	oVirt 用代理程式 (虛擬裝置)	在虛擬化主機上。
由 oVirt 管理的核心虛擬機器 (KVM)		
由 oVirt 管理的 Oracle 虛擬機器		
行動裝置		
執行 Android 的行動裝置	執行 Android 的行動應用程式	在將進行備份的行動裝置上。
執行 iOS 的行動裝置	執行 iOS 的行動應用程式	

*在安裝期間，Exchange 用代理程式會檢查執行所在電腦上是否有足夠的可用空間。在細微復原期間，暫時需要 15% 最大 Exchange 資料庫的可用空間。

**如果您的 ESXi 使用 SAN 連接儲存裝置，請將代理程式安裝在連線至相同 SAN 的電腦上。代理程式將會直接從儲存裝置備份虛擬機器，而不是透過 ESXi 主機和 LAN。如需詳細說明，請參閱 "VMware 用代理程式 - 不透過 LAN 備份" (第 616 頁)。

***若是 Virtuozzo 7，僅支援 ploop 容器。不支援虛擬機器。

****如果虛擬機器是藉由外部代理程式進行備份，則會將其視為虛擬。如果客體系統已安裝代理程式，則備份和復原作業會和實體機器的操作程序相同。但是，如果 Cyber Protection 可以使用 CPUID 指令識別虛擬機器，就可以虛擬機器服務配額指派給該虛擬機器。如果您使用直接通道或可將 CPU 製造商 ID 加上遮罩的其他選項，則僅能指派實體機器的服務配額。

代理程式的系統需求

代理程式	安裝所需的磁碟空間
Windows 用代理程式	1.2 GB
Linux 用代理程式	2 GB
Mac 用代理程式	1 GB

SQL 用代理程式和 Windows 用代理程式	1.2 GB
Exchange 用代理程式和 Windows 用代理程式	1.3 GB
資料洩漏防禦用代理程式	500 MB
Microsoft 365 用代理程式	500 MB
Active Directory 用代理程式和 Windows 用代理程式	2 GB
VMware 用代理程式和 Windows 用代理程式	1.5 GB
Hyper-V 用代理程式和 Windows 用代理程式	1.5 GB
Virtuozzo 用代理程式和 Linux 用代理程式	1 GB
Virtuozzo Hybrid Infrastructure 用代理程式	700 MB
Oracle 用代理程式和 Windows 用代理程式	2.2 GB
Oracle 用代理程式和 Linux 用代理程式	2 GB
MySQL/MariaDB 用代理程式和 Linux 用代理程式	2 GB

備份作業 (包括刪除備份) 每 1 TB 的備份大小需要大約 1 GB 的 RAM。記憶體耗用量可能會視代理程式處理的資料量和資料類型而有所不同。

注意事項
備份到超大的備份集 (4 TB 以上) 時，可能會增加 RAM 使用量。

在 x64 系統上，使用可開機媒體以及透過重新啟動進行磁碟復原的作業，至少需要 2 GB 的記憶體。

在配備新型處理器 (例如 11th Gen Intel Core 或 AMD Ryzen 7) 且支援 CET 技術的工作負載上，資料洩漏防禦用代理程式的部分功能遭到停用以避免發生衝突。下表列出具有此類 CPU 的系統上可用的裝置控制和 Advanced DLP 功能。

功能	裝置控制	Advanced DLP
本機通道		
卸除式儲存裝置	不適用	是
加密的卸除式儲存裝置	是	不適用
印表機	不適用	否
重新導向的對應磁碟機	不適用	是
重新導向的剪貼簿	不適用	否

網路通訊		
SMTP 電子郵件	不適用	是
Microsoft Outlook (MAPI)	不適用	是
IBM Notes	不適用	否
Web 郵件	不適用	是
即時訊息 (ICQ)	不適用	否
即時訊息 (Viber)	不適用	否
即時訊息 (IRC、Jabber、Skype、Viber)	不適用	是
檔案共用服務	不適用	是
社交網路	不適用	是
區域網路檔案共用 (SMB)	不適用	是
Web 存取 (HTTP/HTTPS)	不適用	是
檔案傳輸 (FTP/FTPS)	不適用	是
資料傳輸列入允許名單		
裝置類型的允許名單	不適用	是
網路通訊的允許名單	不適用	是
遠端主機的允許名單	不適用	是
應用程式的允許名單	不適用	是
週邊裝置		
卸除式儲存裝置	是	是
加密的卸除式儲存裝置	是	是
印表機	否	否
連線 MTP 的行動裝置	否	否
藍牙介面卡	是	是
光碟機	是	是
軟碟機	是	是
Windows 剪貼簿	否	否
螢幕擷取畫面擷取	否	否
重新導向的對應磁碟機	是	是

重新導向的剪貼簿	否	否
Cyber Protect 代理程式自我保護		
對一般終端使用者的防護	是	是
對本機系統管理員的防護	是	是

下載保護代理程式

安裝代理程式之前，您必須從 Cyber Protect 主控台下載其安裝檔案。

若要在將工作負載新增至保護時下載代理程式

1. 在 Cyber Protect 主控台中，瀏覽至 **[裝置]** > **[所有裝置]**。
2. 按一下右上方的 **[新增裝置]**。
3. 在 **[新增裝置]** 面板中，從 **[發行通道]** 下拉式功能表選擇代理程式版本。
   - **先前發行版本** - 下載先前發行版本的代理程式版本。
   - **最新版** - 下載可用的最新代理程式版本。
4. 選擇對應於要新增之工作負載作業系統的代理程式。
   [另存新檔] 對話方塊隨即開啟。
5. [僅適用於搭載 Apple Silicon (例如 Apple M1) 處理器的 Mac] 按一下 **[取消]**。在開啟的 **[新增 Mac]** 面板中，按一下 **[下載 ARM 安裝程式]** 連結。
6. 選擇儲存代理程式安裝檔案的位置，然後按一下 **[儲存]**。

若要下載代理程式供之後使用

1. 在 Cyber Protect 主控台的右上角，按一下 **[使用者]** 圖示。
2. 按一下 **[下載]**。
3. 在 **[下載]** 面板中，從 **[發行通道]** 下拉式功能表選擇代理程式版本。
   - **先前發行版本** - 下載先前發行版本的代理程式版本。
   - **最新版** - 下載可用的最新代理程式版本。
4. 捲動可用安裝程式的清單，以找出您需要的代理程式安裝程式，然後按一下該列結尾的下載圖示。
   [另存新檔] 對話方塊隨即開啟。
5. 選擇儲存代理程式安裝檔案的位置，然後按一下 **[儲存]**。

Linux 套件

若要將必要模組新增到 Linux 核心，安裝程式需要下列 Linux 套件：

- 具有核心標頭或來源的套件。套件版本必須與核心版本相符。
- GNU 編譯器集合 (GCC) 編譯器系統。GCC 版本必須是核心編譯時所用的版本。
- Make 工具。
- Perl 解譯器。

- `libelf-dev`、`libelf-devel` 或 `elfutils-libelf-devel` 程式庫從 4.15 開始可用於建置核心，並使用 CONFIG_UNWINDER_ORC=y 加以設定。至於 Fedora 28 之類的一些發行版，則需要與核心標頭分開安裝。

這些套件的名稱會視 Linux 發行版而有所不同。

在 Red Hat Enterprise Linux、CentOS 和 Fedora 中，套件一般會由安裝程式安裝。在其他發行版中，如果套件尚未安裝或並非所需的版本，則您需要安裝套件。

所需的套件是否已安裝?

若要查看套件是否已安裝，請執行以下步驟：

1. 執行下列命令，找出核心版本和所需的 GCC 版本：

   ```
   cat /proc/version
   ```

   此命令會傳回與以下項目類似的命令列：`Linux version 2.6.35.6` 與 `gcc version 4.5.1`
2. 執行下列命令，以檢查是否安裝了 Make 工具和 GCC 編譯器：

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

   若為 **gcc**，請確保該命令傳回的版本與步驟 1 中的 `gcc version` 相同。若為 **make**，只需確保該命令確實執行。
3. 檢查是否安裝了建立核心模組所需的適當套件版本：
   - 在 Red Hat Enterprise Linux、CentOS 和 Fedora 中，執行下列命令：

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

   - 在 Ubuntu 中，執行以下命令：

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

   在上述任一種情況下，請確保套件版本與步驟 1 中的 `Linux version` 相同。
4. 執行下列命令以檢查是否已安裝 Perl 解譯器：

   ```
   perl --version
   ```

   如果您看到關於 Perl 版本的資訊，則表示解譯器已安裝。
5. 在 Red Hat Enterprise Linux、CentOS 和 Fedora 中，執行下列命令來檢查是否已安裝 `elfutils-libelf-devel`：

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

   如果您看到關於程式庫版本的資訊，則表示已安裝該程式庫。

從存放庫安裝套件

下表列出如何在各種 Linux 發行版中安裝所需的套件。

Linux 發行版	套件名稱	如何安裝
Red Hat Enterprise Linux	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	安裝程式將會使用您的 Red Hat 訂購授權自動下載並安裝套件。
	perl	執行下列命令： `yum install perl`
CentOS Fedora	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	安裝程式將會自動下載並安裝套件。
	perl	執行下列命令： `yum install perl`
Ubuntu Debian	**linux-headers** **linux-image** **gcc** **make** **perl**	執行以下命令： `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`

隨即會從發行版的存放庫下載並安裝套件。

對於其他 Linux 發行版，請參閱該發行版文件中所需套件的確切名稱及安裝方法等相關資訊。

手動安裝套件

在下列情況中，您可能需要**手動**安裝套件：

- 電腦沒有有效的 Red Hat 訂購授權或網際網路連線。
- 安裝程式找不到對應於核心版本的 **kernel-devel** 或 **gcc** 版本。如果可用的 **kernel-devel** 比您的核心更新，您需要更新核心或手動安裝相符的 **kernel-devel** 版本。
- 必要的套件位於您的本機網路，且您不希望花時間自動搜尋與下載。

從您的區域網路或信任的第三方網站取得套件，並依下列方式安裝：

- 在 Red Hat Enterprise Linux、CentOS 或 Fedora 中，以 root 使用者身分執行下列命令：

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

- 在 Ubuntu 中，執行下列命令：

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

範例：在 Fedora 14 中手動安裝套件

依照這些步驟，在 32 位元電腦上於 Fedora 14 中安裝所需的套件：

1. 執行下列命令，以判斷核心版本和所需的 GCC 版本：

   ```
   cat /proc/version
   ```

   此命令的輸出包括下列項目：

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

2. 取得對應到此核心版本的 **kernel-devel** 和 **gcc** 套件：

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

3. 取得適用於 Fedora 14 的 **make** 套件：

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

4. 請以 root 使用者身分執行下列命令以安裝套件：

   ```
   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
   ```

   您可以在單一 `rpm` 命令中指定所有這些套件。安裝任一這些套件時，可能需要安裝額外的套件，以解決相依性問題。

設定 Proxy 伺服器設定

保護代理程式可以透過 HTTP/HTTPS Proxy 伺服器傳輸資料。伺服器必須在不掃描也不干擾 HTTP 流量的情況下，透過 HTTP 通道運作。不支援攔截式 Proxy。

安裝期間，代理程式會在雲端註冊本身，因此必須在安裝代理程式期間或事先設定 Proxy 伺服器設定。

適用於 Windows

如果已在 **[控制面板]** > **[網際網路選項]** > **[連線]** 中設定 Proxy 伺服器，安裝程式會從登錄讀取 Proxy 伺服器設定，並自動使用這些設定。

如果您要執行下列工作，請使用此程序。

- 安裝代理程式前設定 Proxy 設定。
- 安裝代理程式後更新 Proxy 設定。

若要在安裝代理程式期間設定 Proxy 設定，請參閱 "在 Windows 中安裝保護代理程式" (第 72 頁)。

注意事項
只有在 `http-proxy.yaml` 檔案不存在於電腦上時，此程序才有效。如果 `http-proxy.yaml` 檔案存在於電腦上，您必須更新檔案中的 Proxy 設定，因為它會覆寫 `aakore.yaml` 檔案中的設定。

當您使用 Cyber Protection Monitor 設定 Proxy 伺服器設定時，會建立 `%programdata%\Acronis\Agent\var\aakore\http-proxy.yaml` 檔案。如需詳細資訊，請參閱 "在 Cyber Protect Monitor中設定 Proxy 伺服器設定" (第 258 頁)。

若要開啟 `http-proxy.yaml` 檔案，您必須是 Windows 中 Administrators 群組的成員。

若要設定 Proxy 設定

1. 建立新文字文件，然後在文字編輯器中開啟此檔案，例如「記事本」。
2. 複製以下幾行並貼到檔案中。

```
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. 將 `proxy.company.com` 取代為您的 Proxy 伺服器主機名稱/IP 位址，並將 `000001bb` 取代為連接埠號碼的十六進位值。例如 `000001bb` 是連接埠 443。
4. 如果您的 Proxy 伺服器需要驗證，請將 `proxy_login` 和 `proxy_password` 取代為 Proxy 伺服器認證。否則，請從檔案中刪除這幾行。
5. 將文件儲存為 `proxy.reg`。
6. 以系統管理員身份執行檔案。
7. 確認您要編輯 Windows 登錄。
8. 如果此工作負載上未安裝代理程式，請現在安裝。如果此工作負載上已安裝代理程式，請繼續進行下一個步驟。
9. 在文字編輯器中開啟 `%programdata%\Acronis\Agent\etc\aakore.yaml` 檔案。

若要開啟此檔案，您必須是 Windows 中 Administrators 群組的成員。

10. 找出 **env** 區段或建立該區段，然後加入下列幾行。

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

11. 將 `proxy_login` 和 `proxy_password` 取代為 Proxy 伺服器認證，並將 `proxy_address:port` 取代為 Proxy 伺服器的位址和連接埠號碼。
12. 在 **[開始]** 功能表中，按一下 **[執行]**、輸入：**cmd**，然後按一下 **[確定]**。
13. 執行下列命令，重新啟動 aakore 服務。

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

14. 執行下列命令，重新啟動代理程式。

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

對於 macOS

如果您要執行下列工作，請使用此程序。

- 安裝代理程式前設定 Proxy 設定。
- 安裝代理程式後更新 Proxy 設定。

若要在安裝代理程式期間設定 Proxy 設定，請參閱 "在 macOS 中安裝保護代理程式" (第 76 頁)。

若要設定 Proxy 設定

1. 建立 `/Library/Application Support/Acronis/Registry/Global.config` 檔案，然後在文字編輯器 (例如 Text Edit) 中開啟此檔案。
2. 複製以下幾行並貼到檔案中。

```
<?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. 將 `proxy.company.com` 取代為您的 Proxy 伺服器主機名稱/IP 位址，並將 `443` 取代為連接埠號碼的十進位值。
4. 如果您的 Proxy 伺服器需要驗證，請將 `proxy_login` 和 `proxy_password` 取代為 Proxy 伺服器認證。否則，請從檔案中刪除這幾行。

5. 儲存檔案。
6. 如果此工作負載上未安裝代理程式，請現在安裝。如果此工作負載上已安裝代理程式，請繼續進行下一個步驟。
7. 在文字編輯器中開啟 `/Library/Application Support/Acronis/Agent/etc/aakore.yaml` 檔案。
8. 找出 **env** 區段或建立該區段，然後加入下列幾行。

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

9. 將 `proxy_login` 和 `proxy_password` 取代為 Proxy 伺服器認證，並將 `proxy_address:port` 取代為 Proxy 伺服器的位址和連接埠號碼。
10. 前往 **[應用程式]** > **[公用程式]** > **[終端機]**。
11. 執行下列命令，重新啟動 aakore 服務。

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

12. 執行下列命令，重新啟動代理程式。

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

適用於 Linux

利用 `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORD` 參數執行安裝檔案。安裝保護代理程式之後，請使用下列程序更新 Proxy 設定。

若要設定 Proxy 設定

1. 在文字編輯器中開啟 `/etc/Acronis/Global.config` 檔案。
2. 執行下列其中一項操作：
   - 如果在代理程式安裝期間指定 Proxy 設定，請找出下列區段。

```
<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>
```

   - 如果未在代理程式安裝期間指定 Proxy 設定，請複製以下幾行，並將其貼到該檔案中的 `<registry name="Global">...</registry>` 標籤之間。

```
<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. 將 ADDRESS 取代為新的 Proxy 伺服器主機名稱/IP 位址，並將 PORT 取代為連接埠號碼的十六進位值。
4. 如果您的 Proxy 伺服器需要驗證，請將 LOGIN 和 PASSWORD 取代為 Proxy 伺服器認證。否則，請從檔案中刪除這幾行。
5. 儲存檔案。
6. 在文字編輯器中開啟檔案 /opt/acronis/etc/aakore.yaml。
7. 找出 **env** 區段，或建立該區段並加入下列幾行：

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

8. 將 proxy_login 和 proxy_password 取代為 Proxy 伺服器認證，並將 proxy_address:port 取代為 Proxy 伺服器的位址和連接埠號碼。
9. 執行下列命令，重新啟動 aakore 服務。

```
sudo service aakore restart
```

10. 在任意目錄中執行下列命令以重新啟動代理程式。

```
sudo service acronis_mms restart
```

對於可開機媒體

在可開機媒體下運作時，您可能需要透過 Proxy 伺服器存取雲端儲存空間。若要設定 Proxy 伺服器設定，請按一下 **[工具]** > **[Proxy 伺服器]**，然後設定 Proxy 伺服器主機名稱/IP 位址、連接埠和認證。

動態安裝與解除安裝元件

對於受到代理程式 15.0.26986 (2021 年 5 月發行) 版或更新版本保護的 Windows 工作負載，會動態安裝下列元件，亦即，只有在保護計劃需要時安裝：

- URL 篩選用代理程式 — 操作 URL 篩選功能所需。
- 防惡意軟體防護用代理程式 – 操作防惡意軟體防護功能時所需。
- 資料洩漏防禦用代理程式 – 操作裝置控制功能時所需。

預設不會安裝這些元件。如果工作負載變成受到啟用下列任何模組所在計劃的保護，則會自動安裝個別的元件：

- 防毒和防惡意程式保護
- URL 篩選
- 裝置控制

同樣地，如果保護計劃不再需要反惡意程式碼保護、URL 篩選或裝置控制功能，則會自動解除安裝個別的元件。

變更保護計劃後，動態安裝或解除安裝元件最多花費 10 分鐘就可以完成。但是，如果正在執行下列任何作業，動態安裝或解除安裝將會在該作業完成後開始：

- 備份
- 復原
- 備份複寫
- 虛擬機器複寫
- 測試複本
- 從備份執行虛擬機器 (包括最終化)
- 災難復原容錯移轉
- 災難復原容錯回復
- 執行指令碼 (針對網路指令碼撰寫功能)
- 修補程式安裝
- ESXi 設定備份

將所需的系統權限授予 Connect 代理程式

若要在 macOS 工作負載上啟用遠端桌面功能的所有功能，除了完整的磁碟存取權限之外，還必須將下列權限授予 Connect 代理程式：

- 畫面錄製 - 透過 NEAR 啟用 macOS 工作負載的畫面錄製。在授予此權限之前，將會拒絕所有遠端控制連線。
- 易用性 - 透過 NEAR 在控制模式下啟用遠端連線
- 麥克風 - 透過 NEAR 啟用從遠端 macOS 工作負載到本機工作負載的聲音重新導向。若要啟用聲音重新導向功能，工作負載上必須安裝聲音擷取驅動程式。如需詳細資訊，請參閱 "遠端聲音重新導向" (第 903 頁)。
- 自動化 - 啟用清空資源回收桶動作

當您在 macOS 工作負載上啟動代理程式之後，它將檢查代理程式是否具有這些權限，並在需要時要求您授予權限。

若要授予畫面錄製權限

1. 在 [Cyber Protect 代理程式] 對話方塊的 **[授予所需的系統權限]** 中，按一下 **[設定系統權限]**。
2. 在 **[系統權限]** 對話方塊中，按一下 **[要求畫面錄製]** 權限。
3. 按一下 **[開啟系統喜好設定]**。
4. 選擇 **Connect 代理程式**。

當您嘗試遠端存取工作負載時，如果代理程式沒有權限，則會顯示 [畫面錄製權限要求] 對話方塊。只有本機使用者可以回答該對話方塊。

若要授予易用性權限

1. 在 [Cyber Protect 代理程式] 對話方塊的 **[授予所需的系統權限]** 中，按一下 **[設定系統權限]**。
2. 在 **[系統權限]** 對話方塊中，按一下 **[要求易用性權限]**。
3. 按一下 **[開啟系統喜好設定]**。

4. 按一下視窗左下角的鎖定圖示，使其變成已解除鎖定圖示。系統會要求您提供系統管理員密碼，以便進行變更。
5. 選擇 **Connect 代理程式**。

若要授予麥克風權限

1. 在 Connect 代理程式 對話方塊的 **[授予所需的系統權限]** 中，按一下 **[設定系統權限]**。
2. 在 **[系統權限]** 對話方塊中，按一下 **[要求麥克風權限]**。
3. 按一下 **[確定]**。

注意事項
您還必須在 macOS 工作負載上安裝聲音擷取驅動程式，讓代理程式運用所給予的權限並重新導向工作負載的聲音。如需詳細資訊，請參閱 "遠端聲音重新導向" (第 903 頁)。

若要授予自動化權限

1. 在 Connect 代理程式 對話方塊的 **[授予所需的系統權限]** 中，按一下 **[設定系統權限]**。
2. 在 **[系統權限]** 對話方塊中，按一下 **[要求自動化權限]**。

使用圖形化使用者介面安裝保護代理程式

在 Windows 中安裝保護代理程式

必要條件

在您打算保護的工作負載上，下載所需的代理程式。請參閱 "下載保護代理程式" (第 63 頁)。

若要安裝 Windows 用代理程式

1. 確定電腦已連線到網際網路。
2. 以系統管理員身分登入並啟動安裝程式。
3. [可選] 按一下 **[自訂安裝設定]**，並進行適當的變更 (如有需要)：
   - 若要變更要安裝的元件 (例如，停用 Cyber Protection Monitor 或命令列工具的安裝，或安裝防惡意軟體防護用代理程式和 URL 篩選用代理程式)。

     注意事項
     在 Windows 電腦上，防惡意軟體防護功能需要安裝防惡意軟體防護用代理程式，URL 篩選功能則需要安裝 URL 篩選用代理程式。如果在其保護計劃中啟用 **[防毒和防惡意軟體防護]** 和/或 **[URL 篩選]** 模組，則會自動為受保護的工作負載安裝這些代理程式。

   - 變更在 Cyber Protection 服務中註冊工作負載的方法。您可以從 **[使用服務主控台]** (預設) 切換到 **[使用認證]** 或 **[使用註冊權杖]**。
   - 變更安裝路徑。
   - 變更將執行代理程式服務所用的使用者帳戶。如需詳細資訊，請參閱 "變更 Windows 電腦上的登入帳戶" (第 73 頁)。

- 驗證或變更 Proxy 伺服器主機名稱/IP 位址、連接埠和認證。如果您在 Windows 中啟用 Proxy 伺服器，系統會自動偵測並使用該伺服器。

4. 按一下 **[安裝]**。
5. [僅適用於安裝 VMware 用代理程式的情況] 針對您要備份和復原虛擬機器所在的 vCenter Server 或獨立 ESXi 主機，指定位址和存取認證，然後按一下 **[完成]**。

   建議您使用專用帳戶來存取 vCenter Server 或 ESXi 主機，而不是使用具有 [系統管理員] 角色的現有帳戶。如需詳細資訊，請參閱 "VMware 用代理程式所需的權限" (第 623 頁)。
6. [此步驟僅適用於安裝網域控制器的情況] 指定要使用哪個使用者帳戶執行代理程式服務，然後按一下 **[完成]**。基於安全理由，安裝程式不會在網域控制站上自動建立新帳戶。

   注意事項

   您指定的使用者帳戶必須獲授予 [以服務方式登入] 權限。此帳戶必須已經在網域控制站上使用，才能在該電腦上建立其設定檔資料夾。

   如需有關在唯讀網域控制站上安裝代理程式的詳細資訊，請參閱這篇知識庫文章。
7. 如果您在步驟 3 中保留預設的註冊方法 **[使用服務主控台]**，則請等到註冊畫面出現，然後再繼續進行下一個步驟。否則，您不需要再進行任何動作。
8. 使用客戶租用戶帳戶註冊代理程式。如需有關註冊的詳細資訊，請參閱 "使用圖形化使用者介面註冊工作負載" (第 106 頁)。
9. [如果是以其租用戶處於合規模式下的帳戶註冊代理程式] 設定加密密碼。

變更 Windows 電腦上的登入帳戶

在 **[選擇元件]** 畫面上，指定 **[代理程式服務的登入帳戶]** 以定義執行服務將使用的帳戶。您可以選擇下列其中一項：

- **使用服務使用者帳戶**(預設適用於代理程式服務)

  服務使用者帳戶是用於執行服務的 Windows 系統帳戶。這種設定的優點在於，網域安全性原則不會影響此類帳戶的使用者權限。依預設，此代理程式在**本機系統**帳戶下執行。
- **建立新帳戶**

  代理程式的帳戶名稱將是 Agent User。
- **使用下列帳戶**

  如果您將代理程式安裝在網域控制站上，則系統會提示您為代理程式指定現有的帳戶 (或相同帳戶)。基於安全理由，系統不會在網域控制站上自動建立新帳戶。

  您在網路控制站上執行安裝程式時所指定的使用者帳戶必須獲授予 [以服務方式登入] 權限。此帳戶必須已經在網域控制站上使用，才能在該電腦上建立其設定檔資料夾。

  如需有關在唯讀網域控制站上安裝代理程式的詳細資訊，請參閱這篇知識庫文章。

若您已選擇**建立新帳戶**或**使用下列帳戶**選項，確保網域安全性原則不會影響相關帳戶的權限。如果帳戶被剝奪了安裝期間分配的使用者權限，則該元件可能工作不正確或不工作。

登入帳戶所需的權限

保護代理程式在 Windows 電腦上是當作 Managed Machine Service (MMS) 執行的。執行代理程式所使用的帳戶必須具備特定權限，代理程式才能正確運作。因此，MMS 使用者應該獲指派下列權

限：

1. 包含在 **[Backup Operators]** 和 **[Administrators]** 群組中。在網域控制站上，使用者必須包含在 **[Domain Admins]** 群組中。
2. 獲授予資料夾 `%PROGRAMDATA%\Acronis` (在 Windows XP 及 Server 2003 中為 `%ALLUSERSPROFILE%\Application Data\Acronis`) 及其子資料夾的**完全控制**權限。
3. 獲授予下列機碼中特定登錄機碼的**完全控制**權限：`HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`。
4. 獲指派下列使用者權限：
   - 以服務方式登入
   - 調整處理程序的記憶體配額
   - 取代處理程序等級權杖
   - 修改韌體環境值

如何指派使用者權限

依照以下的指示，指派使用者權限 (此範例使用的是 **[以服務方式登入]** 使用者權限，其他使用者權限的步驟相同)：

1. 使用具有系統管理權限的帳戶，登入電腦。
2. 從 **[控制台]** (或按一下 Win+R、輸入 **control admintools**，然後按 Enter) 開啟 **[系統管理工具]**，然後開啟 **[本機安全性原則]**。
3. 展開 **[本機原則]**，然後按一下 **[使用者權限指派]**。
4. 在右窗格中，以滑鼠右鍵按一下 **[以服務方式登入]**，然後選擇 **[內容]**。
5. 按一下 **[新增使用者或群組...]** 按鈕，加入新的使用者。
6. 在 **[選擇使用者、電腦、服務帳戶或群組]** 視窗中，尋找您要輸入的使用者，然後按一下 **[確定]**。
7. 在 **[以服務方式登入內容]** 中按一下 **[確定]** 以儲存變更。

重要事項
請確認您已經新增至 **[以服務方式登入]** 使用者權限的使用者未列在 **[本機安全性原則]** 的 **[拒絕以服務方式登入]** 原則中。

請注意，不建議在完成安裝之後，手動變更登入帳戶。

在 Linux 中安裝保護代理程式

準備

- 在您打算保護的電腦上，下載所需的代理程式。請參閱 "下載保護代理程式" (第 63 頁)。
- 確保必要的 Linux 套件 已安裝在電腦上。
- 在 SUSE Linux 中安裝代理程式時，請確認您使用 su - 而不是 sudo。否則，當您嘗試透過 Cyber Protect 主控台註冊代理程式時，會發生下列錯誤：無法啟動網頁瀏覽器。沒有可用的顯示。

  部分 Linux 發行版 (例如 SUSE) 在使用 sudo 時，不會傳遞 DISPLAY 變數，因此安裝程式無法在圖形化使用者介面 (GUI) 中開啟瀏覽器。

安裝

若要安裝 Linux 用代理程式，您需要至少 2 GB 的可用磁碟空間。

安裝 Linux 用代理程式

1. 確定電腦已連線到網際網路。
2. 以 root 使用者身分，瀏覽到有安裝檔案的目錄，讓檔案可以執行，然後加以執行。

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

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

   如果您的網路中已啟用 Proxy 伺服器，執行安裝檔案時，請以下列格式指定伺服器主機名稱 /IP 位址和連接埠：`--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORD`。

   如果您要變更在 Cyber Protection 服務中註冊電腦的預設方法，請使用下列其中一個參數，執行安裝檔案：

   - `--register-with-credentials` – 要求在安裝期間輸入使用者名稱和密碼
   - `--token=STRING` – 使用註冊權杖
   - `--skip-registration` – 略過註冊
3. 選擇要安裝的代理程式的核取方塊。您可以選取下列代理程式：
   - Linux 用代理程式
   - Virtuozzo 用代理程式
   - 適用於 Oracle 的代理程式
   - MySQL/MariaDB 用代理程式

   Virtuozzo 用代理程式、Oracle 用代理程式和 MySQL/MariaDB 用代理程式需要也安裝 Linux 用代理程式 (64 位元)。
4. 如果您在步驟 2 中保留預設的註冊方法，則請繼續進行下一個步驟。否則，請輸入 Cyber Protection 服務的使用者名稱與密碼，或等到電腦使用權杖註冊為止。
5. 使用客戶租用戶帳戶註冊代理程式。如需有關註冊的詳細資訊，請參閱 "使用圖形化使用者介面註冊工作負載" (第 106 頁)。
6. [如果是以其租用戶處於合規模式下的帳戶註冊代理程式] 設定加密密碼。
7. 如果在電腦上啟用 UEFI 安全開機，您會在安裝後收到您需要重新啟動系統的通知。請務必記住應該使用的密碼 (根使用者或 "acronis" 的密碼)。

   注意事項

   此安裝會產生一個用於簽署核心模組的新金鑰。您必須重新啟動電腦，才能將這個新的金鑰註冊到電腦擁有者金鑰 (MOK) 清單。如果沒有註冊新的金鑰，代理程式將無法運作。如果您在代理程式安裝之後啟用 UEFI 安全開機，則您需要重新安裝代理程式。
8. 安裝完成後，請執行下列其中一項操作：

- 如果系統在上一個步驟中提示您重新啟動系統，按一下 **[重新啟動]**。
  在系統重新啟動期間，選擇 MOK (機器擁有者金鑰) 管理、選擇 **[註冊 MOK]**，然後使用上一個步驟中建議的密碼，註冊金鑰。
- 否則，請按一下 **[結束]**。

檔案會提供疑難排解資訊：`/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL`

在 macOS 中安裝保護代理程式

必要條件

在您打算保護的工作負載上，下載所需的代理程式。請參閱 "下載保護代理程式" (第 63 頁)。

若要安裝 Mac 用代理程式 (x64 或 ARM64)

1. 確定電腦已連線到網際網路。
2. 按兩下安裝檔案 (.dmg)。
3. 請等候作業系統掛載安裝磁碟影像。
4. 按兩下 [**安裝**]。
5. 如果您的網路中已啟用 Proxy 伺服器，請按一下功能表列中的 **[保護代理程式]**、按一下 **[Proxy 伺服器設定]**，然後指定 Proxy 伺服器主機名稱/IP 位址、連接埠和認證。
6. 若畫面顯示提示，請提供系統管理員認證。
7. 按一下 **[繼續]**。
8. 等到註冊畫面出現為止。
9. 使用客戶租用戶帳戶註冊代理程式。如需有關註冊的詳細資訊，請參閱 "使用圖形化使用者介面註冊工作負載" (第 106 頁)。
10. [如果是以其租用戶處於合規模式下的帳戶註冊代理程式] 設定加密密碼。
11. 如果您的 macOS 版本為 Mojave 10.14.x 或更新版本，則對保護代理程式授予完成磁碟存取權，才能啟用備份作業。
    如需相關指示，請參閱將「完整磁碟存取」權限授予網路保護代理程式 (64657)。
12. 若要使用遠端桌面功能，請將所需的系統權限授予 Connect 代理程式。如需詳細資訊，請參閱 "將所需的系統權限授予 Connect 代理程式" (第 71 頁)。

解除安裝代理程式

當您從工作負載解除安裝代理程式時，該工作負載會自動從 Cyber Protect 主控台中移除。如果在解除安裝代理程式後仍然顯示該工作負載 (例如，因為網路問題)，請從主控台中手動移除此工作負載。如需有關如何執行此操作的詳細資訊，請參閱 "正在從 Cyber Protect 主控台中移除工作負載" (第 278 頁)。

注意事項
解除安裝代理程式不會刪除任何計劃或備份。

若要解除安裝代理程式

Windows

1. 以系統管理員身分，登入裝有代理程式的電腦。
2. 在 **[控制面板]** 中，移至 **[程式和功能]** (在 Windows XP 中為 **[新增或移除程式]**)。
3. 以滑鼠右鍵按一下 **Acronis Cyber Protect**，然後選擇 **[解除安裝]**。
4. [適用於受密碼保護的代理程式] 指定解除安裝代理程式所需的密碼，然後按一下 **[下一步]**。
5. [選用] 選擇 **[移除記錄和組態設定]** 核取方塊。
   如果您打算再次安裝代理程式，請清除此核取方塊。如果您選擇此核取方塊，且之後再次安裝該代理程式，則可能會在 Cyber Protect 主控台中複製此工作負載，且舊的備份可能無法與其建立關聯。
6. 按一下 **[解除安裝]**。

Linux

1. 在已安裝代理程式的電腦上，以根使用者身分執行 `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall`。
2. [選用] 選擇 **[清理所有產品蹤跡 (移除產品記錄、工作、儲藏庫和組態設定)]** 核取方塊。
   如果您打算再次安裝代理程式，請清除此核取方塊。如果您選擇此核取方塊，且之後再次安裝該代理程式，則可能會在 Cyber Protect 主控台中複製此工作負載，且舊的備份可能無法與其建立關聯。
3. 確認選項無誤。

macOS

1. 在已安裝代理程式的電腦上，按兩下安裝檔 .dmg。
2. 請等到作業系統掛載安裝磁碟映像為止。
3. 在影像中，按兩下 **[解除安裝]**。
4. 若畫面顯示提示，請提供系統管理員認證。
5. 確認選項無誤。

若要解除安裝 Windows 用代理程式搭售的元件

您可以解除安裝 Windows 用代理程式搭售的個別元件 (例如 Cyber Protect Monitor、資料洩漏防禦用代理程式或 Bootable Media Builder)，而不必解除安裝 Windows 用代理程式。

1. 以系統管理員身分，登入裝有代理程式的電腦。
2. 執行安裝程式，然後按一下 **[修改已安裝的元件]**。
3. 清除您要解除安裝的元件旁的核取方塊，然後按一下 **[完成]**。

若要移除 VMware 用代理程式 (虛擬裝置)

1. 使用 vSphere Client 登入 vCenter Server。
2. [如果虛擬裝置已開啟] 以滑鼠右鍵按一下該虛擬裝置，然後按一下 **[電源]** > **[關機]**。確認選項無誤。
3. [如果虛擬裝置在虛擬磁碟上使用本機連接的存放區，且您想要保留該磁碟上的資料] 從虛擬裝置移除虛擬存放區。
   a. 用滑鼠右鍵按一下虛擬裝置，然後按一下 **[編輯設定]**。
   b. 選擇內含存放區的磁碟，然後按一下 **[移除]**。

c. 在 **[移除選項]** 下，按一下 **[從虛擬機器中移除]**。

d. 按一下 **[確定]**。

完成後，磁碟會保留在資料存放區中。您可以將磁碟附加至另一個虛擬裝置。

4. 以滑鼠右鍵按一下虛擬裝置，然後按一下 **[從磁碟中刪除]**。。確認選項無誤。
5. [選用] [如果您不打算再次使用此裝置] 在 Cyber Protect 主控台中，移至 **[備份儲存]** > **[位置]**，然後刪除對應到本機連接的存放區的位置。

使用命令列介面安裝和解除安裝保護代理程式

在 Windows 中安裝和解除安裝保護代理程式

在 Windows 中，您可以透過以下方式執行自動安裝或解除安裝：

- 使用安裝程式的 EXE 檔案，並在命令列上指定安裝參數。
- 使用您從安裝程式解壓縮的 MSI 檔案，並以下列其中一種方式指定安裝參數：
  - 在 MST 檔案中
  - 直接在命令列上

使用 EXE 檔案自動安裝和解除安裝

針對此類型的自動安裝，請下載安裝程式，然後在命令列中使用所需的安裝參數啟動該安裝程式。若要查看您可以使用的參數，請參閱 "用於自動安裝 (EXE) 的參數" (第 80 頁)。

您不需要事先解壓縮安裝套件、MSI 和 MST 檔案。

安裝與解除安裝代理程式和元件 (EXE)

若要使用 EXE 檔案執行自動安裝，請執行安裝程式，並在命令列上指定安裝參數。

若要下載安裝程式，請在 Cyber Protect 主控台中，按一下右上角的帳戶圖示，然後按一下 **[下載]**。您也可以在 **[新增裝置]** 窗格中取得下載連結。

若要安裝代理程式和元件

1. 以系統管理員的身分啟動命令列介面，然後導覽至安裝程式的 EXE 檔案。
2. 若要啟動安裝程式並指定安裝參數，請執行以下命令：

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

使用空格分隔參數，並使用逗號 (不加空格) 分隔參數的值。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
```

若要檢查可用的參數及其值，請參閱 "用於自動安裝 (EXE) 的參數" (第 80 頁)。

範例

- 安裝 Windows 用代理程式、防惡意軟體用代理程式和 URL 篩選用代理程式、命令列工具和 Cyber Protect Monitor。使用使用者名稱和密碼，在 Cyber Protection 服務中註冊工作負載。

```
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
```

- 安裝 Windows 用代理程式、命令列工具和 Cyber Protect Monitor。在 Windows 中，為代理程式服務建立一個新的登入帳戶。使用權杖，在 Cyber Protection 服務中註冊工作負載。

```
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
```

- 安裝 Windows 用代理程式、命令列工具、Oracle 用代理程式和 Cyber Protect Monitor。使用使用者名稱和密碼，在 Cyber Protection 服務中登錄電腦。

```
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
```

- 安裝 Windows 用代理程式、命令列工具和 Cyber Protect Monitor。將使用者介面語言設定為 [德文]。使用權杖，在 Cyber Protection 服務中登錄電腦。設定 HTTP Proxy。

```
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
```

若要移除已安裝的元件

1. 以系統管理員的身分啟動命令列介面，然後導覽至 `%ProgramFiles%\BackupClient\RemoteInstall`。
2. 執行下列命令：

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

若要檢查可用的參數及其值，請參閱 "用於自動安裝 (EXE) 的參數" (第 80 頁)。

範例

- 解除安裝 Cyber Protect Monitor。

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

若要解除安裝代理程式

1. 以系統管理員的身分啟動命令列介面，然後導覽至 `%Program Files%\Common Files\Acronis\BackupAndRecovery`。
2. 執行下列命令：

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

若要檢查可用的參數及其值，請參閱 "用於自動安裝 (EXE) 的參數" (第 80 頁)。

範例

- 解除安裝 Windows 用代理程式及其所有元件。刪除所有記錄、工作和組態設定。

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

- 解除安裝受密碼保護的 Windows 用代理程式及其所有元件。刪除所有記錄、工作和組態設定。

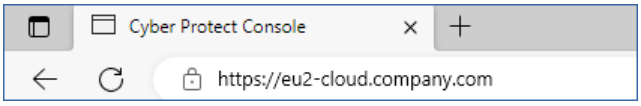
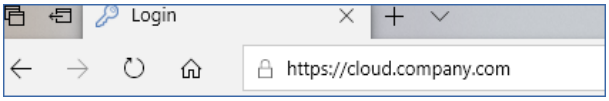
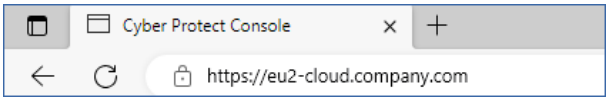
```
C:\Program Files\Common Files\Acronis\BackupAndRecovery\Uninstaller.exe --anti-
tamper-password=<password> --quiet --delete-all-settings
```

用於自動安裝 (EXE) 的參數

下表摘要說明搭配 EXE 檔案使用自動安裝的參數。

參數	描述
一般參數	
`--add-components=<component1,component2,...,componentN>`	要安裝的元件。請在 "用於自動安裝 (EXE) 的元件" (第 84 頁) 中查看可用元件的完整清單。 當您指定多個元件時，請以逗號分隔。請不要在逗號前後空格。 如果您指定已安裝的元件，將會修復或更新這些元件，端視安裝程式版本以及已安裝元件版本而定。 如果您未指定此參數，將會根據您執行安裝所在的電腦，安裝一組預設的元件。例如，SQL 用代理程式僅會安裝在執行 MS SQL Server 的電腦上。

參數	描述
--install-dir=<path>	將安裝所選元件的資料夾。如果指定的資料夾不存在，則會建立該資料夾。 如果您未指定此參數，將會使用預設資料夾：C:\Program Files\BackupClient。
--log-dir=<path>	將儲存安裝記錄的資料夾。 如果您未指定此參數，將會使用預設資料夾：%ProgramData%\Acronis\InstallationLogs。
--language=<code>	產品語言。 可用的值如下：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。 如果您未指定此參數，而且您執行安裝所在電腦的系統語言列在上方，則會使用系統語言。否則，此值會設定為 en。
--quiet	使用此參數可在不顯示圖形化使用者介面的情況下執行安裝程式。 請不要將其與 --register-only 參數一起使用。
--help	使用此參數可查看您可以在命令列及其描述上使用之所有可用參數的清單。
--fss-onboarding-auto-start	將此參數與 --quiet 參數一起使用可在自動安裝後顯示 File Sync & Share 上線精靈。
註冊參數	
--registration={skip | by-credentials | by-token | device-flow}	使用此參數可在安裝後選擇如何註冊代理程式。 若要略過註冊，請指定 skip。您之後可以使用 --register-only 參數註冊代理程式。 若要使用認證註冊代理程式，請指定 by-credentials，然後使用 --reg-login 和 --reg-password 參數。您也可以僅使用 --reg-login 和 --reg-password 參數，如此就不一定要指定 --registration=by-credentials。 若要使用註冊權杖註冊代理程式，請指定 by-token，然後使用 --reg-token 參數。您也可以僅使用 --reg-token 參數，如此就不一定要指定 --registration=by-token。 若要使用 OAuth 2.0 通訊協定註冊代理程式，請指定 device-flow。安裝完成後，註冊頁面隨即自動開啟。 當您使用 --registration=device-flow 時，請指定確實的資料中心位址，作為 --reg-address 參數的值。這是是您

參數	描述
	在**登入** Cyber Protection 服務之後看到的 URL。例如，`https://eu2-cloud.company.com`。  請不要將 `--registration=device-flow` 和 `--quiet` 參數一起使用。
`--reg-address=<url>`	Cyber Protection 服務的 URL。您可以將此參數與 `--reg-login` 和 `--reg-password` 參數一起使用，或與 `--reg-token` 參數一起使用。 • 當您將其與 `--reg-login` 和 `--reg-password` 參數一起使用時，請指定您用來**登入** Cyber Protection 服務的位址。例如，`https://cloud.company.com`：  • 當您將其與 `--reg-token` 參數一起使用時，請指定確實的資料中心位址。這是是您在**登入** Cyber Protection 服務之後看到的 URL。例如，`https://eu2-cloud.company.com`。  請不要將 `https://cloud.company.com` 與 `--reg-token` 參數一起使用。
`--reg-login=<login>` `--reg-password=<password>`	在 Cyber Protection 服務中註冊代理程式所使用之帳戶的認證。這不得是合作夥伴系統管理員帳戶。 當您使用這些參數時，指定 `--registration` 參數是選擇性的。 請不要將這些參數與 `--reg-token` 參數一起使用。
`--reg-token=<token>`	註冊權杖。 註冊權杖是由 12 個字元組成的序列，並以連字號分成三個區段。如需有關如何產生註冊權杖的詳細資訊，請參閱 "產生註冊權杖" (第 108 頁)。 當您使用此參數時，指定 `--registration` 參數是選擇性的。 請不要將此參數與 `--reg-login` 和 `--reg-password` 參數一起使用。
`--register-only`	使用此參數略過安裝，並使用 OAuth 2.0 通訊協定 (device-flow) 註冊代理程式。

參數	描述
	安裝完成後，註冊頁面隨即自動開啟。 請不要將 `--register-only` 和 `--quiet` 參數一起使用。
代理程式服務的登入帳戶	
`--agent-account={system | new | custom}` 或 `--agent-account-login=<login>` `--agent-account-password=<password>`	使用此參數指定執行代理程式服務所使用的登入帳戶。如需有關登入帳戶的詳細資訊，請參閱 "變更 Windows 電腦上的登入帳戶" (第 73 頁)。 若要使用 **[本機系統]** 帳戶，請指定 `--agent-account=system`，或者不要在命令中使用 `--agent-account` 參數。 若要使用自動建立的新登入帳戶 **Acronis Agent User** 執行代理程式服務，請指定 `new`。 若要使用現有的帳戶執行代理程式服務，請使用 `--agent-account-login` 和 `--agent-account-password` 參數指定帳戶認證。在此情況下，指定 `--agent-account=custom` 參數是選擇性的。
vCenter/ESXi 參數	
`--esxi-address=<host>`	vCenter Server 或 ESXi 主機的主機名稱或 IP 位址。 安裝 VMware 用代理程式時，請使用此參數。
`--esxi-login=<login>` `--esxi-password=<password>`	用於 vCenter Server 或 ESXi 主機的存取認證。 安裝 VMware 用代理程式時，請使用這些參數。
Proxy 參數	
`--http-proxy={none | system | custom}`	使用此參數指定您要備份至雲端儲存以及從雲端儲存復原所使用的 HTTP Proxy 伺服器。 如果要停用 Proxy 伺服器連線，請指定 `--http-proxy=none`。 若要使用整個系統的 Proxy 伺服器，請指定 `--http-proxy=system`，或者不要在命令中使用 `--http-proxy` 參數。 若要使用其他 Proxy 伺服器，請使用 `--http-proxy-address`、`--http-proxy-login` 和 `--http-proxy-password` 參數，指定 Proxy 伺服器位址和認證。在此案例下，指定 `--http-proxy=custom` 參數是選擇性的。
`--http-proxy-address=<host>:<port>`	主機名稱或 IP 位址，以及自訂 HTTP Proxy 伺服器的連接埠。
`--http-proxy-login=<login>`	自訂 HTTP Proxy 伺服器的登入。

參數	描述
`--http-proxy-password=<password>`	自訂 HTTP Proxy 伺服器的密碼。
解除安裝參數	
`--remove-components=<component1,component2,...,componentN>`	要解除安裝的元件。請在 "用於自動安裝 (EXE) 的元件" (第 84 頁) 中查看可用元件的完整清單。 當您指定多個元件時，請以逗號分隔。請不要在逗號前後空格。 **重要事項** 使用此參數時，您僅能解除安裝元件。若要完整解除安裝產品，請移至 [Windows 控制台] > [程式和功能]，選擇產品，然後按一下 **[解除安裝]**。
`--delete-all-settings`	當您使用 `--remove-components` 參數刪除所有產品記錄、工作和組態設定時，請使用此選用參數。
`--anti-tamper-password=<password>`	解除安裝受密碼保護之 Windows 用代理程式或修改其元件所需的密碼。

用於自動安裝 (EXE) 的元件

下表摘要說明您可以透過 EXE 檔案，用於自動安裝的元件。使用值名稱指定 `--add-components` 參數的值。

如需詳細資訊，請參閱 "用於自動安裝 (EXE) 的參數" (第 80 頁)"用於自動安裝 (MSI) 的參數" (第 88 頁)

值名稱	元件說明
`agentForWindows`	Windows 用代理程式
`agentForSas`	Files Sync & Share 用代理程式
`agentForAd`	Active Directory 用代理程式
`agentForAmp`	防惡意軟體防護用代理程式和 URL 篩選用代理程式
`agentForDlp`	資料洩漏防禦用代理程式
`agentForEsx`	VMware 用代理程式 (Windows)
`agentForExchange`	Exchange 用代理程式
`agentForHyperV`	Hyper-V 用代理程式
`agentForOffice365`	Office 365 用代理程式
`agentForOracle`	適用於 Oracle 的代理程式

值名稱	元件說明
agentForSql	SQL 用代理程式
commandLine	命令列工具
mediaBuilder	可開機媒體組建
trayMonitor	Cyber Protect Monitor
all	此值結合所有元件。
allAgents	此值結合所有代理程式。

使用 MSI 檔案自動安裝和解除安裝

針對此類型的自動安裝，請使用 Windows Installer (Msiexec 程式)。使用安裝程式的圖形化使用者介面，事先解壓縮安裝套件和 MSI 檔案。

當您使用 MSI 檔案安裝元件時，可以使用 MST 轉換檔案自訂安裝參數。如需有關如何使用 MSI 和 MST 檔案組合的詳細資訊，請參閱 "安裝代理程式和元件 (MSI 和 MST 組合)" (第 86 頁)。您可以在 Active Directory 網域中使用這個安裝方法，透過 Windows 群組原則安裝保護代理程式。如需詳細資訊，請參閱 "透過群組原則部署保護代理程式" (第 120 頁)。

或者，您可以在命令列上手動指定安裝參數。在此情況下，您不需要 MST 檔案。如需詳細資訊，請參閱 "範例" (第 87 頁)。

解壓縮 MSI、MST 和 CAB 檔案

執行安裝程式的圖形化使用者介面，解壓縮 MSI、MST 和 CAB 檔案以及安裝套件。

若要解壓縮 MSI、MST 和 CAB 檔案

1. 執行安裝程式的圖形化使用者介面，然後按一下 **[為自動安裝建立 .mst 和 .msi 檔案]**。
2. 在 **[要安裝的項目]** 中，選擇您要安裝的元件，然後按一下 **[完成]**。

   注意事項
   修改現有安裝時，請選擇已安裝的元件和要新增的元件。

   這些元件的安裝套件將會從安裝程式中解壓縮為 CAB 檔案。
3. 在 **[註冊設定]** 中，選擇 **[使用認證]** 或 **[使用註冊權杖]**。根據您的選擇，指定認證或註冊權杖，然後按一下 **[完成]**。

   如需有關如何產生註冊權杖的詳細資訊，請參閱 "產生註冊權杖" (第 108 頁)。
4. [僅適用於在網域控制站上安裝時] 在 **[代理程式服務的登入帳戶]** 中，選擇 **[使用下列帳戶]**。指定執行代理程式服務所使用的使用者帳戶，然後按一下 **[完成]**。基於安全理由，安裝程式不會在網域控制站上自動建立新帳戶。

注意事項
您指定的使用者帳戶必須獲授予 [以服務方式登入] 權限。此帳戶必須已經在網域控制站上使用，才能在該電腦上建立其設定檔資料夾。

如需有關在唯讀網域控制站上安裝代理程式的詳細資訊，請參閱這篇知識庫文章。

5. 檢閱或修改將新增到 MST 檔案中的其他安裝設定，然後按一下 **[繼續]**。
6. 選擇將解壓縮 MSI、MST 和 CAB 檔案所在的資料夾，然後按一下 **[產生]**。

安裝代理程式和元件 (MSI 和 MST 組合)

使用 MST 檔案自訂 MSI 檔案的安裝設定。當您在多部電腦上透過 Windows 群組原則安裝代理程式時，請使用 MSI 和 MST 組合。如需詳細資訊，請參閱 "透過群組原則部署保護代理程式" (第 120 頁)。

若要使用 MSI 和 MST 檔案安裝元件

1. 解壓縮 MSI 和 MST 檔案，如 "解壓縮 MSI、MST 和 CAB 檔案" (第 85 頁) 中所述。
2. 在您要安裝元件所在電腦的命令列介面上，執行以下命令：

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

例如：

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

安裝與解除安裝代理程式和元件 (MSI 和直接選擇)

執行 MSI 檔案，手動選擇要安裝的元件，然後在命令列上指定其安裝參數。在此情況下，您不需要 MST 檔案。

若要安裝代理程式和元件

1. 解壓縮 MSI 檔案和安裝套件 (CAB 檔案)，如 "解壓縮 MSI、MST 和 CAB 檔案" (第 85 頁) 中所述。對於此安裝方法，您只需要 MSI 和 CAB 檔案。您不需要 MST 檔案。
2. 在電腦的命令列介面中，執行以下命令：

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

使用空格分隔參數，並使用逗號 (不加空格) 分隔參數的值。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
```

若要檢查可用的參數及其值，請參閱 "用於自動安裝 (MSI) 的參數" (第 88 頁)。

範例

- 安裝 Windows 用代理程式、防惡意軟體用代理程式和 URL 篩選用代理程式、命令列工具和 Cyber Protect Monitor。使用使用者名稱和密碼，在 Cyber Protection 服務中註冊工作負載。

```
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
```

- 安裝 Windows 用代理程式、命令列工具和 Cyber Protect Monitor。在 Windows 中，為代理程式服務建立一個新的登入帳戶。使用權杖，在 Cyber Protection 服務中註冊工作負載。

```
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
```

- 安裝 Windows 用代理程式、命令列工具、Oracle 用代理程式和 Cyber Protect Monitor。使用使用者名稱和以 base64 編碼的密碼，在 Cyber Protection 服務中登錄電腦。如果密碼包含特殊字元或空格，您可能需要將其編碼。如需有關如何將密碼編碼的詳細資訊，請參閱 "使用包含特殊字元或空格的密碼" (第 112 頁)。

```
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==
```

- 安裝 Windows 用代理程式、命令列工具和 Cyber Protect Monitor。使用權杖，在 Cyber Protection 服務中登錄電腦。設定 HTTP Proxy。

```
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
```

若要移除已安裝的元件

1. 解壓縮 MSI 檔案和安裝套件 (CAB 檔案)，如 "解壓縮 MSI、MST 和 CAB 檔案" (第 85 頁) 中所述。對於此安裝方法，您只需要 MSI 和 CAB 檔案。您不需要 MST 檔案。
2. 在電腦的命令列介面中，執行以下命令：

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

若要檢查可用的參數及其值，請參閱 "用於自動安裝 (MSI) 的參數" (第 88 頁)。

範例

- 移除 Cyber Protect Monitor。

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

若要解除安裝代理程式

1. 解壓縮 MSI 檔案和安裝套件 (CAB 檔案)，如 "解壓縮 MSI、MST 和 CAB 檔案" (第 85 頁) 中所述。對於此安裝方法，您只需要 MSI 和 CAB 檔案。您不需要 MST 檔案。
2. 在電腦的命令列介面中，執行以下命令：

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

若要檢查可用的參數及其值，請參閱 "用於自動安裝 (MSI) 的參數" (第 88 頁)。

範例

- 解除安裝 Windows 用代理程式及其所有元件。刪除所有記錄、工作和組態設定。

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

- 解除安裝受密碼保護的 Windows 用代理程式及其所有元件。刪除所有記錄、工作和組態設定。

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

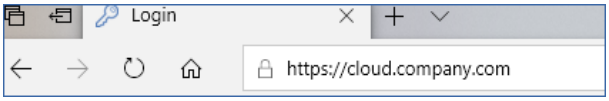
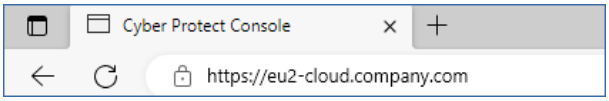
用於自動安裝 (MSI) 的參數

下表摘要說明使用 MSI 檔案時用於自動安裝的參數。

您也可以使用其他 `msiexec` 參數。例如，使用 `/qn` 防止顯示任何 GUI 元素。若要深入瞭解 `msiexec` 參數，請參閱 Microsoft 文件。

參數	描述
一般參數	
`ADDLOCAL=` <component1,component2,...,componentN>	要安裝的元件。請在 "用於自動安裝 (MSI) 的元件" (第 92 頁) 中查看可用元件的完整清單。 當您指定多個元件時，請以逗號分隔。請不要在逗號前後空格。

參數	描述
	注意事項 您必須為您要安裝的所有元件解壓縮檔案。如需有關如何解壓縮的詳細資訊，請參閱 "解壓縮 MSI、MST 和 CAB 檔案" (第 85 頁)。
TARGETDIR=<path>	將安裝所選元件的資料夾。如果指定的資料夾不存在，則會建立該資料夾。 如果您未指定此參數，將會使用預設資料夾：C:\Program Files\BackupClient。
REBOOT=ReallySuppress	如果您要在不重新啟動電腦的情況下安裝元件，請指定此參數。
/l*v <log file>	指定此參數可儲存詳細記錄。調查安裝問題時需要此記錄。
CURRENT_LANGUAGE=<language ID>	產品語言。 可用的值如下：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。 如果您未指定此參數，而且您執行安裝所在電腦的系統語言列在上方，則會使用系統語言。否則，此值會設定為 en。
SKIP_SHA2_KB_CHECK={0,1}	使用此參數選擇是否要檢查是否已在電腦上安裝 Microsoft 的 SHA2 程式碼簽署支援更新 (KB4474419)。此檢查只會在需要此更新的作業系統上執行。若要查看您的作業系統上是否需要此更新，請參閱 "支援的作業系統和環境" (第 22 頁)。 使用此參數搭配設定為 1 的值可略過檢查。 如果您未指定此參數或將其值設定為 0，而且在電腦上找不到 SHA2 程式碼簽署支援更新，則安裝會失敗。
FSS_ONBOARDING_AUTO_START={0,1}	使用此參數搭配設定為 1 的值可在自動安裝後顯示 File Sync & Share 上線精靈。 如果您未指定此參數或將其值設定為 0，則不會顯示上線精靈。
註冊參數	
REGISTRATION_ADDRESS	Cyber Protection 服務的 URL。您可以將此參數與 REGISTRATION_LOGIN 和 REGISTRATION_PASSWORD 參數一起使用，或與 REGISTRATION_TOKEN 一起使用。 • 當您將其與 REGISTRATION_LOGIN 和 REGISTRATION_

參數	描述
	PASSWORD 參數一起使用時，請指定您用來**登入** Cyber Protection 服務的位址。例如，https://cloud.company.com：  • 當您將其與 REGISTRATION_TOKEN 參數一起使用時，請指定確實的資料中心位址。這是是您在**登入** Cyber Protection 服務之後看到的 URL。例如，https://eu2-cloud.company.com。  請不要將 https://cloud.company.com 與 REGISTRATION_TOKEN 參數一起使用。
REGISTRATION_LOGIN REGISTRATION_PASSWORD	在 Cyber Protection 服務中註冊代理程式所使用之帳戶的認證。這不得是合作夥伴系統管理員帳戶。 請不要將這些參數與 REGISTRATION_TOKEN 參數一起使用。
REGISTRATION_PASSWORD_ENCODED	在 Cyber Protection 服務中註冊代理程式所使用之帳戶的密碼 (以 base64 編碼)。如需有關如何將密碼編碼的詳細資訊，請參閱 "使用包含特殊字元或空格的密碼" (第 112 頁)。
REGISTRATION_TOKEN	註冊權杖。 註冊權杖是由 12 個字元組成的序列，並以連字號分成三個區段。如需有關如何產生註冊權杖的詳細資訊，請參閱 "產生註冊權杖" (第 108 頁)。 請不要將此參數與 REGISTRATION_LOGIN 和 REGISTRATION_PASSWORD 參數一起使用。
REGISTRATION_REQUIRED={0,1}	使用此參數選擇註冊失敗時發生的情況。 如果您將值設定為 1，安裝也會失敗。如果您將值設定為 0，或者不指定此參數，即使註冊失敗，安裝也會成功完成。
代理程式服務的登入帳戶	
MMS_USE_SYSTEM_ACCOUNT={0,1}	將此參數與值 1 一起使用時，可使用 **[本機系統]** 登入帳戶執行服務。 如需有關登入帳戶的詳細資訊，請參閱 "變更 Windows 電腦上的登入帳戶" (第 73 頁)。

參數	描述
MMS_CREATE_NEW_ACCOUNT={0,1}	將此參數與值 1 一起使用時，可使用自動建立的新登入帳戶 **Acronis Agent User** 執行代理程式服務。
MMS_SERVICE_USERNAME=<user name> MMS_SERVICE_PASSWORD=<password>	使用這些參數指定執行代理程式服務將使用的現有登入帳戶。
vCenter/ESXi 參數	
SET_ESX_SERVER={0,1}	安裝 VMware 用代理程式時，請使用此參數。 如果您將值設定為 0，VMware 用代理程式將不會連線至 vCenter Server 或 ESXi 主機。 如果您將值設定為 1，請指定下列參數：ESX_HOST、EXI_USER、ESX_PASSWORD。
ESX_HOST=<host name>	vCenter Server 或 ESXi 主機的主機名稱或 IP 位址。
ESX_USER=<user name> ESX_PASSWORD=<password>	用於 vCenter Server 或 ESXi 主機的存取認證。
Proxy 參數	
HTTP_PROXY_ADDRESS=<IP address> HTTP_PROXY_PORT=<port>	使用這些參數指定代理程式將使用的 HTTP Proxy 伺服器。 如果您未使用 Proxy 伺服器，請不要指定這些參數。
HTTP_PROXY_LOGIN=<login> HTTP_PROXY_PASSWORD=<password>	HTTP Proxy 伺服器的認證。 如果 Proxy 伺服器需要驗證，請使用這些參數。
解除安裝參數	
REMOVE={<list of components>|ALL}	要解除安裝的元件。 當您指定多個元件時，請以逗號分隔。請不要在逗號前後空格。 若要移除所有產品元件，請將值設定為 ALL。
DELETE_ALL_SETTINGS={0, 1}	若要刪除所有產品記錄、工作和組態設定，請將值設定為 1。 當您使用 REMOVE 參數時，請使用此選用參數。
ANTI_TAMPER_PASSWORD=<password>	解除安裝受密碼保護之 Windows 用代理程式或修改其元件所需的密碼。

用於自動安裝 (MSI) 的元件

下表摘要說明您可以透過 MSI 檔案，用於自動安裝的元件。使用值名稱指定 ADDLOCAL 參數的值。如需詳細資訊，請參閱 "用於自動安裝 (MSI) 的參數" (第 88 頁)。

值名稱	元件說明	務必一起安裝	位元
AgentFeature	適用於代理程式的核心元件		32 位元/64 位元
MmsMspComponents	適用於備份的核心元件	AgentFeature	32 位元/64 位元
BackupAndRecoveryAgent	Windows 用代理程式	MmsMspComponents	32 位元/64 位元
AmpAgentFeature	Agent for Antimalware protection	BackupAndRecoveryAgent	32 位元/64 位元
UrlFilteringAgentFeature	Agent for URL Filtering	BackupAndRecoveryAgent	32 位元/64 位元
DlpAgentFeature	資料洩漏防禦用代理程式	BackupAndRecoveryAgent	32 位元/64 位元
SasAgentFeature	File Sync & Share 用代理程式	TrayMonitor	32 位元/64 位元
ArxAgentFeature	Exchange 用代理程式	MmsMspComponents	32 位元/64 位元
ArsAgentFeature	SQL 用代理程式	BackupAndRecoveryAgent	32 位元/64 位元
ARADAgentFeature	Active Directory 用代理程式	BackupAndRecoveryAgent	32 位元/64 位元
ArxOnlineAgentFeature	Microsoft 365 用代理程式	MmsMspComponents	32 位元/64 位元

OracleAgentFeature	適用於 Oracle 的代理程式	BackupAndRecoveryAgent	32 位元/64 位元
AcronisESXSupport	VMware ESX(i) 用代理程式 (Windows)	BackupAndRecoveryAgent	64 位元
HyperVAgent	Hyper-V 用代理程式	BackupAndRecoveryAgent	32 位元/64 位元
CommandLineTool	命令列工具		32 位元/64 位元
TrayMonitor	Cyber Protect Monitor	AgentFeature	32 位元/64 位元
BackupAndRecoveryBootableComponents	可開機媒體組建		32 位元/64 位元

在 Linux 中安裝和解除安裝保護代理程式

本節描述如何使用命令列，在執行 Linux 的電腦上以自動模式安裝或解除安裝保護代理程式。

若要安裝代理程式

1.開啟終端機。

2。執行下列其中一項操作：

- 若要在命令列上指定參數以開始安裝，請執行下列命令：

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

  其中，<package name> 是安裝套件 (.i686 或 .x86_64 檔案) 的名稱。所有可用的參數及其值詳述於 "自動安裝或解除安裝參數" (第 94 頁) 中。
- 若要使用在另一個文字檔案中指定的參數開始安裝，請執行下列命令：

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

  如果您不想要在命令列上輸入敏感資訊，此方法可能會很實用。在此情況下，您可以在另一個文字檔案中指定組態設定，並確保只有您可以存取該檔案。將每個參數放在新的一行，後面緊接著該參數的值，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
```

如果在命令列和文字檔案中指定相同的參數，命令列值將位於前面。

3.如果在電腦上啟用 UEFI 安全開機，您會在安裝後收到您需要重新啟動系統的通知。請務必記住應該使用的密碼 (根使用者或 "acronis" 的密碼)。在系統重新啟動期間，選擇 MOK (電腦擁有者金鑰) 管理、選擇 **[註冊 MOK]**，然後使用建議的密碼，註冊金鑰。

如果您在代理程式安裝之後啟用 UEFI 安全開機，請重複安裝步驟，包括步驟 3。否則，備份將會失敗。

若要解除安裝代理程式

1. 開啟終端機。
2. 執行下列其中一項操作：
   - 若要解除安裝代理程式，並移除所有記錄、工作和組態設定，請執行下列命令：

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

   - 若要解除安裝代理程式，但保留其 ID (例如，如果您打算之後安裝代理程式)，請執行下列命令：

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

   - 若要使用安裝檔案解除安裝代理程式，請執行下列命令：

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

     其中，<package name> 是安裝套件 (.i686 或 .x86_64 檔案) 的名稱。所有可用的參數及其值詳述於 "自動安裝或解除安裝參數" (第 94 頁) 中。

     注意事項
     僅在安裝套件的版本與所安裝的代理程式版本相同時，以及 /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall 損毀或無法存取時，才使用此命令。

自動安裝或解除安裝參數

本節描述在 Linux 中自動安裝或解除安裝期間所使用的參數。

自動安裝的最小設定包括 -a 和註冊參數 (例如，--login 和 --password 參數；--rain 和 --token 參數)。您可以使用更多參數自訂您的安裝。

安裝參數

基本參數

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

要安裝的元件，以逗點區隔，且沒有空格字元。下列元件可在 .x86_64 安裝套件中取得：

元件	元件說明
BackupAndRecoveryAgent	Linux 用代理程式
AgentForPCS	Virtuozzo 用代理程式
OracleAgentFeature	適用於 Oracle 的代理程式
MySQLAgentFeature	MySQL/MariaDB 用代理程式

若無此參數，則將安裝以上所有元件。

Virtuozzo 用代理程式、Oracle 用代理程式和 MySQL/MariaDB 用代理程式需要也安裝 Linux 用代理程式。

.i686 安裝套件僅包含 BackupAndRecoveryAgent。

{-a|--auto}

安裝和註冊程序將會完成，而不需要其他任何使用者互動。使用此參數時，您必須使用 --token 參數或使用 --login 和 --password 參數，指定在 Cyber Protection 服務中註冊代理程式所使用的帳戶。

{-t|--strict}

若指定此參數，則在安裝期間出現的任何警告都會導致安裝失敗。若無此參數，即使出現警告，安裝也會順利完成。

{-n|--nodeps}

在安裝期間將會忽略缺少所需的 Linux 套件。

{-d|--debug}

在詳細模式下寫入安裝記錄。

--options-file=<位置>

安裝參數將會從文字檔案而非命令列讀取。

--language=<語言 ID>

產品語言。可用的值如下：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。

如果未指定此參數，則產品語言將由您的系統語言定義，但前提是該語言在上述清單中。否則，產品語言將設定為 [英文] (en)。

註冊參數

指定下列其中一個參數：

- `{-g|--login=}`<使用者名稱> 和 `{-w|--password=}`<密碼>

  在 Cyber Protection 服務中註冊代理程式所使用之帳戶的認證。這不得是合作夥伴系統管理員帳戶。

- `--token=`<權杖>

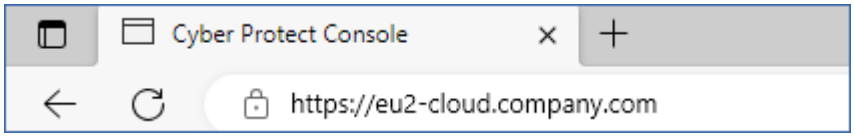
  註冊權杖是由 12 個字元組成的序列，並以連字號分成三個區段。如需詳細資訊，請參閱 "產生註冊權杖" (第 108 頁)。

  注意事項
  使用 `--token` 參數時，也必須包含 `{-C|--rain=}` 參數，並指定確切的資料中心位址。
  您無法使用 `--token` 參數搭配 `--login`、`--password` 和 `--register-with-credentials` 參數。

  - `{-C|--rain=}`<服務位址>

    Cyber Protection 服務的 URL。

    您必須使用 `{-C|--rain=}` 參數，並在使用 `--token` 參數時指定確切的資料中心位址。確切的資料中心位址是**您登入** Cyber Protection 主控台後看到的 URL。例如：

    當您使用 `--login` 和 `--password` 參數進行註冊時，可以略過 `{-C|--rain=}` 參數，因為安裝程式預設會使用正確的位址。

- `--register-with-credentials`

  如果已指定此參數，安裝程式的圖形介面將會啟動。若要完成註冊，請輸入在 Cyber Protection 服務中註冊代理程式所使用之帳戶的使用者名稱和密碼。這不得是合作夥伴系統管理員帳戶。

- `--skip-registration`

  如果您想要安裝代理程式，但是您打算稍後在 Cyber Protection 服務中註冊該代理程式，請使用此參數。如需有關操作方式的詳細資訊，請參閱 "使用命令列介面註冊和取消註冊工作負載" (第 111 頁)。

其他參數

`--http-proxy-host=`<IP 位址> 和 `--http-proxy-port=`<連接埠>

代理程式將用於從雲端備份和復原，以及用於連線至管理伺服器的 HTTP Proxy 伺服器。若無這些參數，將不會使用任何 Proxy 伺服器。

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

HTTP Proxy 伺服器的認證。如果伺服器需要驗證，請使用這些參數。

`--tmp-dir=<位置>`

指定安裝期間存放暫存檔的資料夾。預設資料夾為 **/var/tmp**。

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

即使您的系統可能已經存在可轉散發程式庫，也將在安裝期間使用。

`--skip-prereq-check`

將不會檢查是否已安裝編譯 snapapi 模組所需的套件。

`--force-weak-snapapi`

安裝程式將不會編譯 snapapi 模組。它將改用可能無法與 Linux 核心完全相符的現成模組。不建議您使用此選項。

`--skip-svc-start`

安裝後將不會自動啟動此服務。此參數最常搭配 `--skip-registration` 參數使用。

資訊參數

`{-?|--help}`

顯示參數說明。

`--usage`

顯示命令使用的簡要說明。

`{-v|--version}`

顯示安裝套件版本。

`--product-info`

顯示產品名稱和安裝套件版本。

`--snapapi-list`

顯示可用的現成 snapapi 模組。

`--components-list`

顯示安裝程式元件。

舊版功能的參數

這些參數與舊版元件 agent.exe 相關。

`{-e|--ssl=}<路徑>`

指定用於 SSL 通訊之自訂憑證檔案的路徑。

`{-p|--port=}<連接埠>`

指定 agent.exe 接聽連線的連接埠。預設連接埠為 9876。

解除安裝參數

`{-u|--uninstall}`

解除安裝產品。

`--purge`

解除安裝產品並移除其記錄、工作和組態設定。當您使用 `--purge` 參數時，不需要明確地指定 `--uninstall` 參數。

範例

- 安裝 Linux 用代理程式但不註冊。

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

- 安裝 Linux 用代理程式、Virtuozzo 用代理程式和 Oracle 用代理程式，並使用認證進行註冊。

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

- 安裝 Oracle 用代理程式和 Linux 用代理程式，並使用註冊權杖進行註冊。

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

- 使用另一個文字檔案中的組態設定，安裝 Linux 用代理程式、Virtuozzo 用代理程式和 Oracle 用代理程式。

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

- 解除安裝 Linux 用代理程式、Virtuozzo 用代理程式和 Oracle 用代理程式，並移除其所有記錄、工作和組態設定。

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

在 macOS 中安裝和解除安裝保護代理程式

本節描述如何使用命令列，在執行 macOS 的電腦上，以自動模式安裝和解除安裝保護代理程式。

所需權限

在 Mac 工作負載上起始自動安裝之前，您必須修改 [隱私喜好設定原則控制]，以允許應用程式在工作負載的 macOS 中，存取核心和系統擴充功能，才能啟用 Cyber Protection 代理程式的安裝。請參閱 "在 macOS 中自動安裝所需的權限" (第 100 頁)。

部署 PPPC 承載之後，您可以繼續以下的程序。

若要下載安裝檔案 (.dmg)

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 按一下 **[新增]**，然後按一下 **[Mac]**。

若要安裝代理程式

1. 開啟終端機。
2. 建立一個您將在其中掛載安裝檔案 (.dmg) 的暫存目錄。

   ```
   mkdir <dmg_root>
   ```

   在這裡，<dmg_root> 是您選擇的名稱。
3. 掛載 .dmg 檔案。

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

   在這裡，<dmg_file> 是安裝檔案的名稱。例如，**Cyber_Protection_Agent_for_MAC_x64.dmg**。
4. 執行安裝程式。
   - 如果您使用適用於 Mac 的完整安裝程式 (例如 CyberProtect_AgentForMac_x64.dmg 或 CyberProtect_AgentForMac_arm64.dmg)，請執行下列命令。

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

     注意事項
     如果您需要為 File Sync & Share 啟用自動上線，請改為執行以下命令。此選項將要求系統管理員密碼。

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

   - 如果您使用適用於 Mac 的通用安裝程式 (例如 CyberProtect_AgentForMac_web.dmg)，請執行下列命令。

     ```
     sudo <dmg_root>/Install.app/Contents/MacOS/cyber_installer -a
     ```
5. 卸離安裝檔案 (.dmg)。

   ```
   hdiutil detach <dmg_root>
   ```

範例

```
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
```

若要解除安裝代理程式

1. 開啟終端機。
2. 執行下列其中一項操作：
   - 若要解除安裝代理程式，請執行下列命令：

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

   - 若要解除安裝代理程式，並移除所有記錄、工作和組態設定，請執行下列命令：

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

在 macOS 中自動安裝所需的權限

在 Mac 工作負載上起始自動安裝之前，您必須修改 [隱私喜好設定原則控制]，以允許應用程式在工作負載的 macOS 中，存取核心和系統擴充功能，才能啟用 Cyber Protection 代理程式的安裝。方法是，部署自訂的 PPPC 承載，或在工作負載的圖形化使用者介面中設定喜好設定。需要下列權限。

macOS 11 (Big Sur) 或更新版本的需求

索引標籤	區段	欄位	數值

隱私喜好設定原則控制	應用程式存取	識別元	com.acronis.backup

		識別碼類型	套件 ID
		程式碼需求	`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`
		應用程式或服務	SystemPolicyAllFiles
		ACCESS	允許
	應用程式存取	識別元	com.acronis.backup.aakore
		識別碼類型	套件 ID
		程式碼需求	`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`
		應用程式或服務	SystemPolicyAllFiles
		ACCESS	允許
	應用程式存取	已識別	com.acronis.backup.activeprotection
		識別碼類型	套件 ID
		程式碼需求	`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`
		應用程式或服務	SystemPolicyAllFiles
		ACCESS	允許

	應用程式存取	識別元	cyber-protect-service
		識別碼類型	套件 ID
		程式碼需求	`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`
		應用程式或服務	SystemPolicyAllFiles
		ACCESS	允許
系統擴充功能		允許使用者核准系統擴充功能	Enabled
	允許小組 ID 和系統擴充功能	顯示名稱	Acronis Cyber Protection Agent 系統擴充功能
		系統擴充功能類型	允許的小組識別碼
		小組識別碼	ZU2TV78AA6

macOS 11 版之前的需求

索引標籤	區段	欄位	數值

隱私喜好設定原則控制	應用程式存取	識別元	com.acronis.backup

		識別碼類型	套件 ID
		程式碼需求	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
		應用程式或服務	SystemPolicyAllFiles
		ACCESS	允許
	應用程式存取	識別元	com.acronis.backup.aakore
		識別碼類型	套件 ID
		程式碼需求	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
		應用程式或服務	SystemPolicyAllFiles
		ACCESS	允許
	應用程式存取	已識別	com.acronis.backup.activeprotection
		識別碼類型	套件 ID
		程式碼需求	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
		應用程式或服務	SystemPolicyAllFiles
		ACCESS	允許
	應用程式存取	識別元	cyber-protect-service
		識別碼類型	套件 ID
		程式碼需求	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
		應用程式或服務	SystemPolicyAllFiles
		ACCESS	允許

核准的核心擴充功能		允許使用者核准核心擴充功能	Enabled
		允許標準使用者核准舊版核心擴充功能 (macOS 11 或更新版本)	Enabled
	核准的小組 ID 和核心擴充功能	核准的小組 ID - 顯示名稱	Acronis Cyber Protection Agent 核心擴充功能
		小組 ID	ZU2TV78AA6
		核心擴充功能套件 ID	• com.acronis.systeminterceptors • com.acronis.ngscan • com.acronis.notifyframework
系統擴充功能		允許使用者核准系統擴充功能	Enabled
	允許小組 ID 和系統擴充功能	顯示名稱	Acronis Cyber Protection Agent System Extensions
		系統擴充功能類型	允許的小組識別碼
		小組識別碼	ZU2TV78AA6

工作負載註冊

註冊是將安裝保護代理程式所在的工作負載連接到客戶租用戶中的使用者帳戶。註冊完成後，您可以在 Cyber Protect 主控台的 **[裝置]** > **[包含代理程式的電腦]** 下查看工作負載。您可以透過對已註冊的工作負載套用計劃來管理它們。

使用圖形化使用者介面安裝保護代理程式時，註冊是安裝程序的一部分。

使用命令列介面時，您可以將註冊當作獨立程序執行。

使用圖形化使用者介面註冊工作負載

使用圖形化使用者介面安裝保護代理程式時，註冊是安裝程序的一部分。

下列註冊方法可供使用：

- 在 Cyber Protect 主控台中註冊
- 使用使用者帳戶認證註冊
- 使用註冊權杖註冊

當您解除安裝代理程式時，會自動取消註冊該代理程式。

使用 Cyber Protect 主控台註冊工作負載

此程序適用於當您使用預設安裝設定 (**[註冊設定]** > **[使用 Cyber Protect 主控台]**) 安裝保護代理程式時。

若要從 Cyber Protect 主控台註冊工作負載

1. 在安裝精靈中，按一下 **[註冊工作負載]**。
   Cyber Protect 主控台隨即開啟。

   注意事項
   在完成註冊之前，請勿關閉安裝精靈。否則，您將必須重複安裝，並重新開始註冊。

2. 登入 Cyber Protect 主控台。
3. [如果以系統管理員身分登入] 在 **[工作負載註冊]** 畫面上，選擇要註冊工作負載所使用的帳戶。
   此帳戶必須是客戶租用戶中的帳戶。合作夥伴系統管理員可以查看所管理的客戶租用戶，並使用這些租用戶的帳戶註冊工作負載。
4. 按一下 **[驗證代碼]**。
5. 按一下 **[註冊]**。

因此，工作負載會使用指定的使用者帳戶註冊。

使用使用者認證註冊工作負載

您可以修改預設安裝程序並選擇使用使用者名稱和密碼註冊，而不是在 Cyber Protect 主控台中註冊。

若要使用使用者名稱和密碼註冊工作負載

1. 在安裝精靈中，按一下 **[自訂安裝設定]**。
2. 在 **[註冊設定]** 區段中，按一下 **[變更]**。
3. 選擇 **[使用認證]**。
4. 使用您註冊工作負載所要使用之帳戶的使用者名稱和密碼。
   此帳戶必須是客戶租用戶中的帳戶。

   注意事項
   您只能使用未啟用雙重驗證機制的帳戶。

5. 按一下 **[完成]**，然後完成安裝。

使用註冊權杖註冊工作負載

您可以修改預設安裝程序並選擇使用註冊權杖註冊，而不是在 Cyber Protect 主控台中註冊。

若要使用註冊權杖註冊工作負載

1. 在安裝精靈中，按一下 **[自訂安裝設定]**。
2. 在 **[註冊設定]** 區段中，按一下 **[變更]**。

3. 選擇 **[使用註冊權杖]**。
4. 輸入註冊權杖。
5. 按一下 **[完成]**，然後完成安裝。

產生註冊權杖

註冊權杖是由 12 個字元組成的序列，並以連字號分成三個區段。註冊權杖會將使用者的身分識別傳遞至代理程式安裝程式，但不會儲存用於 Cyber Protect 主控台的使用者認證。這可讓使用者無需登入主控台，即可使用其帳戶註冊工作負載，或將保護計劃套用到工作負載中。

注意事項
工作負載註冊期間不會自動套用保護計劃。套用保護計劃是一項單獨的工作。

基於安全性，權杖的存留時間受到限制，但您可以調整。預設存留時間為 3 天。

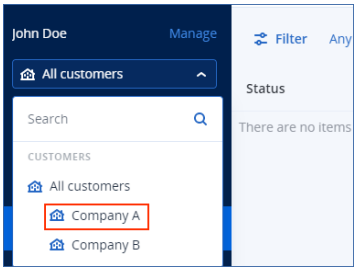
系統管理員可以為其管理的租用戶中的所有使用者帳戶產生註冊權杖。使用者只能為自己的帳戶產生註冊權杖。

若要產生註冊權杖

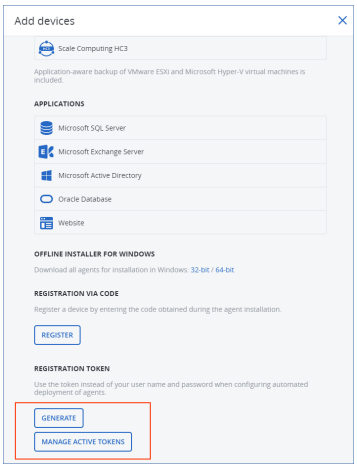
以系統管理員身分

1. 以系統管理員身分登入 Cyber Protect 主控台。
   如果您已經登入管理入口網站，可以前往 Cyber Protect 主控台，方法是，導覽至 **[監控]** > **[使用狀況]**，然後在 **[保護]** 索引標籤下，按一下 **[管理服務]**。

   [針對管理客戶租用戶的合作夥伴系統管理員] 在 Cyber Protect 主控台中，針對您要為其產生權杖的使用者，選擇其租用戶。您無法在 **[所有客戶]** 層級產生權杖。



2. 在 **[裝置]** 底下，按一下 **[所有裝置]** > **[新增]**。
   [新增裝置] 窗格隨即在右側開啟。
3. 向下捲動至 **[註冊權杖]**，然後按一下 **[產生]**。



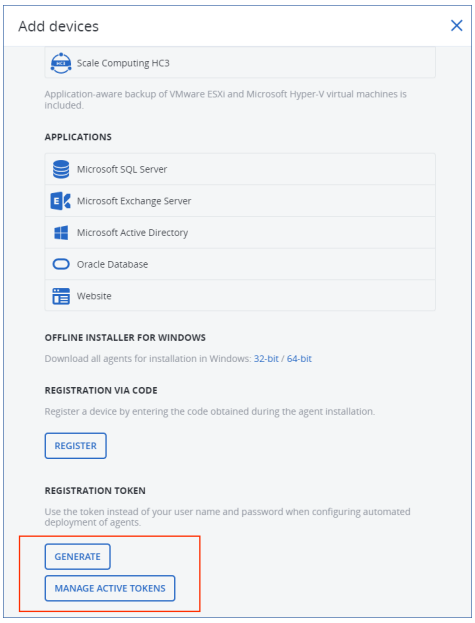
4. 指定權杖存留時間。
5. 選擇您要為其產生權杖的使用者。

注意事項
使用權杖時，工作負載將以您在此處選擇的使用者帳戶註冊。

6. [選擇性] 若要讓權杖的使用者在新增的工作負載上套用和撤銷保護計劃，請從下拉式清單中選擇該計劃。
   請注意，您需要執行將在新增的工作負載上套用或撤銷保護計劃的指令碼。如需詳細資訊，請參閱這篇知識庫文章。
7. 按一下 **[產生權杖]**。
8. 按一下 **[複製]**，將權杖複製到您的裝置剪貼簿，或手動記下權杖。

以使用者身分

1. 登入 Cyber Protect 主控台。
2. 按一下 **[裝置]** > **[所有裝置]** > **[新增]**。
   [新增裝置] 窗格隨即在右側開啟。
3. 向下捲動至 **[註冊權杖]**，然後按一下 **[產生]**。



4. 指定權杖存留時間。
5. 按一下 **[產生權杖]**。
6. 按一下 **[複製]**，將權杖複製到您的裝置剪貼簿，或手動記下權杖。

管理註冊權杖

您可以檢視和刪除作用中的註冊權杖。

若要檢視註冊權杖

1. 登入 Cyber Protect 主控台。
2. 按一下 **[裝置]** > **[所有裝置]** > **[新增]**。
3. 向下捲動至 **[註冊權杖]**，然後按一下 **[管理使用中的權杖]**。
   其中包含針對租用戶所產生之使用中權杖的清單隨即在右側開啟。

> **注意事項**
> 基於安全，在 **[權杖]** 欄中，只會顯示權杖值的前兩個字元。

若要刪除註冊權杖

1. 登入 Cyber Protect 主控台。
2. 按一下 **[裝置]** > **[所有裝置]** > **[新增]**。
3. 向下捲動至 **[註冊權杖]**，然後按一下 **[管理使用中的權杖]**。
   其中包含針對租用戶所產生之使用中權杖的清單隨即在右側開啟。

> **注意事項**
> 基於安全，在 **[權杖]** 欄中，只會顯示權杖值的前兩個字元。

4. 選擇權杖，然後按一下 **[刪除]**。

使用命令列介面註冊和取消註冊工作負載

使用命令列介面時，您可以將註冊當作獨立程序執行。

因此，例如，如果您想要使用其他帳戶註冊保護代理程式，則無需解除安裝該保護代理程式。

使用使用者認證註冊工作負載

使用您註冊工作負載所要使用的帳戶的使用者名稱和密碼。此帳戶必須是客戶租用戶中的帳戶。如果密碼包含特殊字元或空格，請參閱 "使用包含特殊字元或空格的密碼" (第 112 頁)。

服務位址是您用來**登入** Cyber Protection 服務的 URL。

例如，`https://cloud.company.com`。

若要使用使用者名稱和密碼註冊工作負載

在 Windows 中

- 在命令提示字元中，執行下列命令：

```
"%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

- 在命令提示字元中，執行下列命令：

```
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

重要事項

如果您使用的是 macOS 10.14 或更新版本，請授予保護代理程式的完整磁碟存取權。方法是，移至 **[應用程式]** > **[公用程式]**，然後執行 **[Cyber Protect 代理程式助理]**。接著，依照應用程式視窗中的指示進行。

- 在命令提示字元中，執行下列命令：

```
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
```

使用包含特殊字元或空格的密碼

如果密碼包含特殊字元或空格，請在命令列上輸入密碼時，以引號括住。

例如，在 Windows 中，執行此命令：

命令範本：

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

命令範例：

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

如果此命令失敗，請在 https://www.base64encode.org/，將密碼編碼為 base64 格式。接著，在命令列上，使用 -b 或 --base64 參數指定編碼的密碼。

例如，在 Windows 中，執行此命令：

命令範本：

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

命令範例：

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

使用註冊權杖註冊工作負載

註冊權杖是由 12 個字元組成的序列，並以連字號分成三個區段。註冊權杖會將使用者的身分識別傳遞至代理程式安裝程式，但不會儲存用於 Cyber Protect 主控台的使用者認證。這可讓使用者無需登入主控台，即可使用其帳戶註冊工作負載，或將保護計劃套用到工作負載中。

如需詳細資訊，請參閱 "產生註冊權杖" (第 108 頁)。

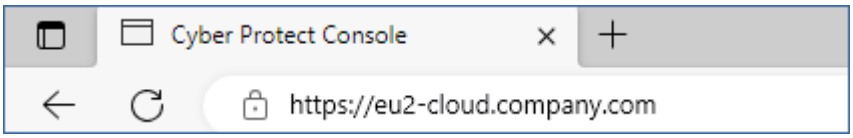
注意事項

工作負載註冊期間不會自動套用保護計劃。套用保護計劃是一項單獨的工作。

如需詳細資訊，請參閱本知識庫文章。

當您使用註冊權杖時，必須指定確實的資料中心位址。這是您在登入 服務**之後**看到的 URL。

例如，`https://eu2-cloud.company.com`。



若要使用註冊權杖註冊工作負載

在 Windows 中

- 在命令提示字元中，執行下列命令：

```
"%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

- 在命令提示字元中，執行下列命令：

```
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

重要事項

如果您使用的是 macOS 10.14 或更新版本，請授予保護代理程式的完整磁碟存取權。方法是，移至 **[應用程式]** > **[公用程式]**，然後執行 **[Cyber Protect 代理程式助理]**。接著，依照應用程式視窗中的指示進行。

- 在命令提示字元中，執行下列命令：

```
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
```

虛擬裝置

1. 在虛擬裝置的主控台中，按下 CTRL+SHIFT+F2 以開啟命令列介面。
2. 在命令提示字元中，執行下列命令：

   ```
   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. 若要返回裝置的圖形化介面，按下 ALT+F1。

取消註冊工作負載

您可以從命令列介面取消註冊保護代理程式，而無需解除安裝。

若要取消註冊工作負載

在 Windows 中

- 在命令提示字元中，執行下列命令：

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

例如：

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

在 Linux 中

- 在命令提示字元中，執行下列命令：

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

在 macOS 中

在命令提示字元中，執行下列命令：

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

虛擬裝置

1. 在虛擬裝置的主控台中，按下 CTRL+SHIFT+F2 以開啟命令列介面。
2. 在命令提示字元中，執行下列命令：

```
register_agent -o unregister
```

3. 若要返回裝置的圖形化介面，按下 ALT+F1。

變更工作負載的註冊

您可以在新的租用戶中或使用新的使用者帳戶註冊工作負載，以變更其註冊。

重要事項
當您變更工作負載的註冊時，將會撤銷其所套用的所有保護計劃。若要繼續保護工作負載，請為其套用新的保護計劃。

如果您在新的租用戶中註冊工作負載，該工作負載將無法存取原始租用戶雲端儲存空間中的備份。非雲端儲存空間中的備份仍可供存取。

若要變更工作負載的註冊

透過使用命令列介面

1. 取消註冊保護代理程式，如 "取消註冊工作負載" (第 114 頁) 中所述。
2. 在新的租用戶中或使用新的使用者帳戶註冊保護代理程式，如 "使用使用者認證註冊工作負載" (第 111 頁) 或 "使用註冊權杖註冊工作負載" (第 113 頁) 中所述。

透過使用圖形化使用者介面

1. 解除安裝保護代理程式。
2. 安裝保護代理程式，然後在新的租用戶中或使用新的使用者帳戶註冊該保護代理程式。

如需有關如何安裝並註冊代理程式的詳細資訊，請參閱 "使用圖形化使用者介面安裝保護代理程式" (第 72 頁)。

將工作負載移至另一個租用戶

將工作負載移至另一個租用戶不受到原生支援。您可以取消註冊工作負載，然後在其他租用戶中註冊該工作負載，作為因應措施。所有已套用的保護計劃都將從該工作負載撤銷，而且將失去對其在原始租用戶雲端儲存空間之備份的存取權。

如需有關如何在新租用戶中註冊工作負載或使用新的使用者帳戶註冊工作負載的詳細資訊，請參閱 "變更工作負載的註冊" (第 115 頁)。

更新保護代理程式

您可以使用 Cyber Protect 主控台，或下載並執行安裝檔案，以手動更新所有代理程式。

您可以針對下列代理程式設定自動更新：

- Windows 用代理程式
- Linux 用代理程式
- Mac 用代理程式
- File Sync & Share 用 Cyber Files Cloud 代理程式

自動更新代理程式需要在下列位置中有 4.2 GB 的可用空間，也可以使用 Cyber Protect 主控台進行手動更新：

- 若是 Linux – 根目錄
- 若為 Windows – 安裝代理程式的磁碟區

在 macOS 中更新代理程式需要 5 GB 的可用空間 – 在根目錄中。

注意事項
[若是以虛擬裝置形式提供的所有代理程式，包括 VMware 用代理程式、Scale Computing 用代理程式、Virtuozzo Hybrid Infrastructure 用代理程式、RHV (oVirt) 用代理程式]

若要自動或手動更新位於 Proxy 後面的虛擬裝置，必須在每個虛擬裝置上設定 Proxy 伺服器，如下所示。

在 `/opt/acronis/etc/va-updater/config.yaml` 檔案中，將下列一行加入至檔案底部，並輸入您環境專用的值：

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

手動更新保護代理程式

您可以使用 Cyber Protect 主控台，或下載並執行安裝檔案，以更新代理程式。

具有下列版本的虛擬裝置僅能使用 Cyber Protect 主控台更新：

- VMware 用代理程式 (虛擬裝置)：12.5.23094 版和更新版本。
- Virtuozzo Hybrid Infrastructure 用代理程式 (虛擬裝置)：12.5.23094 版和更新版本。

具有下列版本的代理程式也可以使用 Cyber Protect 主控台更新：

- Windows 用代理程式、VMware 用代理程式 (Windows)、Hyper-V 用代理程式：12.5.21670 版及更新版本。
- Linux 用代理程式：12.5.23094 版及更新版本。
- 其他代理程式：12.5.23094 版及更新版本。

若要尋找代理程式版本，請在 Cyber Protect 主控台中選擇電腦，然後按一下 **[詳細資料]**。

若要更新這些代理程式的舊版代理程式，請下載並安裝最新的版本。若要尋找下載連結，請按一下 **[所有裝置]** > **[新增]**。

必要條件

在 Windows 電腦上，Cyber Protect 功能需要使用 Microsoft Visual C++ 2017 可轉散發套件。請確認已在電腦上安裝該可轉散發套件，或在更新代理程式前加以安裝。安裝後，可能需要重新啟動。您可以在 Microsoft 網址上找到 Microsoft Visual C++ 可轉散發套件：https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows。

若要使用 Cyber Protect 主控台更新代理程式

1. 請按一下 **[設定]** > **[代理程式]**。
   軟體會顯示電腦清單。有過期代理程式版本的電腦，會標示橙色驚嘆號。
2. 選擇您要更新代理程式的電腦。電腦必須在線上。
3. 請按一下 **[更新代理程式]**。

注意事項
在更新期間，進行中的所有備份都將失敗。

若要更新其版本低於 12.5.23094 的 VMware 用代理程式 (虛擬裝置)

1. 按一下 **[設定]** > **[代理程式]** > 您要更新的代理程式 > **[詳細資料]**，然後檢查 **[已指派的虛擬機器]** 區段。更新後，您將需要重新輸入這些設定。
   a. 記下 **[自動指派]** 開關的位置。
   b. 若要尋找手動指派給代理程式的虛擬機器，請按一下 **[已指派:]** 連結。軟體會顯示已指派之虛擬機器的清單。請記下 **[代理程式]** 欄中的代理程式名稱後面有 (M) 的電腦。
2. 移除 VMware 用代理程式 (虛擬裝置)，如「解除安裝代理程式」中所述。在步驟 5 中，即使您打算再次安裝代理程式，還是要從 **[設定]** > **[代理程式]** 中刪除該代理程式。
3. 部署 VMware 用代理程式 (虛擬裝置)，如「部署 OVF 範本」中所述。
4. 設定 VMware 用代理程式 (虛擬裝置)，如「設定虛擬裝置」中所述。
   如果您要重新架構本機連接的存放區，請在步驟 7 中執行下列操作：
   a. 將含有本機存放區的磁碟新增至虛擬裝置。
   b. 按一下 **[重新整理]** > **[建立存放區]** > **[掛載]**。
   c. 此軟體會顯示磁碟的原始**代號**和**標籤**。請不要變更它們。
   d. 按一下 **[確定]**。
5. 按一下 **[設定]** > **[代理程式]** > 您要更新的代理程式 > **[詳細資料]**，然後重新建構您在步驟 1 中記下的設定。如果部分虛擬機器已手動指派給代理程式，請再次指派它們，如「虛擬機器繫結」中

所述。

一旦完成代理程式設定之後，套用至舊代理程式的保護計劃就會自動重新套用至新代理程式。

6. 啟用應用程式感知備份的計劃需要重新輸入客體作業系統認證。編輯這些計劃，然後重新輸入認證。
7. 備份 ESXi 設定的計劃需要重新輸入 "root" 密碼。編輯這些計劃，然後重新輸入密碼。

在電腦上更新網路保護定義

1. 請按一下**[設定]** > **[代理程式]**。
2. 選擇您要更新網路保護定義所在的電腦，然後按一下 **[更新定義]**。電腦必須在線上。

將 [更新者] 角色指派給代理程式

1. 請按一下**[設定]** > **[代理程式]**。
2. 選擇要指派 [更新者角色] 的電腦，按一下 **[詳細資料]**，然後在 **[資安防護定義]** 區段中，啟用 **[使用此代理程式下載並散佈修補程式和更新]**。

注意事項
具有更新者角色的代理程式僅能為 Windows 協力廠商產品下載並散佈修補程式。對於 Microsoft 產品，更新者代理程式不支援散佈修補程式。

清除代理程式上的快取資料

1. 請按一下**[設定]** > **[代理程式]**。
2. 選擇您要清除快取資料 (過期的更新檔案和修補程式管理資料) 所在的電腦，然後按一下 **[清除快取]**。

自動更新保護代理程式

若要簡化多個工作負載的管理，您可以設定自動更新 Windows 用代理程式、Linux 用代理程式和 Mac 用代理程式。自動更新適用於代理程式 15.0.26986 (2021 年 5 月發行) 版或之後版本。舊版代理程式則必須先手動更新至最新版本。

在執行下列任何作業系統的電腦上支援自動更新：

- Windows XP SP 3 和更新版本
- Red Hat Enterprise Linux 6 和更新版本、CentOS 6 和更新版本
- OS X 10.9 Mavericks 和更新版本

自動更新的設定是在資料中心層級預先設定的。公司系統管理員可以針對公司或單位中的所有電腦，或針對個別電腦，自訂這些設定。如果未套用任何自訂設定，則會以下列順序，使用更上層的設定：

1. Cyber Protection 資料中心
2. 公司 (客戶租用戶)
3. 單位
4. 電腦

例如，單位系統管理員可以針對單位中的所有電腦，設定自訂自動更新設定，這可能與套用到公司層級上電腦的設定不同。系統管理員也可以針對單位中，既未套用單位設定也未套用公司設定的一或多部電腦，進行不同的設定。

啟用自動更新之後，您可以設定下列選項：

- **更新通道**

  在 **[更新通道]** 區段中，您可以選擇要使用哪個版本的保護代理程式：
  - **最新**：一律安裝最新版本的保護代理程式。
  - **上一個穩定版本**：從先前版本安裝最新的穩定版保護代理程式。
- **維護時段**

  維護時段可定義安裝更新的時間。如果已停用維護時段，則可以隨時執行更新。

  即使是在已啟用的維護時段內，當代理程式正在執行下列任何作業時，也不會安裝更新：
  - 備份
  - 復原
  - 備份複寫
  - 虛擬機器複寫
  - 測試複本
  - 從備份執行虛擬機器 (包括最終化)
  - 災難復原容錯移轉
  - 災難復原容錯回復
  - 執行指令碼 (針對網路指令碼撰寫功能)
  - 修補程式安裝
  - ESXi 設定備份

若要自訂自動更新設定

1. 在 Cyber Protect 主控台中，移至 **[設定]** > **[代理程式]**。
2. 選擇設定的範圍：
   - 若要變更所有電腦的設定，請按一下 **[編輯預設的代理程式更新設定]**。
   - 若要變更特定電腦的設定，選擇所需的電腦，然後按一下 **[代理程式更新設定]**。
3. 根據您的需求進行設定，然後按一下 **[套用]**。

若要移除自訂自動更新設定

1. 在 Cyber Protect 主控台中，移至 **[設定]** > **[代理程式]**。
2. 選擇設定的範圍：
   - 若要移除所有電腦的自訂設定，請按一下 **[編輯預設的代理程式更新設定]**。
   - 若要移除特定電腦的自訂設定，選擇所需的電腦，然後按一下 **[代理程式更新設定]**。
3. 按一下 **[重設為預設設定]**，然後按一下 **[套用]**。

若要檢查自動更新狀態

1. 在 Cyber Protect 主控台中，移至 **[設定]** > **[代理程式]**。
2. 按一下表格右上角的齒輪圖示，然後確認已選擇 **[自動更新]** 核取方塊。

3. 檢查 **[自動更新]** 欄中顯示的狀態。

在 BitLocker 加密工作負載上更新保護代理程式

引入對 Startup Recovery Manager 的變更的代理程式更新會干擾在同時啟用 BitLocker 和 Startup Recovery Manager 的工作負載上的 BitLocker。在此情況下，重新啟動後需要 BitLocker 復原金鑰。若要緩解此問題，請在更新代理程式前先暫停或停用 BitLocker。

受影響的代理程式版本：

- 23.12.36943，2023 年 12 月發行

您也可以在保護代理程式的版本資訊中，檢查更新是否引入了對 Startup Recovery Manager 的變更。

若要在已啟用 BitLocker 和 Startup Recovery Manager 的工作負載上更新代理程式

1. 在您要更新其代理程式的工作負載上，暫停或停用 BitLocker。
2. 更新代理程式。
3. 請重新啟動工作負載。
4. 啟用 BitLocker。

透過群組原則部署保護代理程式

您可以使用 Windows 群組原則，將 Windows 用代理程式集中安裝 (或部署) 到屬於 Active Directory 網域成員的電腦。

在此節中，您將會瞭解如何設定群組原則物件，以將代理程式部署至整個網域或其組織單位中的電腦上。

每當電腦登入網域時，所產生的群組原則物件皆能確保代理程式確實安裝及登錄。

必要條件

- 其網域控制站執行 Microsoft Windows Server 2003 或更新版本的 Active Directory 網域。
- 您必須是此網域中 **[Domain Admins]** 群組的成員。
- 您已下載**所有 Windows 用代理程式**安裝程式。
  若要下載安裝程式，請在 Cyber Protect 主控台中，按一下右上角的帳戶圖示，然後按一下 **[下載]**。您也可以在 **[新增裝置]** 窗格中取得下載連結。

若要透過群組原則部署代理程式

1. 產生註冊權杖，如 "產生註冊權杖" (第 108 頁) 中所述。
2. 建立 .mst 檔案、.msi 檔案和 .cab 檔案，如 "建立轉換檔案並解壓縮安裝套件" (第 121 頁) 中所述。
3. 設定群組原則物件，如 "設定群組原則物件" (第 121 頁) 中所述。

建立轉換檔案並解壓縮安裝套件

若要透過 Windows 群組原則部署保護代理程式，您需要有轉換檔案 (.mst) 和安裝套件 (.msi 和 .cab 檔案)。

注意事項
以下程序使用預設的註冊選項，亦即，使用權杖註冊。若要瞭解如何產生註冊權杖，請參閱 "產生註冊權杖" (第 108 頁)。

若要建立 .mst 檔案並解壓縮安裝套件 (.msi 和 .cab 檔案)

1. 在 Active Directory 網域中的任何電腦上，以系統管理員身分登入。
2. 建立一個將容納安裝套件的共用資料夾。透過諸如為 **[每人]** 保留預設共用設定等方式，確保網域使用者可存取共用資料夾。
3. 執行代理程式安裝程式。
4. 按一下 **[為自動安裝建立 .mst 和 .msi 檔案]**。
5. 在 **[要安裝的項目]** 中，選擇您要包含在安裝中的元件，然後按一下 **[完成]**。
6. 在 **[註冊設定]** 中，按一下 **[指定]**，輸入註冊權杖，然後按一下 **[完成]**。
   您可以將註冊方法從 **[使用註冊權杖]** (預設) 變更為 **[使用認證]** 或 **[略過註冊]**。**[略過註冊]** 選項是假設您之後將會手動註冊工作負載。
7. 檢閱或修改將新增到 .mst 檔案中的安裝設定，然後按一下 **[繼續]**。
8. 在 **[將檔案儲存至]** 中，指定您建立的共用資料夾的路徑。
9. 按一下 **[產生]**。

因此，將建立 .mst 檔案、.msi 檔案和 .cab 檔案，並將其複製到您指定的共用資料夾中。

接下來，設定 Windows 群組原則物件。若要了解如何操作，請參閱 "設定群組原則物件" (第 121 頁)。

設定群組原則物件

在此程序中，您要使用您在 "建立轉換檔案並解壓縮安裝套件" (第 121 頁) 中建立的安裝套件來設定群組原則物件 (GPO)。GPO 會將代理程式部署到您網域中的電腦上。

若要設定群組原則物件

1. 以網域系統管理員的身分，登入網域控制站。
   如果網域中有多個網域控制站，請以網域系統管理員身分，登入到任一個網域控制站。
2. [如果您要在組織單位中部署代理程式] 請確保您要在其中部署代理程式的組織單位存在於此網域中。
3. 在 Windows 的 **[開始]** 功能表中，指向 **[系統管理工具]**，然後按一下 **[群組原則管理]** (或 **[Active Directory 使用者和電腦]** (在 Windows Server 2003 中))。
4. [對於 Windows Server 2008 或更新版本] 以滑鼠右鍵按一下網域或組織單位的名稱，然後按一下 **[在此網域中建立 GPO，並將其連結至此]**。

5. [對於 Windows Server 2003] 以滑鼠右鍵按一下網域或組織單位的名稱，然後按一下 **[屬性]**。在對話方塊中按一下 **[群組原則]** 索引標籤，然後按一下 **[新增]**。
6. 將新的群組原則物件命名為 **[Windows 用代理程式]**。
7. 開啟 **[Windows 用代理程式]** 群組原則物件進行編輯：
   - [在 Windows Server 2008 或更新版本中] 在 **[群組原則物件]** 下，以滑鼠右鍵按一下該群組原則物件，然後按一下 **[編輯]**。
   - [在 Windows Server 2003 中] 按一下群組原則物件，然後按一下 **[編輯]**。
8. 在群組原則物件編輯器嵌入式管理單元中，展開 **[電腦設定]**。
9. [對於 Windows Server 2012 或更新版本] 展開 **[原則]** > **[軟體設定]**。
10. [對於 Windows Server 2003 和 Windows Server 2008] 展開 **[軟體設定]**。
11. 以滑鼠右鍵按一下 **[軟體安裝]**，指向 **[新增]**，然後按一下 **[套件]**。
12. 在共用資料夾中，選擇您所建立的之代理程式的 .msi 安裝套件，然後按一下 **[開啟]**。
13. 在 **[部署軟體]** 對話方塊中，按一下 **[進階]**，然後按一下 **[確定]**。
14. 在 **[修改]** 索引標籤上，按一下 **[新增]**，然後在共用資料夾中，選擇您所建立的 .mst 檔案。
15. 按一下 **[確定]** 關閉 **[部署軟體]** 對話方塊。

部署虛擬裝置

部署 VMware 用代理程式 (虛擬裝置)

在您開始之前

代理程式的系統需求

根據預設，虛擬裝置獲指派 4 GB 的 RAM 和 2 個 vCPU，非常適合而且足以適用於大多數作業。

若要提升備份效能並避免與 RAM 記憶體不足相關的失敗，建議您在較嚴苛的情況下，將這些資源增加到 16 GB 的 RAM 和 4 個 vCPU。例如，當您預期備份流量每秒超過 100 MB (例如，使用 10 GB 網路) 時，或者如果您同時備份具有大型硬碟 (500 GB 以上) 的多部虛擬機器，請增加指派的資源。

裝置自己的虛擬磁碟不會佔用超過 6 GB 空間。磁碟格式的厚薄都不會影響裝置效能。

我需要多少個代理程式?

即使一個虛擬裝置可以保護整個 vSphere 環境，最佳作法還是每個 vSphere 叢集 (如果沒有叢集，則每個主機) 部署一個虛擬機器。這可以讓備份更快速，因為該裝置可以透過使用 HotAdd 傳輸來連接備份磁碟，因此，備份流量是由一個本端磁碟導向至另一個本端磁碟。

同時使用虛擬裝置和 VMware 用代理程式 (Windows) 很正常，但前提是，這兩者都要連線到相同的 vCenter Server *或者*連線到不同的 ESXi 主機。請避免將一個代理程式直接連線到 ESXi，另一個代理程式則連線到管理此 ESXi 的 vCenter Server。

如果您有多個代理程式，則不建議使用本機連接的儲存空間 (亦即，在新增至虛擬裝置的虛擬磁碟上儲存備份)。有關其他考量，請參閱 "使用本機附加的存放區" (第 618 頁)。

停用代理程式的自動 DRS

如果虛擬裝置部署至 vSphere 叢集，請務必為其停用自動 vMotion。在叢集 DRS 設定中，啟用個別虛擬機器自動化層級，然後將虛擬裝置的 **[自動化層級]** 設定為 **[已停用]**。

部署 OVF 範本

1. 按一下 **[所有裝置]** > **[新增]** > **[VMware ESXi]** > **[虛擬裝置 (OVF)]**。
   .zip 封存將會下載到您的電腦中。
2. 解壓縮 .zip 封存。資料夾包含一個 .ovf 檔案和兩個 .vmdk 檔案。
3. 請確保這些檔案可從執行 vSphere Client 的電腦存取。
4. 啟動 vSphere Client 並登入 vCenter Server。
5. 部署 OVF 範本。
   - 設定儲存空間時，請選擇共用資料存放區 (如果存在的話)。磁碟格式的厚薄都不會影響裝置效能。
   - 設定網路連線時，請務必選取允許網際網路連線的網路，讓代理程式可以在雲端正確地註冊本身。

設定虛擬裝置

部署虛擬裝置之後，您必須進行設定，使其可以存取 vCenter Server 或 ESXi 主機以及 Cyber Protection 服務。

若要設定虛擬設備

1. 在 vSphere Client 中，開啟虛擬裝置的主控台。
2. 請確認已設定網路連線。
   連線是透過動態主機設定協定 (DHCP) 自動設定的。
   若要變更該預設組態，在 **[代理程式選項]** 下的 **[eth0]** 中，按一下 **[變更]**，然後指定網路設定。
3. 將虛擬裝置連線至 vCenter Server 或 ESXi 主機。
   a. 在 **[代理程式選項]** 下的 **[vCenter/ESX(i)]** 欄位中，按一下 **[變更]**，然後指定下列項目。
      - [如果您使用 vCenter Server] vCenter Server 名稱或 IP 位址。
      - [如果您未使用 vCenter Server] 您要備份與復原虛擬機器所在 ESXi 主機的名稱或 IP 位址。若要加快備份速度，請在相同的主機上部署虛擬裝置。
      - 連線至 vCenter Server 或 ESXi 主機之裝置所需的認證。
        建議您使用專用帳戶來存取 vCenter Server 或 ESXi 主機，而不是使用具有 [系統管理員] 角色的現有帳戶。如需詳細資訊，請參閱 "VMware 用代理程式所需的權限" (第 623 頁)。
   b. 按一下 **[檢查連線]** 以確保設定正確。
   c. 按一下 **[確定]**。
4. 使用以下其中一種方法，在 Cyber Protection 服務中註冊裝置。
   - [僅適用於不含雙重驗證機制的租用戶] 在其圖形化介面中註冊裝置。
     a. 在 **[代理程式選項]** 的 **[管理伺服器]** 欄位中，按一下 **[變更]**。
     b. 在 **[伺服器名稱/IP]** 欄位中，選擇 **[雲端]**。

Cyber Protection 服務位址隨即出現。除非特別指示，否則請不要變更此位址。

c. 在 **[使用者名稱]** 和 **[密碼]** 欄位中，指定您的帳戶在 Cyber Protection 服務中的認證。裝置所管理的虛擬裝置和虛擬機器會使用此帳戶註冊。

d. 按一下 **[確定]**。

- 在命令列介面中註冊裝置。

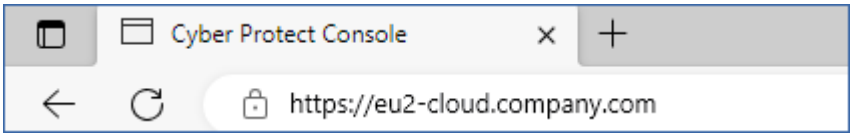
注意事項
使用此方法時，您需要註冊權杖。如需有關如何產生註冊權杖的詳細資訊，請參閱 "產生註冊權杖" (第 108 頁)。

a. 按下 CTRL+SHIFT+F2 以開啟命令列介面。

b. 執行下列命令：

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

注意事項
當您使用註冊權杖時，必須指定確實的資料中心位址。這是是您在**登入** Cyber Protect 主控台之後看到的 URL。例如，`https://eu2-cloud.company.com`。



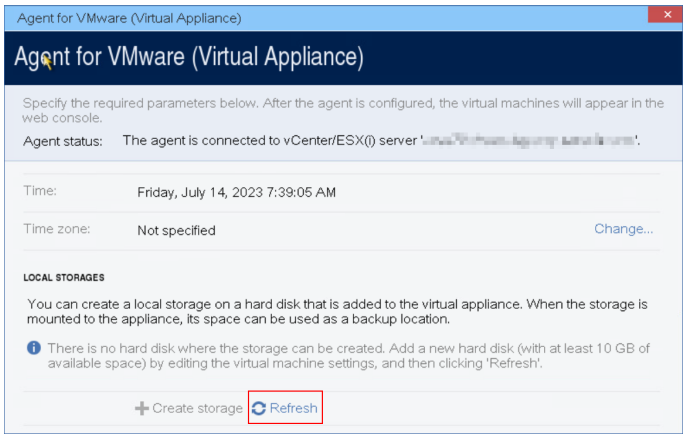
請不要在這裡使用 `https://cloud.company.com`。

c. 若要返回裝置的圖形化介面，按下 ALT+F1。

5. [選用] 新增本機儲存空間。

a. 在 vSphere Client 中，將虛擬磁碟附加到虛擬裝置。虛擬磁碟必須至少有 10 GB 的可用空間。

b. 在裝置的圖形化使用者介面中，按一下 **[重新整理]**。



[建立存放區] 按鈕變成作用中。

c. 按一下 **[建立存放區]**。

d. 指定媒體的標籤，然後按一下 **[確定]**。

e. 按一下 **[是]**，確認您的選擇。

6. [如果您的網路中已啟用 Proxy 伺服器] 設定 Proxy 伺服器。

   a. 按下 CTRL+SHIFT+F2 以開啟命令列介面。

   b. 使用文字編輯器開啟檔案 **/etc/Acronis/Global.config**。

   c. 執行下列其中一項操作：

      - 如果在代理程式安裝期間指定 Proxy 設定，請找出下列區段：

        ```
        <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>
        ```

      - 否則，複製以上幾行，並將其貼入檔案的 `<registry name="Global">...</registry>` 標籤之間。

   d. 將 `ADDRESS` 取代為新的 Proxy 伺服器主機名稱/IP 位址，並將 `PORT` 取代為連接埠號碼的十六進位值。

   e. 如果您的 Proxy 伺服器需要驗證，請將 `LOGIN` 和 `PASSWORD` 取代為 Proxy 伺服器認證。否則，請從檔案中刪除這幾行。

   f. 儲存檔案。

   g. 在文字編輯器中開啟檔案 **/opt/acronis/etc/aakore.yaml**。

   h. 找出 **env** 區段，或建立該區段並加入下列幾行：

      ```
      env:
          http-proxy: proxy_login:proxy_password@proxy_address:port
          https-proxy: proxy_login:proxy_password@proxy_address:port
      ```

   i. 將 `proxy_login` 和 `proxy_password` 取代為 Proxy 伺服器認證，並將 `proxy_address:port` 取代為 Proxy 伺服器的位址和連接埠號碼。

   j. 執行 `reboot` 命令。

注意事項

為能夠更新在 Proxy 後部署的虛擬裝置，請編輯裝置的 `config.yaml` 檔案 (`/opt/acronis/etc/va-updater/config.yaml`)，方法是，將以下一行新增到該檔案的底部，然後輸入專用於您環境的值：

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

例如：

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

正在部署 Scale Computing HC3 用代理程式 (虛擬裝置)

在您開始之前

此裝置是您在 Scale Computing HC3 叢集中部署的預先設定虛擬機器。其中隨附的保護代理程式可讓您針對叢集中的所有虛擬機器，管理網路保護。

代理程式的系統需求

根據預設，已安裝代理程式的虛擬機器使用 2 個 vCPU 和 4 GiB 的 RAM。這些設定對於大多數的作業已經足夠，但是您可以在 Scale Computing HC3 Web 介面中編輯虛擬機器來加以變更。

若要提升備份效能並避免與 RAM 記憶體不足相關的失敗，建議您在較嚴苛的情況下，將這些資源增加到 4 個 vCPU 和 8 GiB 的 RAM。例如，當您預期備份流量每秒超過 100 MB (例如，使用 10 GB 網路) 時，或者如果您同時備份具有大型硬碟 (500 GB 以上) 的多部虛擬機器，請增加指派的資源。

裝置虛擬磁碟的大小為 9 GB。

我需要多少個代理程式?

一個代理程式可以保護整個叢集。不過，如果您需要分配備份流量頻寬負載，則叢集中可以有多個代理程式。

如果您在叢集中有多個代理程式，則會在代理程式之間自動平均分配虛擬機器，讓每個代理程式管理相似數量的機器。

當代理程式間負載不平衡的情況達到 20% 的程度時，就會進行自動重新分配。新增或移除機器或代理程式時，可能會發生這種情況。例如，您發現需要更多代理程式來增進處理能力，而且您要將額外的虛擬裝置部署到叢集。管理伺服器會指派最適合的虛擬機器給新的代理程式。舊代理程式的負載將會減少。當您從管理伺服器移除代理程式時，指派給代理程式的機器會在剩餘的代理程式之間重新分配。但是，如果代理程式損毀，或未手動從 Scale Computing HC3 叢集刪除代理程式，就不會發生這種情況。只有在您從 Cyber Protect 主控台移除這種代理程式後，才會開始重新分配。

檢查哪個代理程式管理特定的機器

1. 在 Cyber Protect 主控台中，按一下 **[裝置]**，然後選擇 **[Scale Computing]**。
2. 按一下表格右上角的齒輪圖示，然後在 **[系統]** 底下，選擇 **[代理程式]** 核取方塊。
3. 在出現的欄中，檢查代理程式的名稱。

部署 QCOW2 範本

1. 請登入您的 Cyber Protection 帳戶。
2. 按一下 **[裝置]** > **[所有裝置]** > **[新增]** > **[Scale Computing HC3]**。
   .zip 封存將會下載到您的電腦中。
3. 解壓縮 .zip 存檔，然後將 .qcow2 檔案和 .xml 檔案儲存到名為 **ScaleAppliance** 的資料夾中。
4. 將 **ScaleAppliance** 資料夾上傳到網路共用，並確認 Scale Computing HC3 叢集可以存取該資料夾。

5. 以獲指派 **[VM 建立/編輯]** 角色的系統管理員身分，登入 Scale Computing HC3 叢集。如需有關操作 Scale Computing HC3 虛擬機器所需角色的詳細資訊，請參閱 "Scale Computing HC3 用代理程式 – 必要角色" (第 129 頁)。
6. 在 Scale Computing HC3 Web 介面中，從 **ScaleAppliance** 資料夾匯入虛擬機器範本。
   a. 按一下 **[匯入 HC3 VM]** 圖示。
   b. 在 **[匯入 HC3 VM]** 視窗中，指定下列內容：
      - 新虛擬機器的名稱。
      - **ScaleAppliance** 資料夾所在的網路共用。
      - 存取此網路共用所需的使用者名稱和密碼。
      - [選用] 新虛擬機器的網域標籤。
      - 網路共用上的 **ScaleAppliance** 資料夾路徑。
   c. 按一下 **[匯入]**。

部署完成後，您必須設定虛擬裝置。如需有關設定方式的詳細資訊，請參閱 "設定虛擬裝置" (第 127 頁)。

注意事項
如果您的叢集中需要多個虛擬裝置，請重複上述步驟，並部署其他虛擬裝置。請不要使用 Scale Computing HC3 Web 介面中的 **[複製 VM]** 選項來複製現有的虛擬裝置。

設定虛擬裝置

部署虛擬裝置之後，您需要進行設定，使其可以連線至將保護的 Scale Computing HC3 叢集以及 Cyber Protection 服務。

若要設定虛擬設備

1. 登入您的 Scale Computing HC3 帳戶。
2. 選擇您要設定的虛擬裝置，然後按一下 **[主控台]** 圖示。
3. 在 **[eth0]** 欄位中，設定裝置的網路介面。
   請確認自動指派的 DHCP 位址 (如果有的話) 在您虛擬機器所使用的網路內有效，或手動指派這些位址。可能有一或多個介面需要設定，端視裝置所使用的網路數量而定。
4. 在 **[Scale Computing]** 欄位中，按一下 **[變更]** 以指定 Scale Computing HC3 叢集位址以及存取該位址所使用的認證。
   a. 在 **[伺服器名稱/IP]** 欄位中，輸入叢集的 DNS名稱或 IP 位址。
   b. 在 **[使用者名稱]** 和 **[密碼]** 欄位中，輸入 Scale Computing HC3 系統管理員帳戶的認證。
      請確保此帳戶具備操作 Scale Computing HC3 虛擬機器所需的角色。如需有關這些角色的詳細資訊，請參閱 "Scale Computing HC3 用代理程式 – 必要角色" (第 129 頁)。
   c. 按一下 **[檢查連線]** 以確保設定正確。
   d. 按一下 **[確定]**。
5. 使用以下其中一種方法，在 Cyber Protection 服務中註冊裝置。

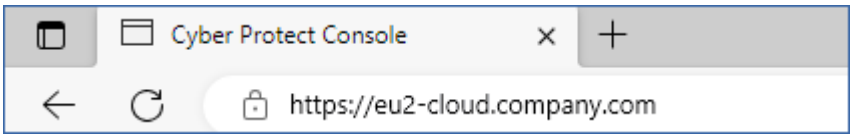
- [僅適用於不含雙重驗證機制的租用戶] 在其圖形化介面中註冊裝置。
  a. 在 **[代理程式選項]** 的 **[管理伺服器]** 欄位中，按一下 **[變更]**。
  b. 在 **[伺服器名稱/IP]** 欄位中，選擇 **[雲端]**。
     Cyber Protection 服務位址隨即出現。除非特別指示，否則請不要變更此位址。
  c. 在 **[使用者名稱]** 和 **[密碼]** 欄位中，指定您的帳戶在 Cyber Protection 服務中的認證。裝置所管理的虛擬裝置和虛擬機器會使用此帳戶註冊。
  d. 按一下 **[確定]**。
- 在命令列介面中註冊裝置。

  注意事項
  使用此方法時，您需要註冊權杖。如需有關如何產生註冊權杖的詳細資訊，請參閱 "產生註冊權杖" (第 108 頁)。

  a. 按下 CTRL+SHIFT+F2 以開啟命令列介面。
  b. 執行下列命令：

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

  注意事項
  當您使用註冊權杖時，必須指定確實的資料中心位址。這是是您在**登入** Cyber Protect 主控台之後看到的 URL。例如，`https://eu2-cloud.company.com`。

  請不要在這裡使用 `https://cloud.company.com`。

  c. 若要返回裝置的圖形化介面，按下 ALT+F1。
6. [選用] 在 **[名稱]** 欄位中，按一下 **[變更]** 以變更虛擬裝置的預設名稱，亦即 **localhost**。此名稱會顯示在 Cyber Protect 主控台中。
7. [選用] 在 **[時間]** 欄位中，按一下 **[變更]**，然後選擇您所在位置的時區，以確保排程作業在適當時間執行。
8. [如果您的網路中已啟用 Proxy 伺服器] 設定 Proxy 伺服器。
   a. 按下 CTRL+SHIFT+F2 以開啟命令列介面。
   b. 使用文字編輯器開啟檔案 **/etc/Acronis/Global.config**。
   c. 執行下列其中一項操作：
      - 如果在代理程式安裝期間指定 Proxy 設定，請找出下列區段：

      ```
      <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>
```

- 否則，複製以上幾行，並將其貼入檔案的 `<registry name="Global">...</registry>` 標籤之間。

d. 將 `ADDRESS` 取代為新的 Proxy 伺服器主機名稱/IP 位址，並將 `PORT` 取代為連接埠號碼的十六進位值。

e. 如果您的 Proxy 伺服器需要驗證，請將 `LOGIN` 和 `PASSWORD` 取代為 Proxy 伺服器認證。否則，請從檔案中刪除這幾行。

f. 儲存檔案。

g. 在文字編輯器中開啟檔案 **/opt/acronis/etc/aakore.yaml**。

h. 找出 **env** 區段，或建立該區段並加入下列幾行：

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

i. 將 `proxy_login` 和 `proxy_password` 取代為 Proxy 伺服器認證，並將 `proxy_address:port` 取代為 Proxy 伺服器的位址和連接埠號碼。

j. 執行 `reboot` 命令。

注意事項

為能夠更新在 Proxy 後部署的虛擬裝置，請編輯裝置的 `config.yaml` 檔案 (`/opt/acronis/etc/va-updater/config.yaml`)，方法是，將以下一行新增到該檔案的底部，然後輸入專用於您環境的值：

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

例如：

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

保護 Scale Computing HC3 叢集中的虛擬機器

1. 請登入您的 Cyber Protection 帳戶。
2. 瀏覽至 **[裝置]** > **[Scale Computing HC3]** > <您的叢集> >，或在 **[裝置]** > **[所有裝置]** 中尋找您的電腦。
3. 選擇電腦，並為其套用保護計劃。

Scale Computing HC3 用代理程式 – 必要角色

本節說明 Scale Computing HC3 虛擬機器操作所需的角色。

作業	角色
備份虛擬機器	備份

	VM 建立/編輯 VM 刪除
復原至現有的虛擬機器	備份 VM 建立/編輯 VM 電源控制 VM 刪除 叢集設定
復原至新的虛擬機器	備份 VM 建立/編輯 VM 電源控制 VM 刪除 叢集設定

部署 Virtuozzo Hybrid Infrastructure 用代理程式 (虛擬裝置)

在您開始之前

此裝置是您在 Virtuozzo Hybrid Infrastructure 中部署的預先設定虛擬機器。其中隨附的保護代理程式可讓您針對 Virtuozzo Hybrid Infrastructure 叢集中的所有虛擬機器，管理網路保護。

注意事項

為確保已啟用 **[虛擬機器的磁碟區陰影複製服務 VSS]** 備份選項的備份正常運作，並在應用程式一致的狀態下擷取資料，請確認是否已在受保護的虛擬機器上安裝 Virtuozzo Guest Tools，而且處於最新狀態。

代理程式的系統需求

部署虛擬裝置時，您可以在預先定義的不同 vCPU 和 RAM (類別) 組合中選擇。您也可以建立自己的類別。

2 個 vCPU 搭配 4 GB 的 RAM (中等類別) 非常適合而且足以適用於大多數作業。若要提升備份效能並避免與 RAM 記憶體不足相關的失敗，建議您在較嚴苛的情況下，將這些資源增加到 4 個 vCPU 和 8 GB 的 RAM。例如，當您預期備份流量每秒超過 100 MB (例如，使用 10 GB 網路) 時，或者如果您同時備份具有大型硬碟 (500 GB 以上) 的多部虛擬機器，請增加指派的資源。

我需要多少個代理程式?

一個代理程式可以保護整個叢集。不過，如果您需要分配備份流量頻寬負載，則叢集中可以有多個代理程式。

如果您在叢集中有多個代理程式，則會在代理程式之間自動平均分配虛擬機器，讓每個代理程式管理相似數量的機器。

當代理程式間負載不平衡的情況達到 20% 的程度時，就會進行自動重新分配。新增或移除機器或代理程式時，可能會發生這種情況。例如，您發現需要更多代理程式來增進處理能力，而且您要將額外的虛擬裝置部署到叢集。管理伺服器會指派最適合的虛擬機器給新的代理程式。舊代理程式的負載將會減少。當您從管理伺服器移除代理程式時，指派給代理程式的機器會在剩餘的代理程式之間重新分配。但是，如果代理程式損毀，或未手動從 Virtuozzo Hybrid Infrastructure 節點刪除代理程式，就不會發生這種情況。只有在當您從 Cyber Protection Web 介面移除這種代理程式後，才會開始重新分配。

檢查哪個代理程式管理特定的機器

1. 在 Cyber Protect 主控台中，按一下 **[裝置]**，然後選擇 **[Virtuozzo Hybrid Infrastructure]**。
2. 按一下表格右上角的齒輪圖示，然後在 **[系統]** 底下，選擇 **[代理程式]** 核取方塊。
3. 在出現的欄中，檢查代理程式的名稱。

限制

- 您無法從遠端部署 Virtuozzo Hybrid Infrastructure 裝置。
- 不支援虛擬機器的應用程式感知備份。

在 Virtuozzo Hybrid Infrastructure 中設定網路

部署和設定虛擬裝置之前，您必須在 Virtuozzo Hybrid Infrastructure 中設定網路。

Virtuozzo Hybrid Infrastructure 用代理程式 (虛擬裝置) 的網路需求

- 虛擬裝置需要 2 張網路介面卡。
- 虛擬裝置必須連線到具有下列網路流量類型的 Virtuozzo 網路：
  - 計算 API
  - VM 備份
  - ABGW 公用
  - VM 公用

如需有關設定網路的詳細資訊，請參閱 Virtuozzo 文件中的計算叢集需求。

在 Virtuozzo Hybrid Infrastructure 中設定使用者帳戶

若要設定虛擬裝置，您需要有 Virtuozzo Hybrid Infrastructure 使用者帳戶。此帳戶必須在**預設**網域中具備 **[系統管理員]** 角色。如需有關使用者的詳細資訊，請參閱 Virtuozzo Hybrid Infrastructure 文件中的管理管理員面板使用者。請確認您已經授予此帳戶存取**預設**網域中所有專案的權限。

若要授予存取預設網域中所有專案的權限

1. 為系統系統管理員建立一個環境檔案。方法是，在 Virtuozzo Hybrid Infrastructure 叢集中，透過 OpenStack 命令列介面，執行下列指令碼。如需有關如何連線至此介面的詳細資訊，請參閱 Virtuozzo Hybrid Infrastructure 文件中的連線至 OpenStack 命令列介面。

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

2. 使用環境檔案授權其他 OpenStack 命令：

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

3. 執行以下命令：

```
openstack --insecure user set --project admin --project-domain Default --domain
Default <username>
openstack --insecure role add --domain Default --user <username> --user-domain
Default compute --inherited
```

在這裡，<username> 是 Virtuozzo Hybrid Infrastructure 帳戶，且在**預設**網域中具備 **[系統管理員]** 角色。虛擬裝置將會使用此帳戶，備份和還原**預設**網域底下的任何子專案中的虛擬機器。

範例

```
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
```

若要在不同於**預設**網域的網域中管理虛擬機器的備份，請也執行下列命令。

若要授予存取不同網域中所有專案的權限

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

在這裡，<domain name> 是 <username> 帳戶將可存取之專案的網域。

範例

```
openstack --insecure role add --domain MyNewDomain --inherited --user johndoe --user-
domain Default admin
```

授予對專案的存取權之後，請檢查指派給帳戶的角色。

若要檢查已指派的角色

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

在這裡，<username> 是 Virtuozzo Hybrid Infrastructure 帳戶。

範例

```
openstack --insecure role assignment list --user johndoe --names -c Role -c User -c
Project -c Domain
+--------------+-----------------+---------+-------------+
| Role         | User            | Project | Domain      |
+--------------+-----------------+---------+-------------+
| admin        | johndoe@Default |         | MyNewDomain |
| compute      | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
+--------------+-----------------+---------+-------------+
```

在此範例中，[-c 角色]、[-c 使用者]、[-c 專案]和 [-c 網域]選項用於縮短命令輸出以符合頁面大小。

若要檢查指派給所有專案中帳戶的有效角色，請也執行下列命令。

若要檢查所有專案中的有效角色

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

在這裡，<username> 是 Virtuozzo Hybrid Infrastructure 帳戶。

範例

```
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 |
+--------------+-----------------+-----------------+---------+
```

在此範例中，[-c 角色]、[-c 使用者]、[-c 專案]和 [-c 網域]選項用於縮短命令輸出以符合頁面大小。

部署 QCOW2 範本

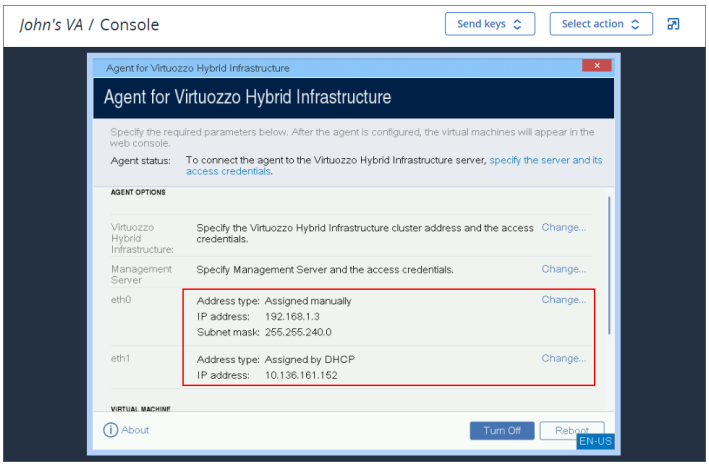
1. 請登入您的 Cyber Protection 帳戶。
2. 按一下 **[裝置]** > **[所有裝置]** > **[新增]** > **[Virtuozzo Hybrid Infrastructure]**。
   .zip 封存將會下載到您的電腦中。
3. 解壓縮 .zip 封存。其中包含一個 .qcow2 影像檔案。
4. 登入您的 Virtuozzo Hybrid Infrastructure 帳戶。
5. 將 .qcow2 影像檔案新增到 Virtuozzo Hybrid Infrastructure 計算叢集，如下所示：
   - 在 **[計算]** > **[虛擬機器]** > **[影像]** 索引標籤上，按一下 **[新增影像]**。
   - 在 **[新增影像]** 視窗中，按一下 **[瀏覽]**，然後選擇 .qcow2 檔案。
   - 指定影像名稱、選擇 **[一般 Linux 作業系統]** 類型，然後按一下 **[新增]**。
6. 在 **[計算]** > **[虛擬機器]** > **[虛擬機器]** 索引標籤中，按一下 **[建立虛擬機器]**。此時將會開啟一個視窗，您必須在其中指定下列參數：
   - 新虛擬機器的名稱。
   - 在 **[部署來源]** 中，選擇 **[影像]**。
   - 在 **[影像]** 視窗中，選擇裝置的 .qcow2 影像檔案，然後按一下 **[完成]**。
   - 在 **[磁碟區]** 視窗中，您不需要新增任何磁碟區。針對系統磁碟自動新增的磁碟區已經足夠。
   - 在 **[類別]** 視窗中，選擇所需的 vCPU 和 RAM 組合，然後按一下 **[完成]**。2 個 vCPU 搭配 4 GiB 的 RAM 通常已經足夠。
   - 在 **[網路介面]** 視窗中，按一下 **[新增]**、選擇 *[公用]* 類型的虛擬網路，然後按一下 **[新增]**。該虛擬網路將會出現在 **[網路介面]** 清單中。
     如果您使用包含多個實體網路 (包含多個公用類型的虛擬網路) 的設定，請重複此步驟，並選擇您需要的虛擬網路。
7. 按一下**[完成]**。
8. 返回 **[建立虛擬機器]** 視窗，按一下 **[部署]** 可建立並啟動虛擬機器。

設定虛擬裝置

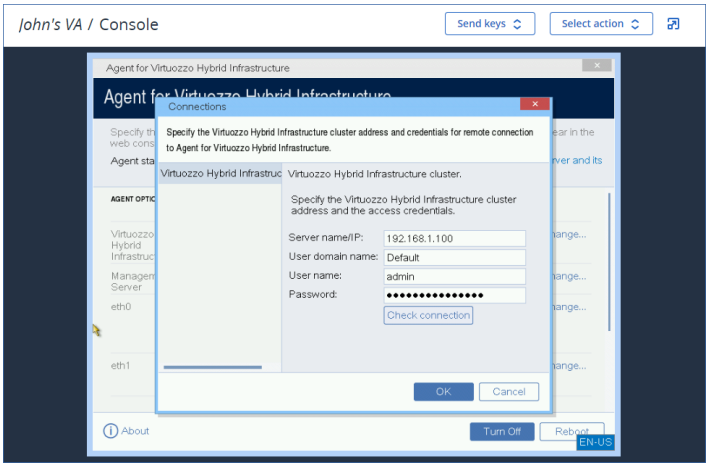
部署 Virtuozzo Hybrid Infrastructure 用代理程式 (虛擬裝置) 之後，您需要設定虛擬裝置，使其可以連線至將保護的 Virtuozzo Hybrid Infrastructure 叢集以及 Cyber Protection 雲端服務。

若要設定虛擬設備

1. 登入您的 Virtuozzo Hybrid Infrastructure 帳戶。
2. 在 **[計算]** > **[虛擬機器]** > **[虛擬機器]** 索引標籤上，選擇您所建立的虛擬機器。接著，按一下 **[主控台]**。
3. 設定裝置的網路介面。您可能有一或多個介面需要設定，端視裝置所使用的虛擬網路數量而定。請確認自動指派的 DHCP 位址 (如果有的話) 在您虛擬機器所使用的網路內有效，或手動指派這些位址。



4. 指定 Virtuozzo 叢集位址和認證：
   - Virtuozzo Hybrid Infrastructure 叢集的 DNS 名稱或 IP 位址 – 這是叢集的管理節點位址。系統將會自動設定預設連接埠 5000。您果您使用不同的連接埠，則必須手動指定。
   - 在 **[使用者網域名稱]** 欄位中，指定您在 Virtuozzo Hybrid Infrastructure 中的網域。例如，**預設**。
     網域名稱區分大小寫。
   - 在 **[使用者名稱]** 和 **[密碼]** 欄位中，輸入指定之網域中，擁有 **[系統管理員]** 角色之 Virtuozzo Hybrid Infrastructure 使用者帳戶的認證。如需有關使用者、角色和網域的詳細資訊，請參閱在 Virtuozzo Hybrid Infrastructure 中設定使用者帳戶。



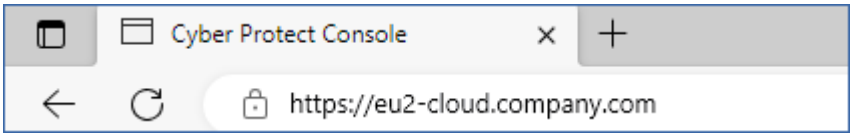
5. 使用以下其中一種方法，在 Cyber Protection 服務中註冊裝置。
   - [僅適用於不含雙重驗證機制的租用戶] 在其圖形化介面中註冊裝置。
     a. 在 **[代理程式選項]** 的 **[管理伺服器]** 欄位中，按一下 **[變更]**。
     b. 在 **[伺服器名稱/IP]** 欄位中，選擇 **[雲端]**。
        Cyber Protection 服務位址隨即出現。除非特別指示，否則請不要變更此位址。
     c. 在 **[使用者名稱]** 和 **[密碼]** 欄位中，指定您的帳戶在 Cyber Protection 服務中的認證。裝置所管理的虛擬裝置和虛擬機器會使用此帳戶註冊。
     d. 按一下 **[確定]**。
   - 在命令列介面中註冊裝置。

注意事項
使用此方法時，您需要註冊權杖。如需有關如何產生註冊權杖的詳細資訊，請參閱 "產生註冊權杖" (第 108 頁)。

a. 按下 CTRL+SHIFT+F2 以開啟命令列介面。
b. 執行下列命令：

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

注意事項
當您使用註冊權杖時，必須指定確實的資料中心位址。這是是您在**登入** Cyber Protect 主控台之後看到的 URL。例如，`https://eu2-cloud.company.com`。



請不要在這裡使用 `https://cloud.company.com`。

c. 若要返回裝置的圖形化介面，按下 ALT+F1。

6. [如果您的網路中已啟用 Proxy 伺服器] 設定 Proxy 伺服器。
   a. 按下 CTRL+SHIFT+F2 以開啟命令列介面。
   b. 使用文字編輯器開啟檔案 **/etc/Acronis/Global.config**。
   c. 執行下列其中一項操作：
      - 如果在代理程式安裝期間指定 Proxy 設定，請找出下列區段：

```
<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>
```

      - 否則，複製以上幾行，並將其貼入檔案的 `<registry name="Global">...</registry>` 標籤之間。
   d. 將 `ADDRESS` 取代為新的 Proxy 伺服器主機名稱/IP 位址，並將 `PORT` 取代為連接埠號碼的十六進位值。
   e. 如果您的 Proxy 伺服器需要驗證，請將 `LOGIN` 和 `PASSWORD` 取代為 Proxy 伺服器認證。否則，請從檔案中刪除這幾行。
   f. 儲存檔案。
   g. 在文字編輯器中開啟檔案 **/opt/acronis/etc/aakore.yaml**。
   h. 找出 **env** 區段，或建立該區段並加入下列幾行：

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

i. 將 `proxy_login` 和 `proxy_password` 取代為 Proxy 伺服器認證，並將 `proxy_address:port` 取代為 Proxy 伺服器的位址和連接埠號碼。

j. 執行 `reboot` 命令。

注意事項

為能夠更新在 Proxy 後部署的虛擬裝置，請編輯裝置的 `config.yaml` 檔案 (`/opt/acronis/etc/va-updater/config.yaml`)，方法是，將以下一行新增到該檔案的底部，然後輸入專用於您環境的值：

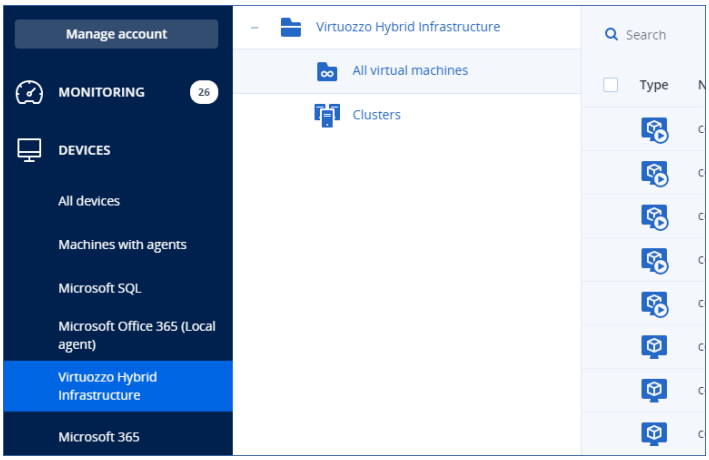
```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

例如：

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

若要保護 Virtuozzo Hybrid Infrastructure 叢集中的虛擬機器

1. 請登入您的 Cyber Protection 帳戶。
2. 瀏覽至 **[裝置]** > **[Virtuozzo Hybrid Infrastructure]** > <您的叢集> > **[預設保護]** > **[系統管理員]**，或在 **[裝置]** > **[所有裝置]** 中尋找您的電腦。
3. 選擇電腦，並為其套用保護計劃。



正在部署 oVirt 用代理程式 (虛擬裝置)

在您開始之前

此裝置是您在 Red Hat Virtualization/oVirt 資料中心部署的預先設定虛擬機器。此裝置隨附的保護代理程式可讓您針對資料中心中的所有虛擬機器，管理網路保護。

代理程式的系統需求

根據預設，已安裝代理程式的虛擬機器使用 2 個 vCPU 和 4 GiB 的 RAM。這些設定對於大多數的作業已經足夠，但是您可以在 Red Hat Virtualization/oVirt 系統管理入口網站中編輯這些設定。

若要提升備份效能並避免與 RAM 記憶體不足相關的失敗，建議您在較嚴苛的情況下，將這些資源增加到 4 個 vCPU 和 8 GiB 的 RAM。例如，當您預期備份流量每秒超過 100 MB (例如，使用 10 GB 網路) 時，或者如果您同時備份具有大型硬碟 (500 GB 以上) 的多部虛擬機器，請增加指派的資源。

裝置虛擬磁碟的大小為 8 GiB。

我需要多少個代理程式?

一個代理程式可以保護整個資料中心。不過，如果您需要分配備份流量頻寬負載，則資料中心中可以有多個代理程式。

如果您在資料中心中有多個代理程式，則會在代理程式之間自動分配虛擬機器，讓每個代理程式管理相似數量的機器。

當代理程式間負載不平衡的情況達到 20% 的程度時，就會進行自動重新分配。新增或移除機器或代理程式時，可能會發生這種情況。例如，您發現需要更多代理程式來增進處理能力，而且您要將額外的虛擬裝置部署到資料中心。管理伺服器會指派最適合的虛擬機器給新的代理程式。舊代理程式的負載將會減少。當您移除代理程式時，指派給代理程式的機器會在剩餘的代理程式之間重新分配。但是，如果代理程式損毀，或未手動從 Red Hat Virtualization/oVirt 系統管理入口網站刪除，就不會發生這種情況。只有在您從 Cyber Protect 主控台移除這種代理程式後，才會開始重新分配。

檢查哪個代理程式管理特定的機器

1. 在 Cyber Protect 主控台中，按一下 **[裝置]**，然後選擇 **[oVirt]**。
2. 按一下表格右上角的齒輪圖示，然後在 **[系統]** 底下，選擇 **[代理程式]** 核取方塊。
3. 在出現的欄中，檢查代理程式的名稱。

限制

Red Hat Virtualization/oVirt 虛擬機器不支援下列作業：

- 應用程式感知備份
- 正在從備份執行虛擬機器
- 虛擬機器的複寫
- Changed Block Tracking

部署 OVA 範本

1. 請登入您的 Cyber Protection 帳戶。
2. 按一下 **[裝置]** > **[所有裝置]** > **[新增]** > **[Red Hat Virtualization (oVirt)]**。
   .zip 封存將會下載到您的電腦中。
3. 解壓縮 .zip 封存。其中包含一個 .ova 檔案。
4. 將 .ova 檔案上傳到 Red Hat Virtualization/oVirt 資料中心中您要保護的主機。

5. 以系統管理員身分，登入 Red Hat Virtualization/oVirt 系統管理入口網站。如需有關操作虛擬機器所需角色的詳細資訊，請參閱 "oVirt 用代理程式 – 所需角色和連接埠" (第 142 頁)。
6. 從導覽功能表中，選擇 **[電腦]** > **[虛擬機器]**。
7. 按一下主要表格上方的垂直省略符號圖示  ，然後按一下 **[匯入]**。
8. 在 **[匯入虛擬機器]** 視窗中，執行下列作業：
   a. 在 **[資料中心]** 中，選擇您要保護的資料中心。
   b. 在 **[來源]** 中，選擇 **[虛擬裝置 (OVA)]**。
   c. 在 **[主機]** 中，選擇您要上傳 .ova 檔案所在的主機。
   d. 在 **[檔案路徑]** 中，指定包含 .ova 檔案的目錄的路徑。
   e. 按一下 **[載入]**。
      .ova 檔案中的 oVirt 虛擬裝置範本隨即出現在 **[來源上的虛擬機器]** 面板中。
      如果範本沒有出現在此面板中，請確認您已經指定該檔案的正確路徑、檔案未損毀，而且可以聯繫主機。
   f. 在 **[來源上的虛擬機器]** 中，選擇 oVirt 虛擬裝置範本，然後按一下向右箭頭。
      範本隨即出現在 **[要匯入的虛擬機器]** 面板中。
   g. 按 **[下一步]**。
9. 在新視窗中，按一下裝置名稱，然後設定下列設定：
   - 在 **[網路介面]** 索引標籤上，設定網路介面。
   - [選用] 在 **[一般]** 索引標籤上，變更裝有代理程式之虛擬機器的預設名稱。

部署現在已完成。接著，您必須設定虛擬裝置。如需有關設定方式的詳細資訊，請參閱 "設定虛擬裝置" (第 139 頁)。

注意事項
如果您的資料中心需要多個虛擬裝置，請重複上述步驟，並部署其他虛擬裝置。請不要使用 Red Hat Virtualization/oVirt 系統管理入口網站中的 **[複製 VM]** 選項來複製現有的虛擬裝置。

若要從動態群組備份排除虛擬裝置，您也必須從 Cyber Protect 主控台中的虛擬機器清單排除該虛擬裝置。若要排除該虛擬裝置，請在 Red Hat Virtualization/oVirt 系統管理入口網站中，選擇裝有代理程式的虛擬機器，然後為其指派 `acronis_virtual_appliance` 標籤。

設定虛擬裝置

部署虛擬裝置之後，您需要進行設定，使其可以連線至 oVirt 引擎以及 Cyber Protection 服務。

若要設定虛擬設備

1. 登入 Red Hat Virtualization/oVirt 系統管理入口網站。
2. 選擇您要設定的虛擬裝置，然後按一下 **[主控台]** 圖示。
3. 在 **[eth0]** 欄位中，設定裝置的網路介面。
   請確認自動指派的 DHCP 位址 (如果有的話) 在您虛擬機器所使用的網路內有效，或手動指派這些位址。可能有一或多個介面需要設定，端視裝置所使用的網路數量而定。
4. 在 **[oVirt]** 欄位中，按一下 **[變更]** 以指定 oVirt 引擎位址以及存取該位址所使用的認證：

a. 在 **[伺服器名稱/IP]** 欄位中，輸入引擎的 DNS名稱或 IP 位址。
b. 在 **[使用者名稱]** 和 **[密碼]** 欄位中，輸入此引擎的系統管理員認證。
   請確認此系統管理員帳戶具備操作 Red Hat Virtualization/oVirt 虛擬機器所需的角色。如需有關這些角色的詳細資訊，請參閱 "oVirt 用代理程式 – 所需角色和連接埠" (第 142 頁)。
   如果 Keycloak 是適用於 oVirt 引擎 (預設為 oVirt 4.5.1) 的單一登入 (SSO) 提供者，請在指定使用者名稱時，使用 Keycloak 格式。例如，將預設系統管理員帳戶指定為 `admin@ovirt@internalsso` 而非 `admin@internal`。
c. [選用] 按一下 **[檢查連線]** 以確保提供的認證正確無誤。
d. 按一下 **[確定]**。

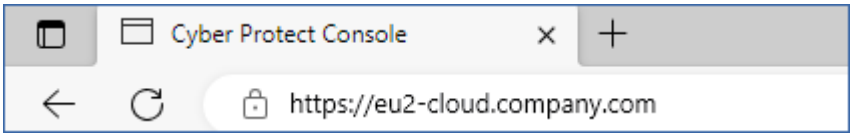
5. 使用以下其中一種方法，在 Cyber Protection 服務中註冊裝置。
   - [僅適用於不含雙重驗證機制的租用戶] 在其圖形化介面中註冊裝置。
     a. 在 **[代理程式選項]** 的 **[管理伺服器]** 欄位中，按一下 **[變更]**。
     b. 在 **[伺服器名稱/IP]** 欄位中，選擇 **[雲端]**。
        Cyber Protection 服務位址隨即出現。除非特別指示，否則請不要變更此位址。
     c. 在 **[使用者名稱]** 和 **[密碼]** 欄位中，指定您的帳戶在 Cyber Protection 服務中的認證。裝置所管理的虛擬裝置和虛擬機器會使用此帳戶註冊。
     d. 按一下 **[確定]**。
   - 在命令列介面中註冊裝置。

     注意事項
     使用此方法時，您需要註冊權杖。如需有關如何產生註冊權杖的詳細資訊，請參閱 "產生註冊權杖" (第 108 頁)。

     a. 按下 CTRL+SHIFT+F2 以開啟命令列介面。
     b. 執行下列命令：

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

     注意事項
     當您使用註冊權杖時，必須指定確實的資料中心位址。這是是您在**登入** Cyber Protect 主控台之後看到的 URL。例如，`https://eu2-cloud.company.com`。

     請不要在這裡使用 `https://cloud.company.com`。

     c. 若要返回裝置的圖形化介面，按下 ALT+F1。

6. [選用] 在 **[名稱]** 欄位中，按一下 **[變更]** 以變更虛擬裝置的預設名稱，亦即 **localhost**。此名稱會顯示在 Cyber Protect 主控台中。
7. [選用] 在 **[時間]** 欄位中，按一下 **[變更]**，然後選擇您所在位置的時區，以確保排程作業在適當時間執行。

8. [選用] [如果您的網路中已啟用 Proxy 伺服器] 設定 Proxy 伺服器。
   a. 按下 CTRL+SHIFT+F2 以開啟命令列介面。
   b. 使用文字編輯器開啟檔案 **/etc/Acronis/Global.config**。
   c. 執行下列其中一項操作：
      - 如果在代理程式安裝期間指定 Proxy 設定，請找出下列區段：

        ```
        <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>
        ```

      - 否則，複製以上幾行，並將其貼入檔案的 `<registry name="Global">...</registry>` 標籤之間。
   d. 將 `ADDRESS` 取代為新的 Proxy 伺服器主機名稱/IP 位址，並將 `PORT` 取代為連接埠號碼的十六進位值。
   e. 如果您的 Proxy 伺服器需要驗證，請將 `LOGIN` 和 `PASSWORD` 取代為 Proxy 伺服器認證。否則，請從檔案中刪除這幾行。
   f. 儲存檔案。
   g. 在文字編輯器中開啟檔案 **/opt/acronis/etc/aakore.yaml**。
   h. 找出 **env** 區段，或建立該區段並加入下列幾行：

      ```
      env:
          http-proxy: proxy_login:proxy_password@proxy_address:port
          https-proxy: proxy_login:proxy_password@proxy_address:port
      ```

   i. 將 `proxy_login` 和 `proxy_password` 取代為 Proxy 伺服器認證，並將 `proxy_address:port` 取代為 Proxy 伺服器的位址和連接埠號碼。
   j. 執行 `reboot` 命令。

注意事項

為能夠更新在 Proxy 後部署的虛擬裝置，請編輯裝置的 `config.yaml` 檔案 (`/opt/acronis/etc/va-updater/config.yaml`)，方法是，將以下一行新增到該檔案的底部，然後輸入專用於您環境的值：

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

例如：

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

保護 Red Hat Virtualization/oVirt 資料中心中的虛擬機器

1. 請登入您的 Cyber Protection 帳戶。
2. 瀏覽至 **[裝置]** > **[oVirt]** > <您的叢集> >，或在 **[裝置]** > **[所有裝置]** 中尋找您的電腦。
3. 選擇電腦，並為其套用保護計劃。

oVirt 用代理程式 – 所需角色和連接埠

所需角色

若要進行部署和操作，oVirt 用代理程式需要有獲指派下列角色的系統管理員帳戶。

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

所需連接埠

oVirt 用代理程式會使用您在設定虛擬裝置時指定的 URL，連線至 oVirt 引擎。引擎 URL 的格式通常如下：`https://ovirt.company.com`。此案例中使用的是 HTTPS 通訊協定和連接埠 443。

非預設的 oVirt 設定可能需要使用其他連接埠。您可以透過分析 URL 格式來尋找確實的連接埠。例如：

oVirt 引擎 URL	連接埠	通訊協定
`https://ovirt.company.com/`	443	HTTPS
`http://ovirt.company.com/`	80	HTTP
`https://ovirt.company.com:1234/`	1234	HTTPS

磁碟讀取/寫入作業不需要其他連接埠，因為備份是在 HotAdd 模式下執行的。

部署 Azure 用代理程式

您可以透過設定 Azure 用代理程式 (可以透明地存取 Microsoft Azure 虛擬機器資料的單一代理程式) 來執行 Microsoft Azure 虛擬機器的無代理程式備份。

Azure 用代理程式可確保：

- 執行 Windows 或 Linux 之 Microsoft Azure 虛擬機器的備份和還原功能。
- 減少 Microsoft Azure 虛擬機器的費用 (僅需管理一個代理程式)。
- 將任何內部部署或雲端機器備份透明移轉至 Microsoft Azure 虛擬機器 (可透過 Cyber Protect 主控台設定)。
- 降低 Microsoft Azure 資源成本 (虛擬機器內僅需要一個負擔代理程式的 CPU 和 RAM 費用)。

在您開始之前

代理程式的系統需求

預設情況下，虛擬裝置會獲指派 **Standard_B2s** 大小 (4 GiB 的 RAM 和 2 個 CPU)，這對大部分操作來說是最佳的且已足夠。如需有關此設定和其他 Azure 虛擬機器屬性的詳細資訊，請參閱 Microsoft Azure 文件。

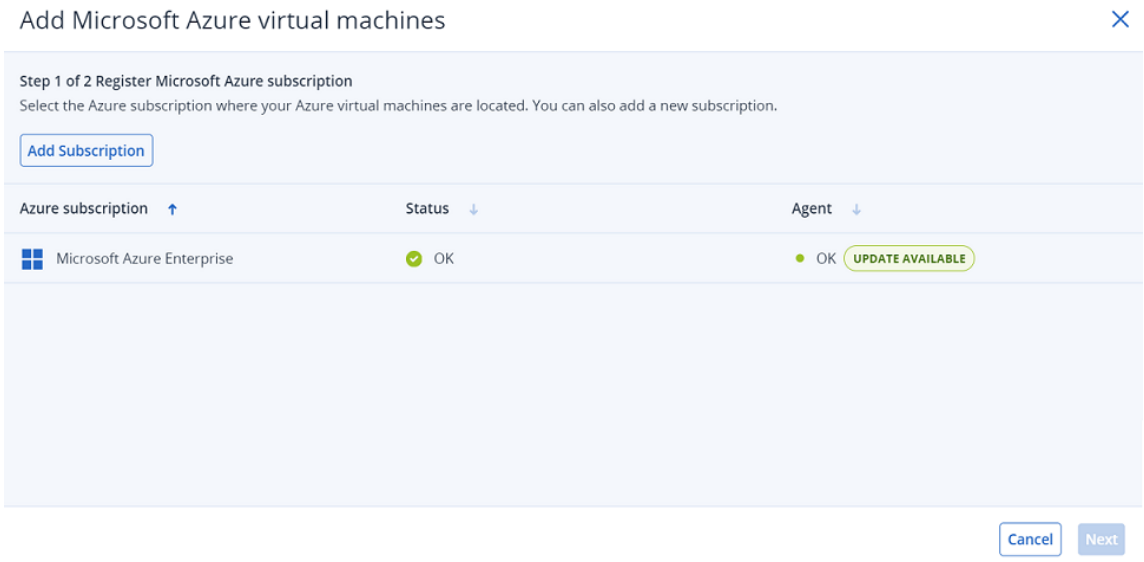
部署 Azure 虛擬裝置用代理程式

您要先連線至相關的 Microsoft Azure 訂閱，然後定義 Azure 部署設定，才能部署 Azure 虛擬裝置用代理程式。

注意事項
透過 **[裝置]** 或 **[備份儲存]** 功能表建立備份位置時，可以設定與 Microsoft Azure 訂閱的連線，如 "在 Microsoft Azure 中定義備份位置" (第 480 頁) 中所述。

若要部署 Azure 虛擬裝置用代理程式

1. 在 Cyber Protect 主控台中，移至 **[裝置]** > **[所有電腦]**。
2. 按一下 **[新增]**。
3. 在 **[雲端工作負載]** 區段下，選擇 **[Microsoft Azure 虛擬機器]**。
   - 如果您已使用現有的 Microsoft Azure 訂閱，則會顯示 [新增 Microsoft Azure 虛擬機器精靈]，並列出您現有的訂閱。您可以選擇相關的訂閱，然後按一下 **[下一步]**。接著，繼續執行步驟 8。



   - 如果您已使用現有的 Microsoft Azure 訂閱，但想要新增訂閱，請按一下 **[新增訂閱]**。
   - 如果您沒有現有的訂閱，請按一下 **[新增]** 以新增訂閱。
4. 在顯示的對話方塊中，按一下 **[登入]**。系統會將您重新導向至 Microsoft 登入頁面。

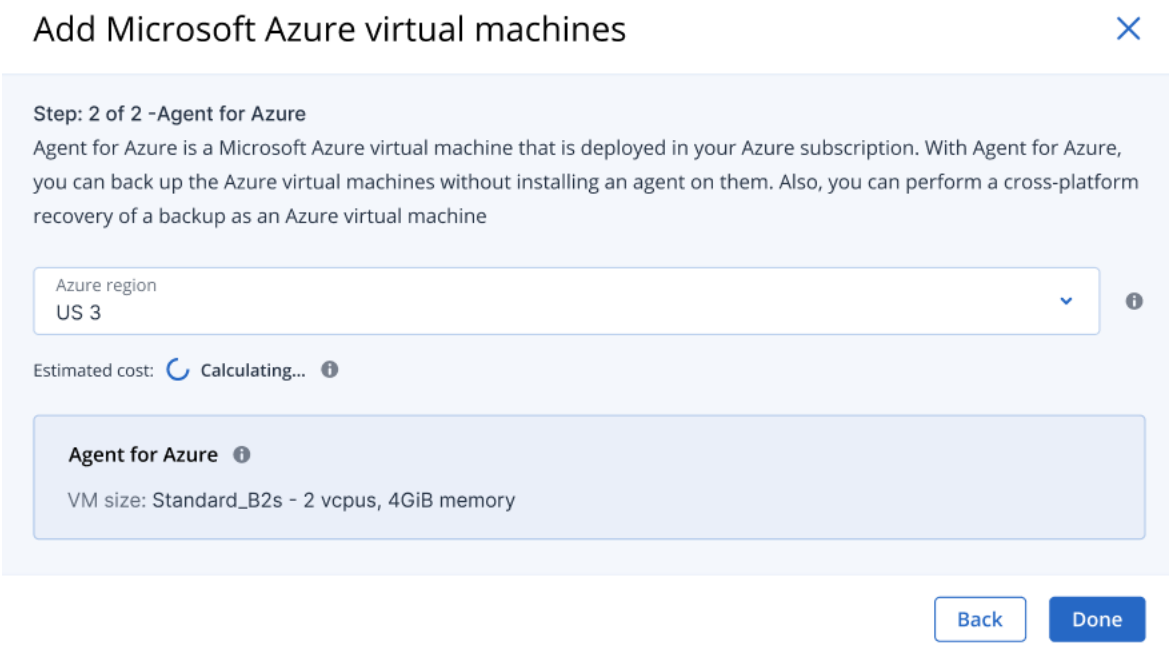
注意事項

您必須在 Microsoft Entra ID 中獲指派以下其中一個角色，才能完成與訂閱的連線：雲端應用程式系統管理員、應用程式系統管理員或全域系統管理員。您也必須獲指派每個所選訂閱的擁有者角色。

5. 輸入您的 Microsoft 登入認證，並接受要求的權限。連線程序隨即開啟，而且可能需要幾分鐘的時間。

   如需有關如何安全地存取 Microsoft Azure 訂閱的詳細資訊，請參閱 Microsoft Azure 連線安全性和稽核 (72684) 一文。
6. 連線完成時：
   - 如果您有多個訂閱，請從顯示的對話方塊中的下拉式清單選擇相關的訂閱，然後按一下 **[新增訂閱]**。接著，系統會將您重新導向至精靈主畫面。
   - 如果您要新增第一個訂閱，則會重新導向至精靈主畫面。
7. 選擇相關的訂閱，然後按一下 **[下一步]**。
8. 從 **[Azure 區域]** 下拉式清單中，選擇訂閱的相關區域。為了最佳化備份效能，您應該選擇部署大部分要受保護的虛擬機器的 Azure 區域。

   系統會計算並顯示該區域的預估成本。這些成本將計入您的 Microsoft Azure 訂閱，並由 Microsoft 開立帳單。



注意事項

部署的 Azure 用代理程式會使用 Standard_B2s 大小。

9. 按一下**[完成]**。

   系統會將您重新導向至 **[裝置]** > **[Microsoft Azure]** 畫面，其中會顯示部署的進度。完成後，您可以開始使用新加入的訂閱來定義保護計劃。

如需有關其他 Microsoft Azure 備份和復原選項的詳細資訊，請參閱 "Azure 還原點" (第 397 頁) 和 "復原虛擬機器您可以從其備份復原虛擬機器。您無法在 Cyber Protect 主控台中，為 [合規] 模式下的租用戶復原備份。如需有關如何復原此類備份的詳細資訊，請參閱 Recovering backups for tenants in the Compliance mode。必要條件復原至虛擬機器時，此虛擬機器必須為停止狀態。軟體預設不會顯示提示，即停止電腦。復原完成後，您必須手動啟動電腦。您可以使用 VM 電源管理復原選項來變更預設行為 (按一下 [復原選項] > [VM 電源管理])。程序執行下列其中一項操作：選擇已備份的電腦，按一下復原，然後選擇復原點。在 [備份儲存] 索引標籤上選擇復原點。按一下[復原] > [整部機器]。如果您想要復原到實體機器，請在復原至中選擇實體機器。否則，請跳過此步驟。只有在目標電腦的磁碟組態完全符合備份中的磁碟組態時，才能復原至實體機器。在此情況下，請繼續在「實體機器」中的步驟 4。否則，我們建議您使用可開機媒體來執行 V2P 移轉。[選用] 軟體預設會自動選擇原始電腦做為目標電腦。若要復原到另一部虛擬機器，請按一下目標機器然後進行以下操作：選擇 Hypervisor ([VMware ESXi]、[Hyper-V]、[Virtuozzo]、[Virtuozzo Hybrid Infrastructure]、[Scale Computing HC3] 或 [oVirt])。只有 Virtuozzo 虛擬機器可復原至 Virtuozzo。如需 V2V 移轉的詳細資訊，請參閱「電腦移轉」。請注意，選擇 Microsoft Azure 作為目標時，您可以選擇相關的 Azure 訂閱、區域和資源群組。選擇主機並指定新電腦名稱，或選擇現有目標電腦。選擇主機並指定新電腦名稱，或選擇現有目標電腦。按一下 [確定]。設定您需要的其他復原選項。[不適用於 Virtuozzo Hybrid Infrastructure 和 Scale Computing HC3] 若要選擇虛擬機器的資料存放區，按一下 [資料存放區] (ESXi)、[路徑] (Hyper-V 和 Virtuozzo)，或 [儲存網域] (Red Hat Virtualization (oVirt))，然後選擇虛擬機器的資料存放區 (儲存空間)。若要檢視每個虛擬磁碟的資料存放區 (儲存空間)、介面以及佈建模式，按一下 [磁碟對應]。除非您要復原 Virtuozzo 容器或 Virtuozzo Hybrid Infrastructure 虛擬機器，否則您可以變更這些設定。若是 Virtuozzo Hybrid Infrastructure，您僅能選擇目標磁碟的儲存原則。方法是，選擇所需的目標磁碟，然後按一下 [變更]。在開啟的刀鋒視窗中，按一下齒輪圖示、選擇儲存原則，然後按一下 [完成]。該對映區段使您還可以選擇要復原的個別磁碟。若是 Microsoft Azure，您可以選擇相關的儲存體類型 (本機備援儲存體 (LRS) 或區域備援儲存體 (ZRS))，以變更每個目標磁碟的儲存體類型。[適用於 VMware ESXi、Hyper-V 和 Virtuozzo] 若要變更記憶體大小、處理器數量，以及虛擬機器的網路連線，請按一下 [VM 設定]。[適用於 Microsoft Azure] 若要變更可用性類型和區域、記憶體大小以及虛擬機器的網路連線 (包括子網路和安全性群組)，請按一下 [VM 設定]。[若是 Virtuozzo Hybrid Infrastructure] 若要變更虛擬機器的記憶體大小和處理器數量，請選擇 [類別]。[僅適用於已安裝保護代理程式的 Windows 電腦] 啟用 [安全復原] 開關以確保復原的資料中沒有惡意軟體。如需有關安全復原如何運作的詳細資訊，請參閱 Safe recovery。按一下 [開始復原]。當復原到現有虛擬機器時，請確認您要覆寫磁碟。復原進度會顯示在 [活動] 索引標籤上。" (第 1 頁)。

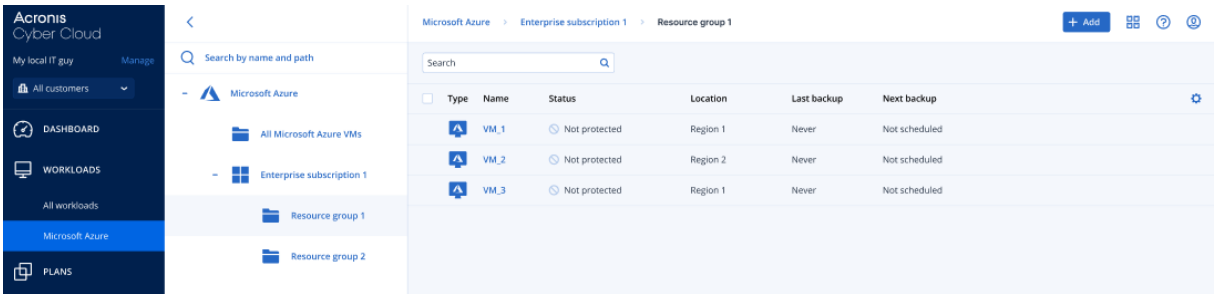
檢視及更新已部署的 Azure 用代理程式

您可以透過下列方式檢視及更新您的 Azure 用代理程式部署：

- 透過 **[裝置] > [Microsoft Azure]** 功能表檢視目前的部署。
- 透過 **[基礎架構] > [公有雲端]** 功能表檢視、更新、存取和重新部署目前的部署。

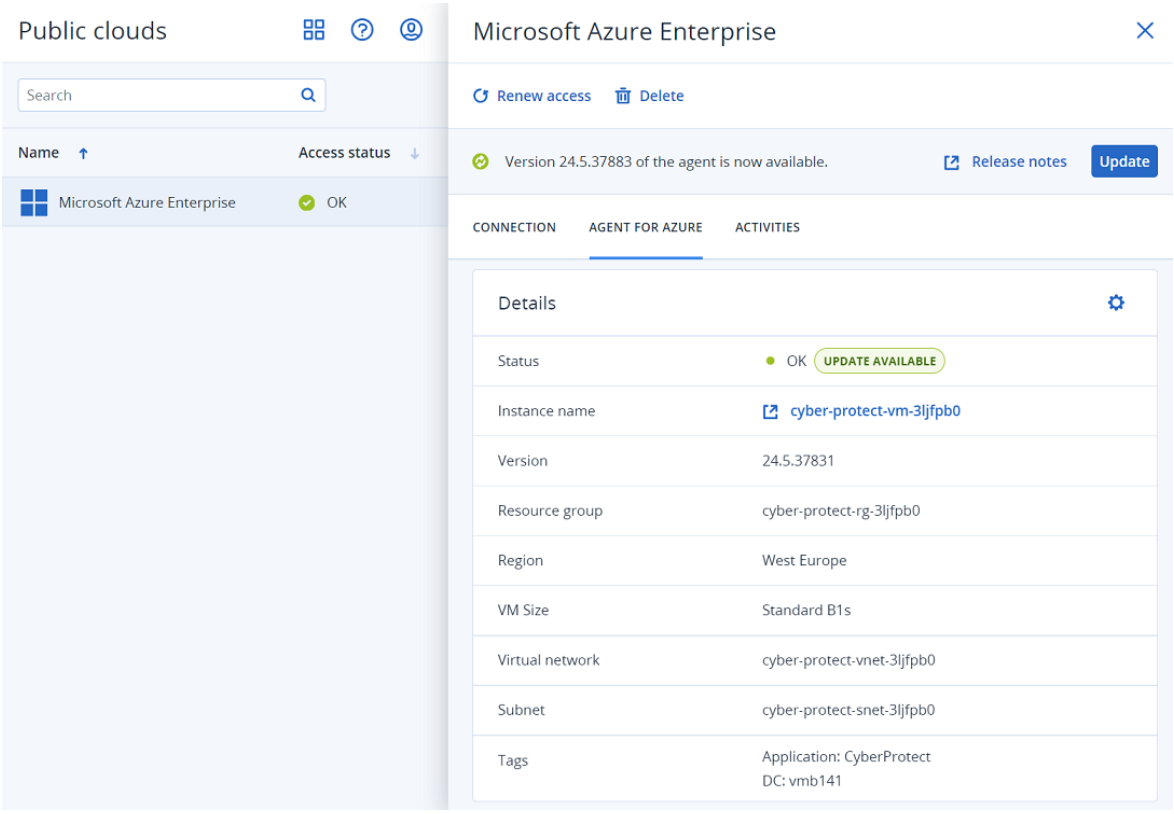
若要透過 [Microsoft Azure] 功能表檢視目前的部署

在 Cyber Protect 主控台中，移至 **[裝置] > [Microsoft Azure]**。目前的 Azure 用代理程式部署清單隨即顯示。請注意，每個列出的訂閱都會在其下方的階層式樹狀目錄中顯示相關的資源群組。



若要透過 [基礎架構] > [公有雲端] 功能表檢視和更新目前的部署

1. 在 Cyber Protect 主控台中，移至 **[基礎架構] > [公有雲端]**。
   目前的公有雲端連線清單隨即顯示。
2. 選擇部署 Azure 用代理程式的相關 Microsoft Azure 訂閱。
3. 在右窗格中，按一下 **[Azure 用代理程式]** 索引標籤。



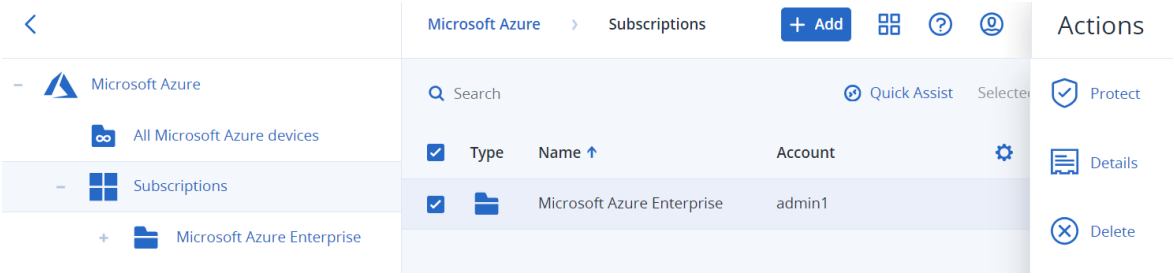
4. 您可以：
   - 檢視部署的目前狀態。
   - 按一下 **[執行個體名稱]** 欄位中的連結，以存取部署 Azure 用代理程式的執行個體。請注意，您必須登入 Microsoft Azure 帳戶，才能存取執行個體。
   - 按一下  以重新部署 Azure 用代理程式。
   - 若有可用的更新，請按一下 **[更新]**。

移除 Azure 虛擬裝置用代理程式

當您移除對應的 Microsoft Azure 訂閱時，會自動移除 Azure 虛擬裝置用代理程式。

若要移除 Azure 虛擬裝置用代理程式

1. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[Microsoft Azure]**。
2. 按一下階層式樹狀目錄中的 **[訂閱]** 節點，然後在右側顯示的清單中選擇相關的訂閱。



3. 在右窗格中，按一下 **[刪除]**。
4. 在顯示的確認對話方塊中，按一下 **[移除]**。

   移除訂閱時，會取消佈建 Azure 虛擬裝置用代理程式，且不會使用 Microsoft Azure 資源。

注意事項

如果 Microsoft Azure 虛擬機器目前正在使用訂閱，則無法移除該訂閱。

部署 Synology 用代理程式

在您開始之前

使用 Synology 用代理程式，您可以從 Synology NAS 裝置備份檔案和資料夾，也可以將檔案和資料夾備份到 Synology NAS 裝置。共用、資料夾和檔案的 NAS 特定屬性與存取權限會保留。

Synology 用代理程式在 NSA 裝置上執行。因此，您可以使用裝置資源進行脫離主機資料處理作業，例如，備份複寫、驗證和清理。若要深入瞭解這些作業，請參閱 "脫離主機資料保護計劃" (第 198 頁)。

注意事項

Synology 用代理程式僅支援配備 x86_64 處理器的 NAS 裝置。不支援 ARM 處理器。請參閱 Synology 知識中心。

您可以將備份復原到 NSA 裝置的原始位置或新位置，也可以復原到可透過該裝置存取的網路資料夾。雲端儲存空間中的備份也可以復原到已安裝 Synology 用代理程式的非原始 NAN 裝置上。

下表摘要了可用備份來源和目的地。

備份內容	要備份的項目 (備份來源)	備份目標位置 (備份目的地)
檔案/資料夾	本機資料夾*	雲端儲存
		本機資料夾*
	網路資料夾 (SMB)**	網路資料夾 (SMB)**
		NFS 資料夾
		公有雲端***

* 包括附加到 NAS 裝置的 USB 磁碟機。

注意事項
不支援加密的資料夾。這些資料夾不會顯示在 Cyber Protection 圖形使用者介面中。

** 透過 SMB 通訊協定使用外部網路共用作為備份來源或備份目的地僅適用於在 Synology DiskStation Manager 6.2.3 和更新版本上執行的代理程式。Synology NAS 本身託管的資料 (包括託管網路共用中的資料) 可以不受限制地備份。

*** 僅 Synology 7.x 用代理程式支援備份到公有雲端，例如 Microsoft Azure、Amazon、Wasabi 或 S3 相容儲存空間。基於 Synology DSM 6.x 的 Linux 核心限制，Synology 6.x 用代理程式不支援此備份目的地。

限制

- Synology 用代理程式僅支援配備 x86_64 處理器的 NAS 裝置。不支援 ARM 處理器。請參閱 Synology 知識中心。
- 已備份的加密共用會被當作未加密復原。
- 已啟用 **[檔案壓縮]** 選項的已備份共用，會以停用該選項的方式復原。
- 您只能將 Synology 用代理程式建立的備份還原到 Synology NAS 裝置。

下載安裝程式

Synology 用代理程式的安裝程式以 SPK 檔案形式提供。

Synology 7.x 用代理程式

若要下載安裝程式

1. 在 Cyber Protect 主控台中，瀏覽至 **[裝置]** > **[所有裝置]**。
2. 按一下右上角的 **[新增]**。
3. 在 **[網路連接儲存裝置 (NAS)]** 底下，按一下 **[Synology]**。
   安裝程式會下載到您的電腦中。

Synology 6.x 用代理程式

若要下載安裝程式

1. 在 Cyber Protect 主控台中，瀏覽至 **[裝置]** > **[所有裝置]**。
2. 按一下右上角的 **[新增]**。
3. 在 **[網路連接儲存裝置 (NAS)]** 底下，按一下 **[Synology]**。
   Synology 7.x 用代理程式的安裝程式會下載到您的電腦中。
   您可以安全地停止下載程序，或忽略下載的檔案。
4. 按一下 **[下載 Synology 6.x 用代理程式]**。
   Synology 6.x 用代理程式的安裝程式會下載到您的電腦中。

安裝 Synology 用代理程式

若要安裝 Synology 用代理程式，請在 Synology DiskStation Manager 中執行SPK 檔案。

注意事項
Synology 用代理程式僅支援配備 x86_64 處理器的 NAS 裝置。不支援 ARM 處理器。請參閱 Synology 知識中心。

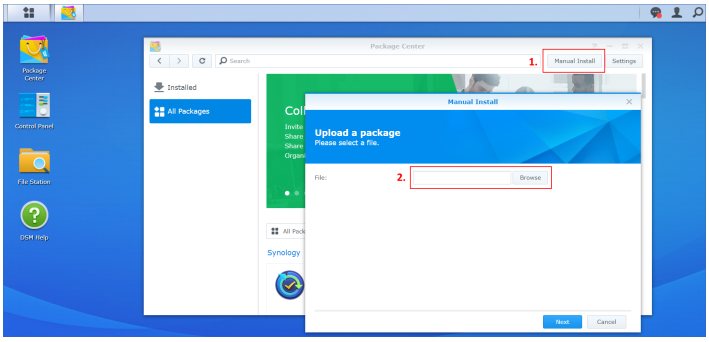
Synology 7.x 用代理程式

必要條件

- NAS 裝置執行 DiskStation Manager 7.x。
- 您是 NAS 裝置上 **Administrators** 群組的成員。
- 在您要安裝代理程式的 NAS 磁碟區上，至少要有 200 MB 的可用空間。
- SSH 用戶端可用於您的電腦。此文件使用 Putty 作為範例。

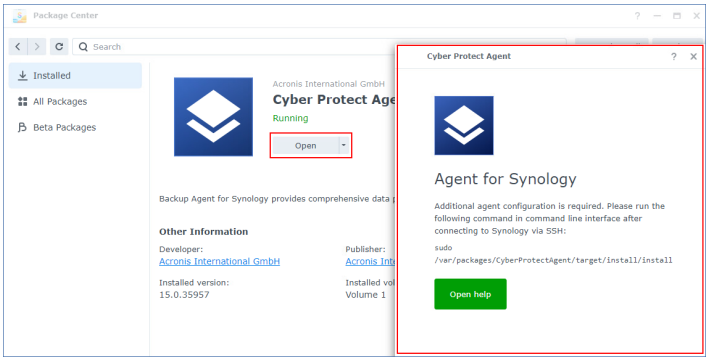
若要安裝 Synology 用代理程式

1. 登入 Synology DiskStation Manager。
2. 開啟 **[套件中心]**。
3. 按一下 **[手動安裝]**，然後按一下 **[瀏覽]**。



4. 選擇您從 Cyber Protect 主控台下載的 SPK 檔案，然後按一下 **[下一步]**。
   此時會顯示您將安裝第三方軟體套件的警告。此訊息是標準安裝程序的一部分。
5. 為確認您要安裝此套件，按一下 **[同意]**。
6. 選擇您要安裝代理程式的磁碟區，然後按一下 **[下一步]**。
7. 檢查設定，然後按一下 **[完成]**。

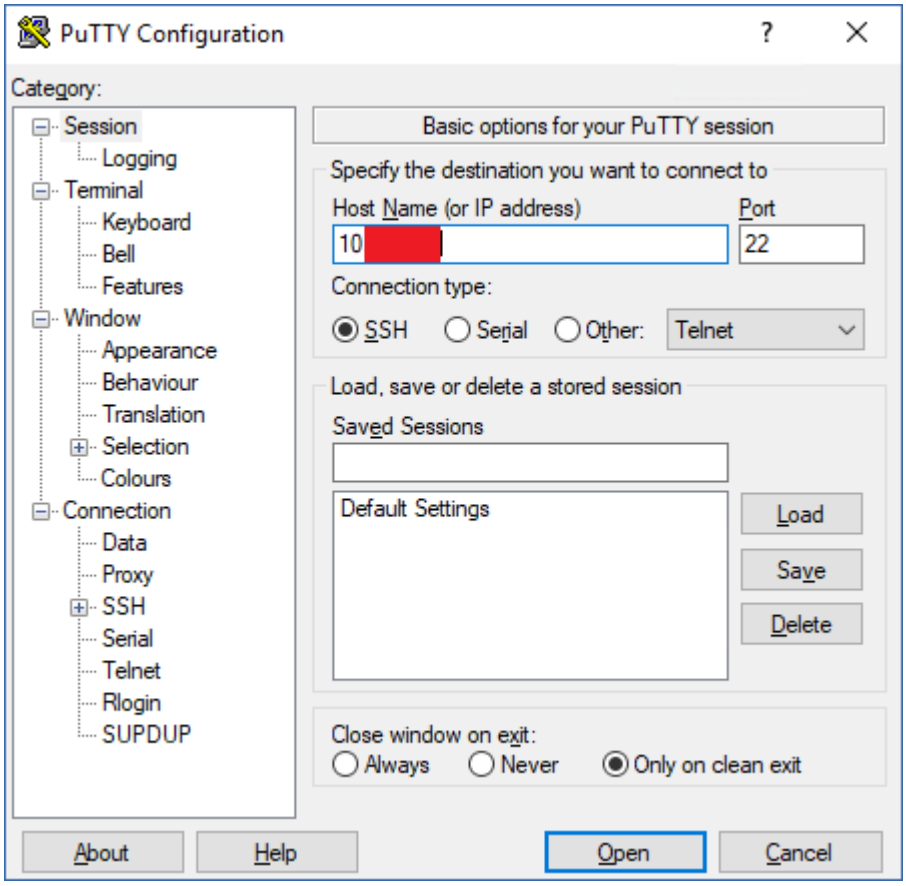
8. 在 Synology DiskStation Manager 的 **[套件中心]** 中，開啟 Cyber Protect Synology 用代理程式，然後確認您看到以下畫面。



9. 在 Synology DiskStation Manager 的 **[控制台]** 中，移至 **[終端機和 SNMP]**，然後對 NAS 裝置啟用 SSH 存取。
10. 在 NAS 裝置上，使用 SSH 用戶端 (在此範例中為 Putty)，執行 `install` 指令碼。

    此指令碼會對 DSM 7.0 或更新版本啟用根存取，這是設定代理程式所必需。

    a. 啟動 Putty，然後指定 Synology NAS 裝置的 IP 位址或主機名稱。



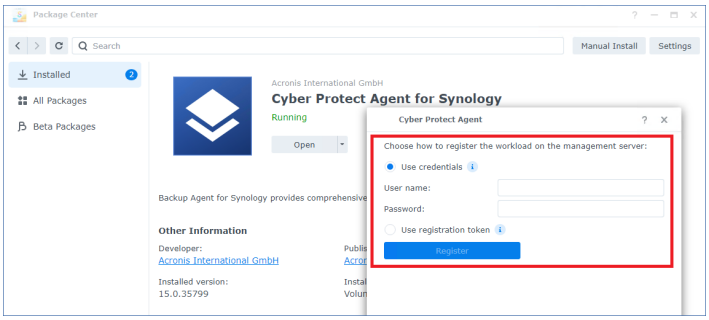
    b. 按一下 **[開啟]**，然後以 Synology DSM 系統管理員身分登入。

    c. 執行下列命令。

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

    指令碼啟動後，等待 15 秒，在此期間 Cyber Protection 服務會初始化。

11. 在 Synology DiskStation Manager 的 **[控制台]** 中，移至 **[終端機和 SNMP]**，然後對 NAS 裝置停用 SSH 存取。您不再需要 SSH 存取。
12. 在 Synology DiskStation Manager 的 **[套件中心]** 中，開啟 Cyber Protect Synology 用代理程式。
13. 選擇註冊方法。



- [使用認證註冊代理程式]
  - 在 **[使用者名稱]** 和 **[密碼]** 欄位中，指定註冊代理程式所使用之帳戶的認證。此帳戶不得是合作夥伴系統管理員帳戶。
- [使用註冊權杖註冊代理程式]
  - 在 **[註冊位址]** 中，指定確切的資料中心位址。確切的資料中心位址是您登入 Cyber Protect 主控台後看到的 URL。例如，`https://us5-cloud.acronis.com`。

    注意事項
    請不要使用不含資料中心位址的 URL 格式。例如，請不要使用 `https://cloud.acronis.com`。

  - 在 **[權杖]** 欄位中，指定註冊權杖。
    如需有關如何產生註冊權杖的詳細資訊，請參閱 "產生註冊權杖" (第 108 頁)。
14. 按一下 **[註冊]**。

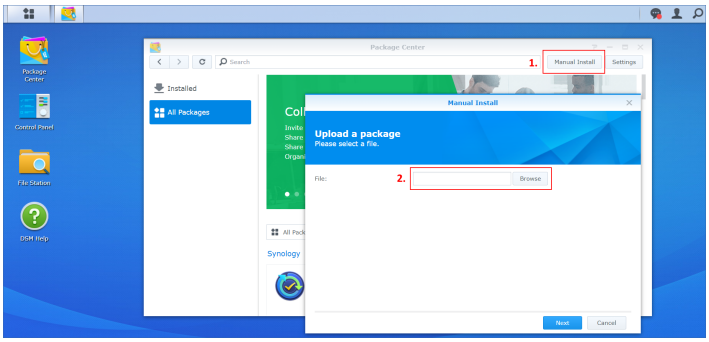
Synology 6.x 用代理程式

必要條件

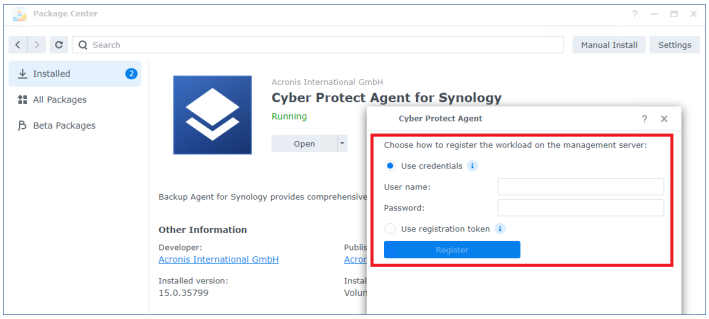
- NAS 裝置執行 DiskStation Manager 6.2.x。
- 您是 NAS 裝置上 **Administrators** 群組的成員。
- 在您要安裝代理程式的 NAS 磁碟區上，至少要有 200 MB 的可用空間。

若要安裝 Synology 用代理程式

1. 登入 Synology DiskStation Manager。
2. 開啟 **[套件中心]**。
3. 按一下 **[手動安裝]**，然後按一下 **[瀏覽]**。



4. 選擇您從 Cyber Protect 主控台下載的 SPK 檔案，然後按一下 **[下一步]**。
   此時會顯示您將安裝不含數位簽章的套件的警告。此訊息是標準安裝程序的一部分。
5. 為確認您要安裝此套件，按一下 **[是]**。
6. 選擇您要安裝代理程式的磁碟區，然後按一下 **[下一步]**。
7. 檢查設定，然後按一下 **[套用]**。
8. 在 Synology DiskStation Manager 的 **[套件中心]** 中，開啟 Cyber Protect Synology 用代理程式。
9. 選擇註冊方法。



   - [使用認證註冊代理程式]
     - 在 **[使用者名稱]** 和 **[密碼]** 欄位中，指定註冊代理程式所使用之帳戶的認證。此帳戶不得是合作夥伴系統管理員帳戶。
   - [使用註冊權杖註冊代理程式]
     - 在 **[註冊位址]** 中，指定確切的資料中心位址。確切的資料中心位址是您登入 Cyber Protect 主控台後看到的 URL。例如，`https://us5-cloud.acronis.com`。

       注意事項
       請不要使用不含資料中心位址的 URL 格式。例如，請不要使用 `https://cloud.acronis.com`。

     - 在 **[權杖]** 欄位中，指定註冊權杖。
       如需有關如何產生註冊權杖的詳細資訊，請參閱 "產生註冊權杖" (第 108 頁)。
10. 按一下 **[註冊]**。

註冊完成之後，Synology NAS 裝置將會出現在 Cyber Protect 主控台的 **[裝置]** > **[網路連接儲存裝置]** 索引標籤上。

若要備份 NAS 裝置上的資料，請套用保護計劃。

更新 Synology 用代理程式

您可以將 Synology 6.x 用代理程式更新為更新版本的 Synology 6.x 用代理程式。同樣地，您可以將 Synology 7.x 用代理程式更新為更新版本的 Synology 7.x 用代理程式。

若要更新代理程式，請在 Synology DiskStation Manager 中執行新版安裝程式。將保留代理程式的原始註冊、其設定，以及套用至受保護工作負載的計劃。

注意事項
您無法從 Cyber Protect 主控台更新代理程式。

僅支援透過解除安裝舊版代理程式後再安裝新版代理程式來將 Synology 6.x 用代理程式升級到 Synology 7.x 用代理程式。在此情況下，所有保護計劃都會遭到撤銷，而且您必須手動重新套用這些保護計劃。

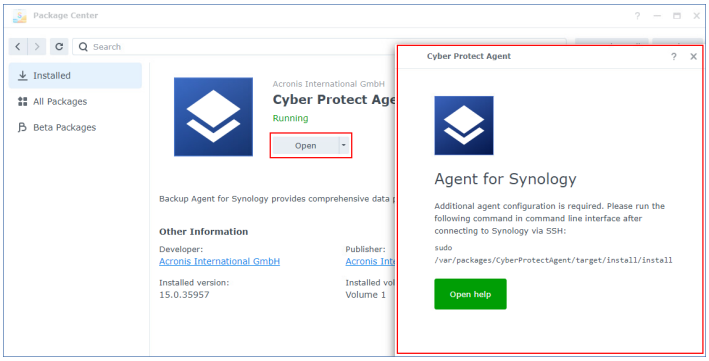
Synology 7.x 用代理程式

必要條件

- 您是 NAS 裝置上 **Administrators** 群組的成員。
- 在您要安裝代理程式的 NAS 磁碟區上，至少要有 200 MB 的可用空間。
- SSH 用戶端可用於您的電腦。此文件使用 Putty 作為範例。

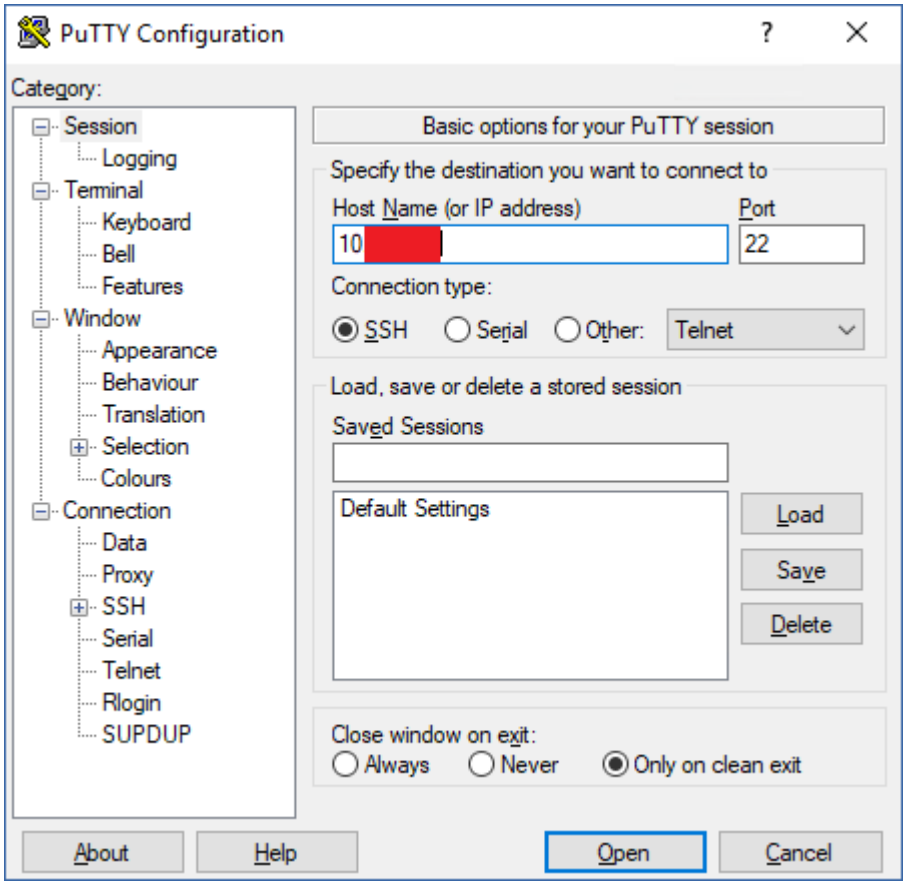
若要更新 Synology 用代理程式

1. 在 DiskStation Manager 中，開啟 **[套件中心]**。
2. 按一下 **[手動安裝]**，然後按一下 **[瀏覽]**。
3. 選擇您從 Cyber Protect 主控台下載的 Synology 7.x 用代理程式的新版 SPK 檔案，然後按一下 **[下一步]**。
   此時會顯示您將安裝第三方軟體套件的警告。此訊息是標準安裝程序的一部分。
4. 為確認您要安裝此套件，按一下 **[同意]**。
5. 檢查設定，然後按一下 **[完成]**。
6. 在 Synology DiskStation Manager 的 **[套件中心]** 中，開啟 Cyber Protect Synology 用代理程式，然後確認您看到以下畫面。



7. 在 Synology DiskStation Manager 的 **[控制台]** 中，移至 **[終端機和 SNMP]**，然後對 NAS 裝置啟用 SSH 存取。

8. 在 NAS 裝置上，使用 SSH 用戶端 (在此範例中為 Putty)，執行 `install` 指令碼。
   此指令碼會對 DSM 7.0 或更新版本啟用根存取，這是設定代理程式所必需。
   a. 啟動 Putty，然後指定 Synology NAS 裝置的 IP 位址或主機名稱。



   b. 按一下 **[開啟]**，然後以 Synology DSM 系統管理員身分登入。
   c. 執行下列命令。

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

9. 在 Synology DiskStation Manager 的 **[控制台]** 中，移至 **[終端機和 SNMP]**，然後對 NAS 裝置停用 SSH 存取。您不再需要 SSH 存取。

Synology 6.x 用代理程式

必要條件

- 您是 NAS 裝置上 **Administrators** 群組的成員。
- 在您要安裝代理程式的 NAS 磁碟區上，至少要有 200 MB 的可用空間。

若要更新 Synology 用代理程式

1. 在 DiskStation Manager 中，開啟 **[套件中心]**。
2. 按一下 **[手動安裝]**，然後按一下 **[瀏覽]**。
3. 選擇您從 Cyber Protect 主控台下載的 Synology 6.x 用代理程式的新版 SPK 檔案，然後按一下 **[下一步]**。

此時會顯示您將安裝不含數位簽章的套件的警告。此訊息是標準安裝程序的一部分。

4. 為確認您要安裝此套件，按一下 **[是]**。
5. 檢查設定，然後按一下 **[套用]**。

虛擬裝置的 SSH 連線

當您從遠端存取虛擬裝置進行維護時，請使用 Secure Socket Shell (SSH) 連線。

啟動安全殼層精靈

若要允許虛擬裝置的 SSH 連線，請在裝置上啟動安全殼層精靈 (sshd)。

若要啟動安全殼層精靈

1. 在 Hypervisor 軟體中，開啟虛擬裝置的主控台。
2. 在裝置的圖形使用者介面中，按下 CTRL+SHIFT+F2 以開啟命令列介面。
3. 執行下列命令：

   ```
   /bin/sshd
   ```

4. [只有在第一次連線到裝置期間] 設定 root 使用者的密碼。

   若要瞭解如何設定密碼，請參閱 "在虛擬裝置上設定根密碼" (第 155 頁)。

注意事項

建議您在不使用 SSH 連線時，停止安全殼層精靈。

在虛擬裝置上設定根密碼

在首次建立虛擬裝置的 SSH 連線之前，您必須在裝置上設定根密碼。

若要設定根密碼

1. 在 Hypervisor 軟體中，開啟虛擬裝置的主控台。
2. 在裝置的圖形使用者介面中，按下 CTRL+SHIFT+F2 以開啟命令列介面。
3. 執行下列命令：

   ```
   passwd
   ```

4. 指定密碼，然後按下 Enter。

   密碼必須包含至少 9 個字元，且複雜度分數必須為 3 或更高。複雜度分數是自動計算的。若要獲得更高的分數，請使用特殊符號、大寫和小寫符號以及數字的組合。
5. 確認密碼，然後按下 Enter。

透過 SSH 用戶端存取虛擬裝置

必要條件

- 遠端電腦必須有一個 SSH 用戶端。以下程序使用 WinSCP 用戶端作為範例。您可以使用任何 SSH 用戶端，只需相應地調整步驟即可。
- 安全殼層精靈 (sshd) 必須在虛擬裝置上啟動。如需詳細資訊，請參閱 "啟動安全殼層精靈" (第 155 頁)。

若要透過 WinSCP 存取虛擬裝置

1. 在遠端電腦上，開啟 WinSCP。
2. 按一下 **[工作階段]** > **[新增工作階段]**。
3. 在 **[檔案通訊協定]** 中，選擇 **[SCP]**。
4. 在 **[主機名稱]** 中，指定您虛擬裝置的 IP 位址。
5. 在 **[使用者名稱]** 和 **[密碼]** 中，指定 `root` 和 `root` 使用者的密碼。
6. 按一下 **[登入]**。

虛擬裝置上所有目錄的清單隨即顯示。

裝置探索

使用裝置探索功能，您可以：

- 全盤掌握組織網路中可用網路裝置的狀況。
- 使用與 Active Directory 的同步，以減少在大型 Active Directory 網域中佈建資源及管理電腦的工作。
- 偵測 Active Directory 網域或區域網路中的機器，自動安裝保護代理程式並自動註冊機器。
- 在多個工作負載上安裝保護代理程式。

您可以使用下列其中一種方法執行裝置探索：

- Active Directory 探索。

  在 Active Directory 探索期間，探索代理程式會收集有關電腦組織單位 (OU) 的資訊以及有關其名稱及作業系統的詳細資訊。不過，不會收集 IP 與 MAC 位址。
- 使用 Device Sense ™ 進行區域網路探索。如需詳細資訊，請參閱 "使用 Device Sense ™ 進行裝置探索" (第 163 頁)。
- 手動探索 – 透過使用電腦 IP 位址或主機名稱，或從檔案匯入電腦清單。

  在手動探索過程中，會更新並重新註冊現有的保護代理程式。如果您使用註冊代理程式的相同帳戶執行裝置探索，則代理程式只會更新到最新版本。如果您使用其他帳戶執行裝置探索，則代理程式會更新到最新版本，並使用帳戶所屬的租用戶重新註冊。

您也可以使用 Device Sense ™ 設定被動式裝置探索，並檢視組織中公司區域網路內可用裝置的詳細資訊。如需詳細資訊，請參閱 "使用 Device Sense ™ 進行被動式裝置探索" (第 164 頁)。

探索多個裝置

探索多個裝置的流程可總結為以下步驟：

1. 選擇探索方法：
   - Active Directory 探索。
   - 使用 Device Sense ™ 進行區域網路探索。
   - 手動探索 – 透過使用電腦 IP 位址或主機名稱，或從檔案匯入電腦清單。
2. [對於 Active Directory 探索和手動探索] 選擇要新增至租用戶的電腦。
3. [對於 Active Directory 探索和手動探索] 選擇如何新增這些電腦：
   - 在電腦上安裝保護代理程式和其他元件，並在 Cyber Protect 主控台中註冊。
   - 在 Cyber Protect 主控台中註冊電腦 (如果已安裝保護代理程式)。
   - 將電腦當作未受管理的裝置新增至 Cyber Protect 主控台，而無需安裝保護代理程式。

   您也可以將保護計劃、監控計劃和遠端管理計劃套用至安裝保護代理程式的電腦或在 Cyber Protect 主控台中註冊的電腦。
4. [對於 Active Directory 探索和手動探索] 提供所選電腦的系統管理員認證。
5. [對於 Active Directory 探索和手動探索] 確認您是否可以使用提供的認證，連線至這些電腦。

Cyber Protect 主控台中顯示的電腦分為以下類別：

- **探索到的裝置** – 已探索到但尚未安裝保護代理程式的電腦。
- **包含代理程式的電腦** – 已安裝保護代理程式的電腦。
- **探索到的裝置/無代理程式的裝置** – 可在其上安裝保護代理程式的電腦。
- **[探索到的裝置]/[區域網路]** – 透過使用 Device Sense ™ 掃描區域網路探索到的電腦和網路裝置。
- **探索到的裝置/Active Directory** – 透過搜尋 Active Directory 探索到的電腦。
- **探索到的裝置/手動/從文字檔案** – 已手動新增或從文字檔案新增的電腦。

裝置探索需求

使用裝置探索功能之前，請確定符合下列需求：

- 您的區域網路或 Active Directory 網域中必須至少有一部已安裝保護代理程式的電腦可供使用。此代理程式將當作探索代理程式使用。
- 您必須獲指派 Cyber Protection 服務的以下其中一個角色：網路系統管理員或系統管理員。

重要事項

只有安裝在 Windows 電腦上的代理程式可以作為探索代理程式。如果您的環境中沒有探索代理程式，將無法使用 **[新增裝置]** 面板中的 **[多個裝置]** 選項。

僅執行 Windows (不支援 Windows XP) 的機器支援遠端安裝代理程式。若要在執行 Windows Server 2012 R2 的電腦上進行遠端安裝，該電腦上必須已安裝 Windows 更新 KB2999226。

新增多個裝置

在新增多個裝置之前，請確定已符合需求。如需詳細資訊，請參閱 "裝置探索需求" (第 157 頁)。

注意事項
代理程式服務需要其他權限才能執行，因此不支援新增網域控制站的功能。

搜尋 Active Directory

若要在 Active Directory 中新增多個裝置

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 按一下 **[新增]**。
3. 在 **[多個裝置]** 中，按一下 **[探索裝置]**。
   探索精靈便會開啟。
4. 選擇租用戶。
5. 選擇將執行掃描以偵測電腦的探索代理程式。

   注意事項
   探索代理程式是安裝有保護代理程式所在的工作負載。
   探索代理程式必須是 Active Directory 網域的成員。
   您可以選擇與所選單位或其子單位相關聯的代理程式。

6. 選擇 **[搜尋 Active Directory]**，然後按一下 **[下一步]**。
7. 在 **[搜尋 Active Directory]** 視窗中，選擇如何搜尋電腦，然後按一下 **[確定]**。

選項	描述
在組織單位清單中	選擇要新增之電腦的群組。
依 LDAP 方言查詢。	使用 [LDAP 方言] 查詢選擇電腦。**[搜尋基礎]** 可定義搜尋位置，而 **[篩選]** 則可讓您指定選擇電腦的條件。

8. 從探索到的電腦清單中，選擇要新增的電腦，然後按一下 **[下一步]**。
9. 在 **[探索後動作]** 索引標籤上：
   a. 選擇要對電腦執行的操作。

選項	描述
安裝代理程式並登錄電腦	您可以按一下 **[選擇元件]**，選擇要在電腦上安裝的元件。如需詳細資訊，請參閱 "選擇要安裝的元件" (第 161 頁)。
使用已安裝的代理程式登錄電腦	如果電腦上已經安裝代理程式，而且您只需將其登錄到 Cyber Protection，請使用此選項。如果在電腦上找不到代理程式，則會將新增到 **[無代理程式的裝置]** 清單。
新增為未受管理的電腦	如果選擇此選項，電腦上將不會安裝在代理程式。您將可以在主控台中檢視電腦，之後再安裝或註冊代理程式。

   b. 選擇您登錄電腦所要使用的使用者帳戶。

c. [選用] 若要選擇將自動套用至電腦的計劃，請在 **[登錄後的動作]** 區段中，對應計劃類型的計劃選擇欄位內，按一下 **[變更]**，選擇計劃，然後再按一下 **[變更]**。

d. 按 **[下一步]**。

10. 在 **[認證]** 索引標籤上，執行下列動作：

a. 按一下 **[新增認證]**。

b. 選擇對所選裝置具有系統管理員權限的使用者的認證，然後按一下 **[選擇認證]**。

重要事項

只有在您指定內建系統管理員帳戶 (安裝作業系統時建立的第一個帳戶) 的認證後，才能在不做任何準備的情況下，從遠端安裝代理程式。如果您要定義自訂系統管理員認證，則必須手動做一些額外的準備，如需詳細資訊，請參閱 "準備電腦以進行遠端手動安裝" (第 167 頁)。

c. 按 **[下一步]**。

系統會對所選裝置進行初步檢查，以確認這些裝置適用且具有用於遠端安裝代理程式和所選元件的正確設定。

11. [如果有連線問題] 請執行對應的修復動作，以解決已識別的連線問題。

12. 按一下 **[安裝]**。

掃描區域網路

若要掃描區域網路來探索多個裝置

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 按一下 **[新增]**。
3. 在 **[多個裝置]** 中，按一下 **[探索裝置]**。

探索精靈便會開啟。

4. 按一下 **[掃描]**。

主動式裝置探索掃描隨即開始。系統會將您重新導向到 **[探索到的裝置]** > **[區域網路]** 畫面。掃描完成後，會顯示通知。此通知會顯示在掃描期間探索到的裝置數目，並包含裝置清單的連結，您可以在此清單中查看有關這些裝置的其他詳細資料。

後續步驟：

- 您可以按一下通知中的 **[檢視新探索到的裝置]** 連結，並在 **[區域網路]** 索引標籤上檢視裝置及其詳細資料。
- 您可以在探索到的裝置上，從遠端安裝保護代理程式，並註冊這些裝置。如需詳細資訊，請參閱 "從遠端安裝代理程式並註冊裝置" (第 170 頁)。
- 您可以從探索中排除裝置。如需詳細資訊，請參閱 "從探索中排除裝置" (第 171 頁)。

手動或透過匯入檔案

若要手動新增多個裝置或透過匯入檔案新增多個裝置

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 按一下 **[新增]**。

3. 在 **[多個裝置]** 中，按一下 **[探索裝置]**。
   探索精靈便會開啟。
4. 按一下 **[手動指定或從檔案匯入]**。
5. 使用下列其中一個選項新增電腦。
   - 若要手動新增電腦：
     a. 在 **[新增電腦]** 欄位中，輸入電腦的 IPv4 位址或主機名稱。
     b. 針對您要新增的每部電腦重複上一個步驟。
   - 若要透過匯入檔案新增電腦：
     a. 按一下 **[從檔案匯入電腦清單]**。
     b. 在 **[從檔案匯入電腦清單]** 視窗中，拖曳包含電腦清單的文字檔案，或按一下 **[瀏覽]**，導覽至檔案，選擇檔案，然後按一下 **[開啟]**。
     檔案必須包含 IP 位址或主機名稱，每行一個。以下是檔案內容的範例：

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

   手動新增電腦位址或從檔案匯入之後，代理程式將會嘗試 Ping 新增的電腦，並檢查其可用性。
6. 按 **[下一步]**。

起始電腦探索時，您將會在 **[監控]** > **[活動]** > **[探索基礎架構中的裝置]** 活動中找到對應的工作。

使用者帳戶控制 (UAC) 的需求

在執行 Windows 7 或更高版本且非 Active Directory 網域成員的機器上，集中管理作業（包括遠端安裝）要求停用 UAC 和 UAC 遠端限制。

若要停用 UAC

依據作業系統版本執行以下其中一項操作：

- **在 Windows 8 之前的 Windows 作業系統：**
  移至 **[控制面板]** > **[檢視方式:小圖示]** > **[使用者帳戶]** > **[變更使用者帳戶控制設定]**，然後將滑桿移至 **[永不通知]**。然後，重新啟動電腦。
- **在任何 Windows 作業系統中**：
  1. 開啟 [登錄編輯程式]。
  2. 找到以下登錄機碼：**HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**
  3. 將 **EnableLUA** 值的設定變更為 **0**。
  4. 重新啟動電腦。

若要停用 UAC 遠端限制

1. 開啟 [登錄編輯程式]。
2. 找到以下登錄機碼：**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. 將 **LocalAccountTokenFilterPolicy** 值的設定變更為 **1**。

   如果 **LocalAccountTokenFilterPolicy** 值不存在，請將其建立為 DWORD (32 位元)。如需有關此值的詳細資訊，請參閱 Microsoft 文件：https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows。

注意事項
基於安全性，建議在完成管理作業 (例如，遠端安裝) 之後，將兩個設定都還原到其原始狀態：**EnableLUA=1** 和 **LocalAccountTokenFilterPolicy** = **0**

選擇要安裝的元件

當您新增多個透過在 Active Directory 中搜尋而探索到的裝置時，您可以設定以下額外設定：

- 執行服務所使用的帳戶。
- 您要安裝的特定元件。
- 安裝後動作。

若要選擇要安裝的元件

1. 在 **[選擇元件]** 畫面上，請確認已啟用 **[在探索到的裝置上安裝保護代理程式]** 開關。
2. [選用] 若要變更執行服務將使用的帳戶：
   a. 在 **[設定]** 窗格的 **[服務登入帳戶]** 列中，按一下 **[變更]**。
   b. 選擇帳戶選項。

選項	描述
使用服務使用者帳戶(預設適用於代理程式服務)	服務使用者帳戶是用於執行服務的 Windows 系統帳戶。這種設定的優點在於，網域安全性原則不會影響此類帳戶的使用者權限。依預設，此代理程式在**本機系統**帳戶下執行。
建立新帳戶	代理程式的帳戶名稱將是 Agent User。 請確認網域安全性原則不會影響相關帳戶的權限。如果帳戶在安裝期間獲指派的使用者權限遭到剝奪，則元件可能無法正常運作或根本無法運作。
使用下列帳戶	如果您將代理程式安裝在網域控制站上，則系統會提示您為代理程式指定現有的帳戶 (或相同帳戶)。基於安全理由，系統不會在網域控制站上自動建立新帳戶。 請確認網域安全性原則不會影響相關帳戶的權限。如果帳戶在安裝期間獲指派的使用者權限遭到剝奪，則元件可能無法正常運作或根本無法運作。

   c. [如果選擇 **[使用下列帳戶]**] 請輸入使用者名稱和密碼。
   d. 按一下 **[儲存]**。
3. [選用] 選擇安裝後動作

選項	描述
必要時重新啟動裝置	如果選擇此選項，電腦將根據需要重新啟動的次數重新啟動以完成安裝。 在下列其中一種情況下，可能需要重新啟動電腦： • 必要條件安裝完成，若要繼續安裝，需要重新啟動電腦。 • 安裝完成，但需要重新啟動，因為部分檔案在安裝期間遭到鎖定。 • 安裝完成，但需要為之前安裝的其他軟體重新啟動。
如果有使用者已登入，請不要重新啟動裝置	選擇 **[必要時重新啟動裝置]** 時，此選項會變成可編輯。 如果選擇此選項，當使用者登入系統時，電腦將不會自動重新啟動。例如，如果使用者在安裝需要重新啟動時正在工作，則系統將不會重新啟動。 如果已安裝必要條件，但電腦因為使用者登入而未重新啟動，則若要完成安裝，您必須重新啟動電腦，然後再次開始安裝。 如果已安裝代理程式但電腦未重新啟動，則必須重新啟動電腦。

4. 在 **[安裝 Windows 的其他元件]** 窗格中，按一下箭頭圖示。
5. 選擇您要安裝的元件。

元件	描述
必要元件	
Windows 用代理程式	此代理程式會備份磁碟、磁碟區和檔案，而且將會安裝在 Windows 電腦上。您一律得安裝，無法選擇。
其他元件	
資料洩漏防禦用代理程式	此代理程式可讓您在保護計劃下的電腦上，限制使用者對本機和重新導向的週邊裝置、連接埠以及剪貼簿的存取。如果選擇，則要安裝。
反惡意程式碼和 URL 篩選	此元件可在保護計劃中啟用 [防毒和防惡意程式保護] 模組和 [URL 篩選] 模組。即使您選擇不安裝，如果在電腦的保護計劃中啟用以上任何模組，之後還是會自動安裝。
Hyper-V 用代理程式	此代理程式會備份 Hyper-V 虛擬機器，而且將會安裝在 Hyper-V 主機上。如果選擇並在電腦上偵測到 Hyper-V 角色，則要安裝。
SQL 用代理程式	此代理程式會備份 SQL Server 資料庫，而且將會安裝在執行 Microsoft SQL Server 的電腦上。如果選擇並在電腦上偵測到應用程式，則要安裝。
Exchange 用代理程式	此代理程式會備份 Exchange 資料庫和信箱，而且將會安裝在執行 Microsoft Exchange Server 信箱角色的電腦上。如果選擇並在電腦上偵測到應用程式，則要安裝。
Active Directory 用代理程式	此代理程式會備份 Active Directory 網域服務的資料，而且將會安裝在網域控制站上。如果選擇並在電腦上偵測到應用程式，則要安裝。
VMware 用代	此代理程式會備份 VMware 虛擬機器，而且將會安裝在可透過網路存取 vCenter

理程式 (Windows)	Server 的 Windows 電腦上。如果選擇，則要安裝。
Microsoft 365 用代理程式	此代理程式會將 Microsoft 365 信箱備份到本機目的地，而且將會安裝在 Windows 電腦上。如果選擇，則要安裝。
適用於 Oracle 的代理程式	此代理程式會備份 Oracle 資料庫，而且將會安裝在執行 Oracle Database 的電腦上。如果選擇，則要安裝。
Cyber Protection Monitor	此元件可讓使用者監視通知區內執行中工作的執行，而且將會安裝在 Windows 電腦上。如果選擇，則要安裝。 支援 Windows 7 Service Pack 1 和更新版本，以及 Windows Server 2008 R2 Service Pack 1 和更新版本。

6. 按一下 **[選擇]**。

   [選擇元件] 畫面會關閉，而且您會返回 **[探索後動作]** 畫面/索引標籤。

使用 Device Sense™ 進行裝置探索

Device Sense™ 使用複雜的技術組合掃描組織的區域網路，以探索並識別裝置。除了探索實體和虛擬機器以及平板電腦外，Device Sense™ 也可以探索其他網路裝置，例如路由器、交換器、印表機、智慧型手機和 IP 攝影機。

使用 Device Sense™ 可實現：

- 全面的網路能見度 - 識別連線至客戶網路的每個裝置。
  這有助於您維持準確的資產清查，並有效管理和支援 IT 基礎架構，這對於資產追蹤和生命週期管理至關重要，而且可確保符合授權合約。
- 安全性與合規性 - 偵測可能構成安全風險的未經授權或惡意裝置。Device Sense™ 可協助您確保網路中的每個裝置符合安全性原則和法規要求。
- 資源的有效配置 - 瞭解客戶網路的範圍和規模，因此可以更有效地配置資源並達到更佳的服務規劃。

使用 Device Sense™ 進行裝置探索包含下列功能：

- 自動智慧選擇要掃描的探索代理程式和網路
- 防止在家用或非公司網路中探索裝置

注意事項

使用 Device Sense™ 進行被動式探索時，將不會掃描代理程式數量少於在 **[防止在非公司網路中探索裝置]** 設定中指定之數量的網路。在資料中心層級上，此設定的預先設定值為 3，但此值會由上限值租用戶繼承，且可能不同。為確保被動式探索掃描所有公司網路，您可以更新適用於組織的設定。如需詳細資訊，請參閱 "設定被動式裝置探索" (第 164 頁)。

- 隨需主動式裝置探索
- 裝置分類 (依類型)
- 用於瀏覽探索到的裝置的進階搜尋和篩選選項

- 探索到的裝置的全方位詳細資料
- 在探索到的裝置上遠端安裝保護代理程式，並套用不同的計劃類型
- 有關探索到的裝置的詳細報告

您可以使用 Device Sense ™ 執行被動式裝置探索掃描或主動式裝置探索掃描。如需詳細資訊，請參閱 "使用 Device Sense ™ 進行被動式裝置探索" (第 164 頁) 和 "使用 Device Sense ™ 進行主動式裝置探索" (第 165 頁)。

注意事項
資料庫中有關探索到的裝置的資訊的保留期為 3 個月。

使用 Device Sense ™ 進行被動式裝置探索

被動式裝置探索是一種非侵入式方法，可用來識別並編目網路環境中的裝置，而無需主動探查或將要求傳送至組織網路中的這些裝置。

被動裝置探索會收集下列裝置資料：

- 裝置名稱
- 裝置類型
- 作業系統系列
- 廠商
- 模組
- MAC 位址
- IP 位址

被動式探索的設定是在資料中心層級預先設定的。公司系統管理員可以針對公司或單位中的所有裝置，自訂這些設定。如果未套用任何自訂設定，則會以下列順序，使用更上層的設定：

1. Cyber Protection 資料中心
2. 公司 (客戶租用戶)
3. 單位

例如，單位系統管理員可以針對單位，設定自訂的裝置探索設定，這可能與在公司層級套用的設定不同。

設定被動式裝置探索

被動式裝置探索會持續掃描公司網路中的裝置。使用被動式裝置探索：

- 合作夥伴可以瞭解客戶的網路以及這些網路中可用的裝置數目和類型。
- 客戶可以瞭解其組織的網路，以及這些網路中可用的裝置數目和類型。

若要設定被動式裝置探索設定

1. 在 Cyber Protect 主控台中，前往 **[設定]** > **[保護]**。
2. 按一下 **[被動式裝置探索]** 索引標籤。
3. 請確認已啟用 **[啟用被動式裝置探索]** 開關。

系統會自動指派 Windows 代理程式作為探索代理程式。

4. [選用] 變更預設設定。

設定	描述
自動智慧選擇探索代理程式	將自動選擇以便在區域網路中執行被動式裝置探索的代理程式數目。預設值為 1。* 最大值為 3。
防止在非公司網路中探索裝置	必須在網路中存在的代理程式數目下限，以將其分類為公司環境並啟用其掃描。預設值為 3。* 最大值為 10。
增強識別網路中的裝置	啟用或停用多點傳送訊號，以便更精確地識別加入區域網路的裝置類型。預設會停用此開關。*

* 預設值可能會有所不同，這取決於上層租用戶的設定。預設值是繼承的，且與針對上層租用戶設定的值相同。不過，您可以根據組織的需求，變更預設值。

5. 按一下 **[儲存]**。

使用 Device Sense™ 進行主動式裝置探索

主動式裝置探索是網路管理中使用的一種方法，系統會主動探查網路上的裝置或與其進行通訊，以識別並收集有關這些裝置的資訊。

您可以在網路中擷取有關裝置的完整準確資料，從而確保所有裝置資訊都清楚可見。

主動裝置探索會收集下列裝置資料：

- 裝置名稱
- 裝置類型
- 廠商
- 模組
- IP 位址
- MAC 位址

使用 Device Sense™ 執行主動式裝置探索掃描

您可以執行主動式掃描，以便全面收集資料並識別連線至區域網路的裝置。

若要執行主動式掃描

1. 在 保護 主控台中，移至 **[裝置]** > **[探索到的裝置]**。
2. 按一下 **[區域網路]** 索引標籤。
3. 按一下 **[執行主動式掃描]**。
4. 選擇要執行主動式掃描的網路，然後按一下 **[執行]**。
5. 在 **[租用戶]** 欄位中，選擇租用戶。
6. 在 **[探索代理程式]** 欄位中，選擇在租用戶中註冊的工作負載。系統將使用安裝在此工作負載上的保護代理程式作為探索代理程式。
7. 按一下 **[執行]**。

開始主動式裝置探索掃描。掃描完成後，會顯示通知。此通知會顯示在掃描期間探索到的裝置數目，並包含裝置清單的連結，您可以在此清單中查看有關這些裝置的其他詳細資料。

注意事項
您無法同時執行多個主動式掃描。如果正在進行主動式掃描，您必須取消該掃描或等待其完成，然後才能開始新的掃描。

檢視探索到的裝置的相關資訊

您可以使用合併到 **[探索到的裝置]** 頁面上的篩選條件，以快速在清單中尋找特定裝置並檢視其詳細資料。

若要尋找探索到的裝置並檢視其詳細資料

1. 在 保護 主控台中，按一下 **[探索到的裝置]**。
   預設會開啟 **[無代理程式的裝置]** 索引標籤。
2. [選用] 若要從特定類別搜尋裝置，請按一下對應的索引標籤。

索引標籤	描述
無代理程式的裝置	此索引標籤會列出所有探索到的電腦，無論使用何種探索方法進行探索，都可以在這些電腦上安裝保護代理程式。
Active Directory	此索引標籤會列出透過掃描 Active Directory 探索到的電腦。
區域網路	此索引標籤會列出透過使用 Device Sense ™ 掃描公司區域網路而探索到的裝置 (電腦或其他網路裝置)。
手動/從文字檔案匯入	此索引標籤會列出手動或從文字檔案中探索到的電腦。
排除	此索引標籤會列出已從探索中排除的裝置。

3. [選用] 若要依裝置名稱搜尋，請在 **[搜尋]** 欄位中輸入裝置名稱。
   清單中的結果會經過動態篩選。
4. [選用] 若要使用篩選條件搜尋結果，請按一下 **[篩選]**，選擇一或多個篩選條件，然後按一下 **[套用]**。

篩選器	描述
裝置類型	若要搜尋一個或多個裝置類型，請按一下欄位，然後從清單中選擇相關的裝置類型。 此篩選條件不適用於 **[手動/從文字檔案匯入]** 索引標籤。
探索類型	若要依據探索方法篩選結果，請按一下欄位，然後從下列方法中選擇。 • **Active Directory** • **手動** • **區域網路 (被動式)**

篩選器	描述
	• **區域網路 (主動式)** 此篩選條件僅適用於 **[無代理程式的裝置]** 索引標籤。
MAC 位址	若要搜尋具有特定 MAC 位址的裝置，請在此欄位中輸入 MAC 位址。 此篩選條件不適用於 **[手動/從文字檔案匯入]** 索引標籤。
IP 位址範圍	若要依據裝置 IP 位址篩選結果，請在第一個欄位輸入起始 IP 位址，並在第二個欄位輸入結束 IP 位址。
首次探索到的時間	若要依據初始探索到裝置的日期篩選結果，請按一下欄位，然後使用預先定義或自訂的範圍。
上次探索時間	若要依據上次探索到裝置的日期篩選結果，請按一下欄位，然後使用預先定義或自訂的範圍。
組織單位	裝置所屬 Active Directory 的組織單位。 此篩選條件僅適用於 **[Active Directory]** 索引標籤。

5. 按一下裝置，然後按一下 **[詳細資料]**。
6. 在 **[原始資料]** 窗格中，按一下箭頭圖示。
7. 若要下載 JSON 檔案中的原始資料，請按一下 **[下載]**。
   檔案隨即儲存在您從中登入 保護 主控台的電腦上的預設下載目錄中。

代理程式之遠端安裝

裝置探索程序完成後，您可以在探索到的 Windows 裝置上遠端安裝代理程式。

遠端安裝代理程式的方式如下：

1. 探索代理程式會使用探索精靈中指定的主機名稱、IP 位址和系統管理員認證來連線到目標電腦，然後將 `web_installer.exe` 檔案上傳到那些電腦上。
2. `web_installer.exe` 檔案會以自動模式在目標電腦上執行。
3. Web 安裝程式會從雲端擷取其他套件，然後透過 `msiexec` 命令將其安裝到目標電腦上。
4. 在安裝完成之後，將在雲端註冊元件。

注意事項
由於代理程式服務需要其他權限才能執行，因此網域控制站不支援遠端安裝代理程式。

準備電腦以進行遠端手動安裝

- 若要在執行 Windows 7 或更高版本的遠端電腦上成功安裝，必須在該電腦上停用 **[控制台]** > **[資料夾選項]** > **[檢視]** > **[使用共用精靈]**。
- 若要在*非* Active Directory 網域成員的遠端電腦上成功安裝，必須在該電腦上*停用*使用者帳戶控制 (UAC)。如需有關停用方式的詳細資訊，請參閱「使用者帳戶控制 (UAC) 的需求」>「若要停用 UAC」。

- 根據預設，您需要有內建系統管理員帳戶的認證，才能在任何 Windows 電腦上進行遠端安裝。若要使用其他系統管理員帳戶的認證執行遠端安裝，必須*停用*使用者帳戶控制 (UAC) 遠端限制。如需有關停用方式的詳細資訊，請參閱「使用者帳戶控制 (UAC) 的需求」>「若要停用 UAC 遠端限制」。
- 遠端電腦上的檔案及印表機共用必須為*[啟用]*。若要存取此選項：
  - 在執行 Windows 2003 Server 的電腦上：移至 **[控制台]** > **[Windows 防火牆]** > **[例外]** > **[檔案及印表機共用]**。
  - 在執行 Windows Server 2008、Windows 7 或更新版本的電腦上：移至 **[控制台]** > **[Windows 防火牆]** > **[網路和共用中心]** > **[變更進階共用設定]**。
- Cyber Protection 使用 TCP 連接埠 445、25001 和 43234 進行遠端安裝。

  當您啟用 [檔案及印表機共用] 時，會自動開放連接埠 445。連接埠 43234 和 25001 會透過 Windows 防火牆自動開啟。如果您使用不同的防火牆，請確定這三個連接埠都已開啟 (新增至例外)，以便讓內送和外送要求通過。

  遠端安裝完成之後，連接埠 25001 會透過 Windows 防火牆自動關閉。若您想要在未來遠端更新代理程式，則必須將連接埠 445 和 43234 保留為開啟狀態。在每次更新期間，會透過 Windows 防火牆自動開放和關閉連接埠 25001。若使用不同的防火牆，則所有三個連接埠均將保留為開啟狀態。

使用 GPO 準備電腦以進行遠端安裝

您可以設定並套用 Active Directory 群組原則物件 (GPO) 以準備 Active Directory 成員的一組電腦，以便遠端安裝 保護 代理程式。

必要條件

- 您的使用者是 [網域系統管理員] 群組的成員或網域系統管理員。
- **群組原則管理主控台** (GPMC) 已安裝在您登入以建立 GPO 的電腦上。

若要使用 GPO 準備電腦以進行遠端安裝

1. 若要開啟 GPMC，請按下 **Win** + **R**，輸入 `gpmc.msc`，然後按下 **Enter**。
2. 在主控台樹狀目錄中，以滑鼠右鍵按一下您要套用 GPO 的網域或組織單位 (OU)。
3. 按一下 **[在此網域中建立 GPO，並將其連結至此...]**。
4. 在 **[新 GPO]** 快顯視窗中，輸入 GPO 的名稱，然後按一下 **[確定]**。
5. 在主控台樹狀目錄中，以滑鼠右鍵按一下您在上一個步驟中建立的 GPO，然後按一下 **[編輯...]**。
6. 依照下列步驟，停用 **[使用共用精靈]**。
   a. 在主控台樹狀目錄中，導覽至 **[使用者設定]** > **[喜好設定]** > **[Windows 設定]** > **[登錄]**。
   b. 以滑鼠右鍵按一下 **[登錄]**，然後按一下 **[新增]** > **[登錄項目]**。

c. 在 **[新增登錄內容]** 視窗的 **[一般]** 索引標籤上，設定登錄項目，如下所示。

參數	數值
動作	更新
Hive	HKEY_CURRENT_USER
機碼路徑	Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
值名稱	SharingWizardOn
值類型	REG_DWORD
數值資料	0

d. 按一下 **[套用]**，然後按一下 **[確定]**。

7. [適用於 Windows Vista 及更新版本] 依照下列步驟，停用使用者帳戶控制 (UAC)。
   a. 在主控台樹狀目錄中，導覽至 **[電腦設定]** > **[喜好設定]** > **[Windows 設定]** > **[登錄]**。
   b. 以滑鼠右鍵按一下 **[登錄]**，然後按一下 **[新增]** > **[登錄項目]**。
   c. 在 **[新增登錄內容]** 視窗的 **[一般]** 索引標籤上，設定登錄項目，如下所示。

參數	數值
動作	更新
Hive	HKEY_LOCAL_MACHINE
機碼路徑	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\
值名稱	EnableLUA
值類型	REG_DWORD
數值資料	0

   d. 按一下 **[套用]**，然後按一下 **[確定]**。

8. [適用於 Windows Vista 及更新版本] 依照下列步驟，停用使用者帳戶控制 (UAC) 遠端限制。
   a. 在主控台樹狀目錄中，導覽至 **[電腦設定]** > **[喜好設定]** > **[Windows 設定]** > **[登錄]**。
   b. 以滑鼠右鍵按一下 **[登錄]**，然後按一下 **[新增]** > **[登錄項目]**。

c. 在 **[新增登錄內容]** 視窗的 **[一般]** 索引標籤上，設定登錄項目，如下所示。

參數	數值
動作	更新
Hive	HKEY_LOCAL_MACHINE
機碼路徑	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
值名稱	LocalAccountTokenFilterPolicy
值類型	REG_DWORD
數值資料	1

d. 按一下 **[套用]**，然後按一下 **[確定]**。

9. 依照以下步驟，啟用 **[檔案及印表機共用]**。
   a. 在主控台樹狀目錄中，導覽至 **[電腦設定]** > **[原則]** > **[Windows 設定]** > **[安全性設定]** > **[Windows Defender 防火牆與進階安全性]** > **[輸入規則]**。
   b. 以滑鼠右鍵按一下 **[輸入規則]**，然後按一下 **[新增規則]**。
   c. 在 **[新增輸入規則精靈]** 中，設定規則如下。
   d. 在 **[規則類型]** 索引標籤上，選擇 **[預先定義]**，選擇 **[檔案及印表機共用]**，然後按一下 **[下一步]**。
   e. 在 **[預先定義的規則]** 索引標籤上，按一下 **[下一步]**。
   f. 在 **[動作]** 索引標籤上，選擇 **[允許連線]**，然後按一下 **[完成]**。
   g. 在主控台樹狀目錄中，導覽至 **[電腦設定]** > **[原則]** > **[Windows 設定]** > **[安全性設定]** > **[Windows Defender 防火牆與進階安全性]** > **[輸出規則]**。
   h. 以滑鼠右鍵按一下 **[輸出規則]**，然後選擇 **[新增規則]**。
   i. 在 **[新增輸出規則精靈]** 中，執行與步驟 d - f 相同的動作來設定規則。
10. 依照以下步驟，將 GPO 連結至網域或 OU。
    a. 在主控台樹狀目錄中，以滑鼠右鍵按一下目標網域或 OU，然後按一下 **[連結現有的 GPO...]**。
    b. 在 **[選擇 GPO]** 畫面上，選擇您建立的 GPO，然後按一下 **[確定]**。
11. 依照以下步驟，在您要準備進行遠端代理程式安裝的目標電腦上，強制執行群組原則更新。
    a. 以系統管理員身分執行 **[命令提示字元]**。
    b. 執行下列命令：

    ```
    gpupdate /force
    ```

從遠端安裝代理程式並註冊裝置

注意事項

只有 Windows 裝置支援從遠端安裝代理程式。

在多個裝置上安裝代理程式僅適用於位於相同網路且透過相同探索方法探索到的裝置。

若要從遠端安裝代理程式

1. 在 保護 主控台中，前往 **[裝置]** > **[無代理程式的裝置]**。
2. 選擇裝置。
3. 按一下 **[安裝並登錄]**。
4. 在 **[探索後動作]** 索引標籤上，選擇租用戶帳戶。
5. 在 **[探索代理程式]** 欄位中，選擇將用於遠端安裝代理程式和註冊電腦的工作負載。

   注意事項
   探索代理程式是安裝有保護代理程式所在的工作負載。
   探索代理程式必須是 Active Directory 網域的成員。
   您可以選擇與所選單位或其子單位相關聯的代理程式。

6. 選擇要在電腦上執行的動作。

選項	描述
安裝代理程式並登錄電腦	您可以按一下 **[選擇元件]**，選擇要在電腦上安裝的元件。如需詳細資訊，請參閱 "選擇要安裝的元件" (第 161 頁)。
使用已安裝的代理程式登錄電腦	如果電腦上已經安裝代理程式，而且您只需將其登錄到 Cyber Protection，請使用此選項。如果在電腦上找不到代理程式，則將會新增到 **[無代理程式的裝置]** 清單。

7. 選擇您登錄電腦所要使用的使用者帳戶。
8. [選用] 若要選擇將自動套用至電腦的計劃，請在 **[登錄後的動作]** 區段中，對應計劃類型的計劃選擇欄位內，按一下 **[變更]**，選擇計劃，然後再按一下 **[變更]**。
9. 按 **[下一步]**。
10. 在 **[認證]** 索引標籤上，執行下列動作：
    a. 按一下 **[新增認證]**。
    b. 選擇認證，選擇對所選裝置具有系統管理員權限的使用者的認證，然後按一下 **[選擇認證]**。

       重要事項
       只有在您指定內建系統管理員帳戶 (安裝作業系統時建立的第一個帳戶) 的認證後，才能在不做任何準備的情況下，從遠端安裝代理程式。如果您要定義自訂系統管理員認證，則必須手動做一些額外的準備，如需詳細資訊，請參閱 "準備電腦以進行遠端手動安裝" (第 167 頁)。

    c. 按 **[下一步]**。
       系統會對所選裝置進行初步檢查，以確認這些裝置適用且具有用於遠端安裝代理程式和所選元件的正確設定。
11. [如果有連線問題] 請執行對應的修復動作，以解決已識別的連線問題。
12. 按一下 **[安裝]**。

從探索中排除裝置

如果您從探索中排除裝置，執行裝置探索掃描時，這些裝置將不會列在探索到的裝置結果中。

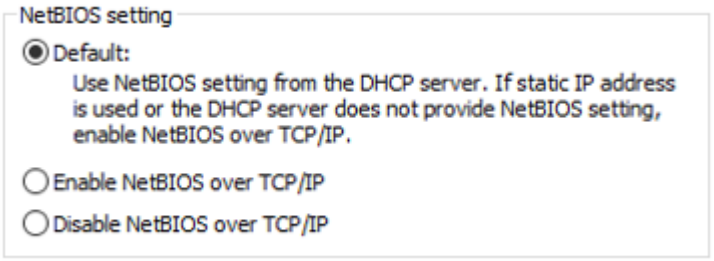
若要從探索中排除裝置

1. 在 保護 主控台中，移至 **[裝置]**。
2. 按一下要從探索中排除的裝置，然後按一下 **[從探索中排除]**。
   該裝置隨即從探索中排除，並新增至 **[排除項目]** 頁面上的裝置清單中。

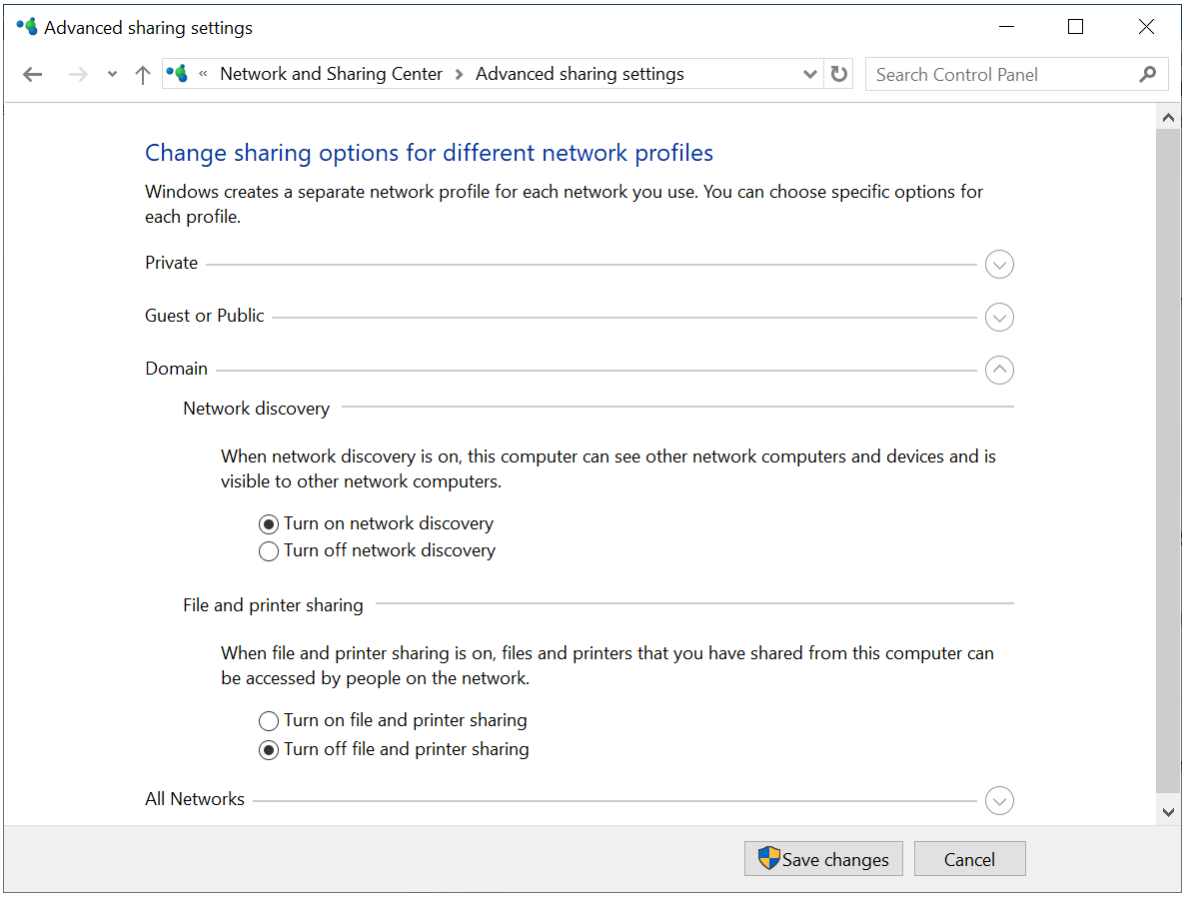
疑難排解裝置探索

如果您對裝置探索功能有任何問題，請嘗試檢查下列項目：

- 檢查是透過 TCP/IP 啟用 NetBIOS 還是設為預設值。



- 在 [控制台\網路和共用中心\進階共用設定] 中，開啟 [網路探索]。



- 檢查功能探索提供者裝載服務是否正在執行探索的電腦以及要探索的電腦上執行。
- 檢查功能探索資源發佈服務是否正在要探索的電腦上執行。

防止未經授權者解除安裝或修改代理程式

您可以在保護計劃中啟用 **[密碼保護]** 設定，以保護 Windows 用代理程式，免於未經授權者解除安裝或修改。此設定僅適用於啟用 **[自我保護]** 設定時。

若要啟用密碼保護

1. 在保護計劃中，展開 **[防毒和反惡意程式碼保護]** 模組 (適用於 Cyber Backup 版本的 **Active Protection** 模組)。
2. 按一下 **[自我保護]** 並確認已啟用 **[自我保護]** 開關。
3. 啟用 **[密碼保護]** 開關。
4. 在開啟的視窗中，複製您需要解除安裝或修改受保護之 Windows 用代理程式元件的密碼。
   此密碼是唯一的，而且您關閉此視窗之後，將無法復原該密碼。如果您遺失或忘記此密碼，可以編輯保護計劃並建立新的密碼。
5. 按一下**[關閉]**。
6. 在 **[自我保護]** 窗格中，按一下 **[完成]**。
7. 儲存保護計劃。

系統將會為套用此保護計劃的電腦啟用密碼保護。密碼保護僅適用於 Windows 用代理程式 *15.0.25851* 版或更新版本。電腦必須在線上。

您可以將已啟用 [密碼保護] 的保護計劃套用到執行 macOS 的電腦，但不會提供任何保護。您無法將這種計劃套用到執行 Linux 的電腦。

此外，您無法將已啟用 [密碼保護] 的多個保護計劃套用到相同的 Windows 電腦。若要瞭解如何解決可能的衝突，請參閱解決計劃衝突。

若要在現有的保護計劃中變更密碼

1. 在保護計劃中，展開 **[防毒和反惡意程式碼保護]** 模組 (適用於 Cyber Backup 版本的 **Active Protection** 模組)。
2. 按一下 **[自我保護]**。
3. 按一下 **[建立新密碼]**。
4. 在開啟的視窗中，複製您需要解除安裝或修改受保護之 Windows 用代理程式元件的密碼。
   此密碼是唯一的，而且您關閉此視窗之後，將無法復原該密碼。如果您遺失或忘記此密碼，可以編輯保護計劃並建立新的密碼。
5. 按一下**[關閉]**。
6. 在 **[自我保護]** 窗格中，按一下 **[完成]**。
7. 儲存保護計劃。

變更電腦的服務配額

保護計劃第一次套用到電腦時，便會自動指派服務配額。

系統會根據受保護電腦的類型、其作業系統、所需的保護層級，以及配額可用性，指派最適當的配額。如果貴組織無法使用最適當的配額，則會指派次佳配額。例如，如果最適當的配額為 **Web 託管伺服器**但無法使用，則會指派**伺服器**配額。

配額指派的範例：

- 執行 Windows Server 或 Linux Server 作業系統 (例如 Ubuntu Server) 的實體機器會獲指派**伺服器**配額。
- 執行 Windows 或 Linux Desktop 作業系統 (例如 Ubuntu Desktop) 的實體機器會獲指派**工作站**配額。
- 執行已啟用 Hyper-V 角色之 Windows 10 的實體機器會獲指派**工作站**配額。
- 在虛擬桌面基礎架構上執行且客體作業系統內部安裝其保護代理程式 (例如，Windows 用代理程式) 的桌上型電腦會獲指派**虛擬機器**配額。如果無法使用**虛擬機器**配額，此類型的電腦也可以使用**工作站**配額。
- 在虛擬桌面基礎架構上執行且在無代理程式模式 (例如，VMware 用代理程式或 Hyper-V 用代理程式) 下備份的桌上型電腦會獲指派**虛擬機器**配額。
- Hyper-V 或 vSphere 伺服器會獲指派**伺服器**配額。
- 具有 cPanel 或 Plesk 的伺服器會獲指派 **Web 託管伺服器**配額。根據網頁伺服器執行所在電腦的類型，如果無法使用 Web 託管伺服器配額，也可以使用**虛擬機器**或**伺服器**配額。
- 即使是針對工作站，應用程式感知備份也需要使用**伺服器**配額。

您之後可以手動變更原始指派。例如，若要將更進階的保護計劃套用到相同的電腦，您可能需要升級電腦的服務配額。如果目前指派的服務配額不支援此保護計劃所需的功能，保護計劃將會失敗。

或者，如果您在指派原始配額之後購買更多合適的配額，則可以變更服務配額。例如，**工作站**配額會被指派給虛擬機器。在您購買**虛擬機器**配額之後，可以手動將其指派給此機器，而不是指派原始的**工作站**配額。

您也可以釋出目前指派的服務配額，然後將此配額指派給其他機器。

您可以變更個別機器的服務配額，或一組機器的服務配額。

若要變更個別機器的服務配額

1. 在 Cyber Protect 主控台中，移至 **[裝置]**。
2. 選擇所需的電腦，然後按一下 **[詳細資料]**。
3. 在 **[服務配額]** 區段中，按一下 **[變更]**。
4. 在 **[變更配額]** 視窗中，選擇所需的服務配額或 **[無配額]**，然後按一下 **[變更]**。

若要變更一組機器的服務配額

1. 在 Cyber Protect 主控台中，移至 **[裝置]**。
2. 選擇多部機器，然後按一下 **[指派配額]**。
3. 在 **[變更配額]** 視窗中，選擇所需的服務配額或 **[無配額]**，然後按一下 **[變更]**。

保護設定

若要設定 Cyber Protection 的一般保護設定，請移至 Cyber Protect 主控台中的 **[設定]** > **[保護]**。

元件自動更新

根據預設，所有代理程式都可以連線至網際網路，並下載更新。

系統管理員可以在環境中選擇一或數個代理程式，並為其指派 [更新者] 角色，以便將網路頻寬流量降至最低。因此，專用的代理程式將會連線至網際網路，並下載更新。其他所有代理程式將會使用對等技術連線至專用的更新程式代理程式，然後從中下載更新。

如果環境中沒有專用的更新程式代理程式，或者無法在大約五分鐘內建立與專用更新程式代理程式的連線，則沒有 [更新者] 角色的代理程式將會連限制網際網路。

更新者代理程式會散佈 [防毒和防惡意軟體防護]、[弱點評估] 和 [修補程式管理] 的更新和修補程式，但不包含代理程式版本的更新。

注意事項
具有更新者角色的代理程式僅能為 Windows 協力廠商產品下載並散佈修補程式。對於 Microsoft 產品，更新者代理程式不支援散佈修補程式。

將 [更新者] 角色指派給代理程式之前，請確認執行代理程式所在電腦的功能夠強大，而且具備穩定的高速網際網路連線以及足夠的磁碟空間。

準備 [更新者] 角色的電腦

1. 在您打算啟用 [更新者] 角色的代理程式電腦上，套用下列防火牆規則：
   - 輸入 (傳入) "updater_incoming_tcp_ports"：允許連線到所有防火牆設定檔 (公用、私人和網域) 的 TCP 連接埠 18018 和 6888。
   - 輸入 (傳入) "updater_incoming_udp_ports"：允許連線到所有防火牆設定檔 (公用、私人和網域) 的 UDP 連接埠 6888。
2. 重新啟動 Acronis Agent Core Service。
3. 重新啟動防火牆服務。

如果您沒有套用這些規則而且已啟用防火牆，則對等代理程式會從雲端下載更新。

將 [更新者] 角色指派給保護代理程式

1. 在 Cyber Protect 主控台中，移至 **[設定]** > **[代理程式]**。
2. 選擇您要將 [更新者] 角色指派給裝有代理程式的哪部電腦。
3. 按一下 **[詳細資料]**，然後啟用 **[使用此代理程式下載並散佈修補程式和更新]** 開關。

對等更新運作方式如下。

1. 擁有 [更新者] 角色的代理程式依排程，檢查服務提供者所提供的索引檔，以更新核心元件。
2. 擁有 [更新者] 角色的代理程式開始下載更新，並將其散佈至所有代理程式。

您可以將 [更新者] 角色指派給環境中的多個代理程式。因此，如果擁有 [更新者] 角色的代理程式離線，擁有此角色的其他代理程式可以當作定義更新的來源。

依排程更新 Cyber Protection 定義

在 **[排程]** 索引標籤上，您可以設定排程，以自動更新下列每個元件的 Cyber Protection 定義：

- 反惡意程式碼
- 弱點評估
- 修補程式管理

若要變更定義更新設定，請瀏覽至 **[設定]** > **[保護]** > **[保護定義更新]** > **[排程]**。

排程類型：

- **每天** – 定義在一週的哪幾天更新定義。
  開始時間 – 選擇在哪個時間更新定義。
- **每小時** – 定義更細微的每小時排程，以進行更新。
  執行週期 – 定義更新的週期。
  從 ...到 – 定義特定的時間範圍，以進行更新。

視需要更新 Cyber Protection 定義

若要視需要更新特定電腦的 Cyber Protection 定義

1. 在 Cyber Protect 主控台中，移至 **[設定]** > **[代理程式]**。
2. 選擇您要更新保護定義所在的電腦，然後按一下 **[更新定義]**。

快取儲存空間

快取資料的位置如下：

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

若要變更快取儲存設定，請瀏覽至 **[設定]** > **[保護]** > **[保護定義更新]** > **[快取儲存]**。

在 **[過期的更新檔案和修補程式管理資料]** 中，指定在哪個期限後移除快取資料。

代理程式的最大快取儲存空間大小 (GB)：

- **更新者角色** – 定義快取在具有 [更新者] 角色的電腦上的儲存空間大小。
- **其他角色** – 定義快取在其他電腦上的儲存空間大小。

注意事項
Cyber Protection 會收集偵測到的惡意軟體的範例進行額外分析，讓我們可以改進我們的軟體。您可以隨時在 **[保護]** 索引標籤中變更此設定，只要停用 **[收集惡意軟體範例並將其上傳至 CPOC]** 切換開關即可。

安裝在您環境中的 Cyber Protection 服務

Cyber Protection 會安裝下列部分或所有服務，端視您所使用的 Cyber Protection 選項而定。

安裝在 Windows 中的服務

服務名稱	目的
Acronis Managed Machine Service	提供備份、復原、複寫、保留、驗證功能
Acronis Scheduler2 Service	針對特定活動執行排程工作
Acronis Active Protection Service	防禦勒索軟體
Acronis Cyber Protection Service	提供反惡意程式碼保護

安裝在 macOS 中的服務

服務的名稱與位置	目的
/Library/LaunchDaemons/com.acronis.aakore.plist	用於代理程式和管理元件間通訊的伺服器
/Library/LaunchDaemons/com.acronis.cyber-protect-service.plist	偵測惡意程式碼
/Library/LaunchDaemons/com.acronis.mms.plist	提供備份與復原功能
/Library/LaunchDaemons/com.acronis.schedule.plist	執行排程工作

儲存代理程式記錄檔

您可以將代理程式記錄檔儲存為 .zip 檔。如果因不明原因備份失敗，此檔案將協助技術支援人員找出問題所在。

預設情況下，記錄檔中的資訊會針對最近三天進行最佳化，但您可以變更此期間。

線上工作負載

若要收集代理程式記錄檔

1. 執行下列其中一項操作：
   - 在 **[裝置]** 下，選擇您要收集記錄檔的來源工作負載，然後按一下 **[活動]**。
   - 在 **[設定]** > **[代理程式]** 下，選擇您要收集記錄檔的來源工作負載，然後按一下 **[詳細資料]**。
2. [選用] 若要變更包含系統資訊的預設期間，按一下 **[收集系統資訊]** 按鈕旁的箭頭，然後選擇期間。
3. 按一下 **[收集系統資訊]**。
4. 如果 Web 瀏覽器出現提示，請指定要儲存檔案的位置。

離線工作負載和可開機媒體

若要收集代理程式記錄檔

- 請依照此知識庫文章中的步驟進行。

內部部署管理伺服器的授權管理

如需有關如何啟用內部部署管理伺服器或如何為其配置授權的詳細資訊，請參閱 Cyber Protect 使用指南中的「管理授權」一節。

使用計劃

瞭解計劃

注意事項
部分功能的可用性取決於為您的帳戶啟用的產品項目。

計劃是一組設定和規則，您可以將其套用在一個或多個工作負載上，以實現不同的目標，例如，備份工作負載、保護工作負載免受惡意軟體侵害、監控工作負載的效能等。

計劃由您可以啟用或停用的模組組成。每個模組都包含與特定功能相關的設定。

您建立的所有計劃都可以在 **[管理]** 索引標籤上看到。

計劃	描述
保護計劃	保護工作負載上的資料。 保護計劃由以下模組組成： • 備份 • "實作災難復原"(第 655 頁) • 防毒和反惡意程式碼保護 • Endpoint Detection and Response (EDR) • URL 篩選 • Windows Defender 防毒軟體 • Microsoft Security Essentials • 弱點評估 • 修補程式管理 • 資料保護圖 • 裝置控制 • Advanced Data Loss Prevention 如需有關保護計劃的詳細資訊，請參閱 "保護計劃和模組"(第 191 頁)。
遠端管理計劃	在託管工作負載上啟用遠端桌面和協助功能。有關更多信息，請參閱"遠端管理計劃"(第 905 頁)。
指令碼計劃	在多個工作負載上啟用指令碼執行、排程指令碼執行，以及其他指令碼設定的組態。如需詳細資訊，請參閱 "指令碼計劃"(第 343 頁)。
監控計劃	監控受管理工作負載的效能、硬體、軟體、系統和安全性參數。如需詳細資訊，請參閱 "監控計劃"(第 961 頁)。
雲端應用程式備份	透過在雲端執行的代理程式，備份在雲端執行的應用程式，並使用雲端儲存空間作為備份位置。如需詳細資訊，請參閱 "雲端應用程式的備份計劃"(第 211 頁)
備份掃描計劃	掃描備份中是否有惡意軟體 (包括勒索軟體)。

計劃	描述
VM 複寫	掃描備份中是否有惡意軟體 (包括勒索軟體)。如需詳細資訊，請參閱 "虛擬機器的複寫" (第 610 頁)。
驗證	驗證備份並確認備份中的資料是否可以復原。如需詳細資訊，請參閱 "驗證" (第 201 頁)。
清理	根據保留規則，刪除過期的備份。此計劃僅適用於代理程式和工作負載，不適用於雲端對雲端備份。如需詳細資訊，請參閱 "清理" (第 206 頁)。
轉換成 VM	此計劃僅適用於磁碟層級的備份。 檢查備份是否包含系統磁碟區以及啟動作業系統所需的所有資訊，讓產生的虛擬機器可以自行啟動。如需詳細資訊，請參閱 "轉換為虛擬機器" (第 207 頁)。
備份複寫	將備份複寫到另一個位置。如需詳細資訊，請參閱 "備份複寫" (第 198 頁)。

內建計劃

內建計劃是使用部分最常使用或最常建議的設定預先設定的計劃。內建計劃可用於開箱即用的選擇。您無法變更內建計劃，但您可以在將內建計劃套用到工作負載後編輯設定。

內建計劃可用於以下計劃類型：保護計劃、監控計劃和遠端管理計劃。

內建保護計劃

下表提供有關內建保護計劃的詳細資訊。

模組和設定	內建保護計劃		
	基本保護	**擴充保護**	**全面保護**
	將停機時間和資料洩漏降至最低、輕鬆復原、RPO 短且易於維護	**第二層級保護：業務連續性、主動緩解安全風險和合規性**	**第三層級保護：業務連續性、接近零的 RPO、主動緩解安全風險、資料外洩防禦與合規性**
備份	開啟	開啟	開啟
要備份的內容 要備份的項目	整部電腦	整部電腦	整部電腦
連續資料保護 (CDP)	停用	停用	Enabled
備份目標位置	雲端儲存	雲端儲存	雲端儲存
排程	每週一到	星期一到星期五凌晨 12:00	星期一到星期五凌晨 12:00

模組和設定	內建保護計劃		
	基本保護	**擴充保護**	**全面保護**
	將停機時間和資料洩漏降至最低、輕鬆復原、RPO 短且易於維護	**第二層級保護:業務連續性、主動緩解安全風險和合規性**	**第三層級保護:業務連續性、接近零的 RPO、主動緩解安全風險、資料外洩防禦與合規性**
	週五中午 12:00 另外啟用的選項和開始條件: • 如果電腦關閉,則在電腦啟動時執行遺漏的工作 • 從睡眠或休眠模式中喚醒,開始進行排程的備份 • 節省電池電力:不要在使用電池電力時開始 • 不要在使用計量付費連線時開始	另外啟用的選項和開始條件: • 如果電腦關閉,則在電腦啟動時執行遺漏的工作 • 從睡眠或休眠模式中喚醒,開始進行排程的備份 • 節省電池電力:不要在使用電池電力時開始 • 不要在使用計量付費連線時開始	另外啟用的選項和開始條件: • 如果電腦關閉,則在電腦啟動時執行遺漏的工作 • 從睡眠或休眠模式中喚醒,開始進行排程的備份 • 節省電池電力:不要在使用電池電力時開始 • 不要在使用計量付費連線時開始
備份配置	一律增量	一律增量	一律增量
保留備份的時間長度	保留所有備份 90 天	保留所有備份 90 天	保留所有備份 90 天

模組和設定	內建保護計劃		
	基本保護	**擴充保護**	**全面保護**
	將停機時間和資料洩漏降至最低、輕鬆復原、RPO 短且易於維護	**第二層級保護：業務連續性、主動緩解安全風險和合規性**	**第三層級保護：業務連續性、接近零的 RPO、主動緩解安全風險、資料外洩防禦與合規性**
備份選項	預設選項	預設選項，加上： • 效能和備份時窗 (綠色組)： CPU 優先順序：低 輸出速度：50%	預設選項，加上： • 效能和備份時窗 (綠色組)： CPU 優先順序：低 輸出速度：50%
EDR	關閉	關閉	開啟
防毒和防惡意程式保護	開啟	開啟	開啟
Active Protection	開啟	開啟	開啟
進階反惡意程式碼	開啟	開啟	開啟
網路資料夾保護	開啟	開啟	開啟
伺服器端保護	關閉	關閉	關閉
自我保護	開啟	開啟	開啟
加密採礦程序偵測	開啟	開啟	開啟
隔離	30 天後移除隔離的檔案	30 天後移除隔離的檔案	30 天後移除隔離的檔案
行為引擎	隔離	隔離	隔離
漏洞利用防禦	通知並停止程序	通知並停止程序	通知並停止程序
即時保護	隔離	隔離	隔離
排程掃描	快速掃描：隔離	快速掃描：隔離 星期日到星期六晚上 08:00	快速掃描：隔離 星期日到星期六晚上 08:00

模組和設定	內建保護計劃		
	基本保護	**擴充保護**	**全面保護**
	將停機時間和資料洩漏降至最低、輕鬆復原、RPO 短且易於維護	**第二層級保護：業務連續性、主動緩解安全風險和合規性**	**第三層級保護：業務連續性、接近零的 RPO、主動緩解安全風險、資料外洩防禦與合規性**
	星期日到星期六晚上 08:00 完整掃描：隔離 星期三和星期五晚上 09:00 另外啟用的選項和開始條件： 從睡眠或休眠模式中喚醒，開始進行排程的備份	完整掃描：隔離 星期三和星期五晚上 09:00 另外啟用的選項和開始條件： 從睡眠或休眠模式中喚醒，開始進行排程的備份	完整掃描：隔離 星期三和星期五晚上 09:00 另外啟用的選項和開始條件： 從睡眠或休眠模式中喚醒，開始進行排程的備份
排除	無	無	無
URL 篩選	關閉	開啟	開啟
惡意網站存取	封鎖	封鎖	封鎖
要篩選的類別	預設選項	預設選項	預設選項
排除	無	無	無
Microsoft Defender 防毒軟體	關閉	關閉	關閉
防火牆管理	關閉	開啟	開啟
Microsoft Security Essentials	關閉	關閉	關閉

模組和設定	內建保護計劃		
	基本保護	**擴充保護**	**全面保護**
	將停機時間和資料洩漏降至最低、輕鬆復原、RPO 短且易於維護	**第二層級保護：業務連續性、主動緩解安全風險和合規性**	**第三層級保護：業務連續性、接近零的 RPO、主動緩解安全風險、資料外洩防禦與合規性**
弱點評估	開啟	開啟	開啟
弱點評估範圍	Microsoft 產品、Windows 協力廠商產品、Apple 產品、macOS 協力廠商產品、掃描 Linux 套件	Microsoft 產品、Windows 協力廠商產品、Apple 產品、macOS 協力廠商產品、掃描 Linux 套件	Microsoft 產品、Windows 協力廠商產品、Apple 產品、macOS 協力廠商產品、掃描 Linux 套件
排程	僅限星期三和星期五上午 11:00	僅限星期三和星期五上午 11:00	僅限星期三和星期五上午 11:00
修補程式管理	開啟	開啟	開啟
Microsoft 產品	所有更新	所有更新	所有更新
Windows 協力廠商產品	所有更新	所有更新	所有更新
排程	僅限星期三和星期五中午 12:30	僅限星期三和星期五中午 12:30	僅限星期三和星期五中午 12:30
預先更新備份	開啟	開啟	開啟
資料保護圖	關閉	關閉	開啟
副檔名和例外規則	–	–	預設選項 (要偵測的 66 個副檔名)

模組和設定	內建保護計劃		
	基本保護	擴充保護	全面保護
	將停機時間和資料洩漏降至最低、輕鬆復原、RPO 短且易於維護	第二層級保護:業務連續性、主動緩解安全風險和合規性	第三層級保護:業務連續性、接近零的 RPO、主動緩解安全風險、資料外洩防禦與合規性
排程	–	–	星期一到星期五下午 03:40
裝置控制	關閉	關閉	關閉
存取設定	已允許:全部	已允許:全部	已允許:全部
裝置類型允許名單	允許 1 個 USB HID (滑鼠、鍵盤等)	允許 1 個 USB HID (滑鼠、鍵盤等)	允許 1 個 USB HID (滑鼠、鍵盤等)
USB 裝置允許名單	空	空	空
排除	無	無	無
資料洩漏防禦	關閉	關閉	關閉
模式	–	–	–
進階設定	–	–	–
災難復原	關閉	關閉	關閉

如需有關保護計劃的詳細資訊，請參閱 "保護計劃和模組" (第 191 頁)。

內建監控計劃

下表提供有關內建監控計劃的詳細資訊。

名稱	描述	已啟用的監視器
建議用於 Windows	監控 Windows 電腦的健全狀況和效能	此計劃中啟用了以下 13 個監視器: • 反惡意程式碼軟體狀態 • 自動執行功能狀態 • CPU 溫度 • CPU 使用量

名稱	描述	已啟用的監視器
		• 磁碟空間 • 磁碟傳輸速率 • 失敗的登入 • 防火牆狀態 • GPU 溫度 • 上次系統重新開機 • 記憶體使用量 • 網路使用 • Windows Update 狀態
建議用於 macOS	監控 macOS 電腦的健全狀況和效能	此計劃中啟用了以下 10 個監視器： • 反惡意程式碼軟體狀態 • CPU 溫度 • CPU 使用量 • 磁碟空間 • 磁碟傳輸速率 • 防火牆狀態 • GPU 溫度 • 上次系統重新開機 • 記憶體使用量 • 網路使用
建議用於伺服器	監控 Windows 伺服器的健全狀況和效能	此計劃中啟用了以下 20 個監視器： • 反惡意程式碼軟體狀態 • CPU 溫度，2 個監視器： 80 度，10 分鐘，警告 90 度，10 分鐘，嚴重 • CPU 使用率，3 個監視器： 低於 20%，10 分鐘，資訊 超過 80%，10分鐘，警告 超過 90%，10 分鐘，嚴重 • 磁碟空間，2 個顯示器： 低於 20%，30分鐘，警告 低於 10%，30 分鐘，嚴重 • 磁碟傳輸速率 • 登入失敗，3 個監視器： 5 次嘗試，1 小時，資訊 10 次嘗試，1 小時，警告 20 次嘗試，1 小時，嚴重 • 防火牆狀態 • 硬體變更

名稱	描述	已啟用的監視器
		• 已安裝的軟體 • 記憶體使用量，3 個監視器： 低於 20%，10 分鐘，資訊 超過 80%，10分鐘，警告 超過 90%，10 分鐘，嚴重 • 網路使用 • Windows Update 狀態

如需有關監控計劃的詳細資訊，請參閱 "監控計劃" (第 961 頁)。

內建遠端管理計劃

下表提供有關內建遠端管理計劃的詳細資訊。

名稱	描述	設定
基本遠端桌面	啟用遠端桌面和檔案傳輸功能	連線通訊協定 **允許透過 NEAR 連線**：開啟 NEAR 安全性設定 • **當使用者中斷與主控台工作階段的連線時，鎖定工作負載**：關閉 • **一次僅允許一個使用者使用 NEAR 連線，或進行檔案傳輸**：關閉 • **允許工作負載系統管理員連線到任何工作階段**：開啟 • **允許建立系統工作階段**：關閉 • **允許剪貼簿同步**：開啟 **允許透過 RDP 連線**：開啟 **允許透過 [Apple 畫面共用] 連線**：關閉 安全性設定 • **顯示工作負載是否從遠端控制**：開啟 • **要求使用者擷取工作負載螢幕擷取畫面的權限**：開啟 工作負載管理 • **檔案傳輸**：開啟 • **螢幕擷取畫面傳輸**：關閉 顯示設定 • **使用桌面重複資料刪除擷取桌面**：開啟 • **使用 OpenCL 加速**：開啟 • **使用硬體 H.264 編碼**：開啟 工具箱

名稱	描述	設定
		顯示上次登入的使用者：關閉

如需有關遠端管理計劃的詳細資訊，請參閱 "遠端管理計劃" (第 905 頁)。

預設計劃

預設計劃是預先選取的計劃，而且會在計劃清單和計劃選擇欄位中顯示為第一個。對於每個支援的計劃類型，每個租用戶一次只能有一個預設計劃。

您將會看到的計劃清單和預設計劃取決於您使用 保護 主控台所在的層級。

例如，如果您是在合作夥伴層級使用主控台，您將會看到在合作夥伴、客戶和單位層級建立的計劃，但預設計劃將是在合作夥伴層級設定為預設的計劃。如果您在客戶層級使用主控台，您將不會看到在合作夥伴層級建立的任何計劃，包括合作夥伴層級的預設計劃。同樣地，如果您在單位層級使用主控台，您將不會看到在合作夥伴或客戶層級建立的任何計劃，包括這些層級的預設計劃。

在您將另一個計劃設為預設之前，無法刪除預設計劃。

以下計劃類型支援預設計劃：保護計劃、監控計劃和遠端管理計劃。

將計劃設為預設

您可以將受支援計劃類型 (保護計劃、監控計劃或遠端管理計劃) 中的一種計劃設定為預設。

注意事項
此功能不適用於獲指派保護服務唯讀系統管理員角色的使用者。

保護計劃

必要條件

已至少為您的租用戶建立一個保護計劃。如需詳細資訊，請參閱 "建立保護計劃" (第 192 頁)。

若要將保護計劃設為預設

1. 在 **[保護計劃]** 畫面上，找出您要設為預設的計劃，然後按一下該計劃。
2. 按一下 **[設為預設]**。
3. 在確認視窗中，按一下 **[設定]**。
   在 **[保護計劃]** 畫面上，**[預設]** 標籤會出現在計劃名稱旁。

遠端管理計劃

必要條件

- 已為您的使用者帳戶啟用 2FA。
- 已至少為您的租用戶建立一個遠端管理計劃。如需詳細資訊，請參閱 "建立遠端管理計劃" (第 906 頁)。

若要將遠端管理計劃設為預設

1. 在 **[遠端管理計劃]** 畫面上，找出您要設為預設的計劃。
2. 在同一列中，按一下 **[更多動作]** 圖示。
3. 按一下 **[設為預設]**。
4. 在確認視窗中，按一下 **[設定]**。

   在 **[遠端管理計劃]** 畫面上，**[預設]** 標籤會出現在計劃名稱旁。

監控計劃

必要條件

- 已為您的使用者帳戶啟用 2FA。
- 已至少為您的租用戶建立一個監控計劃。如需詳細資訊，請參閱 "建立監控計劃" (第 961 頁)。

若要將監控計劃設為預設

1. 在 **[監控計劃]** 畫面上，找出您要設為預設的計劃。
2. 在同一列中，按一下 **[更多動作]** 圖示。
3. 按一下 **[設為預設]**。
4. 在確認視窗中，按一下 **[設定]**。

   在 **[監控計劃]** 畫面上，**[預設]** 標籤會出現在計劃名稱旁。

我的最愛計劃

我的最愛計劃會顯示在計劃清單的頂端，預設計劃後面。若要確保組織有許多計劃時，仍然可以看到並輕鬆找到某個計劃，您可以將計劃新增至我的最愛。

您將會看到的計劃清單和我的最愛計劃取決於您使用 保護 主控台所在的層級。

例如，如果您是在合作夥伴層級使用主控台，您將會看到在所有層級 (合作夥伴、客戶和單位) 建立的計劃，但我的最愛計劃將是在合作夥伴層級新增到我的最愛的計劃。如果您在客戶層級使用主控台，您將不會看到在合作夥伴層級建立的任何計劃，包括合作夥伴層級的我的最愛計劃。同樣地，如果您在單位層級使用主控台，您將不會看到在合作夥伴或客戶層級建立的任何計劃，包括這些層級的我的最愛計劃。

以下計劃類型支援我的最愛計劃：保護計劃、監控計劃和遠端管理計劃。

將計劃設為我的最愛

您可以為每個租用戶的每個受支援計劃類型 (保護計劃、監控計劃或遠端管理計劃) 設定最多 10 個我的最愛計劃。

注意事項
此功能不適用於獲指派保護服務唯讀系統管理員角色的使用者。

保護計劃

必要條件

已至少為您的租用戶建立一個保護計劃。如需詳細資訊，請參閱 "建立保護計劃" (第 192 頁)。

若要將保護計劃設為我的最愛

1. 在 **[保護計劃]** 畫面上，按一下您要設為我的最愛的計劃。
2. 按一下 **[設為我的最愛]**。
   在 **[保護計劃]** 畫面上，星形圖示會出現在計劃名稱旁。

遠端管理計劃

必要條件

- 已為您的使用者帳戶啟用 2FA。
- 已至少為您的租用戶建立一個遠端管理計劃。如需詳細資訊，請參閱 "建立監控計劃" (第 961 頁)。

若要將遠端管理計劃設為我的最愛

1. 在 **[遠端管理計劃]** 畫面上，找出您要設為我的最愛的計劃。
2. 在計劃的列中，按一下 **[更多動作]** 圖示。
3. 按一下 **[新增至我的最愛]**。
   在 **[遠端管理計劃]** 畫面上，星形圖示會出現在計劃名稱旁。

監控計劃

必要條件

- 已為您的使用者帳戶啟用 2FA。
- 已至少為您的租用戶建立一個管理計劃。如需詳細資訊，請參閱 "建立監控計劃" (第 961 頁)。

若要將監控計劃設為我的最愛

1. 在 **[監控計劃]** 畫面上，找出您要設為我的最愛的計劃。
2. 在計劃的列中，按一下 **[更多動作]** 圖示。
3. 按一下 **[新增至我的最愛]**。
   在 **[監控計劃]** 畫面上，星形圖示會出現在計劃名稱旁。

從我的最愛移除計劃

您可以從我的最帶清單中移除我的最愛保護計劃、監控計劃和遠端管理計劃。

注意事項
此功能不適用於獲指派保護服務唯讀系統管理員角色的使用者。

保護計劃

必要條件

為您的租用戶至少將一個保護計劃設為我的最愛。

若要從我的最愛移除保護計劃

1. 在 **[保護計劃]** 畫面上，按一下您要從我的最愛移除的計劃。
2. 按一下 **[從我的最愛移除]**。

遠端管理計劃

必要條件

- 已為您的使用者帳戶啟用 2FA。
- 為您的租用戶至少將一個遠端管理計劃設為我的最愛。

若要從我的最愛移除遠端管理計劃

1. 在 **[遠端管理計劃]** 畫面上，找出您要從我的最愛移除的計劃。
2. 在計劃的列中，按一下 **[更多動作]** 圖示。
3. 按一下 **[從我的最愛移除]**。

監控計劃

必要條件

- 已為您的使用者帳戶啟用 2FA。
- 為您的租用戶至少將一個監控計劃設為我的最愛。

若要從我的最愛移除監控計劃

1. 在 **[監控計劃]** 畫面上，找出您要從我的最愛移除的計劃。
2. 在計劃的列中，按一下 **[更多動作]** 圖示。
3. 按一下 **[從我的最愛移除]**。

設定我的最愛計劃的順序

您可以設定已設為我的最愛的保護計劃在計劃選擇欄位中的顯示順序。

必要條件

至少將兩個計劃設定為我的最愛。

若要設定我的最愛計劃的順序

1. 在 Cyber Protect 主控台計劃畫面中，移至 **[管理]** > **[保護計劃]**。
2. 按一下 **[管理我的最愛]**。
3. 拖放計劃以設定其在計劃選擇欄位中的顯示順序。

   注意事項
   若要拖曳計劃，請按一下計劃名稱前的拖曳區域。

4. 按一下 **[儲存]**。

保護計劃和模組

為保護您的資料，您必須建立保護計劃，然後將其套用到您的工作負載。

由不同保護模組組成的保護計劃。啟用您需要的模組並進行設定，以建立符合您特定需求的保護計劃。

您可以選擇下列模組：

- 備份。將資料來源備份到本機或雲端儲存空間。
- "實作災難復原" (第 655 頁)。在雲端站台上啟動確切的電腦副本，並將工作負載從損毀的原始電腦切換到雲端的復原伺服器。
- 防毒和防惡意程式保護。使用內建防惡意軟體解決方案檢查工作負載。
- 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 篩選。透過封鎖對惡意 URL 和可下載內容的存取來保護電腦，免受源自網際網路的威脅。
- Windows Defender 防毒軟體。管理 Windows Defender 防毒軟體的設定以保護您的環境。
- Microsoft Security Essentials。管理 Microsoft Security Essentials 的設定以保護您的環境。
- 弱點評估。自動檢查您電腦上所安裝之 Windows、Linux、macOS、Microsoft 協力廠商產品和 macOS 協力廠商產品中的弱點，並對您發送通知。
- 修補程式管理。安裝電腦上 Windows、Linux、macOS、Microsoft 協力廠商產品和 macOS 協力廠商產品的修補程式和更新，以解決偵測到的弱點。
- 資料保護圖。探索資料以監視重要檔案的保護狀態。
- 裝置控制。指定允許或禁止使用者在電腦上使用的裝置。
- Advanced Data Loss Prevention。根據資料流程原則，防止透過週邊裝置 (例如印表機或卸除式儲存裝置) 或內部和外部網路傳輸，洩漏敏感資料。

建立保護計劃

您可使用下列方式建立保護計劃：

- 在 **[裝置]** 索引標籤。請選擇要保護的一或多個工作負載，然後為其建立保護計劃。
- 在 **[管理]** > **[保護計劃]** 索引標籤上。建立保護計劃，然後選擇要套用計劃的一或多個工作負載。

當您建立保護計劃時，只會顯示適用於您工作負載類型的模組。

您可以將保護計劃套用至超過一個工作負載。您還可以將多個保護計劃套用製相同工作負載。若要深入瞭解可能的衝突，請參閱 "解決計劃衝突" (第 197 頁)。

若要建立保護計劃

裝置

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 選擇您要保護的工作負載，然後按一下 **[保護]**。
3. [如果已套用計劃] 按一下 **[新增計劃]**。
4. 按一下 **[建立計劃]** > **[保護]**。
   保護計劃面板隨即開啟。
5. [選用] 若要重新命名保護計劃，請按一下鉛筆圖示，然後輸入新名稱。

6. [選用] 若要啟用或停用計劃中的模組，請切換模組名稱旁邊的開關。
7. [選用] 若要設定模組，請按一下以將其展開，然後根據您的需求變更設定。
8. 準備就緒後，按一下 **[建立]**。

注意事項
若要使用加密建立保護計劃，請指定加密密碼。如需詳細資訊，請參閱 "加密" (第 390 頁)。

[管理] > [保護計劃]

1. 在 Cyber Protect 主控台，前往 **[管理]** > **[保護計劃]**。
2. 按一下 **[建立計劃]**。
   此時將打開保護計劃的範本。
3. [選擇性] 若要重新命名保護計劃，請按一下鉛筆圖示，然後輸入新名稱。
4. [選用] 若要啟用或停用計劃中的模組，請切換模組名稱旁邊的開關。
5. [選用] 若要設定模組，請按一下以將其展開，然後根據您的需求變更設定。
6. [選用] 若要選擇想套用計劃的工作負載，請按一下 **[新增裝置]**。

注意事項
您可以建立計劃而不將其套用至任何工作負載。您之後可以透過編輯計劃來新增工作負載。如需有關如何將工作負載新增到計劃的詳細資訊，請參閱 "將保護計劃套用到工作負載" (第 194 頁)。

7. 準備就緒後，按一下 **[建立]**。

注意事項
若要使用加密建立保護計劃，請指定加密密碼。如需詳細資訊，請參閱 "加密" (第 390 頁)。

若要視需要執行模組 (例如 **[備份]**、**[防毒和防惡意程式保護]**、**[弱點評估]**、**[修補程式管理]** 或 **[資料保護圖]**) 時，按一下 **[立即執行]**。

觀看建立第一個保護計劃操作說明影片。

如需有關災難復原模組的詳細資訊，請參閱 "建立災難復原保護計劃" (第 660 頁)。

如需有關裝置控制模組的詳細資訊，請參閱 "使用裝置控制模組" (第 301 頁)。

具有保護計劃的動作

建立保護計劃後，您可以將其用於執行下列動作：

- 將計劃套用至工作負載或裝置群組。
- 重新命名計劃。
- 編輯計劃。
  您可以啟用和停用計劃中的模組，並變更其設定。
- 啟用或停用計劃。
  已停用的計劃將不會在套用該計劃的工作負載上執行。

對於之後打算使用相同計劃保護相同工作負載的系統管理員而言，此動作相當方便。計劃未從工作負載撤銷，因此，您可以透過重新啟用該計劃快速還原保護。

- 從工作負載撤銷計劃。

  已撤銷的計劃不會再套用至工作負載。

  對於不需要再次使用相同計劃迅速保護相同工作負載的系統管理員而言，此動作相當方便。若要還原對已撤銷計劃提供的保護，您必須知道此計劃的名稱、從可用計劃清單中選擇該計劃，然後將其重新套用至相關工作負載。
- 停止計劃。

  此動作會停止套用計劃所在所有工作負載上所有執行中的備份作業。備份將會根據計劃排程再次開始。

  反惡意程式碼掃描不會受到此動作影響，而且將會按照排程中設定繼續進行。
- 複製計劃。

  您可以建立與現有計劃相同的副本。此新計劃未指派至任何工作負載。
- 匯出與匯入計劃。

  您可以將計劃匯出成 JSON 格式的檔案，可以稍後再重新匯入。因此，您不需要手動建立新計劃並進行設定。

注意事項

您可以匯入使用 Cyber Protection 9.0 (2020 年 3 月發行) 和更新版本建立的保護計劃。在舊版中建立的計劃與 9.0 版及更新版本的 Cyber Protection 不相容。

- 檢查計劃詳細資料。
- 檢查與計劃相關的活動與警示。
- 刪除計劃。

將保護計劃套用到工作負載

若要保護工作負載，您必須對其套用保護計劃。

您可以從 **[裝置]** 索引標籤和 **[管理]** > **[保護計劃]** 索引標籤套用計劃。

裝置

1. 請選擇您要保護的一或多個工作負載。
2. 按一下 **[保護]**。
3. [如果已將另一個保護計劃套用至選擇的工作負載] 請按一下 **[新增計劃]**。
4. 已顯示可用保護計劃的清單。
5. 選擇您要套用的保護計劃，然後按一下 **[套用]**。

[管理] > [保護計劃]

1. 在 Cyber Protect 主控台，前往 **[管理]** > **[保護計劃]**。
2. 選擇您要套用的保護計劃。
3. 按一下 **[編輯]**。
4. 按一下 **[管理裝置]**。

5. 在 **[裝置]** 視窗中，按一下 **[新增]**。
6. 選取您要套用計劃的工作負載，然後按一下 **[新增]**。
7. 在 **[裝置]** 視窗中，按一下 **[完成]**。
8. 在保護計劃面板中，按一下 **[儲存]**。

若要瞭解如何將保護計劃套用至裝置群組，請參閱 "將計劃套用到群組" (第 299 頁)。

編輯保護計劃

當您編輯計劃時，可以啟用和停用當中的模組，並變更其設定。

您可以編輯套用至所有工作負載的保護計劃，或僅編輯選擇的工作負載。

您可以從 **[裝置]** 索引標籤和 **[管理] > [保護計劃]** 索引標籤編輯計劃。

裝置

1. 選擇已套用計劃的一或多個工作負載。
2. 按一下 **[保護]**。
3. 選擇您要編輯的保護計劃。
4. 按一下計劃名稱旁的省略符號圖示 (...)，然後按一下 **[編輯]**。
5. 按一下您想要編輯的模組，然後視需要進行設定。
6. 按一下 **[儲存]**。
7. [若您未選擇所有已套用計劃的工作負載] 選擇編輯範圍：
   - 若要編輯已套用到所有工作負載的計劃，請按一下 **[將變更套用至此保護計劃](這將會影響其他裝置)**。
   - 若只要變更已選擇工作負載的計劃，按一下 **[只為選擇的裝置建立新保護計劃]**。
     因此，現有計劃將從選擇的工作負載中撤銷。將建立使用您設定的新保護計劃，並套用至這些工作負載。

[管理] > [保護計劃]

1. 在 Cyber Protect 主控台，前往 **[管理] > [保護計劃]**。
2. 選擇您要編輯的保護計劃。
3. 按一下 **[編輯]**。
4. 按一下您想要編輯的模組，然後視需要進行設定。
5. 按一下 **[儲存]**。

注意事項
從 **[管理] > [保護計劃]** 索引標籤編輯計劃會影響套用該計劃的所有工作負載。

撤銷保護計劃

當您撤銷計劃時，會將其從一或多個工作負載中移除。計劃仍會保護其他有套用的工作負載。

您可以從 **[裝置]** 索引標籤和 **[管理] > [保護計劃]** 索引標籤撤銷計劃。

裝置

1. 選擇要撤銷計劃的工作負載。
2. 按一下 **[保護]**。
3. 選擇您要撤銷的保護計劃。
4. 按一下計劃名稱旁的省略符號圖示 (...)，然後按一下 **[撤銷]**。

[管理] > [保護計劃]

1. 在 Cyber Protect 主控台，前往 **[管理] > [保護計劃]**。
2. 選擇您要撤銷的保護計劃。
3. 按一下 **[編輯]**。
4. 按一下 **[管理裝置]**。
5. 在 **[裝置]** 視窗中，選擇要撤銷計劃的工作負載。
6. 按一下 **[移除]**。
7. 在 **[裝置]** 視窗中，按一下 **[完成]**。
8. 在保護計劃範本中，按一下 **[儲存]**。

啟用或停用保護計劃

已啟用的計劃會在套用該計劃的工作負載上啟動並執行。已停用的計劃無效——這仍會套用至工作負載但不會在當中執行。

當您從 **[裝置]** 索引標籤啟用或停用保護計劃時，您的動作僅會影響選擇的工作負載。

當您從 **[管理] > [保護計劃]** 索引標籤啟用或停用保護計劃時，該動作會影響所有套用該計劃的工作負載。此外，您可以啟用或停用多個保護計劃。

裝置

1. 選擇要停用當中計劃的工作負載。
2. 按一下 **[保護]**。
3. 選擇您要停用的保護計劃。
4. 按一下計劃名稱旁的省略符號圖示 (...)，然後分別按一下 **[啟用]** 或 **[停用]**。

[管理] > [保護計劃]

1. 在 Cyber Protect 主控台，前往 **[管理] > [保護計劃]**。
2. 請選擇您要啟用或停用的一或多個保護計劃。
3. 按一下 **[編輯]**。
4. 分別按一下 **[啟用]** 或 **[停用]**。

注意事項
此動作不會影響已在目標狀態的保護計劃。例如，若您的選擇包含已啟用和已停用的計劃，之後按下 **[啟用]**，將會啟用所有選擇的計劃。

刪除保護計劃

當您刪除計劃時，會從所有工作負載中撤銷，並從 Cyber Protect 主控台移除。

您可以從 **[裝置]** 索引標籤和 **[管理]** > **[保護計劃]** 索引標籤刪除計劃。

裝置

1. 選擇已套用您要刪除的保護計劃的任何工作負載。
2. 按一下 **[保護]**。
3. 選擇您要刪除的保護計劃。
4. 按一下計劃名稱旁的省略符號圖示 (...)，然後按一下 **[刪除]**。

[管理]* > *[保護計劃]

1. 在 Cyber Protect 主控台，前往 **[管理]** > **[保護計劃]**。
2. 選擇您要刪除的保護計劃。
3. 請按一下 **[刪除]**。
4. 選擇 **[我確認要刪除計劃]** 核取方塊以確認選擇項目，然後按一下 **[刪除]**。

解決計劃衝突

您可以將多個保護計劃套用製相同工作負載。例如，您可以套用僅啟用並設定 **[防毒與防惡意軟體]** 模組的一個保護計劃，以及另一個僅啟用並設定 **[備份]** 模組的保護計劃。

您可以組合啟用不同模組的保護計劃。您還可以組合多個僅啟用 **[備份]** 模組的保護計劃。然而，若有其他任何模組在超過一個的計劃中啟用，會發生衝突。若要套用計劃，您必須先解決衝突。

新計劃與現有計劃間的衝突

若新計劃與現有計劃衝突，您可以透過以下方式之一解決衝突：

- 建立新計劃、將其套用、然後停用與新計劃衝突的現有計劃。
- 建立一個新計劃，然後停用。

個別與群組計劃之間的衝突

若個別保護計劃與套用至裝置群組的群組計劃衝突，您可以透過以下方式之一解決衝突：

- 從裝置群組中移除該工作負載，並套用個別保護計劃。
- 編輯現有群組計劃或將新的群組計劃套用至裝置群組。

授權問題

保護計劃模組可能會需要將特定服務配額指派至受保護的工作負載。若指派的服務配額不適合，您將無法執行、更新或套用已啟用對應模組的保護計劃。

若要解決授權問題，請執行下列其中一項操作：

- 停用現已指派的服務配額不支援的模組，然後繼續使用保護計劃。
- 手動變更獲指派的服務配額。若要瞭解操作方式，請參閱 "變更電腦的服務配額" (第 173 頁)。

用於託管控制台整合的個別保護計劃

當您在使用 DirectAdmin、cPanel 或 Plesk 的 Web 託管伺服器上啟用託管控制台整合時，Cyber Protection 服務會針對每個工作負載，使用您的使用者帳戶自動建立個別保護計劃。此保護計劃與起始保護計劃建立的特定工作負載相關聯，而且無法撤銷或指派給其他工作負載。

若要停止使用個別的保護計劃，您可以從 Cyber Protect 主控台移除該保護計劃。您可以透過保護計劃名稱旁的 記號，識別個別的保護計劃。

如果您希望保護計劃保護使用託管控制台整合的多個 Web 託管伺服器，您可以在 Cyber Protect 主控台中建立一個標準保護計劃，並將這些工作負載指派給該計劃。不過，對由多個 Web 託管控制台共用的保護計劃的任何修改只能在 Cyber Protect 主控台中進行，而無法從整合內進行。

脫離主機資料保護計劃

注意事項
此功能適用於當作 Advanced Backup 套件一部分啟用的 **Advanced Backup – 伺服器**或 **Advanced Backup – NAS** 配額的客戶租用戶。

複寫、驗證和清理通常由執行備份的保護代理程式執行。即使備份程序完成後，這也會為執行代理程式的電腦帶來額外的負載。若要卸載電腦，您可以建立脫離主機資料保護計劃，即用於複寫、驗證、清理和轉換到虛擬機器的單獨計劃。

透過脫離主機資料保護計劃，您可以執行以下操作：

- 為備份和脫離主機資料保護作業選擇不同的代理程式
- 將脫離主機資料處理作業排程在非尖峰時段，以便將網路頻寬耗用量降至最低
- 如果您不想要為脫離主機資料處理安裝專用的代理程式，請將脫離主機資料處理作業排程在非營業時段

注意事項
脫離主機資料處理計劃會根據安裝保護代理程式所在電腦的時間設定 (包括時區) 執行。若是虛擬裝置 (例如，VMware 用代理程式或 Scale Computing HC3 用代理程式)，您可以在代理程式的圖形化使用者介面中設定時區。

備份複寫

注意事項
此功能適用於當作 Advanced Backup 套件一部分啟用的 **Advanced Backup – 伺服器**或 **Advanced Backup – NAS** 配額的客戶租用戶。

備份複寫是將備份複製到其他位置。作為脫離主機資料處理作業，它是在備份複寫計劃中設定的。

備份複寫也可以是保護計劃的一部分 。如需有關此選項的詳細資訊，請參閱 "複寫" (第 388 頁)。

建立備份複寫計劃

若要將備份複寫為脫離主機資料處理作業，您需要建立一個備份複寫計劃。

若要建立備份複寫計劃

1. 在 Cyber Protect 主控台中，按一下 **[管理]** > **[備份複寫]**。
2. 按一下 **[建立計劃]**。
3. 在 **[代理程式]** 中，選擇將執行複寫的代理程式。
   您可以選擇可同時存取來源位置和複寫位置的任何代理程式。
4. 在 **[要複寫的項目]** 中，選擇要複寫的存檔或備份位置。
   若要在存檔和位置之間切換，請使用右上角的 **[位置]** / **[備份]** 開關。
   如果您選擇多個加密存檔，則其加密密碼必須相同。對於使用不同加密密碼的存檔，請建立單獨的計劃。
5. 在 **[目的地]** 中，指定複寫位置。
6. 在 **[複寫方式]** 中，選擇要複寫的備份 (亦稱為復原點)。
   您可以選取下列選項：
   - **所有備份**
   - **僅限完整備份**
   - **僅限最後一個備份**

   有關這些選項的詳細資訊，請參閱 "要複寫的內容" (第 200 頁)。
7. 在 **[排程]** 中，設定複寫排程。
   設定備份複寫計劃的排程時，確保備份複寫開始時，最後複寫的備份仍可在原始位置中使用。例如，如果因為遭保留規則刪除而無法在原始位置中使用此備份，會將整個存檔複寫為完整備份。這可能非常耗時，且會使用額外儲存空間。
8. 在 **[保留規則]** 中，指定目標位置的保留規則。
   您可以選取下列選項：
   - **按照備份數目**
   - **按照備份存留期** (每月、每週、每日和每小時備份的個別設定)
   - **按照備份大小總計**
   - **無限期保留備份**

   注意事項
   選擇此選項將會導致儲存空間使用量增加。您必須手動刪除不必要的備份。
9. [如果您在 **[要複寫的項目]** 中選擇加密存檔] 啟用 **[備份密碼]** 開關，然後提供加密密碼。
10. [選用] 若要修改計劃選項，請按一下齒輪圖示，然後視需要設定選項。
11. 按一下 **[建立]**。

要複寫的內容

注意事項
某些複寫作業 (例如複寫整個位置或複寫備份集中的所有備份) 可能非常耗時。

您可以複寫個別備份集或整個備份位置。當您複寫備份位置時，將會複寫其中的所有備份集。

備份集由備份 (亦稱為復原點) 所組成。您必須選擇要複寫的備份。

您可以選取下列選項：

- **所有備份**
  每次執行複寫計劃時，都會複寫備份集中的所有備份。
- **僅限完整備份**
  僅複寫備份集中的完整備份。
- **僅限最後一個備份**
  僅複寫備份集中最新的備份，無論其類型為何 (完整、差異或增量)。

根據您的需要和您所使用的備份配置，選擇選項。例如，如果使用 **[一律增量 (單一檔案)]** 備份配置，而您只要複寫最新的增量備份，那麼請在備份複寫計劃中選擇 **[僅限上次備份]**。

下表摘要哪些備份將以不同的備份配置進行複寫。

	一律增量 (單一檔案)	始終完整備份	每週完整備份，每日增量備份	每月完整備份、每週差異備份和每日增量備份 (GFS)
所有備份	備份集中的所有備份	備份集中的所有備份	備份集中的所有備份	備份集中的所有備份
僅限完整備份	僅限第一個備份，其為完整備份	所有備份	每週一次備份*	每月一次備份*
僅限上次備份	僅限備份集中的最新備份*	僅限備份集中的最新備份*	僅限備份集中的最新備份，無論其類型為何*	僅限備份集中的最新備份，無論其類型為何*

*設定備份複寫計劃的排程時，確保備份複寫開始時，最後複寫的備份仍可在原始位置中使用。例如，如果因為遭保留規則刪除而無法在原始位置中使用此備份，會將整個存檔複寫為完整備份。這可能非常耗時，且會使用額外儲存空間。

支援的離線主機資料處理位置

下表摘要說明離線主機資料處理備份複寫計劃中支援的備份位置。

備份位置	支援作為來源	支援作為目標
雲端儲存	+	+

備份位置	支援作為來源	支援作為目標
本機資料夾	+	+
網路資料夾	+	+
公有雲端	+	+
NFS 資料夾	–	–
Secure Zone	–	–

驗證

注意事項
此功能適用於當作 Advanced Backup 套件一部分啟用的 **Advanced Backup – 伺服器**或 **Advanced Backup – NAS** 配額的客戶租用戶。

您可以驗證備份以確認您可以復原資料。

當您驗證備份時，您會將驗證方法套用至備份存檔或備份位置。驗證備份位置會驗證此位置中的所有存檔。

若要將備份驗證為脫離主機資料處理作業，您必須建立一個驗證計劃。如需詳細資訊，請參閱 "建立驗證計劃" (第 205 頁)。

若要在不建立驗證計劃的情況下驗證備份，請依照 "驗證備份" (第 473 頁) 中的程序進行。

支援的驗證位置

下表摘要說明支援的備份位置和驗證方法。

注意事項
由於從公有雲端讀取整個存檔的成本高昂，因此驗證選項不適用於公有雲端備份。

備份位置	總和檢查碼驗證	以虛擬機器身分執行	
		VM 活動訊號	螢幕擷取畫面驗證
雲端儲存	+	+	+
本機資料夾	+	+	+
網路資料夾	+	+	+
NFS 資料夾	–	–	–
Secure Zone	–	–	–

驗證方式

您可以選擇一種或多種驗證方法。如果選擇多種驗證方法，則會按照以下順序套用這些方法：

- VM 活動訊號 (**[以虛擬機器身分執行]** 驗證選項的一部分)
- 螢幕擷取畫面驗證 (**[以虛擬機器身分執行]** 驗證選項的一部分)
- 總和檢查碼驗證

[以虛擬機器身分執行] 驗證選項僅適用於包含作業系統的磁碟層級備份。您可以在受保護代理程式 (VMware 用代理程式或 Hyper-V 用代理程式) 管理的 ESXi 或 Hyper-V 主機上使用此選項。

VM 活動訊號

使用此驗證方式時，代理程式會從備份執行虛擬機器，連線至 VMware Tools 或 Hyper-V Integration Service，然後檢查活動訊號回應，以確認作業系統已成功啟動。如果連線失敗，則代理程式嘗試每兩分鐘連線一次，總共嘗試五次。若連線嘗試沒有一次成功，則驗證失敗。

無論驗證計劃和已驗證備份的數目為何，執行驗證的代理程式會一次執行一個虛擬機器。驗證結果清晰可見之後，代理程式即會刪除該虛擬機器，然後執行下一個虛擬機器。

注意事項
只有在您透過在 ESXi 主機上將這些備份作為虛擬機器執行來驗證 VMware 虛擬機器的備份時，以及在 Hyper-V 主機上將這些備份作為虛擬機器執行來驗證 Hyper-V 虛擬機器的備份時，才使用此方法。

螢幕擷取畫面驗證

代理程式會使用此驗證方法，從備份執行虛擬機器，並在虛擬機器正在開機時擷取螢幕擷取畫面。Machine Intelligence (MI) 模組會檢查螢幕擷取畫面，如果其中有登入畫面，則會驗證該備份。

螢幕擷取畫面會附加到復原點，您可在驗證後一年內，在 Cyber Protect 主控台中下載它。如需有關如何檢查螢幕擷取畫面的詳細資訊，請參閱 "檢查驗證狀態" (第 204 頁)。

如果您的使用者帳戶已啟用通知，您將會收到有關備份驗證狀態的電子郵件。此電子郵件中會附加螢幕擷取畫面。如需有關通知的詳細資訊，請參閱變更使用者的通知設定。

代理程式版本 15.0.30971 (2022 年 11 月發行) 和更新版本支援螢幕擷取畫面驗證。

注意事項
螢幕擷取畫面驗證最適用於具備 GUI 式登入畫面之 Windows 和 Linux 系統的備份。此方法並未針對具備主控台登入畫面的 Linux 系統進行最佳化。

總和檢查碼驗證

透過總和檢查碼驗證的驗證作業會為每個可從備份復原的資料區塊計算一個總和檢查碼，然後將其與備份過程中寫入之資料區塊的原始總和檢查碼相比較。唯一的例外是驗證位於雲端儲存空間中檔案層級的備份。這些備份的驗證方式是檢查備份中儲存之中繼資料的一致性。

透過總和檢查碼驗證的驗證作業非常耗時，即使是規模通常比較小的增量或差異備份也是如此。驗證作業包含必須復原的所有資料。若是增量和差異備份，這些資料可能包含在多個備份中。

透過總和檢查碼驗證的成功驗證可確保資料復原的可能性很高。不過，透過此方法的驗證並未檢查可能影響復原程序的所有因素。

如果要備份作業系統，我們建議您使用下列一些額外作業：

- 在可開機媒體下測試復原至備用硬碟。
- 在ESXi 或 Hyper-V 環境下從備份執行虛擬機器。
- 執行驗證計劃，該計劃中已啟用 **[以虛擬機器身分執行]** 驗證方式。

變更 VM 活動訊號和螢幕擷取畫面驗證的逾時

當您以執行備份作為虛擬機器的方式來驗證備份時，可以設定啟動虛擬機器以及傳送活動訊號要求或擷取螢幕擷取畫面之間的逾時。

預設期間如下：

- 一分鐘 – 針對儲存在本機資料夾或網路共用的備份。
- 五分鐘 – 針對儲存在雲端儲存空間的備份。

若要變更逾時

1. 開啟 VMware 代理程式或 Hyper-V 代理程式的組態檔案以進行編輯。
   組態檔案可在下列位置取得：
   - [針對在 Windows 中執行的 VMware 用代理程式或 Hyper-V 用代理程式] `C:\Program Files\BackupClient\BackupAndRecovery\settings.config`
   - [針對 VMware 用代理程式 (虛擬裝置)] `/bin/mms_settings.config`
     如需有關如何存取虛擬裝置上之設定檔案的詳細資訊，請參閱 "虛擬裝置的 SSH 連線" (第 155 頁)。
2. 前往 `<validation>`，然後視需要變更本機備份和雲端備份的值：

```
<validation>
<run_vm>
<initial_timeout_minutes>
<local_backups>1</local_backups>
<cloud_backups>5</cloud_backups>
</initial_timeout_minutes>
</run_vm>
</validation>
```

3. 儲存組態檔案。
4. 重新啟動代理程式。
   - [針對 Windows 中執行的 VMware 用代理程式或 Hyper-V 用代理程式] 在命令提示字元中執行下列命令：

```
net stop mms
```

```
net start mms
```

- [針對 VMware 用代理程式 (虛擬裝置)] 重新啟動虛擬裝置。

設定發生錯誤時的重試次數

若要讓成功驗證次數達到最高，您可以針對結束時發生錯誤的驗證作業，設定自動重試。

若要設定自動重試

1. 建立驗證計劃時，按一下齒輪圖示。
2. 在 **[選項]** 窗格中，選擇 **[錯誤處理]**。
3. 在 **[發生錯誤時重新嘗試]** 底下，按一下 **[是]**。
4. 在 **[嘗試次數]** 中，設定發生錯誤時的重試次數上限。
   驗證作業將再次執行，直到成功完成或達到重試次數上限為止。
5. 在 **[嘗試間隔]** 中，設定兩次連續重試之間的逾時。
6. 按一下**[完成]**。

驗證狀態

驗證狀態會指派給已完成驗證的備份。

如果驗證成功完成，該備份會標示綠色點和 **[已驗證]** 標籤。

如果驗證失敗，則該備份會標記紅色點。

每次驗證作業後都會更新驗證狀態。每種驗證方法的狀態都會個別更新。如果其中一個設定的驗證方法失敗，驗證就會失敗。在某些情況下，驗證失敗可能是由於驗證計劃設定錯誤所造成。例如，如果您對錯誤主機上的虛擬機器使用 **[VM 活動訊號]** 方法。

注意事項
如果其中一個設定的驗證方法失敗，則備份的驗證狀態將顯示為失敗。即使您停用失敗的方法重新設定驗證計劃，而且透過其他方法成功完成驗證，此狀態仍將持續存在。若是 **[已驗證]** 狀態，失敗的驗證方法必須針對相同的備份成功完成。

檢查驗證狀態

您可以在 **[裝置]** 索引標籤和 **[備份儲存]** 索引標籤上檢查備份的驗證狀態。

您可以查看每個驗證方法的狀態，並在使用螢幕擷取畫面驗證方法時下載螢幕擷取畫面。

若要檢查驗證狀態

裝置

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 選擇工作負載，然後按一下 **[復原]**。
3. [如果有一個以上的備份位置可用] 請選擇備份位置。
4. 選擇您要檢查其驗證狀態的備份。

備份儲存

1. 在 Cyber Protect 主控台中，移至 **[備份儲存]**。
2. 選擇備份位置。
3. 選擇備份存檔，然後按一下 **[顯示備份]**。
4. 選擇您要檢查其驗證狀態的備份。

驗證活動狀態

驗證計劃可能包含多個備份。在單一驗證活動中，所有備份會依序一一處理。

保護代理程式一次只能執行一個驗證活動。例如，同時執行兩個驗證活動需要兩個代理程式，同時執行三個活動需要三個代理程式。

下表總結了驗證活動的可能狀態。

活動結果	具有一個備份的計劃	具有多個備份的計劃
成功	所有驗證方式已成功	所有驗證方式在所有備份中皆已成功
成功，但有警告	不適用	至少有一個驗證方式在至少一個備份中失敗
失敗	至少有一個驗證方式失敗	至少有一個驗證方式在所有備份中失敗

建立驗證計劃

若要將備份存檔驗證為脫離主機資料處理作業，您必須建立一個驗證計劃。

一個驗證計劃可能包括多個備份，而一個備份可以由多個驗證計劃驗證。

若要建立驗證計劃

1. 在 Cyber Protect 主控台中，前往 **[管理]** > **[驗證]**。
2. 按一下 **[建立計劃]**。
3. [選用] 若要修改計劃名稱，請按一下預設名稱，然後指定新的名稱。
4. 在 **[代理程式]** 中，選擇執行驗證的代理程式，然後按一下 **[確定]**。
   - 如果您要透過從備份執行虛擬機器執行驗證，請選擇具有 VMware 用代理程式或 Hyper-V 用代理程式的電腦。
   - 如果您不想透過從備份執行虛擬機器執行驗證，請選擇可存取備份位置的任何電腦。
5. 在 **[要驗證的項目]** 中，選擇要驗證的備份存檔。
   a. 按一下右上角的 **[備份]** 或 **[位置]**，選擇驗證範圍 — 備份存檔或備份位置。
      如果所選存檔經過加密，則所有存檔必須使用相同的加密密碼。對於使用不同加密密碼的存檔，請建立單獨的計劃。
   b. 按一下 **[新增]**。
   c. 視驗證範圍而定，選擇一個或多個位置，或選擇一個位置和一個或多個備份存檔，然後按一下 **[完成]**。
   d. 按一下 **[完成]**。
6. 在 **[要驗證的內容]** 中，選擇要驗證的所選存檔中的備份 (亦稱為復原點)。下列選項可供使用：

- **所有備份**
- **僅限最後一個備份**

7. 在 **[驗證方式]** 中，選擇驗證方式。

   您可以選擇下列方法中的一個或兩個：

   - **總和檢查碼驗證**
   - **以虛擬機器的形式執行**

     [以虛擬機器的形式執行] 選項提供 **[VM 活動訊號]** 和 **[螢幕擷取畫面驗證]** 方法。如需詳細資訊，請參閱 "驗證方式" (第 202 頁)。
8. [如果已選擇 **[總和檢查碼驗證]**] 按一下 **[完成]**。
9. [如果選擇 **[以虛擬機器的形式執行]**] 為此選項進行設定。
   a. 在 **[目標電腦]** 中，選擇虛擬機器類型 (ESXi 或 Hyper-V)、主機和電腦名稱範本，然後按一下 **[確定]**。

      預設名稱為 **[電腦名稱]_validate**。
   b. 在 **[資料存放區]** (針對 ESXi) 或 **[路徑]** (針對 Hyper-V) 中，選擇虛擬機器的資料存放區。
   c. 選擇一種或兩種驗證方法：
      - **VM 活動訊號**
      - **螢幕擷取畫面驗證**
   d. [選用] 按一下 **[虛擬機器設定]** 可變更虛擬機器的記憶體大小和網路連線。

      依預設，虛擬機器未連接至網路，且虛擬機器記憶體大小等於原始電腦的記憶體大小。
   e. 按一下 **[完成]**。
10. [選用] 在驗證計劃中，按一下 **[排程]**，然後設定排程。
11. [如果 **[要驗證的項目]** 中選擇的存檔經過加密] 啟用 **[備份密碼]** 開關，然後提供加密密碼。
12. [選用] 要修改計劃選項，請按一下齒輪圖示。
13. 按一下 **[建立]**。

因此，將建立驗證計劃，並將依據您所設定的排程執行。若要立即執行計劃，請在 **[管理]** > **[驗證]** 中選擇計劃，然後按一下 **[立即執行]**。驗證開始後，您可以在 Cyber Protect 主控台中的 **[監控]** > **[活動]** 下檢查執行中的活動，並向下鑽研其詳細資料。

清理

清理作業會根據保留規則刪除過期的備份。此操作僅適用於代理程式和工作負載，不適用於雲端對雲端備份 (僅能手動刪除)。

注意事項

此功能適用於當作 Advanced Backup 套件一部分啟用的 **Advanced Backup – 伺服器**或 **Advanced Backup – NAS** 配額的客戶租用戶。

支援的位置

清理計劃支援除 NFS 資料夾和 Secure Zone 之外的所有備份位置。

若要建立清理計劃

1. 在 Cyber Protect 主控台中，按一下 **[管理]** > **[清理]**。
2. 按一下 **[建立計劃]**。
3. 在 **[代理程式]** 中，選擇將執行清理的代理程式。
   您可以選擇具有備份位置存取權的任何代理程式。
4. 在 **[要清理的項目]** 中，選擇要清理的存檔或備份位置。
   若要在存檔和位置之間切換，請使用右上角的 **[位置]** / **[備份]** 開關。
   如果您選擇多個加密存檔，則其加密密碼必須相同。對於使用不同加密密碼的存檔，請建立單獨的計劃。
5. 在 **[排程]** 中，設定清理排程。
6. 在 **[保留規則]** 中，指定保留規則。
   您可以選取下列選項：
   - **按照備份數目**
   - **按照備份存留期** (每月、每週、每日和每小時備份的個別設定)
   - **按照備份大小總計**
7. [如果您在 **[要複寫的項目]** 中選擇加密存檔] 啟用 **[備份密碼]** 開關，然後提供加密密碼。
8. [選用] 若要修改計劃選項，請按一下齒輪圖示，然後視需要設定選項。
9. 按一下 **[建立]**。

轉換為虛擬機器

轉換為虛擬機器僅可用於磁碟層級備份。若備份包含系統磁碟區以及啟動作業系統的所有必要資訊，則產生的虛擬機器可以自行啟動。否則，您可將其虛擬磁碟新增至其他虛擬機器。

注意事項
無法備份透過原生 Scale Computing VM 複寫功能複寫的 VM。

您可以為轉換為虛擬機器建立單獨的計劃，然後手動或按計劃執行此計劃。

有關先決條件及限制的資訊，請參閱 "關於轉換，您需要知道的內容" (第 208 頁)。

注意事項
此功能適用於當作 Advanced Backup 套件一部分啟用的 **Advanced Backup – 伺服器**或 **Advanced Backup – NAS** 配額的客戶租用戶。

若要建立轉換至虛擬機器的計劃

1. 按一下 **[管理]** > **[轉換為 VM]**。
2. 按一下 **[建立計劃]**。
   軟體會顯示新的計劃範本。
3. [選用] 要修改計劃名稱，請按一下預設名稱。
4. 在**轉換為**中，選擇目標虛擬機器的類型。**您可以選擇以下其中之一**：
   - **VMware ESXi**
   - **Microsoft Hyper-V**

- **Scale Computing HC3**
- **VMware Workstation**
- **VHDX 檔案**

注意事項
為了節省儲存空間，每次轉換到 VHDX 檔案或 VMware 工作站都會覆寫在上一次轉換過程中在目標位置建立的 VHDX/VMDK 檔案。

5. 執行下列其中一項操作：
   - [VMware ESXi、Hyper-V 和 Scale Computing HC3]：按一下 **[主機]**，選擇目標主機，然後指定新的電腦名稱範本。
   - [其他虛擬機器類型]：在 **[路徑]** 中，指定儲存虛擬機器檔案和檔案名稱範本的位置。

   預設名稱為 **[電腦名稱]_converted**。
6. 按一下 **[代理程式]**，然後選擇將執行轉換的代理程式。
7. 按一下 **[要轉換的項目]**，然後選擇此計劃將轉換為虛擬機器的備份。

   您可以使用右上角的 **[位置]** / **[備份]** 開關，在選擇備份和選擇整個位置之間切換。

   如果選定備份已加密，則所有備份必須使用相同的加密密碼。對於使用不同加密密碼的備份，請建立單獨的計劃。
8. [僅適用於 VMware ESXi 和 Hyper-V] 按一下 **[資料存放區]** (ESXi)，或按一下 **[路徑]** (Hyper-V)，然後選擇虛擬機器的資料存放區 (儲存)。
9. [僅適用於 VMware ESXi 和 Hyper-V]：選擇磁碟佈建模式。預設設定為：**[精簡]** (適用於 VMware ESXi) 和 **[動態延伸]** (適用於 Hyper-V)。
10. [選用] [VMware ESXi、Hyper-V 和 Scale Computing HC3]：按一下 **[VM 設定]** 以修改記憶體大小、處理器數量或虛擬機器的網路連線。
11. [選用] 按一下 **[排程]**，然後變更排程。
12. 如果 **[要轉換的項目]** 中選擇的備份已加密，請啟用 **[備份密碼]** 開關，然後提供加密密碼。否則，請跳過此步驟。
13. [選用] 要修改計劃選項，請按一下齒輪圖示。
14. 按一下 **[建立]**。

關於轉換，您需要知道的內容

支援的虛擬機器類型

將備份轉換至虛擬機器可以由建立備份的相同代理程式或其他代理程式完成。

若要轉換至 VMware ESXi、Hyper-V 或 Scale Computing HC3，您分別需要 ESXi、Hyper-V 或 Scale Computing HC3 主機以及用於管理此主機的保護代理程式 (VMware 用代理程式、Hyper-V 用代理程式或 Scale Computing HC3 用代理程式)。

轉換至 VHDX 檔案時，會假設檔案將當做虛擬磁碟連線至 Hyper-V 虛擬機器。

下表總結可以透過 **[轉換為 VM]** 作業建立虛擬機器的類型。表中的行顯示轉換後的虛擬機器類型。這些欄顯示執行轉換的代理程式。

VM 類型	VMware 用代理程式	Hyper-V 用代理程式	Windows 用代理程式	Linux 用代理程式	Mac 用代理程式	Scale Computing HC3 用代理程式	oVirt (KVM) 代理程式	Virtuozzo Hybrid Infrastructure 用代理程式	Virtuozzo 用代理程式
VMware ESXi	+	–	–	–	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–	–	–	–
VMware 工作站	+	+	+	+	–	–	–	–	–
VHDX 檔案	+	+	+	+	–	–	–	–	–
Scale Computing HC3	–	–	–	–	–	+	–	–	–

限制

- 無法轉換儲存空間在 NFS 上的備份。
- 儲存空間在Secure Zone域中的備份只能由在同一台機器上執行的代理程式進行轉換。
- 只有在含有 Linux 邏輯磁碟區 (LVM) 的備份由 VMware 用代理程式、Hyper-V 用代理程式或 Scale Computing HC3 用代理程式建立，並導向至相同的 Hypervisor 時，才能加以轉換。不支援跨 Hypervisor 轉換。
- 當 Windows 電腦的備份轉換至 VMware Workstation 或 VHDX 檔案時，產生的虛擬機器會繼承執行轉換所在電腦中的 CPU 類型。因此，對應的 CPU 驅動程式會安裝在客體作業系統中。如果在具有不同 CPU 類型的主機上啟動，客體系統會顯示驅動程式錯誤。請手動更新此驅動程式。

定期轉換為虛擬機器和從備份執行虛擬機器

若原始電腦出現故障，則這兩種作業均會向您提供可在幾秒內啟動的虛擬機器。

定期轉換為虛擬機器佔用 CPU 和記憶體資源。虛擬機器的檔案會不斷佔用資料存放區 (儲存) 上的空間。若生產主機用於轉換，則定期轉換可能不實際。然而，虛擬機器效能僅受主機資源限制。

從備份執行虛擬機器僅在虛擬機器執行時佔用資源。資料存放區 (儲存) 空間僅需要保留虛擬磁碟的變更。然而，由於主機不直接存取虛擬磁碟，但是會與從備份中讀取資料的代理程式通訊，因此虛擬機器可能執行較慢。此外，此虛擬機器為臨時機器。

虛擬機器如何定期轉換

定期轉換的工作方式取決於您選擇建立虛擬機器的位置。

- **如果您選擇將虛擬機器儲存為一組檔案:**每次轉換都會從頭開始重新建立虛擬機器。
- **如果您選擇在虛擬化伺服器上建立虛擬機器:**轉換增量或差異備份時，軟體會以增量方式更新現有的虛擬機器，而不會重新建立。這類轉換通常速度較快，可節省網路流量與執行轉換之主機的 CPU 資源。如果無法更新虛擬機器，軟體將會重新建立虛擬機器。

以下詳細說明這兩種情況。

如果您選擇將虛擬機器儲存為一組檔案

第一次轉換後，即會建立新的虛擬機器。後續的每次轉換均會重新建立此虛擬機器。首先，舊的機器會暫時重新命名。接著，會以舊機器的先前名稱建立新的虛擬機器。如果操作成功，將會刪除舊機器。如果此作業失敗，則會刪除新的機器，並給予舊機器其先前名稱。如此一來，轉換程序結束後一律只會剩下一部虛擬機器。但是，在轉換期間需要額外的儲存空間來存放舊的機器。

如果您選擇在虛擬化伺服器建立虛擬機器

第一次轉換會建立一部新的虛擬機器。後續每次轉換的程序如下：

- 如果自上次轉換以來進行 *[完整備份]*，則將從頭開始重新建立虛擬機器，如本節前面所述。
- 否則，系統會更新現有的虛擬機器，反映上次轉換以來的變更。如果無法更新 (例如，如果您刪除下述的中間快照)，系統便會重新建立虛擬機器。

中間快照

為了能夠安全更新轉換後的虛擬機器，軟體會儲存此機器的中間 Hypervisor 快照。快照命名為 **Replica...** 並且必須保留.

Replica... 快照對應到最新轉換的結果。如果要將機器復原到該狀態，可前往此快照；例如，如果您在機器進行操作，現在要放棄對其所做的變更。

對於轉換後的 Scale Computing HC3 虛擬機器，將建立附帶的 **工具快照**。僅供 Cyber Protection 服務使用。

備份掃描計劃

若要掃描備份中的惡意程式碼 (包括勒索軟體)，請建立備份掃描計劃。

重要事項

並非所有工作負載和備份儲存空間都支援備份掃描計劃。如需詳細資訊，請參閱 "限制" (第 767 頁)。

建立備份掃描計劃

1. 在 Cyber Protect 主控台中，移至 **[管理]** > **[備份掃描]**。
2. 在 **[動作]** 窗格中，按一下 **[建立計劃]**。

3. [選用] 變更預設計劃名稱。
4. 在 **[要掃描的備份]** 中，按一下 **[指定]**。
   a. [選擇性] 若要新增位置，按一下 **[新增]**，選擇一個位置，然後按一下 **[完成]**。
   b. 按一下 **[位置]** 或 **[備份]** 以選擇計劃的範圍。
   c. 選擇整個位置或位置中的個別存檔。
      您可以選擇一或多個項目。
   d. 按一下**[完成]**。
5. [如果所選存檔經過加密] 在 **[加密]** 中，啟用切換，然後指定加密密碼。
   所有存檔都必須使用相同的加密密碼。對於使用不同加密密碼的存檔，請建立單獨的計劃。
6. 按一下 **[建立]**。

結果，備份掃描計劃隨即建立。雲端代理程式將每小時自動掃描所選存檔一次。您無法變更計劃排程或兩次連續掃描之間的期間。

雲端應用程式的備份計劃

[管理] > **[雲端應用程式備份]** 索引標千會顯示雲端對雲端備份計劃。這些計劃會透過在雲端執行的代理程式，備份在雲端執行的應用程式，並使用雲端儲存空間做為備份位置。

在本節中，您可以執行下列作業：

- 建立、檢視、執行、停止、編輯，以及刪除備份計劃
- 檢視與每個備份計劃相關的活動
- 檢視與每個備份計劃相關的警示

如需雲端應用程式備份的詳細資訊，請參閱：

- 保護 Microsoft 365 資料
- 保護 Google Workspace 資料

手動執行雲端對雲端備份

為防止中斷 Cyber Protection 服務，手動雲端對雲端備份執行的次數限制為每個 Microsoft 365 或 Google Workspace 組織每小時執行 10 次。達到此次數之後，會將允許的執行次數重設為每小時一次，然後每小時之後可以再額外執行一次 (例如，第 1 個小時，執行 10 次；第 2 個小時，執行 1 次；第 3 個小時，執行 2 次)，直到達到每小時總共執行 10 次為止。

無法手動執行套用至裝置 (信箱、磁碟機、網站) 群組或包含超過 10 個裝置的備份計劃。

協同作業和通訊應用程式的保護

Zoom、Cisco Webex Meetings、Citrix Workspace 和 Microsoft Teams 現在廣泛用於視訊/網路會議和通訊。Cyber Protection 服務可讓您保護協同作業工具。

Zoom、Cisco Webex Meetings、Citrix Workspace 和 Microsoft Teams 的保護設定都類似。在以下的範例中，我們將考慮 Zoom 的設定。

設定 Zoom 保護

1. 在安裝協同作業應用程式所在的電腦上安裝保護代理程式。
2. 登入 Cyber Protect 主控台，並套用保護計劃，其中已啟用下列其中一個模組：
   - **防毒和反惡意程式碼保護**（已啟用 **[自我保護]** 和 **[Active Protection]** 設定）- 如果您有其中一個 Cyber Protect 版本。
   - **Active Protection**（已啟用 **[自我保護]** 設定）- 如果您有其中一個 Cyber Backup 版本。
3. [選用] 若要自動安裝更新，請在保護計劃中設定**路徑管理**模組。

因此，您的 Zoom 應用程式將會受到保護，其中包含下列活動：

- 自動安裝 Zoom 用戶端更新
- 保護 Zoom 程序免於插入程式碼
- 透過 Zoom 程序防止可疑的操作
- 防止「主機」檔案新增與 Zoom 相關的網域

瞭解您目前的保護層級

監控

[監控] 索引標籤可提供關於您目前保護層級的重要資訊，並包含下列儀表板：

- **概觀**
- **活動**
- **警示**
- **威脅摘要** (如需詳細資訊，請參閱 "威脅摘要" (第 251 頁))

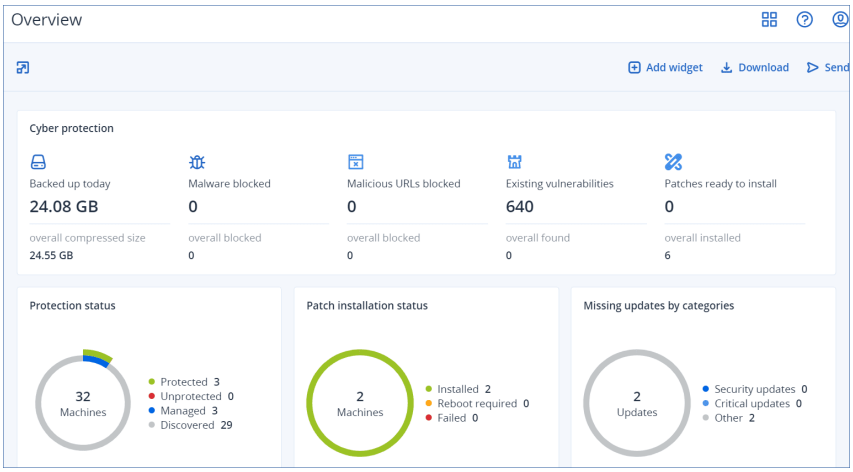
概觀儀表板

[概觀] 儀表板提供許多可自訂的動態桌面小工具，可概覽與 Cyber Protection 服務有關的作業。針對其他服務的動態小工具將在未來版本中提供。

系統會每五分鐘更新一次桌面小工具。動態小工具帶有可按一下的元素，可讓您調查問題並進行疑難排解。您可以透過 .pdf 和/或 .xlsx 格式下載最新狀態的儀表板或透過電子郵件進行傳送。

您可以從各種桌面小工具中選擇：顯示為表格、長條圖和樹狀圖。您可以新增具有不同篩選的相同類型動態小工具。

[監控] > **[概觀]** 中的 **[下載]** 和 **[傳送]** 按鈕無法用於 Cyber Protection 服務的 Standard 版本。



重新排列儀表板上的動態小工具

透過在動態小工具的名稱上按一下，可拖曳它們。

編輯動態小工具

按一下動態小工具名稱旁的鉛筆圖示。編輯桌面小工具可讓您將它重新命名、變更時間範圍、設定篩選，以及為列分組。

新增動態小工具

按一下 **[新增動態小工具]**，然後執行下列其中一項操作：

- 按一下您要新增的動態小工具。接著會以預設設定新增動態小工具。
- 若要在新增之前編輯桌面小工具，請在選取桌面小工具時按一下 [自訂]。編輯動態小工具之後，按一下 **[完成]**。

移除動態小工具

按一下動態小工具名稱旁的 X 符號。

[活動] 儀表板

[活動] 儀表板提供目前與過去活動的概觀。依預設，保留期為 90 天。

若要自訂 **[活動]** 儀表板的檢視，請按一下齒輪圖示，然後選擇您要查看的欄。

若要即時查看活動進度，請選擇 **[自動重新整理]** 核取方塊。不過，經常更新多個活動會降低管理伺服器的效能。

您可以依下列條件搜尋列出來的活動：

- **裝置名稱**
  這是執行活動所在的電腦。
- **啟動者**
  這是啟動活動的帳戶。

您也可以依下列屬性篩選活動：

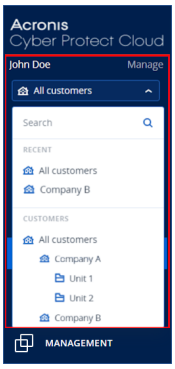
- **狀態**
  例如，成功、失敗、進行中、已取消。
- **類型**
  例如，套用計劃、刪除備份、安裝軟體更新。
- **時間**
  例如，最近的活動、過去 24 小時的活動，或是預設保留期內特定期間的活動。

若要查看有關活動的更多詳細資料，請從清單中選擇此活動，然後在 **[活動詳細資料]** 面板中，按一下 **[所有屬性]**。如需有關可用屬性的詳細資訊，請參閱開發人員網路入口網站中的 [活動] 和 [工作] API 參考資料。

[警示] 儀表板

[監控] > **[警示]** 儀表板會顯示您所管理的租用戶的目前警示。根據導覽功能表中下拉式清單內的所選層級，會顯示所有客戶租用戶或特定客戶租用戶的警示。

如果您僅管理一個租用戶，則無法使用下拉式清單。



每個警示都包含有關其原因或疑難排解建議的一般資訊。若要解決基礎問題的進一步協助，請按一下每個警示下方的 **[取得支援]**。視您的角色以及在您的租用戶中啟用的服務而定，您可以在知識庫中搜尋解決方案，或提交支援票證。

自訂警示儀表板

[警示] 儀表板支援簡易檢視和表格檢視。簡易檢視會顯示可捲動的目前警示清單，而表格檢視則會在一個畫面上顯示更多警示以及這些警示的其他資訊。

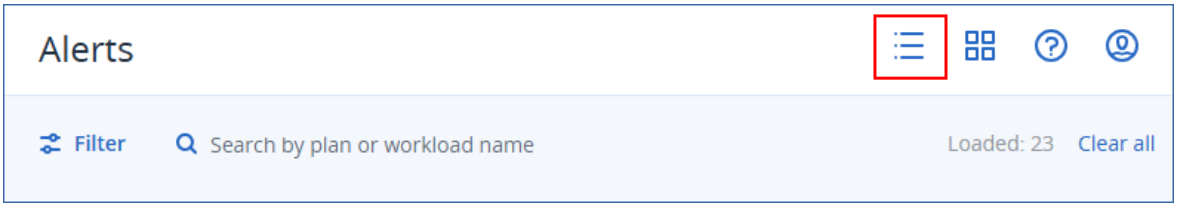
使用表格檢視時，您可以透過新增或移除欄來自訂 **[警示]** 儀表板。

在簡易與表格檢視中，您都可以隱藏快速篩選區段。

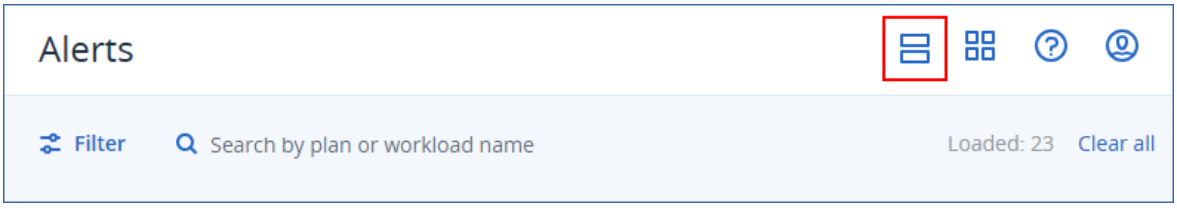
在檢視之間切換

若要在簡易和表格檢視之間切換

1. 在 Cyber Protect 主控台中，移至 **[監控]** > **[警示]**。
2. 若要切換至表格檢視，請按一下表格檢視圖示。



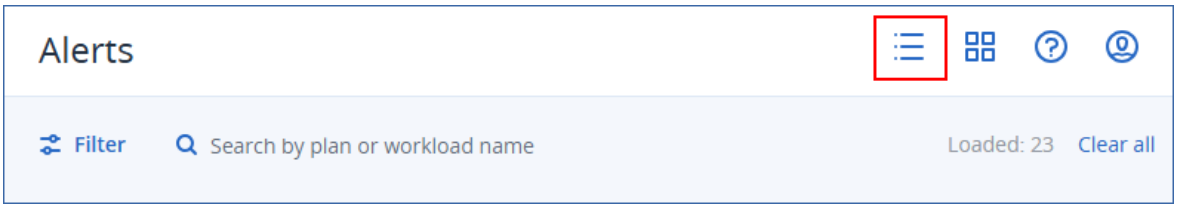
3. 若要切換至簡易檢視，請按一下簡易檢視圖示。



新增或移除欄

若要新增或移除欄

1. 在 Cyber Protect 主控台中，移至 **[監控]** > **[警示]**。
2. [若使用簡易檢視] 按一下表格檢視圖示。



3. 按一下右上角的齒輪圖示，然後選擇您要顯示的欄。
   以下是可用的欄。

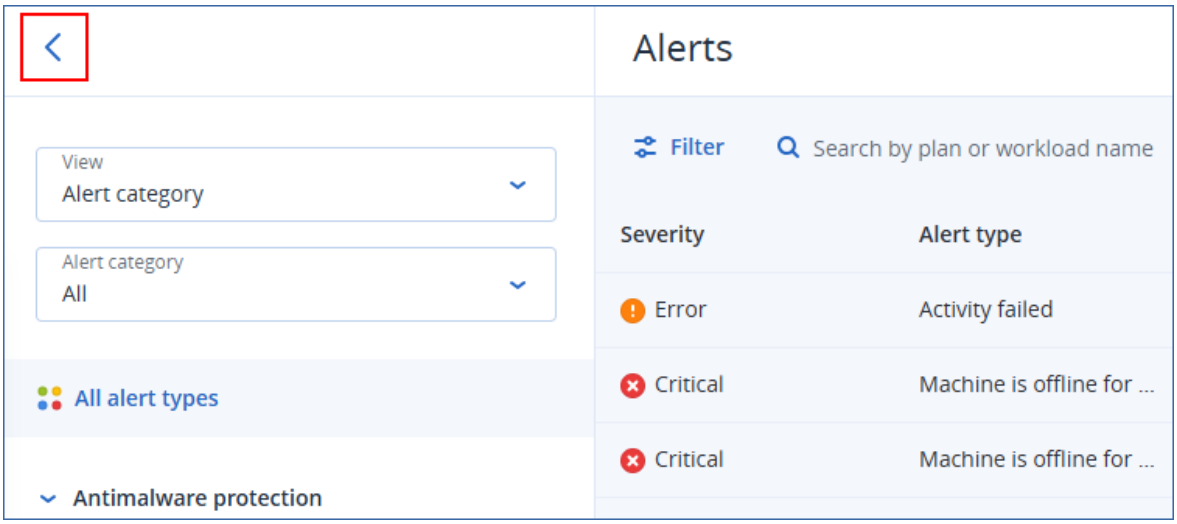
欄	描述
嚴重性 (一律可用)	警示的重要性層級。 嚴重性可能是下列其中一項： • 重大 • 錯誤 • 警告 • 資訊
警示類型	警示摘要。如需詳細資訊，請參閱 "警示類型和類別" (第 218 頁)。
訊息 (一律可用)	警示詳細資料
監控類型	監控類型 – 基於閾值或基於異常。如需詳細資訊，請參閱 "監控工作負載的健全狀況和效能" (第 935 頁)。
工作負載	產生警示的工作負載
日期與時間	警示的時間戳記
計劃	與警示相關的計劃 (若適用)
警示類別	依功能區域顯示的警示群組。如需詳細資訊，請參閱 "警示類型和類別" (第 218 頁)。
來源	警示的來源 – 系統或整合應用程式

注意事項
若選擇多欄，則可能需要水平捲動畫面，才能檢視所有可用的資訊。

隱藏快速篩選

若要隱藏快速篩選區段

1. 在 Cyber Protect 主控台中，移至 **[監控]** > **[警示]**。
2. 按一下快速篩選區段頂端的圖示。



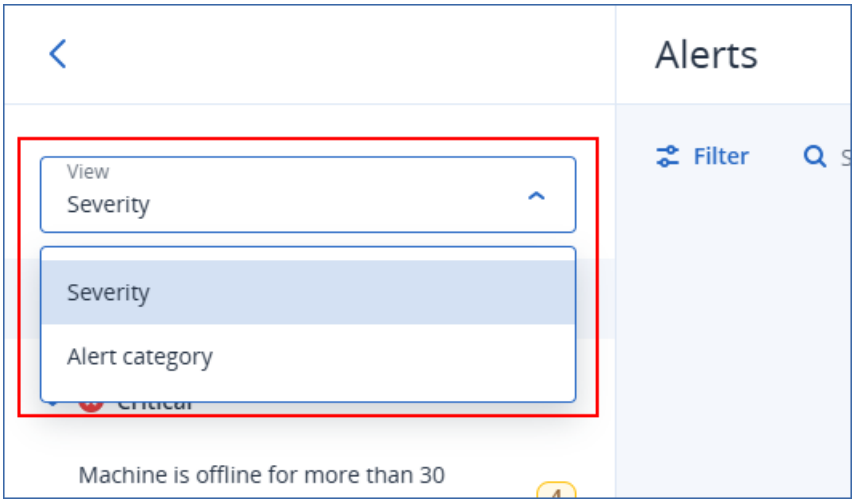
篩選警示

您可以使用快速篩選條件或主要篩選條件。

快速篩選條件

若要篩選警示

1. 在 Cyber Protect 主控台中，移至 **[監控]** > **[警示]**。
2. 在 **[檢視]** 下拉式清單中，選擇篩選條件。



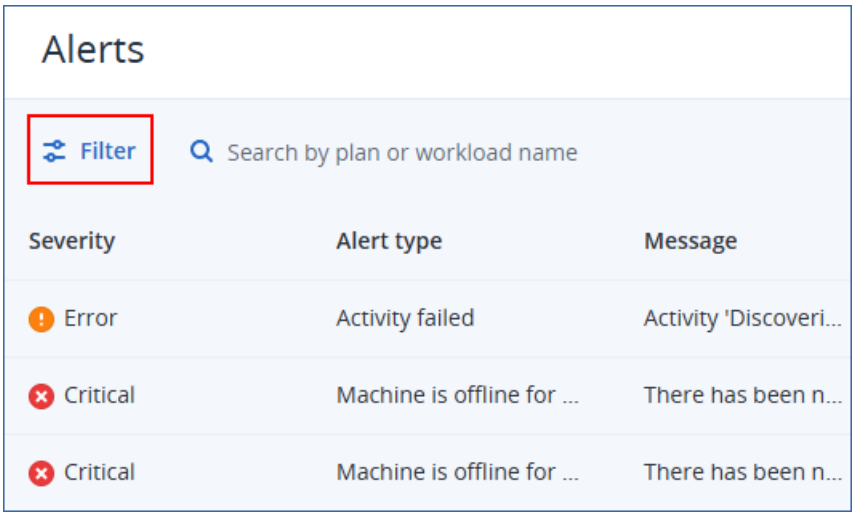
3. [選用] [若選擇 **[警示類別]**] 選擇特定的警示類別。
4. [選用] 選擇特定的警示類型。

結果，符合篩選條件的警示隨即列出。

主要篩選條件

若要篩選警示

1. 在 Cyber Protect 主控台中，移至 **[監控]** > **[警示]**。
2. 按一下 **[篩選]**。



3. 設定篩選條件，然後按一下 **[套用]**。

注意事項
可用的篩選條件取決於您可能已經設定的快速篩選設定。

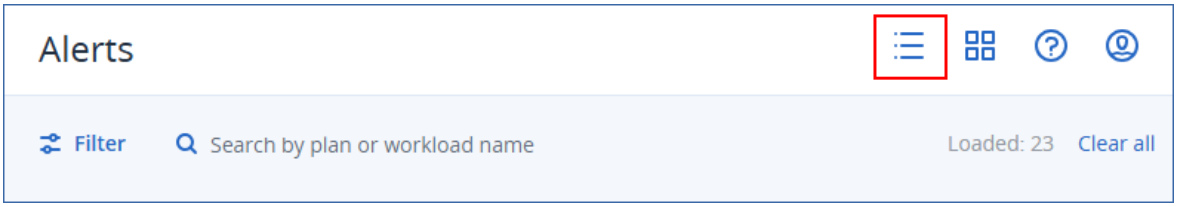
結果，符合篩選條件的警示隨即列出。

排序警示

使用表格檢視時，您可以依遞減或遞增順序排序警示。

若要排序警示

1. 在 Cyber Protect 主控台中，移至 **[監控]** > **[警示]**。
2. [若使用簡易檢視] 按一下表格檢視圖示。



3. 按一下您想要排序其中警示的欄的名稱。

注意事項
您無法按一下 **[訊息]** 欄來排序警示。

結果，警示隨即排序，並在所選欄名稱旁顯示一個箭頭。

警示類型和類別

警示類型依下列類別分組：

- 備份警示
- 災難復原警示
- 防惡意軟體防護警示

- 授權警示
- URL 篩選警示
- EDR 警示
- 裝置控制警示
- 系統警示
- 裝置探索警示

備份警示

警示類型	描述	解析警示的方式
備份失敗	當備份因可解決的錯誤而失敗，或因系統關閉而遭到中斷時，會產生警示。	檢查備份作業記錄：按一下工作負載加以選擇，按一下 **[活動]**，然後在記錄中找出警告。訊息應該會指出問題的根本原因。
備份成功，但出現警告	備份成功但出現警告時，會產生警示。	檢查轉換至 VM、複寫，或驗證計劃的記錄。作業期間的問題會產生「活動失敗」或「活動已完成，但出現警告」等警示。
已取消備份	每次使用者手動取消備份時，都會產生警示。	您可以按一下 **[立即執行]** 手動開始備份，或等到它在下次排程時間執行。
備份視窗關閉，備份已取消	當備份活動因不適合備份選項中指定的時段而錯過時，會產生警示。	在 **[效能與備份]** 視窗中重新設定排程或編輯備份計劃的選項。展開您產品的區段以獲得指示。
備份正在等候執行	發生排程衝突且有兩個備份工作同時起始時，會產生警示。在這種情況下，第二個備份工作會排入佇列，直到第一個工作完成或停止為止。	請確認備份在預期的時段內根據排程執行，且避免排程衝突。
備份沒有回應	當備份在一段時間內沒有顯示任何進度並且可能遭到凍結時，會產生警示。	此問題可能是由鎖定所造成。如需詳細資訊，請參閱本知識庫文章。
備份未開始執行	當排程備份出於未知原因無法啟動時，會產生警示。	請確認您使用的是 Acronis Backup 產品的最新組建。 • 如果可以在備份開始時間使用代理程式電腦： 1. 編輯備份工作開始時間。 2. 如果再次出現警示，請重新建立備份工作。 3. 如果新建立的備份工作也觸發了警示，請聯絡支援團隊尋求協助。 • 若代理程式離線：

警示類型	描述	解析警示的方式
		1. 備份時請勿關閉電腦。 2. 如果電腦未關閉，請確認 Acronis Managed Machine Service 正在執行：開始 -> 搜尋 -> services.msc -> 找出 Acronis Managed Machine Service。如果您需要協助，請聯絡支援團隊。
備份狀態不明	當備份代理程式在排定的備份時間離線時，會產生警示。在備份代理程式上線之前，資源備份狀態將為不明。	1. 檢查代理程式是否預期會離線(例如，當它是管理伺服器網路外的筆記本時)。 2. 如果代理程式不得離線，請確認 Acronis Managed Machine Service 正在執行：開始 -> 搜尋 -> services.msc -> 找出 Acronis Managed Machine Service 並檢查其狀態。如果服務已停止，則將其啟動。
備份遺失	當超過 [Days from last backup] 天未有成功的備份時，會產生警示。	
備份已損毀	當驗證活動成功且顯示備份已損毀時，會產生警示。	請依照疑難排解損毀備份問題一文中的步驟進行。 如果您在識別存檔損毀根本原因時需要協助，請聯絡支援團隊。
連續資料保護失敗	如果備份連續保護失敗，會產生警示。	檢驗下列限制： 1. 僅 NTFS 檔案系統和以下作業系統支援連續資料保護： • 桌面：Windows 7 和更新版本 • 伺服器：Windows Server 2008 R2 和更新版本 2. CDP 不支援將 **Acronis Secure Zone** 當作目的地。 3. 不支援掛載在 Windows 系統上的 NFS 資料夾。 4. 不支援持續複寫：如果保護計劃中有兩個位置，則只會在第一個目的地建立 CDP 片段，然後透過下次備份將變更複寫至第二個目的地。 5. 如果本機受保護資料夾中的變更是套用自網路來源 (例如，使用者自網路存取資料夾時)，CDP 不會偵測到

警示類型	描述	解析警示的方式
		變更。 6. 如果正在使用檔案 (例如，正在 Excel 檔案中進行變更)，CDP 不會偵測到變更。如果要讓 CDP 偵測到變更，請儲存變更並關閉檔案。
Hyper-V 主機設定無效	當有兩個或多個 Hyper-V 用代理程式安裝在主機名稱相同的 Hyper-V 主機上時 (相同的帳戶層級不支援此動作)，會產生警示。	請以帳戶的不同子單位註冊這些 Hyper-V 用代理程式，以避免衝突。
驗證失敗	無法完成備份的驗證程序時，會產生警示。	檢查錯誤操作記錄：按一下電腦加以選擇，按一下 **[活動]**，然後在記錄中找出警告。訊息應該會指出問題的根本原因。
無法將雲端存放區的備份轉換為新格式	當雲端儲存空間中的備份遷移到新格式失敗時，會產生警示。	如需有關 Acronis Cyber Backup Advanced 存檔遷移的詳細資訊，請參閱本知識庫文章。 如需有關 Acronis Cyber Backup 存檔遷移的詳細資訊，請參閱本知識庫文章。 在聯絡支援團隊之前，請使用 **migrate_archives** 工具執行以下命令以收集報告： `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 帳戶，`password` 是該帳戶的密碼。
缺少加密密碼	資料庫加密金鑰不正確、損毀或缺少該金鑰時，會產生警示。	若是遺失或忘記密碼，則無法復原加密的備份。您必須在受保護的裝置本機上設定加密密碼。您無法在保護計劃中設定加密密碼。如需詳細資訊，請參閱 設定加密密碼。
上傳等候中	如果排程檢查時發現此備份計劃的實體資料運送至雲端存檔並未上傳至儲存空間，會產生	

警示類型	描述	解析警示的方式
	警示。	
備份復原失敗	當您嘗試復原檔案或系統備份時，如果復原作業失敗，會產生警示。	找出備份失敗的確切日期，並嘗試使用上次的成功備份復原。

災難復原警示

警示類型	描述	解析警示的方式
超出儲存空間配額	當超過災難復原儲存的彈性配額時，會產生警示。	請增加配額或從雲端儲存空間移除部分備份。
配額已滿	當超出以下產品項目的彈性配額時，會產生警示： • 雲端伺服器。 • 計算點。 • 公共 IP 位址。	
已超出儲存空間配額	當超過災難復原儲存的固定配額時，會產生警示。 此儲存空間是由主要伺服器和復原伺服器使用。如果達到此配額的超額，則無法建立主要伺服器和復原伺服器，或者無法新增或延伸現有主要伺服器的磁碟。如果超過此配額的超額，則無法執行容錯移轉，或者無法只啟動已停止的伺服器。執行中的伺服器會繼續執行。	
已超出配額	當超出以下產品項目的固定配額時，會產生警示： • 雲端伺服器。 • 計算點。 • 公共 IP 位址。	請考慮購買額外的配額，或為不再需要保護的裝置停用備份工作。
容錯移轉錯誤	起始容錯移轉後發生系統問題時，會產生警示。	1. 選擇復原伺服器，然後按一下**[編輯]**。 2. 減少復原伺服器的 CPU/RAM。 3. 嘗試再次執行容錯移轉。
測試容錯移轉錯誤	起始測試容錯移轉後發生系統問題時，會產生警示。	1. 選擇復原伺服器，然後按一下**[編輯]**。 2. 減少復原伺服器的 CPU/RAM。

警示類型	描述	解析警示的方式
		3. 嘗試再次執行測試容錯移轉。 **注意事項** 請確認實際執行網路中的 IP 位址與在 DHCP 伺服器中設定的 IP 位址相同。
容錯回復錯誤	起始容錯回復後發生系統問題時，會產生警示。	您可以在備份儲存清單中見到錯誤位置：當中有編號而非名稱 (一般而言，位置名稱會與其中一個現有終端使用者名稱相符)，而且您尚未建立此位置。請移除錯誤位置： 1. 在 Cyber Protect 主控台中，移至 **[備份儲存]**。 2. 找到位置並按一下叉號 (x) 圖示以刪除。 3. 按一下 **[刪除]**，確認您的選擇。 4. 重試容錯移轉。
容錯回復已取消。	使用者取消容錯回復時，會產生警示。	手動解除主控台中的警示。
VPN 連線錯誤	當因使用者動作以外的原因導致 VPN 連線失敗時，會產生警示。來自 VPN 裝置的狀態報告已過期。	如果您在部署或連線 Acronis VPN 裝置時遇到問題，請聯絡支援團隊。 在您的電子郵件中註明以下資訊： • 錯誤訊息螢幕截圖 (如有) • Acronis VPN 裝置 CLI 介面的螢幕擷取畫面 • 您的 Acronis Backup Cloud 資料中心以及群組名稱。
(無法連線至 VPN) 無法連線至連線閘道	Disaster Recovery 服務無法連線至連線閘道時，會產生警示。來自連線閘道的狀態報告已過期。	如果您在部署或連線至 Acronis VPN 裝置時遇到問題，請聯絡支援團隊。 在您的電子郵件中註明以下資訊： • 錯誤訊息螢幕截圖 (如有) • Acronis VPN 裝置 CLI 介面的螢幕擷取畫面 • 您的 Acronis Backup Cloud 資料中心以及群組名稱
需要重新指派 DR IP	當 VPN 裝置偵測到網路變更時，會產生警示。	重新指派 IP 位址。如需詳細資訊，請參閱 "重新指派 IP 位址" (第 688 頁)

警示類型	描述	解析警示的方式
連線閘道失敗	當雲端 VPN 伺服器部署失敗時，會產生警示。	使用連線驗證工具並檢查其輸出是否有錯誤。 允許 Acronis 軟體透過應用程式控制您的防火牆和防惡意軟體。
主要伺服器建立失敗	因為錯誤而無法建立主要伺服器時，會產生警示。	
復原伺服器建立失敗	因為錯誤而無法建立復原伺服器時，會產生警示。	請確認復原伺服器符合軟體需求。如需詳細資訊，請參閱 "軟體需求" (第 655 頁)。
刪除主要伺服器	主要伺服器遭到刪除時，會產生警示。	
伺服器復原失敗	主要或復原伺服器無法復原時，會產生警示。	尋找詳細資料。如果錯誤訊息是一般錯誤或不明確 (例如「內部錯誤」)，請前往 **[災難復原]** → **[伺服器]**，按一下以選擇受影響的電腦，然後按一下 **[活動]**。按一下某個活動，按住 CTRL 的同時以滑鼠左鍵按一下該活動。按一下活動的省略符號 (...)，然後按一下 **[工作活動資訊]**。
備份失敗	雲端伺服器 (主要伺服器或處於實際運作容錯移轉狀態的伺服器) 備份失敗時，會產生警示。	1. 驗證與備份位置的連線。 2. 檢查備份儲存裝置 (本機備份)。
超過網路限制	已達到雲端網路數目上限 (5 個網路) 時，會產生警示。	
Runbook 失敗	Runbook 執行失敗時，會產生警示。	這不會影響產品功能，可以安心忽略。如需詳細資訊，請參閱 "建立 Runbook" (第 723 頁)。
Runbook 警告	Runbook 執行完成但出現警告時，會產生警示。	這不會影響產品功能，可以安心忽略。如需詳細資訊，請參閱 "建立 Runbook" (第 723 頁)。
需要 Runbook 使用者互動	Runbook 等待使用者互動時，會產生警示。	這不會影響產品功能，可以安心忽略。如需詳細資訊，請參閱 "建立 Runbook" (第 723 頁)。
網際網路流量遭到封鎖	網際網路流量遭到系統管理員封鎖時，會產生警示。	
網際網路流量已解除封鎖	網際網路流量由系統管理員解除封鎖時，會產生警示。	

警示類型	描述	解析警示的方式
區域網路重疊	偵測到相同或重疊的區域網路時，會產生警示。	
授權切換不足的伺服器配額	雲端伺服器配額不足時，會產生警示。	• 如果針對實體伺服器產生警示，請確認租用戶和使用者對 **Web 託管伺服器**或**伺服器**產品項目有足夠的配額。 • 如果針對虛擬伺服器產生警示，請確認租用戶和使用者對 **Web 託管伺服器**或**虛擬機器**產品項目有足夠的配額。虛擬伺服器無法使用**伺服器**產品項目的配額。
授權切換不足的產品項目	**災難復原儲存空間**產品項目遭到停用時，會產生警示。	
授權切換錯誤	災難復原升級發生錯誤時，會產生警示。	
授權切換不足的計算點	沒有可用的計算點時，會產生警示。	請增加**計算點**產品項目的固定配額。
授權切換不足的伺服器產品項目	**雲端伺服器**產品項目遭到停用時，會產生警示。	
原則無法建立復原伺服器	如果在設定災難復原基礎架構時發生錯誤，會產生警示。	請手動建立無**網際網路存取**屬性的復原伺服器。如需詳細資訊，請參閱 "建立復原伺服器" (第 694 頁)。
備份處理器自動測試容錯移轉已重新排定	自動測試容錯移轉遭到重新排程時，會產生警示。	
備份處理器自動測試容錯移轉已逾時	自動測試容錯移轉到期時，會產生警示。 **注意事項** 每個自動測試容錯移轉都會使用計算點。	
備份處理器自動測試容錯移轉整體失敗	復原伺服器上次排程的自動測試容錯移轉失敗時，會產生警示。	• 請手動啟動復原伺服器的測試容錯移轉。如需詳細資訊，請參閱 "執行測試容錯移轉" (第 707 頁)。 • 執行自動測試容錯移轉時，請等待下次排程的日期。
容錯回復資料傳輸錯誤	當容錯回復的資料傳輸階段失敗時，會產生警示。	
容錯回復失敗	容錯回復發生錯誤時，會產生警	您可以在備份儲存清單中見到錯誤

警示類型	描述	解析警示的方式
	示。	位置：當中有編號而非名稱（通常來說，位置名稱會與現有終端使用者名稱相符），且您尚未建立此位置。移除錯誤位置： 1. 在 Cyber Protection 中，移至 **[備份儲存]**。 2. 找到該位置，然後按一下叉號 (x) 圖示將其刪除。 3. 按一下 **[刪除]**，確認您的選擇。 4. 再次開始容錯移轉。
容錯回復確認失敗	容錯回復確認失敗時，會產生警示。	
容錯回復電腦已準備好轉換	當電腦準備好轉換時，會產生警示。	
容錯回復轉換已完成	轉換成功時，會產生警示。	手動解除主控台中的警示。
容錯回復目標代理程式離線	代理程式離線時，會產生警示。	

防惡意軟體防護警示

警示類型	描述	解析警示的方式
偵測到可疑的遠端連線活動	偵測到來自遠端連線的勒索軟體時，會產生警示。	手動解除主控台中的警示。
偵測到可疑的活動	工作負載中偵測到勒索軟體時，會產生警示。	手動解除主控台中的警示。以停用警示。 根據您在 Active Protection 計劃指定的選項停止惡意程序，該程序進行的變更會還原，如果尚未採取任何動作，您將需要手動解決問題。 讀取警示的詳細資料，以檢查哪項程序正在將檔案加密以及哪些檔案受到影響。 如果您決定要批准加密檔案的程序 (誤判警示)，請將此程序新增至受信任的程序： 1. 開啟 Active Protection 計劃。 2. 按一下**[編輯]**以修改以下設定。 3. 在 **[受信任的程序]** 中，指定將永遠不會被視為勒索軟體的受信任程序。指定程序可執行檔的完整路徑，其開頭為磁碟機代號。 例如：`C:\Windows\Temp\er76s7sdkh.exe`。

警示類型	描述	解析警示的方式
偵測到加密採礦活動	在工作負載中偵測到不當加密貨幣挖礦時，會產生警示。	手動解除主控台中的警示。
MBR 防禦：偵測到可疑的活動並暫停	在工作負載中偵測到勒索軟體 (尤其是 MBR/GPT 磁碟分割遭到勒索軟體修改) 時，會產生警示。	手動解除主控台中的警示。
已指定不支援的網路路徑	系統管理員提供的復原路徑並非本機資料夾路徑時，會產生警示。	指定網路資料夾保護的本機路徑 (復原路徑)。請手動解除主控台中的警示。
已新增為對 Active Protection 計劃有害的重要程序	當重要程序新增為保護排除項目清單中已封鎖的程序時，會產生警示。	手動解除主控台中的警示。
無法套用 Active Protection 原則	無法套用 Active Protection 原則時，會產生警示。	檢查錯誤訊息，以查看無法套用 Active Protection 原則的原因。
Secure Zone：偵測到未經授權的作業並加以封鎖	在工作負載中偵測到勒索軟體 (ASZ 磁碟分割遭到勒索軟體修改) 時，會產生警示。	手動解除主控台中的警示。
Active Protection 服務未執行	Active Protection 服務當機或未執行時，會產生警示。	檢查錯誤訊息，以查看 Active Protection 服務未執行的原因。
Active Protection 服務無法使用	驅動程式不相容或缺少驅動程式而使 Active Protection 服務無法使用時，會產生警示。	檢查 Windows 事件記錄中 Acronis Active Protection 服務的當機情形 (acronis_protection_service.exe)。
與另一個安全解決方案發生衝突	因為偵測到與另一個安全解決方案發生衝突，使電腦 '{{resourceName}}' 無法使用 Active Protection 時，會產生警示。若要啟用 Active Protection，請停用或解除安裝發生衝突的安全解決方案。	**解決方案 1**：如果您想要使用 Acronis 即時防護，請從工作負載解除安裝第三方防毒軟體。 **解決方案 2**：如果您想要使用協力廠商防毒軟體，請在套用至工作負載的保護計劃中，停用 Acronis 即時防護、URL 篩選以及 Windows Defender 防毒軟體。
隔離動作失敗	防惡意軟體無法隔離偵測到的惡意軟體時，會產生警示。	檢查錯誤訊息，以查看隔離失敗的原因。
´偵測到惡意程序	當行為引擎偵測到惡意軟體 (程序類型) 時，會產生警示。偵測到的惡意軟體會遭到隔離。	手動解除主控台中的警示。
偵測到惡意程序，但並未隔離	當行為引擎偵測到惡意軟體 (程序類型) 時，會產生警示。偵測到的惡意軟體未遭到隔離。	手動解除主控台中的警示。

警示類型	描述	解析警示的方式
偵測到惡意程式碼並加以封鎖 (ODS)	當排程掃描偵測到惡意軟體時，會產生警示。偵測到的惡意軟體會遭到隔離。	手動解除主控台中的警示。
偵測到惡意程式碼並加以封鎖 (RTP)	當即時防護偵測到惡意軟體時，會產生警示。偵測到的惡意軟體會遭到隔離。	手動解除主控台中的警示。
在備份中偵測到惡意程式碼	在備份掃描期間偵測到惡意軟體時，會產生警示。	手動解除主控台中的警示。
在即時反惡意程式碼保護與安全產品之間偵測到衝突	防惡意軟體無法向 Windows Security Center 註冊時，會產生警示。	請停用或解除安裝第三方安全產品，或停用保護計劃中的即時防惡意軟體防護。
無法執行 Microsoft Security Essentials 模組	當 Microsoft Security Essentials 模組無法執行時，會產生警示。	檢查錯誤訊息，以查看無法執行 Microsoft Security Essentials 模組的原因。
已安裝第三方防毒軟體，即時保護無法使用	由於第三方防毒軟體已啟用即時防護，因此在即時防護無法開啟時，會產生警示。	請停用或解除安裝第三方安全產品，或停用保護計劃中的即時防惡意軟體防護。
驅動程式不相容或缺少驅動程式，即時保護無法使用	當驅動程式不相容或缺少驅動程式而使即時防護無法使用時，會產生警示。	請檢查錯誤訊息以查看在工作負載上安裝驅動程式失敗的原因。
網路保護 (或 Active Protection) 服務沒有回應	當資安防護服務回應主控台的健全狀況檢查 ping 時，會產生警示。	手動解除主控台中的警示。
安全性定義更新失敗	安全性定義更新失敗時，會產生警示。	請檢查錯誤訊息以查看安全性定義更新失敗的原因。
竄改防護已啟用	由於竄改防護已啟用而無法變更 Microsoft Defender 設定時，會產生警示。	停用 Windows 工作負載中的竄改防護設定。
Windows Defender 模組執行失敗	Windows Defender 模組執行失敗時，會產生警示。	請檢查錯誤訊息以查看無法執行 Windows Defender 模組的原因。
Windows Defender 遭到協力廠商防毒軟體封鎖	由於電腦上安裝第三方防毒軟體而使 Windows Defender 遭到封鎖時，會產生警示。	請停用或解除安裝第三方安全產品。
群組原則衝突	由於受到群組原則控制而無法變更 Microsoft Defender 設定時，會產生警示。	請停用 Windows 工作負載上的群組原則設定。
Microsoft Security	Microsoft Security Essentials	手動解除主控台中的警示。

警示類型	描述	解析警示的方式
Essentials 防毒軟體已採取動作以保護此電腦免受惡意程式碼攻擊	刪除或隔離惡意軟體時，會產生警示。	
Microsoft Security Essentials 偵測到惡意程式碼	Microsoft Security Essentials 偵測到惡意軟體或其他可能不需要的軟體時，會產生警示。	手動解除主控台中的警示。

授權警示

警示類型	描述	解析警示的方式
幾乎達到儲存空間配額	使用量低於 80% (清理或配額升級後) 時，會產生警示。	請購買額外的儲存空間，或釋出雲端儲存的空間。
已超出儲存空間配額	當使用全部 100% 儲存空間配額時，會產生警示。	請購買更多的儲存空間。如需詳細資訊，請參閱本知識庫文章。
已達到工作負載配額	當產品項目用量 > 0 且使用量 > 配額，但使用量 <= 配額 + 超額時，會產生警示。	
已超過工作負載配額	當產品項目的使用量 > 配額 + 超額時，會產生警示。	
工作負載沒有套用備份計劃的配額 (資源沒有服務配額)	發生以下情形時，會產生警示： • 配額已手動移除：**[裝置]** > **[詳細資訊]** > **[服務配額]**，然後按一下 **[變更]** 並選擇 **[無配額]** 選項。 • **Management Console** 產品項目遭到停用。 • 產品項目的 **Management Console** 配額 + 超額值降至目前使用量以下。	
無法使用指派的配額保護工作負載	產品項目不足且您需要以下項目時，會產生警示： • 動態群組。 • 指派至該群組的備份計劃。 • 屬於該動態群組的資源，但資源中有部分性質禁止對其套用相同的備份計劃。	
訂購授權已過期	當授權過期時，會產生警示。	訂閱到期後，除了復原外的所有產品功能都將遭到封鎖，直到續訂訂閱為止。已備份的資料仍可供存取以進行復原。

警示類型	描述	解析警示的方式
		購買新授權。 **注意事項** 如果您最近購買了新訂閱，但仍收到訂閱已過期的訊息，請從 Acronis 帳戶中匯入新訂閱：在管理主控台中，移至 **[設定]** -> **[授權]**，然後按一下右上角的 **[同步]**。訂閱將會同步。
訂購授權即將到期	如果授權將在 30 天內過期，會產生警示。	購買新的訂閱。

URL 篩選警示

警示類型	描述	解析警示的方式
已封鎖惡意 URL	惡意 URL 遭到 URL 篩選封鎖時，會產生警示。	檢查 URL 篩選設定。URL 篩選會根據 URL 篩選設定，封鎖應封鎖的頁面。如需詳細資訊，請參閱 "URL 篩選" (第 753 頁)。
已忽略惡意 URL 警告	當您選擇繼續前往遭到 URL 篩選封鎖的惡意 URL 時，會產生警示。	檢查 URL 篩選設定。
在 URL 篩選與安全產品之間偵測到衝突	當 URL 篩選因為與其他安全產品衝突而無法啟用時，會產生警示。	檢查 URL 篩選設定。
網站 URL 遭到封鎖	當 URL 符合在 URL 篩選封鎖類別中指定的所有準則時，會產生警示。	檢查 URL 篩選設定。

EDR 警示

警示類型	描述	解析警示的方式
偵測到事件	當建立事件或現有事件的狀態更新時，會產生警示。	此警示會通知您有新事件或舊事件已更新。您可以檢視警示並將其關閉。您可以選擇開啟事件以便進一步調查。
偵測到入侵指標 (IOC)	EDR IOC 威脅搜尋服務偵測到新的入侵指標時，會產生警示。	此警示通知您一或多個工作負載中偵測到 IOC。您將檢視警示，然後可以按一下警示中的連結檢視 IOC 相關詳細資訊。

警示類型	描述	解析警示的方式
無法從網路隔離工作負載	當使用者觸發將電腦自網路隔離的動作，且隔離動作失敗時，會產生警示。	採取必要動作。
無法將工作負載重新連線至網路	當使用者觸發將電腦重新連回網路的動作，且動作失敗時，會產生警示。	採取必要動作。
Windows Defender 防火牆設定遭到修改	當已隔離電腦上的防火牆設定遭到修改時，會產生警示。	此警示會通知您遭隔離電腦的防火牆詳細資訊遭修改。這僅供參考，檢視後即可關閉警示。

裝置控制警示

警示類型	描述	解析警示的方式
裝置控制與資料外洩防禦將以有限的功能執行 (偵測到不相容的 CPU)	在 CPU 支援 CET 技術的實體機器上啟動 DeviceLock 代理程式時，會產生警示。	請停用受影響電腦上的選項以避免產生這些警示。
macOS Ventura 尚不支援裝置控制功能	當 DeviceLock 代理程式在 macOS Ventura 實體機器上啟動，且包含 [裝置控制] 的保護計劃套用至代理程式時，會產生警示。僅適用於因為 DeviceLock 驅動程式而有核心緊急情況問題的版本。	
允許傳輸敏感資料	允許傳輸敏感內容時，會產生警示。	
合理傳輸敏感資料	證明傳輸敏感內容時，會產生警示。	
拒絕傳輸敏感資料	阻止傳輸敏感內容時，會產生警示。	
檢閱資料洩漏防禦觀察模式的結果	必須檢閱觀察結果時，會產生警示： • Advanced DLP 套件授權未套用。 • 自從在套用到至少一個工作負載的任何保護計劃中啟用觀察模式以來，已經過一個月。 • 自上次提出類似警示，且在觀察模式下偵測到部份 DLP 使用量以來，已經過一個月。	
使用者的安全性識別碼已變更	當更新已知使用者名稱的 SID 時，會產生警示。在非網域工作負載上重新安裝作業系統時，可能會發生這種情況。	
週邊裝置存取遭到封鎖	受支援裝置的部分動作 (讀取 / 寫入	

警示類型	描述	解析警示的方式
	作業) 遭到封鎖時，會產生警示。	
無法連線到遠端 SSL 資源。	當對遠端 SSL 資源的存取因資源上使用的其他交握防禦而遭到封鎖時，會產生警示。	將資源新增到遠端主機的允許名單中。

系統警示

警示類型	描述	解析警示的方式
代理程式已過期	代理程式版本過期時，會產生警示。	請移至 [代理程式] 清單，並開始更新代理程式。
自動更新失敗	當代理程式自動更新失敗時，會產生警示。	請嘗試執行手動更新。
您需要在安裝新代理程式之後重新啟動裝置	當成功遠端安裝後需要重新啟動時，會產生此警示。	請重新啟動工作負載。
活動失敗	活動失敗時，會產生警示。	請重新啟動工作負載上的所有 Acronis 服務。
活動成功，但出現警告	活動成功但產生部分警告時，會產生警示。	
活動沒有回應	進行中的活動沒有回應時，會產生警示。	
計劃部署失敗	保護計劃部署失敗時，會產生警示。	
無法將使用者名稱轉換為 SID	排程 SID 轉換失敗時，會產生警示。	

裝置探索警示

警示類型	描述
已探索到新裝置	這是在區域網路的裝置探索掃描探索到新的未註冊裝置時產生的資訊性警示。 此警示包含 **[檢視探索到的裝置]** 連結，可開啟新探索到的裝置清單。

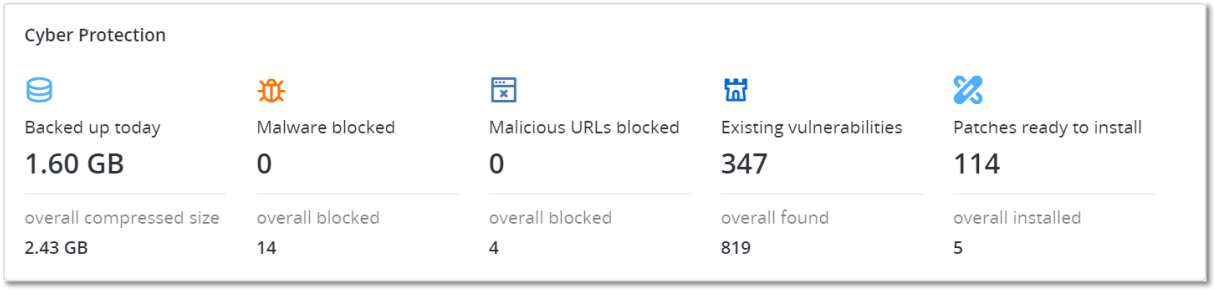
警示桌面小工具

在警示桌面小工具中，您可以查看下列與工作負載相關警示的詳細資料：

欄位	描述
5 個最新的警示桌面小工具	5 個最新警示的清單。
歷史警示摘要	依警示嚴重性、警示類型和時間範圍顯示警示的圖形桌面小工具。
作用中警示摘要	依警示嚴重性和警示類型以及作用中警示的加總顯示作用中警示的圖形桌面小工具。
警示歷程記錄	歷史警示的表格檢視。
作用中警示詳細資料	作用中警示的表格檢視。

網路保護

此桌面小工具會顯示有關備份大小、已封鎖之惡意程式碼、已封鎖之 URL、已發現之弱點，以及已安裝之修補程式的整體資訊。



上排會顯示目前的統計資料：

- **今天備份的資料** – 過去 24 小時的復原點大小總和
- **已封鎖的惡意程式碼** – 已封鎖之惡意程式碼目前作用中警示的數目
- **已封鎖的 URL** – 已封鎖之 URL 目前作用中警示的數目
- **現有的弱點** – 目前現有弱點的數目
- **已準備好安裝的修補程式** – 要安裝之目前可用修補程式的數目

下排會顯示整體的統計資料：

- 所有備份的壓縮大小
- 所有電腦中已封鎖之惡意程式碼的累積數目
- 所有電腦中已封鎖之 URL 的累積數目
- 所有電腦中已發現之弱點的累積數目
- 所有電腦中已安裝之更新/修補程式的累積數目

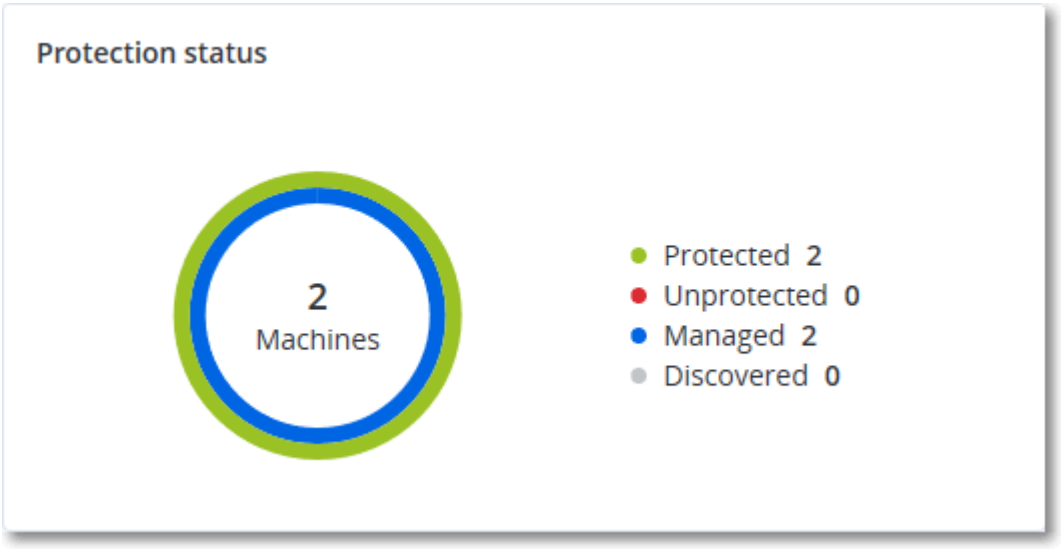
保護狀態

此桌面小工具會顯示所有電腦目前的保護狀態。

電腦可以為下列狀態之一：

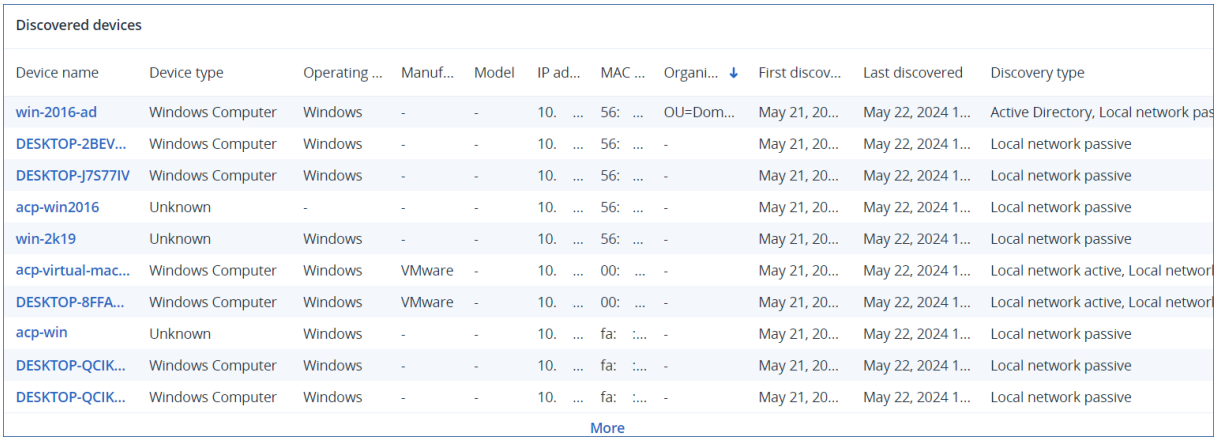
- **受保護** – 已套用保護計劃的電腦。
- **未受保護** – 未套用保護計劃的電腦。這些包括已發現和受管理，但未套用保護計劃的電腦。
- **受管理** – 已安裝保護代理程式的電腦。
- **已發現** – 未安裝保護代理程式的電腦。

如果您按一下電腦狀態，系統會將您重新導向至具有此狀態之電腦的清單以取得詳細資訊。



已探索到的裝置

此動態小工具會顯示在組織網路中探索到的裝置的詳細資訊。



Endpoint Detection and Response (EDR) 桌面小工具

Endpoint Detection and Response (EDR) 包含 7 個桌面小工具，全部都可以從 **[概觀]** 儀表板存取，其中三個桌面小工具預設也會顯示在 EDR 功能中 (請參閱 "檢閱事件" (第 798 頁))。

可用的 7 個桌面小工具包括：

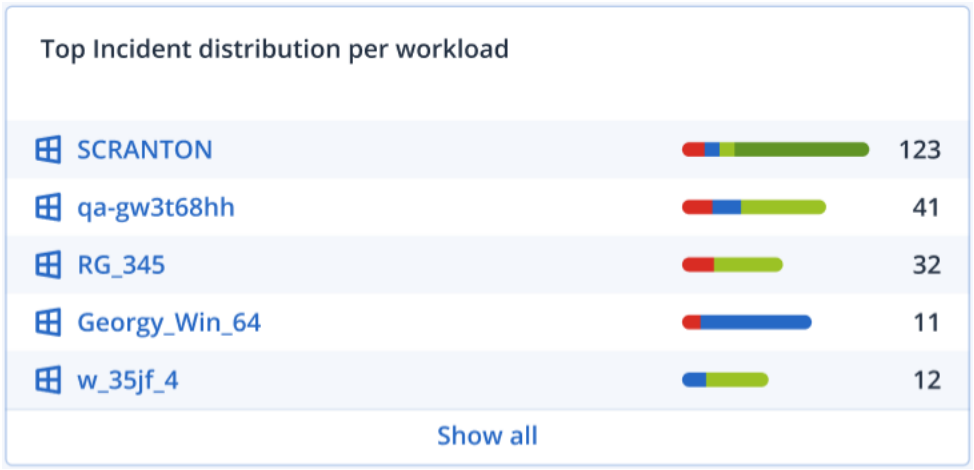
- 每個工作負載的最高事件分佈
- 威脅狀態 (顯示在 EDR 中)

- 事件嚴重性歷程記錄 (顯示在 EDR 中)
- 安全性事件 MTTR
- 安全性事件待執行工作
- 手法偵測 (顯示在 EDR 中)
- 工作負載網路狀態

每個工作負載的最高事件分佈

此桌面小工具會顯示包含最多事件的前五個工作負載 (按一下 **[全部顯示]** 可重新導向至根據桌面小工具設定篩選的事件清單)。

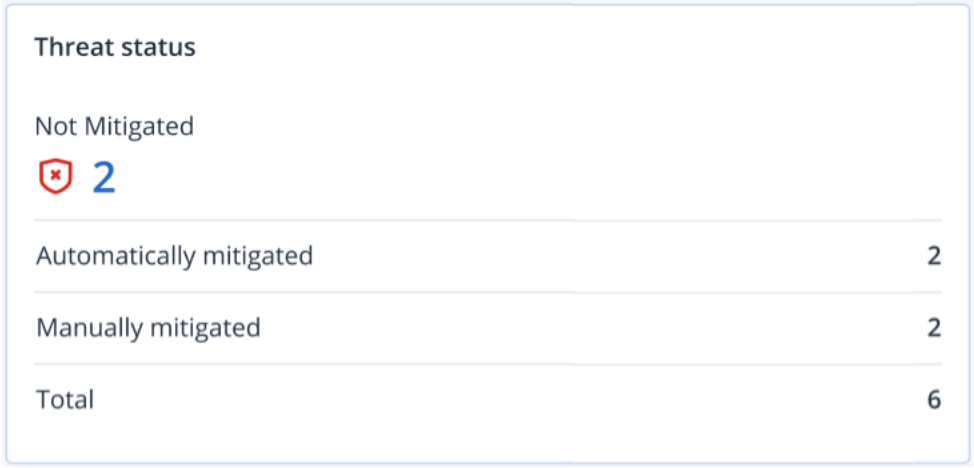
將滑鼠暫留在某個工作負載列上可檢視目前事件調查狀態的明細;這些調查狀態包括 **[未開始]**、**[調查中]**、**[已結案]** 以及 **[誤報]**。接著,按一下您要進一步分析的工作負載;系統會根據桌面小工具設定,重新整理事件清單。



威脅狀態

此桌面小工具會顯示所有工作負載的目前威脅狀態,並醒目提示未緩解而且需要調查的目前事件數目。此桌面小工具也會指出已緩解 (系統手動和/或自動) 的事件數目。

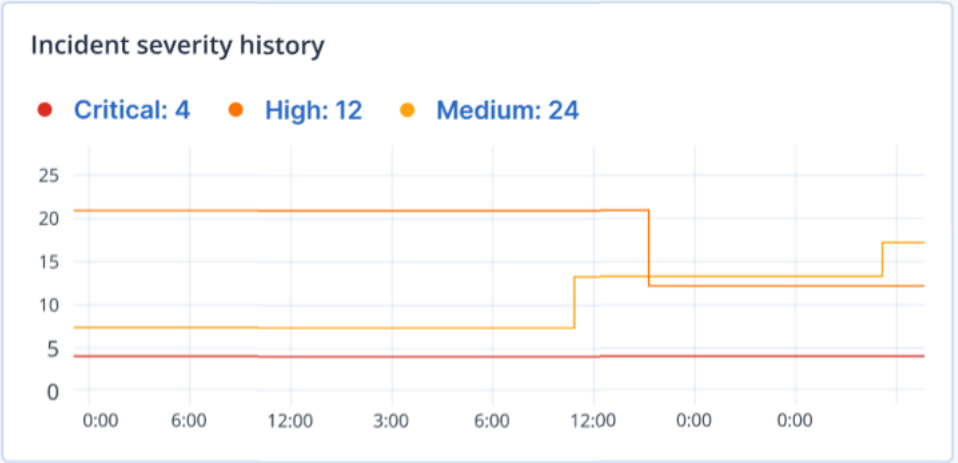
按一下 **[未緩解]** 數字可顯示篩選過的事件清單,以顯示未緩解的事件。



事件嚴重性歷程記錄

此桌面小工具會依嚴重性顯示攻擊的演變，而且可以指出攻擊活動。看到尖峰時，這可能表示此組織正受到攻擊。

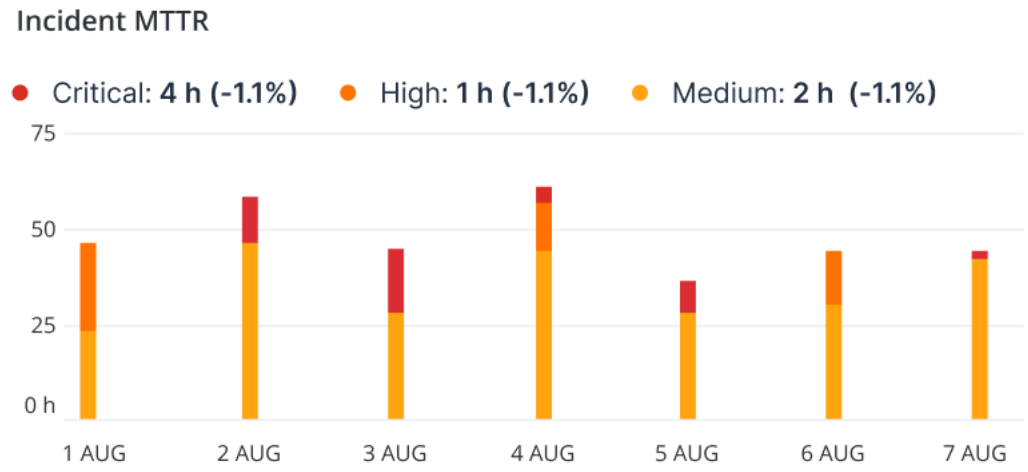
將滑鼠暫留在圖表上可檢視過去 24 小時 (預設期間) 內特定時間事件歷程記錄的明細。如果您想要檢視相關事件的清單，請按一下嚴重性層級 (**[重大]**、**[高]** 或 **[中]**)，系統就會將您重新導向至預先篩選的事件清單，其中包含符合所選嚴重性層級的事件。



安全性事件 MTTR

此桌面小工具會顯示安全性事件的平均解決時間。它會指出調查並解決事件的速度。

按一下某個欄可根據嚴重性 (**[重大]**、**[高]** 和 **[中]**) 檢視事件的明細，以及解決不同嚴重性層級所需的時間。顯示在括號中的 % 值表示與前一段時間相比增加或減少。

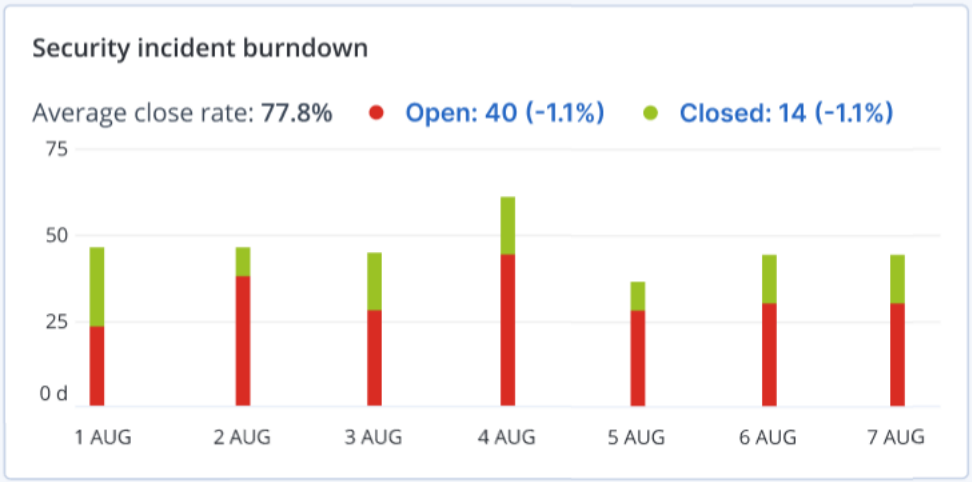


安全性事件待執行工作

此桌面小工具會顯示將事件結案的效率；未結案事件的數目是根據一段時間內已結案事件的數目來衡量的。

將滑鼠暫留在某個欄上可檢視所選日期已結案和未結案事件的明細。如果您按一下 [未結案] 值，便會顯示事件清單，經過篩選後，即可顯示目前未結案 (處於 **[調查中]** 或 **[未開始]** 狀態) 的事件。如果您按一下 [已結案] 值，便會事件清單，經過篩選後，即可顯示不再是未結案 (處於 **[已結案]** 或 **[誤報]** 狀態) 的事件。

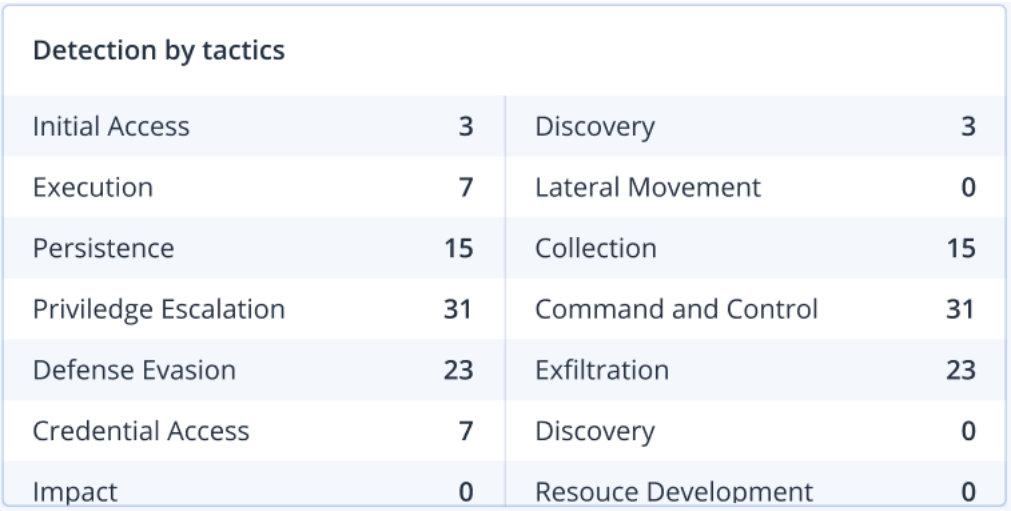
顯示在括號中的 % 值表示與前一段時間相比增加或減少。



手法偵測

此桌面小工具會顯示所選期間在事件中找到的特定攻擊手法的次數。

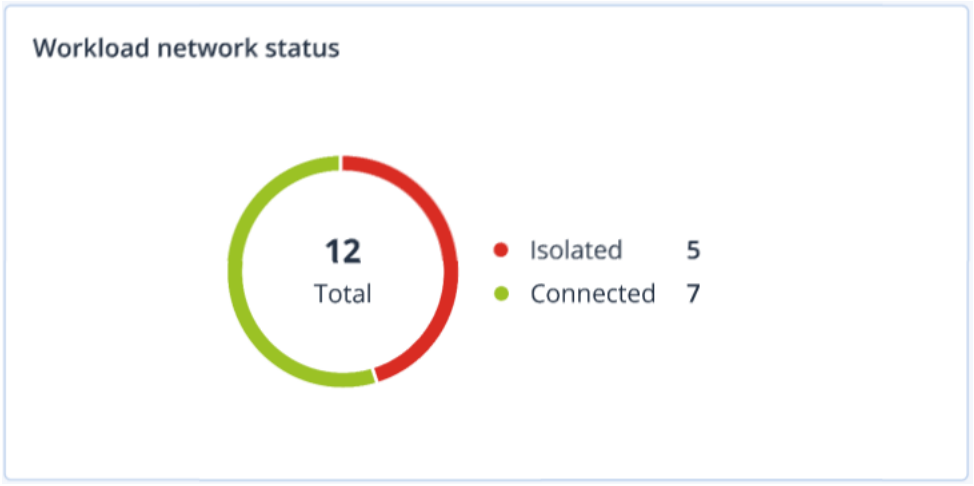
綠色和紅色的值表示與上一個時段相比是增加還是減少。在以下的範例中，[權限提升] 及 [命令和控制] 攻擊與上一個時段相比有所增加；這可能表示需要分析您的認證管理並增強安全性。



工作負載網路狀態

此桌面小工具會顯示您工作負載的目前網路狀態，並指出工作負載隔離的數目以及連線的數目。

按一下 [已隔離] 值可檢視 [含代理程式的工作負載] 清單 (在 主控台中的 **[工作負載]** 功能表下)，經過篩選後可顯示已隔離的工作負載。按一下 [已連線] 值可檢視 [含代理程式的工作負載] 清單，經過篩選後可顯示已連線的工作負載。



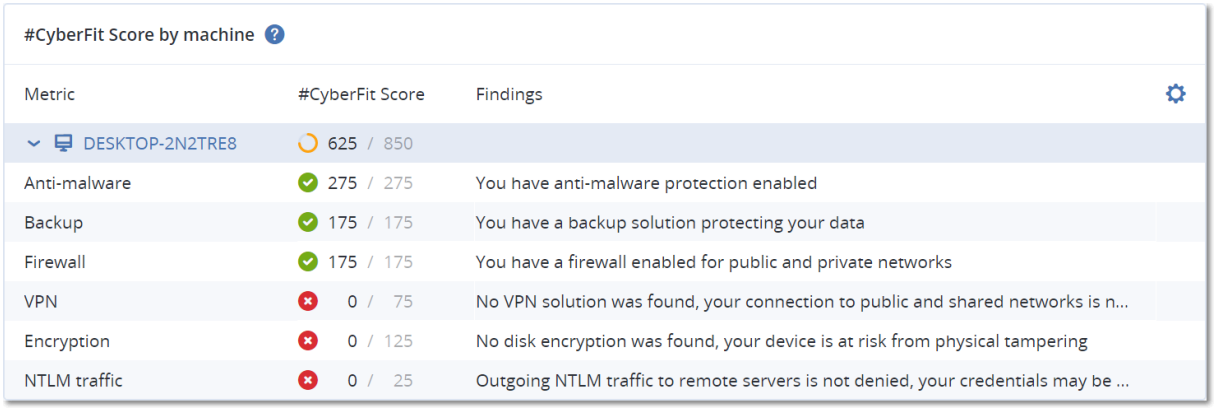
依電腦分類的 #CyberFit 分數

此桌面小工具可針對每部電腦顯示 #CyberFit 總分、其綜合分數，以及每個評估指標的結果：

- 反惡意程式碼
- 備份
- 防火牆
- VPN
- 加密
- NTLM 流量

若要提高每個指標的分數，您可以檢視報告中提供的建議。

如需有關 #CyberFit 分數的詳細資訊，請參閱「電腦的 #CyberFit 分數」。



磁碟健全狀況監控

「磁碟健全狀況監控」提供目前磁碟健全狀況狀態及其預測的相關資訊，讓您可以防止可能與磁碟故障相關的資料洩漏。HDD 和 SSD 磁碟都受到支援。

限制

- 僅執行 Windows 的電腦支援磁碟健全狀況預測。
- 只有實體機器的磁碟受到監控。虛擬機器的磁碟無法受到監控，而且不會顯示在磁碟健全狀況桌面小工具中。
- 不支援 RAID 設定。磁碟健全狀況桌面小工具不包含實作 RAID 之電腦的任何相關資訊。
- 不支援 NVMe SSD。
- 不支援外接式儲存裝置。

磁碟健全狀況以下列其中一種狀態表示：

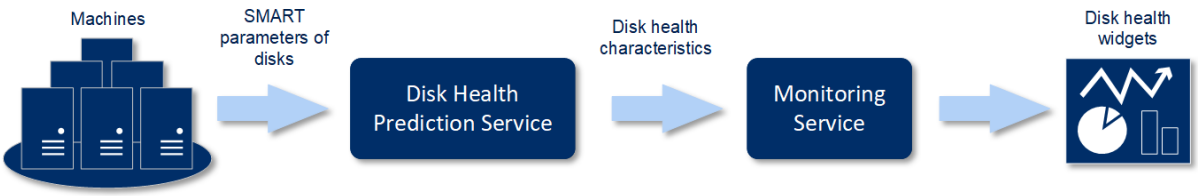
- **正常**
  磁碟健全狀況介於 70% 到 100% 之間。
- **警告**
  磁碟健全狀況介於 30% 到 70% 之間。
- **重大**
  磁碟健全狀況介於 0% 到 30% 之間。
- **正在計算磁碟資料**
  目前的磁碟狀態和預測正在計算中。

運作原理

磁碟健全狀況預測服務使用以 AI 為基礎的預測模型。

1. 保護代理程式會收集磁碟的 SMART 參數，並將此資料傳遞給磁碟健全狀況預測服務：
   - SMART 5 – 重新配置的磁區計數。
   - SMART 9 – 開機時數。
   - SMART 187 – 報告的無法更正錯誤數。
   - SMART 188 – 命令逾時。
   - SMART197 – 目前擱置中的磁區計數。
   - SMART 198 – 離線的無法更正磁區計數。
   - SMART 200 – 寫入錯誤率。
2. 磁碟健全狀況預測服務會處理收到的 SMART 參數、進行預測，然後提供下列磁碟健全狀況特徵：
   - 磁碟健全狀況目前狀態：正常、警告、嚴重。
   - 磁碟健全狀況預測：負面、穩定、正面。
   - 磁碟健全狀況預測機率 (百分比)。

   預測期間為一個月。
3. 監控服務會收到這些特徵，然後在 Cyber Protect 主控台的磁碟健全狀況桌面小工具中顯示相關的資訊。



磁碟健全狀況桌面小工具

磁碟健全狀況監控的結果會顯示在 Cyber Protect 主控台中提供的下列桌面小工具內。

- **磁碟健全狀況概觀**是一個樹狀圖桌面小工具，其中包含可以透過查找切換的兩個詳細資料層級。
  - 電腦層級
    針對選取的客戶電腦，顯示磁碟健全狀況狀態的摘要資訊。只有最嚴重的磁碟狀態才會顯示。當您將滑鼠暫留在特定區塊時，工具提示中會顯示其他狀態。電腦區塊大小取決於電腦所有磁碟的大小總計。電腦區塊色彩取決於所發現的最關鍵磁碟狀態。

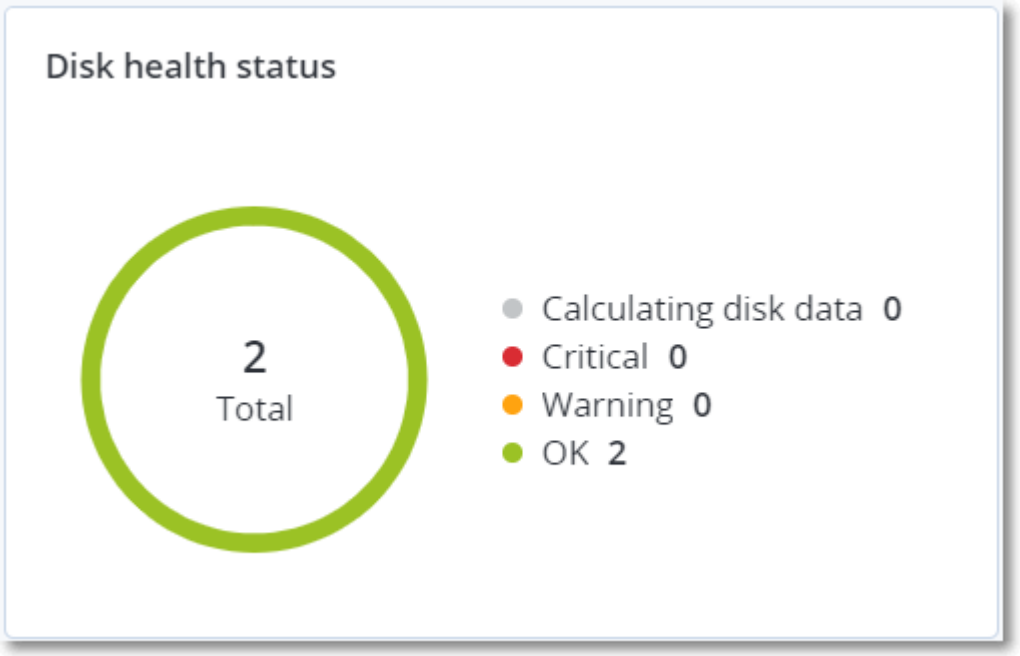
    

  - 磁碟層級
    針對所選電腦，顯示所有磁碟目前的磁碟健全狀況狀態。每個磁碟區塊都會顯示下列其中一

個磁碟健全狀況預測及其機率 (百分比):

- 將降級
- 將保持穩定
- 將改善

- **磁碟健全狀況狀態**是一個圓形圖桌面小工具，可顯示每個狀態的磁碟數。



磁碟健全狀況狀態警示

磁碟健全狀況檢查每 30 分鐘執行一次，而對應的警示則一天產生一次。當磁碟健全狀況從 **[警告]** 變更為 **[重大]** 時，一律會產生警示。

警示名稱	嚴重性	磁碟健全狀況狀態	描述
磁碟可能故障	警告	(30 – 70)	此電腦上的 <磁碟名稱> 磁碟之後可能會故障。請儘速對此磁碟執行完整映像備份、更換該磁碟，然後將映像復原到新的磁碟。
磁碟故障即將發生	重大	(0 – 30)	此電腦上的 <磁碟名稱> 磁碟處於嚴重狀態，很可能很快就會發生故障。目前不建議對此磁碟執行映像備份，因為增加的壓力可能會使磁碟故障。請立即備份此磁碟上最重要的檔案，然後更換該磁碟。

資料保護圖

注意事項
此功能適用於 Advanced Backup 套件。

資料保護圖功能可讓您探索對您重要的所有資料，並在樹狀圖的可擴充檢視中，取得所有重要檔案的數目、大小、位置、保護狀態等資訊。

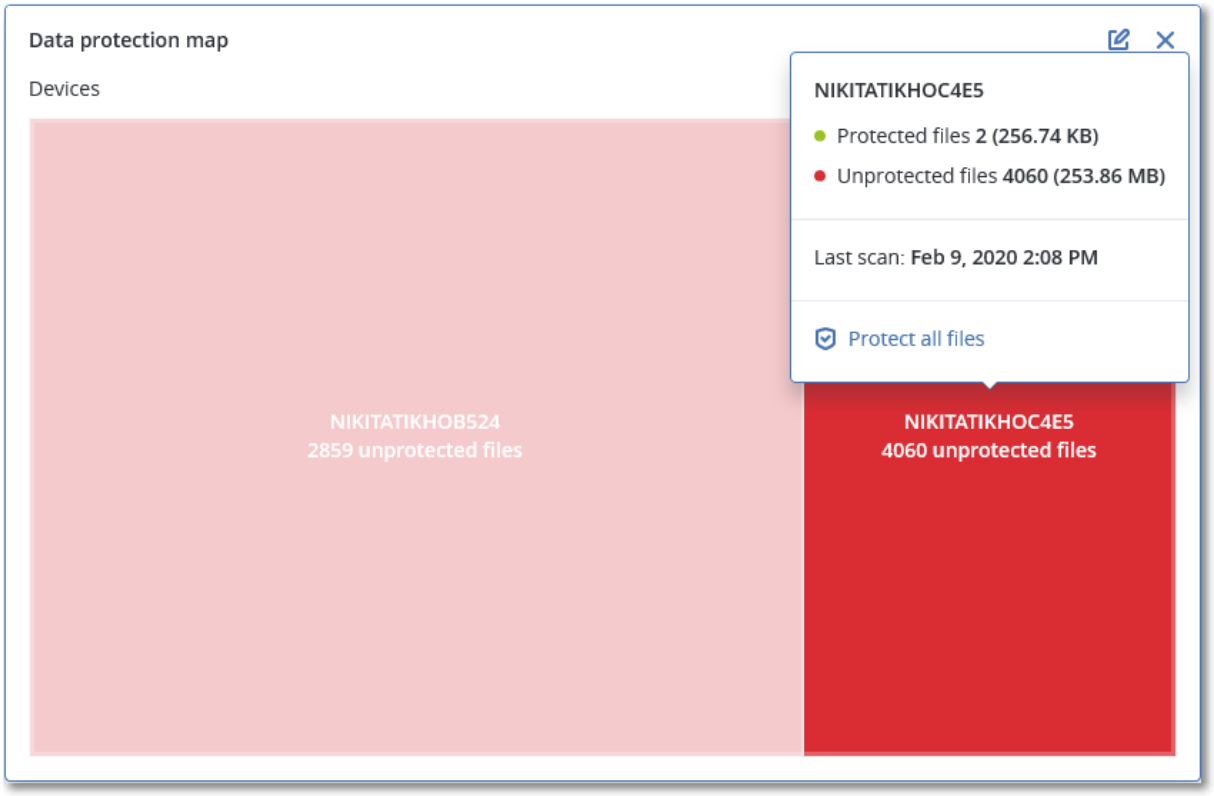
每個區塊大小取決於客戶/電腦所屬所有重要檔案的總數/大小總計。

檔案可以擁有以下保護狀態之一：

- **重大** – 有 51-100% 具有您指定之副檔名的未受保護檔案未針對所選電腦/位置進行備份，而且將不會以現有的備份設定進行備份。
- **低** – 有 21-50% 具有您指定之副檔名的未受保護檔案未針對所選電腦/位置進行備份，而且將不會以現有的備份設定進行備份。
- **中** – 有 1-20% 具有您指定之副檔名的未受保護檔案未針對所選電腦/位置進行備份，而且將不會以現有的備份設定進行備份。
- **高** – 具有您指定之副檔名的所有檔案都針對所選電腦/位置受到保護 (備份)。

資料保護檢查的結果可以在資料保護圖桌面小工具 (顯示電腦層級詳細資料的樹狀圖桌面小工具) 的監控儀表板上找到：

- 電腦層級 – 針對所選客戶的每部電腦，顯示重要檔案保護狀態的相關資訊。

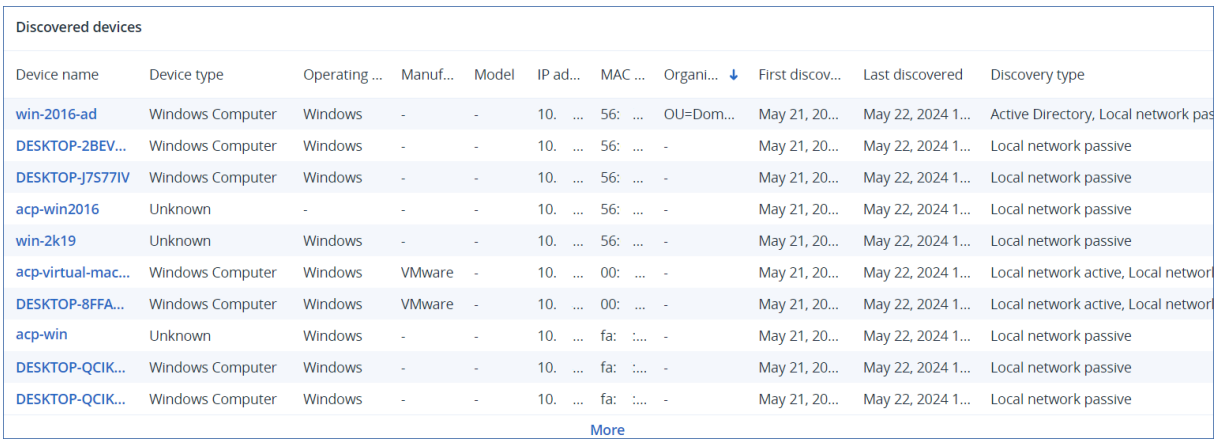


若要保護未受保護的檔案，請將滑鼠移至該區塊，然後按一下 **[保護所有檔案]**。在對話視窗中，您可以找到未受保護檔案數目及其位置的相關資訊。若要保護這些檔案，按一下 **[保護所有檔案]**。

您也可以下載 CSV 格式的詳細報告。

探索到的裝置動態小工具

[探索到的裝置] 表格動態小工具會顯示組織網路中透過主動式掃描和被動式掃描探索到的裝置的詳細資訊。裝置資訊包括裝置類型、製造商、作業系統、IP 位址、MAC 位址、探索日期等。



弱點評估桌面小工具

易受攻擊的電腦

此桌面小工具會依弱點嚴重性顯示易受攻擊的電腦。

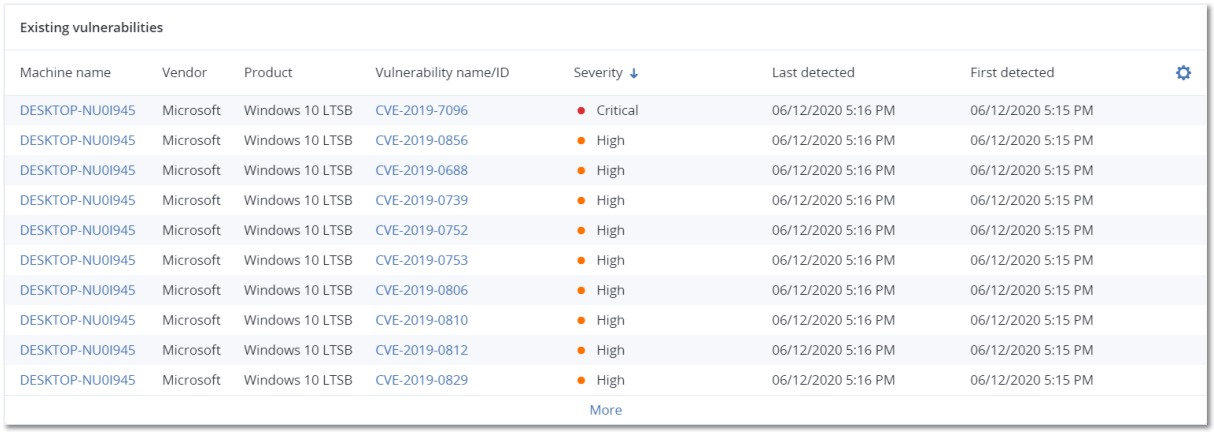
根據通用弱點評分系統 (CVSS) v3.0, 發現的弱點可以擁有以下嚴重性層級之一:

- 受保護:找不到弱點
- 重大:9.0 - 10.0 CVSS
- 高:7.0 - 8.9 CVSS
- 中:4.0 - 6.9 CVSS
- 低:0.1 - 3.9 CVSS
- 無:0.0 CVSS

現有的弱點

此桌面小工具會顯示電腦上目前現有的弱點。在 **[現有的弱點]** 桌面小工具中, 有兩欄顯示時間戳記:

- **第一次偵測到的** – 最初在電腦上偵測到弱點的日期和時間。
- **上次偵測到的** – 上次在電腦上偵測到弱點的日期和時間。



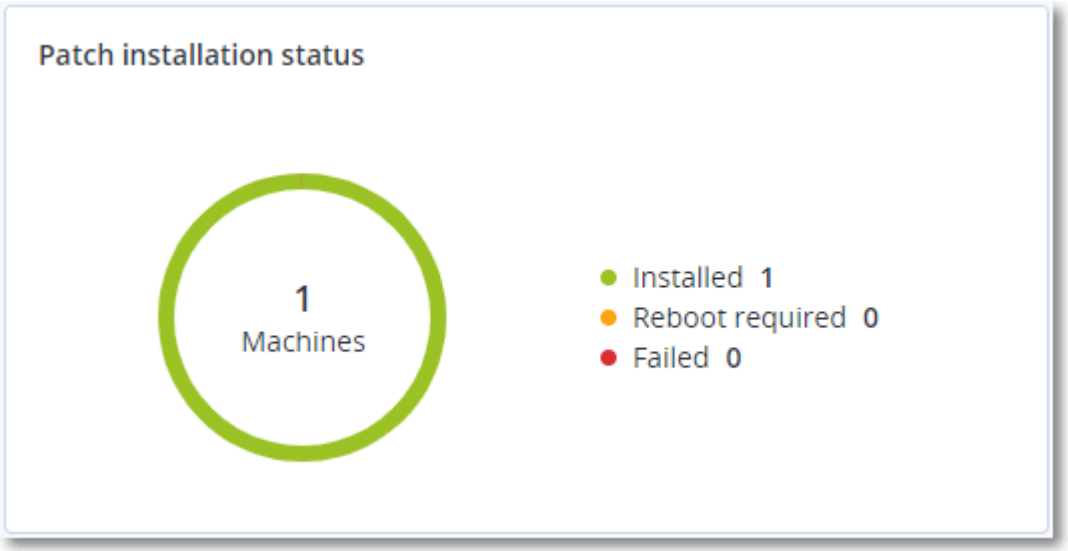
修補程式安裝桌面小工具

有四個與修補程式管理功能相關的桌面小工具。

修補程式安裝狀態

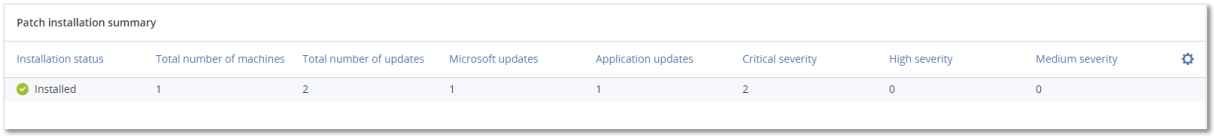
此桌面小工具會顯示依修補程式安裝狀態分組的電腦數目。

- **已安裝** – 電腦上已安裝所有可用的修補程式
- **需要重新開機** – 修補程式安裝之後，電腦需要重新開機
- **失敗** – 在電腦上安裝修補程式失敗



修補程式安裝摘要

此桌面小工具會在電腦上顯示依修補程式安裝狀態排列的修補程式摘要。



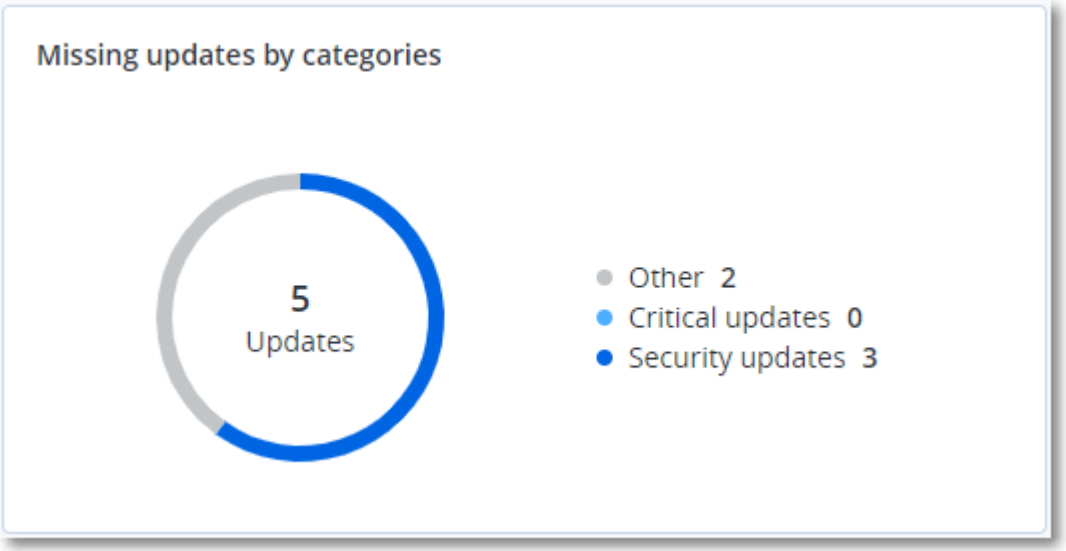
修補程式安裝歷史記錄

此桌面小工具會顯示電腦上修補程式的詳細資訊。

遺漏的更新 (依類別)

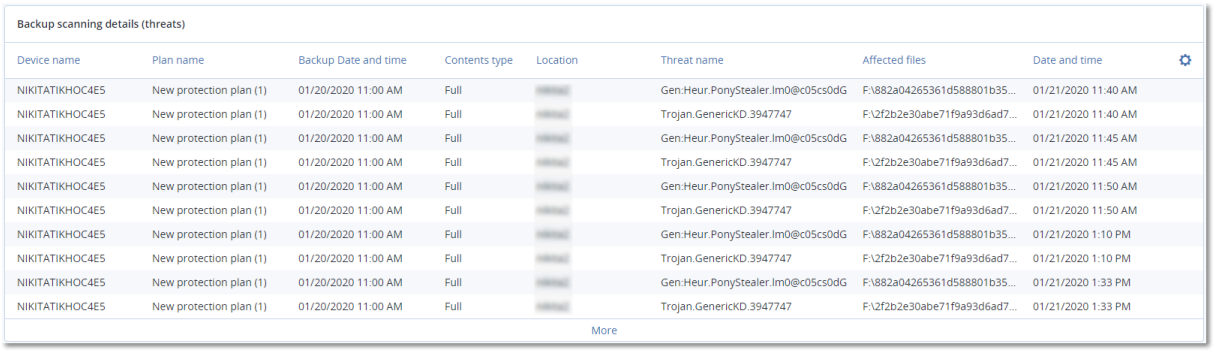
此桌面小工具會依類別顯示遺漏的更新數目。顯示下列類別：

- 安全性更新
- 重大更新
- 其他



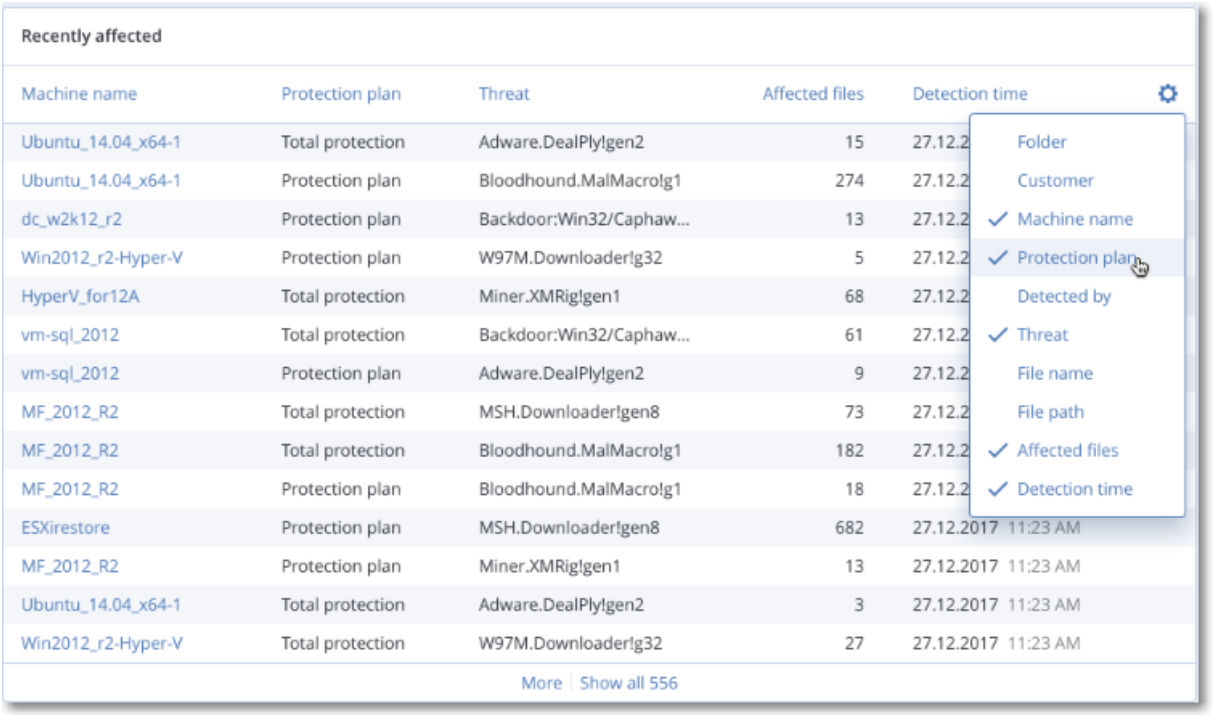
備份掃描詳細資料

此桌面小工具會顯示備份中偵測到之威脅的詳細資訊。



最近受影響

此桌面小工具會顯示受到病毒、惡意程式碼和勒索軟體之類威脅影響的工作負載的詳細資訊。您可以找到的相關資訊包括偵測到的威脅、偵測到威脅的時間，以及受感染檔案數目。



下載最近受影響工作負載的資料

您可以下載最近受影響工作負載的資料、產生 CSV 檔案，然後將其傳送給您指定的收件者。

若要下載最近受影響工作負載的資料

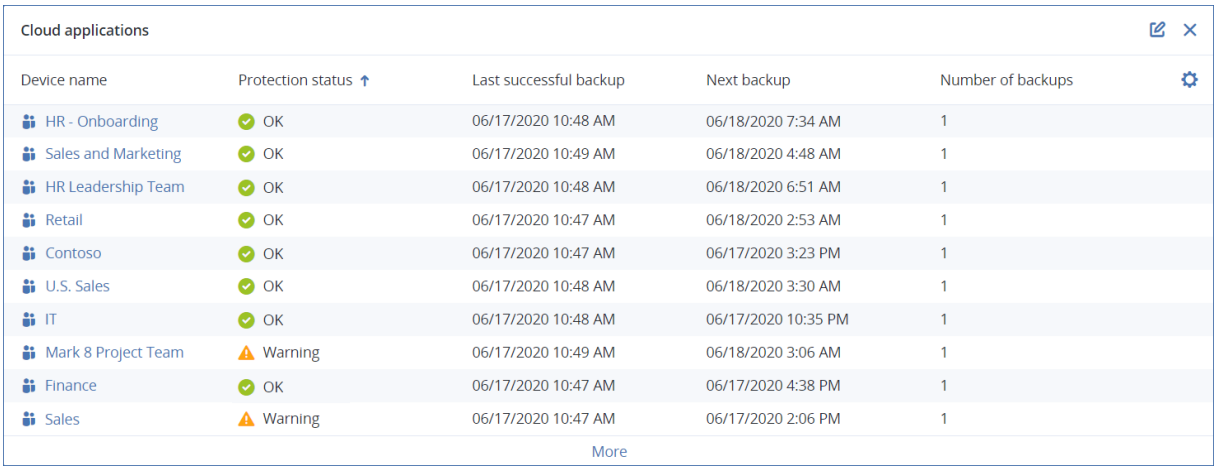
1. 在 **[最近受影響]** 桌面小工具中，按一下 **[下載資料]**。
2. 在 **[時間期限]** 欄位中，輸入您要下載資料的天數。您可以輸入的天數上限為 200。
3. 在 **[收件者]** 欄位中，輸入將收到電子郵件的所有人員的電子郵件地址，且電子郵件中會包含用於下載 CSV 檔案的連結。
4. 按一下 **[下載]**。

系統會使用您指定的時間期限內受影響工作負載的資料，開始產生 CSV 檔案。當 CSV 檔案完成時，系統會傳送一封電子郵件給收件者。接著，每個收件者都可以下載 CSV 檔案。

雲端應用程式

此桌面小工具會顯示雲端對雲端資源的詳細資訊：

- Microsoft 365 使用者 (信箱、OneDrive)
- Microsoft 365 群組 (信箱、群組網站)
- Microsoft 365 公用資料夾
- Microsoft 365 網站集合
- Microsoft 365 Teams
- Google Workspace 使用者 (Gmail、Google 雲端硬碟)
- Google Workspace 共用磁碟機

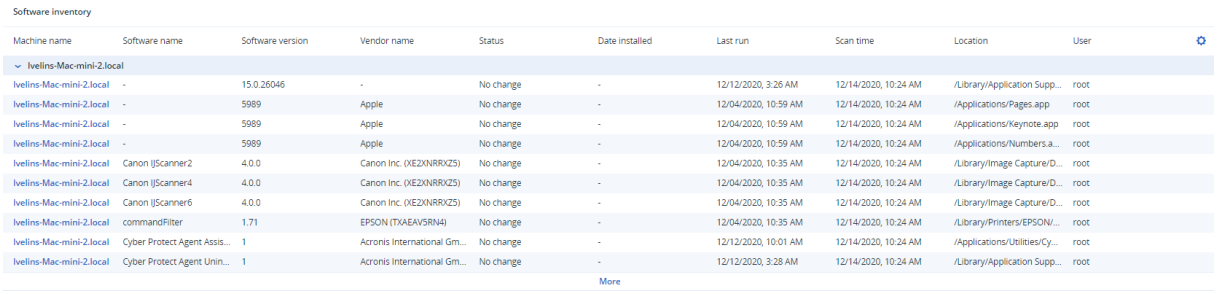


有關雲端對雲端資源的其他資訊也可以在下列桌面小工具中取得：

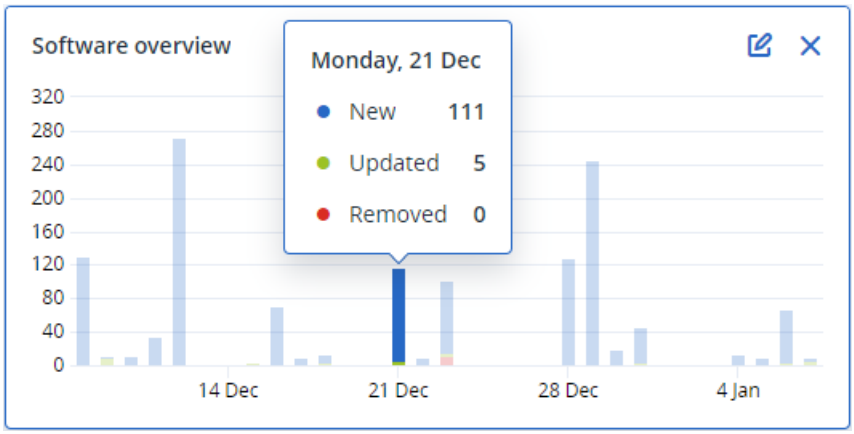
- 活動
- 活動清單
- 5 個最新的警示
- 警示歷程記錄
- 作用中警示摘要
- 歷史警示摘要
- 作用中警示詳細資訊
- 位置摘要

軟體清查桌面小工具

[軟體清查] 表格動態小工具會顯示安裝在組織中 Windows 和 macOS 裝置上的所有軟體的詳細資訊。



[軟體概觀] 桌面小工具會顯示指定的期間 (7 天、30 天或當月), 組織中 Windows 和 macOS 裝置上新的、已更新和已刪除的應用程式的數目。



當您將滑鼠暫留在圖表上的某一列時, 就會顯示包含下列資訊的工具提示:

新的 - 新安裝的應用程式的數目。

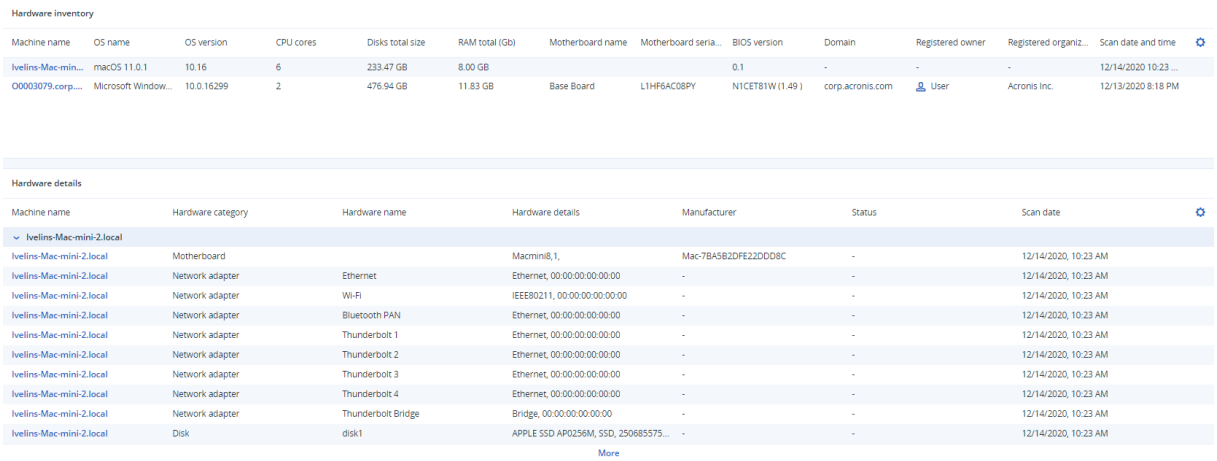
已更新 - 已更新的應用程式的數目。

已移除 - 已移除的應用程式的數目。

當您按一下某個狀態列的部分時, 就會將您重新導向至 **[軟體管理]** -> **[軟體清查]** 頁面。系統會針對對應的日期和狀態, 篩選頁面中的資訊。

硬體清查桌面小工具

[硬體清查] 和 **[硬體詳細資料]** 表格桌面小工具會顯示安裝在組織中實體與虛擬 Windows 和 macOS 裝置上的所有硬體的相關資訊。



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

[硬體變更] 表格桌面小工具會顯示指定的期間 (7 天、30 天或當月), 組織中實體與虛擬 Windows 和 macOS 裝置上新增、移除和變更的硬體的相關資訊。

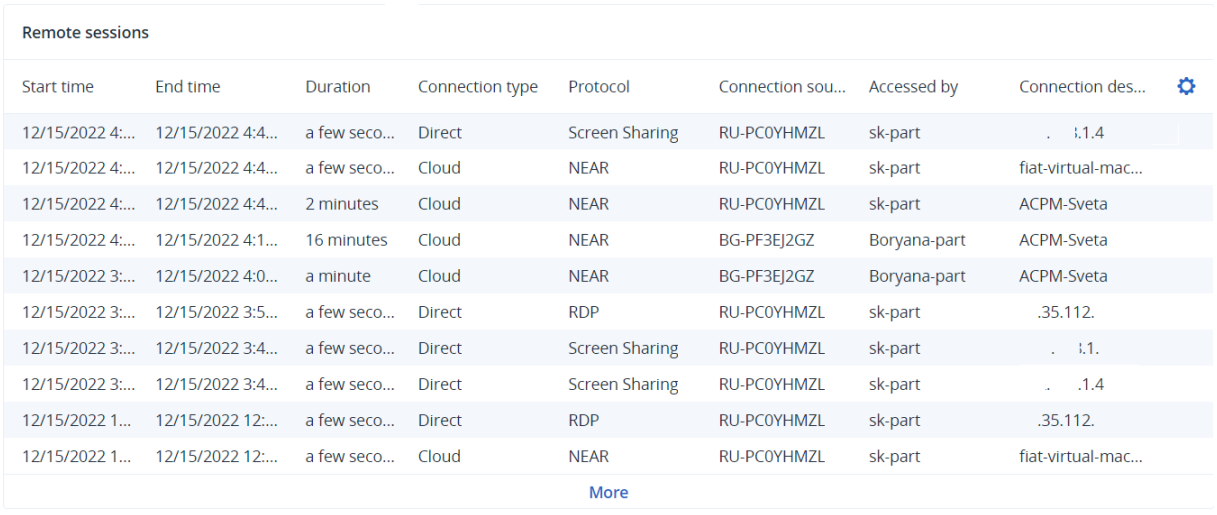
Hardware changes

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

遠端工作階段桌面小工具

此桌面小工具會顯示遠端桌面與檔案傳輸工作階段的詳細資訊。



Remote sessions

Start time	End time	Duration	Connection type	Protocol	Connection sou...	Accessed by	Connection des...
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...
12/15/2022 4:...	12/15/2022 4:4...	2 minutes	Cloud	NEAR	RU-PC0YHMZL	sk-part	ACPM-Sveta
12/15/2022 4:...	12/15/2022 4:1...	16 minutes	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 4:0...	a minute	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 3:5...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 1...	12/15/2022 12:...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 1...	12/15/2022 12:...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...

More

智慧型保護

威脅摘要

Acronis 網路保護營運中心 (CPOC) 會產生僅傳送至相關地理區域的安全性警示。這些安全性警示所提供的資訊包括惡意程式碼、弱點、自然災害、公共衛生，以及可能會影響資料保護的其他類型全球事件。威脅摘要會通知您所有潛在威脅，並可讓您預防這些威脅。

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

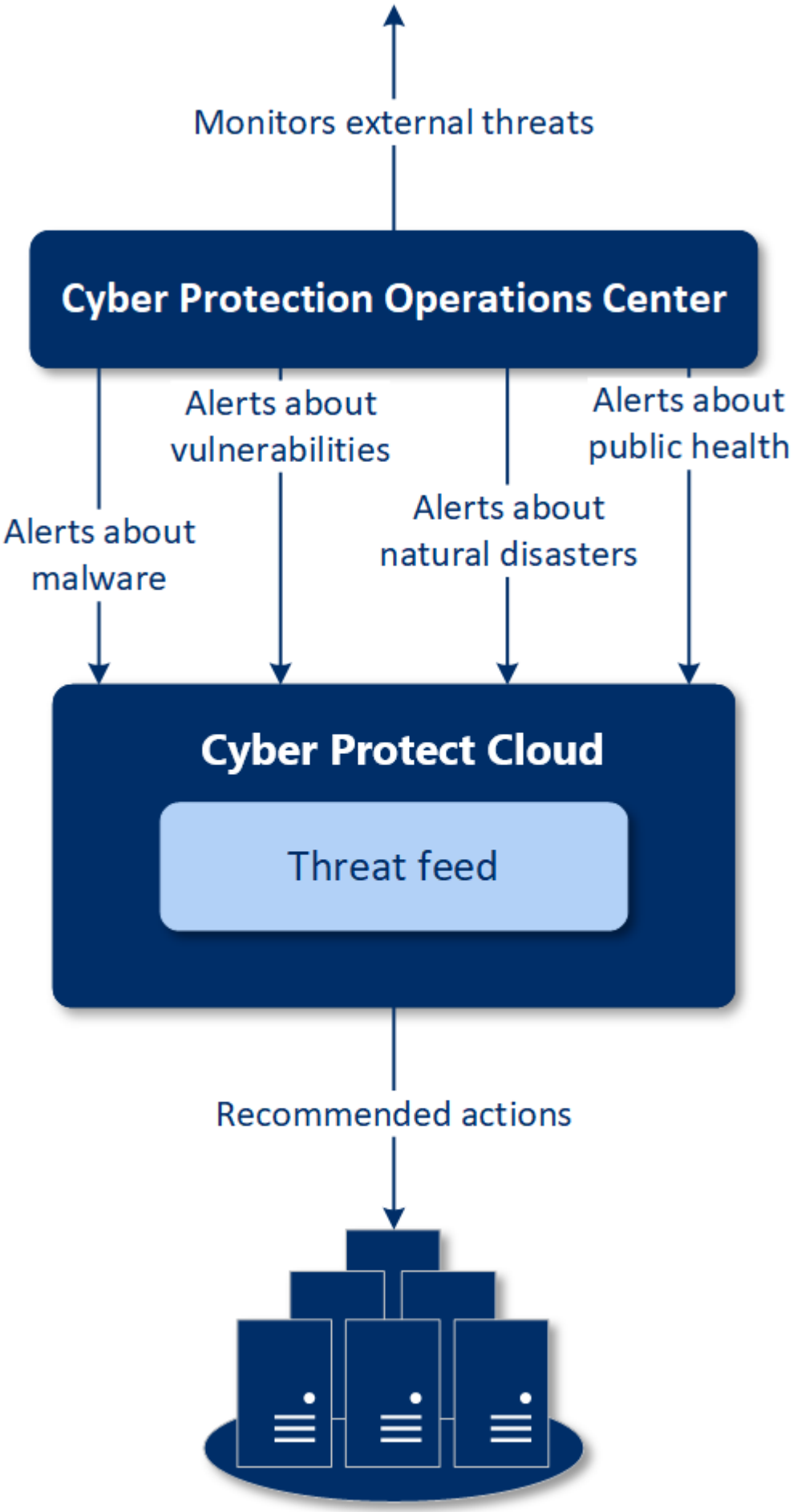
您可以利用安全專家所提供的下列一組特定動作，解決部分安全性警示。其他安全性警示只是用於通知您即將來臨的威脅，但是沒有可用的建議動作。

注意事項
系統僅會針對已安裝反惡意程式碼保護用代理程式的電腦，產生惡意程式碼警示。

運作原理

Acronis 網路保護營運中心可監控外部威脅，並產生有關惡意程式碼、弱點、自然災害和公共衛生威脅的警示。您將能夠在 Cyber Protect 主控台的 **[威脅摘要]** 區段中看到所有這些警示。您可以根據警示的類型，執行個別的建議動作。

威脅摘要的主要工作流程如下圖所示。



若要對從 Acronis 網路保護營運中心收到的警示執行建議的動作，請執行以下操作：

1. 在 Cyber Protect 主控台中，移至 **[監控]** > **[威脅摘要]** 以檢閱是否有任何現有的安全性警示。
2. 在清單中選擇一個警示，然後檢閱所提供的詳細資料。
3. 按一下 **[開始]** 以啟動精靈。
4. 啟用您想要執行的動作，以及必須套用這些動作的電腦。可以建議下列動作：
   - **弱點評估** – 掃描電腦中的弱點
   - **修補程式管理** – 將修補程式安裝在所選電腦上
   - **反惡意程式碼保護** – 對所選電腦執行完整掃描

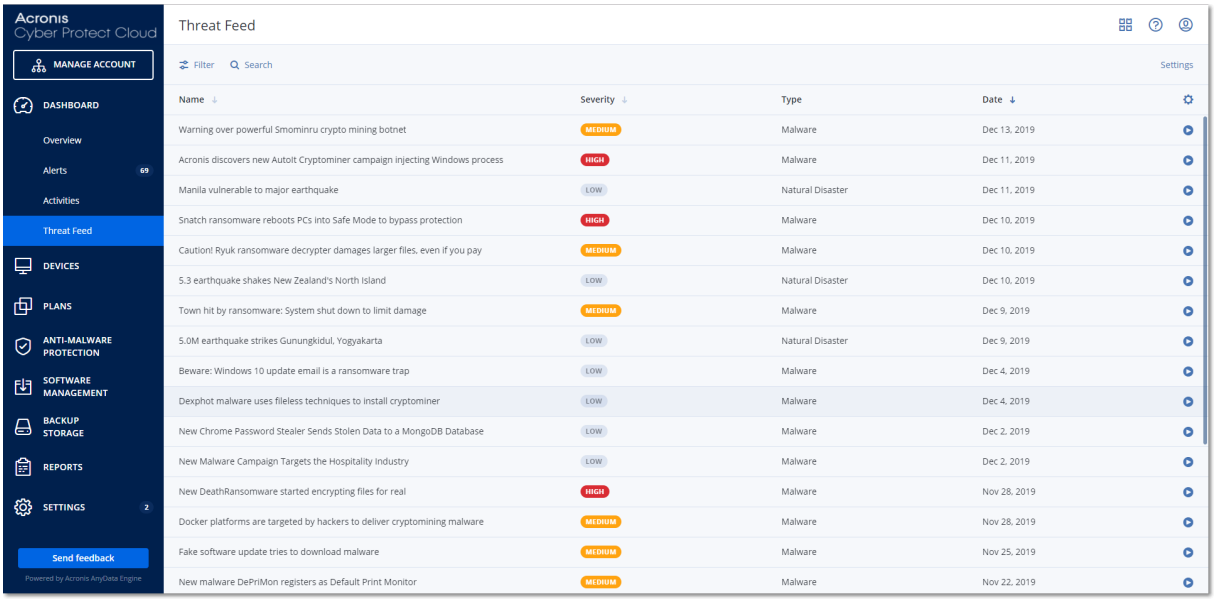
     注意事項
     此動作僅是用於已安裝反惡意程式碼保護用代理程式的電腦。

   - **備份受保護或未受保護的電腦** – 備份受保護和未受保護的工作負載。
     如果還沒有適用於工作負載 (在所有可存取的位置、雲端和本機) 的備份，或現有備份經過加密，則系統會使用下列名稱格式，建立一個完整備份：

     `%workload_name%-Remediation`

     根據預設，備份的目的地是 Cyber Protect Cloud 儲存空間，但是您可以在開始作業之前，設定其他位置。

     如果未加密的備份已存在，系統將會在現有的存檔中，建立一個增量備份。
5. 按一下 **[開始]**。
6. 在 **[活動]** 頁面上，確認已成功執行活動。



刪除所有警示

在下列期限之後，從威脅摘要進行自動清理：

- 自然災害 – 1 週
- 弱點 – 1 個月

- 惡意程式碼 – 1 個月
- 公共衛生 – 1 週

資料保護圖

資料保護圖功能可讓您

- 取得電腦上已儲存之資料的詳細資訊 (分類、位置、保護狀態以及其他資訊)。
- 偵測資料是否受到保護。如果資料是以備份方式保護 (已啟用 [備份] 模組的保護計劃), 則會將資料視為受到保護。
- 執行資料保護的動作。

運作原理

1. 首先, 您在啟用資料保護圖模組的情況下, 建立一個保護計劃。
2. 接著, 在執行計劃並發現和分析資料之後, 您將在 [資料保護圖] 桌面小工具上, 取得資料保護的視覺表示。
3. 您也可以移至 **[裝置]** > **[資料保護圖]**, 並在該處尋找每個裝置上未受保護檔案的相關資訊。
4. 您可以採取動作以保護裝置上偵測到的未受保護檔案。

管理偵測到的未受保護檔案

若要保護偵測為未受保護的重要檔案, 請執行以下操作:

1. 在 Cyber Protect 主控台中, 移至 **[裝置]** > **[資料保護圖]**。
   在裝置的清單中, 您可以找到未受保護檔案數目、每個裝置這類檔案大小, 以及上次資料探索的相關資訊。
   若要保護特定電腦上的檔案, 按一下省略符號圖示, 然後按一下 **[保護所有檔案]**。系統會將您重新導向到計劃清單, 您可以在已啟用 [備份] 模組的情況下, 在其中建立一個保護計劃。
   若要從清單中刪除具有未受保護檔案的特定裝置, 按一下 **[在下次資料探索之前隱藏]**。
2. 若要檢視特定裝置上未受保護檔案的更詳細資訊, 請按一下該裝置的名稱。
   您將根據副檔名和位置, 看到未受保護檔案的數目。在搜尋欄位中, 定義您要取得其未受保護檔案相關資訊的副檔名。
3. 若要保護所有未受保護的檔案, 按一下 **[保護所有檔案]**。系統會將您重新導向到計劃清單, 您可以在已啟用 [備份] 模組的情況下, 在其中建立一個保護計劃。

若要以報告形式取得未受保護檔案的相關資訊, 按一下 **[下載 CSV 格式的詳細報告]**。

資料保護圖設定

若要瞭解如何使用 [資料保護圖] 模組建立保護計劃, 請參閱「建立保護計劃」。

您可以針對 [資料保護圖] 模組指定下列設定。

排程

您可以根據將會對資料保護圖執行的工作, 定義不同的設定以建立排程。

欄位	描述
使用下列事件，排程工作執行	此設定會定義執行工作的時間。 您可以選取下列值： • **依時間排程** – 這是預設設定。工作將會根據指定的時間執行。 • **當使用者登入系統時** – 根據預設，任何使用者的登入都將觸發工作。您可以修改此設定，因此只有特定使用者帳戶能夠觸發工作。 • **當使用者登出系統時** – 根據預設，任何使用者的登出都將觸發工作。您可以修改此設定，因此只有特定使用者帳戶能夠觸發工作。 **注意事項** 工作將不會在系統關機時執行。關機和登出在排程設定上是不同的動作。 • **在系統啟動時** – 工作將會在作業系統啟動時執行。 • **在系統關機時** – 工作將會在作業系統關機時執行。
排程類型	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[依時間排程]**，此欄位將會出現。 您可以選取下列值： • **每月** – 選擇執行工作的月份以及該月的週數或日期。 • **每天** – 這是預設設定。選擇工作將在一週的哪幾天執行。 • **每小時** – 選擇工作將在一週的哪幾天執行、重複次數以及時間間隔。
開始時間	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[依時間排程]**，此欄位將會出現 選擇執行工作的明確時間。
在日期範圍內執行	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[依時間排程]**，此欄位將會出現。 設定一個範圍，已設定的排程將在該範圍內生效。
指定使用者帳戶，該帳戶登入作業系統時將啟動工作	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[當使用者登入系統時]**，此欄位將會出現。 您可以選取下列值： • **任何使用者** - 如果您希望任何使用者登入時都能觸發工作，請使用此選項。 • **下列使用者** - 如果您僅希望在特定使用者帳戶登入時觸發工作，請使用此選項。
指定使用者帳戶，該帳戶登出作業系統時將啟動工作	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[當使用者登出系統時]**，此欄位將會出現。 您可以選取下列值： • **任何使用者** - 如果您希望任何使用者登出時都能觸發工作，請使用此選

欄位	描述
	項。 • **下列使用者** - 如果您僅希望在特定使用者帳戶登出時觸發工作，請使用此選項。
開始條件	定義必須同時符合，工作才能執行的所有條件。 防惡意軟體掃描的開始條件與 **[備份]** 模組的開始條件類似，其詳述於「開始條件」中。 您可以定義下列額外的開始條件： • **在時間視窗中分配工作開始時間** – 此選項可讓您設定工作的時間範圍，以避免網路瓶頸。您可以以小時或分鐘，指定延遲時間。例如，如果預設開始時間為上午 10:00，且延遲為 60 分鐘，則工作將會在上午 10:00 到上午 11:00 之間開始。 • **如果電腦關閉，則在電腦啟動時執行遺漏的工作** • **防止在工作執行期間進入睡眠或休眠模式** – 此選項僅適用於執行 Windows 的電腦。 • **如果未符合開始條件，請無論如何在此時間後執行工作** – 指定無論開始條件為何，將會在其後執行工作的時段。 **注意事項** Linux 不支援開始條件。

副檔名和例外規則

在 **[副檔名]** 索引標籤上，您可以定義在資料復原期間將被視為重要並檢查其是否受到保護之副檔名的清單。使用下列格式定義副檔名：

`.html、.7z、.docx、.zip、.pptx、.xml`

在 **[例外規則]** 索引標籤上，您可以定義在資料復原期間，不檢查保護狀態的檔案和資料夾。

- **隱藏的檔案和資料夾** – 如果已選擇，在資料檢查期間，將會略過隱藏的檔案和資料夾。
- **系統檔案和資料夾** – 如果已選擇，在資料檢查期間，將會略過系統檔案和資料夾。

活動索引標籤

[活動] 索引標籤提供過去 90 天內的活動總覽。

若要在儀表板上篩選活動

1. 在 **[裝置名稱]** 欄位中，指定執行活動所在的電腦。
2. 從 **[狀態]** 下拉式清單中選擇狀態。例如，成功、失敗、進行中、已取消。
3. 從 **[遠端動作]** 下拉式清單中選擇動作。例如，套用計劃、刪除備份、安裝軟體更新。
4. 在 **[最近]** 欄位中，設定活動期間。例如，最近的活動、過去 24 小時的活動，或過去 90 天內特定時間內的活動。

5. 如果您以合作夥伴系統管理員身份存取 **[活動]** 索引標籤，您可針對系統管理的特定客戶篩選活動。

若要自訂 **[活動]** 索引標籤，請按一下齒輪圖示，然選擇您要查看的欄位。若要即時查看活動進度，請選擇 **[自動重新整理]** 核取方塊。

若要[取消]執行中的活動，請按一下名稱，然後在 **[詳細資料]** 畫面按一下 **[取消]**。

您可以依下列條件搜尋列出來的活動：

- 裝置名稱
  這是執行活動所在的電腦。
- 啟動者
  這是開始活動的帳戶。

遠端桌面活動可以依下列屬性進行篩選：

- 建立計劃
- 正在套用計劃
- 正在撤銷計劃
- 正在刪除計劃
- 遠端連線
  - 透過 RDP 的雲端遠端桌面連線
  - 透過 NEAR 的雲端遠端桌面連線
  - 透過 Apple 畫面共用的雲端遠端桌面連線
  - 透過 Web 用戶端進行遠端桌面連線
  - 透過快速協助的遠端桌面連線
  - 透過 RDP 的直接遠端桌面連線
  - 透過 Apple 畫面共用的直接遠端桌面連線
  - 檔案傳輸
  - 透過快速協助的檔案傳輸
- 遠端動作
  - 關閉工作負載
  - 重新啟動工作負載
  - 登出工作負載上的遠端使用者
  - 針對工作負載上的使用者清空資源回收筒
  - 讓工作負載進入睡眠狀態

Cyber Protect Monitor

Cyber Protect Monitor會顯示安裝 Windows 用代理程式或 Mac 用代理程式所在電腦保護狀態的相關資訊，並可讓使用者設定備份加密和 Proxy 伺服器設定。

當 File Sync & Share 用代理程式安裝在電腦上時，Cyber Protect Monitor會提供對 File Sync & Share 服務的存取。在使用者登入自己的 File Sync & Share 帳戶並選擇個人同步資料夾強制上線之後，就

可以存取 File Sync & Share 功能。如需有關 File Sync & Share 用代理程式的詳細資訊，請參閱 Cyber Files Cloud 使用者指南。

重要事項
Cyber Protect Monitor可供對 Cyber Protection 或 File Sync & Share 服務可能沒有系統管理權限的使用者存取。

下表摘要說明沒有系統管理權限的使用者可以執行的操作。

已安裝的代理程式	使用者可以	使用者無法
Windows 用代理程式或 Mac 用代理程式	• 將預設保護計劃套用至其電腦 • 檢查其電腦的保護狀態 • 接收 Active Protection 通知 • 暫時暫停備份其電腦 • 設定 Proxy 伺服器設定 • 變更備份加密設定 **警告！** 變更 Cyber Protect Monitor中的加密設定會覆寫保護計劃中的設定，並影響電腦的所有備份。此作業可能會使部分保護計劃失敗。如需詳細資訊，請參閱 "加密" (第 390 頁)。 若是遺失或忘記密碼，則無法復原加密的備份。	• 套用自訂保護計劃 • 管理已套用的保護計劃
Windows 用代理程式和 Sync and Share 用代理程式 Mac 用代理程式和 Sync and Share 用代理程式	• 同步本機同步資料夾及其 File Sync & Share 帳戶之間的內容 • 暫停同步作業 • 變更同步資料夾 • 檢查無法同步的檔案類型	• 編輯無法同步的檔案類型

在 Cyber Protect Monitor中設定 Proxy 伺服器設定

您可以在 Cyber Protect Monitor中設定 Proxy 伺服器設定。此設定將會影響安裝在電腦上的所有代理程式。

若要設定 Proxy 伺服器設定

1. 開啟 Cyber Protect Monitor，然後按一下右上角的齒輪圖示。
2. 按一下 **[設定]**，然後按一下 **[Proxy]**。
3. 啟用 **[使用 Proxy 伺服器]** 開關，然後輸入 Proxy 伺服器位址和連接埠。

4. [如果 Proxy 伺服器存取受到密碼保護] 啟用 **[需要密碼]** 開關，然後輸入使用者名稱和密碼以存取 Proxy 伺服器。
5. 按一下 **[儲存]**。

   Proxy 伺服器設定隨即儲存在 `http-proxy.yaml` 檔案中。

報告

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

關於操作的報告可能包括任何一組儀表板桌面小工具。所有桌面小工具都會顯示整個公司的摘要資訊。

根據桌面小工具類型，報告包含時間範圍和瀏覽或報告產生時的資料。請參閱 "根據桌面小工具類型回報的資料" (第 262 頁)。

所有歷史桌面小工具都會顯示相同時間範圍的資料。您可在報告設定中變更此範圍。

您可以使用預設報告或建立自訂報告。

您可以下載報告，或透過電子郵件，以 XLSX (Excel) 或 PDF 格式傳送。

預設報告的集合取決於您所擁有的 Cyber Protection 服務版本。預設報告如下所列：

報告名稱	描述
依電腦分類的 #CyberFit 分數	根據每部電腦的安全指標和設定的評估，顯示 #CyberFit 分數以及改進的建議。
警示	顯示指定期間發生的警示。
備份掃描詳細資料	顯示備份中偵測到的威脅的詳細資訊。
每日活動	顯示指定期間所執行活動的摘要資訊。
資料保護圖	顯示電腦上所有重要檔案之數目、大小、位置、保護狀態的詳細資訊。
偵測到的威脅	按照遭封鎖的威脅數目，以及狀況良好與易受攻擊電腦的數目，顯示受影響電腦的詳細資料。
探索到的電腦	顯示組織網路中所有找到的電腦。
磁碟健全狀況預測	顯示 HDD/SSD 故障時間的預測以及目前的磁碟狀態。
現有的弱點	顯示組織中作業系統和應用程式現有的弱點。此報告也會針對網路中所列出的每個產品，顯示受影響電腦的詳細資料。
軟體清查	顯示安裝在公司裝置上的軟體的相關資訊。

硬體清查	顯示適用於公司裝置上的硬體的相關資訊。
修補程式管理摘要	顯示遺漏的修補程式數目、已安裝的修補程式數目，以及適用的修補程式數目。您可以向下鑽研報告以取得遺漏/已安裝的修補程式資訊，以及所有系統的詳細資料。
摘要	顯示指定期間受保護裝置的摘要資訊。
每週各項活動	顯示指定期間所執行活動的摘要資訊。
遠端工作階段	顯示有關遠端桌面與檔案傳輸工作階段的詳細資訊。

具有報告的動作

新增

若要新增報告

1. 在 Cyber Protect 主控台中，移至 **[報告]**。
2. 在可用報告的清單下，按一下 **[新增報告]**。
3. [新增預先定義的報告] 請按一下預先定義之報告的名稱。
4. [新增自訂報告] 按一下 **[自訂]**，然後將桌面小工具新增到報告。
5. [選用] 拖放桌面小工具將其重新排列。

檢視

若要檢視報告

- 若要檢視報告，請按一下其名稱。

編輯

若要˙編輯報告

1. 在 Cyber Protect 主控台中，移至 **[報告]**。
2. 在報告清單中，選擇您要編輯的報告。
3. 按一下畫面右上角的 **[設定]**。
4. 編輯報告，然後按一下 **[儲存]**。

刪除

若要刪除報告

1. 在 Cyber Protect 主控台中，移至 **[報告]**。
2. 在報告清單中，選擇您要刪除的報告。
3. 按一下畫面右上角的省略符號圖示 (...)，然後按一下 **[刪除報告]**。
4. 在確認視窗中，按一下 **[刪除]**。

排程

若要排程報告

1. 在 Cyber Protect 主控台中，移至 **[報告]**。
2. 在報告清單中，選擇您要排程的報告。
3. 按一下畫面右上角的 **[設定]**。
4. 啟用 **[排程]** 旁的開關。
   - 指定收件者的電子郵件地址。
   - 選擇報告格式。

     注意事項
     一個 PDF 檔案中最多可以匯出 1,000 個項目，而一個 XLSX 檔案中最多可以匯出 10,000 個項目。PDF 和 XLSX 檔案中的時間戳記使用您電腦的當地時間。
   - 選擇報告語言。
   - 配置排程。
5. 按一下 **[儲存]**。

下載

若要下載報告

1. 在 Cyber Protect 主控台中，移至 **[報告]**。
2. 在報告清單中，選擇報告。
3. 按一下畫面右上角的 **[下載]**。
4. 選擇報告格式。

結果，所選格式的檔案隨即下載到您的電腦。

如果選擇 **[Excel 和 PDF]**，則會將 ZIP 檔案下載到您的電腦。

傳送

若要傳送報告

1. 在 Cyber Protect 主控台中，移至 **[報告]**。
2. 在報告清單中，選擇報告。
3. 按一下畫面右上角的 **[傳送]**。
4. 指定收件者的電子郵件地址。
5. 選擇報告格式。
6. 按一下 **[傳送]**。

匯出結構

若要匯出報告結構

1. 在 Cyber Protect 主控台中，移至 **[報告]**。
2. 在報告清單中，選擇報告。
3. 按一下畫面右上角的省略符號圖示 (...)，然後按一下 **[匯出]**。

結果，報告結構以 JSON 檔案儲存在您的電腦上。

傾印資料

要傾印報告資料

您可以在不篩選的情況下，將自訂期間的所有資料匯出至 CSV 檔案，並將 CSV 檔案傳送給電子郵件收件者。CSV 檔案僅包含報告中包含的小工具的相關資料。

注意事項
一個 CSV 檔案中最多可以匯出 150,000 個項目。CSV 檔案中的時間戳記使用國際標準時間 (UTC)。

1. 在 Cyber Protect 主控台中，移至 **[報告]**。
2. 在報告清單中，選擇您要傾印其資料的報告。
3. 按一下畫面右上角的省略符號圖示 (...)，然後按一下 **[傾印資料]**。
4. 指定收件者的電子郵件地址。
5. 在 **[時間範圍]** 中，指定您要傾印資料的自訂期間。

   注意事項
   準備較長時間的 CSV 檔案需要更多時間。

6. 按一下 **[傳送]**。

根據桌面小工具類型回報的資料

根據所顯示的資料範圍，儀表板上的桌面小工具有兩種類型：

- 顯示瀏覽或報告產生時實際資料的桌面小工具。
- 顯示歷史資料的桌面小工具。

當您在報告設定中，將資料範圍設定為特定期間的傾印資料時，所選時間範圍僅適用於顯示歷史資料的桌面小工具。若是顯示瀏覽時實際資料的桌面小工具，則時間範圍參數不適用。

下表列出可用的桌面小工具及其資料範圍。

桌面小工具名稱	顯示在桌面小工具和報告中的資料
依電腦分類的 #CyberFit 分數	實際
5 個最新的警示	實際
作用中警示詳細資訊	實際
作用中警示摘要	實際
活動	歷史報告
活動清單	歷史報告
警示歷程記錄	歷史報告
攻擊手法統計資料	歷史報告
備份掃描詳細資料 (威脅)	歷史報告

備份狀態	歷史 - 在 **[執行總計]** 和 **[成功執行的數量]** 欄中 實際 - 在其他所有欄中
已封鎖的 URL	實際
雲端應用程式	實際
Cyber protection	實際
資料保護圖	歷史報告
裝置	實際
已探索到的裝置	實際
磁碟健全狀況概觀	實際
實體裝置的磁碟健全狀況狀態	實際
現有的弱點	歷史報告
硬體變更	歷史報告
硬體詳細資料	實際
硬體清查	實際
歷史警示摘要	歷史報告
事件嚴重性歷程記錄	歷史報告
位置摘要	實際
遺漏的更新 (依類別)	實際
未保護	實際
修補程式安裝歷史記錄	歷史報告
修補程式安裝狀態	歷史報告
修補程式安裝摘要	歷史報告
保護狀態	實際
最近受影響	歷史報告
遠端工作階段	歷史報告
安全性事件待執行工作	歷史報告
安全性事件 MTTR	歷史報告
軟體清查	實際
軟體概觀	歷史報告

威脅狀態	實際
易受攻擊的電腦	實際
工作負載網路狀態	實際

管理 Cyber Protect 主控台中的工作負載

本節描述如何在 Cyber Protect 主控台中管理工作負載。

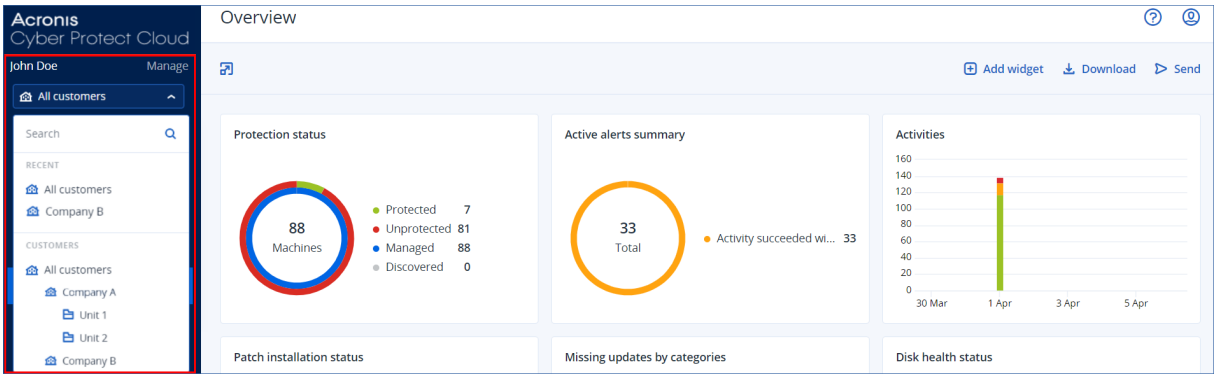
Cyber Protect 主控台

在 Cyber Protect 主控台，您可管理工作負載和計劃、變更保護設定、設定報告或檢查備份儲存。

Cyber Protect 主控台可讓您存取其他服務或功能，例如File Sync & Share 或防毒與防惡意軟體防護、修補程式管理、裝置控制和弱點評估。這些服務和功能的類型和數量根據您的 Cyber Protection 權限而有所不同。

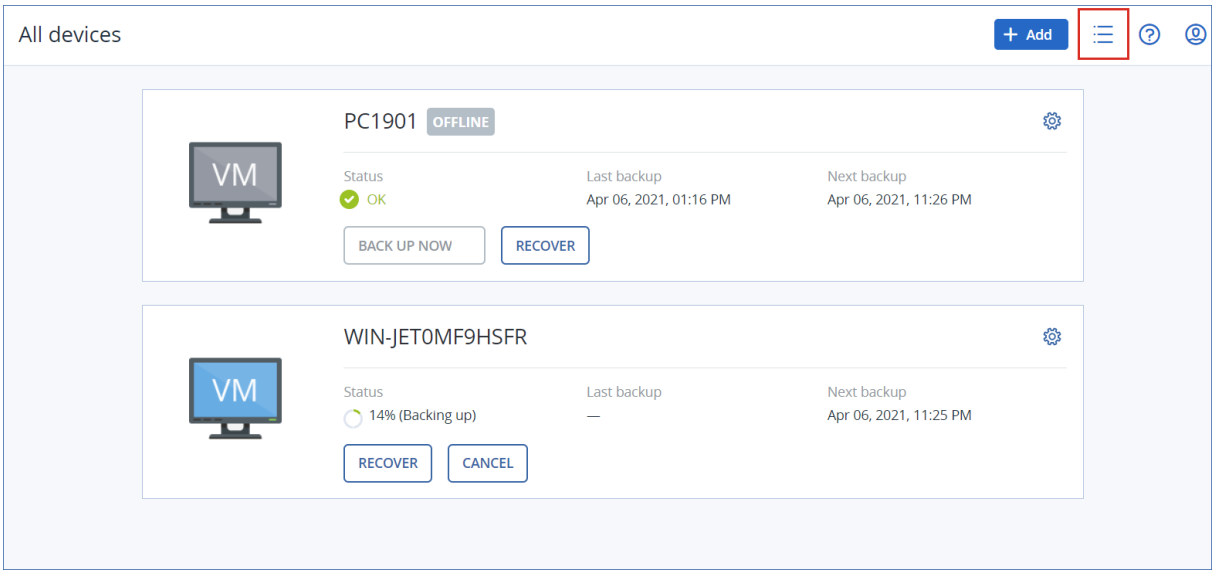
若要檢查儀表板以及有關保護的最重要資訊，請前往 **[監控]** > **[總覽]**。

視您的存取權限而定，您可以為一個或多個客戶租用戶，或租用戶中的單位，管理保護。若要切換階層層級，請使用導覽功能表中的下拉式清單。系統僅會顯示您可以存取的層級。若要前往管理入口網站，請按一下 **[管理]**。

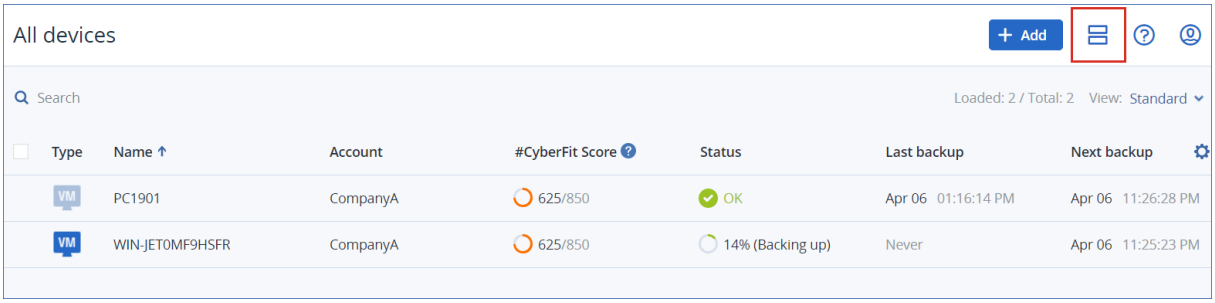


[裝置] 區段可在簡易檢視和表格檢視中使用。若要在這兩者之間切換，請按一下右上角對應的圖示。

簡易檢視僅顯示少數工作負載。



當工作負載數量變大時，表格檢視會自動啟用。



可從這兩個檢視畫面存取相同的功能與作業。本文件說明從表格檢視畫面存取作業。

當工作負載連線或離線時，需要部分時間才能在 Cyber Protect 主控台變更其狀態。工作負載狀態會每分鐘檢查一次。如果對應電腦安裝的代理程式未傳輸資料，且連續五次檢查沒有回應，工作負載會顯示為離線。當工作負載回應狀態檢查或開始傳輸資料時，工作負載會顯示為重新上線。

Cyber Protect 主控台的新功能

Cyber Protect Cloud 的新功能可供使用時，您會在登入 Cyber Protect 主控台時看到一個快顯視窗，其中包含這些功能的簡短描述。

您也可以按一下 主控台主視窗左下角的 **[新功能]** 連結來檢視新功能的描述。

如果沒有新功能，就不會顯示**新增功能**連結。

以夥伴系統管理員身分使用 Cyber Protect 主控台

身為合作夥伴系統管理員，您可以在合作夥伴租用戶 (**所有客戶**) 層級或在客戶租用戶層級使用 Cyber Protect 主控台。

夥伴租用戶 (所有客戶) 層級

在合作夥伴租用戶 (**所有客戶**) 層級上，您可以執行以下動作：

- 從所有受管理的客戶租用戶，管理工作負載的指令馬編寫計劃。
  您可以將相同的指令碼編寫計劃套用至不同客戶的工作負載，也可使用不同客戶的工作負載建立裝置群組。若要瞭解如何在合作夥伴層級建立靜態或動態裝置群組，請參閱 "在合作夥伴層級建立靜態裝置群組" (第 269 頁) 和 "在合作夥伴層級建立動態裝置群組" (第 269 頁)。如需有關指令碼和指令碼編寫計劃的詳細資訊，請參閱 "網路指令碼撰寫" (第 332 頁)。
- 從所有受管理的客戶租用戶，建立工作負載的監控計劃。
- 從所有受管理的客戶租用戶，建立工作負載的遠端管理計劃。
- 在單一事件管理介面中檢視和管理所有客戶租用戶的 Endpoint Detection and Response (EDR) 事件，無需存取每個客戶的事件畫面。
- 為所有受管理的客戶租用戶執行自動探索電腦。

客戶租用戶戶層級

您在此層級跟代表您行事的公司系統管理員擁有相同權限。

選擇租用戶層級

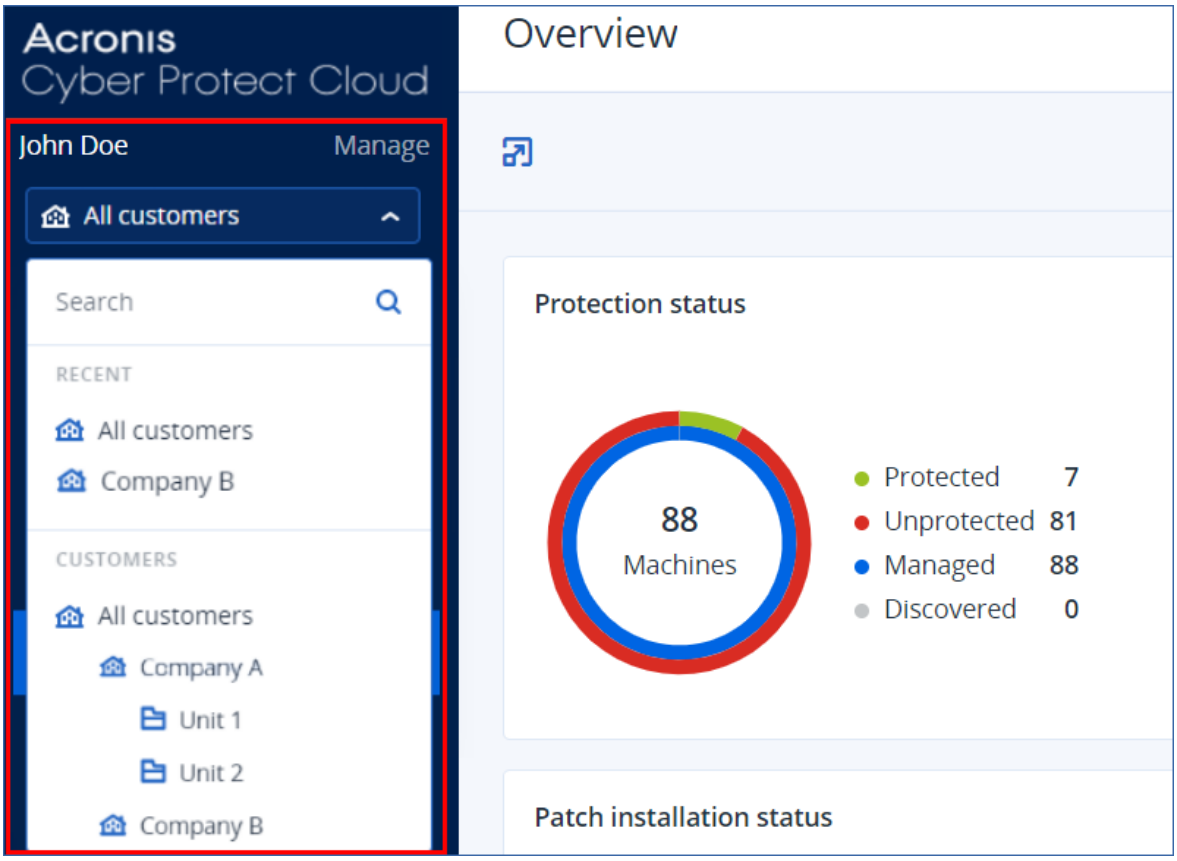
您可以在 Cyber Protect 主控台中選擇要在其上工作的租用戶層級。

必要條件

- 您有存取 Cyber Protect 主控台和管理入口網站的權限。
- 您可以管理多個租用戶或單位。

若要在 Cyber Protect 主控台中選擇租用戶層級

1. 在左側的導覽功能表中，按一下客戶租用戶名稱旁的箭頭。
2. 選擇以下選項之一：
   - 若要在合作夥伴層級作業，請選取 **[所有客戶]**。
   - 若要在客戶或單位層次作業，請選取該客戶或單位的名稱。



Cyber Protect 主控台中的合作夥伴租用戶層級

當您在合作夥伴租用戶 (**所有客戶**) 層級使用 Cyber Protect 主控台時，可使用自訂檢視。

[警示] 和 **[活動]** 索引標籤提供其他合作夥伴相關篩選條件，而 **[裝置]** 和 **[管理]** 索引標籤僅針對可存取的功能或物件合作夥伴系統管理員提供存取權。

警示索引標籤

您可在此查看所有受控客戶的警示，進行搜尋並根據以下條件進行篩選：

- 裝置
- 客戶
- 計劃

您可為每個條件選取多個項目。

活動標籤

您可針對您管理的所有租用戶在此查看活動，或特定客戶租用戶的活動。

您可按客戶、狀態、時間和類型來篩選活動。

系統會在此等級自動預先選取下列類型的活動：

- 正在套用計劃
- 建立保護計劃
- 保護計劃
- 正在撤銷計劃
- 指令碼

裝置索引標籤

在 **[具有代理程式的電腦]** 索引標籤，您可查看受控客戶租用戶的所有工作負載，並可從一或多個租用戶選取工作負載。您也可建立裝置群組，其中包含來自不同租用戶的工作負載。

重要事項
當您在合作夥伴 (**所有客戶**) 層級工作時，您可以使用裝置執行有限數量的操作。例如，您無法執行以下任何操作：

- 查看並管理客戶裝置上的現有保護計劃。
- 建立新的保護計劃。
- 復原備份。
- 使用 Disaster Recovery。
- 存取 Cyber Protection Desktop 功能。

若要執行其中任何操作，請在客戶層級進行。

軟體管理索引標籤

如果已針對客戶工作負載啟用軟體清查掃描，您可以看到軟體掃描結果。

檢視特定客戶的工作負載

身為合作夥伴系統管理員，您可以檢視您管理的客戶租用戶所屬的工作負載。

若要檢視特定客戶的工作負載

1. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[具有代理程式的電腦]**。
2. 在樹狀結構按一下 **[具有代理程式的電腦]** 來展開清單。

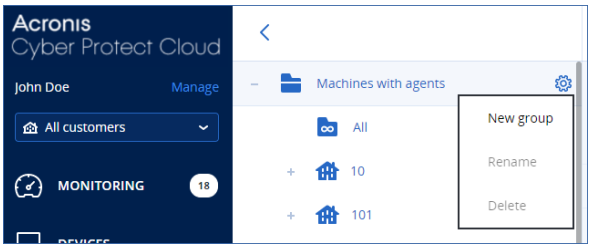
3. 按一下您要檢視並管理其工作負載的客戶名稱。

在合作夥伴層級建立靜態裝置群組

您可以在合作夥伴 (**所有裝置**) 層級建立靜態裝置群組。

在合作夥伴層級建立靜態裝置群組

1. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[具有代理程式的電腦]**。
2. 按一下 **[具有代理程式的電腦]** 旁邊的齒輪圖示，然後按一下 **[新增群組]**。



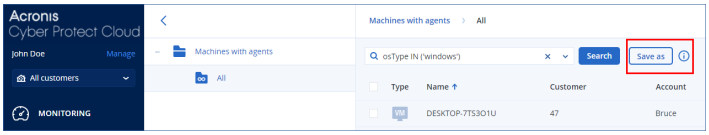
3. 指定群組名稱。
4. [選用] 新增說明。
5. 按一下 **[確定]**。

在合作夥伴層級建立動態裝置群組

您可以在合作夥伴 (**所有裝置**) 層級建立動態裝置群組。

在合作夥伴層級建立動態裝置群組

1. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[具有代理程式的電腦]**。
2. 在樹狀結構按一下 **[具有代理程式的電腦]** 來展開清單。
3. 按一下 **全部**。
4. 在搜尋欄位，根據您要建立動態裝置群組的條件來指定條件，然後按一下 **[搜尋]**。
   若要深入瞭解可用的搜尋條件，請參閱 "搜尋屬性中的非雲端對雲端工作負載" (第 288 頁) 和 "搜尋屬性中的雲端對雲端工作負載" (第 287 頁)。
5. 按一下 **另存為**，然後指定群組名稱。



6. [選用] 新增說明。
7. 按一下 **[確定]**。

在合作夥伴租用戶層級執行自動探索電腦

您可以在合作夥伴租用戶 (**所有客戶**) 層級執行自動探索電腦。

必要條件

客戶的區域網路或 Active Directory 網域中至少有一部已安裝保護代理程式的電腦。

重要事項

只有安裝在 Windows 電腦上的代理程式可以作為探索代理程式。如果您客戶的環境中沒有探索代理程式，將無法使用 **[新增裝置]** 面板中的 **[多個裝置]** 選項。

由於代理程式服務需要其他權限才能執行，因此不支援透過自動探索來新增網域控制站。

僅執行 Windows 的電腦支援遠端安裝代理程式 (Windows XP 不受支援)。若要在執行 Windows Server 2012 R2 的電腦上進行遠端安裝，則必須安裝 Windows 更新 KB2999226。

若要在合作夥伴租用戶層級執行自動探索電腦

1. 在 Cyber Protect 主控台中，選擇 **[所有客戶]**。
2. 移至 **[裝置]** > **[所有裝置]**。
3. 按一下 **[新增]**。
4. 在 **[多個裝置]** 中，按一下 **[僅限 Windows]**。探索精靈便會開啟。
5. 選擇客戶租用戶，然後選擇將執行掃描以偵測電腦的探索代理程式。
6. 選擇探索方法：
   - **搜尋 Active Directory**。請確認安裝探索代理程式所在的電腦是 Active Directory 網域的成員。
   - **掃描區域網路**。將使用 Device Sense 來執行區域網路掃描。如果選取的探索代理程式找不到任何電腦，請選擇另一個探索代理程式。
   - **手動指定或從檔案匯入**。手動定義要新增的電腦，或從文字檔匯入。
7. [如果選擇 [Active Directory] 探索方法] 選擇搜尋電腦的方式：
   - **在組織單位清單中**。選擇要新增之電腦的群組。
   - **依 LDAP 方言查詢**。使用 [LDAP 方言] 查詢選擇電腦。**[搜尋基礎]** 可定義搜尋位置，而 **[篩選]** 則可讓您指定選擇電腦的條件。
8. 根據您選擇的探索方法，執行以下其中一個動作：

探索方法	動作
搜尋 Active Directory	從探索到的電腦清單中，選擇要新增的電腦。
掃描區域網路	從探索到的電腦清單中，選擇要新增的電腦。
手動指定或從檔案匯入	指定電腦的 IP 位址或主機名稱，或從文字檔匯入電腦清單。此檔案必須包含 IP 位址/主機名稱，每行一個。以下是檔案範例： `156.85.34.10` `156.85.53.32` `156.85.53.12` `EN-L00000100` `EN-L00000101` 手動新增電腦位址或從檔案匯入之後，代理程式會嘗試 Ping 新增的電腦，並定義其可用性。

9. 選擇在探索之後必須執行的動作：

選項	描述
安裝代理程式並登錄電腦	您可以按一下 **[選擇元件]**，選擇要在電腦上安裝的元件。如需詳細資訊，請參閱 "選擇要安裝的元件" (第 161 頁)。
代理程式服務的登入帳戶	此設定可在 **[選擇元件]** 畫面上使用。 此設定可定義執行服務所使用的帳戶。 您可以選擇下列其中一個選項： • **使用服務使用者帳戶**(預設適用於代理程式服務) 服務使用者帳戶是用於執行服務的 Windows 系統帳戶。這種設定的優點在於，網域安全性原則不會影響此類帳戶的使用者權限。依預設，此代理程式在**本機系統**帳戶下執行。 • **建立新帳戶** 代理程式的帳戶名稱將是 Agent User。 • **使用下列帳戶** 如果您將代理程式安裝在網域控制站上，則系統會提示您為代理程式指定現有的帳戶 (或相同帳戶)。基於安全理由，系統不會在網域控制站上自動建立新帳戶。 如果您已選擇 **[建立新帳戶]** 或 **[使用下列帳戶]** 選項，請確認網域安全性原則不會影響相關帳戶的權限。如果帳戶被剝奪了在安裝期間指派的使用者權限，則該元件可能無法正確運作或根本無法運作。
使用已安裝的代理程式登錄電腦	如果電腦上已經安裝代理程式，而且您只需將其登錄到 Cyber Protection，請使用此選項。如果在電腦上找不到代理程式，則會將其當作**未受管理**電腦新增。
新增為未受管理的電腦	如果選擇此選項，電腦上將不會安裝在代理程式。您將可以在主控台中檢視電腦，之後再安裝或註冊代理程式。
需要時，重新啟動電腦	選擇 **[安裝代理程式並登錄電腦]** 時，會出現此選項。 如果選擇此選項，電腦將根據需要重新啟動的次數重新啟動以完成安裝。 在下列其中一種情況下，可能需要重新啟動電腦： • 必要條件安裝完成，若要繼續安裝，需要重新啟動電腦。 • 安裝完成，但需要重新啟動，因為部分檔案在安裝期間遭到鎖定。 • 安裝完成，但需要為之前安裝的其他軟體重新啟動。
如果使用者已登入，則不重新啟動	選擇 **[需要時，重新啟動電腦]** 時，會出現此選項。 如果選擇此選項，當使用者登入系統時，電腦將不會自動重新啟動。例如，如果使用者在安裝需要重新啟動時正在工作，則系統將不會重新啟動。 如果已安裝必要條件，但電腦因為使用者登入而未重新啟動，則若要完成安裝，您必須重新啟動電腦，然後再次開始安裝。 如果已安裝代理程式但電腦未重新啟動，則必須重新啟動電腦。
登錄電腦的使用者	[如果您的組織中有單位] 選擇要登錄電腦所使用的單位或下屬單位的使用者帳戶。 [在合作夥伴租用戶層級執行自動探索時] 在您管理的客戶租用戶清單中，展開樹狀結構，然後選擇要登錄電腦所使用的使用者帳戶。 [以客戶系統管理員身分執行自動探索時] 如果您已選擇 **[安裝代理程式並登錄電腦]**

選項	描述
	或 **[使用已安裝的代理程式登錄電腦]**，則也可以選擇將保護計劃套用到電腦。如果您有多個保護計劃，您可以選擇使用哪一個。

10. 為所有電腦指定擁有系統管理員權限之使用者的認證。

重要事項
只有在您指定內建系統管理員帳戶 (安裝作業系統時建立的第一個帳戶) 的認證後，才能在不需要做任何準備的情況下，從遠端安裝代理程式。如果您要定義一些自訂系統管理員認證，則您必須做一些額外的準備，如 "必要條件" (第 269 頁) 中所述。

11. 系統會檢查所有電腦的連線。如果與部分電腦的連線失敗，可以變更這些電腦的認證。

起始電腦探索後，您將會在 **[監控]** > **[活動]** > **[探索電腦]** 活動中看到對應的工作。

多租用戶支援

該 Cyber Protection 服務支援多組織用戶管理，這表示在以下層級進行管理：

- [服務提供者] 合作夥伴用戶 (**所有客戶**) 層級
  此層級僅適用於管理客戶租用戶的合作夥伴系統管理員。
- 客戶租用戶戶層級
  此層級由公司系統管理員管理。
  合作夥伴系統管理員也可在他們管理的客戶租用戶工作。合作夥伴系統管理員在此層級跟其所代表的客戶系統管理員擁有相同權限。
- 單位層級
  此層級由單位管理員及上層客戶的公司系統管理員管理。
  管理上層客戶的合作夥伴系統管理員也可存取單位層級。他們在此層級跟他們所代表的客戶系統管理員具有相同權限。

系統管理員可以管理其自己租用戶及其子系租用戶。他們無法查看或存取上級管理等級的對象，如果有。

例如，公司系統管理員可在客戶租用戶層級及單位層級管理保護計劃。單位系統管理員僅能在單位層級管理自己的保護計劃。他們無法管理客戶租用戶層級的任何保護計劃，也無法管理客戶系統管理員在單位層級建立的保護計劃。

此外，合作夥伴系統管理員可在其管理的客戶租用戶建立並套用指令碼計劃。這類租用戶的公司系統管理員僅能以唯讀方式存取合作夥伴管理套用至其工作負載的指令碼計劃。不過，客戶系統管理員可建立並套用自己的指令碼或保護計劃。

工作負載

工作負載是任何類型的受保護資源，例如實體機器、虛擬機器、信箱或資料庫執行個體。在 Cyber Protect 主控台中，工作負載會顯示為可套用計劃的物件 (保護計劃、備份計劃，或指令碼計劃)。

部分工作負載需要安裝保護代理程式，或部署虛擬裝置。您可以使用圖形化使用者介面或命令列介面安裝代理程式 (自動安裝)您可以使用自動安裝以自動進行安裝程序。如需有關如何安裝保護代理程式的詳細資訊，請參閱 "安裝並部署 Cyber Protection 代理程式" (第 54 頁)。

虛擬裝置 (VA) 是包含保護代理程式的現成虛擬機器。您可以使用虛擬裝置備份相同環境中的其他虛擬機器，而無需在其上安裝保護代理程式 (無代理程式備份)。虛擬裝置以 Hypervisor 專用格式提供，例如 .ovf、.ova 或 .qcow。如需有關哪些虛擬化平台支援無代理程式備份的詳細資訊，請參閱 "支援的虛擬化平台" (第 30 頁)。

重要事項
代理程式每 30 天必須至少在線上一次。否則，計劃將遭撤銷且工作負載將不受保護。

下表摘要說明工作負載類型及相應的代理程式。

工作負載類型	代理程式	範例 (非詳盡清單)
實體機器	保護代理程式已安裝在每台受保護的電腦上。	工作站 筆記型電腦 伺服器
虛擬機器	視虛擬化平台而定，可能可以使用以下備份方式： • 代理程式型備份 – 保護代理程式已安裝在每台受保護的電腦上。 • 無代理程式備份 – 僅在 Hypervisor 主機、專門虛擬機器上安裝保護代理程式，或部署為虛擬裝置。此代理程式會備份環境中的所有虛擬機器。	VMware 虛擬機器 Hyper-V 虛擬機器 由 oVirt 管理的核心虛擬機器 (KVM) VMware Cloud Director (vCD) 虛擬機器*
Microsoft 365 商務版工作負載 Google Workspace 工作負載	這些工作負載由不需安裝的雲端代理程式備份。 若要使用雲端代理程式，您需要將 Microsoft 365 或 Google Workspace 組織新增至 Cyber Protect 主控台。 此外，也提供本機 Office 365 用代理程式。此代理程式需要安裝而且只能用於備份 Exchange Online 信箱。如需有關本機和雲端代理程式間差異的詳細資訊，請參閱 "保護 Microsoft 365 資料" (第 542 頁)。	Microsoft 365 信箱 Microsoft 365 OneDrive Microsoft Teams SharePoint 網站 Google 信箱 Google Drive
應用程式	特定應用程式的資料會由專用代理程式備份，例如 SQL 用代理程式、Exchange 用代理程式、MySQL/MariaDB 用代理程式，或 Active Directory 用代理程式。	SQL Server 資料庫 MySQL/MariaDB 資料庫 Oracle 資料庫

工作負載類型	代理程式	範例 (非詳盡清單)
		Active Directory
行動裝置	受保護的裝置上已安裝手機應用程式。	Android 或 iOS 裝置
網站	這些網站由不需安裝的雲端代理程式備份。	透過 SFTP 或 SSH 通訊協定存取的網站

如需有關所需代理程式以及安裝位置的詳細資訊，請參閱 "我需要哪種代理程式？ "(第 57 頁)

* 如需有關將 VMware Cloud Director 與 Cyber Protect Cloud 整合的詳細資訊，請參閱合作夥伴系統管理員指南。

將工作負載新增 Cyber Protect 主控台

若要開始保護工作負載，請先將其新增至 Cyber Protect主控台。

注意事項

您可以新增的工作負載類型視'帳戶的服務配額而定。若缺少特定工作負載類型，該類型會在**新增裝置**窗格中以灰色顯示。

合作夥伴系統管理員可以在管理入口網站中啟用必要的服務配額。如需詳細資訊，請參閱 "為合作夥伴管理員提供的資訊"(第 278 頁)。

若要新增工作負載

1. 登入 Cyber Protect 主控台。
2. 移至**[裝置]** > **[所有裝置]**，然後按一下**[新增]**。
   [新增裝置] 窗格隨即在右側開啟。
3. 選擇發行通道。
4. 按一下要新增的工作負載類型，並依照所選特定工作負載的指示說明進行。

下表摘述工作負載類型和必要動作。

要新增的工作負載	必要動作	要遵循的程序
多個 Windows 電腦	在您環境中執行自動探索。 若要執行自動探索，您的區域網路或 Active Directory 網域中至少需要一部已安裝保護代理程式的電腦。此代理程式用來當作探索代理程式。	"新增多個裝置"(第 157 頁)
Windows 工作站 Windows 伺服器	安裝 Windows 用代理程式。	"在 Windows 中安裝保護代理程式"(第 72 頁)

要新增的工作負載	必要動作	要遵循的程序
		或 "在 Windows 中安裝和解除安裝保護代理程式" (第 78 頁)
macOS 工作站	安裝 macOS 用代理程式。	"在 macOS 中安裝保護代理程式" (第 76 頁) 或 "在 macOS 中安裝和解除安裝保護代理程式" (第 98 頁)
Linux 伺服器	安裝 Linux 用代理程式。	"在 Linux 中安裝保護代理程式" (第 74 頁) 或 "在 Linux 中安裝和解除安裝保護代理程式" (第 93 頁)
行動裝置 (iOS, Android)	安裝手機應用程式。	"保護行動裝置" (第 536 頁)
雲端對雲端工作負載		
Microsoft 365 商務版	將 Microsoft 365 組織新增至 Cyber Protect 主控台，並使用雲端代理程式保護 Exchange online 信箱、OneDrive 檔案、Microsoft Teams，以及 SharePoint 網站。 或者，您也可以安裝本機 Office 365 用代理程式。這僅會提供 Exchange Online 信箱的備份。 如需本機和雲端代理程式間差異的詳細資訊，請參閱 "保護 Microsoft 365 資料" (第 542 頁)。	"保護 Microsoft 365 資料" (第 542 頁)
Google Workspace	將 Google Workspace 組織新增至 Cyber Protect 主控台，並使用雲端代理程式保護 Gmail 信箱以及 Google 雲端硬碟檔案。	"保護 Google Workspace 資料" (第 577 頁)
虛擬機器		
VMware ESXi	在您的環境中部署 VMware 用代理程式 (虛擬裝置)。	"部署 VMware 用代理程式 (虛擬裝置)" (第 122 頁)
	安裝 VMware 用代理程式 (Windows)。	"在 Windows 中安裝保護代理程式"

要新增的工作負載	必要動作	要遵循的程序
		(第 72 頁) 或 "在 Windows 中安裝和解除安裝保護代理程式" (第 78 頁)
Virtuozzo Hybrid Infrastructure	在您的環境中部署 Virtuozzo Hybrid Infrastructure 用代理程式 (虛擬裝置)。	"部署 Virtuozzo Hybrid Infrastructure 用代理程式 (虛擬裝置)" (第 130 頁)
Hyper-V	安裝 Hyper-V 用代理程式。	"在 Windows 中安裝保護代理程式" (第 72 頁) 或 "在 Windows 中安裝和解除安裝保護代理程式" (第 78 頁)
Virtuozzo	安裝 Virtuozzo 用代理程式。	"在 Linux 中安裝保護代理程式" (第 74 頁) 或 "在 Linux 中安裝和解除安裝保護代理程式" (第 93 頁)
KVM	安裝 Windows 用代理程式。	"在 Windows 中安裝保護代理程式" (第 72 頁) 或 "在 Windows 中安裝和解除安裝保護代理程式" (第 78 頁)
	安裝 Linux 用代理程式。	"在 Linux 中安裝保護代理程式" (第 74 頁) 或 "在 Linux 中安裝和解除安裝保護代理程式" (第 93 頁)
Red Hat Virtualization (oVirt)	在您的環境中部署 oVirt 用代理程式 (虛擬裝置)。	"正在部署 oVirt 用代理程式 (虛擬裝置)" (第 137 頁)
Citrix XenServer	安裝 Windows 用代理程式。	"在 Windows 中安裝保護代理程式" (第 72 頁) 或 "在 Windows 中安裝和解除安裝保護代理程式" (第 78 頁)
	安裝 Linux 用代理程式。	"在 Linux 中安裝保護代理程式" (第 74 頁)

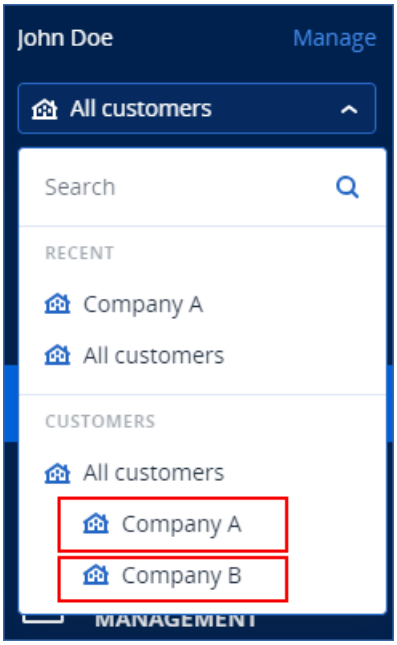
要新增的工作負載	必要動作	要遵循的程序
		或 "在 Linux 中安裝和解除安裝保護代理程式" (第 93 頁)
Nutanix AHV	安裝 Windows 用代理程式。	"在 Windows 中安裝保護代理程式" (第 72 頁) 或 "在 Windows 中安裝和解除安裝保護代理程式" (第 78 頁)
	安裝 Linux 用代理程式。	"在 Linux 中安裝保護代理程式" (第 74 頁) 或 "在 Linux 中安裝和解除安裝保護代理程式" (第 93 頁)
Oracle VM	安裝 Windows 用代理程式。	"在 Windows 中安裝保護代理程式" (第 72 頁) 或 "在 Windows 中安裝和解除安裝保護代理程式" (第 78 頁)
	安裝 Linux 用代理程式。	"在 Linux 中安裝保護代理程式" (第 74 頁) 或 "在 Linux 中安裝和解除安裝保護代理程式" (第 93 頁)
Scale Computing HC3	在您的環境中部署 Scale Computing HC3 用代理程式 (虛擬裝置)。	"正在部署 Scale Computing HC3 用代理程式 (虛擬裝置)" (第 126 頁)
網路附加儲存裝置		
Synology	在您的環境中部署 Synology 用代理程式 (虛擬裝置)。	"部署 Synology 用代理程式" (第 147 頁)
應用程式		
Microsoft SQL Server	安裝 SQL 用代理程式。	"在 Windows 中安裝保護代理程式" (第 72 頁) 或 "在 Windows 中安裝和解除安裝保護代理程式" (第 78 頁)
Microsoft Exchange Server	安裝 Exchange 用代理程式。	
Microsoft Active Directory	安裝 Active Directory 用代理程式。	

要新增的工作負載	必要動作	要遵循的程序
Oracle 資料庫	安裝 Oracle 用代理程式。	"保護 Oracle 資料庫"(第 598 頁)
網站	設定與網站之間的連線。	"保護網站和託管伺服器"(第 604 頁)

如需有關可用保護代理程式以及安裝位置的詳細資訊，請參閱 "我需要哪種代理程式？"(第 57 頁)

為合作夥伴管理員提供的資訊

- 如果未在管理入口網站啟用必要服務配額，**新增裝置**窗格中可能會缺少工作負載類型。如需有關哪項工作負載需要哪種服務配額的詳細資訊，請參閱合作夥伴系統管理員中啟用或停用產品項目。
- 身為合作夥伴系統管理員，您無法在 **[所有客戶]** 層級新增工作負載。若要新增工作負載，請選擇單獨客戶租用戶。



正在從 Cyber Protect 主控台中移除工作負載

您可以從 Cyber Protect 主控台中移除不再需要保護的工作負載。程序依工作負載的版本而定。

或者，您也可以將受保護工作負載上的代理程式解除安裝。當您將代理程式解除安裝時，受保護的工作負載會自動從 Cyber Protect 主控台中移除。

重要事項
當您從 Cyber Protect 主控台中移除工作負載時，所有套用至該工作負載的計劃都會撤銷。移除工作負載不會刪除任何計劃或備份，且不會將保護代理程式解除安裝。

下表摘述工作負載類型和必要動作。

要移除的工作負載	必要動作	要遵循的程序
實體和虛擬機器		
已安裝保護代理程式的實體或虛擬機器	1. 從 Cyber Protect 主控台復原工作負載。 2. [選用] 解除安裝保護代理程式。	"若要從 Cyber Protect 主控台移除工作負載" (第 280 頁) (包含保護代理程式的工作負載)
在 Hypervisor 層級備份 (無代理程式備份) 的虛擬機器	1. 在 Cyber Protect 主控台中，移除已安裝保護代理程式的電腦。此代理程式備份的所有虛擬機器都將自動從主控台中移除。 2. [選用] 解除安裝保護代理程式。	"若要從 Cyber Protect 主控台移除工作負載" (第 280 頁) (無保護代理程式的工作負載)
雲端對雲端工作負載		
Microsoft 365 商務版工作負載 Google Workspace 工作負載	自 Cyber Protect 主控台刪除 Microsoft 365 或 Google Workspace 組織。所有該組織的資源都將自動從主控台中移除。	"若要從 Cyber Protect 主控台移除工作負載" (第 280 頁) (雲端對雲端工作負載)
行動裝置		
Android 裝置 iOS 裝置	1. 從 Cyber Protect 主控台移除行動裝置。 2. [選用] 在行動裝置上，將應用程式解除安裝。	"若要從 Cyber Protect 主控台移除工作負載" (第 280 頁) (行動裝置)
網路附加儲存裝置		
Synology	1. 從 Cyber Protect 主控台復原工作負載。 2. [選用] 解除安裝保護代理程式。	"若要從 Cyber Protect 主控台移除工作負載" (第 280 頁) (包含保護代理程式的工作負載)

要移除的工作負載	必要動作	要遵循的程序
應用程式		
Microsoft SQL Server Microsoft Exchange Server Microsoft Active Directory Oracle 資料庫	1. 在 Cyber Protect 主控台中，移除已安裝保護代理程式的電腦。此代理程式備份的物件都將自動從主控台中移除。 2. [選用] 解除安裝保護代理程式。	"若要從 Cyber Protect 主控台移除工作負載" (第 280 頁) (無保護代理程式的工作負載)
網站	從 Cyber Protect 主控台移除網站。	"若要從 Cyber Protect 主控台移除工作負載" (第 280 頁) (網站)

若要從 Cyber Protect 主控台移除工作負載

包含保護代理程式的工作負載

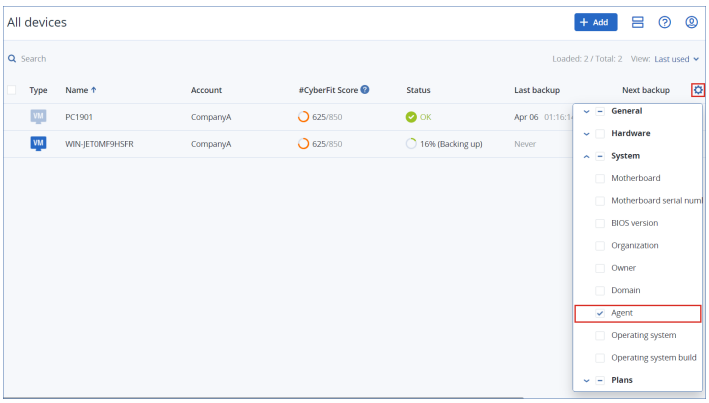
您可以直接移除此類型工作負載。

1. 在 Cyber Protect 主控台中，瀏覽至 **[裝置]** > **[所有裝置]**。
2. 請選擇您要移除的一或多個工作負載旁的核取方塊。
3. 在 **[動作]** 窗格中，按一下 **[刪除]**。
4. 按一下 **[刪除]**，確認您的選擇。
5. [選用] 依照 "解除安裝代理程式" (第 76 頁) 中的說明解除安裝代理程式。

無保護代理程式的工作負載

若要移除此類型工作負載，您需要移除已安裝保護代理程式的電腦。

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 按一下右上角的齒輪圖示，然後選擇 **[代理程式]** 核取方塊。



這會出現 **[代理程式]** 欄。

3. 在 **[代理程式]** 欄中，檢查安裝保護代理程式所在電腦的名稱。

4. 在 Cyber Protect 主控台中，選擇已安裝保護代理程式的電腦旁的核取方塊。
5. 在 **[動作]** 窗格中，按一下 **[刪除]**。
6. 按一下 **[刪除]**，確認您的選擇。
7. [選用] 依照 "解除安裝代理程式" (第 76 頁) 中的說明解除安裝代理程式。

雲端對雲端工作負載

若要移除由雲端代理程式備份的工作負載，請刪除 Cyber Protect 主控台中的 Microsoft 365 或 Google Workspace 組織。

1. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[Microsoft 365]** 或 **[裝置]** > **[Google Workspace]**。
2. 按一下 Microsoft 365 或 Google Workspace 組織的名稱。
3. 在 **[動作]** 窗格中，按一下 **[刪除群組]**。
4. 按一下 **[刪除]** 以確認動作。

行動裝置

1. 在 Cyber Protect 主控台中，瀏覽至 **[裝置]** > **[所有裝置]**。
2. 請選擇您要刪除的工作負載旁的核取方塊。
3. 在 **[動作]** 窗格中，按一下 **[刪除]**。
4. 按一下 **[刪除]**，確認您的選擇。
5. [選用] 解除安裝行動裝置上的應用程式。

網站

1. 在 Cyber Protect 主控台中，瀏覽至 **[裝置]** > **[所有裝置]**。
2. 請選擇您要刪除的工作負載旁的核取方塊。
3. 在 **[動作]** 窗格中，按一下 **[刪除]**。
4. 按一下 **[刪除]**，確認您的選擇。

各 Device 群組

您可以使用裝置群組，透過群組計劃保護多個類似的工作負載。該計劃會套用到整個群組，因此無法從群組成員撤銷。

工作負載可以是多個群組的成員。包含在裝置群組中的工作負載仍然能夠受到個別計劃的保護。

您可以僅將相同類型的工作負載新增至裝置群組。例如，在 **Hyper-V** 下，您僅能建立 Hyper-V 虛擬機器的群組。在 **[具有代理程式的電腦]** 下，您僅能建立已安裝代理程式之電腦的群組。

您無法在任何 **[全部]** 類型的群組中建立裝置群組 (例如根群組 **[所有裝置]**) 或內建群組 (例如 **[具有代理程式的電腦]** > **[全部]**、**[Microsoft 365]** > 您的組織 > **[使用者]** > **[所有使用者]**)。

內建群組和自訂群組

內建群組

在 Cyber Protect 主控台中註冊工作負載之後，該工作負載就會出現在 **[裝置]** 索引標籤上的其中一個內建根群組中，例如 **[具有代理程式的電腦]**、**[Microsoft 365]** 或 **[Hyper-V]**。

所有註冊的非雲端對雲端工作負載也會列在 **[所有裝置]** 根群組中。以您的租用戶命名的另一個內建根群組包含所有非雲端對雲端工作負載以及此租用戶中的所有單位。

您無法刪除或編輯根群組，或在其中套用計劃。

部分根群組包含一或多層的內建子群組，例如，**[具有代理程式的電腦]** > **[全部]**、**[Microsoft 365]** > 您的組織 > **團隊** > **[所有團隊]**、**[Google Workspace]** > 您的組織 > **[共用磁碟機]** > **[所有共用磁碟機]**。

您無法編輯或刪除內建子群組。

自訂群組

保護內建群組中的所有工作負載可能不方便，因為可能有需要不同保護設定或不同保護排程的工作負載。

在部分根群組 (例如 **[具有代理程式的電腦]**、**[Microsoft 365]** 或 **[Google Workspace]**) 中，您可以建立自訂子群組。這些可以是靜態或動態子群組。

您可以編輯、重新命名或刪除任何自訂群組。

靜態群組和動態群組

您可以建立以下類型的自訂群組：

- 靜態
- 動態磁碟

靜態群組

靜態群組包含手動新增的工作負載。

只有在您明確地新增或移除工作負載時，靜態群組的內容才會變更。

範例：您要為公司的會計部建立靜態群組，然後將會計的電腦手動新增至此群組。當您套用群組計劃時，該群組中的電腦會變成受保護。如果聘用新的會計，您將必須將該會計的電腦手動新增至靜態群組。

動態群組

動態群組包含符合特定條件的工作負載。您要建立包含屬性 (例如，`osType`)、其值 (例如，`Windows`)，以及搜尋運算子 (例如，`IN`) 的搜尋查詢，以便事先定義這些條件。

因此，您可以針對其作業系統為 Windows 的所有電腦建立一個動態群組，或在其電子郵件地址開頭為 john 的 Microsoft 365 組織中，建立一個包含所有使用者的動態群組。

具備所需屬性和值的所有工作負載都會自動新增到該群組，而且失去所需屬性或值的任何工作負載都會自動從該群組中移除。

範例 1: 帳戶會計部所屬電腦的主機名稱包含 accounting 一字。您要搜尋其名稱包含 accounting 的電腦，然後您要將搜尋結果儲存為動態群組。接著，您要將保護計劃套用至該群組。如果聘用新的會計，會計電腦的名稱將會有 accounting 一字，而且當您在 Cyber Protect 主控台中登錄該電腦時，就會立即新增至該動態群組。

範例 2: 財務部形成了一個獨立的 Active Directory 組織單位 (OU)。您要將會計 OU 指定為必要屬性，然後將搜尋結果儲存為動態群組。接著，您要將保護計劃套用至該群組。如果聘用新的會計，會計的電腦只要新增到 Active Directory OU，並在 Cyber Protect 主控台中登錄 (不論何者先執行)，該電腦就會立即新增至該動態群組。

雲端對雲端群組和非雲端對雲端群組

雲端對雲端群組包含雲端代理程式備份的 Microsoft 365 或 Google Workspace 工作負載。

非雲端對雲端群組包含其他所有工作負載類型。

裝置群組支援的計劃

下表摘要說明您可以套用到裝置群組的計劃。

群組	可用的計劃	計劃位置
雲端對雲端工作負載 (Microsoft 365 和 Google Workspace 工作負載)	備份計劃	**[管理]** > **[雲端應用程式備份]**
非雲端對雲端工作負載	保護計劃	**[管理]** > **[保護計劃]**
	遠端管理計劃	**[管理]** > **[遠端管理計劃]**
	指令碼計劃	**[管理]** > **[指令碼計劃]**

雲端資源 (例如 Microsoft 365 或 Google Workspace 使用者、OneDrive 和 Google 雲端硬碟共用、Microsoft Teams，或 Azure AD 群組) 都會在您將 Microsoft 365 或 Google Workspace 組織新增至主控台之後，同步到 Cyber Protect 主控台中。組織中的其他任何變更則會一天同步一次。

如果您需要立即同步變更，請在 Cyber Protect 主控台中，分別導覽至 **[裝置]** > **[Microsoft 365]** 或 **[裝置]** > **[Google Workspace]**，選擇所需的組織，然後按一下 **[重新整理]**。

建立靜態群組

您可以建立空的靜態群組，然後在其中新增工作負載。

或者，您可以選擇工作負載，並從您的選擇中建立新的靜態群組。

您無法在任何 **[全部]** 類型的群組中建立裝置群組 (例如根群組 **[所有裝置]**) 或內建群組 (例如 **[具有代理程式的電腦]** > **[全部]**、**[Microsoft 365]** > 您的組織 > **[使用者]** > **[所有使用者]**)。

若要建立靜態群組

在主視窗中

1. 按一下 **[裝置]**, 然後選擇包含您要為其建立靜態群組之工作負載的根群組。
2. [選用] 若要建立巢狀群組, 請導覽至現有的靜態群組。

   注意事項
   建立巢狀靜態群組不適用於雲端對雲端工作負載。

3. 按一下群組樹狀目錄下方的 **[+ 新靜態群組]**, 或按一下 **[動作]** 窗格中的 **[新靜態群組]**。
4. 指定新群組的名稱。
5. [選用] 為群組新增註解。
6. 按一下 **[確定]**。

在群組樹狀目錄中

1. 按一下 **[裝置]**, 然後選擇包含您要為其建立靜態群組之工作負載的根群組。
2. 按一下您想要建立新靜態群組所在群組的名稱旁的齒輪圖示。

   注意事項
   建立巢狀靜態群組不適用於雲端對雲端工作負載。

3. 按一下 **[新靜態群組]**。
4. 指定新群組的名稱。
5. [選用] 為群組新增註解。
6. 按一下 **[確定]**。

從選取項目中

1. 按一下 **[裝置]**, 然後選擇包含您要為其建立靜態群組之工作負載的根群組。

   注意事項
   您無法在任何 **[全部]** 類型的群組中建立裝置群組 (例如根群組 **[所有裝置]**) 或內建群組 (例如 **[具有代理程式的電腦]** > **[全部]**、**[Microsoft 365]** > 您的組織 > **[使用者]** > **[所有使用者]**)。

2. 選擇要建立新群組的工作負載旁的核取方塊, 然後按一下 **[新增至群組]**。
3. 在資料夾樹狀目錄中, 選擇新群組的父層級, 然後按一下 **[新靜態群組]**。

   注意事項
   建立巢狀靜態群組不適用於雲端對雲端工作負載。

4. 指定新群組的名稱。
5. [選用] 為群組新增註解。
6. 按一下 **[確定]**。

新群組隨即出現在資料夾樹狀目錄中。

7. 按一下**[完成]**。

將工作負載新增至靜態群組

您可以先選擇目標群組，然後在其中新增工作負載。

或者，您可以先選擇工作負載，然後將其新增到某個群組。

若要將工作負載新增至靜態群組

先選擇目標群組

1. 按一下 **[裝置]**，然後導覽至您的目標群組。
2. 選擇目標群組，然後按一下 **[新增裝置]**。
3. 在資料夾樹狀目錄中，選擇包含所需工作負載的群組。
4. 選擇要新增的工作負載旁的核取方塊，然後按一下 **[新增]**。

先選擇工作負載

1. 按一下 **[裝置]**，然後選擇包含所需工作負載的根群組。
2. 選擇要新增的工作負載旁的核取方塊，然後按一下 **[新增至群組]**。
3. 在資料夾樹狀目錄中，選擇目標群組，然後按一下 **[完成]**。

建立動態群組

若要建立動態群組，您搜尋的工作負載中要包含您在搜尋查詢中定義其值的特定屬性。接著，您要將搜尋結果儲存為動態群組。

針對搜尋和建立動態群組而支援的屬性會因為雲端對雲端工作負載和非雲端對雲端工作負載而異。如需有關所支援屬性的詳細資訊，請參閱 "搜尋屬性中的非雲端對雲端工作負載" (第 288 頁) 和 "搜尋屬性中的雲端對雲端工作負載" (第 287 頁)。

動態群組是在其個別根群組中建立的。不支援巢狀動態群組。

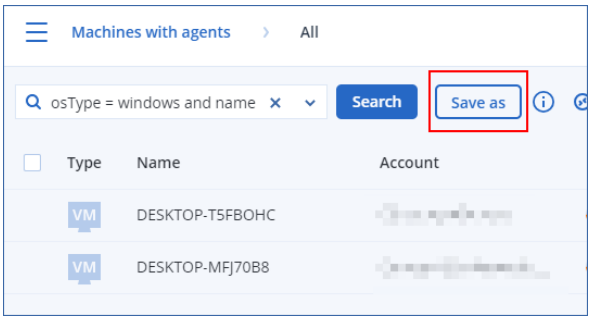
您無法在任何 **[全部]** 類型的群組中建立裝置群組 (例如根群組 **[所有裝置]**) 或內建群組 (例如 **[具有代理程式的電腦]** > **[全部]**、**[Microsoft 365]** > 您的組織 > **[使用者]** > **[所有使用者]**)。

若要建立動態群組

非雲端對雲端工作負載

1. 按一下 **[裝置]**，然後選擇包含您要為其建立新動態群組之工作負載的群組。
2. 使用支援的搜尋屬性和運算子，搜尋工作負載。

   您可以在單一查詢中使用多個屬性和運算子。如需有關支援的屬性的詳細資訊，請參閱 "搜尋屬性中的非雲端對雲端工作負載" (第 288 頁)。
3. 按一下搜尋欄位旁邊的 **[另存新檔]**。



注意事項

當您無法在特定層級建立動態群組時，無法使用 **[另存新檔]** 按鈕。例如，在根群組 **[裝置]** > **[所有裝置]** 中。

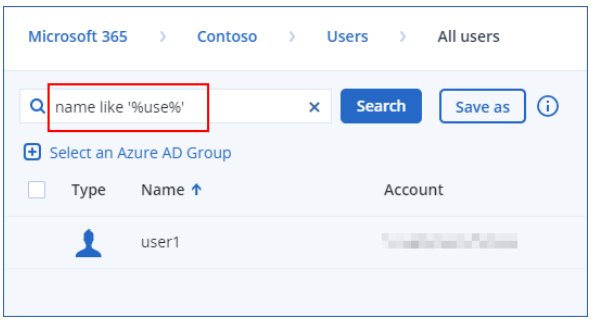
選擇另一個層級 (例如，**[裝置]** > **[具有代理程式的電腦]** > **[全部]**)，然後重複上述步驟。透過此搜尋，您可以在 **[具有代理程式的電腦]** 中建立動態群組，而不是在 **[具有代理程式的電腦]** > **[全部]** 中建立動態群組。

4. 指定新群組的名稱。
5. [選用] 在 **[註解]** 欄位中，新增新群組的描述。
6. 按一下 **[確定]**。

雲端對雲端工作負載

1. 按一下 **[裝置]**，然後選擇 **[Microsoft 365]** 或 **[Google Workspace]**。
2. 選擇包含您要為其建立新動態群組之工作負載的群組，例如 **[使用者]** > **[所有使用者]**。
3. 使用支援的搜尋屬性和運算子，或從特定的 Active Directory 群組選擇 Microsoft 365 使用者，以搜尋工作負載。

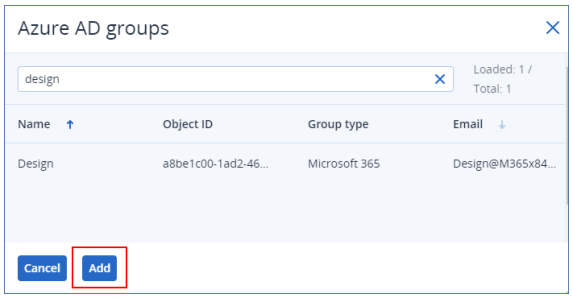
   您可以在單一查詢中使用多個屬性和運算子。如需有關支援的屬性的詳細資訊，請參閱 "搜尋屬性中的雲端對雲端工作負載" (第 287 頁)。



4. [僅適用於 **[Microsoft 365]** > **[使用者]**] 若要從特定的 Active Directory 群組選擇使用者，請執行以下操作：
   a. 導覽至 **[使用者]** > **[所有使用者]**。
   b. 按一下 **[選擇 Azure AD 群組]**。

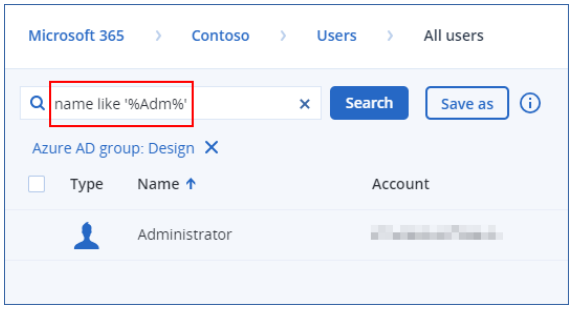
      您組織中的 Active Directory 群組清單隨即開啟。

      在此清單中，您可以搜尋特定群組，或者依名稱或電子郵件排序群組。
   c. 選擇您需要的 Active Directory 群組，然後按一下 **[新增]**。



d. [選用] 若要在選取的 Active Directory 群組中包含或排除特定使用者，請使用支援的搜尋屬性和運算子，建立搜尋查詢。

您可以在單一查詢中使用多個屬性和運算子。如需有關支援的屬性的詳細資訊，請參閱 "搜尋屬性中的雲端對雲端工作負載" (第 287 頁)。



5. 按一下搜尋欄位旁邊的 **[另存新檔]**。

注意事項

當您無法在特定層級建立動態群組時，無法使用 **[另存新檔]** 按鈕。例如，在 **[Microsoft 365]** > 您的組織 > **[使用者]** 中。

選擇另一個層級 (例如，**[Microsoft 365]** > 您的組織 > **[使用者]** > **[全部]**)，然後重複上述步驟。透過此搜尋，您可以在 **[Microsoft 365]** > 您的組織 > **[使用者]** 中建立動態群組，而不是在 **[使用者]** > **[全部]** 中建立動態群組。

6. 指定新群組的名稱。
7. [選用] 在 **[註解]** 欄位中，新增新群組的描述。
8. 按一下 **[確定]**。

搜尋屬性中的雲端對雲端工作負載

下表摘要說明您可以在 Microsoft 365 和 Google Workspace 工作負載的搜尋查詢中使用的屬性。

若要查看您可以在其他類型工作負載的搜尋查詢中使用的屬性，請參閱 "搜尋屬性中的非雲端對雲端工作負載" (第 288 頁)。

屬性	含義	可用於	搜尋查詢範例	支援建立群組
name	Microsoft 365 或 Google Workspace 工作負載的顯示名稱	所有雲端對雲端資源	`name = 'My Name'` `name LIKE '*nam*'`	是

屬性	含義	可用於	搜尋查詢範例	支援建立群組
email	Microsoft 365 使用者或群組，或 Google Workspace 使用者的電子郵件地址	Microsoft 365 > 群組 Microsoft 365 > 使用者 Google Workspace > 使用者	email = 'my_group_email@mycompany.com' email LIKE '*@company*' email NOT LIKE '*enterprise.com'	是
siteName	與 Microsoft 365 群組相關聯之網站的名稱	Microsoft 365 > 群組	siteName = 'my_site' siteName LIKE '*company.com*support*'	是
url	Microsoft 365 群組或 SharePoint 網站的網址	Microsoft 365 > 群組 Microsoft 365 > 網站集合	url = 'https://www.mycompany.com/' url LIKE '*www.mycompany.com*'	是

搜尋屬性中的非雲端對雲端工作負載

下表摘要說明您可以在非雲端對雲端工作負載的搜尋查詢中使用的屬性。

若要查看您可以在雲端對雲端工作負載的搜尋查詢中使用的屬性，請參閱 "搜尋屬性中的雲端對雲端工作負載" (第 287 頁)。

屬性	含義	搜尋查詢範例	支援建立群組
一般			
name	工作負載名稱，例如： • 實體機器的主機名稱 • 虛擬機器的名稱 • 資料庫名稱 • 信箱的電子郵件地址	name = 'en-00'	是
id	裝置 ID。 若要查看裝置 ID，請在 **[裝置]** 下，選擇裝置，按一下 **[詳細資料]** > **[所有屬性]**。 ID 會顯示在 id 欄位中。	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	是

屬性	含義	搜尋查詢範例	支援建立群組
resourceType	工作負載類型。 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' • 'virtual_network.mshyperv' • 'virtual_folder.mshyperv' • 'virtual_data_center.mshyperv' • 'datastore.mshyperv' • 'virtual_machine.msvs'	resourceType = 'machine' resourceType in ('mssql_aag_database', 'mssql_database')	是

屬性	含義	搜尋查詢範例	支援建立群組
	• 'virtual_machine.parallelsw' • 'virtual_host.parallelsw' • 'virtual_cluster.parallelsw' • 'virtual_machine.rhev' • 'virtual_machine.kvm' • 'virtual_machine.xen' • 'bootable_media'		
chassis	機箱類型。 可能的值： • laptop • desktop • server • other • unknown	chassis = 'laptop' chassis IN ('laptop', 'desktop')	是
ip	IP 位址 (僅適用於實體機器)。	ip RANGE ('10.250.176.1','10.250.176.50')	是
comment	裝置的註解。您可以自動或手動指定註解。 預設值： • 若是執行 Windows 的實體電腦，則會自動複製 Windows 中的電腦描述作為註解。系統每 15 分鐘會同步一次這個值。 • 其他裝置留空。 **注意事項** 在註解欄位中有手動新增的文字時，便會停用自動同步。若要再次啟用同步，請清除此文字。 若要為您的工作負載重新整理自動同步的註解，請重新啟動 **[Windows 服務]** 中的 Managed Machine Service，或在命令提示字元下執行下列命令：	comment = 'important machine' comment = '' (不含註解所有電腦)	是

屬性	含義	搜尋查詢範例	支援建立群組
	`net stop mms` `net start mms` 若要檢視裝置註解，在 **[裝置]** 底下選取裝置、按一下 **[詳細資料]**，然後找出 **[註解]** 區段。 若要手動新增或變更註解，按一下 **[新增]** 或 **[編輯]**。 若是已安裝保護代理程式的裝置，則有兩個不同的註解欄位： • 代理程式註解 ◦ 若是執行 Windows 的實體電腦，則會自動複製 Windows 中的電腦描述作為註解。系統每 15 分鐘會同步一次這個值。 ◦ 其他裝置留空。 **注意事項** 在註解欄位中有手動新增的文字時，便會停用自動同步。若要再次啟用同步，請清除此文字。 • 裝置註解 ◦ 如果代理程式註解是自動指定的，則系統會將其複製為裝置註解。系統不會將手動新增的代理程式註解複製為裝置註解。 ◦ 系統不會將裝置註解複製為代理程式註解。 裝置可以指定其中一個或兩個註解，或者將兩個註解都留空。如果指定兩個註解，則裝置註解優先。 若要檢視代理程式註解，在 **[裝置]** > **[代理程式]** 底下，選取已安裝代理程式的裝置、按一下 **[詳**		

屬性	含義	搜尋查詢範例	支援建立群組
	細資料], 然後找出 **[註解]** 區段。 若要檢視裝置註解, 在 **[裝置]** 底下選取裝置、按一下 **[詳細資料]**, 然後找出 **[註解]** 區段。 若要手動新增或變更註解, 按一下 **[新增]** 或 **[編輯]**。		
isOnline	工作負載可用性。 可能的值: • true • false	isOnline = true	否
hasAsz	Secure Zone 可用性。 可能的值: • true • false	hasAsz = true	是
tzOffset	與國際標准時間 (UTC) 的時區位移, 以分鐘為單位。	tzOffset = 120 tzOffset > 120 tzOffset < 120	是
CPU、記憶體、磁碟			
cpuArch	CPU 架構。 可能的值: • 'x64' • 'x86'	cpuArch = 'x64'	是
cpuName	CPU 名稱。	cpuName LIKE '%XEON%'	是
memorySize	RAM 的大小, 以 MB 為單位。	memorySize < 1024	是
diskSize	硬碟大小, 以 GB 或 MB 為單位 (僅適用於實體機器)。	diskSize < 300GB diskSize >= 3000000MB	否
作業系統			
osName	作業系統名稱。	osName LIKE '%Windows XP%'	是
osType	作業系統類型。 可能的值:	osType = 'windows' osType IN ('linux', 'macosx')	是

屬性	含義	搜尋查詢範例	支援建立群組
	• 'windows' • 'linux' • 'macosx'		
osArch	作業系統架構。 可能的值： • 'x64' • 'x86'	cpuArch = 'x86'	是
osProductType	作業系統產品類型。 可能的值： • 'dc' 代表網域控制站。 **注意事項** 在 Windows 伺服器上指派網域控制站角色時，osProductType 會從 server 變更為 dc。這類電腦將不會包含在 osProductType='server' 的搜尋結果中。 • 'server' • 'workstation'	osProductType = 'server'	是
osSp	作業系統的 Service Pack。	osSp = 1	是
osVersionMajor	作業系統的主要版本。	osVersionMajor = 1	是
osVersionMinor	作業系統的次要版本。	osVersionMinor > 1	是
代理程式			
agentVersion	已安裝的保護代理程式版本。	agentVersion LIKE '12.0.*'	是
hostId	保護代理程式的內部 ID。 若要查看保護代理程式 ID，請在 **[裝置]** 下，選擇裝置，按一下 **[詳細資料]** > **All properties**。檢查 agent 屬性的 id 值。	hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	是
virtualType	虛擬機器類型。 可能的值：	virtualType = 'vmwesx'	是

屬性	含義	搜尋查詢範例	支援建立群組
	• 'vmwesx' VMware 虛擬機器。 • 'mshyperv' Hyper-V 虛擬機器。 • 'pcs' Virtuozzo 虛擬機器。 • 'hci' Virtuozzo Hybrid Infrastructure 虛擬機器。 • 'scale' Scale Computing HC3 虛擬機器。 • 'ovirt' oVirt 虛擬機器		
insideVm	內部具有代理程式的虛擬機器。 可能的值： • true • false	insideVm = true	是
位置			
tenant	裝置所屬租用戶的名稱。	tenant = 'Unit 1'	是
tenantId	裝置所屬租用戶的識別碼。 若要查看租用戶 ID，請在 **[裝置]** 下，選擇裝置，按一下 **[詳細資料]** > **[所有屬性]**。ID 會顯示在 ownerId 欄位中。	tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'	是
ou	屬於指定 Active Directory 組織單位的裝置。	ou IN ('RnD', 'Computers')	是
狀態			
state	裝置狀態。 可能的值： • 'idle' • 'interactionRequired' • 'canceling' • 'backup' • 'recover'	state = 'backup'	否

屬性	含義	搜尋查詢範例	支援建立群組
	• 'install' • 'reboot' • 'failback' • 'testReplica' • 'run_from_image' • 'finalize' • 'failover' • 'replicate' • 'createAsz' • 'deleteAsz' • 'resizeAsz'		
status	保護狀態。 可能的值： • ok • warning • error • critical • protected • notProtected	status = 'ok' status IN ('error', 'warning')	否
protectedByPlan	由保護計劃保護的裝置具有給定 ID。 若要查看計劃 ID，請在 **[管理]** > **[保護計劃]** 中選擇一個計劃，按一下 **[狀態]** 欄中的列，然後按一下狀態名稱。將建立具有計劃 ID 的新搜尋。	protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否
okByPlan	由保護計劃保護的裝置具有給定 ID，且具有 **[正常]** 狀態。	okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否
errorByPlan	由保護計劃保護的裝置具有給定 ID，且具有 **[錯誤]** 狀態。	errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否
warningByPlan	由保護計劃保護的裝置具有給定 ID，且具有 **[警告]** 狀態。	warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否
runningByPlan	由保護計劃保護的裝置具有給定 ID，且具有 **[執行中]** 狀態。	runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否
interactionByPlan	由保護計劃保護的裝置具有給定 ID，且具有 **[需要互動]** 狀態。	interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否

屬性	含義	搜尋查詢範例	支援建立群組
lastBackupTime*	上次成功備份的日期和時間。 格式為 'YYYY-MM-DD HH:MM'。	lastBackupTime > '2023-03-11' lastBackupTime <= '2023-03-11 00:15' lastBackupTime is null	否
lastBackupTryTime*	上次備份嘗試的時間。 格式為 'YYYY-MM-DD HH:MM'。	lastBackupTryTime >= '2023-03-11'	否
nextBackupTime*	下次備份的時間。 格式為 'YYYY-MM-DD HH:MM'。	nextBackupTime >= '2023-08-11'	否
lastVAScanTime*	上次成功漏洞評估的日期和時間。 格式為 'YYYY-MM-DD HH:MM'。	lastVAScanTime > '2023-03-11' lastVAScanTime <= '2023-03-11 00:15' lastVAScanTime is null	是
lastVAScanTryTime*	上次嘗試漏洞評估的時間。 格式為 'YYYY-MM-DD HH:MM'。	lastVAScanTimeTryTime >= '2022-03-11'	是
nextVAScanTime*	下次漏洞評估的時間。 格式為 'YYYY-MM-DD HH:MM'。	nextVAScanTime <= '2023-08-11'	是
network_status	Endpoint Detection and Response (EDR) 的網路隔離狀態。 可能的值： • connected • isolated	network_status= 'connected'	是

注意事項

如果您略過小時和分鐘值，則會將開始時間視為 YYYY-MM-DD 00:00，並將結束時間視為 YYYY-MM-DD 23:59:59。例如，lastBackupTime = 2023-01-20 表示搜尋結果將包含自 lastBackupTime >= 2023-01-20 00:00 到 lastBackupTime <= 2023-01-20 23:59:59 這段間隔的所有備份。

搜尋運算子

下表摘要說明您可以用於搜尋查詢的運算子。

您可以在單一查詢中使用多個運算子。

運算子	支援	含義	範例
AND	所有工作負載	邏輯接合運算子	name like 'en-00' AND tenant = 'Unit 1'
OR	所有工作負載	邏輯分離運算子	state = 'backup' OR state = 'interactionRequired'
NOT	所有工作負載	邏輯否定運算子	NOT(osProductType = 'workstation')
IN (<value1>,... <valueN>)	所有工作負載	此運算子會檢查運算式是否符合值清單中的任何值。	osType IN ('windows', 'linux')
NOT IN	所有工作負載	此運算子與 IN 運算子相反。	NOT osType IN ('windows', 'linux')
LIKE 'wildcard pattern'	所有工作負載	此運算子會檢查運算式是否符合萬用字元模式。 您可以使用以下萬用字元運算子: • * 或 % 星號和百分比符號代表零、一或多個字元 • _ 底線代表單一字元	name LIKE 'en-00' name LIKE '*en-00' name LIKE '*en-00*' name LIKE 'en-00_'
NOT LIKE 'wildcard pattern'	所有工作負載	此運算子與 LIKE 運算子相反。 您可以使用以下萬用字元運算子: • * 或 % 星號和百分比符號代表零、一或多個字元 • _ 底線代表單一字元	NOT name LIKE 'en-00' NOT name LIKE '*en-00' NOT name LIKE '*en-00*' NOT name LIKE 'en-00_'
RANGE (<starting_value>,	所有工作負載	此運算子會檢查運算式是否在值範圍內(含兩個值)。	ip RANGE('10.250.176.1','10.250.176.50') name RANGE('a','d')

運算子	支援	含義	範例
<ending_value>)		包含字母數字字串的搜尋查詢使用 ASCII 排序順序，但不區分大小寫。	您可以利用此查詢，篩選開頭為 A、B 和 C 的所有名字，例如 Alice、Bob、Claire。但是，單一字母 D 符合需求，因此包含更多字母的名字 (例如 Diana 或 Don) 將不包括在內。 為達到相同的結果，您也可以使用以下查詢： name >= 'a' AND name <= 'd'
= 或 ==	所有工作負載	等於運算子	osProductType = 'server'
!= 或 <>	所有工作負載	不等於運算子	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'
<	非雲端對雲端工作負載	小於運算子	memorySize < 1024
>	非雲端對雲端工作負載	大於運算子。	diskSize > 300GB
<=	非雲端對雲端工作負載	小於或等於運算子	lastBackupTime <= '2022-03-11 00:15'
>=	非雲端對雲端工作負載	大於或等於運算子	nextBackupTime >= '2022-08-11'

編輯動態群組

您可以透過變更可定義群組內容的搜尋查詢來編輯動態群組。

在以 Active Directory 為基礎的動態群組中，您也可以變更 Active Directory 群組。

若要編輯動態群組

透過變更搜尋查詢

1. 按一下 **[裝置]**，導覽至您要編輯的動態群組，然後選擇該群組。
2. 按一下群組名稱旁的齒輪圖示，然後按一下 **[編輯]**。或者，按一下 **[動作]** 窗格中的 **[編輯]**。
3. 透過修改搜尋屬性、其值或搜尋運算子來變更搜尋查詢，然後按一下 **[搜尋]**。
4. 按一下搜尋欄位旁的 **[儲存]**。

透過變更 Active Directory 群組

注意事項
此程序適用於以 Active Directory 為基礎的動態群組。以 Active Directory 為基礎的動態群組僅適用於 **[Microsoft 365]** > **[使用者]**。

1. 按一下 **[裝置]**，導覽至 **[裝置]** > **[Microsoft 365]** > 您的組織 > **[使用者]**。
2. 選擇您想要編輯的動態群組。
3. 按一下群組名稱旁的齒輪圖示，然後按一下 **[編輯]**。或者，按一下 **[動作]** 窗格中的 **[編輯]**。
4. 執行下列任何一項操作以變更群組內容：
   - 按一下所選 Active Directory 群組的名稱，然後從開啟的清單中選擇新的 Active Directory 群組，藉此變更該群組。
   - 編輯搜尋查詢，然後按一下 **[搜尋]**。
     搜尋查詢限制為目前選取的 Active Directory 群組。
5. 按一下搜尋欄位旁的 **[儲存]**。

您也可以在不覆寫目前群組的情況下，儲存您所做的編輯。若要將編輯過的設定另存為新的群組，請按一下搜尋欄位旁的箭頭按鈕，然後按一下 **[另存新檔]**。

刪除群組

當您刪除裝置群組時，套用至該群組的所有計劃都會遭到撤銷。如果群組中未套用其他任何計劃，則該群組中的工作負載將會變成未受保護。

若要刪除裝置群組

1. 按一下 **[裝置]**，然後導覽至您要刪除的群組。
2. 按一下群組名稱旁的齒輪圖示，然後按一下 **[刪除]**。
3. 按一下 **[刪除]**，確認您的選擇。

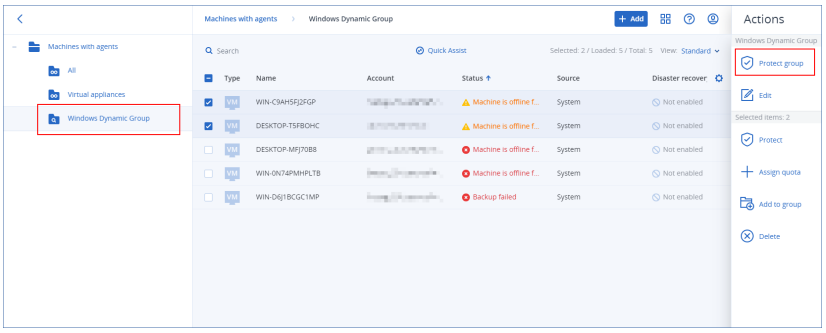
將計劃套用到群組

您可以先選擇群組，然後將計劃指派到某個群組，以便將計劃套用至該群組。

或者，您可以開啟計劃進行編輯，然後在其中新增群組。

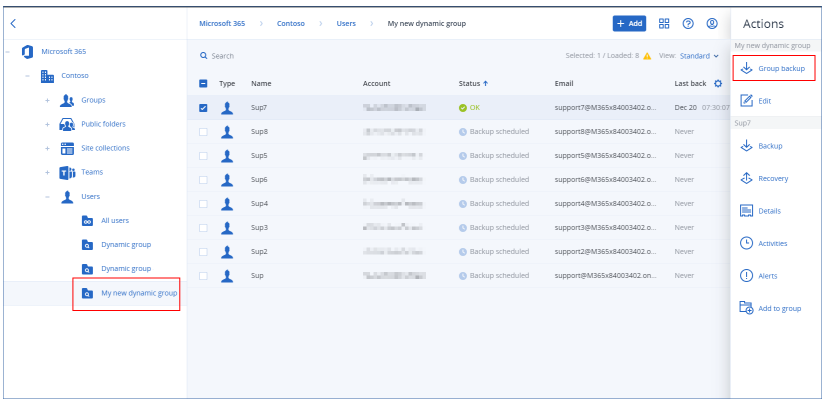
若要將計劃套用到群組

1. 按一下 **[裝置]**，然後導覽至您要套用計劃的群組。
2. [對於非雲端對雲端工作負載] 按一下 **[保護群組]**。



可套用之計劃的清單隨即顯示。

3. [對於雲端對雲端工作負載] 按一下 **[群組備份]**。



可套用之備份計劃的清單隨即顯示。

4. [套用現有的計劃] 選擇計劃，然後按一下 **[套用]**。
5. [建立新計劃] 按一下 **[建立計劃]**，選擇計劃類型，然後建立新計劃。

   如需有關可用計劃類型以及如何建立計劃的詳細資訊，請參閱 "裝置群組支援的計劃" (第 283 頁)。

注意事項

套用至雲端對雲端裝置群組的備份計劃會自動排程為每天執行一次。您無法視需要按一下 **[立即執行]** 來執行這些計劃。

從群組撤銷計劃

您可以先選擇群組，然後從中撤銷計劃，以便撤銷該群組中的計劃。

或者，您可以開啟計劃進行編輯，然後從其中移除群組。

若要從群組撤銷計劃

1. 按一下 **[裝置]**，然後導覽至您要在其中撤銷計劃的群組。
2. [對於非雲端對雲端工作負載] 按一下 **[保護群組]**。

   套用至群組之計劃的清單隨即顯示。
3. [對於雲端對雲端工作負載] 按一下 **[群組備份]**。

   套用至群組之備份計劃的清單隨即顯示。
4. 選擇要撤銷的計劃。

5. [對於非雲端對雲端工作負載] 按一下省略符號圖示 (...), 然後按一下 **[撤銷]**。
6. [對於雲端對雲端工作負載] 按一下齒輪圖示, 然後按一下 **[撤銷]**。

使用裝置控制模組

裝置控制模組[1]運用每個受保護電腦上的資料洩漏防禦用代理程式[2]功能子集, 偵測並防止本機電腦通道上未經授權的資料存取和傳輸, 作為 Cyber Protection 服務保護計劃的一部分。其對各式各樣的資料洩漏途徑提供細微的控制, 包括使用卸除式媒體、印表機、虛擬和重新導向的裝置, 以及 Windows 剪貼簿交換資料。

此模組適用於按工作負載授權的 Cyber Protect Essentials、Cyber Protect Standard 以及 Cyber Protect Advanced 版本。

注意事項
在 Windows 電腦上, 裝置控制功能需要安裝資料洩漏防禦用代理程式。如果在其保護計劃中啟用 **[裝置控制]** 模組, 則會為受保護的工作負載自動安裝該代理程式。

裝置控制模組依賴代理程式的資料洩漏防禦[3]功能, 強制對受保護電腦上的資料存取和傳輸作業, 執行情境控制。這些包括使用者對週邊裝置和連接埠的存取、文件列印、剪貼簿複製/貼上作業、媒體格式化和退出作業, 以及與本機連線行動裝置的同步。資料洩漏防禦用代理程式包含裝置控制模組所有中央管理和系統管理元件的架構, 因此其必須安裝在要使用裝置控制模組保護的每部電腦上。此代理程式會根據其接收自受保護電腦所套用之保護計劃的裝置控制設定, 允許、限制或拒絕使用者動作。

無論是直接在受保護電腦上使用, 還是在受保護電腦上託管的虛擬化環境中重新導向, 裝置控制模組都可以控制對各種週邊裝置的存取。此模組可辨識在 Microsoft Remote Desktop Server、Citrix XenDesktop / XenApp / XenServer, 以及 VMware Horizon 中重新導向的裝置。它也可以控制在 VMware Workstation / Player、Oracle VM VirtualBox 或 Windows Virtual PC 上執行之客體作業系統的剪貼簿, 以及在受保護電腦上執行之主機作業系統的剪貼簿之間的資料複製作業。

裝置控制模組可以保護執行下列作業系統的電腦:

裝置控制

- Microsoft Windows 7 Service Pack 1 和更新版本
- Microsoft Windows Server 2008 R2 和更新版本
- macOS 10.15 (Catalina)

---

[1]裝置控制模組運用每個受保護電腦上的資料洩漏防禦代理程式功能子集, 偵測並防止本機電腦通道上未經授權的資料存取和傳輸, 作為保護計劃的一部分。這些包括使用者對週邊裝置和連接埠的存取、文件列印、剪貼簿複製/貼上作業、媒體格式化和退出作業, 以及與本機連線行動裝置的同步。裝置控制模組對允許使用者在受保護的電腦上存取的裝置和連接埠的類型, 以及使用者可以在這些裝置上執行的動作, 提供精細的情境控制。
[2]資料洩漏防禦系統的用戶端元件, 可透過套用環境和內容分析技術的組合, 並強制執行集中管理的資料洩漏防禦政策, 保護其主機電腦, 免於未經授權者使用、傳輸和儲存機密、受保護或敏感的資料。網路保護提供一個功能全面的資料洩漏防禦代理程式。但是, 代理程式在受保護電腦上的功能受限於網路保護授權使用的一組資料洩漏防禦功能, 並取決於套用至該電腦的保護計劃。
[3]一種整合式技術和組織措施的系統, 旨在偵測和防止組織內外部未經授權的實體有意和無意地洩露/存取機密、受保護或敏感的資料, 或將此類資料傳輸到不受信任的環境。

- macOS 11.2.3 (Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)

注意事項
適用於 macOS 的資料洩漏防禦用代理程式僅支援 x64 處理器。不支援 Apple Silicon ARM 型處理器。

資料洩漏防禦

- Microsoft Windows 7 Service Pack 1 和更新版本
- Microsoft Windows Server 2008 R2 和更新版本

注意事項
資料洩漏防禦用代理程式可能安裝在不支援的 macOS 系統上，因為它是 Mac 用代理程式的完整部分。在此情況下，Cyber Protect 主控台將會指出資料洩漏防禦用代理程式已安裝在電腦上，但是裝置控制和資料洩漏防禦功能將無法運作。裝置控制功能僅適用於資料洩漏防禦用代理程式支援的 macOS 系統。

使用資料洩漏防禦用代理程式搭配 Hyper-V 的限制

請勿將資料洩漏防禦用代理程式安裝在 Hyper-V 叢集中的 Hyper-V 主機上，因為這可能會造成 BSOD 問題，主要是在具有叢集式共用磁碟區 (CSV) 的 Hyper-V 叢集中。

如果您使用下列任何版本的 Hyper-V 用代理程式，您需要手動移除資料洩漏防禦用代理程式：

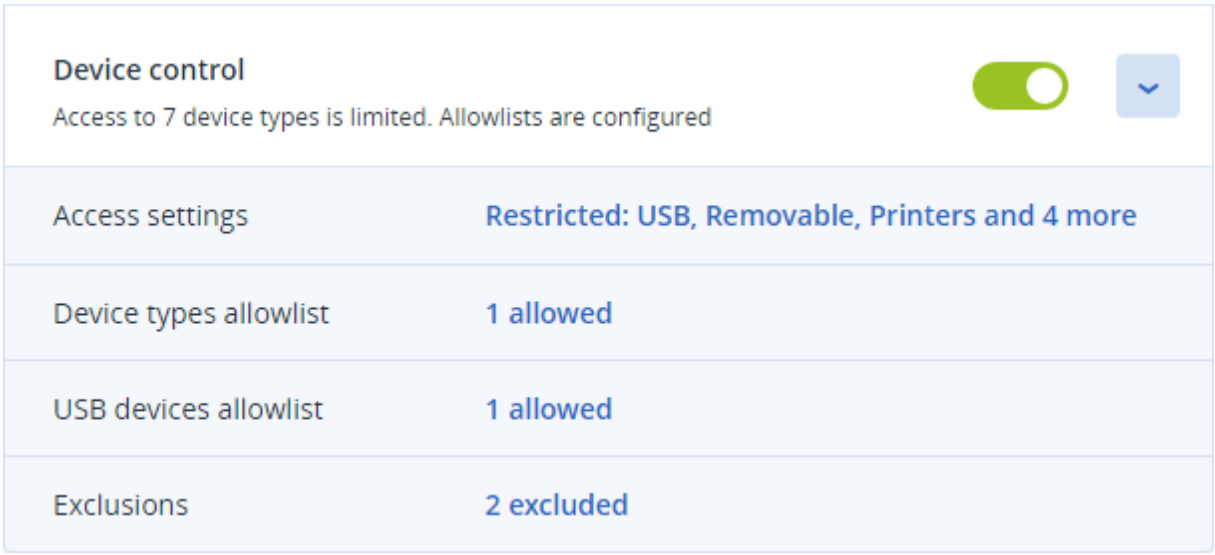
- 15.0.26473 (C21.02)
- 15.0.26570 (C21.02 HF1)
- 15.0.26653 (C21.03)
- 15.0.26692 (C21.03 HF1)
- 15.0.26822 (C21.04)

若要移除資料洩漏防禦用代理程式，請在 Hyper-V 主機上，手動執行安裝程式，然後清除 [資料洩漏防禦用代理程式] 核取方塊，或執行下列命令：

```
<installer_name> --remove-components=agentForDlp -quiet
```

您可以在 Cyber Protect 主控台中保護計劃的 **[裝置控制]** 區段內啟用並設定裝置控制模組。如需指示，請參閱啟用或停用裝置控制的步驟。

[裝置控制] 區段會顯示模組設定的摘要：



- 存取設定 - 顯示具有受限 (拒絕或唯讀) 存取權之裝置類型和連接埠的摘要 (如果有的話)。否則，指明允許所有裝置類型。按一下此摘要可檢視或變更存取設定 (請參閱檢視或變更存取設定的步驟)。
- 裝置類型允許名單 - 透過從裝置存取控制排除，顯示允許的裝置子類別數量 (如果有的話)。否則，指明允許名單是空的。按一下此摘要可檢視或變更允許的裝置子類別選項 (請參閱從存取控制排除裝置子類別的步驟)。
- USB 裝置允許名單 - 透過從裝置存取控制排除，顯示允許的 USB 裝置/型號數量 (如果有的話)。否則，指明允許名單是空的。按一下此摘要可檢視或變更允許的 USB 裝置/型號清單 (請參閱從存取控制排除各個 USB 裝置的步驟)。
- 排除 - 顯示針對 Windows 剪貼簿、螢幕擷取畫面擷取、印表機和行動裝置設定的存取控制排除數目。

使用裝置控制

本節涵蓋使用裝置控制模組時基本工作的逐步指示。

啟用或停用裝置控制

您可以在建立保護計劃時啟用裝置控制。您可以將現有的保護計劃變更為啟用或停用裝置控制。

啟用或停用裝置控制

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 執行下列其中一項操作以開啟保護計劃面板：
   - 如果您要建立新的保護計劃，選擇要保護的電腦，按一下 **[保護]**，然後按一下 **[建立計劃]**。
   - 如果您要變更現有的保護計劃，選擇受保護的電腦，按一下 **[保護]**，按一下保護計劃名稱旁的省略符號 (...)，然後按一下 **[編輯]**。
3. 在保護計劃面板中，瀏覽至 **[裝置控制]** 區域，然後啟用或停用 **[裝置控制]**。
4. 執行下列其中一項操作以套用您的變更：

- 若要建立保護計劃，按一下 **[建立]**。
- 若要編輯保護計劃，按一下 **[儲存]**。

您也可以從 [管理] 索引標籤存取保護計劃面板。但是，此功能無法用於 Cyber Protection 服務的所有版本。

在 macOS 上啟用裝置控制模組

保護計劃的裝置控制設定僅會在受保護的工作負載上載入裝置控制驅動程式之後生效。本節描述如何載入裝置控制驅動程式，以便在 macOS 上啟用裝置控制模組。這是需要端點電腦系統管理員權限的一次性作業。

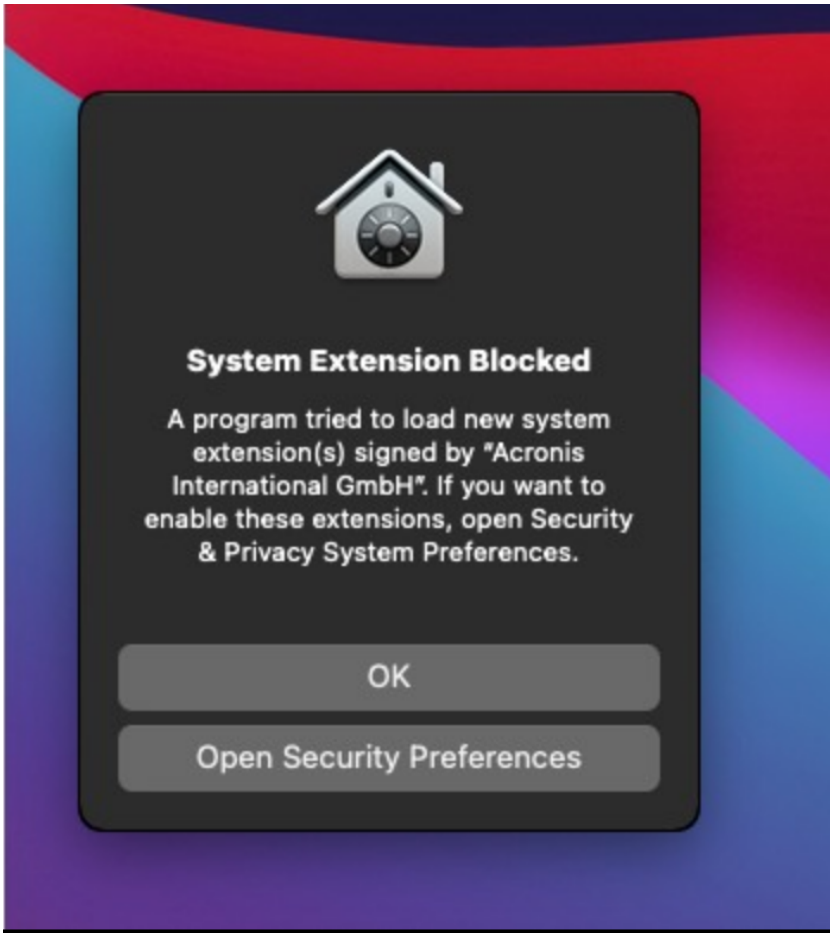
支援的 macOS 版本：

- macOS 10.15 (Catalina) 和更新版本
- macOS 11.2.3 (Big Sur) 和更新版本
- macOS 12.2 (Monterey) 和更新版本
- macOS 13.2 (Ventura) 和更新版本

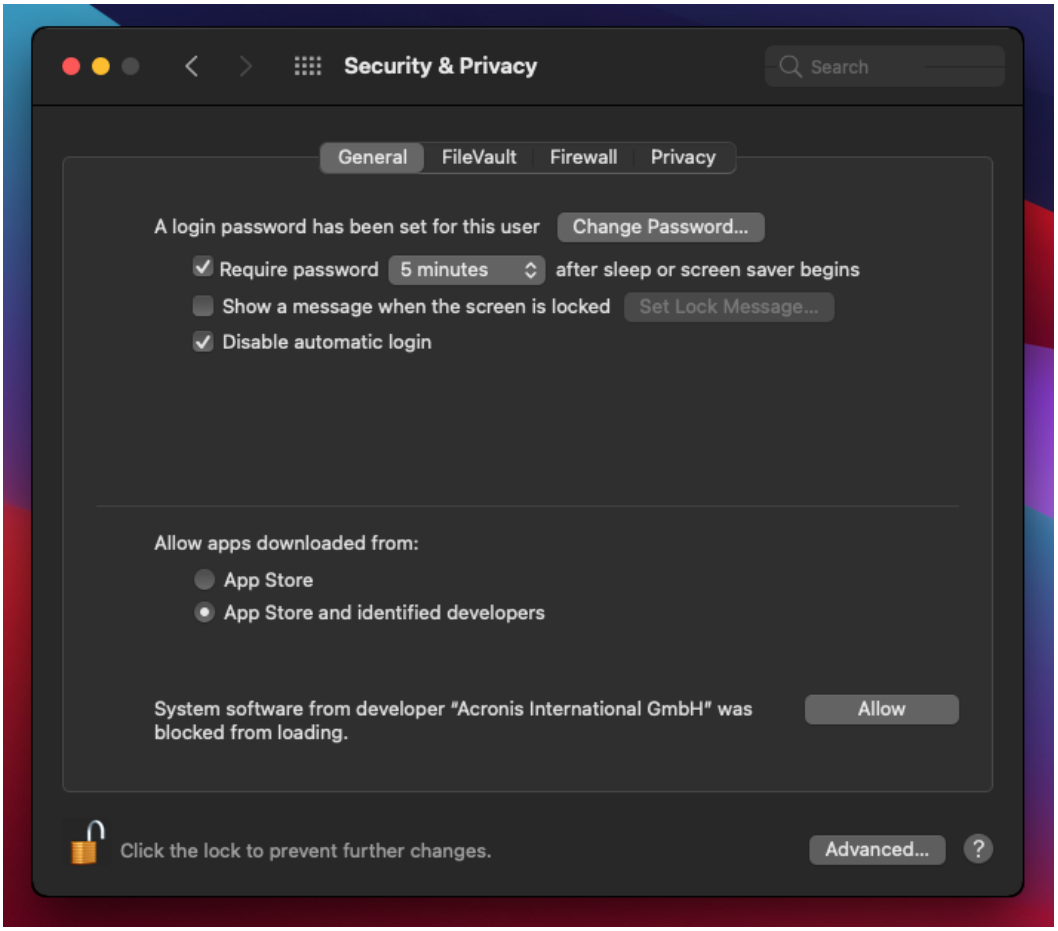
若要在 macOS 上啟用裝置控制模組

1. 在您要保護的電腦上，安裝 Mac 用代理程式。
2. 在保護計劃中，啟用裝置控制設定。
3. 套用保護計劃。

4. 「系統擴充功能已封鎖」警告將會出現在受保護的工作負載上。按一下 **[開啟安全性喜好設定]**。



5. 在出現的 **[安全性與隱私權]** 窗格中，選擇 **[App Store 和識別的開發人員]**，然後按一下 **[允許]**。



6. 在出現的對話方塊中，按一下 **[重新啟動]** 以重新啟動工作負載，並啟用裝置控制設定。

注意事項
如果停用裝置控制設定後再次啟用，您就不必重複這些步驟。

檢視或變更存取設定

從保護計劃面板中，您可以管理裝置控制模組的存取設定。如此一來，您可以允許或拒絕存取特定類型的裝置，以及啟用或停用通知和警示。

檢視或變更存取設定

1. 開啟保護計劃的保護計劃面板，然後在該計劃中啟用裝置控制 (請參閱啟用或停用裝置控制的步驟)。
2. 按一下 **[裝置控制]** 開關旁的箭頭圖示以展開設定，然後按一下 **[存取設定]** 旁的連結。
3. 在出現的管理存取設定頁面上，視需要檢視或變更存取設定。

注意事項
在 [裝置控制] 中設定的存取設定在同時使用 [裝置控制] 和 [Advanced DLP] 保護工作負載時，可能會遭到覆寫。請參閱 "在保護計劃中啟用 Advanced Data Loss Prevention" (第 778 頁)。

啟用或停用作業系統通知和服務警示

管理存取設定時，您可以啟用或停用 [作業系統通知和服務警示]，告知使用者嘗試執行不允許的動作。

啟用或停用作業系統通知

1. 依照檢視或變更存取設定的步驟進行。
2. 在管理存取設定的頁面上，選取或清除 **[當終端使用者嘗試使用封鎖的裝置類型或連接埠時，向其顯示作業系統通知]** 核取方塊。

啟用或停用服務警示

1. 依照檢視或變更存取設定的步驟進行。
2. 在管理存取設定的頁面上，為所需的裝置類型選取或清除 **[顯示警示]** 核取方塊。

[顯示警示] 核取方塊僅適用於存取權有限 (唯讀或拒絕存取) 的裝置類型，但螢幕擷取畫面擷取除外。

從存取控制排除裝置子類別

您可以從保護計劃面板選擇要從存取控制排除的裝置子類別。結果，無論裝置控制存取設定為何，都允許存取這些裝置。

從存取控制排除裝置子類別

1. 開啟保護計劃的保護計劃面板，然後在該計劃中啟用裝置控制 (請參閱啟用或停用裝置控制的步驟)。
2. 按一下 **[裝置控制]** 開關旁的箭頭圖示以展開設定，然後按一下 **[裝置類型允許名單]** 旁的連結。
3. 在出現的管理允許名單頁面上，檢視或變更要從存取控制排除的裝置子類別選項。

從存取控制排除個別 USB 裝置

在保護計劃面板上，您可以指定要從存取控制排除的個別 USB 裝置或 USB 裝置型號。結果，無論裝置控制存取設定為何，都允許存取這些裝置。

從存取控制排除 USB 裝置

1. 開啟保護計劃的保護計劃面板，然後在該計劃中啟用裝置控制 (請參閱啟用或停用裝置控制的步驟)。
2. 按一下 **[裝置控制]** 開關旁的箭頭圖示以展開設定，然後按一下 **[USB 裝置允許名單]** 旁的連結。
3. 在出現的管理允許名單頁面上，按一下 **[從資料庫新增]**。
4. 在出現的選取 USB 裝置頁面上，從透過 USB 裝置資料庫登錄的裝置，選擇所需的裝置。
5. 按一下 **[新增至允許名單]** 按鈕。

停止從存取控制排除 USB 裝置

1. 開啟保護計劃的保護計劃面板，然後在該計劃中啟用裝置控制 (請參閱啟用或停用裝置控制的步驟)。

2. 按一下 **[裝置控制]** 開關旁的箭頭圖示以展開設定，然後按一下 **[USB 裝置允許名單]** 旁的連結。
3. 在出現的管理允許名單頁面上，按一下代表所需 USB 裝置的清單項目尾端的刪除圖示。

從資料庫新增或移除 USB 裝置

若要從存取控制排除特定 USB 裝置，您需要將其新增至 USB 裝置資料庫。接著，您可以透過從該資料庫中選擇，將裝置新增至允許名單。

下列程序適用於已啟用裝置控制功能的保護計劃。

將 USB 裝置新增至資料庫

1. 開啟裝置的保護計劃進行編輯：
   按一下保護計劃名稱旁的省略符號 (...)，然後選擇 **[編輯]**。

   注意事項
   計劃中必須啟用裝置控制，您才可以存取裝置控制設定。

2. 按一下 **[裝置控制]** 開關旁的箭頭圖示以展開設定，然後按一下 **[USB 裝置允許名單]** 旁的連結。
3. 在出現的 **[USB 裝置允許名單]** 頁面上，按一下 **[從資料庫新增]**。
4. 在出現的 USB 裝置資料庫管理頁面上，按一下 **[新增至資料庫]**。
5. 在出現的 **[新增 USB 裝置]** 對話方塊中，按一下連接 USB 裝置的電腦。
   只有連線的電腦會顯示在電腦清單中。
   系統僅會針對已安裝資料洩漏防禦用代理程式的電腦，顯示 USB 裝置的清單。
   USB 裝置列在樹狀目錄檢視中。樹狀目錄的第一層表示裝置型號。第二層則表示該行號的特定裝置。
   裝置描述旁的藍色圖示表示裝置目前連接至電腦。如果裝置未連接至該電腦，圖示會呈現灰色。
6. 選擇要新增至資料庫的 USB 裝置的核取方塊，然後按一下 **[新增至資料庫]**。
   選擇的 USB 裝置隨即新增至資料庫。
7. 關閉或儲存保護計劃。

將 USB 裝置從電腦詳細資料面板新增至資料庫

注意事項
此程序僅適用於已連線且其上已安裝資料洩漏防禦用代理程式的裝置。您無法針對離線或未安裝資料洩漏防禦代理程式的電腦，檢視 USB 裝置的清單。

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 選擇已連接所需 USB 裝置的電腦，然後在右側的功能表中，按一下 **[清查]**。
   電腦詳細資料面板隨即開啟。
3. 在電腦詳細資料面板上，按一下 **[USB 裝置]** 索引標籤。
   所選電腦上已知 USB 裝置的清單隨即開啟。
   USB 裝置列在樹狀目錄檢視中。樹狀目錄的第一層表示裝置型號。第二層則表示該行號的特定裝置。

裝置描述旁的藍色圖示表示裝置目前連接至電腦。如果裝置未連接至該電腦，圖示會呈現灰色。

4. 選擇要新增至資料庫的 USB 裝置的核取方塊，然後按一下 **[新增至資料庫]**。

將 USB 裝置從服務警示新增至資料庫

1. 在 Cyber Protect 主控台中，移至 **[監控]** > **[警示]**。
2. 找出裝置控制警示，其會告知拒絕存取 USB 裝置。
3. 在警示的簡易檢視中，按一下 **[允許此 USB 裝置]**。
   如此會從存取控制排除 USB 裝置，並將其新增至資料庫，以供進一步參考。

透過將裝置清單匯入至資料庫來新增 USB 裝置

您可以將包含 USB 裝置清單的 JSON 檔案匯入至資料庫。請參閱 "將 USB 裝置的清單匯入至資料庫 " (第 317 頁)。

從資料庫移除 USB 裝置

1. 開啟裝置的保護計劃進行編輯：
   按一下保護計劃名稱旁的省略符號 (...)，然後選擇 **[編輯]**。

   注意事項
   計劃中必須啟用裝置控制，您才可以存取裝置控制設定。

2. 按一下 **[裝置控制]** 開關旁的箭頭以展開設定，然後按一下 **[USB 裝置允許名單]** 列。
3. 在出現的管理允許名單頁面上，按一下 **[從資料庫新增]**。
4. 在從資料庫選取 USB 裝置的頁面上，按一下代表裝置之清單項目尾端的省略符號 (...)，按一下 **[刪除]**，然後確認刪除。
   USB 裝置隨即從資料庫刪除。
5. 關閉或儲存保護計劃。

檢視裝置控制警示

裝置控制模組可以設定為引發警示，告知拒絕使用者嘗試使用特定裝置類型 (請參閱啟用或停用作業系統通知和服務警示)。使用下列步驟，檢視這些警示。

檢視裝置控制警示

1. 在 Cyber Protect 主控台中，移至 **[監控]** > **[警示]**。
2. 尋找具有下列狀態的警示：「週邊裝置存取遭到封鎖」。

如需進一步的詳細資料，請參閱裝置控制警示。

存取設定

在 **[存取設定]** 頁面上，您可以允許或拒絕存取特定類型的裝置，以及啟用或停用作業系統通知和裝置控制警示。

注意事項

在 [裝置控制] 中設定的存取設定在同時使用 [裝置控制] 和 [Advanced DLP] 保護工作負載時，可能會遭到覆寫。請參閱 "在保護計劃中啟用 Advanced Data Loss Prevention" (第 778 頁)。

存取設定可讓您限制使用者對下列裝置類型和連接埠的存取：

- **卸除式** (依裝置類型的存取控制) - 具有任何介面的裝置，這些介面可連接至作業系統視為卸除式儲存裝置 (例如，USB 隨身碟、讀卡機、電磁光碟機等) 的電腦 (USB、FireWire、PCMCIA、IDE、SATA、SCSI 等)。裝置控制可將透過 USB、FireWire 和 PCMCIA 連接的所有硬碟機分類為卸除式裝置。如果某些硬碟機 (通常具有 SATA 和 SCSI) 支援熱插拔功能，而且其上未安裝執行中的作業系統，則裝置控制也會將這些硬碟機分類為卸除式裝置。

  您可以對卸除式裝置允許完整存取、唯讀存取，或拒絕存取，從而控制將資料複製到受保護電腦上的任何卸除式裝置，或從受保護電腦上的任何卸除式裝置複製資料的作業。存取權限不會影響使用 BitLocker 或 FileVault 加密的裝置 (僅限 HFS+ 檔案系統)。

  Windows 和 macOS 都支援此裝置類型。
- **加密的卸除式裝置** (依裝置類型的存取控制) - 使用 BitLocker (在 Windows 上) 或 FileVault (在 macOS 上) 磁碟機加密來加密的卸除式裝置。

  在 macOS 上，僅支援使用 HFS+ (亦稱為 HFS Plus 或 Mac OS Extended，或 HFS Extended) 檔案系統的已加密卸除式磁碟機。使用 APFS 檔案系統的已加密卸除式裝置會被視為卸除式磁碟機。

  您可以對加密的卸除式裝置允許完整存取、唯讀存取，或拒絕存取，從而控制將資料複製到受保護電腦上的任何加密的卸除式裝置，或從受保護電腦上的任何加密的卸除式裝置複製資料的作業。存取權限僅會影響使用 BitLocker 或 FileVault 加密的裝置 (僅限 HFS+ 檔案系統)。

  Windows 和 macOS 都支援此裝置類型。
- **印表機** (依裝置類型的存取控制) - 具有可連接至電腦 (USB、LPT、藍牙等) 之任何介面的實體印表機，以及從網路上的電腦存取的印表機。

  您可以允許或拒絕存取印表機，從而控制在受保護電腦的任何印表機上列印文件。

  注意事項

  當您將印表機的存取設定變更為 **[拒絕]** 時，必須重新啟動存取印表機的應用程式和程序，才能強制執行新設定的存取設定。為確保已正確強制執行存取設定，請重新啟動受保護的工作負載。

  僅 Windows 支援此裝置類型。
- **剪貼簿** (依裝置類型的存取控制) - Windows 剪貼簿。

  您可以允許或拒絕存取剪貼簿，從而控制透過受保護電腦上 Windows 剪貼簿的複製和貼上作業。

  注意事項

  當您將剪貼簿的存取設定變更為 **[拒絕]** 時，必須重新啟動存取剪貼簿的應用程式和程序，才能強制執行新設定的存取設定。為確保已正確強制執行存取設定，請重新啟動受保護的工作負載。

  僅 Windows 支援此裝置類型。
- **螢幕擷取畫面擷取** (依裝置類型的存取控制) - 可擷取整個畫面、作用中視窗或畫面所選部分的螢幕擷取畫面。

您可以允許或拒絕存取螢幕擷取畫面擷取，從而控制受保護電腦上的螢幕擷取畫面擷取。

注意事項
當您將螢幕擷取畫面擷取的存取設定變更為 **[拒絕]** 時，必須重新啟動存取螢幕擷取畫面擷取的應用程式和程序，才能強制執行新設定的存取設定。為確保已正確強制執行存取設定，請重新啟動受保護的工作負載。

僅 Windows 支援此裝置類型。

- **行動裝置** (依裝置類型的存取控制) - 透過媒體傳輸通訊協定 (MTP) 通訊，且具有用於連接至電腦 (USB、IP、藍牙) 的任何介面的裝置 (例如，Android 智慧手機等)。
  您可以對行動裝置允許完整存取、允許唯讀存取，或拒絕存取，從而控制將資料複製到受保護電腦上的任何 MTP 型行動裝置，或從受保護電腦上的任何 MTP 型行動裝置複製資料的作業。

注意事項
當您將行動裝置的存取設定變更為 **[唯讀]** 或 **[拒絕]** 時，必須重新啟動存取行動裝置的應用程式和程序，才能強制執行新設定的存取設定。為確保已正確強制執行存取設定，請重新啟動受保護的工作負載。

僅 Windows 支援此裝置類型。

- **藍牙** (依裝置類型的存取控制) - 具有連接至電腦 (USB、PCMCIA 等) 的任何介面的外接式和內建式藍牙裝置。這個設定可控制此類型裝置的使用，而不是控制使用這類裝置交換資料。
  您可以允許或拒絕存取藍牙，從而控制在受保護的電腦上使用任何藍牙裝置。

注意事項
在 macOS 上，藍牙的存取權限不會影響藍牙 HID 裝置。系統一律允許對這些裝置的存取，以防在 iMac 和 Mac Pro 硬體上停用無線 HID 裝置 (滑鼠和鍵盤)。

Windows 和 macOS 都支援此裝置類型。

- **光碟機** (依裝置類型的存取控制) - 具有連接至電腦 (IDE、SATA、USB、FireWire、PCMCIA 等) 的任何介面的外接式和內建式 CD/DVD/BD 光碟機 (包括編寫器)。
  您可以對光碟機允許完整存取、允許唯讀存取，或拒絕存取，從而控制將資料複製到受保護電腦上的任何光碟機，或從受保護電腦上的任何光碟機複製資料的作業。
  Windows 和 macOS 都支援此裝置類型。
- **軟碟機** (依裝置類型的存取控制) - 具有連接至電腦 (IDE、USB、PCMCIA 等) 的任何介面的外接式和內建式軟碟機。作業系統會將某些軟碟機型號視為卸除式磁碟機，在此情況下，裝置控制也會將這些磁碟機視為卸除式裝置。
  您可以對軟碟機允許完整存取、允許唯讀存取，或拒絕存取，從而控制將資料複製到受保護電腦上的任何軟碟機，或從受保護電腦上的任何軟碟機複製資料的作業。
  僅 Windows 支援此裝置類型。
- **USB** (依裝置介面的存取控制) - 連接至 USB 連接埠的任何裝置，但集線器除外。
  您可以對 USB 連接埠允許完整存取、允許唯讀存取，或拒絕存取，從而控制將資料複製到受保護電腦上連接到任何 USB 連接埠的裝置，或從受保護電腦上連接到任何 USB 連接埠的裝置複製資料的作業。

Windows 和 macOS 都支援此裝置類型。

- **FireWire** (依裝置介面的存取控制) - 連接至 FireWire (IEEE 1394) 連接埠的任何裝置，但集線器除外。

  您可以對 FireWire 連接埠允許完整存取、允許唯讀存取，或拒絕存取，從而控制將資料複製到受保護電腦上連接到任何 FireWire 連接埠的裝置，或從受保護電腦上連接到任何 FireWire 連接埠的裝置複製資料的作業。

  Windows 和 macOS 都支援此裝置類型。

- **重新導向的裝置** (依裝置介面的存取控制) - 重新導向至虛擬應用程式/桌面工作階段的對應磁碟機 (硬碟機、卸除式磁碟機、光碟機)、USB 裝置以及剪貼簿。

  裝置控制在受保護 Windows 電腦上託管的 Microsoft RDS、Citrix XenDesktop、Citrix XenApp、Citrix XenServer 和 VMware Horizon 虛擬化環境中，可識別透過 Microsoft RDP、Citrix ICA、VMware PCoIP 和 HTML5/WebSocket 遠端通訊協定重新導向的裝置。它也可以控制在 VMware Workstation、VMware Player、Oracle VM VirtualBox 或 Windows Virtual PC 上執行之客體作業系統的 Windows 剪貼簿，以及在受保護 Windows 電腦上執行之主機作業系統的剪貼簿之間的資料複製作業。

  僅 Windows 支援此裝置類型。

  您可以設定對重新導向裝置的存取，如下所示：

  - **對應磁碟機** - 允許完整存取、允許唯讀存取或拒絕存取，從而控制將資料複製到重新導向至受保護電腦上託管之工作階段的任何硬碟機、卸除式磁碟機或光碟機，或從重新導向至受保護電腦上託管之工作階段的任何硬碟機、卸除式磁碟機或光碟機複製資料的作業。
  - **剪貼簿傳入** - 允許或拒絕存取，從而控制透過剪貼簿，將資料複製到受保護電腦上託管的工作階段的作業。

    注意事項
    當您將剪貼簿傳入的存取設定變更為 **[拒絕]** 時，必須重新啟動存取剪貼簿的應用程式和程序，才能強制執行新設定的存取設定。為確保已正確強制執行存取設定，請重新啟動受保護的工作負載。

  - **剪貼簿傳出** - 允許或拒絕存取，從而控制透過剪貼簿，從受保護電腦上託管的工作階段複製資料的作業。

    注意事項
    當您將剪貼簿傳出的存取設定變更為 **[拒絕]** 時，必須重新啟動存取剪貼簿的應用程式和程序，才能強制執行新設定的存取設定。為確保已正確強制執行存取設定，請重新啟動受保護的工作負載。

  - **USB 連接埠** - 允許或拒絕存取，從而控制將資料複製到連接至任何 USB 連接埠 (重新導向至受保護電腦上託管的工作階段) 的裝置，或從連接至任何 USB 連接埠 (重新導向至受保護電腦上託管的工作階段) 的裝置複製資料的作業。

裝置控制設定會同樣地影響所有使用者。例如，如果您拒絕存取卸除式裝置，您會防止任何使用者將資料複製到受保護電腦上的這類裝置，以及從受保護電腦上的這類裝置複製資料。您可以從存取控制排除個別的 USB 裝置，以選擇性地允許存取個別的 USB 裝置 (請參閱裝置類型允許名單和 USB 裝置允許名單)。

對裝置的存取同時受到其類型和介面的控制時，在介面層級拒絕存取優先。例如，如果拒絕存取 USB 連接埠 (裝置介面)，則無論允許還是拒絕存取行動裝置 (裝置類型)，都會拒絕存取連接至 USB 連接埠的行動裝置。若要允許存取這種裝置，您必須同時允許其介面和類型。

注意事項
如果在 macOS 上使用的保護計劃的設定適用於僅在 Windows 上受支援的裝置類型，則在 macOS 上將忽略這些裝置類型的設定。

重要事項
當卸除式裝置、加密的卸除式裝置、印表機或藍牙裝置連接至 USB 連接埠時，允許存取該裝置將優先於在 USB 介面層級設定的拒絕存取。如果您允許這種裝置類型，則無論是否拒絕存取 USB 連接埠，都允許存取裝置。

作業系統通知和服務警示

您可以設定裝置控制在終端使用者嘗試在受保護的電腦上使用封鎖的裝置類型時，向其顯示作業系統通知。如果在存取設定中選取 **[當終端使用者嘗試使用封鎖的裝置類型或連接埠時，向其顯示作業系統通知]** 核取方塊，代理程式會在發生下列任何事件時，在受保護電腦的通知區域中顯示快顯訊息：

- 拒絕嘗試使用 USB 或 FireWire 連接埠上的裝置。每當使用者插入在介面層級 (例如，拒絕存取 USB 連接埠時) 或在類型層級 (例如，拒絕使用卸除式裝置時) 拒絕的 USB 或 FireWire 裝置時，就會出現這個通知。此通知會告知不允許使用者存取指定的裝置/磁碟機。
- 拒絕嘗試從特定裝置複製資料物件 (例如檔案)。拒絕對下列裝置進行讀取存取時，將會出現這個通知：軟碟機、光碟機、卸除式裝置、加密的卸除式裝置、行動裝置、重新導向的對應磁碟機，以及重新導向的剪貼簿傳入資料。此通知會告知不允許使用者從指定的裝置取得指定的資料物件。

  拒絕對藍牙、FireWire 連接埠、USB 連接埠以及重新導向的 USB 連接埠進行讀取/寫入存取時，也會顯示拒絕讀取通知。
- 拒絕嘗試將資料物件 (例如檔案) 複製到特定裝置。拒絕對下列裝置進行寫入存取時，將會出現這個通知：軟碟機、光碟機、卸除式裝置、加密的卸除式裝置、行動裝置、本機剪貼簿、螢幕擷取畫面擷取、印表機、重新導向的對應磁碟機，以及重新導向的剪貼簿傳出資料。此通知會告知不允許使用者將指定的資料物件傳送到指定的裝置。

使用者嘗試在受保護的電腦上存取封鎖的裝置類型可能會引發在 Cyber Protect 主控台中記錄的警示。在存取設定中選取 **[顯示警示]** 核取方塊可以分別為每個裝置類型 (螢幕擷取畫面擷取除外) 或連接埠啟用警示。例如，如果對卸除式裝置的存取限制為唯讀，且已針對該裝置類型選取 **[顯示警示]** 核取方塊，則每次使用者在受保護的電腦上嘗試將資料複製到卸除式裝置時，就會記錄一個警示。如需進一步的詳細資料，請參閱裝置控制警示。

另請參閱啟用或停用作業系統通知和服務警示的步驟。

裝置類型允許名單

在 **[裝置類型允許名單]** 頁面上，您可以選擇要從裝置存取控制排除的裝置子類別。結果，無論裝置控制模組中的存取設定為何，都允許存取這些裝置。

裝置控制模組可以讓您選擇允許存取拒絕的裝置類型中某些子類別的裝置。此選項可讓您拒絕某個特定類型的所有裝置，但此類型裝置的某些子類別除外。這可能非常實用，例如，當您需要拒絕存取所有 USB 連接埠，同時允許使用 USB 鍵盤和滑鼠時。

設定裝置控制模組時，您可以指定要從裝置存取控制排除的裝置子類別。當某個裝置屬於排除的子類別時，無論是否拒絕該裝置類型或連接埠，都允許存取該裝置。您可以從裝置存取控制，選擇性地排除下列裝置子類別：

- **USB HID (滑鼠、鍵盤等)** - 選取時，即使拒絕 USB 連接埠，也允許存取連接到 USB 連接埠的人性化介面裝置 (滑鼠、鍵盤等等)。預設會選取此項目，因此，拒絕存取 USB 連接埠並不會停用鍵盤或滑鼠。
  支援 Windows 和 macOS。
- **USB 和 FireWire 網路卡** - 選取時，即使拒絕 USB 連接埠和/或 FireWire 連接埠，也允許存取連接到 USB 或 FireWire (IEEE 1394) 連接埠的網路卡。
  支援 Windows 和 macOS。
- **USB 掃描器和靜止影像裝置** - 選取時，即使拒絕 USB 連接埠，也允許存取連接到 USB 連接埠的掃描器和靜止影像裝置。
  僅支援 Windows。
- **USB 音訊裝置** - 選取時，即使拒絕 USB 連接埠，也允許存取連接到 USB 連接埠的音訊裝置，例如耳機和麥克風。
  僅支援 Windows。
- **USB 攝影機** - 選取時，即使拒絕 USB 連接埠，也允許存取連接到 USB 連接埠的網路攝影機。
  僅支援 Windows。
- **藍牙 HID (滑鼠、鍵盤等)** - 選取時，即使拒絕藍牙，也允許存取透過藍牙連接的人性化介面裝置 (滑鼠、鍵盤等等)。
  僅支援 Windows。
- **應用程式內的剪貼簿複製/貼上** - 選取時，即使拒絕剪貼簿，也允許透過相同應用程式中的剪貼簿複製/貼上資料。
  僅支援 Windows。

注意事項
如果在已套用的保護計劃中設定這些設定，就會忽略不支援裝置子類別的設定。

將裝置類型加入允許名單時，請考慮以下情況：

- 您僅能透過裝置類型允許名單，允許整個裝置子類別。您無法在允許某個特定裝置型號的同時，拒絕其他所有相同子類別的裝置。例如，您可以透過從裝置存取控制排除 USB 攝影機，允許使用任何型號和廠商的 USB 攝影機。關於如何允許個別的裝置/型號，請參閱 USB 裝置允許名單。
- 您只能從裝置子類別的封閉式清單中選擇裝置類型。如果允許的裝置屬於不同的子類別，則無法透過使用裝置類型允許名單來允許該裝置。例如，USB 智慧卡讀取機之類的子類別無法新增到允許名單。若要在拒絕 USB 連接埠時允許 USB 智慧卡讀取機，請依照 USB 裝置允許名單中的指示進行。
- 裝置類型允許名單僅適用於使用標準 Windows 驅動程式的裝置。裝置控制可能無法辨識部分具有專屬驅動程式之 USB 裝置的子類別。因此，您無法使用裝置類型允許名單，允許對此類 USB 裝置的存取。在此情況下，您可以根據裝置/型號，允許存取 (請參閱 USB 裝置允許名單)。

USB 裝置允許名單

允許名單旨在允許使用特定 USB 裝置，而與其他任何裝置控制設定無關。您可以將個別的裝置或裝置型號新增至允許名單，以停用這些裝置的存取控制。例如，如果您將擁有唯一 ID 的行動裝置新增至允許名單，表示即使拒絕其他任何 USB 裝置，您也允許使用該特定裝置。

在 **[USB 裝置允許名單]** 頁面上，您可以指定要從裝置存取控制排除的個別 USB 裝置或 USB 裝置型號。結果，無論裝置控制模組中的存取設定為何，都允許存取這些裝置。

識別允許名單中的裝置有兩種方法：

- 裝置型號 - 共同識別特定型號的所有裝置。每個裝置型號都以廠商 ID (VID) 和產品 ID (PID) 識別，例如 USB\VID_0FCE&PID_E19E。

  這個 VID 和 PID 組合無法識別特定裝置，但是可以識別整個裝置型號。您可以透過將裝置型號新增到允許名單，允許對該型號任何裝置的存取。例如，如此一來，您可以允許使用特定型號的 USB 印表機。
- 唯一的裝置 - 識別特定的裝置。每個唯一的裝置都以廠商 ID (VID)、產品 ID (PID) 以及序號識別，例如 USB\VID_0FCE&PID_E19E\D55E7FCA。

  並非所有 USB 裝置都有獲指派序號。您只有裝置有在生產期間獲指派序號時，才可以將裝置以序號新增至允許名單。例如，擁有唯一序號的 USB 隨身碟。

若要將裝置新增至允許名單，您必須先將其新增至 USB 裝置資料庫。接著，您可以透過從該資料庫中選擇，將裝置新增至允許名單。

允許名單是在稱為 **USB 裝置允許名單**的個別設定頁面上管理的。清單中的每個項目都代表一個裝置或裝置型號，而且包含下列欄位：

- **描述** - 作業系統會在連接 USB 裝置時，指定特定的描述。您可以在 USB 裝置資料庫中修改裝置的描述 (請參閱 USB 資料庫管理頁面)。
- **裝置類型** - 如果清單項目代表唯一的裝置，請顯示 [唯一]；如果代表裝置型號，則顯示 [型號]。
- **唯讀** - 選取時，僅允許從裝置接收資料。如果裝置不支援唯讀存取，則對裝置的存取會遭到封鎖。清除此核取方塊可允許對裝置的完整存取。
- **重新初始化** - 選取時，會使裝置模擬在新使用者登入時中斷連接/重新連接。部分 USB 裝置需要重新初始化才能運作，因此建議您為這類裝置 (滑鼠、鍵盤等等) 選擇此核取方塊。同時建議您為資料儲存裝置 (USB 隨身碟、光碟機、外接式硬碟機等等) 清除此核取方塊。
  裝置控制可能無法重新初始化部分具有專屬驅動程式的 USB 裝置。如果無法存取此種裝置，您必須從 USB 連接埠移除 USB 裝置，然後再將其插回。

注意事項
[重新初始化] 欄位預設為隱藏狀態。若要在表格中顯示此欄，按一下表格右上角的齒輪圖示，然後選擇 **[重新初始化]** 核取方塊。

注意事項
在 macOS 上，不支援 **[唯讀]** 和 **[重新初始化]** 欄位。如果在已套用的保護計劃中設定這些欄位，將會遭到忽略。

您可以從允許名單中新增或移除裝置/型號，如下所示：

- 按一下清單上方的 **[從資料庫新增]**，然後從透過 USB 裝置資料庫登錄的裝置，選擇所需的裝置。所選裝置會新增至清單，您可以在其中進行設定並確認變更。
- 按一下警示中的 **[允許此 USB 裝置]**，告知拒絕存取 USB 裝置 (請參閱裝置控制警示)。如此會將裝置新增至允許名單以及 USB 裝置資料庫。
- 按一下清單項目尾端的刪除圖示。如此會從允許名單中移除個別的裝置/型號。

USB 裝置資料庫

裝置控制模組會維護 USB 裝置的資料庫，您可以從該資料庫中，將裝置新增到排除清單 (請參閱 USB 裝置允許名單)。使用下列任何一種方式，都可以向資料庫登錄 USB 裝置：

- 在將裝置新增至排除清單時出現的頁面上新增裝置 (請參閱 USB 裝置資料庫管理頁面)。
- 在 Cyber Protect 主控台中，從電腦 [清查] 窗格的 [USB 裝置] 索引標籤新增裝置 (請參閱電腦上的 USB 裝置清單)。
- 從拒絕存取 USB 裝置的警示允許裝置 (請參閱裝置控制警示)。

另請參閱從資料庫新增或移除 USB 裝置的步驟。

USB 裝置資料庫管理頁面

設定 USB 裝置的允許名單時，您可以選擇從資料庫新增裝置。如果您選擇此選項，將會出現管理頁面以及裝置清單。在此頁面上，您可以檢視向資料庫登錄的所有裝置的清單、您可以選擇要新增到允許名單的裝置，並執行下列作業：

向資料庫登錄裝置

1. 按一下頁面頂端的 **[新增至資料庫]**。
2. 在出現的 **[新增 USB 裝置]** 對話方塊中，選擇連接 USB 裝置的電腦。
   只有連線的電腦會顯示在電腦清單中。
   系統僅會針對已安裝資料洩漏防禦用代理程式的電腦，顯示 USB 裝置的清單。
   USB 裝置列在樹狀目錄檢視中。樹狀目錄的第一層表示裝置型號。第二層則表示該行號的特定裝置。
   裝置描述旁的藍色圖示表示裝置目前連接至電腦。如果裝置未連接至該電腦，圖示會呈現灰色。
3. 選擇要登錄的 USB 裝置的核取方塊，然後按一下 **[新增至資料庫]**。

變更裝置的描述

1. 在 **[USB 裝置資料庫]** 頁面上，按一下代表裝置之清單項目尾端的省略符號 (...)，然後按一下 **[編輯]**。
2. 在出現的對話方塊中，對描述進行變更。

從資料庫移除裝置

1. 按一下代表裝置之清單項目尾端的省略符號 (...)。
2. 按一下 **[刪除]**，並確認刪除。

針對每個裝置，頁面上的清單都會提供下列資訊：

- **描述** - 裝置可讀取的識別碼。您可以視需要變更描述。
- **裝置類型** - 如果清單項目代表唯一的裝置，請顯示 [唯一]；如果代表裝置型號，則顯示 [型號]。唯一的裝置必須具備序號以及廠商 ID (VID) 和產品 ID (PID)，其中裝置型號是以 VID 和 PID 的組合識別。
- **廠商 ID**、**產品 ID**、**序號** - 這些值共同組成裝置 ID，其格式為 USB\VID_<廠商 ID>&PID_<產品 ID>\<序號>。
- **帳戶** - 指出此裝置所屬的租用戶。此租用戶包含向資料庫登錄裝置所使用的使用者帳戶。

注意事項
此欄預設為隱藏狀態。若要在表格中顯示此欄，按一下表格右上角的齒輪圖示，然後選擇 **[帳戶]**。

最左側的欄用於選擇要新增至允許名單的裝置：選擇要新增的每個裝置的核取方塊，然後按一下 **[新增至允許名單]** 按鈕。若要選擇或清除所有核取方塊，按一下欄標頭中的核取方塊。

您可以搜尋或篩選裝置清單：

- 按一下頁面頂端的 **[搜尋]**，然後輸入一個搜尋字串。此清單會顯示其描述符合所輸入字串的裝置。
- 按一下 **[篩選]**，然後在出現的對話方塊中，設定並套用篩選。此清單限制為包含您在設定篩選時所選擇之類型、廠商 ID、產品 ID 和帳戶的裝置。若要取消篩選並列出所有裝置，按一下 **[重設為預設值]**。

匯出資料庫中的 USB 裝置清單

您可以匯出新增至資料庫的 USB 裝置的清單。

1. 開啟裝置的保護計劃進行編輯。
2. 按一下 **[裝置控制]** 開關旁的箭頭圖示以展開設定，然後按一下 **[USB 裝置允許名單]** 列。
3. 在 [USB 裝置允許名單] 頁面上，按一下 **[從資料庫新增]**。
4. 在出現的 USB 裝置資料庫管理頁面上，按一下 **[匯出]**。
   標準的 [瀏覽] 對話方塊隨即開啟。
5. 選擇您要儲存檔案的位置、輸入新的檔案名稱 (如有需要)，然後按一下 **[儲存]**。

USB 裝置的清單隨即匯出至 JSON 檔案。

您可以編輯所產生的 JSON 檔案，以便從中新增或移除裝置，並對裝置描述進行大量變更。

將 USB 裝置的清單匯入至資料庫

您可以匯入 USB 裝置的清單，而不必從 Cyber Protect 主控台新增 USB 裝置。此清單是一個 JSON 格式的檔案。

注意事項
您可以將 JSON 檔案匯入至不包含檔案中所述之裝置的資料庫。若要將修改過的檔案匯入至從中匯出該檔案的資料庫，您必須先清理資料庫，因為您無法匯入重複的項目。如果您匯出 USB 裝置的清單並加以修改，然後嘗試在不清理的情況下匯入至相同的資料庫，匯入將會失敗。

1. 開啟裝置的保護計劃進行編輯。
2. 按一下 **[裝置控制]** 開關旁的箭頭圖示以展開設定，然後按一下 **[USB 裝置允許名單]** 列。
3. 在 [USB 裝置允許名單] 頁面上，按一下 **[從資料庫新增]**。
4. 在出現的 USB 裝置資料庫管理頁面上，按一下 **[匯入]**。
   [從檔案匯入 USB 裝置] 對話方塊隨即開啟。
5. 使用拖放方式或瀏覽您要匯入的檔案。

Cyber Protect 主控台會檢查清單中是否包含已存在於資料庫的重複項目，並略過這些項目。在資料庫中找不到的 USB 裝置則會附加到該資料庫中。

電腦上的 USB 裝置清單

在 Cyber Protect 主控台中，電腦的 [清查] 面板包含 **[USB 裝置]** 索引標籤。如果電腦已連線且其上已安裝資料洩漏防禦用代理程式，則 **[USB 裝置]** 索引標籤會顯示曾經連接至該電腦的所有 USB 裝置的清單。

USB 裝置列在樹狀目錄檢視中。樹狀目錄的第一層表示裝置型號。第二層則表示該行號的特定裝置。

針對每個裝置，清單都會提供下列資訊：

- **描述** - 作業系統會在連接 USB 裝置時指派描述。此描述可以作為裝置可讀取的識別碼。
  裝置描述旁的藍色圖示表示裝置目前連接至電腦。如果裝置未連接至該電腦，圖示會呈現灰色。
- **裝置 ID** - 作業系統指派給裝置的識別碼。此識別碼的格式如下：有下列格式：USB\VID_<廠商 ID>&PID_<產品 ID>\<序號>，其中 <序號> 是選擇性的。範例：USB\VID_0FCE&PID_ADDE\D55E7FCA (含序號的裝置)；USB\VID_0FCE&PID_ADDE (不含序號的裝置)。

若要將裝置新增至 USB 裝置資料庫，請選擇所需裝置的核取方塊，然後按一下 **[新增至資料庫]** 按鈕。

從存取控制排除程序

您可以透過插入程序的勾點，控制對 Windows 剪貼簿、螢幕擷取畫面擷取、印表機和行動裝置的存取。如果程序未遭到攔截，對這些裝置的存取將不會受到控制。

注意事項
在 macOS 上不支援從存取控制排除程序。如果在已套用的保護計劃中設定排除程序的清單，將會遭到忽略。

在 **[排除]** 頁面上，您可以指定將不會遭到攔截的程序的清單。也就是說，剪貼簿 (本機和重新導向的)、螢幕擷取畫面擷取、印表機和行動裝置存取控制將不會套用到這類程序。

例如，您套用拒絕存取印表機的保護計劃，然後啟動 Microsoft Word 應用程式。嘗試從此應用程式列印將會遭到封鎖。但是如果您將 Microsoft Word 程序新增至排除清單，則應用程式將不會遭到封鎖。因此，從 Microsoft Word 列印將不會遭到封鎖，但是從其他應用程式列印仍將遭到封鎖。

將程序新增至排除

1. 開啟裝置的保護計劃進行編輯：
   按一下保護計劃名稱旁的省略符號 (...)，然後選擇 **[編輯]**。

   注意事項
   計劃中必須啟用裝置控制，您才可以存取裝置控制設定。

2. 按一下 **[裝置控制]** 開關旁的箭頭以展開設定，然後按一下 **[排除]** 列。
3. 在 **[排除]** 頁面上的 **[程序和資料夾]** 列中，按一下 **[+新增]**。
4. 新增您要從存取控制排除的程序。
   例如，`C:\Folder\subfolder\process.exe`。
   您可以使用萬用字元：
   - ***** 可取代任意數目的字元。
   - **?** 可取代一個字元。

   例如：

   ```
   C:\Folder\*
   *\Folder\SubFolder?\*
   *\process.exe
   ```
5. 按一下核取標記，然後按一下 **[完成]**。
6. 在保護計劃中，按一下 **[儲存]**。
7. 重新啟動您排除的程序，以確保已正確移除勾點。

無論剪貼簿、螢幕擷取畫面擷取、印表機和行動裝置的存取設定為何，已排除的程序都可以存取這些裝置。

從排除移除程序

開啟裝置的保護計劃進行編輯：

按一下保護計劃名稱旁的省略符號 (...)，然後選擇 **[編輯]**。

注意事項
計劃中必須啟用裝置控制，您才可以存取裝置控制設定。

1. 按一下 **[裝置控制]** 開關旁的箭頭以展開設定，然後按一下 **[排除]** 列。
2. 在 **[排除]** 頁面上，按一下您要從排除移除的程序旁的垃圾桶圖示。
3. 按一下**[完成]**。
4. 在保護計劃中，按一下 **[儲存]**。
5. 重新啟動程序，以確保已正確插入勾點。

保護計劃中的存取設定將會套用到您從排除移除的程序。

´編輯排除中的程序

1. 開啟裝置的保護計劃進行編輯：
   按一下保護計劃名稱旁的省略符號 (...)，然後選擇 **[編輯]**。

注意事項
計劃中必須啟用裝置控制，您才可以存取裝置控制設定。

2. 按一下 **[裝置控制]** 開關旁的箭頭以展開設定，然後按一下 **[排除]** 列。
3. 在 **[排除]** 頁面上，按一下您要編輯的程序旁的 **[編輯]** 圖示。
4. 套用變更，然後按一下核取標記確認。
5. 按一下**[完成]**。
6. 在保護計劃中，按一下 **[儲存]**。
7. 重新啟動受影響的程序以確保正確套用您的變更。

裝置控制警示

裝置控制透過追蹤使用者對存取控制的裝置類型、連接埠或介面的嘗試，維護事件記錄。部分事件可能會引發在 Cyber Protect 主控台中記錄的警示。例如，裝置控制模組可以設定為透過每次使用者嘗試將資料複製到此種裝置或從此種裝置複製資料時記錄的警示，防止使用卸除式裝置。

設定裝置控制模組時，您可以為列在裝置類型 (螢幕擷取畫面擷取除外) 或連接埠底下的大多數項目啟用警示。如果啟用警示，每個使用者對執行不允許的作業的嘗試都會產生一個警示。例如，如果對卸除式裝置的存取限制為唯讀，且已針對該裝置類型選取 **[顯示警示]** 選項，則每次使用者在受保護的電腦上嘗試將資料複製到卸除式裝置時，就會產生一個警示。

若要檢視 Cyber Protect 主控台中的警示，請移至 **[監控]** > **[警示]**。在每個裝置控制警示中，主控台都會針對個別事件提供下列資訊：

- **類型** - 警告。
- **狀態** - 顯示「週邊裝置存取遭到封鎖」。
- **訊息** - 顯示「存取『<電腦名稱>』上的『<裝置類型或連接埠>』遭到封鎖」。例如，「存取 'accountant-pc' 上的 'Removable' 遭到封鎖」。
- **日期和時間** - 事件發生的日期和時間。
- **裝置** - 事件發生所在電腦的名稱。
- **計劃名稱** - 導致事件發生的保護計劃的名稱。
- **來源** - 事件涉及的裝置類型或連接埠。例如，如果拒絕使用者嘗試存取卸除式裝置，此欄位會顯示「卸除式裝置」。
- **動作** - 導致事件發生的操作。例如，如果拒絕使用者嘗試將資料複製到裝置，此欄位會顯示「寫入」。如需詳細資訊，請參閱動作欄位值。
- **名稱** - 事件目標物件的名稱，例如，使用者嘗試複製的檔案，或使用者嘗試使用的裝置。如果無法識別目標物件，則不會顯示。
- **資訊** - 關於事件目標裝置的其他資訊，例如 USB 裝置的裝置 ID。如果沒有關於目標裝置的其他資訊可用，則不會顯示。
- **使用者** - 導致事件發生之使用者的名稱。
- **程序** - 導致事件發生之應用程式的可執行檔完整路徑。在某些情況下，可能會顯示程序名稱而非路徑。如果沒有可用的程序資訊，則不會顯示。

如果某個警示適用於 USB 裝置 (包括卸除式裝置和加密的卸除式裝置), 則系統管理員可以直接從警示中, 將裝置新增到允許名單, 如此可防止裝置控制模組限制對該特定裝置的存取。按一下 **[允許此 USB 裝置]** 可將其新增至裝置控制模組設定中的 USB 裝置允許名單, 也會將其新增至 [USB 裝置資料庫] 以供進一步參考。

另請參閱檢視裝置控制警示的步驟。

動作欄位值

[警示動作] 欄位可以包含下列值:

- **讀取** - 從裝置或連接埠取得資料。
- **寫入** - 將資料傳送至裝置或連接埠。
- **格式化** - 直接存取 (格式化、檢查磁碟等) 裝置。若是連接埠, 則適用於連接至該連接埠的裝置。
- **退出** - 從系統移除裝置, 或從裝置退出媒體。若是連接埠, 則適用於連接至該連接埠的裝置。
- **列印** - 將文件傳送到印表機。
- **複製音訊** - 透過本機剪貼簿複製/貼上音訊資料。
- **複製檔案** - 透過本機剪貼簿複製/貼上檔案。
- **複製影像** - 透過本機剪貼簿複製/貼上影像。
- **複製文字** - 透過本機剪貼簿複製/貼上文字。
- **複製未識別的內容** - 透過本機剪貼簿複製/貼上其他資料。
- **複製 RTF 資料 (影像)** - 使用 RTF 格式, 透過本機剪貼簿複製/貼上影像。
- **複製 RTF 資料 (檔案)** - 使用 RTF 格式, 透過本機剪貼簿複製/貼上檔案。
- **複製 RTF 資料 (文字、影像)** - 使用 RTF 格式, 透過本機剪貼簿複製/貼上文字以及影像。
- **複製 RTF 資料 (文字、檔案)** - 使用 RTF 格式, 透過本機剪貼簿複製/貼上文字以及檔案。
- **複製 RTF 資料 (影像、檔案)** - 使用 RTF 格式, 透過本機剪貼簿複製/貼上影像以及檔案。
- **複製 RTF 資料 (文字、影像、檔案)** - 使用 RTF 格式, 透過本機剪貼簿複製/貼上文字以及影像和檔案。
- **刪除** - 從裝置 (例如, 卸除式裝置、行動裝置等等) 刪除資料。
- **裝置存取** - 存取特定裝置或連接埠 (例如, 藍牙裝置、USB 連接埠等等)。
- **傳入音訊** - 透過重新導向的剪貼簿, 將音訊資料從用戶端電腦複製/貼上到裝載的工作階段。
- **傳入檔案** - 透過重新導向的剪貼簿, 將檔案從用戶端電腦複製/貼上到裝載的工作階段。
- **傳入影像** - 透過重新導向的剪貼簿, 將影像從用戶端電腦複製/貼上到裝載的工作階段。
- **傳入文字** - 透過重新導向的剪貼簿, 將文字從用戶端電腦複製/貼上到裝載的工作階段。
- **傳入未識別的內容** - 透過重新導向的剪貼簿, 將其他資料從用戶端電腦複製/貼上到裝載的工作階段。
- **傳入 RTF 資料 (影像)** - 使用 RTF 格式, 透過重新導向的剪貼簿, 將影像從用戶端電腦複製/貼上到裝載的工作階段。
- **傳入 RTF 資料 (檔案)** - 使用 RTF 格式, 透過重新導向的剪貼簿, 將檔案從用戶端電腦複製/貼上到裝載的工作階段。
- **傳入 RTF 資料 (文字、影像)** - 使用 RTF 格式, 透過重新導向的剪貼簿, 將文字以及影像從用戶端電腦複製/貼上到裝載的工作階段。

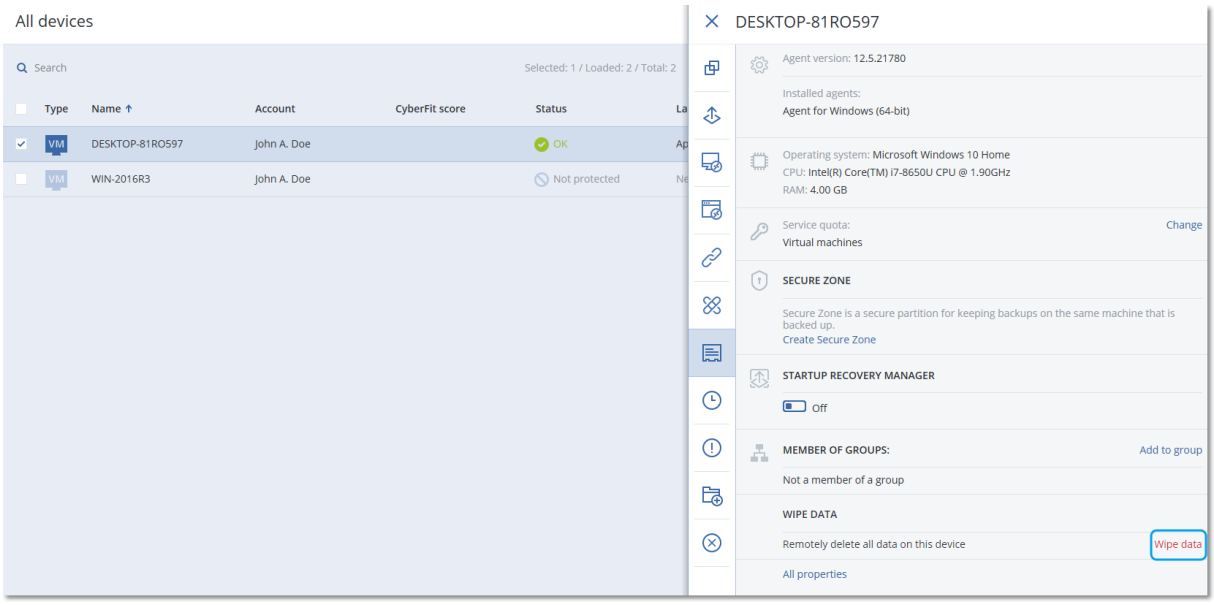
- **傳入 RTF 資料 (文字、檔案)** - 使用 RTF 格式，透過重新導向的剪貼簿，將文字以及檔案從用戶端電腦複製/貼上到裝載的工作階段。
- **傳入 RTF 資料 (影像、檔案)** - 使用 RTF 格式，透過重新導向的剪貼簿，將影像以及檔案從用戶端電腦複製/貼上到裝載的工作階段。
- **傳入 RTF 資料 (文字、影像、檔案)** - 使用 RTF 格式，透過重新導向的剪貼簿，將文字以及影像和檔案從用戶端電腦複製/貼上到裝載的工作階段。
- **插入** - 連接 USB 裝置或 FireWire 裝置。
- **傳出音訊** - 透過重新導向的剪貼簿，將音訊資料從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出檔案** - 透過重新導向的剪貼簿，將檔案從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出影像** - 透過重新導向的剪貼簿，將影像從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出文字** - 透過重新導向的剪貼簿，將文字從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出未識別的內容** - 透過重新導向的剪貼簿，將其他資料從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出 RTF 資料 (影像)** - 使用 RTF 格式，透過重新導向的剪貼簿，將影像從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出 RTF 資料 (檔案)** - 使用 RTF 格式，透過重新導向的剪貼簿，將檔案從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出 RTF 資料 (文字、影像)** - 使用 RTF 格式，透過重新導向的剪貼簿，將文字以及影像從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出 RTF 資料 (文字、檔案)** - 使用 RTF 格式，透過重新導向的剪貼簿，將文字以及檔案從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出 RTF 資料 (影像、檔案)** - 使用 RTF 格式，透過重新導向的剪貼簿，將影像以及檔案從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出 RTF 資料 (文字、影像、檔案)** - 使用 RTF 格式，透過重新導向的剪貼簿，將文字以及影像和檔案從裝載的工作階段複製/貼上到用戶端電腦。
- **重新命名** - 將裝置 (例如，卸除式裝置、行動裝置等等) 上的檔案重新命名。

從受管理的工作負載抹除資料

注意事項
Advanced Security 套件提供遠端抹除功能。

遠端抹除可讓 Cyber Protection 服務系統管理員和電腦擁有者刪除受管理電腦上的資料，例如，當資料遺失或遭竊時。因此，將會防止任何未經授權者存取機密資訊。

遠端抹除僅適用於執行 Windows 10 及更新版本的電腦。若要收到抹除命令，必須開啟電腦並連線到網際網路。



從電腦中抹除資料

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 選擇您要抹除其資料的電腦。

   注意事項
   您一次可以抹除一部電腦中的資料。

3. 按一下 **[詳細資料]**，然後按一下 **[抹除資料]**。
   如果您選擇的電腦離線，則無法存取 **[抹除資料]** 選項。
4. 確認選擇項目。
5. 輸入此電腦本機系統管理員的認證，然後按一下 **[抹除資料]**。

   注意事項
   您可以在 **[監控]** > **[活動]** 中檢查抹除程序以及啟動者的詳細資料。

CyberApp 工作負載

CyberApp 工作負載是由 ISV (獨立軟體供應商) 所建立，在您啟用 CyberApp 整合之後，將會出現在 Cyber Protect 主控台中。必須符合以下條件：

- 必須在 CyberApp 中啟用**工作負載和動作**擴充點。
- 必須在 CyberApp 中定義至少一個**工作負載類型**。
- ISV 託管的連接器服務必須確保已將 CyberApp 工作負載新增並更新至 Acronis 平台。

如需有關供應商入口網站以及如何建立 CyberApp 的詳細資訊，請參閱《供應商入口網站使用指南》。

彙總的工作負載

實體工作負載可以同時安裝 Cyber Protect 代理程式和一或多個 CyberApp 代理程式。在此情況下，相同的工作負載在 **[所有裝置]** 畫面上將有多種表示法，亦即，將針對 Acronis 工作負載和每個 CyberApp 工作負載顯示個別的記錄。如果從供應商入口網站或從 Cyber Protect 主控台啟用並設定自動合併工作負載，則系統將會比較 Acronis 工作負載與 CyberApp 工作負載的主機位址和 MAC 位址，而且會將所有表示法合併為彙總的單一工作負載。您也可以在 Cyber Protect 主控台中手動合併和取消合併工作負載。

使用 CyberApp 工作負載

除了內建到 Cyber Protect 主控台中的標準動作之外，您可以執行在主控台中出現 CyberApp 工作負載之後可用的動作：將工作負載手動合併到彙總的工作負載，以及執行在 CyberApp 中設定的自訂動作。

合併

必要條件

- 來自不同來源的工作負載可供租用戶使用。

您可以將 Acronis 工作負載與一或多個 CyberApp 工作負載手動合併到彙總的單一工作負載中。

若要將工作負載手動合併到彙總的工作負載中

1. 在 **[所有裝置]** 畫面中，選擇您要合併的工作負載。

   注意事項
   如果您選擇來自不同來源的工作負載 (例如 Acronis 工作負載和 CyberApp 工作負載)，則會顯示合併動作。

2. 按一下 **[合併工作負載]**。

執行自訂動作

必要條件

- 為租用戶啟用一個已定義**工作負載動作**的 CyberApp 整合。

自訂動作是在 CyberApp 中設定的動作，當您為租用戶啟用 CyberApp 整合時，這些動作可用於對應的 CyberApp 工作負載。

若要執行自訂動作

1. 在 **[所有裝置]** 畫面中，按一下工作負載。
2. 按一下 **[整合式應用程式動作]**。
3. 按一下該動作。

使用彙總的工作負載

除了內建到 Cyber Protect 主控台中的標準動作之外，您可以使用彙總的工作負載執行以下作業：檢視詳細資料、取消合併來源工作負載，以及執行在 CyberApp 中設定的自訂動作。

檢視詳細資料

必要條件

- 至少一個彙總的工作負載可供租用戶使用。

若要檢視彙總的工作負載詳細資料

1. 在 **[所有裝置]** 畫面中，按一下彙總的工作負載。
2. 按一下**[詳細資料]**。
   彙總的工作負載詳細資料會分為多個索引標籤。每個索引標籤都會顯示每個工作負載表示法的詳細資料。

取消合併

必要條件

- 至少一個彙總的工作負載可供租用戶使用。

當您取消合併彙總的工作負載時，裝置清單中將不會再顯示該工作負載。您將針對已合併到彙總工作負載的每個來源工作負載，檢視個別的項目。

若要取消合併彙總的工作負載

1. 在 **[所有裝置]** 畫面中，按一下您要取消合併的彙總工作負載。
2. 按一下 **[取消合併來源工作負載]**。
3. 在確認視窗中，按一下 **[取消合併]**。

執行自訂動作

必要條件

- 至少為租用戶啟用一個已定義**工作負載動作**的 CyberApp 整合。

自訂動作是在 CyberApp 中設定的動作，當您為租用戶啟用 CyberApp 整合時，這些動作可用於對應的 CyberApp 工作負載。

若要執行自訂動作

1. 在 **[所有裝置]** 畫面中，按一下工作負載。
2. 按一下 **[整合式應用程式動作]**。
3. 根據可用的自訂動作而定，執行以下其中一項操作。
   - 如果彙總的工作負載有一個 CyberApp 工作負載，按一下該動作。
   - 如果彙總的工作負載有多個 CyberApp 工作負載，按一下 CyberApp 的名稱，然後按一下該動作。

找出最後登入的使用者

系統管理員為了管理裝置，必須識別正登入和曾登入裝置的使用者。此資訊會顯示在[儀表板]或工作負載詳細資訊中。

您可以啟用或停用在 [遠端管理計劃] 中顯示 [上次登入資訊]。

在儀表板中：

1. 按一下 **[裝置]**。會顯示 **[所有裝置]** 視窗。
2. 在**[上次登入]**欄中，會顯示每個裝置上次登入的使用者的名稱。
3. 在**[上次登入時間]**欄中，會顯示每個裝置上次有使用者登入的時間。

在裝置詳細資訊中：

1. 按一下 **[裝置]**。會顯示 **[所有裝置]** 視窗。
2. 按一下要檢驗詳細資訊的裝置。
3. 按一下 **[詳細資訊]** 圖示。在 **[上次登入的使用者]** 區段中，會顯示所選裝置上次登入的使用者的名稱、登入的日期和時間。

注意事項
在 **[上次登入的使用者]** 區段中，會顯示最多 5 名登入至該裝置的使用者。

若要顯示或隱藏儀表板中 [上次登入] 和 [上次登入時間] 等欄

1. 按一下 **[裝置]**。會顯示 **[所有裝置]** 視窗。
2. 按一下右上角的齒輪圖示，並進行 **[一般]** 區段中以下其中一項操作：
   - 若要在儀表板中顯示，請啟用 **[上次登入]** 和 **[上次登入時間]** 等欄。
   - 若要在儀表板中隱藏，請停用 **[上次登入]** 和 **[上次登入時間]** 等欄。

電腦的 #CyberFit 分數

#CyberFit 分數為您提供一個安全評估和評分機制，可評估電腦的安全態勢。此分數可識別 IT 環境中的安全漏洞以及向端點開放的攻擊媒介，並以報告的形式提供改進的建議動作。所有 Cyber Protect 版本都提供這項功能。

下列系統支援 #CyberFit 分數功能：

- Windows 7 (第一版) 和更新版本
- Windows Server 2008 R2 和更新版本

運作原理

電腦上安裝的保護代理程式會執行安全評估，並計算電腦的 #CyberFit 分數。系統會定期自動重新計算電腦的 #CyberFit 分數。

#CyberFit 評分機制

系統會根據下列指標，計算電腦的 #CyberFit 分數：

- 反惡意程式碼保護 0-275
- 備份保護 0-175
- 防火牆 0-175
- 虛擬私人網路 (VPN) 0-75
- 完整磁碟加密 0-125
- 網路安全 0-25

電腦的 #CyberFit 分數上限為 850。

公制	評估的內容為何？	對使用者的建議	評分
反惡意程式碼	代理程式會檢查電腦上是否安裝反惡意程式碼軟體。	發現： • 您已啟用反惡意程式碼保護 (+275 分) • 您沒有反惡意程式碼保護，您的系統可能有風險 (0 分) #CyberFit 分數提供的建議： 您應該在電腦上安裝並啟用反惡意程式碼解決方案，才能持續防禦安全風險。 如需建議的反惡意程式碼解決方案清單，請參閱 AV-Test 或 AV-Comparatives 等網站。	275 - 電腦上已安裝反惡意程式碼軟體 0 - 電腦上未安裝反惡意程式碼軟體
備份	代理程式會檢查電腦上是否安裝備份解決方案。	發現： • 您有可保護您資料的備份解決方案 (+175 分) • 找不到備份解決方案，您的資料可能有風險 (0 分) #CyberFit 分數提供的建議： 建議您定期備份資料以防止資料遺失或勒索軟體攻擊。以下是您應該考慮使用的一些備份解決方案： • Acronis Cyber Protect / Cyber Backup / True Image • Windows Server Backup (Windows Server 2008 R2 和更新版本)	175 - 電腦上已安裝備份解決方案 0 - 電腦上未安裝備份解決方案
防火牆	代理程式會檢查環境中是否有防火牆並已啟用。 代理程式會執行下列操作： 1.檢查 Windows 防火牆和網路保護是	發現： • 您已針對公用網路和私人網路啟用防火牆，或找到協力廠商防火牆解決方案 (+175 分) • 您僅針對公用網路啟用防火牆 (+100 分) • 您僅針對私人網路啟用防火牆 (+75 分) • 您未啟用防火牆，您的網路連線不安全 (0 分) #CyberFit 分數提供的建議：	100 - Windows 公用防火牆已啟用 75 - Windows 私人防火牆已啟用 175 - Windows

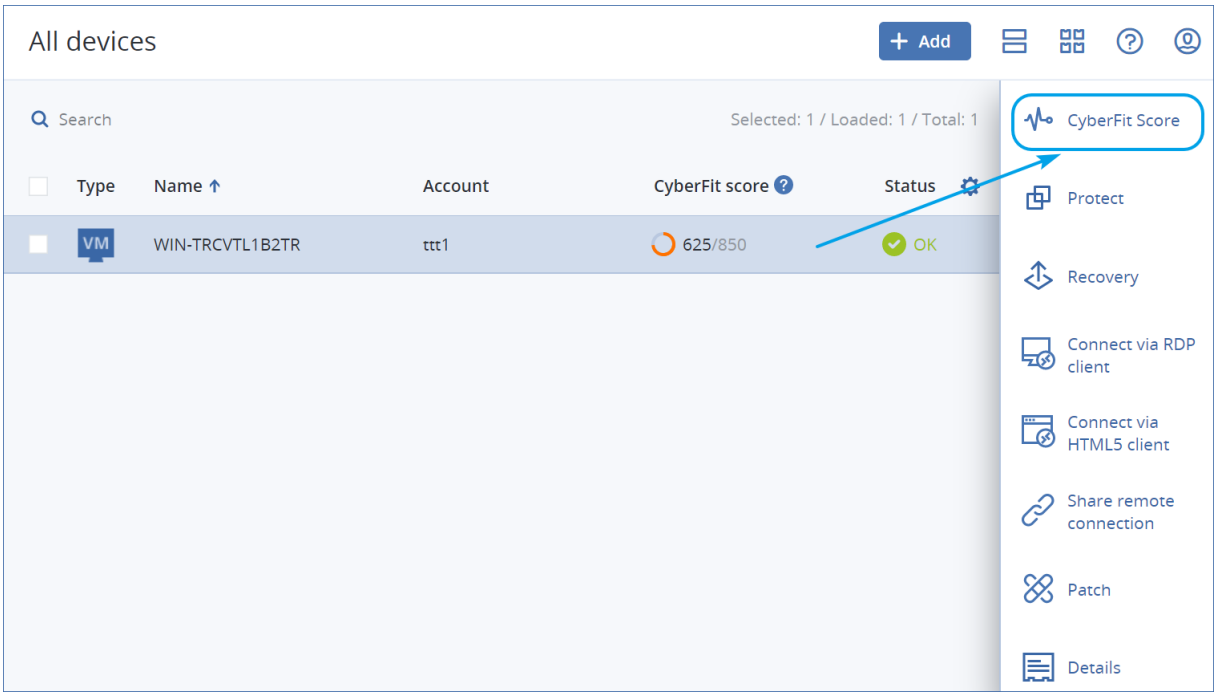
	否已開啟公用防火牆。 2。檢查 Windows 防火牆和網路保護是否已開啟私人防火牆。 3.檢查協力廠商防火牆解決方案/代理程式是否已停用 Windows 公用和私人防火牆。	建議為您的公用和私人網路啟用防火牆，以提高對系統上惡意攻擊的安全保護。以下是根據您的安全性需求和網路架構，提供有關設定 Windows 防火牆的詳細指南： 適用於使用者/員工的指南： 如何在 PC 上設定 Windows Defender 防火牆 如何在 PC 上設定 Windows 防火牆 適用於系統管理員和工程師的指南： 如何使用進階安全性部署 Window Defender 防火牆 如何在 Windows 防火牆中建立進階規則	公用和私人防火牆已啟用 或者 第三方防火牆解決方案已啟用 0 - 未啟用 Windows 防火牆，也未啟用協力廠商防火牆解決方案
虛擬私人網路 (VPN)	代理程式會檢查電腦上是否已安裝 VPN 解決方案，且是否已啟用 VPN 並在執行中。	發現： • 您有 VPN 解決方案，因此可以在公用網路和共用網路上安全地接收和傳送資料 (+75 分) • 找不到 VPN 解決方案，您與公用網路和共用網路的連線不安全 (0 分) #CyberFit 分數提供的建議： 建議您使用 VPN 存取您的公司網路和機密資料。使用 VPN 確保您的通訊安全並維持私密性至關重要，尤其是當您使用咖啡店、圖書館、機場等地方的免費網際網路存取時。以下是您應該考慮使用的一些 VPN 解決方案： • Acronis Business 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 - 已啟用 VPN 並在執行中 0 - 未啟用 VPN
磁碟加密	代理程式會檢查電腦是否已啟用磁碟	發現： • 您已啟用完整磁碟加密，您的電腦受到保護，免受	125 - 所有磁碟都經過加密

	加密。 代理程式會檢查是否已開啟 Windows BitLocker。	實體竄改影響 (+125 分) • 只有部分硬碟機經過加密，您的電腦可能面臨實體竄改的風險 (+75 分) • 找不到磁碟加密，您的電腦面臨實體竄改的風險 (0 分) #CyberFit 分數提供的建議： 建議您開啟 Windows BitLocker 以提高資料和檔案的保護。 指南：如何在 Windows 上開啟裝置加密	75 - 您的磁碟中至少有一個磁碟經過加密，但也有未加密的磁碟 0 - 未加密任何磁碟
網路安全 (遠端伺服器的輸出 NTLM 流量)	代理程式會檢查電腦對遠端伺服器是否有限制輸出 NTLM 流量。	發現： • 遠端伺服器的輸出 NTLM 流量遭到拒絕，您的認證受到保護 (+25 分) • 遠端伺服器的輸出 NTLM 流量未遭到拒絕，您的認證可能容易暴露 (0 分) #CyberFit 分數提供的建議： 建議拒絕遠端伺服器的所有輸出 NTLM 流量，以獲得更好的安全防護。您可以依照下列連結，找到如何變更 NTLM 設定以及新增例外的相關資訊。 指南：限制遠端伺服器的輸出 NTLM 流量	25 - 輸出 NTLM 流量設為 [全部拒絕] 0 - 輸出 NTLM 流量設為另一個值

根據授予每個指標的加總分數，電腦的 #CyberFit 總分可以滿足以下反映端點保護層級的其中一個評分：

- 0 - 579 - 差
- 580 - 669 - 尚可
- 670 - 739 - 好
- 740 - 799 - 非常好
- 800 - 850 - 非常出色

您可以在 Cyber Protect 主控台中查看電腦的 #CyberFit 分數：移至 **[裝置]** > **[所有裝置]**。在裝置清單中，您可以看到 **[#CyberFit 分數]** 欄。您也可以為電腦執行 #CyberFit 分數掃描以檢查其安全態勢。

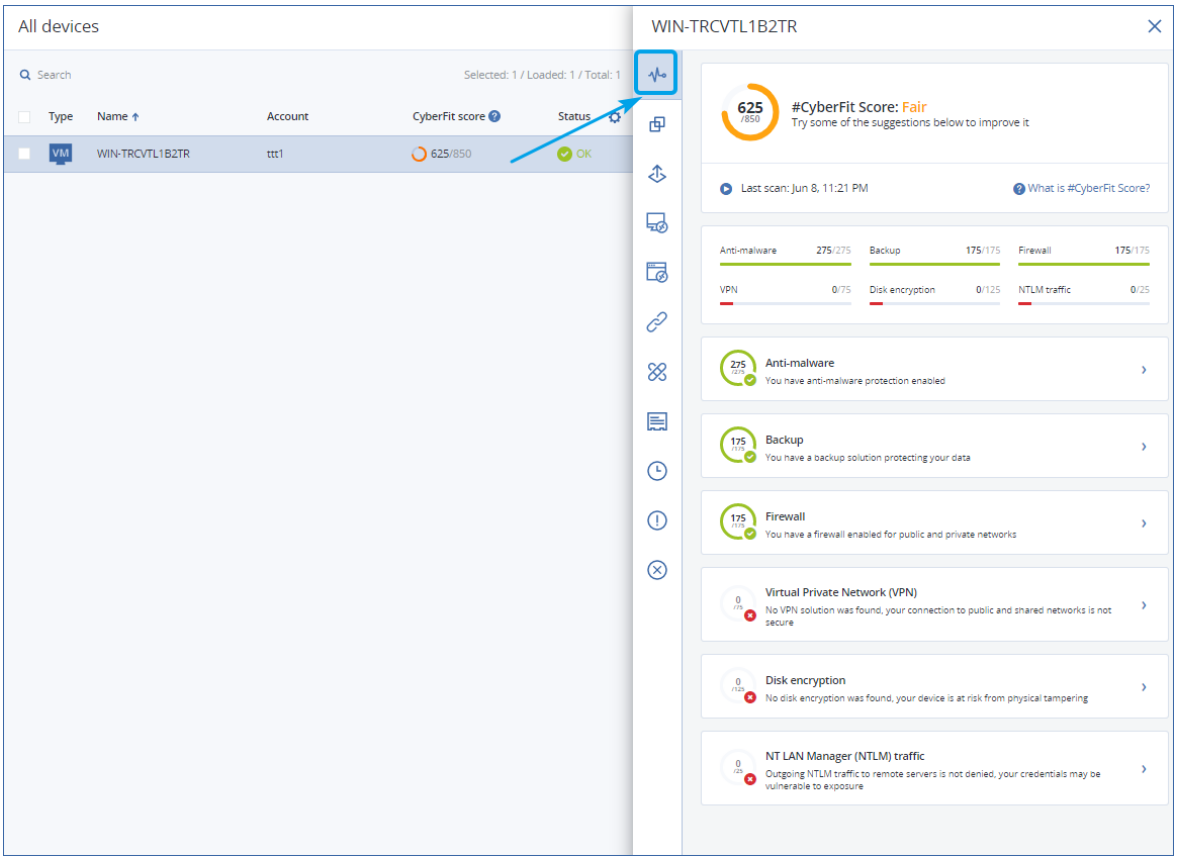


您也可以在對應的桌面小工具和報告頁面中，取得 #CyberFit 分數的相關資訊。

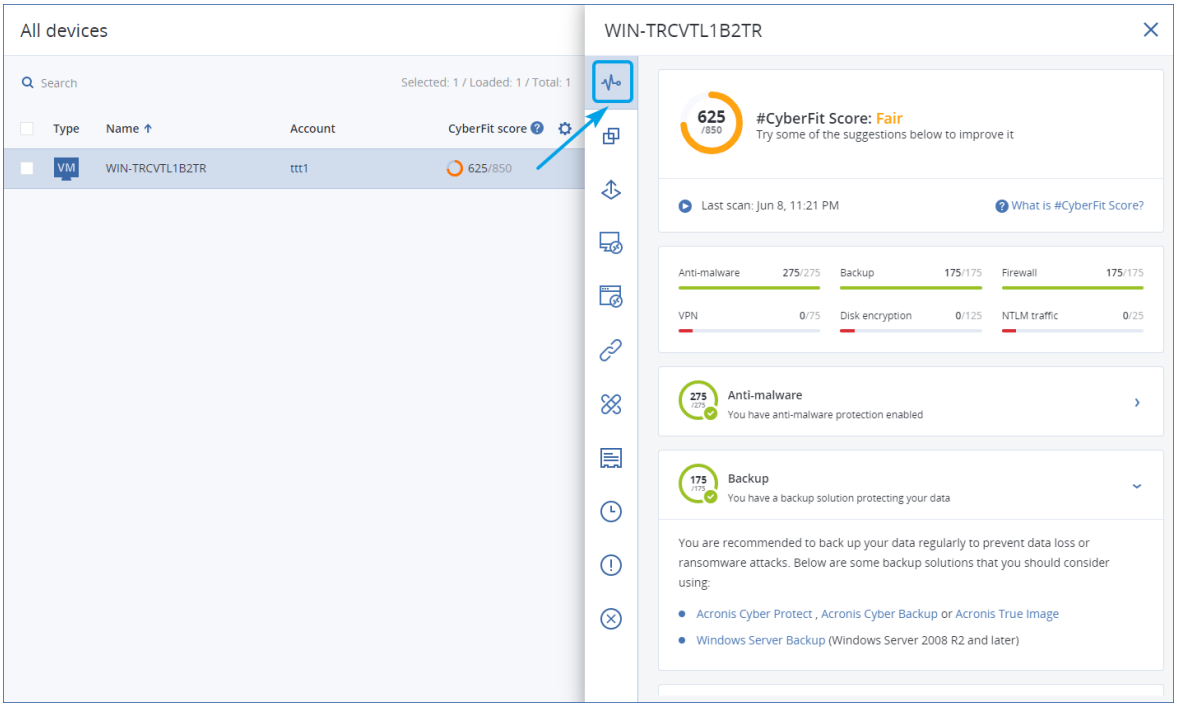
執行 #CyberFit 分數掃描

若要執行 #CyberFit 分數掃描

1. 在 Cyber Protect 主控台中，移至 **[裝置]**。
2. 選擇電腦，然後按一下 **[#CyberFit 分數]**。
3. 如果之前從未掃描過電腦，則按一下 **[執行第一次掃描]**。
4. 掃描完成後，您將看到電腦的 #CyberFit 總分，以及六個評估指標分別的分數：反惡意程式碼、備份、防火牆、虛擬私人網路 (VPN)、磁碟加密，以及 NT LAN Manager (NTLM) 流量。



5. 若要檢查如何針對可以改善安全設定的各個指標提高其分數，請展開對應的章節並閱讀建議。



6. 因應建議之後，您一律可以按一下 #CyberFit 總分正下方的箭頭按鈕，重新計算電腦的 #CyberFit 分數。

網路指令碼撰寫

透過 Cyber Scripting，您可以使用指令碼，將您環境中 Windows 及 macOS 電腦上的例行作業自動化，例如，安裝軟體、修改設定、啟動或停止服務，以及建立帳戶。因此，您可以減少花在此類作業上的時間，並降低手動執行這些作業時發生錯誤的風險。

Cyber Scripting 可供系統管理員和客戶層級的使用者，以及合作夥伴系統管理員 (服務提供者) 使用。如需有關不同系統管理層級的詳細資訊，請參閱 "多租用戶支援" (第 272 頁)。

您可以使用的指令碼必須事先經過核准。只有具備 **[網路系統管理員]** 角色的系統管理員才能核准及測試新的指令碼。如需有關變更指令碼狀態的詳細資訊，請參閱 "變更指令碼狀態" (第 341 頁)。

根據您的使用者角色，您可以使用指令碼和指令碼計劃執行不同的操作。如需有關角色的詳細資訊，請參閱 "使用者角色及網路指令碼權限" (第 333 頁)。

必要條件

- Cyber Scripting 功能需要使用 Advanced Management 套件。
- 要使用網路指令碼的所有功能，例如指令碼編輯、指令碼執行、指令碼計劃建立等等，必須為您的帳戶啟用雙因素驗證。

限制

- 支援以下指令碼語言：
  - PowerShell
  - Bash
- 網路指令碼操作僅能在已安裝保護代理程式的目標電腦執行。

支援的平台

網路指令碼撰寫適用於 Windows 和 macOS 工作負載。

下表摘要說明支援的版本。

作業系統	版本
Windows	Windows 7 SP1 和更新版本 – 所有版本
	Windows 8/8.1 – 所有版本(x86、x64) , 但 Windows RT 版除外
	Windows 10 - Home、Pro、Education、Enterprise、IoT Enterprise 版本
	Windows 11
	Windows Server 2008 R2 SP1 和更新版本 – Standard、Enterprise、Datacenter、Foundation 和 Web 版本
	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

使用者角色及網路指令碼權限

指令碼及指令碼計劃的可用操作取決於指令碼狀態及您的使用者角色。

系統管理員可以管理其自己租用戶及其子系租用戶。他們無法查看或存取上級管理等級的對象，如果有。

較低層級的系統管理員僅能以唯讀方式存取上層系統管理員套用至其工作負載的指令碼計劃。

以下角色提供有關網路指令碼的權限：

- **公司系統管理員**
  此角色授予所有服務的完整系統管理員權限。關於網路指令碼，其與網路系統管理員角色授予相同的權限。
- **網路系統管理員**
  此角色授予完整權限，包含核准可在租用戶使用的指令碼，以及具有執行 **[測試]** 狀態指令碼的能力。
- **系統管理員**
  此角色授予部分權限，並能執行核准的指令碼，使用核准的指令碼來建立並執行指令碼計劃。
- **唯讀系統管理員**

此角色授予有限權限，並能檢視使用者使用的指令碼及保護計劃。

- **使用者**

  此角色授予部分權限，並能執行核准的指令碼，使用核准的指令碼來建立並執行指令碼計劃，但僅能在使用者自己的電腦執行。

下表列出所有可用的操作，取決於指令碼狀態及使用者角色而定。

角色	物件	指令碼狀態		
		草稿	正在測試	已核准
網路系統管理員 **公司系統管理員**	指令碼計劃	編輯(從計劃移除草稿指令碼) 刪除 撤回 停用 停止	建立 編輯 套用 啟用 執行 刪除 撤回 停用 停止	建立 編輯 套用 啟用 執行 刪除 撤回 停用 停止
	指令碼	建立 編輯 變更狀態 複製 刪除 取消執行	建立 編輯 變更狀態 執行 複製 刪除 取消執行	建立 編輯 變更狀態 執行 複製 刪除 取消執行
系統管理員 **使用者**(針對自己的工作負載)	指令碼計劃	檢視 撤回 停用 停止	檢視 取消執行	建立 編輯 套用 啟用 執行 刪除 撤回 停用

				停止
	指令碼	建立 編輯 複製 刪除 取消執行	檢視 複製 取消執行	執行 複製 取消執行
唯讀系統管理員	指令碼計劃	檢視	檢視	檢視
	指令碼	檢視	檢視	檢視

指令碼

指令碼是在執行階段解譯並在目標電腦上執行的一組指令。指令碼可為自動執行重複或複雜的工作提供便利的解決方案。

您可以使用 Cyber Scripting 執行預先定義的指令碼，或建立自訂指令碼。您可以在 **[管理]** > **[指令碼存放庫]** 中找到可用的所有指令碼。預先定義的指令碼位於 **[程式庫]** 區段。您所建立或複製到租用戶的指令碼位於 **[我的指令碼]** 區段。

您可以將指令碼包含在指令碼計劃中，或執行 **[指令碼快速執行]** 作業來使用指令碼。

注意事項
您僅能使用在租用戶中建立或複製到租用戶中的已核准指令碼。如果指令碼已從指令碼存放庫移除，或其處於 **[草稿]** 狀態，將不會執行該指令碼。您可以檢查指令碼操作的詳細資料，或在 **[監控]** > **[活動]** 中取消操作。

下表根據指令碼的狀態，提供有關指令碼可能執行的動作的詳細資訊。

狀態	可能的動作
草稿	您建立的新指令碼以及複製到存放庫的指令碼均處於 **[草稿]** 狀態。您無法執行這些指令碼，或將其包含在指令碼計劃中。
正在測試	擁有 **[網路系統管理員]** 角色的系統管理員可以執行這些指令碼，並將其包含在指令碼計劃中。
已核准	您可以執行這些指令碼，並將其包含在指令碼計劃中。

只有擁有 **[網路系統管理員]** 角色的系統管理員才能變更指令碼的狀態或刪除已核准的指令碼。如需詳細資訊，請參閱 "變更指令碼狀態"(第 341 頁)。

建立指令碼

您可以透過手動編寫程式碼來建立指令碼。

建立指令碼

1. 在 Cyber Protect 主控台，前往 **[管理]** > **[指令碼存放庫]**。
2. 在 **[我的指令碼]** 中，按一下 **[使用 AI 建立指令碼]**。
3. 在主窗格寫出指令碼主文。

重要事項
當您建立指令碼時，包含每項作業的結束碼檢查。否則，可能會忽略失敗的作業，且 **[監控]** > **[活動]** 的指令碼活動狀態可能會錯誤顯示為 **[成功]**。

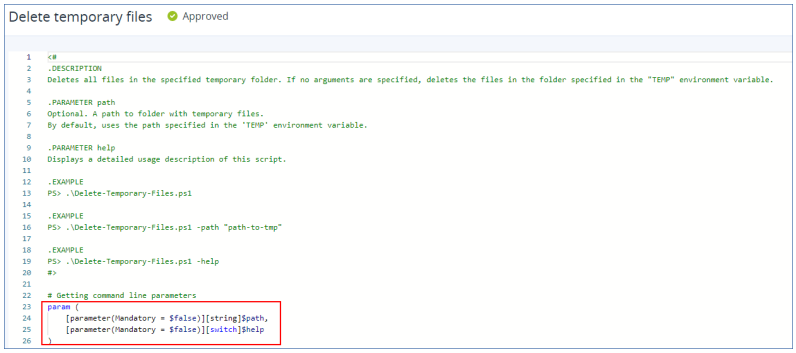
4. 指定指令碼設定。

設定	描述
指令碼名稱	指令碼名稱。此欄位會自動填入，但您可以變更值。
描述	指令碼描述。此設定是選擇性的。 [若是 AI 產生的指令碼] 此欄位將在產生指令碼時自動填入。您可以編輯 AI 提供的描述。
語言	指令碼語言。可用的值為： • **PowerShell**。這是預設值。 • **Bash** [若是 AI 產生的指令碼] 此設定是在產生指令碼之前設定。
作業系統	安裝在將執行指令碼所在目標工作負載上的作業系統。可用的值為： • **Windows**。這是預設值。 • **macOS** [若是 AI 產生的指令碼] 此設定是在產生指令碼之前設定。
狀態	指令碼狀態。 • **草稿**。這是預設值。您建立的新指令碼以及複製到存放庫的指令碼均處於 **[草稿]** 狀態。您無法執行 **[草稿]** 指令碼，或將其包含在指令碼計劃中。 • **正在測試**。只有擁有 **[網路系統管理員]** 角色的系統管理員才能將指令碼的狀態變更為 **[正在測試]**、在 **[正在測試]** 狀態下執行指令碼，以及使用此類指令碼執行指令碼計劃。 • **已核准**。您可以執行**已核准的**指令碼，並將其包含在指令碼計劃中。 只有擁有 **[網路系統管理員]** 角色的系統管理員才能變更指令碼的狀態或刪除已核准的指令碼。如需詳細資訊，請參閱 "變更指令碼狀態" (第 341 頁)。
標籤	標籤不區分大小寫，最長可達 32 個字元。您不得使用圓括號和尖角括號、逗號或空格。 此設定是選擇性的。 [若是 AI 產生的指令碼] 產生指令碼時會自動新增 **AI 產生的**標籤。您可以手動刪除此標籤或新增其他標籤。

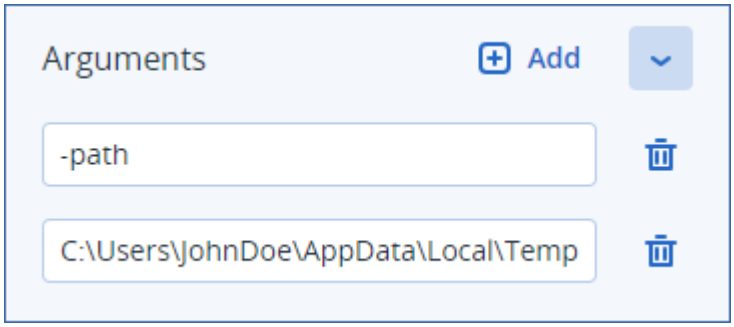
5. [僅適合需要憑證的指令碼] 指定憑證。
   您可使用單一憑證 (例如，權杖) 或一對憑證 (例如，使用者名稱和密碼) 。
6. [僅適合需要引數的指令碼] 指定引數及參數值，如下所示：

a. 按一下 **[新增]**。
b. 在 **[新增引數]** 欄位中，指定引數。
c. 按一下 **[新增]**。
d. 在出現的第二個欄位中，指定引數值。

注意事項
您僅能指定已在指令碼主文定義的引數。



例如：



e. 如果您需要新增更多引數，請重複上述步驟。

7. 按一下 **[儲存]**。

指令碼會以 **[草稿]** 狀態儲存到您的存放庫。

在擁有 **[網路系統管理員]** 角色的系統管理員將其狀態變更為 **[已核准]** 之前，您無法使用此指令碼。如需詳細資訊，請參閱 "變更指令碼狀態" (第 341 頁)。

若要在您管理的另一個租用戶中使用指令碼，您必須將指令碼複製到該租用戶。如需詳細資訊，請參閱 "複製指令碼" (第 340 頁)。

使用 AI 建立指令碼

注意事項
此功能需要使用 Advanced Management 套件。

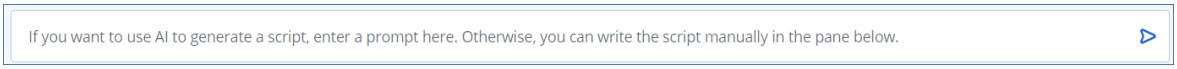
您可以使用 AI 將提示轉換為功能強大的指令碼，從而節省您的時間和精力。您可以透過以下方式使用此功能：

- 輸入提示，要求 AI 從頭開始產生指令碼。
- 輸入提示，要求 AI 檢閱並完成您在指令碼本文中輸入的程式碼。當您一直在努力處理更複雜的程式碼時，可以使用此功能。

此功能使用 OpenAI 的 GPT-4 模型。您可以使用此功能，每個月為您的組織免費建立最多 100 個指令碼。

若要使用 AI 建立指令碼

1. 在 Cyber Protect 主控台，前往 **[管理]** > **[指令碼存放庫]**。
2. 在 **[我的指令碼]** 中，按一下 **[使用 AI 建立指令碼]**。
3. 在提示中，針對指令碼應執行的操作，輸入其描述。起確認您輸入的描述盡可能清楚且詳細。

   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，按一下箭頭按鈕。
5. 在確認視窗中，選擇 [語言] 和 [作業系統]，然後按一下 **[產生]**。

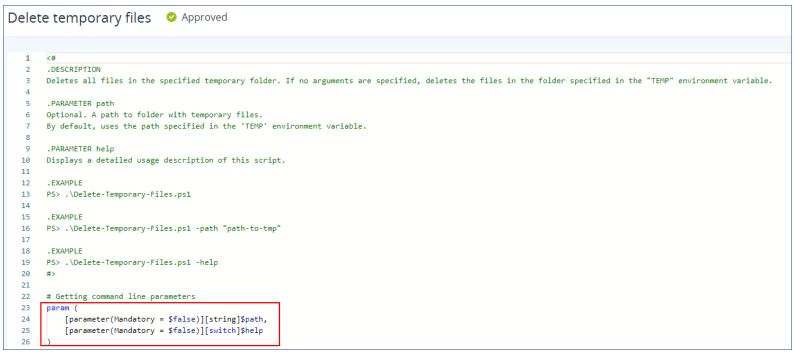
   AI 產生的指令碼隨即顯示在主窗格中。指令碼的名稱和描述由 AI 自動產生，以便符合指令碼。**AI 產生的**標籤會自動指派給指令碼。
6. 檢閱 AI 產生的指令碼，如有必要，請手動編輯。
7. 如有必要，請編輯指令碼設定。

設定	描述
指令碼名稱	指令碼名稱。此欄位會自動填入，但您可以變更值。
描述	指令碼描述。此設定是選擇性的。 [若是 AI 產生的指令碼] 此欄位將在產生指令碼時自動填入。您可以編輯 AI 提供的描述。
語言	指令碼語言。可用的值為： • **PowerShell**。這是預設值。 • **Bash** [若是 AI 產生的指令碼] 此設定是在產生指令碼之前設定。
作業系統	安裝在將執行指令碼所在目標工作負載上的作業系統。可用的值為： • **Windows**。這是預設值。 • **macOS** [若是 AI 產生的指令碼] 此設定是在產生指令碼之前設定。
狀態	指令碼狀態。 • **草稿**。這是預設值。您建立的新指令碼以及複製到存放庫的指令碼均處於 **[草稿]** 狀態。您

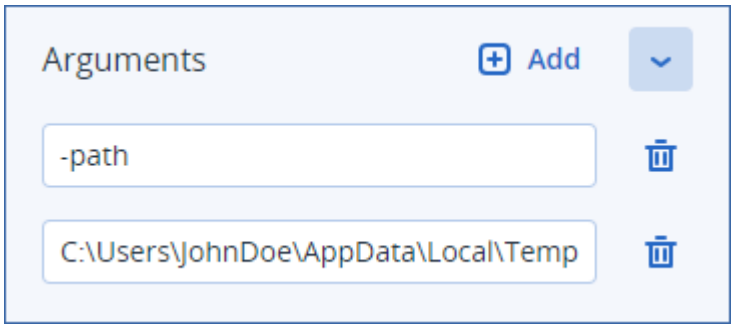
設定	描述
	無法執行 **[草稿]** 指令碼，或將其包含在指令碼計劃中。 • **正在測試**。只有擁有 **[網路系統管理員]** 角色的系統管理員才能將指令碼的狀態變更為 **[正在測試]**、在 **[正在測試]** 狀態下執行指令碼，以及使用此類指令碼執行指令碼計劃。 • **已核准**。您可以執行**已核准的**指令碼，並將其包含在指令碼計劃中。 只有擁有 **[網路系統管理員]** 角色的系統管理員才能變更指令碼的狀態或刪除已核准的指令碼。如需詳細資訊，請參閱 "變更指令碼狀態" (第 341 頁)。
標籤	標籤不區分大小寫，最長可達 32 個字元。您不得使用圓括號和尖角括號、逗號或空格。 此設定是選擇性的。 [若是 AI 產生的指令碼] 產生指令碼時會自動新增 **AI 產生的**標籤。您可以手動刪除此標籤或新增其他標籤。

8. [選用] [僅適合需要憑證的指令碼] 指定憑證。
   您可使用單一憑證 (例如，權杖) 或一對憑證 (例如，使用者名稱和密碼) 。
9. [僅適合需要引數的指令碼] 指定引數及參數值，如下所示：
   a. 按一下 **[新增]**。
   b. 在 **[新增引數]** 欄位中，指定引數。
   c. 按一下 **[新增]**。
   d. 在出現的第二個欄位中，指定引數值。

   注意事項
   您僅能指定已在指令碼主文定義的引數。

   例如：

   e. 如果您需要新增更多引數，請重複上述步驟。

10. 按一下 **[儲存]**。

    指令碼會以 **[草稿]** 狀態儲存到您的存放庫。

    在擁有 **[網路系統管理員]** 角色的系統管理員將其狀態變更為 **[已核准]** 之前，您無法使用此指令碼。如需詳細資訊，請參閱 "變更指令碼狀態" (第 341 頁)。

    若要在您管理的另一個租用戶中使用指令碼，您必須將指令碼複製到該租用戶。如需詳細資訊，請參閱 "複製指令碼" (第 340 頁)。

複製指令碼

在下列情況下，有必要複製指令碼：

- 在從 **[程式庫]** 使用指令碼之前。在此情況下，首先您必須將指令碼複製到 **[我的指令碼]** 區段。
- 當您想要把在上層租用戶建立的指令碼複製到其子項租用戶或單位時。

複製指令碼

1. 在 **[指令碼存放庫]**，尋找您要複製的指令碼。
2. 執行下列其中一項操作：
   - [如果您從 **[我的指令碼]** 複製指令碼] 按一下指令碼名稱旁邊的省略符號 (...)，然後按一下 **[複製]**。
   - [如果從 **[程式庫]** 複製指令碼] 按一下您所選指令碼之名稱旁的 **[複製]**。
3. 在 **[複製指令碼]** 快顯視窗中，從 **[狀態]** 下拉式清單選擇以下其中一個指令碼狀態：
   - **草稿** (預設) — 此狀態不允許您立即執行指令碼。
   - **正在測試** — 此狀態允許您執行指令碼。
   - **已核准** — 此狀態允許您執行指令碼。
4. [如果您管理多個租用戶或單位] 選取您要複製指令碼的位置。

   在 **[複製指令碼]** 對話方塊，您只會看到可管理且已套用 Advanced Management 元件的租用戶。

因此，指令碼會複製到所選租用戶或單位的 **[我的指令碼]** 區段。如果您僅管理一個沒有單位的租用戶，則指令碼會自動複製到 **[我的指令碼]** 區段。

重要事項

當把指令碼複製到非原始租用戶時，不會複製指令碼使用的憑證。

編輯或刪除指令碼

注意事項

根據您的使用者角色，您可以使用指令碼和指令碼計劃執行不同的操作。如需有關角色的詳細資訊，請參閱 "使用者角色及網路指令碼權限" (第 333 頁)。

編輯指令碼

1. 在 **[指令碼存放庫]**，前往 **[我的指令碼]**，然後尋找您要編輯的指令碼。
2. 按一下指令碼名稱旁邊的省略符號 (...)，然後按一下 **[編輯]**。
3. 編輯指令碼，然後按一下 **[儲存]**。

4. [如果您編輯指令碼計劃所使用的指令碼] 按一下 **[儲存指令碼]** 確認您的選擇。

注意事項
下次執行指令碼計劃的時候，將使用最新版本的指令碼。

指令碼版本

如果您編輯下列任一指令碼屬性，會建立新版本的指令碼：

- 指令碼主文
- 指令碼名稱
- 說明
- 指令碼語言
- 認證
- 引數

如果您變更其他屬性，您的編輯會加入目前的指令碼版本。深入瞭解版本及其如何比較，請參閱 "比較指令碼版本" (第 342 頁)。

注意事項
只有當您修改 **[狀態]** 欄位值時，指令碼狀態才會更新。只有具備網路系統管理員角色的管理員才能變更指令碼狀態。

刪除指令碼

1. 在 **[指令碼存放庫]**，前往 **[我的指令碼]**，然後尋找您要刪除的指令碼。
2. 按一下指令碼名稱旁邊的省略符號 (...)，然後按一下 **[刪除]**。
3. 請按一下 **[刪除]**。
4. [如果您要刪除指令碼計劃所使用的指令碼] 按一下 **[儲存指令碼]** 確認您的選擇。

注意事項
指令碼計劃如果使用已刪除的指令碼將會無法執行。

變更指令碼狀態

已建立並處於 **[草稿]** 狀態的新指令碼只有在其狀態變更為 **[已核准]** 後才能使用。根據使用案例，指令碼在獲得核准之前，可能會在一段時間內處於 **[正在測試]** 狀態。

注意事項
根據您的使用者角色，您可以使用指令碼和指令碼計劃執行不同的操作。如需有關角色的詳細資訊，請參閱 "使用者角色及網路指令碼權限" (第 333 頁)。

先決條件

- 您的使用者是獲指派 **[網路系統管理員]** 角色的系統管理員。
- 具有對應狀態的指令碼可供使用。

變更指令碼狀態

1. 在 **[指令碼存放庫]** 中，移至 **[我的指令碼]**。
2. 按一下指令碼名稱旁邊的省略符號 (...)，然後按一下 **[編輯]**。
3. 在 **[狀態]** 下拉式清單中，選擇狀態。
4. 按一下 **[儲存]**。
5. [如果您要變更已核准指令碼的狀態] 若要確認變更，按一下 **[儲存指令碼]**。

注意事項
如果指令碼狀態降級為 **[草稿]**，使用該指令碼的指令碼計劃將無法執行。
只有具備 **[網路系統管理員]** 角色的系統管理員才能在 **[正在測試]** 狀態中執行指令碼，並使用此類指令碼執行指令碼計劃。

比較指令碼版本

您可比較指令碼的兩個版本，並還原為較早的版本。您也可檢查建立特定版本的人員，以及建立時間。

比較指令碼版本

1. 在 **[指令碼存放庫]**，前往 **[我的指令碼]**，然後尋找您要比較版本的指令碼。
2. 按一下指令碼名稱旁邊的省略號 (...)，然後按一下 **[版本記錄]**。
3. 選擇您要比較的兩個版本，然後按一下 **[比較版本]**。
   變更任何指令碼主文、其引數或憑證都會突出顯示。

若要還原為先前的版本

1. 在 **[比較指令碼版本]** 視窗中，按一下 **[還原為此版本]**。
2. 在 **[還原至上一版]** 快顯視窗的 **[狀態]** 下拉式清單中，選擇指令碼狀態。

還原選擇的版本並儲存為版本記錄的最新版本。

若要還原指令碼，您也可以從 **[版本記錄]** 視窗中選擇一個版本，然後按一下 **[還原]** 按鈕。

重要事項
您僅能執行狀態為 **[正在測試]** 或 **[已核准]** 的指令碼。如需詳細資訊，請參閱 "變更指令碼狀態" (第 341 頁)。

下載指令碼作業的輸出

您可將指令碼作業的輸出下載為 .zip 檔案。它包含兩個文字檔 – `stdout` 與 `stderr`。您可在 `stdout`，看到成功完成指令碼操作的結果。`stderr` 檔案包含指令碼作業期間發生的錯誤之相關資訊。

下載輸出檔案

1. 在 Cyber Protect 主控台，前往 **[監控]** > **[活動]**。
2. 按一下您要下載輸出的網路指令碼活動。
3. 在 **[活動詳情]** 畫面上，按一下 **[下載輸出]**。

指令碼存放庫

您可在 **[管理]** 索引標籤找到指令碼存放庫。您可在存放庫按照指令碼的名稱和描述來搜尋指令碼。您也可使用篩選條件，或依指令碼的名稱或狀態排序指令碼。

管理指令碼，請按一下指令碼名稱旁的省略符號 (...)，然後選擇所需的動作。或者，按一下指令碼，然後在開啟的螢幕使用按鈕。

指令碼存放庫包含下列區段：

- **[我的指令碼]**

  您可在此找到可直接在環境使用的指令碼。這些是您從頭開始建立的指令碼，與您在此複製的指令碼。

  您可依照下列條件篩選此區段的指令碼：

  - 標籤
  - 狀態
  - 語言
  - 作業系統
  - 指令碼擁有者
- **[程式庫]**

  程式庫包含預設指令碼，您可將它們複製到 **[我的指令碼]** 區段，之後在環境使用這些指令碼。您僅能檢查並複製這些指令碼。

  您可依照下列條件篩選此區段的指令碼：

  - 標籤
  - 語言
  - 作業系統

  如需詳細資訊，請參閱廠商核准的指令碼 (70595)。

指令碼計劃

指令碼計劃可讓您在多項工作負載執行指令碼、排程執行指令碼，以及編輯其他設定。

您可在 **[管理]** > **[指令碼 計劃]** 找到您建立的指令碼計劃及套用至工作負載的 指令碼計劃。您可在此檢查計劃執行位置、擁有者或狀態。

可點選的欄位會顯下列示指令碼計劃的顏色程式碼狀態：

- 執行(藍色)
- 檢查相容性(深灰色)
- 已停用(淺灰色)
- OK (綠燈)
- 嚴重警示(紅色)
- 錯誤(橙色)
- 警告(黃色)

按一下欄位，您可查看計劃的狀態還有多少工作負載。每個狀態也可點選。

您可在 **[指令碼計劃]** 索引標籤執行下列動作來管理計劃：

- 執行
- 停止
- 編輯
- 重新命名
- 停用
- 啟用
- 複製
- 匯出。計劃設定將以 JSON 格式匯出到本機電腦。
- 刪除

指令碼計劃的可見度及可用動作取決於計劃擁有者及您的使用者角色。例如，公司系統管理員僅能看到合作夥伴擁有的指令碼計劃，這些計劃無法執行任何動作。

需有關誰可建立及管理指令碼計劃的詳細資訊，請參閱 "使用者角色及網路指令碼權限" (第 333 頁)。

管理指令碼計劃

1. 在 Cyber Protect 主控台，前往 **[管理]** > **[指令碼計劃]**。
2. 找到您要管理的計劃，然後按一下計劃旁邊的省略符號 (...)。
3. 選取所需的動作，然後請按照螢幕的指示操作。

建立指令碼計劃

您可使用下列方式建立指令碼計劃：

- 在 **[裝置]** 索引標籤
  選擇工作負載，然後為其建立指令碼計劃。
- 在 **[管理]** > **[指令碼計劃]** 索引標籤
  建立指令碼計劃，然後選擇要套用計劃的工作負載。

在裝置索引標籤建立指令碼計劃

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[電腦與代理程式]**。
2. 選擇工作負載或您要套用指令碼計劃的裝置群組，然後分別按一下 **[保護]** 或 **[保護群組]**。
3. [如果已套用計劃] 按一下 **[新增計劃]**。
4. 按一下 **[建立計劃]** > **[指令碼計劃]**
   指令碼計劃範本隨即開啟。
5. [選用] 若要修改指令碼計劃名稱，請按一下鉛筆圖示。
6. 按一下 **[選擇指令碼]**，選取您要使用的指令碼，然後按一下 **[完成]**。

注意事項
您僅能從 **[指令碼存放庫]** > **[我的指令碼]** 使用您已核准的指令碼。只有擁有 **[網路系統管理員]** 角色的系統管理員才能使用 **[正在測試]** 狀態的指令碼。如需有關角色的詳細資訊，請參閱 "使用者角色及網路指令碼權限" (第 333 頁)。

7. 設定指令碼計劃的排程和啟動條件。
8. 選擇指令碼要在目標工作負載執行的帳戶。您可以選取下列選項：
   - 系統帳戶(在 macOS 這是根帳戶)
   - 目前已登入的帳戶
9. 指定指令碼可在目標工作負載執行的時間長度。
   如果指令碼無法在設定的時間範圍內完成執行，Cyber Scripting 操作將會失敗。
   您可以指定的最小值為一分鐘，最大值為 1440 分鐘。
10. [僅適用於 PowerShell 指令碼] 設定 PowerShell 執行原則。
    有關此原則的詳細資訊，請參閱 Microsoft 文件。
11. 按一下 **[建立]**。

在指令碼計劃索引標籤建立指令碼計劃

1. 在 Cyber Protect 主控台，前往 **[管理]** > **[指令碼計劃]**。
2. 按一下 **[建立計劃]**。
   指令碼計劃範本隨即開啟。
3. [選用] 選擇要套用新計劃的工作負載或裝置群組，按一下 **[新增工作負載]**。
   a. 按一下 **[具有代理程式的電腦]** 展開清單，然後選取所需的工作負載或裝置群組。
   b. 按一下 **[新增]**。
   有關更多如何在合作夥伴等級建立裝置群組的詳細資訊，請參閱 "裝置索引標籤" (第 268 頁)。

注意事項
您也可在建立計劃之後選擇工作負載或裝置群組。

4. [選用] 若要修改指令碼計劃名稱，請按一下鉛筆圖示。
5. 按一下 **[選擇指令碼]**，選取您要使用的指令碼，然後按一下 **[完成]**。

注意事項
您僅能從 **[指令碼存放庫]** > **[我的指令碼]** 使用您已核准的指令碼。只有擁有 **[網路系統管理員]** 角色的系統管理員才能使用 **[正在測試]** 狀態的指令碼。如需有關角色的詳細資訊，請參閱 "使用者角色及網路指令碼權限" (第 333 頁)。

6. 設定指令碼計劃的排程和啟動條件。
7. 選擇指令碼要在目標工作負載執行的帳戶。您可以選取下列選項：
   - 系統帳戶(在 macOS 這是根帳戶)
   - 目前已登入的帳戶
8. 指定指令碼可在目標工作負載執行的時間長度。

如果指令碼無法在設定的時間範圍內完成執行，Cyber Scripting 操作將會失敗。
您可以指定的最小值為一分鐘，最大值為 1440 分鐘。

9. [僅適用於 PowerShell 指令碼] 設定 PowerShell 執行原則。
   有關此原則的詳細資訊，請參閱 Microsoft 文件。
10. 按一下 **[建立]**。

排程和開始條件

排程

您可將指令碼計劃設定為執行一次或重複執行，還可按排程啟動或由特定事件觸發。

您可以選取下列選項：

- 執行一次
  對於此選項，您必須設定執行計劃的日期和時間。
- 依時間排程
  您可透過此選項設定每小時、每天或每月執行的指令碼計劃。
  若要讓排程僅暫時生效，請選擇 **[在日期範圍內執行]** 核取方塊，然後設定排程計劃執行的期間。
- 當使用者登入系統時
  您可選擇登入的特定使用者或任何觸發指令碼計劃的使用者。
- 當使用者登出系統時
  您可選擇登出的特定使用者或任何觸發指令碼計劃的使用者。
- 在系統啟動時
- 當系統關閉時

注意事項
此排程選項僅適用於在系統帳戶執行的指令碼。

- 當系統上線時

開始條件

啟動條件為您的排程計劃新增了更多彈性。如果您設定多個條件，必須同時符合所有條件，才能開始計劃。

如果您使用 **[立即執行]** 選項手動執行計劃，啟動條件不會生效。

條件	描述
僅在工作負載連線時執行	當目標工作負載連線到網際網路時，指令碼將執行。
使用者空閒時	當電腦執行螢幕保護程式或本機已鎖定時，符合此條件。
使用者登出	在此情況下，您可延遲排程指令碼計劃，直到目標工作負載的使用者登出為止。

條件	描述
符合時間間隔時	在此情況下，指令碼計劃僅能在指定的時間間隔內開始。例如，您可使用此條件來限制 **[使用者已登出]** 條件。
節省電池電力	在這種情況下，您可確保指令碼計劃不會因電量不足而中斷。您可以選取下列選項： • 不要在使用電池電力時開始 只有當本機連接電源時，計劃才會開始。 • 如果電池電量高於下列設定，可在使用電池電力時開始 如果本機連接至電源或電量高於指定值，計劃開始。
請勿在計量付費連線上開始	如果目標工作負載透過計量付費連線存取網際網路，此情況會阻止計劃開始。
不要在連線至下列 Wi-Fi 網路時開始	如果目標工作負載連線到任何指定的 Wi-Fi，此情況會阻止計劃開始。若要使用此條件，您必須指定禁止網路的 SSID。 該限制適用於所有包含以其名稱作為子字串之指定名稱的網路，不區分大小寫。例如，如果您將 [電話] 指定為網路名稱，當裝置連線至下列任何網路時，計劃將不會開始：John 的 iPhone、phone_wifi 或 my_PHONE_wifi。
檢查裝置 IP 位址	如果目標工作負載的任何 IP 位址在指定 IP 位址範圍內或之外，此條件將阻止計劃開始。 您可以選取下列選項： • 在 IP 範圍之外時開始 • 在 IP 範圍之內時開始 僅支援 IPv4 位址。
如果不符合開始條件，請執行工作	此選項可讓您設定計劃執行的時間間隔，不考慮其他條件。一旦滿足其他條件或指定的期限結束，計劃將立即開始，具體取決於哪個優先。 如果您將指令碼計劃設定為只執行一次，無法使用此選項。

管理計劃的目標工作負載

您可在建立計劃時選擇要套用指令碼計劃的工作負載或裝置群組，或更新版本。

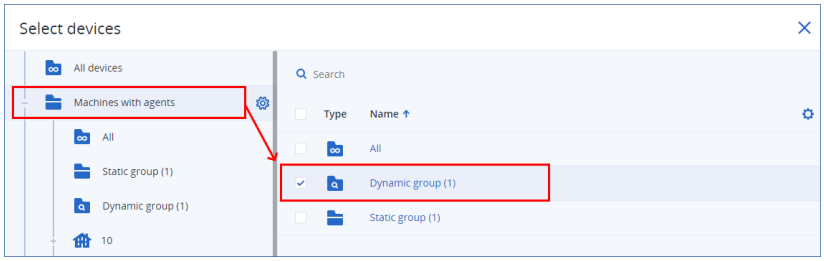
合作夥伴系統管理員可將相同計劃套用來自不同客戶的工作負載，並可為包含來自不同顧客的工作負載建立裝置群組。若要瞭解如何在合作夥伴層級建立靜態或動態裝置群組，請參閱 "裝置索引標籤" (第 268 頁)。

在計劃新增初始工作負載

1. 在 Cyber Protect 主控台，前往 **[管理]** > **[指令碼計劃]**。
2. 按一下您要指定目標工作負載的計劃名稱。
3. 按一下 **[新增工作負載]**。
4. 選擇所需的工作負載或裝置群組，然後按一下 **[新增]**。

注意事項

若要選擇裝置群組，請按一下其父層級，在主窗格選取其名稱旁邊的核取方塊。



5. 若要儲存編輯的計劃，按一下 **[儲存]**。

管理計劃的現有工作負載

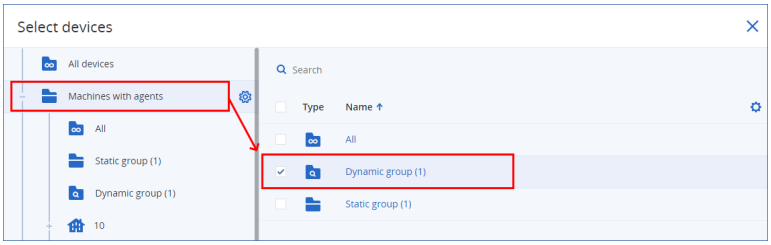
1. 在 Cyber Protect 主控台，前往 **[管理]** > **[指令碼計劃]**。
2. 按一下您要變更目標工作負載的計劃名稱。
3. 按一下 **[管理工作負載]**。

   [裝置] 畫面會列出目前套用指令碼計劃的工作負載。如果您管理多個租用戶，工作負載會依租用戶排序。

   - 若要新增工作負載或裝置群組，按一下 **[新增]**。
     a. 選擇所需的工作負載或裝置群組。您可從您管理的所有租用戶新增工作負載。

     注意事項

     若要選擇裝置群組，請按一下其父層級，在主窗格選取其名稱旁邊的核取方塊。

     b. 按一下 **[新增]**。
   - 若要移除工作負載或裝置群組，請選取然後按一下 **[移除]**。
4. 按一下**[完成]**。
5. 若要儲存編輯的計劃，按一下 **[儲存]**。

不同行政層面的計劃

下表列出不同層級的系統管理員可以查看及管理的計劃。

系統管理員	管理層級	計劃	權限
合作夥伴系統管理員	合作夥伴等級	自己的計劃	完整存取

系統管理員	管理層級	計劃	權限
		客戶計劃(包含單位計劃)	完整存取
		單位計劃	完整存取
	客戶層級 (適用於服務提供者管理的客戶)	套用至此客戶工作負載的合作夥伴計劃	唯讀
		客戶計劃(包含單位計劃)	完整存取
		單位計劃	完整存取
	單位層級 (適用於服務提供者管理的客戶)	套用至此單位工作負載的合作夥伴計劃	唯讀
		套用至此單位工作負載的客戶計劃	唯讀
		單位計劃	完整存取
公司系統管理員	客戶層級	套用至此客戶或單位工作負載的合作夥伴計劃	唯讀
		客戶計劃(包含單位計劃)	完整存取
		單位計劃	完整存取
	單位層級	套用至此單位工作負載的合作夥伴計劃	唯讀
		套用至此單位工作負載的客戶計劃	唯讀
		單位計劃	完整存取
單位系統管理員	單位層級	套用至此單位工作負載的合作夥伴計劃	唯讀
		套用至此單位工作負載的客戶計劃	唯讀
		單位計劃	完整存取

重要事項

計劃的擁有者是在建立計劃的租用戶。因此，如果合作夥伴系統管理員在客戶租用戶層級建立方案，客戶租用戶就是方案的擁有者。

指令碼計劃的相容性問題

在某些情況下，對工作負載套用指令碼計劃可能會導致相容性問題。您可能會觀察到下列相容性問題：

- 不相容的作業系統 – 當工作負載的作業系統不受支援時，會出現此問題。
- 不支援的代理程式 – 當工作負載上的保護代理程式版本已過期，而且不支援網路指令碼功能時，會出現此問題。
- 配額不足 – 當租用戶中沒有足夠的服務配額可指派給所選的工作負載時，會出現此問題。

如果指令碼計劃套用至多達 150 項個別選取的工作負載，系統會提示您先解決現有衝突，然後才能儲存計劃。若要解決衝突，請移除其根本原因或從計劃移除受影響的工作負載。如需詳細資訊，請參閱 "解決指令碼計劃的相容性問題" (第 350 頁)。如果在未解決衝突的情況下儲存計劃，對於不相容的工作負載，該計劃將自動停用，並且會顯示警示。

如果將指令碼計劃套用至超過 150 項工作負載或裝置群組，則會先儲存計劃，然後再檢查相容性。系統會自動針對不相容的工作負載停用此計劃，並顯示警示。

解決指令碼計劃的相容性問題

根據相容性問題的原因，您可以執行不同的動作來解決相容性問題，作為建立新指令碼計劃程序的一部分。

注意事項
透過移除計劃中的工作負載來解決相容性問題時，您無法移除屬於裝置群組一部分的工作負載。

若要解決相容性問題

1. 按一下 **[檢閱問題]**。
2. [解決與不相容作業系統的相容性問題]
   a. 在 **[不相容的作業系統]** 索引標籤上，選擇您要移除的工作負載。
   b. 按一下 **[從計劃中移除工作負載]**。
   c. 按一下 **[移除]**，然後按一下 **[關閉]**。
3. [透過從計劃中移除工作負載來解決與不支援的代理程式的相容性問題]
   a. 在 **[不支援的代理程式]** 索引標籤上，選擇您要移除的工作負載。
   b. 按一下 **[從計劃中移除工作負載]**。
   c. 按一下 **[移除]**，然後按一下 **[關閉]**。
4. [透過更新代理程式版本來解決與不支援的代理程式的相容性問題] 按一下 **[移至代理程式清單]**。

   注意事項
   此選項僅適用於客戶系統管理員。

5. [透過從計劃中移除工作負載來解決配額不足的相容性問題]

a. 在 **[配額不足]** 索引標籤上，選擇您要移除的工作負載。
b. 按一下 **[從計劃中移除工作負載]**。
c. 按一下 **[移除]**，然後按一下 **[關閉]**。

6. [透過增加租用戶配額來解決配額不足的相容性問題]

注意事項
此選項僅適用於合作夥伴系統管理員。

a. 在 **[配額不足]** 索引標籤上，按一下 **[前往管理入口網站]**。
b. 增加客戶的服務配額。

指令碼快速執行

您可以立即執行指令碼，而無需將其包含在指令碼計劃中。您無法對超過 150 個工作負載、離線工作負載或裝置群組使用此操作。

必須為目標工作負載指派支援指令碼快速執行功能的服務配額，而且必須為其用戶啟用 Advanced Management 元件。如果租用戶具有適當的服務配額，會自動指派。

注意事項
您僅能從 **[指令碼存放庫]** > **[我的指令碼]** 使用您已核准的指令碼。只有擁有 **[網路系統管理員]** 角色的系統管理員才能使用 **[正在測試]** 狀態的指令碼。如需有關角色的詳細資訊，請參閱 "使用者角色及網路指令碼權限" (第 333 頁)。

您可透過下列方式開始快速執行：

- 從 **[裝置]** 索引標籤
  選取一項或多項工作負載，然後選取要執行的指令碼。
- 從 **[管理]** > **[指令碼存放庫]** 索引標籤
  選取指令碼，然後選取一項或多項目標工作負載。

從裝置標籤執行指令碼

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 選取您要執行指令碼的工作負載，然後按一下 **保護**。
3. 按一下 **[指令碼快速執行]**。
4. 按一下 **[選擇指令碼]**，選取您要使用的指令碼，然後按一下 **[完成]**。
5. 選擇指令碼要在目標工作負載執行的帳戶。您可以選取下列選項：
   - 系統帳戶(在 macOS 這是根帳戶)
   - 目前已登入的帳戶
6. 指定指令碼可在目標工作負載執行的時間長度。
   如果指令碼無法在設定的時間範圍內完成執行，Cyber Script 操作將會失敗。
   您可以使用 1 到 1440 分鐘之間的值。
7. [僅適用於 PowerShell 指令碼] 設定 PowerShell 執行原則。

如需有關此原則的詳細資訊，請參閱 Microsoft 文件。

8. 按一下 **[立即執行]**。

從指令碼存放庫標籤執行指令碼

1. 在 Cyber Protect 主控台，前往 **[管理]** > **[指令碼存放庫]**。
2. 選取您要執行的指令碼，然後按一下 **[指令碼快速執行]**。
3. 按一下 **[新增工作負載]** 選取目標工作負載，然後按一下 **[新增]**。
4. 按一下 **[選擇指令碼]**，選取您要使用的指令碼，然後按一下 **[完成]**。
5. 選擇指令碼要在目標工作負載執行的帳戶。您可以選取下列選項：
   - 系統帳戶(在 macOS 這是根帳戶)
   - 目前已登入的帳戶
6. 指定指令碼可在目標工作負載執行的時間長度。
   如果指令碼無法在設定的時間範圍內完成執行，Cyber Script 操作將會失敗。
   您可以使用 1 到 1440 分鐘之間的值。
7. [僅適用於 PowerShell 指令碼] 設定 PowerShell 執行原則。
   如需有關此原則的詳細資訊，請參閱 Microsoft 文件。
8. 按一下 **[立即執行]**。

管理工作負載和檔案的備份與復原

備份模組可啟用實體與虛擬機器、檔案與資料庫的備份與復原到本機或雲端儲存空間。

備份

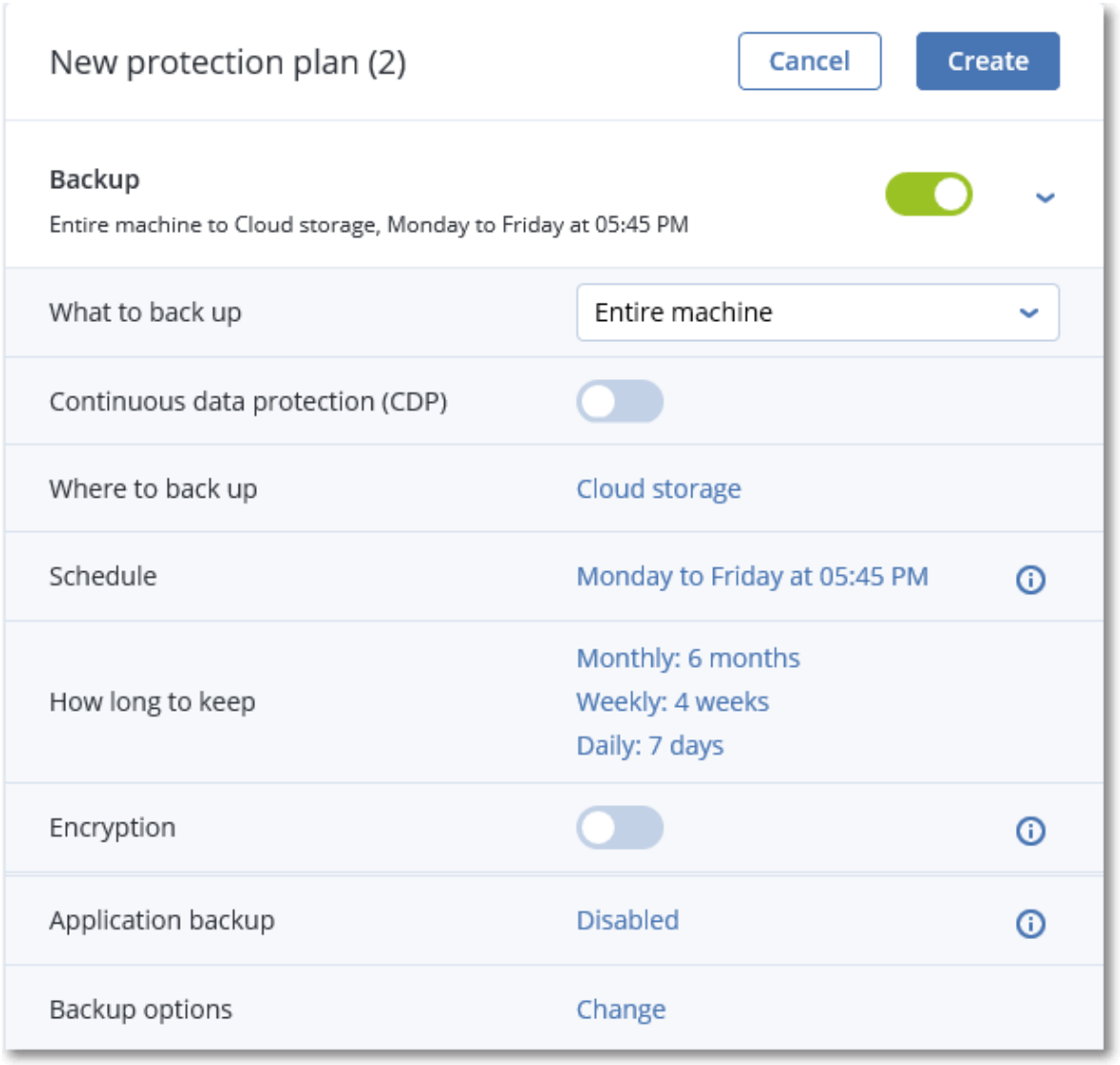
已啟用 [備份] 模組的保護計劃是一組規則，用於指定將在指定電腦上保護指定資料的方式。

保護計劃可在其建立時 (或之後) 套用至多部電腦。

在啟用 [備份] 模組的情況下，建立第一個保護計劃

1. 選擇您要備份的電腦。
2. 按一下 **[保護]**。

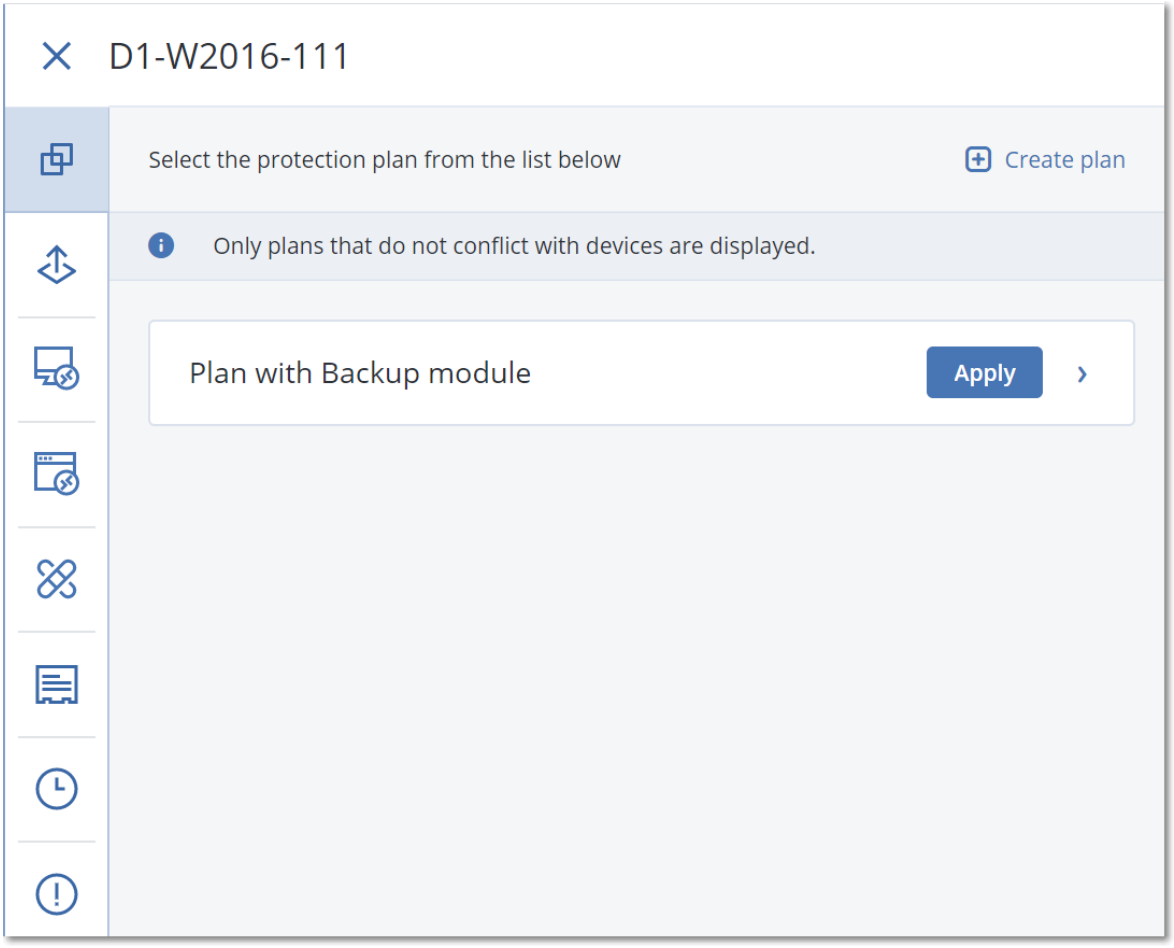
   顯示套用於機器的保護計劃。如果機器尚未指派任何計劃，則您將看到可套用的預設保護計劃。您可以視需要調整設定，並套用此計劃或建立新的計劃。
3. 若要建立新的計劃，按一下 **[建立計劃]**。啟用 **[備份]** 模組，並展開設定。



4. [選用] 若要修改保護計劃名稱，請按一下預設名稱。
5. [選用] 若要修改 [備份] 模組參數，請按一下保護計劃面板的對應設定。
6. [選用] 若要修改備份選項，請按一下 **[備份選項]** 旁邊的 **[變更]**。
7. 按一下 **[建立]**。

套用現有的保護計劃

1. 選擇您要備份的電腦。
2. 按一下 **[保護]**。如果已將一般保護計劃套用至選擇的電腦，請按一下 **[新增計劃]**。
   軟體會顯示先前建立的保護計劃。



3. 選擇要套用的保護計劃。
4. 按一下**[套用]**。

保護計劃速查表

下表摘述可用的保護計劃參數。使用本表格建立最符合您需求的保護計劃。

要備份的內容	要備份的項目	備份目標位置	排程 備份配置	保留多長時間

	選擇方法			
磁碟/磁碟區 (實體機器[1])	直接選擇 原則規則 檔案篩選器	雲端 本機資料夾 網路資料夾 NFS* Secure Zone**	一律增量 (單一檔案) 一律完整備份 每週完整備份，每日增量備份 每月完整備份、每週差異備份和每日增量備份 (GFS) 自訂 (F-D-I)	按照備份存留期 (單一規則/每一組備份) 按照備份數目 依備份大小總計*** 永久保留
磁碟/磁碟區 (虛擬機器[2])	原則規則 檔案篩選器	雲端 本機資料夾 網路資料夾 NFS*		
檔案 (僅限實體機器[3])	直接選擇 原則規則 檔案篩選器	雲端 本機資料夾 網路資料夾 NFS* Secure Zone**	一律增量 (單一檔案) 一律完整備份 每週完整備份，每日增量備份 每月完整備份、每週差異備份和每日增量備份 (GFS) 自訂 (F-D-I)	
ESXi 設定	直接選擇	本機資料夾 網路資料夾 NFS*		
網站 (檔案和 MySQL 資料庫)	直接選擇	雲端	—	

[1]作業系統中所安裝之代理程式備份的電腦。
[2]外部代理程式 (例如 VMware 用代理程式或 Hyper-V 用代理程式) 在 Hypervisor 層級備份的虛擬機器。從備份觀點來看，內部具有代理程式的虛擬機器會被視為實體機器。
[3]作業系統中所安裝之代理程式備份的電腦。

系統狀態		直接選擇	雲端 本機資料夾 網路資料夾	一律完整備份 每週完整備份，每日增量備份 自訂 (F-I)
SQL 資料庫				
Exchange 資料庫				
Microsoft 365	信箱 (本機 Microsoft 365 用代理程式)	直接選擇	本機資料夾 網路資料夾	一律增量 (單一檔案) - 僅是用於 SQL 資料庫 一律增量 (單一檔案)
	信箱 (雲端 Microsoft 365 用代理程式)	直接選擇	雲端	每天最多 6 個備份
	公用資料夾			
	Teams			
	OneDrive 檔案	直接選擇		
	SharePoint Online 資料	原則規則		
Google Workspace	Gmail 信箱	直接選擇	雲端	每天最多 6 個備份
	Google 雲端硬碟檔案	直接選擇		
	共用磁碟機檔案	原則規則		

* 在 Windows 中無法使用備份至 NFS 共用。

** 在 Mac 上無法建立 Secure Zone。

*** **依備份大小總計**保留規則不適用於**一律增量 (單一檔案)**備份配置或備份到雲端儲存空間時。

選擇要備份的資料

選擇整部機器

整部電腦的備份就是其所有非卸除式磁碟的備份。有關磁碟備份的更多資訊，請參閱 "選擇磁碟或磁碟區" (第 357 頁)。

限制

- 遭到鎖定的加密 APFS 磁碟區不支援磁碟層級備份。在整部電腦備份期間，將會略過這類磁碟區。
- 依預設，OneDrive 根資料夾會從備份作業中排除。如果您選取備份特定 OneDrive 檔案與資料夾，則會備份它們。裝置上無法使用的檔案將會在備份集中有無效內容。

選擇磁碟或磁碟區

磁碟層級備份包含磁碟或磁碟區的封裝式複本。您可以從磁碟層級備份復原磁碟、磁碟區、資料夾和檔案。

您可以在保護計劃中，針對各個工作負載選擇要備份的磁碟或磁碟區 (直接選擇)，或者您可以從多個工作負載中設定原則規則。此外，您可以透過設定檔案篩選，從備份中排除特定檔案，或在備份中僅包含特定檔案。如需詳細資訊，請參閱 "檔案篩選器 (包含/排除)" (第 408 頁)。

若要選擇磁碟或磁碟區

直接選擇

只有實體機器才能進行直接選擇。

1. 在 **[要備份的內容]** 中選擇 **[磁碟/磁碟區]**。
2. 按一下 **[要備份的項目]**。
3. 在 **[選擇要備份的項目]** 中，選擇 **[直接]**。
4. 針對保護計劃中包含的每個工作負載，選擇要備份的磁碟或磁碟區旁的核取方塊。
5. 按一下**[完成]**。

按原則規則

1. 在 **[要備份的內容]** 中選擇 **[磁碟/磁碟區]**。
2. 按一下 **[要備份的項目]**。
3. 在 **[選擇要備份的項目]** 中，選擇 **[使用原則規則]**。
4. 選擇任何預先定義的規則、輸入您自己的規則，或兩者並用。
   如需有關可用原則規則的詳細資訊，請參閱 "磁碟和磁碟區的原則規則" (第 359 頁)。
   原則規則將會套用至包含在保護計劃中的所有工作負載。
   如果沒有任何指定的規則可以套用至工作負載，備份該工作負載將失敗。
5. 按一下**[完成]**。

限制

- 遭到鎖定的加密 APFS 磁碟區不支援磁碟層級備份。在整部電腦備份期間，將會略過這類磁碟區。
- 依預設，OneDrive 根資料夾會從備份作業中排除。如果您選取備份特定 OneDrive 檔案與資料夾，則會備份它們。裝置上無法使用的檔案將會在備份集中有無效內容。

- 您可以備份透過 iSCSI 通訊協定連線至實體機器的磁碟。但是，如果您使用 VMware 用代理程式或 Hyper-V 用代理程式備份 iSCSI 連線的磁碟，則會有一些限制。如需詳細資訊，請參閱 "限制" (第 31 頁)。

磁碟或磁碟區備份儲存哪些內容？

磁碟或磁碟區備份會將磁碟或磁碟區**檔案系統**作為一個整體來儲存，並且會包括啟動作業系統的一切必要資訊。從這種備份，您可以將磁碟或磁碟區及單個資料夾或檔案作為一個整體來復原。

在 **逐個磁區 (原始模式)** 備份選項為啟用的情況下，磁碟備份會儲存磁碟的所有磁區。逐個磁區備份可用來備份具有無法識別或不支援檔案系統的磁碟和其他專的資料格式。

Windows

磁碟區備份會儲存所選磁碟區的所有檔案和資料夾 (包括隱藏和系統檔案，不論其屬性為何)、開機記錄、檔案分配表 (FAT) (若有)、載有主要開機記錄 (MBR) 的硬碟的根目錄和零磁軌。

磁碟備份儲存所選磁碟的所有磁碟區 (包括諸如廠商的維護磁碟分割的隱藏磁碟區) 以及載有主要開機記錄的零磁軌。

下列項目*不*包含在磁碟或磁碟區備份 (以及檔案層級備份):

- 置換檔案 (pagefile.sys) 和當電腦進入休眠狀態 (hiberfil.sys) 時用於記載 RAM 內容的檔案。復原後，將在相應的位置以零大小重新建立這些檔案。
- 如果在作業系統下執行備份 (而不是可開機媒體或在 hypervisor 層級備份虛擬機器):
  - Windows 陰影存放區。該存放區的路徑取決於登錄值 **VSS Default Provider**，該值位於登錄機碼 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup**。也就是說，採用 Windows Vista 開始的作業系統，均未對 Windows 還原點進行備份。
  - 如果**磁碟區陰影複製服務 (VSS)** 備份選項已啟用，檔案和資料夾指定於 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** 登錄機碼中。

Linux

磁碟區備份會儲存所選磁碟區的所有檔案和目錄 (不論其屬性為何)、開機記錄及檔案系統超級區塊。

磁碟備份儲存所有磁碟磁碟區以及包含主開機記錄的第零軌。

Mac

磁碟或磁碟區備份儲存所選磁碟或磁碟區的所有檔案和目錄，以及磁碟區版面配置說明。

排除下列項目:

- 系統中繼資料，如檔案系統日誌和 Spotlight 索引
- 垃圾桶
- Time Machine 備份

實際，備份 Mac 上檔案層級的磁碟和磁碟區。可從磁碟區進行裸機復原，並可進行磁碟區備份，但逐一磁區備份模式不可用。

磁碟和磁碟區的原則規則

當您選擇要備份的磁碟或磁碟區時，可以根據受保護工作負載的作業系統，使用下列原則規則。

Windows

- `[All Volumes]` 會選擇電腦上的所有磁碟區。
- 磁碟機代號 (例如 `C:\`) 會選擇具有指定磁碟機代號的磁碟區。
- `[Fixed Volumes (physical machines)]` 會選擇實體機器的所有磁碟區，而不會選擇卸除式媒體的磁碟區。固定磁碟區包括 SCSI、ATAPI、ATA、SSA、SAS 和 SATA 裝置以及 RAID 陣列上的磁碟區。
- `[BOOT+SYSTEM]` 會選擇系統與開機磁碟區。這是您可以復原作業系統的最小組合。
- `[Disk 1]` 會選擇電腦的第一個磁碟，包含該磁碟上所有磁碟區。如果要選擇其他磁碟，請輸入對應編號。

Linux

- `[All Volumes]` 會選擇電腦上所有的已掛載磁碟區。
- `/dev/hda1` 會選擇第一個 IDE 硬碟上的第一個磁碟區。
- `/dev/sda1` 會選擇第一個 SCSI 硬碟上的第一個磁碟區。
- `/dev/md1` 會選擇第一個軟體 RAID 硬碟。
- 若要選擇其他基本磁碟區，請指定 `/dev/xdyN`，其中：
  - "x" 對應磁碟類型
  - "y" 對應磁碟編號 (a 表示第一個磁碟、b 表示第二個磁碟，以此類推)
  - "N" 是磁碟區編號。
- 若要選擇邏輯磁碟區，請在以根帳戶的身分執行 `ls /dev/mapper` 命令之後，指定該磁碟區所顯示的路徑。

  例如：

  ```
  [root@localhost ~]# ls /dev/mapper/
  control vg_1-lv1 vg_1-lv2
  ```

  此輸出會顯示兩個邏輯磁碟區 `lv1` 和 `lv2`，這兩個邏輯磁碟區都屬於磁碟區群組 `vg_1`。若要備份這些磁碟區，請指定：

  `/dev/mapper/vg_1-lv1`
  `/dev/mapper/vg-l-lv2`

macOS

- `[All Volumes]` 會選擇電腦上所有的已掛載磁碟區。
- `[Disk 1]` 會選擇電腦的第一個磁碟，包含該磁碟上所有磁碟區。若要選擇其他磁碟，請指定對應編號。

選擇檔案或資料夾

使用檔案層級備份僅能保護特定資料，例如，您目前專案中的檔案。檔案層級備份比磁碟層級備份小，因此可節省儲存空間。

重要事項
您無法從檔案層級備份復原作業系統。

您可以在保護計劃中，針對各個工作負載選擇要備份的檔案和資料夾 (直接選擇)，或者您可以從多個工作負載中設定原則規則。此外，您可以透過設定篩選，從備份中排除特定檔案，或在備份中僅包含特定檔案。如需詳細資訊，請參閱 "檔案篩選器 (包含/排除)" (第 408 頁)。

若要選擇檔案或資料夾

直接選擇

1. 在 **[要備份的內容]** 中，選擇 **[檔案/資料夾]**。
2. 在 **[要備份的項目]** 中，按一下 **[指定]**。
3. 在 **[選擇要備份的項目]** 中，選擇 **[直接]**。
4. 在保護計劃中，針對每個工作負載指定要備份的檔案或資料夾。
   a. 按一下 **[選擇檔案和資料夾]**。
   b. 按一下 **[本機資料夾]** 或 **[網路資料夾]**。
      網路資料夾必須可從所選電腦存取。
      當您選擇 **[網路資料夾]** 作為來源時，可以從網路連接儲存裝置 (NAS) (例如 NetApp 裝置) 備份資料。所有廠商的 NAS 裝置皆受支援。
   c. 在資料夾樹狀目錄中，導覽至所需的檔案或資料夾。
      或者，指定檔案或資料夾的路徑，然後按一下箭頭按鈕。
   d. [針對共用資料夾] 出現提示時，指定共用資料夾的存取認證。
      不支援備份具有匿名存取權的資料夾。
   e. 選擇所需的檔案和資料夾。
   f. 按一下**[完成]**。

按原則規則

1. 在 **[要備份的內容]** 中，選擇 **[檔案/資料夾]**。
2. 在 **[要備份的項目]** 中，按一下 **[指定]**。
3. 在 **[選擇要備份的項目]** 中，選擇 **[使用原則規則]**。
4. 選擇任何預先定義的規則、輸入您自己的規則，或兩者並用。
   如需有關可用原則規則的詳細資訊，請參閱 "檔案與資料夾的原則規則" (第 361 頁)。
   原則規則將會套用至包含在保護計劃中的所有工作負載。
   如果沒有任何指定的規則可以套用至工作負載，備份該工作負載將失敗。
5. 按一下**[完成]**。

限制

- 您可以在備份安裝代理程式所在的實體機器或虛擬機器 (代理程式型備份) 時，選擇檔案和資料夾。檔案層級備份不適用於在用無代理程式模式下備份的虛擬機器。如需有關這些備份類型間差異的詳細資訊，請參閱 "代理程式型和無代理程式備份" (第 56 頁)。
- 依預設，OneDrive 根資料夾會從備份作業中排除。如果您選取備份特定 OneDrive 檔案與資料夾，則會備份它們。裝置上無法使用的檔案將會在備份集中有無效內容。
- 您可以備份透過 iSCSI 通訊協定連線至實體機器的磁碟上的檔案和資料夾。如果您使用 VMware 用代理程式或 Hyper-V 用代理程式備份 iSCSI 連線磁碟上的資料，則會有一些限制。

檔案與資料夾的原則規則

當您選擇要備份的檔案或資料夾時，可以根據受保護工作負載的作業系統，使用下列原則規則。

Windows

- 檔案或資料夾的完整路徑。例如 `D:\Work\Text.doc` 或 `C:\Windows`。
- 預先定義的規則：
  - `[All Files]` 會選擇電腦的所有磁碟區上的所有檔案。
  - `[All Profiles Folder]` 會選擇所有使用者設定檔所在的資料夾。例如 `C:\Users` 或 `C:\Documents and Settings`。
- 環境變數：
  - `%ALLUSERSPROFILE%` 會選擇所有使用者設定檔的一般資料所在的資料夾。例如 `C:\ProgramData` 或 `C:\Documents and Settings\All Users`。
  - `%PROGRAMFILES%` 會選擇 `Program Files` 資料夾。例如 `C:\Program Files`。
  - `%WINDIR%` 會選擇 `Windows` 資料夾。例如 `C:\Windows`。

  您可使用其他環境變數或環境變數和文字的組合。例如，若要選擇 [Program Files] 資料夾中的 [Java] 資料夾，請指定：`%PROGRAMFILES%\Java`。

Linux

- 檔案或目錄的完整路徑。

  例如，若要將 `file.txt` 檔案備份在掛載於 `/home/usr/docs` 的磁碟區 `/dev/hda3`，請指定 `/dev/hda3/file.txt` 或 `/home/usr/docs/file.txt`。
- 預先定義的規則：
  - `[All Profiles Folder]` 會選擇 `/home`。根據預設，所有使用者設定檔都儲存在此資料夾中。
  - `/home` 會選擇一般使用者的主目錄。
  - `/root` 會選擇 root 使用者的主目錄。
  - `/usr` 會選擇所有使用者相關程式的目錄。
  - `/etc` 會選擇系統組態檔案的目錄。

macOS

- 檔案或目錄的完整路徑。

  例如：

- 若要在使用者的桌面備份 `file.txt`，請指定 `/使用者/<使用者名稱>/桌面/file.txt`。
- 若要備份使用者的 [桌面]、[文件] 和 [下載] 資料夾，請指定 `/使用者/<使用者名稱>/桌面`、`/使用者/<使用者名稱>/文件` 和 `/使用者/<使用者名稱>/下載`。
- 若要備份在此電腦上擁有帳戶的所有使用者的主資料夾，請指定 `/使用者`。
- 若要備份安裝應用程式所在的資料夾，請指定 `/Applications`。

- 預先定義的規則
  - `[All Profiles Folder]` 會選擇 `/Users`。根據預設，所有使用者設定檔都儲存在此資料夾中。

選擇系統狀態

注意事項
系統狀態備份可用於執行 Windows 7 或更新版本且安裝 Windows 用代理程式的電腦上。系統狀態備份不適用於在 Hypervisor 層級備份 (無代理程式備份) 的虛擬機器上。

若要備份系統狀態，請在 **[要備份的內容]** 中選擇 **[系統狀態]**。

系統狀態備份包含下列檔案：

- 工作排程器設定
- VSS 中繼資料儲存庫
- 效能計數器設定資訊
- MSSearch Service
- Background Intelligent Transfer Service (BITS)
- 登錄
- Windows Management Instrumentation (WMI)
- Component Services Class 登錄資料庫

選擇 ESXi 設定

ESXi 主機設定備份可將 ESXi 主機復原至裸機。此復原會以可開機媒體執行。

在主機上執行的虛擬機器並未包含在備份中。這些虛擬機器可以另行單獨備份和復原。

ESXi 主機設定備份包含下列幾項：

- 主機的開機載入器和開機程式組磁碟分割。
- 主機狀態 (虛擬網路和存放區設定、SSL 金鑰、伺服器網路設定，和本機使用者資訊)。
- 已安裝或儲存在主機上的副檔名和修補。
- 記錄檔。

必要條件

- 必須在 ESXi 主機設定的**安全設定檔**中啟用 SSH。
- 您必須知道 ESXi 主機上「根」帳戶的密碼。

限制

- 執行 VMware ESXi 7.0 和更新版本的主機不支援 ESXi 設定備份。
- 無法將 ESXi 設定備份至雲端儲存空間。

選擇 ESXi 設定

1. 按一下 **[裝置]** > **[所有裝置]**, 然後選擇要備份的 ESXi 主機。
2. 按一下 **[保護]**。
3. 在**要備份的內容**中, 選擇 **ESXi 配置**。
4. 在**ESXi「根」密碼**中, 為每個所選擇的主機指定「根」帳戶的密碼, 或是讓所有主機適用同一個密碼。

連續資料保護 (CDP)

連續資料保護 (CDP) 是 Advanced Backup 套件的一部分。它會在變更此資料後立即備份關鍵資料, 確保如果系統在兩次排程備份之間出現故障, 不會遺失任何變更。您可以為以下資料設定連續資料保護:

- 特定位置的檔案或資料夾
- 特定應用程式修改的檔案

僅 NTFS 檔案系統和以下作業系統支援連續資料保護:

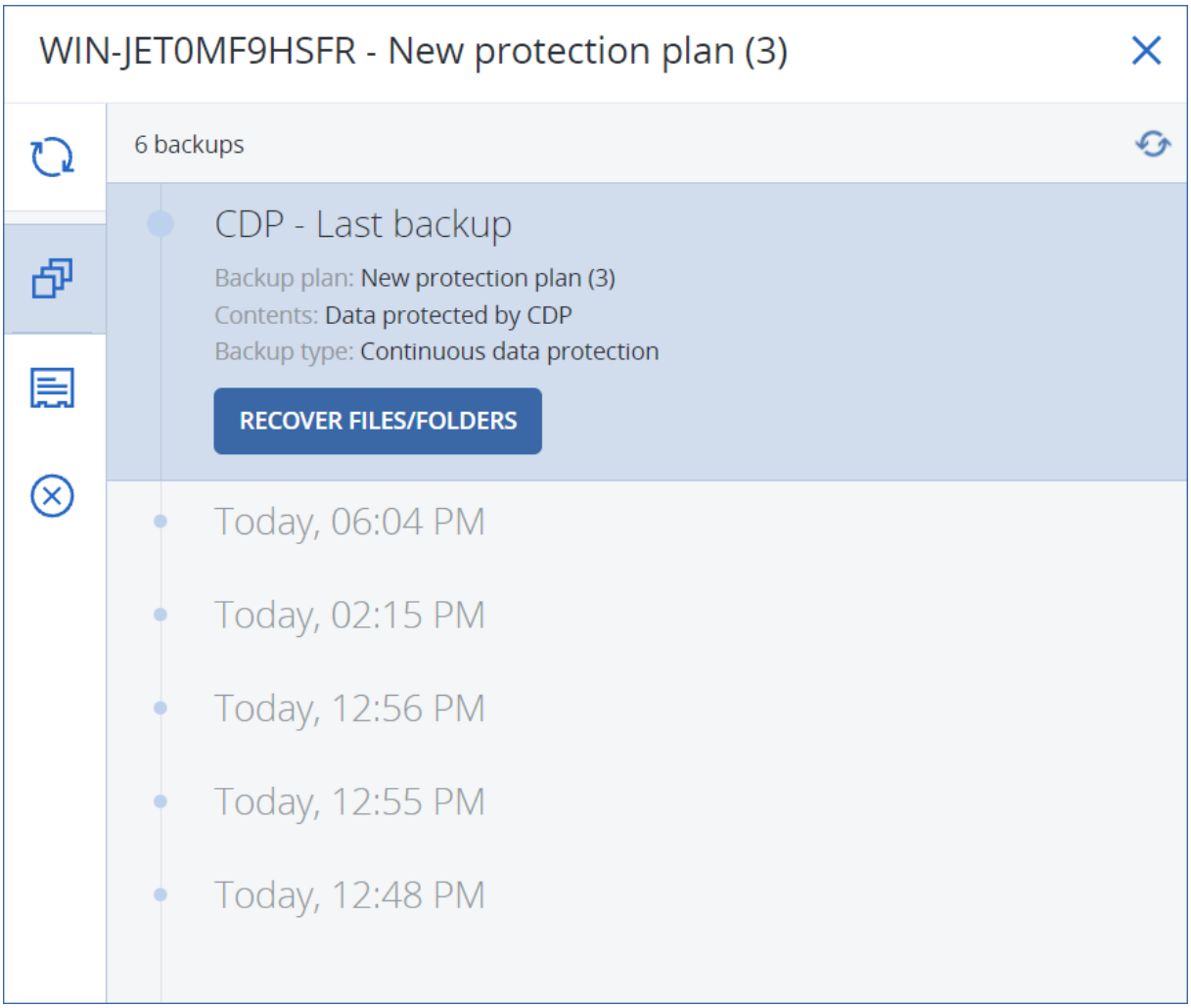
- 桌面:Windows 7 和更新版本
- 伺服器:Windows Server 2008 R2 和更新版本

僅支援本機資料夾。無法選擇網路資料夾進行連續資料保護。

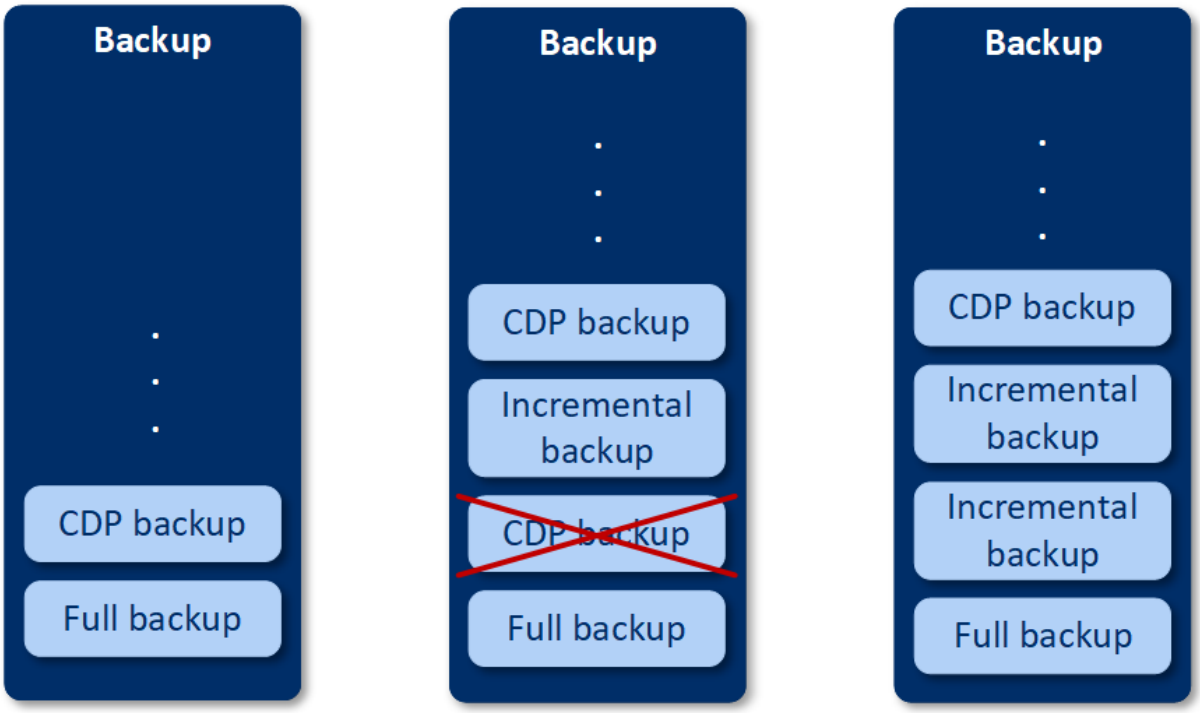
連續資料保護與 **[應用程式備份]** 選項不相容。

運作原理

透過連續資料保護追蹤的檔案和資料夾, 其中的變更會立即保存到特殊 CDP 備份中。一個備份組中只有一個 CDP 備份, 始終是最新備份。



當排程備份啟動時，連續資料保護將被置於暫停狀態，因為最新資料將包含在排程備份中。當排程的備份完成後，連續資料保護將會繼續，舊的 CDP 備份會遭到刪除，並建立新的 CDP 備份。因此，CDP 備份始終保留備份組的最新備份，並且僅儲存追蹤檔案或資料夾的最新狀態。



如果機器在定期備份期間當機，連續資料保護會在機器重新啟動後自動復原，並在上次成功的排程備份之上建立 CDP 備份。

繼續資料保護要求在 CDP 備份之前至少建立一個定期備份。這就是為什麼，當您首次執行包含連續資料保護的保護計劃時，會建立完整備份，並立即在備份之上加入 CDP 備份。如果為現有保護計劃啟用 **[連續資料保護]** 選項，則 CDP 備份將加入現有備份組。

注意事項

如果系統為您啟用 Advanced Backup 功能，而且您未將其他 Advanced Backup 功能用於所選電腦，則預設會針對您從 **[裝置]** 索引標籤建立的保護計劃，啟用連續資料保護。如果您已經為所選電腦制定了具有連續資料保護的計劃，則預設不會在新建立的計劃中，為該電腦啟用連續資料保護。系統預設不會針對為裝置群組建立的計劃，啟用連續資料保護。

支援的資料來源

您可以使用以下資料來源設定連續資料保護：

- 整部電腦
- 磁碟/磁碟區
- 檔案/資料夾

在保護計劃的 **[備份內容]** 部分選擇資料來源後，在 **[要連續保護的項目]** 部分中，選擇用於連續資料保護的檔案、資料夾或應用程式。有關如何設定連續資料保護的詳細資訊，請參閱 "設定 CDP 備份" (第 366 頁)。

支援的目的地

您可以使用以下目的地設定連續資料保護：

- 本機資料夾
- 網路資料夾
- 雲端儲存
- Acronis Cyber Infrastructure
- 指令碼所定義的位置

注意事項
您只能透過指令碼定義上面列出的位置。

設定 CDP 備份

您可以在保護計劃的 **[備份]** 模組中設定連續資料保護。有關如何建立保護計劃的詳細資訊，請參閱 "建立保護計劃" (第 192 頁)。

編輯連續資料保護設定

1. 在保護計劃的 **[備份]** 模組中，啟用 **[連續資料保護 (CDP)]** 開關。
   此開關僅適用於以下資料來源：
   - 整部電腦
   - 磁碟 / 磁碟區
   - 檔案/資料夾
2. 在 **[要連續保護的項目]**中，為 **[應用程式]** 或 **[檔案/資料夾]** 或兩者設定連續資料保護。
   - 按一下 **[應用程式]** 為特定應用程式修改的檔案設定 CDP 備份。
     您可以從預先定義的類別中選擇應用程式，或透過指定可執行檔的路徑來加入其他應用程式，例如：
     - `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`
     - `*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`
   - 按一下 **[檔案/資料夾]** 為特定位置的檔案設定 CDP 備份。
     您可以使用選擇規則或直接選擇檔案和資料夾來定義這些位置。
     - [對於所有機器] 要建立選擇規則，請使用文字方塊。
       您可以使用檔案的完整路徑或具有萬用字元(* 和?) 的路徑。星號代表零個或多個字元。問號代表單一字元。

       重要事項
       要為資料夾建立 CDP 備份，必須使用星號萬用字元指定其內容：
       正確的路徑：`D:\Data\*`
       不正確的路徑：`D:\Data\`

     - [對於連線機器] 要直接選擇檔案和資料夾：
       - 在 **[要瀏覽的電腦]** 中，選擇檔案或資料夾所在的機器。
       - 按一下 **[選擇檔案和資料夾]** 以瀏覽選定的機器。
         直接選擇將建立選擇規則。如果將保護計劃套用於多台機器，並且某個選擇規則對某台機器無效，則在此機器上將跳過該保護計劃。

3. 在保護計劃窗格中，按一下 **[建立]**。

因此，您指定的資料將在排程備份之間進行連續備份。

選擇目的地

請按一下 **[備份目標位置]**，然後選擇下列其中一項：

- **雲端儲存**

  備份將儲存在雲端資料中心。
- **本機資料夾**

  如果選擇單一電腦，請瀏覽所選擇電腦上的資料夾，或是輸入資料夾路徑。

  如果選擇多部機器，請輸入資料夾路徑。備份將儲存在所選擇的每部實體機器裡的這個資料夾中，或是儲存在已安裝虛擬機器用代理程式的電腦上。如果資料夾不存在，則會建立資料夾。
- **網路資料夾**

  這是透過 SMB/CIFS/DFS 共用的資料夾。

  瀏覽所需的共用資料夾或按下列格式輸入路徑：
  - SMB/CIFS 共用：`\\<主機名稱>\<路徑>\` 或 `smb://<主機名稱>/<路徑>/`
  - DFS 共用：`\\<完整 DNS 網域名稱>\<DFS 根>\<路徑>`

    例如 `\\example.company.com\shared\files`

  然後按一下箭頭按鈕。如果看到提示，請指定共用資料夾的使用者名稱和密碼。您可以隨時按一下資料夾名稱旁邊的鑰匙圖示來變更這些認證。

  不支援備份至具有匿名存取權的資料夾。
- **公有雲端**

  此選項可當作 Advanced Backup 套件的一部分提供。

  它可讓您設定直接備份至公有雲端相容的儲存空間，而不需要部署額外的元件 (例如，Microsoft Azure 或當作閘道的其他虛擬機器)。視需要選擇並連線至相關的公有雲端。

  如需詳細資訊，請參閱 "將工作負載備份至公有雲端" (第 480 頁)。
- **NFS 資料夾**(可用於執行 Linux 或 Mac OS 的電腦)

  請確認安裝 Linux 用代理程式所在的 Linux 伺服器上已安裝 nfs-utils 套件。

  瀏覽所需的 NFS 資料夾，或在下列格式中輸入路徑：

  `nfs://<主機名稱>/<匯出的資料夾>:/<子資料夾>`

  然後按一下箭頭按鈕。

  注意事項

  無法備份至受密碼保護的 NFS 資料夾。
- **Secure Zone** (若存在每個所選擇的電腦中，則可以使用)

  Secure Zone 是指位於備份電腦磁碟上的安全磁碟分割。此磁碟分割必須在設定備份之前手動建立。如需有關如何建立 Secure Zone 及其優點和限制的資訊，請參閱 "關於 Secure Zone" (第 368 頁)。

進階儲存選項

注意事項
此功能僅適用於 Cyber Protection 服務的 Advanced 版本。

由指令碼定義 (適用於執行 Windows 的電腦)

您可以將每台電腦的備份儲存在指令碼定義的資料夾中。此軟體支援以 JScript、VBScript 或 Python 3.5 撰寫的指令碼。部署保護計劃時，此軟體會在每部電腦上執行指令碼。每台電腦的指令碼輸出應該是本機或網路資料夾路徑。如果資料夾不存在，系統會建立一個資料夾 (限制：以 Python 撰寫的指令碼無法在網路共用上建立資料夾)。在 **[備份儲存]** 索引標籤上，每個資料夾都會顯示為個別的備份位置。

在 **[指令碼類型]** 中，選擇指令碼類型 (**JScript**、**VBScript** 或 **Python**)，然後匯入或複製並貼上指令碼。對於網路資料夾，請使用讀取/寫入權限指定存取認證。

範例：

- 下列 JScript 指令碼會以 \\bkpsrv\<電腦名稱> 格式，輸出電腦的備份位置：

  ```
  WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject("WScript.Network").ComputerName);
  ```

  因此，每台電腦的備份將會儲存在伺服器 **bkpsrv** 上的同名資料夾中。
- 以下 JScript 指令碼將輸出備份位置到位於執行指令碼的機器上的資料夾：

  ```
  WScript.Echo("C:\\Backup");
  ```

  因此，此機器的備份將保存在同一台機器上的 C:\Backup 資料夾中。

  注意事項
  這些指令碼中的位置路徑區分大小寫。因此，C:\Backup 和 C:\backup 在 Cyber Protect 主控台中顯示為不同的位置。此外，使用大寫作為磁碟機代號。

關於 Secure Zone

Secure Zone 是指位於備份電腦磁碟上的安全磁碟分割。其可儲存該電腦的磁碟或檔案備份。

若磁碟發生實體故障，則可能會失去位於 Secure Zone 中的備份。這就是為什麼 Secure Zone 不應該是儲存備份所在唯一位置的原因。在企業環境中，當普通位置暫時無法使用或透過緩慢或繁忙的通道連線時，可將 Secure Zone 視為用於備份的中間位置。

為什麼要使用 Secure Zone?

Secure Zone：

- 可將磁碟復原至磁碟備份所在的同一磁碟。
- 提供具有成本效益且易用的方法，可保護資料免受軟體故障、病毒攻擊、操作員錯誤的影響。

- 無需另外使用媒體或網路連線即可備份或復原資料。這對漫遊使用者尤為方便。
- 使用備份的複寫時，可以做為主要目的地。

限制

- 您無法在 Mac 上組織管理 Secure Zone。
- Secure Zone 是位於基本磁碟上的磁碟分割。無法在動態磁碟上進行組織管理，或是建立為邏輯磁碟區 (由 LVM 管理)。
- Secure Zone 採用 FAT32 檔案系統的格式。由於 FAT32 設有 4-GB 檔案大小的限制，因此在儲存到 Secure Zone 時，系統會分割大型備份。這不會影響復原程序和速度。

建立 Secure Zone 如何轉換磁碟

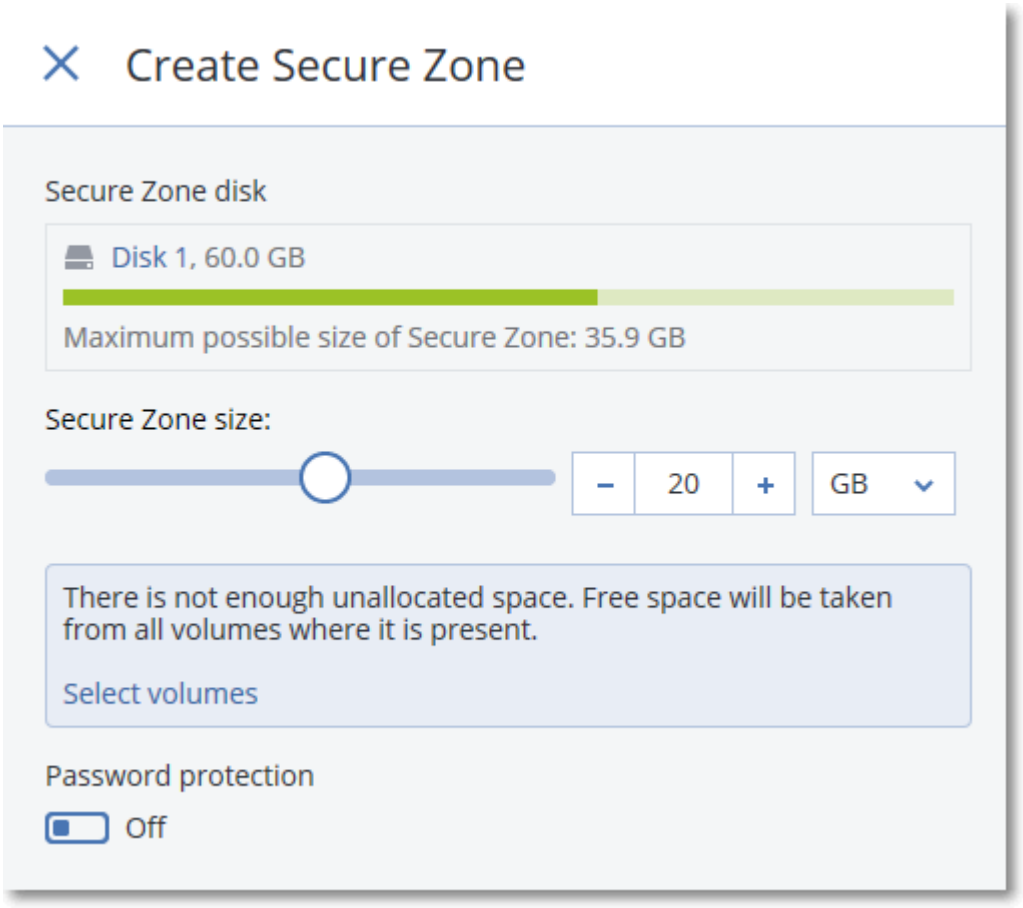
- Secure Zone 一律會在硬碟的末尾區域建立。
- 如果在磁碟末尾沒有未配置空間或未配置空間不足，但是在磁碟區之間有未配置空間，則將會移動磁碟區以便在磁碟末尾增加更多的未配置空間。
- 當集合了所有的未配置空間仍然不足，軟體將使用您選擇的磁碟區上的可用空間，成比例降低磁碟區的大小。
- 但是，在磁碟區上應該有可用空間，這樣作業系統和應用程式才能 運行；例如建立暫存檔。如果可用空間等於或低於磁碟區總大小的 25%，軟體將不會減少磁碟區的大小。僅在磁碟上所有磁碟區的可用空間都為 25% 或更低時，軟體才會繼續按比例減少磁碟區大小。

可見直接指定可能的 Secure Zone 大小上限並不是明智的選擇。最後所有磁碟區都會沒有可用空間，這將導致作業系統或應用程式運作不穩定，甚至無法啟動。

重要事項
移動系統開機使用的磁碟區或調整其大小需要重新開機。

如何建立 Secure Zone

1. 選擇您要在上面建立 Secure Zone 的電腦。
2. 按一下 **[詳細資料]** > **[建立 Secure Zone]**。
3. 在 **Secure Zone 磁碟**下，按一下 **[選擇]**，然後選擇要在上面建立安全區的硬碟(若有數個硬碟)。
   軟體會計算 Secure Zone 可能的大小上限。
4. 輸入 Secure Zone 大小，或拖曳滑桿以選擇大小下限與上限之間的任何大小。
   最小大小約為 50 MB，視硬碟的幾何分佈而定。最大大小等於磁碟的未配置空間，加上磁碟所有磁碟區上的總可用空間。
5. 如果所有未配置空間不能滿足您指定的大小，軟體將使用現有磁碟區的可用空間。系統預設為全選所有磁碟區。如果您要排除一些磁碟區，按一下**[選擇磁碟區]**。否則，請跳過此步驟。



6. [選用] 啟用**[密碼保護]**開關，並指定密碼。
   存取位於 Secure Zone 的備份需要密碼。除非備份是在可開機媒體下執行的，否則備份至 Secure Zone 不需要密碼。
7. 按一下 **[建立]**。
   軟體會顯示將產生的的磁碟分割配置。按一下 **[確定]**。
8. 等待軟體建立 Secure Zone。

您現在可以在建立保護計劃時，於 **[備份目標位置]** 中選擇 Secure Zone。

如何刪除 Secure Zone

1. 選擇包含 Secure Zone 的電腦。
2. 按一下**[詳細資料]**。
3. 按一下 **Secure Zone** 旁邊的齒輪圖示，然後按一下 **[刪除]**。
4. [選用] 請指定用於儲存安全區所釋放空間的磁碟區。系統預設為全選所有磁碟區。
   空間將會在所選的磁碟區之間平均分配。如果您沒有選擇任何磁碟區，釋放出的空間將成為未配置空間。
   調整系統開機使用的磁碟區的大小會要求重啟。
5. 請按一下 **[刪除]**。

因此，Secure Zone 將連同其中儲存的所有備份一併刪除。

備份排程

您可以將備份設定為在特定時間、特定間隔或針對特定事件，自動執行。

非雲端對雲端資源的排程備份會根據安裝保護代理程式所在工作負載的時區設定執行。例如，如果您將相同的保護計劃套用到時區設定不同的工作負載，則備份將會根據每個工作負載的本機時區開始。

排程備份包括下列動作：

- 選擇備份配置
- 設定時間或選擇觸發備份的事件
- 設定選用設定和開始條件

備份配置

備份配置是保護計劃排程的一部分，可定義建立的備份類型 (完整、差異或增量) 以及建立時間。您可以選擇其中一個預先定義的備份配置或是建立自訂配置。

可用的備份配置和類型視備份位置與來源而定。例如，備份 SQL 資料、Exchange 資料或系統狀態時，無法使用差異備份。磁帶裝置不支援 **[一律增量 (單一檔案)]** 配置。

備份配置	描述	可設定的元素
一律增量 (單一檔案)	第一個備份是完整備份，因此可能很耗時。後續的備份為增量備份，因此速度明顯更快。 備份使用 [單一檔案備份格式][1]*。 依預設，由週一至週五，每天執行備份。 建議您在將備份儲存在雲端儲存中時使用此配置，因為增量備份速度快且網路流量少。	• 排程類型：每月、每週、每天、每小時 • 備份觸發：時間或事件 • 開始時間 • 開始條件 • 其他選項
始終完整備份	備份集中的所有備份都是完整備份。 依預設，由週一至週五，每天執行備份。	• 排程類型：每月、每週、每天、每小時 • 備份觸發：時間或事件 • 開始時間 • 開始條件 • 其他選項
每週完整備份，每日增量備份	完整備份是每週建立一次，其他備份則是增量備份。	• 備份觸發：時間或事件

[1]備份格式，會將初始完整備份及後續增量備份儲存為單一的 .tibx 檔案。此格式可以善用了增量備份方法的速度，同時避免其主要的缺點 - 不容易刪除過期備份。軟體會將過期備份所使用的區塊標示為「可用」，並在區塊中寫入新備份。結果會以耗費最少資源的方式，產生極快速的清理。備份至不支援隨機存取讀寫的位置時，無法使用單一檔案備份格式。

備份配置	描述	可設定的元素
	第一個備份是完整備份，當週內的其他備份則是增量備份，然後重複循環。 若要選擇在哪一天建立每週完整備份，請在保護計劃中，按一下齒輪圖示，然後移至 **[備份選項]** > **[每週備份]**。 依預設，由週一至週五，每天執行備份。	• 開始時間 • 開始條件 • 其他選項
每月完整備份、每週差異備份和每日增量備份 (GFS)	根據預設，增量備份是在星期一至星期五每天執行。差異備份是在每個星期六執行。完整備份是在每個月的第一天執行。 **注意事項** 這是預先定義的自訂配置。在保護計劃中顯示為 **[自訂]**。	• 變更每個備份類型的現有排程： ◦ 排程類型：每月、每週、每天、每小時 ◦ 備份觸發：時間或事件 ◦ 開始時間 ◦ 開始條件 ◦ 其他選項 • 新增每個備份類型的新排程
自訂	您必須選擇備份類型 (完整、差異和增量)，然後為每個類型設定個別的排程*。	• 變更每個備份類型的現有排程： ◦ 排程類型：每月、每週、每天、每小時 ◦ 備份觸發：時間或事件 ◦ 開始時間 ◦ 開始條件 ◦ 其他選項 • 新增每個備份類型的新排程

* 建立保護計劃之後，您就無法在 **[一律增量 (單一檔案)]** 和其他備份配置之間切換，反之亦然。**[一律增量 (單一檔案)]** 是一種單一檔案格式配置，其他配置則為多檔案格式。如果要在格式之間切換，請建立新的保護計劃。

備份類型

下列備份類型可供使用：

- 完整 — 完整備份中包含所有來源資料。此備份屬於自給自足型。若要復原資料，您不需要存取其他任何備份。

注意事項
任何保護計劃建立的第一個備份都是完整備份。

- 增量 — 增量備份會儲存針對最新備份 (無論是完整備份、差異備份還是增量備份) 的資料所做的變更。若要將資料復原回最初的完整備份，您將需要與增量備份相依的完整備份鏈。
- 差異 — 差異備份會儲存針對最新完整備份的資料所做的變更。若要復原資料，您將同時需要差異備份以及與差異備份相依的對應完整備份。

按計劃執行備份

若要在特定時間或對特定事件自動執行備份，請在保護計劃中啟用排程。

若要啟用排程

1. 在保護計劃中，展開 **[備份]** 模組。
2. 按一下 **[排程]**。
3. 啟用 [排程] 開關。
4. 選擇備份配置。
5. 視需要設定排程，然後按一下 **[完成]**。
   如需有關可用排程選項的詳細資訊，請參閱 "依時間排程" (第 373 頁) 和 "依據事件排程" (第 375 頁)。
6. [選用] 設定開始條件或其他排程選項。
7. 儲存保護計劃。

因此，每次符合排程條件時，備份作業便會開始。

若要停用排程

1. 在保護計劃中，展開 **[備份]** 模組。
2. 按一下 **[排程]**。
3. 停用 [排程] 開關。
4. 儲存保護計劃。

因此，只有在您手動啟動該開關時，才會執行備份。

注意事項
如果停用排程，就不會自動套用保留規則。若要套用保留規則，請手動執行備份。

依時間排程

下表摘要說明以時間為基礎的排程選項。這些選項的可用性取決於備份配置。如需詳細資訊，請參閱 "備份配置" (第 371 頁)。

選項	描述	範例
每月	選擇月份、日期或星期幾，然後選擇備份	在 1 月 1 日和 2 月 3 日的凌晨 12:00 執

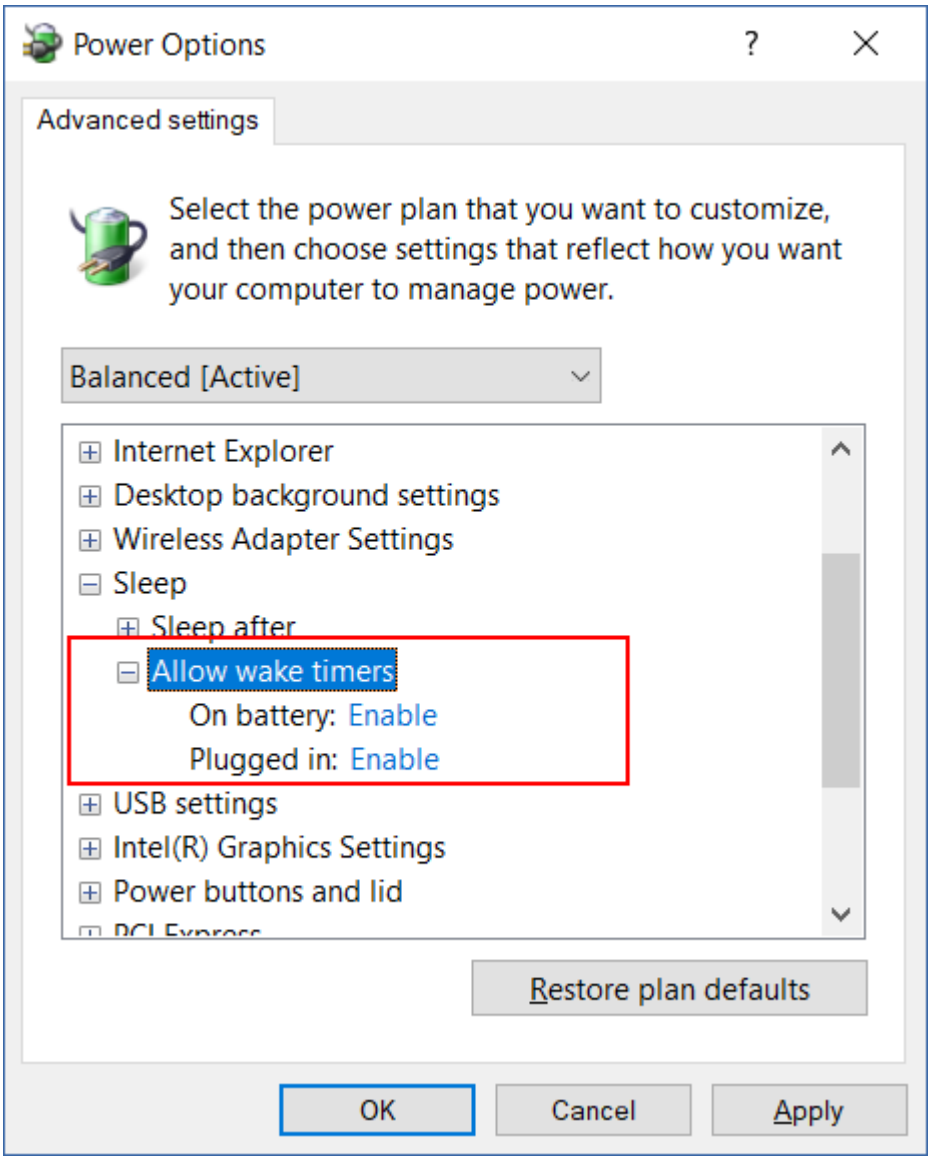
選項	描述	範例
	開始時間。	行備份。 在每個月第一天的上午 10:00 執行備份。 在 3 月 1 日、3 月 5 日、4 月 1 日和 4 月 5 日的上午 09:00 執行備份。 在每個月第二個和第三個星期五的上午 11:00 執行備份。 在每個月最後一個星期三晚上 10:30 執行備份。
每週	選擇星期幾，然後選擇備份開始時間。	在星期一到星期五上午 10:00 執行備份。 在星期一晚上 11:00 執行備份。 在星期二和星期六上午 08:00 執行備份。
每天	選擇天數 (每天或僅工作日)，然後選擇備份開始時間。	每天上午 11:45 執行備份。 在星期一到星期五晚上 09:30 執行備份。
每小時	選擇星期幾，然後選擇兩次連續備份之間的時間間隔，以及執行備份的時間範圍。 當您設定分鐘間隔時，可以選擇 10 到 60 分鐘之間的建議間隔，或指定一個自訂間隔，例如，45 或 75 分鐘。	在星期一到星期五的上午 08:00 到下午 06:00 之間，每小時執行一次備份。 在星期六和星期日的凌晨 01:00 到下午 06:00 之間，每 3 小時執行一次備份。

其他選項

當您依時間排程備份時，可以使用以下其他排程選項。

若要存取這些選項，請在 **[排程]** 窗格中，按一下 **[顯示更多]**。

- **如果電腦關閉，則在電腦啟動時執行遺漏的工作**
  預設設定：[已停用]。
- **防止在備份期間進入睡眠或休眠模式**
  此選項僅適用於執行 Windows 的電腦。
  預設設定：[啟用]。
- **從睡眠或休眠模式中喚醒，開始進行排程的備份**
  此選項僅適用於執行 Windows，並在其電源計劃中啟用 **[允許喚醒計時器]** 選項的電腦。



此選項不會使用 LAN 喚醒功能，而且不適用於已關機的電腦。

預設設定：[已停用]。

依據事件排程

若要設定針對特定事件執行的備份，請選擇以下其中一個選項。

選項	描述	範例
自上次備份後的時間	備份將在上次成功備份後的指定期間後開始。 **注意事項** 此選項將取決於上次完成備份的方式。如果備份失敗，將不會自動開始下一次備份。在此情況下，您必須手動執行備份並確保其成功完成，才能重設排程。	在上次成功備份一天後執行備份。 在上次成功備份四小時後執行備份。

選項	描述	範例
當使用者登入系統時	備份將在使用者登入電腦時開始。 您可以針對任何登入或特定使用者的登入，設定此選項。 **注意事項** 使用臨時使用者設定檔登入將不會開始備份。	使用者 John Doe 登入時執行備份。
當使用者登出系統時	備份將在使用者登出電腦時開始。 您可以針對任何登出或特定使用者的登出，設定此選項。 **注意事項** 從臨時使用者設定檔登出將不會開始備份。 關閉電腦將不會開始備份。	每個使用者登出時執行備份。
在系統啟動時	備份將會在受保護的電腦啟動時執行。	使用者啟動電腦時執行備份。
在系統關閉時	備份將會在受保護的電腦關閉時執行。	使用者關閉電腦時執行備份。
發生 Windows 事件記錄中的事件時	備份將會在發生您指定的 Windows 事件時執行。	當 Windows 系統記錄檔中記錄錯誤類型為事件 7 且來源為磁碟時，執行備份。

這些選項的可用性取決於備份來源和受保護工作負載的作業系統。下表摘要說明可用於 Windows、Linux 和 macOS 的選項。

事件	備份來源 (要備份的內容)					
	整部電腦、磁碟/磁碟區或檔案/資料夾 (實體機器)	**整部電腦或磁碟/磁碟區 (虛擬機器)**	**ESXi 設定**	**Microsoft 365 信箱**	**Exchange 資料庫和信箱**	**SQL 資料庫**
自上次備份後的時間	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
當使用者登入系統時	Windows	不適用	不適用	不適用	不適用	不適用
當使用者登出系統時	Windows	不適用	不適用	不適用	不適用	不適用

事件	備份來源 (要備份的內容)					
	整部電腦、磁碟/磁碟區或檔案/資料夾 (實體機器)	整部電腦或磁碟/磁碟區 (虛擬機器)	ESXi 設定	Microsoft 365 信箱	Exchange 資料庫和信箱	SQL 資料庫
在系統啟動時	Windows, Linux, macOS	不適用	不適用	不適用	不適用	不適用
在系統關閉時	Windows	不適用	不適用	不適用	不適用	不適用
發生 Windows 事件記錄中的事件時	Windows	不適用	不適用	Windows	Windows	Windows

發生 Windows 事件記錄中的事件時

您可以在 Windows 事件記錄 (例如應用程式記錄檔、安全性記錄檔或系統記錄檔) 中記錄特定事件時，自動執行備份。

注意事項
您可以在 Windows 的 **[電腦管理]** > **[事件檢視器]** 中瀏覽事件並檢視其內容。若要開啟安全性記錄檔，您需要有系統管理員權限。

事件參數

下表摘要說明您在設定 **[發生 Windows 事件記錄中的事件時]** 選項時必須指定的參數。

參數	描述
記錄名稱	記錄名稱。 選擇標準記錄的名稱 (應用程式、安全性或系統)，或輸入其他記錄名稱。例如，Microsoft Office 工作階段。
事件來源	事件來源會指出導致該事件的程式或系統元件。例如，磁碟。 含有指定之文字字串的任何事件來源都將觸發排程備份。此選項不區分大小寫。因此，如果您指定 `service`，則 Service Control Manager 和 Time-Service 事件來源都將觸發備份。
事件類型	事件類型：錯誤、警告、資訊、稽核成功或稽核失敗。
事件識別碼	事件 ID 可識別事件來源內特定種類的事件。 例如，當 Windows 探索到磁碟上的一個磁區損壞時，會發生包

參數	描述
	含事件來源磁碟和事件 ID 7 的錯誤事件，而當磁碟尚未準備就緒進行存取時，則會發生包含事件來源磁碟和事件 ID 15 的錯誤事件。

範例：硬碟磁區損壞時緊急備份

硬碟上有一或多個磁區損壞可能代表硬碟即將故障。這就是您可能需要在偵測到磁區損壞時建立備份的原因。

當 Windows 在磁碟上偵測到一個損壞磁區時，將在系統記錄檔中記錄一個事件來源為磁碟，且事件編號為 7 的錯誤事件。在保護計劃中，設定下列排程：

- 排程：發生 Windows 事件記錄中的事件時
- 記錄名稱：系統
- 事件來源：磁碟
- 事件類型：錯誤
- 事件識別碼：7

重要事項
為確保備份在磁區損壞時仍能完成，請在 **[備份選項]** 中，移至 **[錯誤處理]**，然後選擇 **[忽略損壞的磁區]** 核取方塊。

開始條件

如果只能在符合特定條件時才執行備份，請設定一或多個開始條件。如果您設定多個條件，必須同時符合所有條件，備份才會開始。您可以指定一個期限，在該期限後，無論是否符合條件，都將執行備份。如需有關此備份選項的詳細資訊，請參閱 "工作開始條件" (第 438 頁)。

開始條件不適用於手動開始備份時。

下表列出在 Windows、Linux 和 macOS 下可用於不同資料的開始條件。

開始條件	備份來源 (要備份的內容)					
	整部電腦、磁碟/磁碟區或檔案/資料夾 (實體機器)	整部電腦或磁碟/磁碟區 (虛擬機器)	ESXi 設定	Microsoft 365 信箱	Exchange 資料庫和信箱	SQL 資料庫
使用者空閒時	Windows	不適用	不適用	不適用	不適用	不適用
備份位置的主機可用	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
使用者已登出	Windows	不適用	不適用	不適用	不適用	不適用

開始條件	備份來源 (要備份的內容)					
	整部電腦、磁碟/磁碟區或檔案/資料夾 (實體機器)	**整部電腦或磁碟/磁碟區 (虛擬機器)**	**ESXi 設定**	**Microsoft 365 信箱**	**Exchange 資料庫和信箱**	**SQL 資料庫**
符合時間間隔時	Windows, Linux, macOS	Windows, Linux	不適用	不適用	不適用	不適用
節省電池電力	Windows	不適用	不適用	不適用	不適用	不適用
不要在使用計量付費連線時開始	Windows	不適用	不適用	不適用	不適用	不適用
不要在連線至下列 Wi-Fi 網路時開始	Windows	不適用	不適用	不適用	不適用	不適用
檢查裝置 IP 位址	Windows	不適用	不適用	不適用	不適用	不適用

使用者空閒時

「使用者空閒時」表示螢幕保護程式正在電腦上執行或電腦處於鎖定狀態。

範例

每天晚上 09:00 執行備份，最好是在使用者閒置時。如果使用者到晚上 11:00 仍在作用中，則強制執行備份。

- 排程：**每天**，**每天執行**。啟動時間：**晚上 09:00**。
- 條件：**使用者空閒時**。
- 備份開始條件：**等到符合條件**，**強制在 2** 小時後開始工作。

結果：

- 如果使用者在晚上 09:00 之前閒置，備份將在晚上 09:00 開始。
- 如果使用者在晚上 09:00 到晚上 11:00 之間閒置，備份將立即開始。
- 如果使用者在晚上 11:00 仍在作用中，備份將在晚上 11:00 開始。

備份位置的主機可用

「備份位置的主機可用」的意思是，託管備份位置的電腦可透過網路使用。

此條件適用於網路資料夾、雲端儲存和儲存節點管理的位置。

此條件並不涵蓋位置本身的可用性 - 僅主機可用性。例如，如果主機可用，但該主機上的網路資料夾未共用或資料夾認證不再有效，則仍認為滿足該條件。

範例

您在每個工作日的晚上 09:00 執行備份至網路資料夾。如果此時裝載資料夾的電腦無法使用 (例如，由於維護工作)，則要跳過備份並等待下一個工作日的已排程啟動。

- 排程：**每天**，**星期一至星期五執行**。啟動時間：**晚上 09:00**。
- 條件：**備份位置的主機可用**。
- 備份開始條件：**略過排程備份**。

結果：

- 如果主機在晚上 09:00 可用，備份就會立即開始。
- 如果主機在晚上 09:00 無法使用，則備份會在下一個工作日 (如果主機在這一天的晚上 09:00 可用) 開始。
- 如果主機在工作日的晚上 09:00 永遠無法使用，則備份永遠不會開始。

使用者已登出

使用此開始條件延後備份，直到所有使用者都登出 Windows 電腦為止。

範例

您每個星期五晚上 08:00 執行備份，最好是在所有使用者都登出時。如果在晚上 11:00 仍有一個使用者處於登入狀態，則務必執行備份。

- 排程：**每週**，星期五。啟動時間：**晚上 08:00**。
- 條件：**使用者已登出**。
- 備份開始條件：**等到符合條件**，**強制在 3** 小時後開始備份。

結果：

- 如果所有使用者在晚上 08:00 都已登出，備份將在晚上 08:00 開始。
- 如果最後一個使用者在晚上 08:00 到晚上 11:00 之間登出，備份將立即開始。
- 如果晚上 11:00 仍有使用者處於登入狀態，備份將在晚上 11:00 開始。

符合時間間隔時

使用這個開始條件可將備份的開始時間限制在指定的時段。

範例

某家公司將使用者資料和伺服器備份到相同網路連接儲存裝置上的不同位置。

工作日從上午 08:00 開始到下午 05:00 結束。使用者資料應在使用者登出後立即備份，但不能早於下午 04:30。

公司伺服器的備份時間是每天晚上 11:00。最好在晚上 11:00 之前備份使用者資料，才能為伺服器釋放網路頻寬。

備份使用者資料所需時間不超過一小時，因此備份最晚開始時間為晚上 10:00。如果在指定的時段內有一個使用者仍處於登入狀態，或在任何其他時間登出，則不應跳過備份該使用者的資料。

- 事件：**當使用者登出系統時**。指定使用者帳戶：**任何使用者**。
- 條件：**符合時間間隔時**，從**下午 04:30** 至**晚上 10:00**。
- 備份開始條件：**略過排程備份**。

結果：

- 如果使用者在下午 04:30 到晚上 10:00 之間登出，備份工作將立即開始。
- 如果使用者在其他任何時間登出，將跳過備份。

節省電池電力

如果電腦 (筆記型電腦或平板電腦) 未連線到電源，使用此開始條件可防止進行備份。視 [備份開始條件] 選項的值而定，在電腦連線到電源之後，跳過的備份將會開始，也可能不會開始。

您可以選取下列選項：

- **不要在使用電池電力時開始**
  只有在電腦連線到電源時，備份才會開始。
- **如果電池電量高於下列設定，可在使用電池電力時開始**
  如果電腦連線到電源或電池電力高於指定的值，備份才會開始。

範例

您會在每個工作日晚上 09:00 備份資料。如果您的電腦未連線到電源，則您需要跳過備份，以節省電池電力並等到您將電腦連線到電源。

- 排程：**每天，星期一至星期五執行**。啟動時間：**晚上 09:00**。
- 條件：**節省電池電力，不要在使用電池電力時開始**。
- 備份開始條件：**等到符合條件**。

結果：

- 如果電腦在晚上 09:00 連線到電源，備份就會立即開始。
- 如果電腦在晚上 09:00 時使用電池電力運轉，則備份會在您將電腦連線到電源時開始。

不要在使用計量付費連線時開始

如果電腦透過在 Windows 中設定為使用計量付費的連線來連線至網際網路，使用這個開始條件可防止進行備份 (包括備份至本機磁碟)。如需 Windows 中使用計量付費連線的相關資訊，請參閱 https://support.microsoft.com/en-us/help/17452/windows-metered-internet-connections-faq。

當您啟用 **[不要在使用計量付費連線時開始]** 條件時，會自動啟用其他開始條件 **[不要在連線至下列 Wi-Fi 網路時開始]**。這是防止透過行動熱點進行備份的另一個方法。預設會指定下列網路名稱：android、phone、mobile 和 modem。

若要從清單中移除這些名稱，請按一下 X 符號。若要新增名稱，請在空的欄位中輸入該名稱。

範例

您會在每個工作日晚上 09:00 備份資料。如果電腦使用計量付費連線來連線至網際網路，則您需要跳過備份以節省網路流量並等待下一個工作日的排程開始。

- 排程：**每天，星期一至星期五執行**。啟動時間：**晚上 09:00**。
- 條件：**不要在使用計量付費連線時開始**。
- 備份開始條件：**略過排程備份**。

結果：

- 如果電腦在晚上 09:00 未透過計量付費連線來連線到網際網路，備份就會立即開始。
- 如果電腦在晚上 09:00 透過計量付費連線來連線到網際網路，則備份會在下一個工作日開始。
- 如果在工作日的晚上 09:00 時電腦一律透過計量付費連線來連線到網際網路，則備份永遠不會開始。

不要在連線至下列 Wi-Fi 網路時開始

如果電腦連線至任何指定的無線網路 (例如，如果您要透過行動電話熱點限制備份)，使用這個開始條件可防止進行備份 (包括備份至本機磁碟)。

您可以指定 Wi-Fi 網路名稱，也稱為服務組識別元 (SSID)。此限制適用於名稱中包含指定名稱作為子字串的所有網路，不區分大小寫。例如，如果您指定 phone 作為網路名稱，備份將不會在電腦連線至以下任何網路時開始：John's iPhone、phone_wifi 或 my_PHONE_wifi。

當您啟用 **[不要在使用計量付費連線時開始]** 條件時，會自動啟用開始條件 **[不要在連線至下列 Wi-Fi 網路時開始]**。預設會指定下列網路名稱：android、phone、mobile 和 modem。

若要從清單中移除這些名稱，請按一下 X 符號。若要新增名稱，請在空的欄位中輸入該名稱。

範例

您會在每個工作日晚上 09:00 備份資料。如果電腦透過行動熱點連線至網際網路，則您需要跳過備份，並等待下一個工作日的排程開始。

- 排程：**每天，星期一至星期五執行**。啟動時間：**晚上 09:00**。
- 條件：**不要在連線至下列網路時開始，網路名稱：**<熱點網路的 SSID>。
- 備份開始條件：**略過排程備份**。

結果：

- 如果電腦在晚上 09:00 未連線到指定的網路，備份就會立即開始。
- 如果電腦在晚上 09:00 連線到指定的網路，則備份會在下一個工作日開始。
- 如果在工作日的晚上 09:00 時電腦一律連線到指定的網路，則備份永遠不會開始。

檢查裝置 IP 位址

如果任何電腦 IP 位址在指定的 IP 位址範圍之內或之外，使用這個開始條件可以防止進行備份 (包括備份到本機磁碟)。因此，例如，您可以在備份海外使用者的電腦時避免大量資料傳輸費用，或者您可以防止透過虛擬私人網路 (VPN) 連線進行備份。

您可以選取下列選項：

- **在 IP 範圍之外時開始**
- **在 IP 範圍之內時開始**

使用任一選項，您可以指定數個範圍。僅支援 IPv4 位址。

範例

您會在每個工作日晚上 09:00 備份資料。如果電腦使用的是 VPN 通道連線至企業網路，則您需要跳過備份。

- 排程：**每天，星期一至星期五執行**。**晚上 09:00** 開始。
- 條件：**檢查裝置 IP 位址**、**在 IP 範圍之外時開始**、**寄件者**：<VPN IP 位址範圍的開頭>、**收件者**：<VPN IP 位址範圍的結尾>。
- 備份開始條件：**等到符合條件**。

結果：

- 如果晚上 09:00 時電腦 IP 位址未在指定的範圍內，則備份將立即開始。
- 如果晚上 09:00 時電腦 IP 位址在指定的範圍內，則備份會在電腦取得非 VPN IP 位址時開始。
- 如果在工作日的晚上 09:00 時電腦 IP 位址一律在指定的範圍內，則備份永遠不會開始。

其他排程選項

您可以將備份設定為僅在符合特定條件時執行、僅在指定的期間內執行，或者在比排程延遲時執行。

若要設定開始條件

1. 在保護計劃中，展開 **[備份]** 模組。
2. 按一下 **[排程]**。
3. 在 **[排程]** 窗格上，按一下 **[顯示更多]**。
4. 選擇您要包含的開始條件旁的核取方塊，然後按一下 **[完成]**。
   如需有關可用開始條件及其設定方式的詳細資訊，請參閱 "開始條件" (第 378 頁)。
5. 儲存保護計劃。

若要設定時間範圍

1. 在保護計劃中，展開 **[備份]** 模組。
2. 按一下 **[排程]**。
3. 選擇 **[在日期範圍內執行計劃]** 核取方塊。

4. 根據您的需求指定期間，然後按一下 **[完成]**。
5. 儲存保護計劃。

因此，備份將僅在指定的期間內執行。

若要設定延遲

為了避免在將多個工作負載備份到網路位置時網路負載過大，設定較小的隨機延遲作為備份選項。您可以停用此功能或變更其設定。

1. 在保護計劃中，展開 **[備份]** 模組。
2. 按一下 **[備份選項]**，然後選擇 **[排程]**。
   每個工作負載的延遲值是隨機選擇的，範圍介於零到您指定的最大值之間。根據預設，最大值是 30 分鐘。
   如需有關此備份選項的詳細資訊，請參閱 "排程" (第 436 頁)
   每個工作負載的延遲值是在將保護計劃套用至該工作負載時計算的，並會保留相同的值，直到您編輯最大延遲值為止。
3. 根據您的需求指定期間，然後按一下 **[完成]**。
4. 儲存保護計劃。

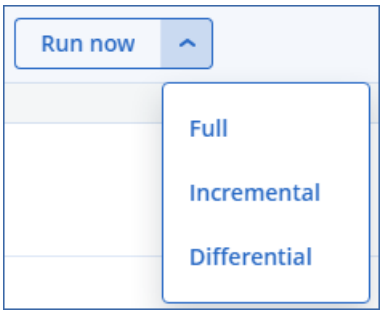
手動執行備份

您可以手動執行已排程和未排程的備份。

若要手動執行備份

1. 在 Cyber Protect 主控台中，移至 **[裝置]**。
2. 選擇您要執行備份的工作負載，然後按一下 **[保護]**。
3. 選擇您要建立備份的保護計劃。
   如果沒有保護計劃套用到工作負載，則會套用現有的計劃，或建立一個新計劃。
   如需有關如何建立保護計劃的詳細資訊，請參閱 "建立保護計劃" (第 192 頁)。
4. [建立預設備份類型] 在保護計劃中，按一下 **[立即執行]** 圖示。

   或者，在保護計劃中，展開 **[備份]** 模組，然後按一下 **[立即執行]** 按鈕。
5. [建立特定備份類型] 在保護計劃中，展開 **[備份]** 模組，按一下 **[立即執行]** 按鈕旁的箭頭，然後選擇備份類型。



注意事項
選擇類型不適用於僅使用一種備份方法的備份配置，例如，**[一律增量 (單一檔案)]** 或 **[一律完整備份]**。

因此，備份作業將會開始。您可以在 **[裝置]** 索引標籤的 **[狀態]** 欄中檢查其進度及其結果。

保留規則

若要自動刪除較舊的備份，請在保護計劃中設定備份保留規則。

您可以將保留規則當作以下任何備份屬性的基礎：

- 編號
- 存留期
- 大小

可用的保留規則及其選項視備份配置而定。這些規則也與代理程式、工作負載和雲端對雲端備份相關。如需詳細資訊，請參閱 "根據備份配置的保留規則" (第 386 頁)。

根據保護計劃的設定，保留規則會在備份之前或之後套用到存檔。

您可以在設定保留規則時選擇 **[無限期保留備份]** 選項來停用自動清理較舊的備份。這可能會導致增加儲存空間使用量，而且您必須手動刪除不需要的舊備份。

重要提示

- 保留規則是保護計劃的一部分。如果您撤銷或刪除某個計劃，將不會再套用該計劃中的保留規則。如需有關如何刪除您不再需要的備份的詳細資訊，請參閱 "刪除備份" (第 474 頁)。
- 如果根據備份配置和備份格式，將每個備份儲存為單獨檔案，則您無法刪除與其他增量或差異備份相依的備份。根據套用到相依備份的保留規則，將會刪除此備份。此設定可能會因為延後刪除部分備份而導致增加儲存空間使用量。此外，備份的存留期、數目或大小可能會超過您所指定的值。如需有關如何變更此行為的詳細資訊，請參閱 "備份合併" (第 399 頁)。
- 預設永遠不會刪除保護計劃所建立的最新備份。但是，如果您將保留規則設定為在開始新的備份作業之前清除備份，並將要保留的備份數目設為零，則最新的備份也將遭到刪除。

警告！
如果您將此保留規則套用至包含單一備份的備份集，而且備份作業失敗，則您將無法復原資料，因為在建立新的備份之前，現有的備份將遭到刪除。

根據備份配置的保留規則

可用的保留規則及其設定視您在保護計劃中使用的備份配置而定。如需有關備份配置的詳細資訊，請參閱 "備份配置" (第 371 頁)。

下表摘要說明可用的保留規則及其設定。

備份配置	排程	可用的保留規則及設定
一律增量 (單一檔案)	每月 每週 每天 每小時 事件觸發的備份	按照備份數目 按照備份存留期 (每月、每週、每日和每小時備份的個別設定) 無限期保留備份
始終完整備份	每月 每週 每天 每小時 事件觸發的備份	按照備份數目 按照備份存留期 (每月、每週、每日和每小時備份的個別設定) 依備份大小總計 無限期保留備份
每週完整備份，每日增量備份	每天 事件觸發的備份	按照備份數目 按照備份存留期 (每週和每日備份的個別設定) 依備份大小總計 無限期保留備份
每月完整備份、每週差異備份、每日增量備份	每月 每週 每天 每小時 事件觸發的備份	按照備份數目 按照備份存留期 (完整、差異和增量備份的個別設定) 依備份大小總計 無限期保留備份
自訂	每月 每週 每天 每小時 事件觸發的備份	按照備份數目 按照備份存留期 (完整、差異和增量備份的個別設定) 依備份大小總計 無限期保留備份

為什麼有包含每小時配置的每月備份?

根據備份配置,您可以針對下列其中一個備份,設定 **[按照備份存留期]** 選項:

- 每月、每週、每日和每小時備份。

  這些設定適用於所有非自訂備份配置,而且是以時間為基礎。即使您將備份設定為每小時執行,也可以使用所有這些備份 (每月、每週、每日和每小時)。請參閱以下範例。

備份	描述
每月	每月備份是每個月的第一個備份。
每週	每週備份是在 [每週備份] 選項中指定的星期幾的第一個備份。就保留規則而言,這一天被視為一週的開始。 如果每週備份也是當月的第一個備份,則此備份會被視為每月備份。在此情況下,每週備份將會在隔週選定的那一天建立。
每天	除非此備份落在每月或每週備份的定義範圍內,否則每日備份是當天的第一個備份。在此情況下,每日備份將會在隔天建立。
每小時	除非此備份落在每月、每週或每日備份的定義範圍內,否則每小時備份是該小時的第一個備份。在此情況下,每小時備份將會在下一小時建立。

- 完整、差異和增量備份。

  這些設定適用於 **[自訂]** 備份配置,而且是以備份方法為基礎。**[每月完整備份、每週差異備份、每日增量備份]** 是預先設定的自訂配置。

範例

對於每小時備份,您要使用具有預設設定的 **[一律增量 (單一檔案)]** 備份配置:

- 依時間排程。
- 每小時執行備份:星期一至星期五上午 08:00 至下午 06:00,每小時備份一次。
- **[每週備份]** 選項設定為 [星期一]。

在保護計劃的 **[保留時間]** 區段中,您可以將保留規則套用至每月、每週、每日和每小時備份。

下表摘要說明在 8 天期間內建立的備份類型。

日期	一週中的日期	描述
7 月 1 日	星期一	每個月的第一個備份是每月備份,因此今天的第一個備份是每月備份。當天內的其他備份則是每小時備份。 本週的第一個備份會被視為每月備份。這就是為什麼沒有每週備份的原因。下週的第一個備份將是每週備份。
7 月 2 日	星期二	第一個備份是每日備份,當天內的其他備份則是每小時備份。

日期	一週中的日期	描述
7 月 3 日	星期三	第一個備份是每日備份，當天內的其他備份則是每小時備份。
7 月 4 日	星期四	第一個備份是每日備份，當天內的其他備份則是每小時備份。
7 月 5 日	週五	第一個備份是每日備份，當天內的其他備份則是每小時備份。
7 月 6 日	星期六	第一個備份是每日備份，當天內的其他備份則是每小時備份。
7 月 7 日	星期日	第一個備份是每日備份，當天內的其他備份則是每小時備份。
7 月 8 日	星期一	第一個備份是每週備份，當天內的其他備份則是每小時備份。

設定保留規則

保留規則是保護計劃的一部分，其可用性和選項取決於備份配置。如需詳細資訊，請參閱 "根據備份配置的保留規則" (第 386 頁)。

若要設定保留規則

1. 在保護計劃中，展開 **[備份]** 模組。
2. 按一下 **[保留的數量]**。
3. 選擇以下選項之一：
   - **按照備份數目**
   - **按照備份存留期**

     每月、每週、每日和每小時備份的個別設定可供使用。所有類型的最大值都是 9999。

     您也可以為所有備份使用單一設定。
   - **按照備份大小總計**

     此設定不適用於 **[一律增量 (單一檔案)]** 備份配置。
   - **無限期保留備份**
4. [如果您未選擇 **[無限期保留備份]**] 針對所選選項設定值。
5. [如果您未選擇 **[無限期保留備份]**] 選擇套用保留規則的時機：
   - 備份後
   - 備份前

     此選項不適用於備份 Microsoft SQL Server 叢集或 Microsoft Exchange Server 叢集時。
6. 按一下 **[完成]**。
7. 儲存保護計劃。

複寫

透過複寫，每個新備份都會自動複製到複寫位置。複寫位置中的備份不相依於來源位置中的備份，反之亦然。

系統只會複寫來源位置中的最後一個備份。不過，如果未複寫較早的備份 (例如，因為網路連線問題)，則複寫作業將包含上次成功複寫後建立的所有備份。

如果複寫作業遭到中斷，下次複寫作業將會使用處理過的資料。

注意事項

本主題描述保護計劃中的複寫。您也可以建立單獨的備份複寫計劃。如需詳細資訊，請參閱 "備份複寫" (第 198 頁)。

使用範例

- 確保可靠的復原

  使用現場 (適合立即復原) 與異地 (即使發生儲存裝置故障或影響主要位置的自然災害，也能保證備份安全無虞) 方式儲存您的備份。
- 使用雲端存放區保護資料免受自然災難影響

  僅傳輸資料變更，將備份複寫到雲端存放區。
- 僅保留最新的復原點

  設定保留規則刪除高速儲存裝置中較舊的備份，以節省儲存裝置成本。

支援的位置

位置	作為來源位置	作為複寫位置
本機資料夾	+	+
網路資料夾	+	+
雲端儲存	-	+
Secure Zone	+	+
公有雲端	- *	+

*從公有雲端複寫僅適用於離線主機資料處理計劃。請參閱 "支援的離線主機資料處理位置" (第 200 頁)。

若要啟用複寫

1. 在保護計劃中，展開 **[備份]** 模組，然後按一下 **[新增位置]**。

   注意事項

   當您在 **[備份目標位置]** 中選擇雲端儲存空間時，無法使用 **[新增位置]** 選項。

2. 從可用位置的清單，選擇複寫位置。

   根據您針對複寫新增的位置數目，此位置在保護計劃中會顯示為 **[第 2 個位置]**、**[第 3 個位置]**、**[第 4 個位置]** 或 **[第 5 個位置]**。
3. [選用] 按一下齒輪圖示，設定複寫位置的選項。
   - **[效能和備份時窗]** – 設定所選位置的備份視窗，如 "效能和備份時窗" (第 428 頁) 中所述。這些設定會定義複寫效能。
   - **[移除位置]** - 刪除目前選定的複寫位置。

- [僅適用於雲端儲存] **實體資料運送** – 將初始備份儲存在卸除式儲存裝置上，然後將其上傳到雲端儲存，而非透過網際網路複寫。

  此選項適合網路連線慢的位置，或是您想要透過網路節省大檔案傳輸頻寬的情況。啟用此選項並不需要進階 Cyber Protect 服務配額，但是您需要有實體資料運送服務配額，才能建立裝貨單並進行追蹤。請參閱 "實體資料運送" (第 432 頁)。

  注意事項
  保護代理程式 C21.06 版或更新版本支援此選項。

4. [選用] 在複寫位置下的 **[保留的數量]** 中，設定該位置的保留規則，如 "保留規則" (第 385 頁) 中所述。
5. [選用] 重複步驟 1 – 4 以新增其他複寫位置。

   您最多可以設定四個複寫位置 (**第 2 個位置**、**第 3 個位置**、**第 4 個位置**和**第 5 個位置**)。如果您選擇 **[雲端儲存]**，則無法新增其他複寫位置。

重要事項
如果在同一個保護計劃中啟用備份和複寫，請確認在下一次計劃備份之前完成複寫。如果複寫仍在進行中，排程的備份將無法開始；例如，如果複寫需要 26 小時完成，則每 24 小時執行一次的排程備份將不會開始。

為了避免這樣的相依性，請使用單獨的備份複寫計劃。如需有關此特定計劃的詳細資訊，請參閱 "備份複寫" (第 198 頁)。

加密

進階加密標準 (AES) 加密演算法可在 Galois/Counter 模式 (GCM) 下運作，並使用隨機產生的 256 位元金鑰。接著，使用密碼的 SHA-2 (256 位元) 雜湊作為金鑰，透過 AES-256 演算法對加密金鑰進行加密。密碼本身不會儲存在磁碟或備份中的任何位置，而且密碼雜湊用於驗證。

有了這兩層安全保護，備份資料即可免於未經授權的存取，但是無法復原遺失的密碼。

注意事項
搭配高強度密碼使用 AES-256 演算法可提供抵抗量子加密。它可以安全地抵禦與量子運算相關的密碼分析攻擊。

建議您將所有儲存在雲端儲存的備份加密，特別是如果您的公司須遵循法規約的情況下。

您可以透過以下方式設定加密：

- 在保護計劃中
- 當作電腦屬性，使用 Cyber Protect Monitor或命令列介面

在保護計劃中設定加密

在保護計劃中，預設啟用加密。使用 AES-256 演算法。

透過高強度密碼，AES-256 演算法可提供抗量子加密。

對於合規模式下的帳戶，您無法在保護計劃中設定加密。如需有關如何在受保護裝置上設定加密的詳細資訊，請參閱 "將加密設定為電腦屬性" (第 391 頁)。

若要設定加密

1. 在保護計劃中，展開 **[備份]** 模組。
2. 在 **[加密]** 中，按一下 **[指定密碼]**。
3. 指定並確認加密密碼。
4. 按一下 **[確定]**。

警告！
若是遺失或忘記密碼，則無法復原加密的備份。

您無法在套用保護計劃後變更加密設定。若要使用不同的加密設定，請建立新的計劃。

將加密設定為電腦屬性

您可以將備份加密設定為電腦屬性。在此情況下，備份加密不是在保護計劃中設定的，而是在受保護的工作負載上設定的。當作電腦屬性的加密使用具有 256 位元金鑰 (AES-256) 的 AES 演算法。

注意事項
搭配高強度密碼使用 AES-256 演算法可提供抵抗量子加密。它可以安全地抵禦與量子運算相關的密碼分析攻擊。

將加密設定為電腦屬性會以下列方式影響保護計劃：

- **已套用至電腦的保護計劃。**如果保護計劃中的加密設定各不相同，備份便會失敗。
- **之後套用至電腦的保護計劃。**電腦上儲存的加密設定將會覆寫保護計劃中的加密設定。即使在 [備份] 模組設定中停用加密，所有備份仍會經過加密。

對於合規模式下的帳戶，只能使用當作電腦屬性的加密。

如果您有多個連線到相同 vCenter Server 的 VMware 用代理程式，而且您將加密設定為電腦屬性，則基於代理程式間的負載平衡，您必須在具有 VMware 用代理程式的所有電腦上使用相同的加密密碼。

您可以透過以下方式，將加密設定為電腦屬性：

- 在命令列上
- 在 Cyber Protect Monitor上 (適用於 Windows 和 macOS)

若要設定加密

在命令列上

1. 以系統管理員身分 (Windows) 或以 root 使用者身分 (Linux) 登入。
2. 在命令列上，執行下列命令：

- 對於 Windows:

  ```
  <installation_path>\PyShell\bin\acropsh.exe -m manage_creds --set-password
  <encryption_password>
  ```

  根據預設，安裝路徑為 `%ProgramFiles%\BackupClient`。
- 對於 Linux:

  ```
  /usr/sbin/acropsh -m manage_creds --set-password <encryption_password>
  ```

- 若是虛擬裝置:

  ```
   /./sbin/acropsh -m manage_creds --set-password <encryption_password>
  ```

警告！
若是遺失或忘記密碼，則無法復原加密的備份。

在 Cyber Protect Monitor 中

1. 以系統管理員身分登入。
2. 按一下通知區域 (Windows) 或功能表列 (macOS) 中的 [Cyber Protect Monitor] 圖示。
3. 按一下齒輪圖示，然後按一下 **[設定]** > **[加密]**。
4. 選擇 **[為此電腦設定密碼]**。指定並確認加密密碼。
5. 按一下 **[儲存]**。

警告！
若是遺失或忘記密碼，則無法復原加密的備份。

若要重設加密設定

1. 以系統管理員身分 (Windows) 或以 root 使用者身分 (Linux) 登入。
2. 在命令列上，執行下列命令:
   - 對於 Windows:

     ```
     <installation_path>\PyShell\bin\acropsh.exe -m manage_creds --reset
     ```

     根據預設，安裝路徑為 `%ProgramFiles%\BackupClient`。
   - 對於 Linux:

     ```
     /usr/sbin/acropsh -m manage_creds --reset
     ```

   - 若是虛擬裝置:

     ```
     /./sbin/acropsh -m manage_creds --reset
     ```

重要事項
如果您在保護計劃建立備份後重設加密作為電腦屬性，或變更加密密碼，下次備份作業將會失敗。若要繼續備份工作負載，請建立新的保護計劃。

公證

注意事項
此功能適用於 Advanced Backup 套件。

公證讓您證明檔案在備份後即是真實和未變更的。建議您在備份法律檔案或需要證明真實性的任何其他檔案時啟用公證。

公證僅適用於檔案層級備份。具有數位簽章的檔案無需公證，因此將其略過。

在下列狀況下，公證不可用：

- 若備份格式設定為 **11 版**
- 若備份目的地為 Secure Zone

如何使用公證

若要對選定備份的所有檔案啟用公證 (具有數位簽章的檔案除外)，建立保護計劃時請啟用 **[公證]** 開關。

在設定復原時，公證檔將標記有特殊圖示，並且您可以 [驗證檔案真實性]。

運作原理

在備份過程中，代理程式會計算備份檔案的雜湊代碼，組建雜湊樹狀結構 (基於資料夾結構)，儲存備份中的樹狀結構，然後將雜湊樹狀結構根部發送給公證服務。公證服務將雜湊樹狀結構根部儲存在 Ethereum 區塊鏈資料庫中，以確保此值不會變更。

在驗證檔案真實性時，代理程式會計算檔案雜湊，然後將其與儲存在備份內雜湊樹狀結構中的雜湊相比較。若這些雜湊不相符，則檔案被視為不真實。否則，由雜湊樹狀結構保證檔案的真實性。

若要驗證雜湊樹狀結構自身未受損，代理程式會將雜湊樹狀結構根部發送給公證服務。公證服務將其與儲存在區塊鏈資料庫中的雜湊相比較。若雜湊相符，則所選檔案保證為真實的。否則，軟體會顯示一則訊息，指示檔案不真實。

預設備份選項

備份選項的預設值存在於公司、單位和使用者層級。在公司或單位內建立單位或使用者帳戶時，它會繼承針對公司或針對單位設定的預設值。

公司系統管理員、單位系統管理員，以及沒有系統管理員權限的每個使用者，都可以針對預先定義的選項，變更預設選項值。依預設，新值將用於變更生效後在個別層級建立的所有保護計劃中。

建立保護計劃時，使用者可以使用僅專用於此計劃的自訂值，來覆寫預設值。

若要變更預設選項值

1. 執行下列其中一項操作：
   - 若要變更公司的預設值，請以公司系統管理員身分登入 Cyber Protect 主控台。
   - 若要變更單位的預設值，請以單位系統管理員身分登入 Cyber Protect 主控台。
   - 若要變更您自己的預設值，請使用不含系統管理員權限的帳戶，登入 Cyber Protect 主控台。
2. 按一下 **[設定]** > **[系統設定]**。
3. 展開 **[預設備份選項]** 區段。
4. 選擇該選項，然後進行必要的變更。
5. 按一下 **[儲存]**。

備份選項

若要修改保護計劃的備份選項，請在 **[備份]** 模組的 **[備份選項]** 欄位中，按一下 **[變更]**。

備份選項的可用性

可用的備份選項集取決於：

- 代理程式作業的環境(Windows、Linux、macOS) 。
- 備份的資料類型 (磁碟、檔案、虛擬機器、應用程式資料)。
- 備份目的地 (雲端儲存、本機或網路資料夾)

下表摘述備份選項的可用性。

	磁碟層級備份			**檔案層級備份**			**虛擬機器**				**SQL 與 Exchange**
	Windows	**Linux**	**macOS**	**Windows**	**Linux**	**macOS**	**ESXi**	**Hyper-V**	**Virtuozzo**	**Azure**	**Windows**
警示	+	+	+	+	+	+	+	+	+	-	+
Azure 還原點：保留	-	-	-	-	-	-	-	-	-	+	-
Azure 還原點：一致性層級	-	-	-	-	-	-	-	-	-	+	-
Azure 還原點：處	-	-	-	-	-	-	-	-	-	+	-

理不支援的磁碟											
備份合併	+	+	+	+	+	+	+	+	+	-	-
備份檔案名稱	+	+	+	+	+	+	+	+	+	+	+
備份格式	+	+	+	+	+	+	+	+	+	-	+
備份驗證	+	+	+	+	+	+	+	+	+	-	+
變更區塊追蹤 (CBT)	+	-	-	-	-	-	+	+	-	-	-
叢集備份模式	-	-	-	-	-	-	-	-	-	-	+
壓縮層級	+	+	+	+	+	+	+	+	+	+	+
錯誤處理											
發生錯誤時重新嘗試	+	+	+	+	+	+	+	+	+	+	+
處理時不顯示訊息和對話方塊 (無訊息模式)	+	+	+	+	+	+	+	+	+	+	+
忽略損壞的磁區	+	-	+	+	-	+	+	+	+	+	-
若建立 VM 快照期間發生錯誤，會重新嘗試	-	-	-	-	-	-	+	+	+	+	-

快速增量/差異備份	+	+	+	-	-	-	-	-	-	-	-
檔案層級備份快照	-	-	-	+	+	+	-	-	-	-	-
檔案篩選器	+	+	+	+	+	+	+	+	+	+	-
鑑識資料	+	-	-	-	-	-	-	-	-	-	-
記錄截斷	-	-	-	-	-	-	+	+	-	-	僅 SQL
LVM 快照	-	+	-	-	-	-	-	-	-	-	-
掛載點	-	-	-	+	-	-	-	-	-	-	-
多重分割檔快照	+	+	-	+	+	-	-	-	-	-	-
單鍵復原	+	+	-	-	-	-	-	-	-	-	-
效能和備份時窗	+	+	+	+	+	+	+	+	+	-	+
實體資料運送	+	+	+	+	+	+	+	+	+	-	-
事前/事後命令	+	+	+	+	+	+	+	+	+	-	+
資料擷取前/後命令	+	+	+	+	+	+	-	-	-	-	+
排程											
在時間視窗內分配開始時間	+	+	+	+	+	+	+	+	+	-	+
限制同	-	-	-	-	-	-	+	+	+	-	-

時執行備份的數目											
逐一磁區備份	+	+	-	-	-	-	+	+	+	+	-
分割	+	+	+	+	+	+	+	+	+	-	+
工作失敗處理	+	+	+	+	+	+	+	+	+	-	+
工作開始條件	+	+	-	+	+	-	+	+	+	-	+
磁碟區陰影複製服務 (VSS)	+	-	-	+	-	-	-	+	-	-	+
虛擬機器的磁碟區陰影複製服務 (VSS)	-	-	-	-	-	-	+	+	-	-	-
每週備份	+	+	+	+	+	+	+	+	+	+	+
Windows 事件日誌	+	-	-	+	-	-	+	+	-	-	+

警示

連續數天未成功的備份已達指定的數量

預設為：**[已停用]**。

此選項可決定當保護計劃在指定時限內未成功執行備份時是否產生警示。除備份失敗外，軟體會對依排程未執行的備份（遺漏備份）進行計數。

警示以每部電腦為單位產生並顯示在 **[警示]**索引標籤上。

您可指定不進行備份的連續天數，這段時間過後便會產生警示。

Azure 還原點

設定 Microsoft Azure 虛擬機器的無代理備份時，有三種 Microsoft Azure 備份選項可用：

- Azure 還原點：保留
- Azure 還原點：一致性層級
- Azure 還原點：處理不支援的磁碟

Azure 還原點：保留

此選項可讓您定義備份後要保留多少 Microsoft Azure 還原點 (預設值為 3)。這些還原點可提升使用 Changed Block Tracking (CBT) 功能的增量備份效能。

您可以保留的 Azure 還原點數量上限為 200 (Microsoft 建議)，且每部虛擬機器僅能建立一個還原點集合。

從 Microsoft Azure 中仍有對應 Microsoft Azure 還原點的備份中，對原始 Microsoft Azure 虛擬機器執行復原時，復原程序會使用此還原點自動還原虛擬機器狀態，而非從備份檔案擷取資料。這有助於最佳化復原的流量和效能。

請注意，還原點輪換邏輯由保護計劃管理。如果有兩個計劃已套用到相同的虛擬機器，則每個計劃都會將集合內的所有還原點視為自己的還原點，並根據已定義的 **[還原點]** 值輪換備份。

Azure 還原點：一致性層級

這可讓您選擇還原點的一致性層級，例如應用程式一致的還原點或檔案系統一致的還原點。

注意事項
此選項僅適用於已開啟電源的虛擬機器。

您可以選擇下列其中一項：

- **需要應用程式一致的還原點**：如果還原點與應用程式不一致，備份將會失敗。
  請注意，虛擬機器還原點支援執行 Windows 作業系統的虛擬機器的應用程式一致性，並支援執行 Linux 作業系統的虛擬機器的檔案系統一致性。應用程式一致的還原點使用 VSS 編寫器 (或 Linux 的預先/後續指令碼) 來確保建立還原點之前應用程式資料的一致性。
- **對檔案系統或當機一致的還原點發出警告**：如果還原點是檔案系統一致或當機一致，則備份完成時會發出警告。
  如果快照一致性層級為檔案系統一致和低於 (當機一致) 時，此選項會將警告新增至記錄，並將活動標示為警告。
- **對當機一致的還原點發出警告**：如果還原點是當機一致的，則備份完成時會發出警告。檔案系統一致和應用程式一致的還原點不會觸發警告。預設會選擇此選項。
  此選項會將警告新增至記錄，並將活動標示為警告。
- **忽略一致性層級**：無論還原點的一致性層級為何，備份都會成功完成。
  此選項會將資訊訊息新增至記錄，並成功執行保護計劃。

Azure 還原點：處理不支援的磁碟

此選項可讓您決定在備份具有未受管理、共用或暫時性磁碟的虛擬機器時要執行的操作。請注意，這些類型的磁碟在 Microsoft Azure 還原點中不受支援，且無法在無代理程式模式下進行備份。若要備份這些磁碟上的資料，請在虛擬機器的客體作業系統中安裝保護代理程式。

您可以選擇下列其中一項：

- **忽略不支援的磁碟**：備份成功完成，並略過不支援的磁碟。
- **對不支援的磁碟發出警告**：備份完成時會發出不支援磁碟的警告。預設會選擇此選項。
- **在不支援的磁碟上失敗**：如果正在備份具有不受支援磁碟的虛擬機器，則備份會失敗。

備份合併

此選項定義了在清除期間是否要合併備份，或者刪除整個備份鏈。

預設為：**[已停用]**。

「合併」是將兩個以上的後續備份合併成單一備份的程序。

若啟用此選項，則應該在清理期間刪除的備份就會與下一個依存備份 (增量備份或差異備份) 合併。

否則，在可以刪除所有依存備份之前，都會保留該備份。這能協助您避免進行可能的耗時合併，但需要額外的空間來儲存延遲刪除的備份。備份時間或數目可以超過保留規則中指定的數值。

重要事項
請注意，合併只是刪除的一種方法，而不是替代刪除的方法。生成的備份將不包含在已刪除備份中存在的資料，也不包含在增量或差異備份中不存在的資料。

如果以下任何一項為真，則此選項*將不*生效：

- 備份目的地為雲端儲存。
- 備份配置設定為**一律增量 (單一檔案)**。
- 備份格式設定為**12 版**。

儲存在雲端儲存內的備份以及單一檔案備份 (11 和 12 版格式)，都一律會合併，因為其內部結構可以快速、輕鬆地合併。

不過，如果使用的是 12 版，而且出現多個備份鏈 (每個鏈儲存在個別的 .tibx 檔案中) 的話，則只會在最後一個鏈中合併。除了第一個鏈會縮減至最小大小以保存中繼資訊 (~12 KB) 以外，其他所有鏈都會整個刪除。此中繼資訊是必要的，才能確保同時讀取及寫入作業時的資料一致性。當套用保留規則之後，這些鏈中包含的備份會從 GUI 消失，不過實際上仍存在，直到整個鏈刪除為止。

在其他所有情況下，延遲刪除的備份會在 GUI 中標示垃圾桶圖示 ( )。如果您透過按一下 X 符號來刪除這類備份，則會執行合併。

備份檔案名稱

此選項會定義保護計劃或雲端應用程式備份計劃所建立之備份檔案的名稱。

若是保護計劃所建立的備份檔案，您可以在瀏覽備份位置時，在檔案管理員中看到這些名稱。

什麼是備份檔案？

根據所使用的備份配置以及備份格式而定，每個保護計劃都會在備份位置上建立一或多個檔案。以下表格會列出可依機器或信箱建立的檔案的清單。

	一律增量 (單一檔案)	其他備份配置
版本 11 備份格式	一個 TIB 檔案與一個 XML 中繼資料檔案	多個 TIB 檔案與一個 XML 中繼資料檔案
12 版備份格式	每個備份鏈一個 TIBX 檔案 (完整或差異備份，以及所有相依的增量備份)。如果本機或網路 (SMB) 資料夾中儲存之檔案的大小超過 200 GB，則預設會將檔案分割為 200 GB 的檔案。	

所有檔案都有相同的名稱，可包含或不含時間戳記或序號。您可以在建立或編輯保護計劃或雲端應用程式備份計劃時，定義此名稱 (也就是備份檔案名稱)。

注意事項
只有在採用 11 版備份格式時，才會將時間戳記加入至備份檔案名稱。

如果您變更保護計劃或雲端應用程式備份計劃中的備份檔案名稱，下一個備份將是完整備份。

如果您指定的是相同電腦上現有備份的檔案名稱，將會根據計劃排程，建立完整、增量或差異備份。

注意事項
如果您從其原始儲存空間移動備份檔案 (.tibx)，請不要為其重新命名。重新命名的檔案將顯示為已損毀，而且您將無法從其中復原資料。

您可以針對檔案管理員無法瀏覽的位置，設定備份檔案名稱 (例如，雲端儲存)。在此情況下，您將會在 **[備份儲存]** 索引標籤上看到自訂名稱。

我可以在哪裡看到備份檔案名稱?

對於保護計劃，請在 **[備份儲存]** 索引標籤上選擇位置，然後選擇備份存檔。

- 預設備份檔案名稱即會顯示在 **[詳細資料]** 窗格上。
- 如果您設定非預設備份檔案名稱，它將直接顯示在 **[備份儲存]** 索引標籤的 **[名稱]** 欄中。

對於雲端應用程式備份計劃，請在 **[備份儲存]** 索引標籤上選擇位置，選擇備份存檔，然後按一下齒輪圖示。

備份檔案名稱的限制

- 備份檔案名稱結尾不得為數字。
  在預設備份檔案名稱中，為防止名稱結尾是數字，會附加一個字母 "A"。建立自訂名稱時，請一律確定它的結尾不是數字。使用變數時，由於變數結尾可能是數字，因此名稱結尾不得是變數。
- 備份檔案名稱不能包含下列符號：**()&?*$<>":\|/#**、行尾結束符號 (**\n**) 和 Tab 符號 (**\t**)。

注意事項
選擇使用者易記的備份檔案名稱。這將有助於您在使用檔案管理員瀏覽備份位置時輕鬆識別備份。

預設備份檔案名稱

整個實體和虛擬機器、磁碟/磁碟區、檔案/資料夾、Microsoft SQL Server 資料庫、Microsoft Exchange Server 資料庫，以及 ESXi 設定之備份的預設備份檔案名稱為 [Machine Name]-[Plan ID]-[Unique ID]A。

本機 Microsoft 365 用代理程式所建立之 Exchange 信箱備份和 Microsoft 365 信箱備份的預設名稱為 [Mailbox ID]_mailbox_[Plan ID]A。

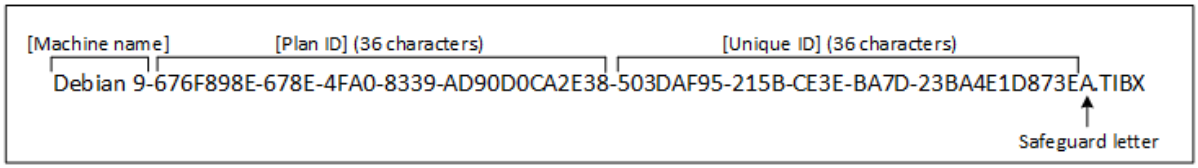
Microsoft Azure 備份的預設名稱首碼為 [Mailbox ID]_。您無法移除此首碼。

雲端代理程式所建立之雲端應用程式備份的預設名稱為 [Resource Name]_[Resource Type]_[Resource Id]_[Plan Id]A。

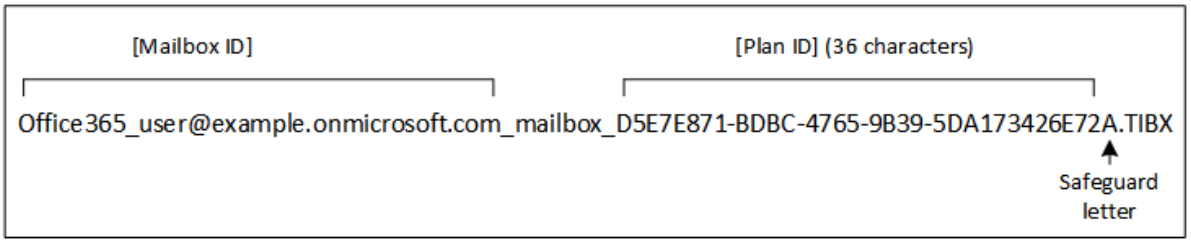
預設名稱包含下列變數：

- [Machine Name] 此變數會取代為電腦的名稱 (與 Cyber Protect 主控台中顯示的名稱相同)。
- [Plan ID], [Plan Id] 這些變數會取代為保護計劃的唯一識別碼。重新命名計劃時，此值不會變更。
- [Unique ID] 此變數會取代為所選電腦的唯一識別碼。重新命名電腦時，此值不會變更。
- [Mailbox ID] 此變數會取代為信箱使用者的主要名稱 (UPN)。
- [Resource Name] 此變數會取代為雲端資料來源名稱，例如使用者的主要名稱 (UPN)、SharePoint 網站 URL 或共用磁碟機名稱。
- [Resource Type] 此變數會取代為雲端資料來源類型，例如 mailbox、O365Mailbox、O365PublicFolder、OneDrive、SharePoint、GDrive。
- [Resource ID] 此變數會取代為雲端資料來源的唯一識別碼。重新命名雲端資料來源時，此值不會變更。
- "A" 是保護字母，附加該字母可避免名稱結尾是數字。

下圖顯示預設備份檔案名稱。



下圖顯示本機代理程式所執行之 Microsoft 365 信箱備份的預設備份檔案名稱。



沒有變數的名稱

如果您將備份檔案名稱變更為 MyBackup，則備份檔案將類似於以下範例。這些範例假設每日增量備份排程於 14:40，並且從 2016 年 9 月 13 日開始。

對於具有 **[一律增量 (單一檔案)]** 備份配置的 12 版格式：

```
MyBackup.tibx
```

對於具有其他備份配置的 12 版格式：

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

使用變數

除了預設使用的變數之外，您還可以使用下列變數：

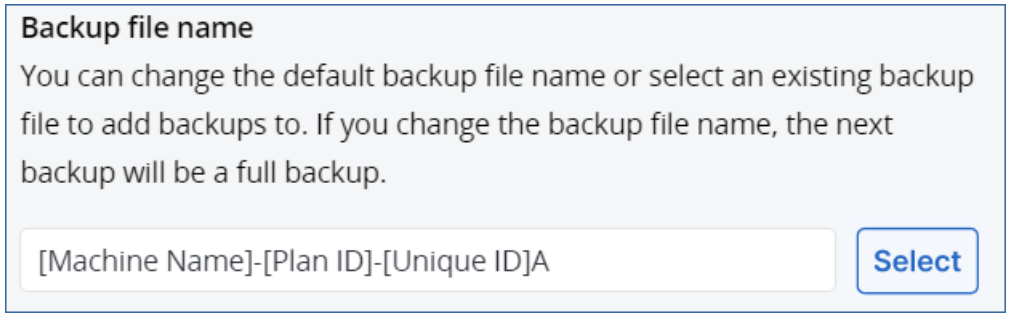
- [Plan name] 變數，這會取代為保護計劃的名稱。
- [Virtualization Server Type] 變數，這會取代為 "vmwesx" (如果虛擬機器透過 VMware 用代理程式備份) 或 "mshyperv" (如果虛擬機器透過 Hyper-V 用代理程式備份)。

如果選擇多個電腦或信箱進行備份，則備份檔案名稱必須包含 [Machine Name]、[Unique ID]、[Mailbox ID]、[Resource Name] 或 [Resource Id] 變數。

在現有的備份存檔中建立備份

您可以設定要新增至現有備份存檔的工作負載的備份。

此選項可能很實用，例如，當保護計劃套用至單一電腦，而且您必須從 Cyber Protect 主控台移除此電腦，或解除安裝代理程式及其組態設定。再次新增電腦或重新安裝代理程式後，您可以強制保護計劃繼續備份到原始存檔。



若要設定要新增至現有備份存檔的工作負載的備份

非雲端對雲端工作負載

1. 在 **[所有裝置]** 畫面上，按一下工作負載，然後按一下 **[保護]**。
2. 在保護計劃設定中，展開 **[備份]** 模組。
3. 按一下 **[備份選項]**，然後按一下 **[變更]**。
4. 在 **[備份檔案名稱]** 索引標籤上，按一下 **[選擇]**。

   [選擇] 按鈕會將備份顯示在保護計劃的 **[備份目標位置]** 區段中選擇的位置。

   注意事項
   [選擇] 按鈕僅適用於針對單一工作負載建立並套用到單一工作負載的保護計劃。

5. 選擇存檔，然後按一下 **[完成]**。
6. 按一下 **[完成]**，然後按一下 **[套用]**。

雲端對雲端工作負載

1. 在 **[管理]** > **[雲端應用程式備份]** 索引標籤上，選擇計劃。
2. 按一下 **[編輯]**，然後按一下計劃名稱旁邊的齒輪圖示。
3. 在 **[檔案備份名稱]** 索引標籤上，按一下 **[選擇]**。

   注意事項
   [選擇] 按鈕僅適用於針對單一工作負載建立並套用到單一工作負載的備份計劃。

4. 選擇備份存檔，然後按一下 **[完成]**。
5. 按一下 **[完成]**，然後按一下 **[儲存變更]**。

備份格式

[備份格式] 選項會定義保護計劃所建立之備份的格式。此選項僅適用於已使用 11 版備份格式的保護計劃。若是如此，您可以將備份格式變更為 12 版。將備份格式切換到 12 版之後，選項將變成無法使用。

- **11 版**

  為回溯相容性而保留的舊版格式。

  注意事項
  您無法使用 11 版的備份格式，備份資料庫可用性群組 (DAG)。只有 12 版格式支援備份 DAG。

- **12 版**

  Acronis Backup 12 中推出的備份格式，備份和復原速度更快。每一個備份鏈 (完整或差異備份，以及與之相依的所有增量備份) 都會儲存至單一 TIBX 檔案。

備份格式和備份檔案

對於可以使用檔案管理員瀏覽的備份位置 (例如本機或網路資料夾)，備份格式會判定檔案數目及其副檔名。以下表格會列出可依機器或信箱建立的檔案的清單。

	一律增量 (單一檔案)	其他備份配置

版本 11 備份格式	一個 TIB 檔案與一個 XML 中繼資料檔案	多個 TIB 檔案與一個 XML 中繼資料檔案
12 版備份格式	每個備份鏈一個 TIBX 檔案 (完整或差異備份，以及所有相依的增量備份)。如果本機或網路 (SMB) 資料夾中儲存之檔案的大小超過 200 GB，則預設會將檔案分割為 200 GB 的檔案。	

將備份格式變更為 12 版 (TIBX)

如果您將備份格式從 11 版 (TIB 格式) 變更為 12 版 (TIBX 格式):

- 下一次備份將為完整備份。
- 在可以使用檔案管理員瀏覽的備份位置 (例如本機或網路資料夾)，將會建立一個新的 TIBX 檔案。新檔案將會以原始檔案命名，但附加 **_v12A** 尾碼。
- 保留規則和複寫只會套用到新的備份。
- 舊的備份將不會遭到刪除，而且仍然保留在 **[備份儲存]** 索引標籤上。您可以手動刪除這些備份。
- 舊的雲端備份將不會耗用**雲端儲存空間**配額。
- 舊的本機備份將會耗用**本機備份**配額，直到您手動刪除這些備份為止。

存檔內重複資料刪除

12 版的 TIBX 備份格式支援存檔內重複資料刪除，其中包含下列優點:

- 透過內建的區塊層級重複資料刪除功能，大幅減少任何類型資料的備份大小
- 有效處理硬式連結可確保沒有儲存重複
- 雜湊型區塊

注意事項
系統預設會針對 TIBX 格式的所有備份，啟用存檔內重複資料刪除。您不必在備份選項中啟用該選項，也無法加以停用。

不同產品版本之間的備份格式相容性

如需有關備份格式相容性的資訊，請參閱不同產品版本之間的備份存檔相容性 (1689)。

備份驗證

驗證是檢視從備份中復原資料的可能性的作業。啟用此選項時，保護計劃建立的每個備份都會在建立後立即使用總和檢查碼驗證方法進行驗證。此作業是由保護代理程式所執行。

預設為:**[已停用]**。

有關透過總和檢查碼驗證來驗證的詳細資訊，請參閱 "總和檢查碼驗證" (第 202 頁)。

注意事項
視您的服務提供者所選擇的設定而定，可能無法在備份到雲端儲存空間時進行驗證。驗證也不適用於公有雲端上的備份位置。

變更區塊追蹤 (CBT)

此選項適用於下列備份：

- 虛擬機器的磁碟層級備份
- 執行 Windows 的實體機器的磁碟層級備份
- Microsoft SQL Server 資料庫的備份
- Microsoft Exchange Server 資料庫的備份

預設為：**[啟用]**。

此選項可決定在執行增量或差異備份時是否要使用 Changed Block Tracking (CBT)。

CBT 技術可加快備份程序的速度。磁碟或資料庫內容的變更會在區塊層級持續追蹤。備份開始時，所有的變更都能立即儲存到備份中。

叢集備份模式

注意事項
此功能適用於 Advanced Backup 套件。

這些選項對 Microsoft SQL Server 和 Microsoft Exchange Server 的資料庫層級備份有效。

只有在選擇叢集本身 (Microsoft SQL Server Always On 可用性群組 (AAG) 或 Microsoft Exchange Server 資料庫可用性群組 (DAG))，而非其中的個別節點或資料庫進行備份時，這些選項才有效。如果您選擇叢集內的個別項目，則備份並非叢集感知，並將僅備份所選擇的項目副本。

Microsoft SQL Server

此選項會確定用於 SQL Server Always On 可用性群組 (AAG) 的備份模式。若要讓此選項生效，所有 AAG 節點上都必須安裝 SQL 用代理程式。如需有關備份 Always On 可用性群組的更多資訊，請參閱 < 保護 Always On 可用性群組 (AAG) > 。

預設為：**次要複本 (如果可能) 。**

可選擇以下一個選項：

- **次要複本 (如果可能)**
  如果所有次要複本都離線，則會備份主要複本。備份主要複本可能會讓 SQL Server 作業速度變慢，但是資料將會以最新的狀態備份。
- **次要複本**
  如果所有次要複本都離線，則備份將會失敗。備份次要複本不會影響 SQL Server 的效能，並且可讓您延伸備份視窗。然而，被動複本包含的資訊可能並非最新，因為此類副本通常會設為非同步更新 (有延遲)。
- **主要複本**
  如果主要複本離線，則備份將會失敗。備份主要複本可能會讓 SQL Server 作業速度變慢，但是資料將會以最新的狀態備份。

無論此選項的值為何，為了確保資料庫一致性，在備份啟動時，軟體會跳過並*非***已同步**或**正在同步**狀態的資料庫。如果跳過所有資料庫，則備份失敗。

Microsoft Exchange Server

此選項會確定用於 Exchange Server 資料庫可用性群組 (DAG) 的備份模式。若要讓此選項生效，所有 DAG 節點上都必須安裝 Exchange 用代理程式。如需有關備份資料庫可用性群組的詳細資訊，請參閱 < 保護資料庫可用性群組 (DAG) > 。

預設為：**被動副本 (如果可能) 。**

可選擇以下一個選項：

- **被動副本 (如果可能)**
  如果所有被動複本都離線，就會備份主動複本。備份主動副本可能會讓 Exchange Server 作業速度變慢，但是資料將會以最新的狀態備份。
- **被動副本**
  如果所有被動複本都離線，則備份將會失敗。備份被動副本不會影響 Exchange Server 效能，而且可讓您延長備份視窗。不過，被動副本可能未包含最新的資訊，因為這類副本通常會設定為非同步更新 (有延遲)。
- **主動副本**
  如果主動複本離線，則備份將會失敗。備份主動副本可能會讓 Exchange Server 作業速度變慢，但是資料將會以最新的狀態備份。

無論此選項的值為何，為了確保資料庫一致性，在備份啟動時，軟體會跳過並*非***狀況良好**或**主動**狀態的資料庫。如果跳過所有資料庫，則備份失敗。

壓縮層級

注意事項
此選項不適用雲端到雲端備份。預設為啟用壓縮備份，並固定對應到以下的 **[正常]** 層級。

此選項可定義套用至欲備份資料的壓縮程度。可用的層級包括：**[無]**、**[一般]**、**[高]**、**[最大]**。

預設為：**[一般]**。

較高的壓縮程度代表備份過程需要更多時間，但備份結果佔用的空間更少。目前，**[高]** 與 **[最高]** 等級的工作方式類似。

最佳的資料壓縮程度取決於欲備份資料的類型。例如，若備份裡包含實質上已壓縮的檔案 (如 .jpg, .pdf 或 .mp3)，那麼即使採用最大的壓縮程度，仍無法大幅縮減備份大小。然而，.doc 或 .xls 等格式則有良好的壓縮效果。

錯誤處理

這些選項可讓您指定如何處理備份期間可能發生的錯誤。

發生錯誤時重新嘗試

預設為：**啟用。嘗試次數:10.嘗試間隔：30 秒。**

如果發生可復原的錯誤，程式將重新嘗試執行未成功的作業。您可以設定時間間隔和嘗試次數。一旦作業成功或是已執行指定次數的嘗試後 (以先發生者為準)，軟體將停止嘗試。

例如，如果網路上的備份目的地在執行備份期間變得無法使用或無法連線，此軟體會每隔 30 秒嘗試連線目的地一次，但不會超過 30 次。一旦連線繼續或執行指定次數的嘗試後 (以先發生者為準)，程式將立即停止嘗試。

不過，如果在備份開始時無法使用備份目的地，則只會嘗試 10 次。

處理時不顯示訊息和對話方塊 (無訊息模式)

預設為：**[啟用]**。

啟用無訊息模式後，程式將自動處理需要使用者互動的情形 (定義為單獨選項的[處理損壞的磁區]除外)。如果需要使用者互動方可繼續，則作業將失敗。可在作業記錄中找到作業的詳細記錄，包括錯誤 (若有)。

忽略損壞的磁區

預設為：**[已停用]**。

停用此選項時，每次程式遭遇損毀的磁區就會將備份活動指派至 **[需要互動]** 狀態。若要備份正在迅速銷毀的磁碟上的有效資訊，請啟用忽略損壞的磁區。剩餘的資料將會進行備份，您可掛載產生的磁碟備份並解壓縮有效檔案至另一個磁碟。

注意事項

Linux 不支援略過損毀的磁區。您可以在離線模式下，使用 Cyber Protect 內部部署版本中的 Bootable Media Builder，備份包含損毀磁區的 Linux 系統。使用內部部署 Bootable Media Builder 時，需要單獨的授權。如需協助，請聯絡支援部門。

若建立 VM 快照期間發生錯誤，會重新嘗試

預設為：**啟用。嘗試次數:3.嘗試間隔：5 分鐘。**

如果無法取得虛擬機器快照，程式會重新嘗試執行未成功的作業。您可以設定時間間隔和嘗試次數。一旦作業成功「或是」已執行指定次數的嘗試後 (以先發生者為準)，軟體將停止嘗試。

快速增量/差異備份

此選項對增量和差異磁碟層級備份均有效。

此選項不適用於 (一律停用) JFS、ReiserFS3、ReiserFS4、ReFS 或 XFS 檔案系統格式的磁碟區。

預設為：**[啟用]**。

增量備份或差異備份僅擷取資料變更。若要加速備份程序，程式會依檔案大小及上次修改檔案的日期/時間來判斷檔案是否已變更。停用此功能將使程式比較整個檔案內容與儲存在備份中的內容。

檔案篩選器 (包含/排除)

您可以使用檔案篩選條件，在備份中僅包含特定的檔案和資料夾，也可以從備份中排除特定的檔案和資料夾。

除非另有說明，否則檔案篩選器適用於整部電腦備份、磁碟層級備份以及檔案層級備份。

檔案篩選不適用於 XFS、JFS、exFAT 和 ReiserFS4 檔案系統。如需詳細資訊，請參閱 "支援的檔案系統" (第 50 頁)。

檔案篩選器不適用於在無代理程式模式下，透過 VMware 用代理程式、Hyper-V 用代理程式或 Scale Computing 用代理程式所備份之虛擬機器的動態磁碟 (LVM 或 LDM 磁碟區)。

檔案篩選條件類型

檔案篩選條件包含以下類型：

- 包含篩選條件 (**僅包含符合下列條件的檔案**)
  如果您在包含篩選條件中指定 `C:\File.exe`，即使您選擇 **[整部電腦]** 備份，還是只會備份此檔案。如需詳細資訊，請參閱 "篩選條件範例" (第 410 頁)。

  注意事項
  未儲存在雲端儲存空間的 **11 版**檔案層級備份不支援此篩選條件。

- 排除篩選條件 (**排除符合下列條件的檔案**)
  如果您在排除篩選條件中指定 `C:\File.exe`，即使您選擇 **[整部電腦]** 備份，備份期間還是會略過此檔案。

檔案篩選條件值

在檔案篩選條件中，您可以使用下列值：

- 檔案或資料夾名稱
  指定檔案或資料夾的名稱，例如 `Document.txt`，如此將會選擇擁有該名稱的所有檔案與資料夾。
- 檔案或資料夾的完整路徑
  指定檔案或資料夾的完整路徑，且開頭為磁碟機代號 (備份 Windows 資料時) 或根目錄 (備份 Linux 或 Mac OS 資料時)。在 Windows、Linux 和 macOS 中，您可以使用正斜線 (`C:/Temp/File.tmp`)。在 Windows 中，您也可以使用傳統的反斜線 (`C:\Temp\File.tmp`)。

重要事項

如果在磁碟層級備份過程中，未正確偵測到所備份電腦的作業系統，則包含完整路徑的檔案篩選條件將沒有作用。若是排除篩選條件，將會顯示警告。若是包含篩選條件，則備份將會失敗。

例如，檔案的完整路徑為 C:\Temp\File.tmp。如果未正確偵測到作業系統，則包含磁碟機代號或根目錄的完整路徑篩選條件 (例如 C:\Temp\File.tmp 或 C:\Temp*) 將會導致警告或失敗。

未使用磁碟機代號或根目錄的篩選條件 (例如 Temp* 或 Temp\File.tmp)，或是開頭為星號的篩選條件 (例如 *C:\) 將不會導致警告或失敗。不過，如果未正確偵測到作業系統，則這些篩選條件也將沒有作用。

萬用字元

檔案或資料夾名稱以及檔案或資料夾路徑都可以使用下列萬用字元：

- 星號 (*)

  星號代表零個或多個字元。

  例如，Doc*.txt 符合 Doc.txt 和 Document.txt 等檔案。
- 雙星號 (**)

  雙星號代表零個或多個字元，包括斜線字元。

  例如，**/Docs/**.txt 符合名為 Docs 的所有資料夾下所有子資料夾內的所有 TXT 檔案。

  您可以將雙星號萬用字元僅用於採用 12 版格式的備份。
- 問號 (?)

  問號僅代表一個字元。

  例如，Doc?.txt 符合 Doc1.txt 和 Docs.txt 等檔案，但不符合 Doc.txt 或 Doc11.txt 等檔案。

注意事項

如果檔案或資料夾名稱包含逗號或分號，請使用問號萬用字元。系統會將逗號和分號解譯為分隔符號，並將篩選條件分割成兩個部分。例如，如果您要在篩選條件中使用資料夾 MyCompany,Inc，請在指定篩選條件值時使用 MyCompany?Inc。否則，您將會建立兩個單獨的篩選條件，如下所示：

- MyCompany
- Inc

設定檔案篩選條件

您可以在保護計劃中設定檔案篩選條件。

若要設定檔案篩選條件

1. 在保護計劃中，展開 **[備份]** 模組。
2. 在 **[備份選項]** 中，按一下 **[變更]**。
3. 選擇 **[檔案篩選器 (包含/排除)]**。
4. 設定檔案篩選條件。

您可以設定一個 (包含或排除) 或兩個篩選條件。排除篩選條件優先於包含篩選條件。例如，如果您在兩個篩選條件中都指定 C:\File.exe，則在備份期間將會略過 C:\File.exe。

使用篩選條件不會影響備份範圍 (**備份內容**) 中特定檔案的選擇。如需詳細資訊，請參閱 "篩選條件範例" (第 410 頁)。

注意事項

如果名稱或路徑包含逗號或分號，請將其取代為問號 (?) 萬用字元。系統會將逗號和分號解譯為分隔符號，並將篩選條件分割成兩個部分。如需詳細資訊，請參閱 " 萬用字元" (第 409 頁)。

5. 按一下**[完成]**。
6. 儲存保護計劃。

結果，檔案篩選條件將套用至保護計劃的 **[備份內容]** 區段中設定的範圍。

篩選條件範例

下表顯示檔案篩選條件組態的範例。

包含篩選條件			
要備份的內容	**篩選條件值**	**備份存檔包含**	**描述**
C:\Folder1 (包含 MyFile.txt 及其他檔案) C:\Folder2 (包含 MyDocument.txt 及其他檔案)	MyFile.txt C:\Folder2\MyDocument.txt	C:\Folder1\MyFile.txt C:\Folder2\MyDocument.txt	包含篩選條件與備份範圍 (**備份內容**) 相符。 備份的資料夾中只會有在包含篩選條件中指定的檔案。 您可以使用檔案或資料夾名稱，或使用檔案或資料夾路徑來設定檔案篩選條件。
C:\Folder1 (包含多個檔案)	C:\Folder2\MyDocument.txt	C:\Folder1 (作為空資料夾)	包含篩選條件與備份範圍 (**備份內容**) 不符。 Folder1 已備份，但是空的，因為它不包含包

包含篩選條件			
要備份的內容	**篩選條件值**	**備份存檔包含**	**描述**
			含篩選條件中的檔案。 包含篩選條件中的檔案不在備份範圍內，因此不會備份。
C:\Folder1 (包含 MyFile.txt 及其他檔案) C:\Folder2 (包含 MyDocument.txt 及其他檔案)	MyFile.txt	C:\Folder1\MyFile.txt C:\Folder2 (作為空資料夾)	包含篩選條件與備份範圍 (**備份內容**) 部分相符。 Folder1 已備份，但僅包含指定在包含篩選條件中的檔案。 Folder2 已備份，但是空的，因為它不包含包含篩選條件中的檔案。
C:\Folder1 (包含 MyFile.txt 及其他檔案) C:\Folder2\MyDocument.txt	MyFile.txt	C:\Folder1\MyFile.txt C:\Folder2\MyDocument.txt	Folder1 已備份，但僅包含指定在包含篩選條件中的檔案。 也會備份第二個選取的檔案。使用篩選條件不會影響備份範圍 (**備份內容**) 中特定檔案的選取。

排除篩選條件			
要備份的內容	**篩選條件值**	**備份存檔包含**	**描述**
C:\Folder1 (包含 MyFile.txt 及其他檔案) C:\Folder2 (包含 MyDocument.txt 及其他檔案)	MyFile.txt C:\Folder2\MyDocument.txt	C:\Folder1 – 所有檔案，但 MyFile.txt 除外 C:\Folder2 – 所有檔案，但 MyDocument.txt 除外	排除篩選條件與備份範圍 (**備份內容**) 相符。 備份的資料夾中缺少在排除篩選條件中指定的檔案。 您可以使用檔案或資料夾名稱，或使用檔案或資料夾路徑來設定檔案篩選條件。
C:\Folder1 (包含多個檔案)	C:\Folder2\MyDocument.txt	C:\Folder1 – 所有檔案	排除篩選條件與備份範圍 (**備份內容**) 不符。 已備份 Folder1 的整個內容。
C:\Folder1 (包含 MyFile.txt 及其他檔案) C:\Folder2 (包含 MyDocument.txt 及其他檔案)	MyFile.txt	C:\Folder1 – 所有檔案，但 MyFile.txt 除外 C:\Folder2 – 所有檔案	包含篩選條件與備份範圍 (**備份內容**) 部分相符。 已備份 Folder1，但缺少在排除篩選條件中指定的檔案。 已備份 Folder2 的整個內容。
C:\Folder1 (包含 MyFile.txt 及其他檔案)	MyFile.txt	C:\Folder1 – 所有檔案，但 MyFile.txt 除外	已備份 Folder1，但

排除篩選條件			
要備份的內容	**篩選條件值**	**備份存檔包含**	**描述**
C:\Folder2\MyDocument.txt		C:\Folder2\MyDocument.txt	缺少在排除篩選條件中指定的檔案。 第二個選取的檔案與排除篩選條件不符，因此已備份該檔案。

檔案層級備份快照

此選項僅對檔案層級備份有效。

此選項定義是否逐個備份檔案或透過擷取即時資料快照來備份檔案。

注意事項
儲存在網路共用位置上的檔案會持續逐一備份。

預設為：

- 如果只選擇執行 Linux 的電腦進行備份：**不要建立快照。**
- 其他情況：**如有可能，則建立快照。**

您可以選擇下列其中一項：

- **如有可能，則建立快照**
  如果無法擷取快照，則直接備份檔案。
- **一律建立快照**
  快照可以讓您備份所有檔案，包括以獨佔存取方式開啟的檔案。檔案將在同一時間點備份。僅在這些因素十分關鍵時選擇此設定，即備份檔案不可缺少快照時。如果無法擷取快照，則無法備份。
- **不要建立快照**
  始終直接備份檔案。嘗試備份以獨佔存取方式開啟的檔案將導致讀取錯誤。備份中的檔案時間可能不一致。

鑑識資料

病毒、惡意程式碼和勒索軟體可能會執行惡意活動，例如竊取或變更資料。這些活動可能需要進行調查，這只有在提供數位證據時才可行。不過，數位證據片段 (例如，檔案或活動蹤跡) 可能會遭到刪除，或者進行惡意活動所在電腦可能會變成無法使用。

包含鑑識資料的備份允許調查人員分析通常不包含在定期磁碟備份中的磁碟區域。**[鑑識資料]** 備份選項可讓您收集下列能夠用於鑑識調查的數位證據片段：未使用磁碟空間的快照、記憶體傾印，以及執行中程序的快照。

系統會自動公證含鑑識資料的備份。

[鑑識資料] 選項僅適用於執行下列作業系統的 Windows 電腦整部電腦備份：

- Windows 8.1、Windows 10
- Windows Server 2012 R2 – Windows Server 2019

包含鑑識資料的備份不適用於下列電腦：

- 透過 VPN 連線到網路，且無法直接存取網際網路的電腦
- 包含使用 BitLocker 加密的磁碟的電腦

注意事項
您無法在將已啟用 **[備份]** 模組的保護計劃套用到電腦後，修改鑑識資料設定。若要使用不同的鑑識資料設定，請建立新的保護計劃。

您可以將包含鑑識資料的備份儲存在下列位置中：

- 雲端儲存
- 本機資料夾

  注意事項
  只有透過 USB 連線的外接式硬碟才支援本機資料夾位置。
  不支援本機動態磁碟作為包含鑑識資料的備份的位置。

- 網路資料夾

鑑識備份程序

系統會在鑑識備份程序期間執行下列動作：

1. 收集原始記憶體傾印以及執行中處理程序的清單。
2. 自動讓電腦重新開機進入可開機媒體。
3. 建立同時包含已佔用空間和未配置空間的備份。
4. 公證備份的磁碟。
5. 重新開機進入即時作業系統並繼續執行計劃 (例如，複寫、保留、驗證等等)。

設定鑑識資料集合

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。或者，您可以從 **[管理]** 索引標籤建立保護計劃。
2. 選擇裝置，然後按一下 **[保護]**。
3. 在保護計劃中，啟用 **[備份]** 模組。
4. 在 **[要備份的內容]** 中選擇 **[整部電腦]**。
5. 在 **[備份選項]** 中，按一下 **[變更]**。

6. 尋找 **[鑑識資料]** 選項。
7. 啟用 **[收集鑑識資料]**。系統將會自動收集記憶體傾印，並建立執行中處理程序的快照。

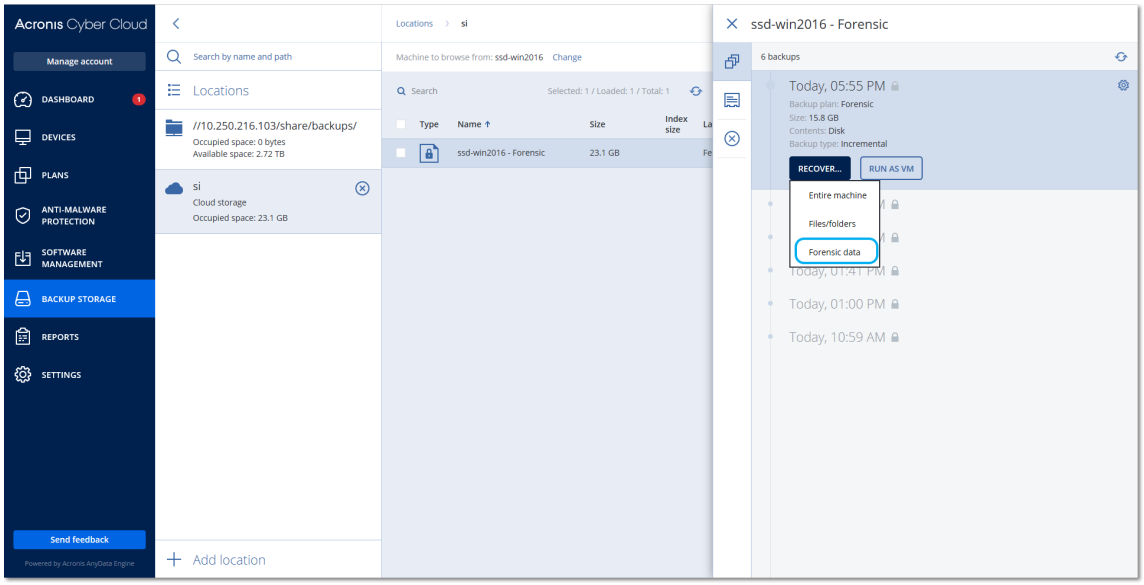
注意事項
完整記憶體傾印可能包含密碼之類的敏感資料。

8. 指定位置。
9. 按一下 **[立即執行]** 可立即執行含鑑識資料的備份，或根據排程，等到建立備份為止。
10. 移至 **[監控]** > **[活動]**，並確認已成功建立含鑑識資料的備份。

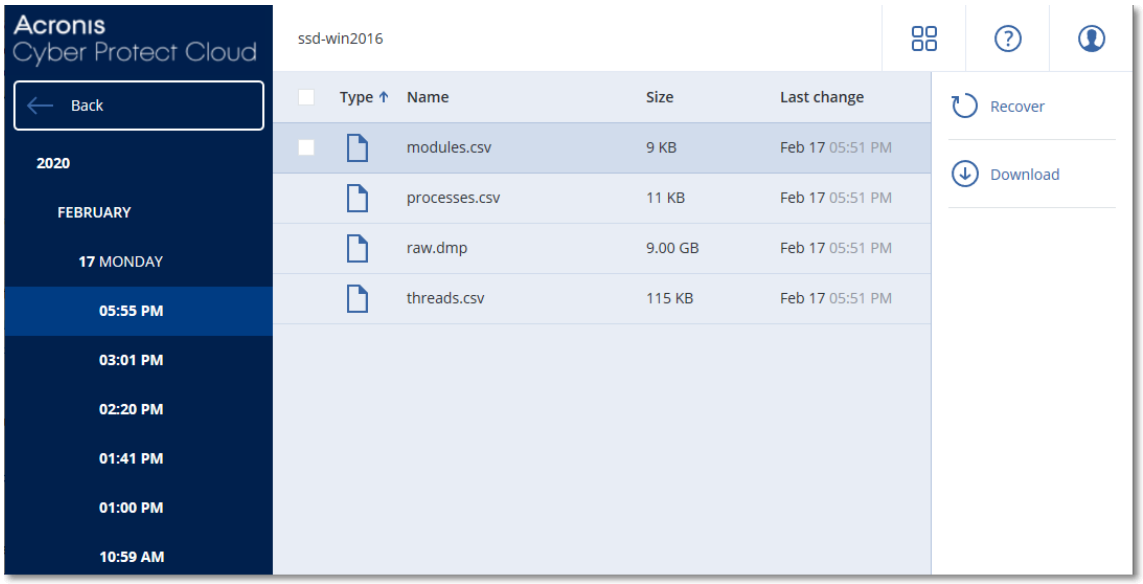
因此，備份將包含鑑識資料，而且您將能夠取得這些備份進行分析。含鑑識資料的備份會經過標示，而且可以使用 **[僅搭配鑑識資料]** 選項，在 **[備份儲存]** > **[位置]** 的其他備份中篩選出來。

如何從備份取得鑑識資料？

1. 在 Cyber Protect 主控台中，移至 **[備份儲存]**，然後選擇具有內含鑑識資料之備份的位置。
2. 選擇含鑑識資料的備份，然後按一下 **[顯示備份]**。
3. 針對含鑑識資料的備份，按一下 **[復原]**。
   - 若要僅取得鑑識資料，按一下 **[鑑識資料]**。



系統將會顯示一個含鑑識資料的資料夾。選擇一個記憶體傾印檔案或其他任何鑑識檔案，然後按一下 **[下載]**。



- 若要復原完整鑑識備份，按一下 **[整部電腦]**。系統將會復原不含開機模式的備份。因此，可以檢查磁碟未經過變更。

您可以使用提供的記憶體傾印搭配數個協力廠商鑑識軟體，例如，使用 https://www.volatilityfoundation.org/ 上的 Volatility Framework 進行進一步的記憶體分析。

公證含鑑識資料的備份

為確保含鑑識資料的備份就是所採用的映像而且未遭到損壞，備份模組可公證含鑑識資料的備份。

運作原理

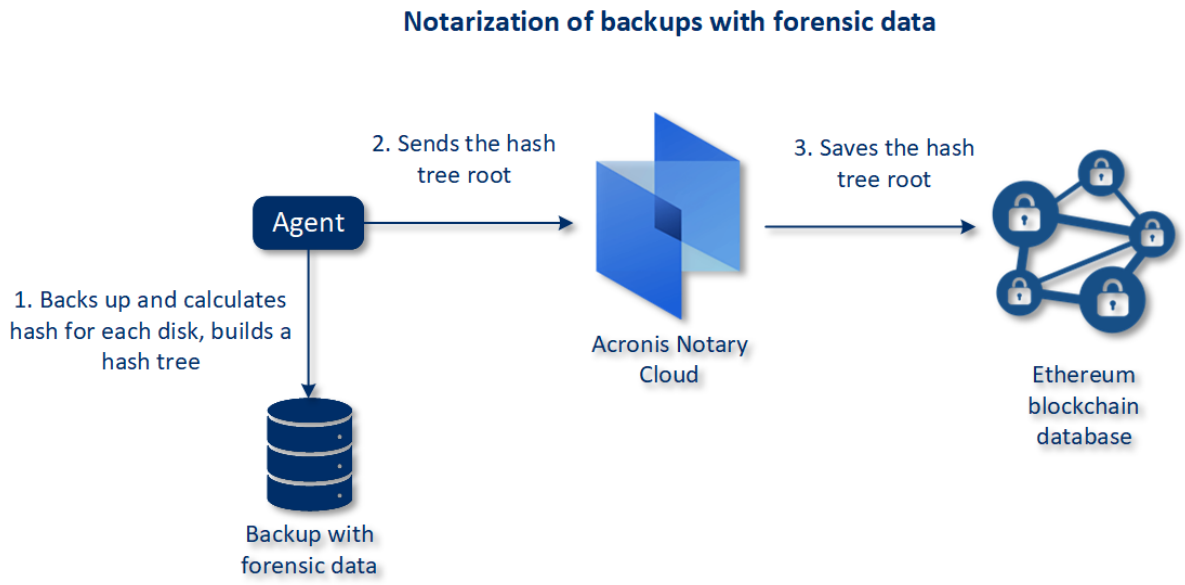
公證可讓您證明含鑑識資料的磁碟在備份後即是真實且未變更的。

在備份過程中，代理程式會計算已備份檔案的雜湊代碼、建置雜湊樹狀結構、儲存備份中的樹狀結構，然後將雜湊樹狀結構根部傳送到公證服務。公證服務將雜湊樹狀結構根部儲存在 Ethereum 區塊鏈資料庫中，以確保此值不會變更。

在驗證含鑑識資料之磁碟的真實性時，代理程式會計算磁碟雜湊，然後將其與儲存在備份內雜湊樹狀結構中的雜湊相比較。如果這些雜湊不相符，則磁碟會被視為不真實。否則，由雜湊樹狀結構保證磁碟的真實性。

若要驗證雜湊樹狀結構自身未受損，代理程式會將雜湊樹狀結構根部發送給公證服務。公證服務將其與儲存在區塊鏈資料庫中的雜湊相比較。如果雜湊相符，則所選磁碟保證為真實的。否則，軟體會顯示一則訊息，指示磁碟不真實。

以下的配置簡要地顯示含鑑識資料之備份的公證程序。



若要手動驗證公證的磁碟備份，您可以取得其憑證，並使用 tibxread 工具，依照與憑證一起顯示的驗證程序進行。

取得含鑑識資料之備份的憑證

若要從主控台取得含鑑識資料之備份的憑證，請執行下列動作：

1. 移至 **[備份儲存]**，然後選擇含鑑識資料的備份。
2. 復原整部電腦
3. 系統會開啟 **[磁碟對應]** 檢視畫面。
4. 按一下磁碟的 **[取得憑證]** 圖示。
5. 系統將會產生憑證，並使用憑證，在瀏覽器中開啟一個新視窗。在憑證下方，您將會看到手動驗證已公證磁碟備份的指示。

取得已備份資料的 "tibxread" 工具

Cyber Protection 提供稱為 `tibxread`的工具，可手動檢查已備份磁碟的完整性。此工具可讓您從備份取得資料，並計算指定之磁碟的雜湊。此工具會自動與下列元件一起安裝：Windows 用代理程式、Linux 用代理程式和 Mac 用代理程式。

安裝路徑：與代理程式擁有的資料夾相同 (例如，`C:\Program Files\BackupClient\BackupAndRecovery`)。

支援的位置為：

- 本機磁碟
- 不需認證即可存取的網路資料夾 (CIFS/SMB)。
  若是受密碼保護的網路資料夾，您可以使用作業系統工具，將網路資料夾掛載到本機資料夾，然後再掛載本機資料夾作為此工具的來源。
- 雲端儲存

您應該提供 URL、連接埠和憑證。URL 和連接埠可以從 Windows 登錄機碼或 Linux/Mac 電腦上的組態檔取得。

對於 Windows：

```
HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<tenant_login>\FesUri
```

對於 Linux：

```
/etc/Acronis/BackupAndRecovery.config
```

對於 macOS：

```
/Library/Application Support/Acronis/Registry/BackupAndRecovery.config
```

憑證可以在下列位置找到：

對於 Windows：

```
%allusersprofile%\Acronis\BackupAndRecovery\OnlineBackup\Default
```

對於 Linux：

```
/var/lib/Acronis/BackupAndRecovery/OnlineBackup/Default
```

對於 macOS：

```
/Library/Application Support/Acronis/BackupAndRecovery/OnlineBackup/Default
```

此工具包含下列命令：

- `list backups`
- `list content`
- `get content`
- `calculate hash`

list backups

列出備份中的復原點。

SYNOPSIS：

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

選項

```
--loc=URI
--arc=BACKUP_NAME
--raw
```

```
--utc
--log=PATH
```

輸出範本：

```
GUID   日期   日期時間戳記
----   ------ --------------
<guid> <date> <timestamp>
```

<guid> – 備份 GUID。

<date> – 備份的建立日期。格式為 “DD.MM.YYYY HH24:MM:SS”。預設為當地時區 (可以使用 --utc 選項變更)。

輸出範例：

```
GUID   日期   日期時間戳記
----   ------ --------------
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

列出復原點中的內容。

SYNOPSIS：

```
tibxread list content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID
--raw --log=PATH
```

選項

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--raw
--log=PATH
```

輸出範本：

```
磁碟     大小   公證狀態
-------- ------ --------------------
<number> <size> <notarization_status>
```

<number> – 磁碟的識別碼。

<size> – 以位元組為單位的大小。

<notarization_status> – 可能是下列狀態：未公證、已公證、下次備份。

輸出範例：

```
磁碟     大小   Notary 狀態
-------- ------ --------------
1        123123465798 Notarized
2        123123465798 Notarized
```

get content

將復原點中指定之磁碟的內容寫入標準輸出 (stdout)。

SYNOPSIS：

```
tibxread get content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID -
-disk=DISK_NUMBER --raw --log=PATH --progress
```

選項

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
--progress
```

calculate hash

使用 SHA-2 (256 位元) 演算法，計算復原點中指定之磁碟的雜湊，然後將其寫入 stdout。

SYNOPSIS：

```
tibxread calculate hash --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_
ID --disk=DISK_NUMBER --raw --log=PATH --progress
```

選項

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
```

選項描述

選項	描述
--arc=BACKUP_NAME	您可以從 Cyber Protect 主控台中的備份內容取得的備份檔案名稱。您必須以副檔名 .tibx 指定備份檔案。
--backup=RECOVERY_POINT_ID	復原點識別碼
--disk=DISK_NUMBER	磁碟編號 (與寫入 "get content" 命令輸出的編號相同)
--loc=URI	備份位置 URI。"--loc" 選項的可能格式為： • 本機路徑名稱 (Windows) `c:/upload/backups` • 本機路徑名稱 (Linux) `/var/tmp` • SMB/CIFS `\\server\folder` • 雲端儲存 `--loc=<IP_address>:443 --cert=<path_to_certificate> [--storage_path=/1]` <IP_address> – 您可以在 Windows 的登錄機碼中找到它：HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<tenant_login>\FesUri <path_to_certificate> – 存取 Cyber Protect Cloud 之憑證檔案的路徑。例如，在 Windows 中，此憑證位於 `C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<username>.crt`，其中 <username> – 是您存取 Cyber Protect Cloud 的帳戶名稱。
--log=PATH	允許依指定的 PATH 撰寫記錄 (僅限本機路徑，格式與 `--loc=URI` 參數的格式相同)。記錄層級為 DEBUG。
--password=PASSWORD	您備份的加密密碼。如果備份未加密，請將此值留空。
--raw	在命令輸出中隱藏標頭 (前 2 列)。應該剖析命令輸出時使用。 不含 "--raw" 的輸出範例： `GUID 日期 日期時間戳記` `---- ------ --------------` `516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865` `516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925` 含 "--raw" 的輸出：

	`` 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	顯示 UTC 日期
--progress	顯示作業的進度。 例如： ``` 1% 2% 3% 4% ... 100% ```

記錄截斷

此選項適用於備份 Microsoft SQL Server 資料庫，以及啟用 Microsoft SQL Server 應用程式備份的磁碟層級備份。

此選項會在備份成功後判斷 SQL Server 交易記錄是否遭到截斷。

預設為：**[啟用]**。

啟用此選項時，只會將資料庫復原至此軟體建立備份的時間點。若使用 Microsoft SQL Server 的原生備份引擎備份交易記錄，則會停用此選項。此時您可以在復原後套用交易記錄，然後將資料庫復原至任一時間點。

LVM 快照

此選項僅對實體機器有效。

此選項對 Linux 邏輯磁碟區管理員 (LVM) 管理的磁碟區之磁碟層級備份有效。這類磁碟區又稱為邏輯磁碟區。

此選項定義了邏輯磁碟區的快照擷取方式。備份軟體可自行完成擷取，亦可由 Linux 邏輯磁碟區管理員 (LVM) 擷取。

預設為：**由備份軟體完成**。

- **由備份軟體完成**。快照資料大部分儲存在 RAM 中。備份速度較快，而且磁碟區群組上不需要有未配置空間。因此，建議您只有在備份邏輯磁碟區遇到問題時才變更預設。
- **由 LVM 完成**。快照會儲存在磁碟區群組的未配置空間上。若沒有未配置空間，則會由備份軟體擷取快照。

快照僅用於備份作業期間，而且在備份作業完成後會自動刪除。不會保留任何暫存檔。

掛載點

只有在 Windows 中針對包括已掛載磁碟區或叢集共用磁碟區在內的資料來源進行檔案層級備份時，此選項才能發揮作用。

注意事項

對於 Linux 和 macOS，將忽略 **[備份掛載點]** 選項，且行為將如下所示：

- 將一律備份「本機」掛載點中的資料，例如本機磁碟、USB 磁碟機等。
- 將永遠不會備份 CIFS/NFS 共用等「遠端」掛載點中的資料。

當您選擇資料夾進行備份時，資料夾的階層必須高於掛載點，此選項才能發揮作用。(掛載點是一個附加了額外的邏輯磁碟區的資料夾。)

- 如果選擇這種資料夾 (父資料夾) 進行備份，且啟用 **[掛載點]** 選項，位在已掛載磁碟區上的所有檔案都會納入備份範圍。如果停用 **[掛載點]** 選項，備份中的掛載點將是空的。

  復原父資料夾期間，是否會復原掛載點內容，取決於**復原的** [掛載點] 選項是啟用還是停用狀態。
- 如果直接選擇掛載點，或選擇掛載磁碟區內任何資料夾，選擇的資料夾將被視為一般資料夾。無論 **[掛載點]** 選項狀態為何，都會備份這些資料夾；無論**復原的** [掛載點] 選項狀態為何，都會復原這些資料夾。

預設為：**[已停用]**。

注意事項

您可以備份位於叢集共用磁碟區的 Hyper-V 虛擬機器，方法是利用檔案層級備份來備份所需的檔案或整個磁碟區。您必須關閉虛擬機器，以確保其備份狀態一致。

範例

假設 **C:\Data1** 資料夾是掛載磁碟區的掛載點。磁碟區包含 **Folder1** 與 **Folder2** 兩個資料夾。您建立了一個檔案層級資料備份的保護計劃。

如果您選取磁碟區 C 的核取方塊，並且啟用 **[掛載點]** 選項，備份中的 **C:\Data1** 資料夾就會包含 **Folder1** 與 **Folder2**。復原備份資料時，請務必正確使用 **復原的 [掛載點]** 選項。

如果您選取磁碟區 C 的核取方塊，並且停用 **[掛載點]** 選項，備份中的 **C:\Data1** 資料夾就會是空的。

如果您選取 **Data1**、**Folder1** 或 **Folder2** 資料夾的核取方塊，無論 **[掛載點]** 選項狀態為何，核取的資料夾都會作為一般資料夾納入備份。

多重磁碟區快照(M)

此選項適用於執行 Windows 或 Linux 之實體機器的備份。

此選項適用於磁碟層級備份。當檔案層級備份是藉由擷取快照的方式執行時，此選項也適用於檔案層級備份。([檔案層級備份快照] 選項會決定是否要在檔案層級備份期間擷取快照)。

此選項會決定要同時或逐一擷取多個磁碟區的快照。

預設為：

- 如果選擇至少一部執行 Windows 的電腦進行備份：**[啟用]**。
- 其他情況：**[已停用]**。

啟用此選項時，系統會同時建立要備份之所有磁碟區的快照。此選項可用來為分佈在多個磁碟區的資料建立時間一致的備份，例如 Oracle 資料庫。

停用此選項時，系統會逐一擷取磁碟區的快照。因此，如果資料分佈在多個磁碟區，所產生的備份可能會有不一致的情形。

單鍵復原

注意事項
此功能適用於 Advanced Backup 套件。

您可以利用單鍵復原，自動復原 Windows 或 Linux 電腦的磁碟備份。此備份可以是整部電腦的備份，也可以是此電腦上特定磁碟或磁碟區的備份。

單鍵復原支援下列作業：

- 從最新的備份自動復原
- 從備份存檔中的特定備份 (也稱為復原點) 復原

單鍵復原支援下列備份儲存空間：

- Secure Zone
- 網路資料夾
- 雲端儲存

重要事項
當您執行下列任何作業時，在下次重新啟動電腦前，暫停 BitLocker 加密：

- 建立、修改或刪除 Secure Zone。
- 啟用或停用 Startup Recovery Manager。
- [只有在還未啟用 Startup Recovery Manager 的情況下] 在保護計劃中啟用 [單鍵復原] 後，執行第一次備份。此作業會自動啟用 Startup Recovery Manager。
- 更新 Startup Recovery Manager，例如，透過更新保護。

如果未在這些作業期間暫停 BitLocker 加密，則您需要在重新啟動電腦後指定 BitLocker PIN。

啟用單鍵復原

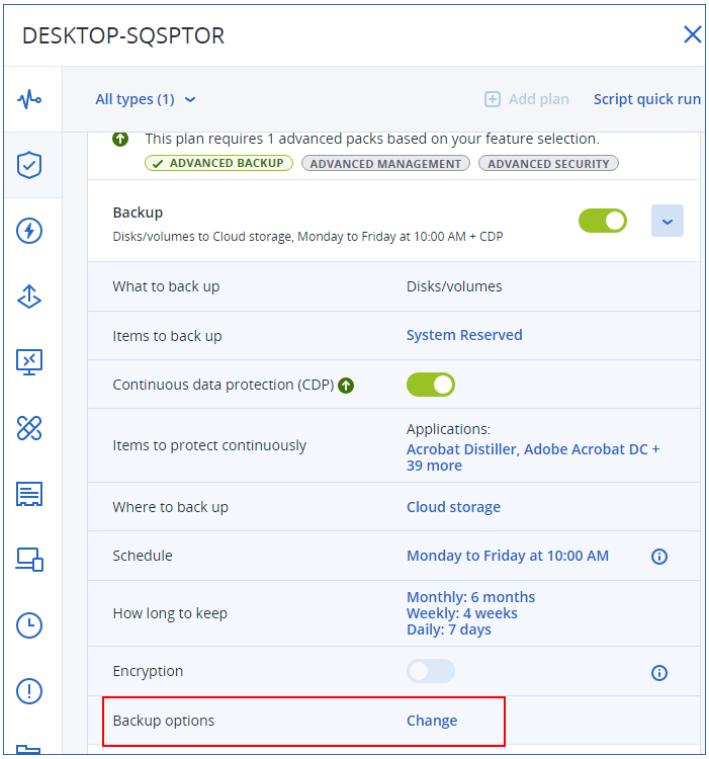
單鍵復原是保護計劃中的備份選項。如需有關如何建立計劃的詳細資訊，請參閱 "建立保護計劃" (第 192 頁)。

注意事項

啟用單鍵復原也會啟用目標電腦上的 Startup Recovery Manager。如果無法啟用 Startup Recovery Manager，建立單鍵復原備份的備份作業將會失敗。如需有關 Startup Recovery Manager 的詳細資訊，請參閱 "Startup Recovery Manager" (第 652 頁)。

若要啟用單鍵復原

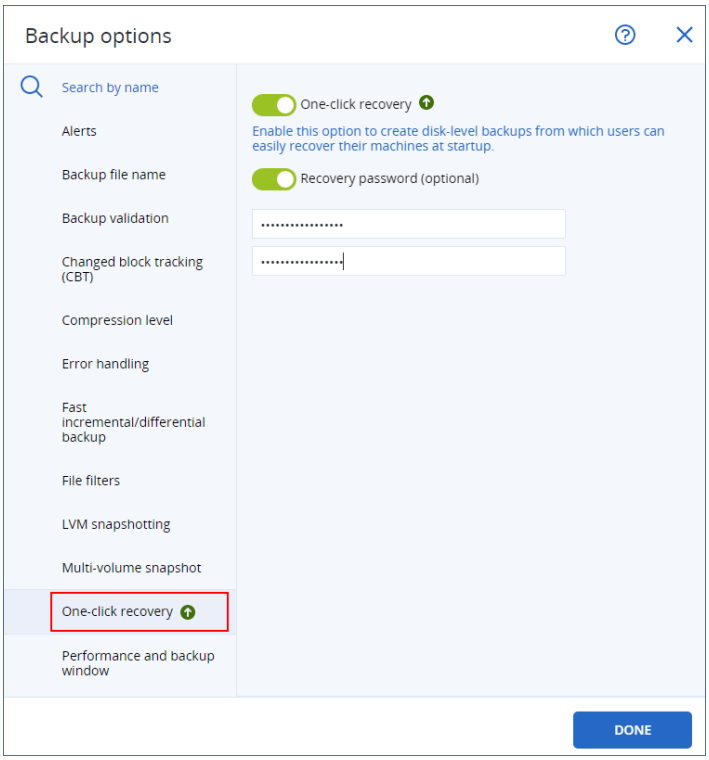
1. 在保護計劃中，展開 **[備份]** 模組。
2. 在 **[要備份的內容]** 中選擇 **[整部電腦]** 或 **[磁碟/磁碟區]**。
3. [如果您選擇 **[磁碟/磁碟區]**]。在 **[要備份的項目]** 中，指定要備份的磁碟或磁碟區。
4. 在 **[備份選項]** 中，按一下 **[變更]**，然後選擇 **[單鍵復原]**。



5. 啟用 **[單鍵復原]** 開關。
6. [選用] 啟用 **[復原密碼]** 開關，然後指定密碼。

重要事項

強烈建議您指定復原密碼。請確保在目標電腦上執行單鍵復原的使用者知道此密碼。



7. 按一下**[完成]**。
8. 根據您的需求設定保護計劃的其他元素，然後儲存計劃。

結果，在保護計劃執行並建立備份之後，受保護電腦的使用者就可以存取單鍵復原。

停用單鍵復原

您可以透過下列方式，為特定工作負載停用單鍵復原：

- 在套用至工作負載的保護計劃中，停用 **[單鍵復原]** 選項。
- 撤銷已啟用 **[單鍵復原]** 選項的保護計劃。
- 刪除已啟用 **[單鍵復原]** 選項的保護計劃。

使用單鍵復原來復原電腦

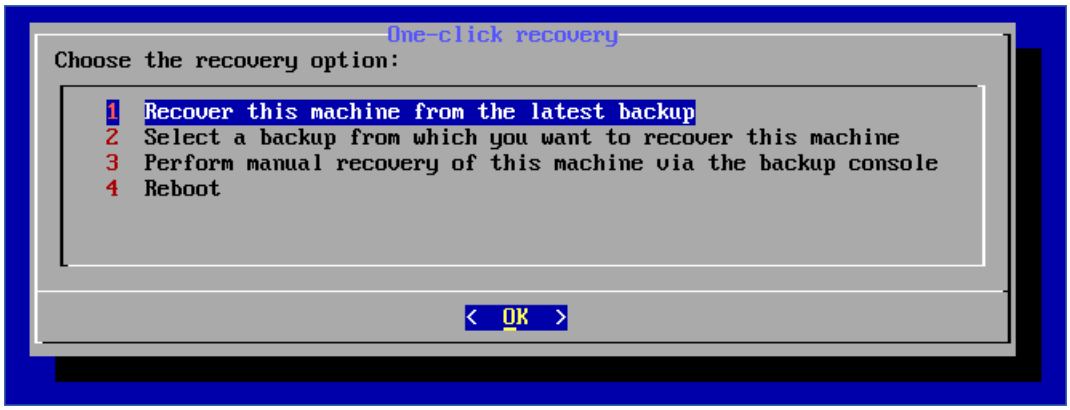
必要條件

- 已啟用 **[單鍵復原]** 備份選項的保護計劃會套用到電腦中。
- 電腦至少有一個磁碟備份。

若要復原電腦

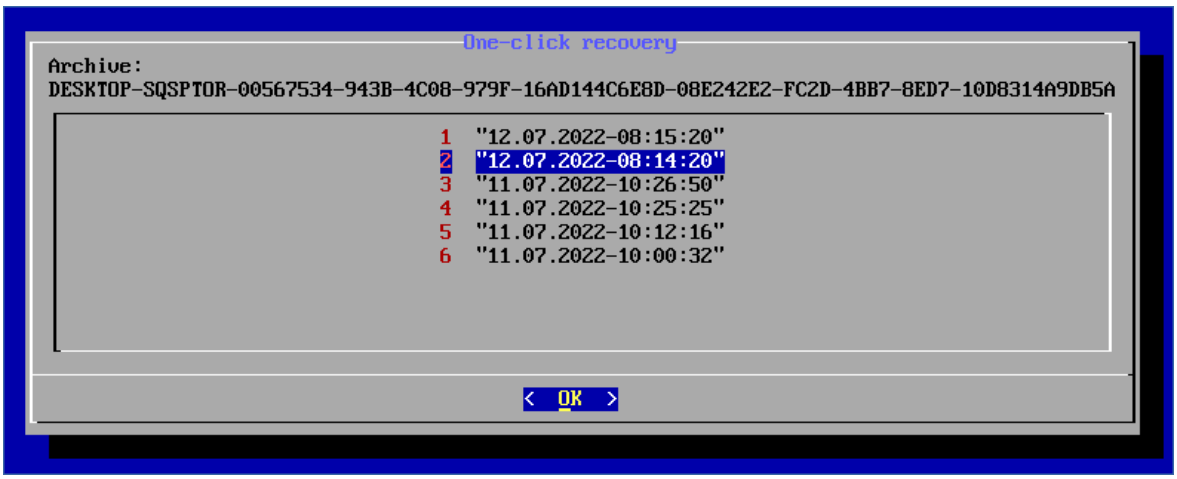
1. 將您要復原的電腦重新開機。
2. 重新開機期間，按下 F11 進入 Startup Recovery Manager。
   救援媒體視窗隨即開啟。
3. 選擇 **Acronis Cyber Protect**。
4. [如果已在保護計劃中指定復原密碼] 輸入復原密碼，然後按一下 **[確定]**。

5. 選擇 [單鍵復原] 選項。
   - 若要自動復原最新的備份，請選擇第一個選項，然後按一下 **[確定]**。
   - 若要復原備份存檔中的另一個備份，請選擇第二個選項，然後按一下 **[確定]**。

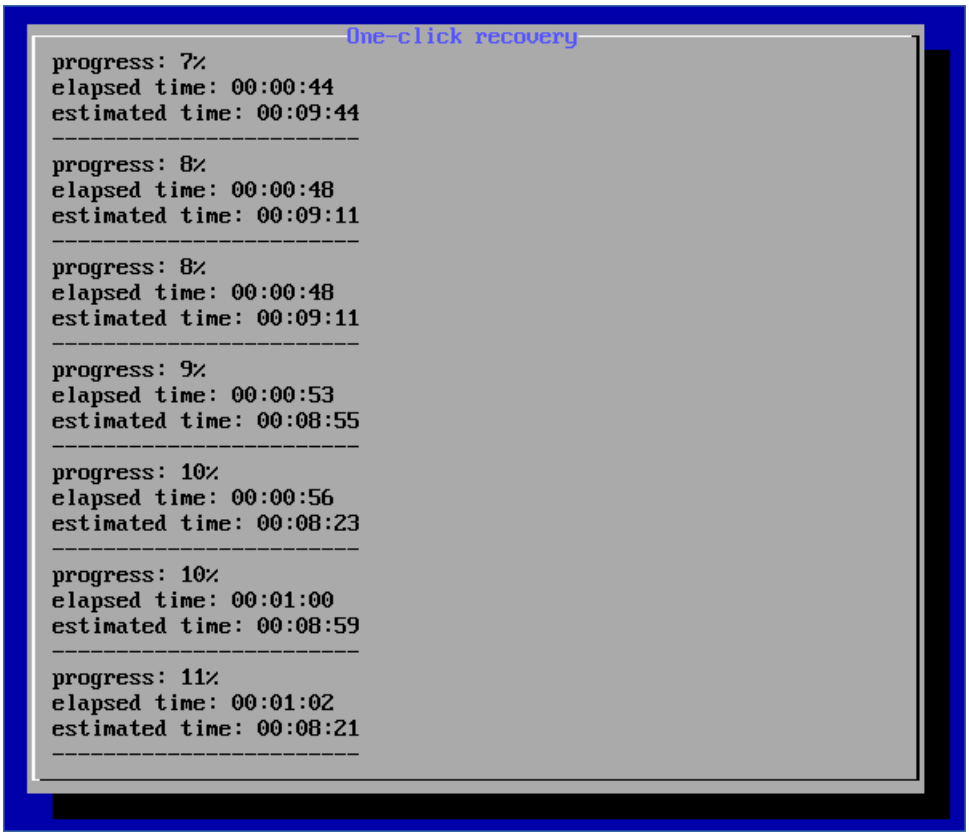


6. 按一下 **[是]**，確認您的選擇。

   救援媒體視窗隨即開啟，然後消失。復原程序會繼續進行，而不需要該視窗。
7. [如果您選擇復原特定備份] 選擇您要復原的備份，然後按一下 **[確定]**。



一段時間後，復原便會開始並顯示其進度。復原完成後，您的電腦會重新開機。



效能和備份時窗

此選項可讓您針對一週內的每個小時，設定三種層級備份效能 (高、低、禁止) 之一。如此一來，您可以定義允許開始並執行備份的時段。高和低效能層級可以根據處理優先順序和輸出速度進行設定。

此選項無法用於雲端代理程式所執行的備份，例如網站備份或雲端復原網站上的伺服器備份。

此選項僅對備份和備份複寫程序有效。保護計劃 (例如驗證) 中包含的備份後命令和其他作業將會執行，而不受此選項影響。

預設為：**[已停用]**。

停用此選項時，可以利用下列參數，隨時執行備份 (無論這些參數是否會針對預設值變更)：

- CPU 優先順序：**[低]** (在 Windows 中，會對應至 **[低於一般]**)
- 輸出速度：**無限制**

啟用此選項後，系統會根據針對目前小時指定的效能參數而允許或阻止排程備份。在阻止備份的那一小時開始，系統會自動停止備份程序並產生警示。即使排程備份遭到阻止，仍然可以手動開始備份。允許備份時，將使用最近一小時的效能參數。

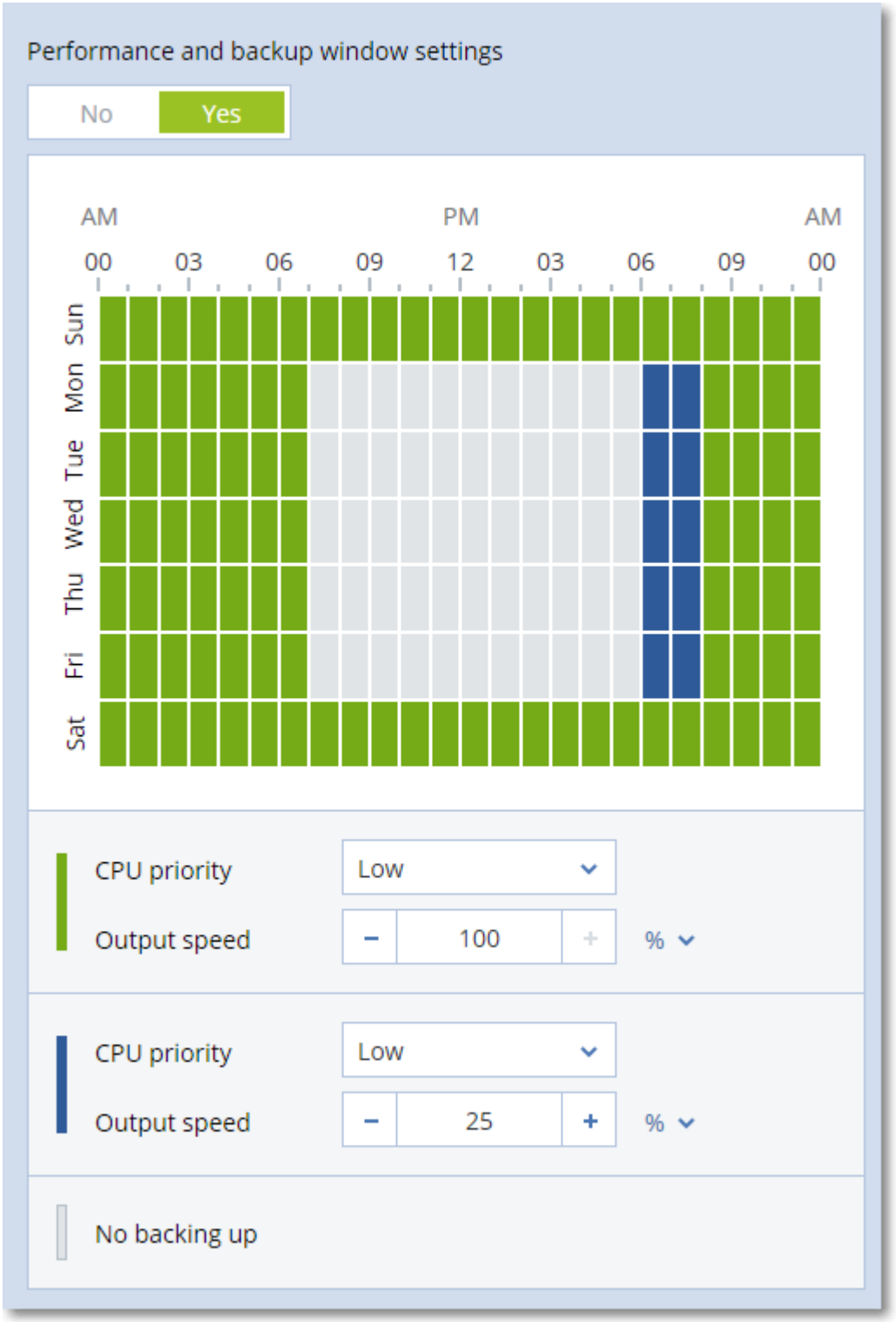
注意事項
您可以為每個複寫位置個別設定效能和備份時段。若要存取複寫位置的設定，請在保護計劃中按一下位置名稱旁的齒輪圖示，然後按一下 **[效能和備份時窗]**。

備份視窗

每個矩形都代表一周內的一小時。按一下某個矩形可循環顯示下列狀態：

- **綠色：**允許使用在以下綠色區段中指定的參數進行備份。
- **藍色：**允許使用在以下藍色區段中指定的參數進行備份。
  如果備份格式設定為 **11 版**，則不提供此狀態。
- **灰色：**阻止備份。

按一下並拖曳就可以同時變更多個矩形的狀態。



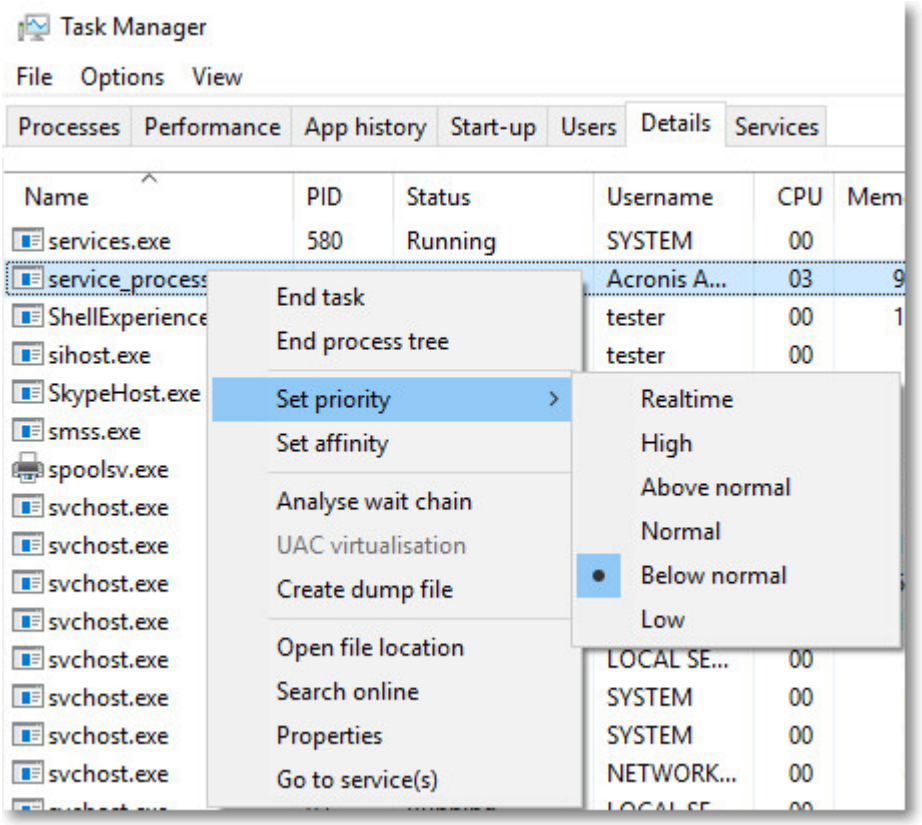
CPU 優先順序

此參數會定義作業系統內備份程序的優先順序。

可用設定包括：**[低]**、**[一般]**、**[高]**。

系統中執行程序的優先順序會決定分配給該程序的 CPU 和系統資源多寡。降低備份優先順序會釋放更多資源給其他應用程式。提高備份優先順序會要求作業系統配置更多資源 (例如 CPU) 給備份應用程式，進而可加快備份程序。但是，實際效果將取決於整體的 CPU 使用量和其他因素 (如磁碟輸入/輸出速度或網路流量)。

此選項可設定 Windows 中備份程序的優先順序 (**service_process.exe**)，以及 Linux 與 macOS 內備份程序的優先度等級 (**service_process**)。



下表摘要此設定在 Windows、Linux 和 macOS 中的對應。

Cyber Protection 優先順序	Windows 優先順序	Linux 和 macOS 優先度等級
低	低於一般	10
一般	一般	0
高	高	-10

備份期間的輸出速度

此參數可讓您限制備份至本機資料夾時的硬碟寫入速度，或限制備份至網路共用或雲端儲存空間時，透過網路傳輸備份資料的速度。

啟用此選項時，您可以指定允許的最大輸出速度：

- (當備份至本機資料夾時) 目的地硬碟之估計寫入速度百分比，或 (當備份至網路共用或雲端儲存時) 網路連線的估計最高速度百分比。

  此設定僅當代理程式是在 Windows 中執行時才能運作。
- 單位是 KB/秒 (針對所有目的地)。

實體資料運送

如果備份或複寫目的地為雲端儲存空間，且備份格式設定為 **12 版**，則可使用此選項。

此選項對於 Windows 用代理程式、Linux 用代理程式、Mac 用代理程式、VMware 用代理程式、Hyper-V 用代理程式，以及 Virtuozzo 用代理程式所建立的磁碟層級備份和檔案備份有效。

使用此選項可透過「實體資料運送」服務，將保護計劃所建立的第一個完整備份傳送至硬碟機上的雲端儲存空間。後續的增量備份則是透過網路執行。

對於複寫至雲端的本機備份，增量備份則會繼續進行，並儲存在本機，直到初始備份上傳到雲端儲存空間為止。接著，所有增量變更都會複寫到雲端，並根據備份排程繼續複寫。

預設為：**[已停用]**。

關於「實體資料運送」服務

「實體資料運送」服務 Web 介面僅適用於系統管理員。

如需有關使用「實體資料運送」服務以及訂單建立工具的詳細指示，請參閱實體資料運送系統管理員指南。若要存取此文件，請在「實體資料運送」服務 Web 介面中，按一下問號圖示。

實體資料運送程序概觀

1. [運送將雲端儲存空間當作主要備份位置的備份]
   a. 建立備份到雲端的新保護計劃。
   b. 在 **[備份選項]** 列中，按一下 **[變更]**。
   c. 在可用選項的清單中，按一下 **[實體資料運送]**。

   您可以直接備份到卸除式磁碟機，或者備份到本機或網路資料夾，然後將備份複製/移動到磁碟機。
2. [運送複寫到雲端的本機備份]

   注意事項
   保護代理程式 C21.06 版或更新版本支援此選項。

   a. 建立備份到本機或網路儲存空間的新保護計劃。
   b. 按一下 **[新增位置]**，然後選擇 **[雲端儲存空間]**。
   c. 在 **[雲端儲存空間]** 位置列中，按一下齒輪，然後選擇 **[實體資料運送]**。
3. 在 **[使用實體資料運送]** 底下，按一下 **[是]**，然後按一下 **[完成]**。
   在保護計劃中，會自動啟用 [加密] 選項，因為運送的所有備份都必須經過加密。
4. 在 **[加密]** 列中，按一下 **[指定密碼]**，然後輸入用於加密的密碼。
5. 在 **[實體資料運送]** 列中，選擇將儲存初始備份的卸除式磁碟機。

6. 按一下 **[建立]** 以儲存保護計劃。
7. 第一個備份完成後，請使用「實體資料運送」服務 Web 介面下載訂單建立工具，然後建立訂單。若要存取此 Web 介面，請登入管理入口網站，按一下 **[概觀]** > **[使用量]**，然後按一下 **[實體資料運送]** 底下的 **[管理服務]**。

   重要事項
   一旦初始完整備份完成後，後續的備份必須由相同的保護計劃執行。另一個保護計劃即使是使用相同的參數且供相同的電腦使用，仍將需要另一個「實體資料運送」週期。

8. 封裝磁碟機並將其運送至資料中心。

   重要事項
   請確認您依照實體資料運送系統管理員指南中提供的封裝指示進行。

9. 使用「實體資料運送」服務 Web 介面追蹤訂單狀態。請注意，後續的備份將會失敗，直到初始備份上傳到雲端儲存為止。

事前/事後命令

此選項可以讓您定義在執行備份程序之前和之後要自動執行的命令。

以下配置說明事前/事後命令的執行時間。

備份事前命令	備份	備份事後命令

事前/事後命令使用方式的範例：

- 在開始備份之前，從磁碟中刪除部分暫存檔案。
- 設定在每次開始備份之前要啟動的第三方防毒產品。
- 選取備份，將其複製至其他位置。因為保護計劃中設定的複寫作業會將*每個*備份均複製至之後的位置，所以此選項可能相當實用。

執行完備份後命令*之後*，代理程式才會執行複寫。

程式不支援互動式命令，即需要使用者輸入的命令 (例如[pause])。

備份事前命令

指定要在備份程序開始之前執行的命令/批次檔案

1. 啟用 **[備份之前執行命令]** 開關。
2. 在 **[命令...]** 欄位中輸入命令，或瀏覽至批次檔案。本程式不支援互動式命令，即需要使用者輸入的命令 (例如「pause」)。
3. 在 **[工作目錄]** 欄位中，指定將執行命令/批次檔案所在目錄的路徑。
4. 如有需要，請在 **[引數]** 欄位中指定該命令的執行引數。
5. 依據您要獲得的結果，選擇下表所述的相應選項。
6. 按一下**[完成]**。

核取方塊	選擇			
若命令執行失敗，則放棄備份*	已選擇	已清除	已選擇	已清除
命令執行完成後再備份	已選擇	已選擇	已清除	已清除
結果				
	預設 僅在成功執行命令後執行備份。若命令執行失敗，則放棄備份。	執行命令後執行備份，無論命令執行是否成功。	不適用	執行命令的同時執行備份，無論命令執行的結果如何。

* 命令的結束碼如果不等於零便視為失敗。

注意事項

如果指令碼因為在 Linux 中發生與所需程式庫版本相關的衝突而失敗，請在指令碼中加入以下幾行，以排除 LD_LIBRARY_PATH 和 LD_PRELOAD 環境變數：

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

備份事後命令

指定備份完成後要執行的命令/可執行檔

1. 啟用 **[備份之後執行命令]** 開關。
2. 在 **[命令...]** 欄位中輸入命令，或瀏覽至批次檔案。
3. 在 **[工作目錄]** 欄位中，指定將執行命令/批次檔案所在目錄的路徑。
4. 在 **[引數]** 欄位中指定命令執行引數 (如有需要)。
5. 如果命令成功執行與否很重要，請選取 **[若命令執行失敗，則放棄備份]** 核取方塊。命令的結束碼如果不等於零，命令就視為失敗。如果命令執行失敗，則備份狀態將設為 **[錯誤]**。

   如果未選擇核取方塊，則命令執行結果不會影響備份執行失敗或成功。您可以瀏覽 **[活動]** 標籤，以追蹤命令的執行結果。
6. 按一下**[完成]**。

資料擷取前/後命令

透過選項，您可以定義要在資料擷取之前和之後自動執行的命令(即拍攝資料快照)。資料擷取將於備份程序一開始的時候執行。

以下配置說明瞭何時在資料擷取前/後執行命令。

	<---------- 備份 ---------->				
備份事前命令	資料擷取事前命令	資料擷取	資料擷取事後命令	將資料寫入備份組	備份事後命令

與其他備份選項互動

其他備份選項可以修改資料擷取前/後執行的命令。

如果啟用了 **[多磁碟區快照]** 選項，則資料擷取前/後的命令將僅執行一次，因為將同時建立所有磁碟區快照。如果停用了 **[多磁碟區快照]** 選項，則將為每個要備份的磁碟區執行資料擷取前/後命令，因為快照是按照順序建立，而且是一個接著一個建立。

如果啟用 **[磁碟區陰影複寫服務 (VSS)]** 選項，則資料擷取前/後命令和 Microsoft VSS 作業將依照如下方式執行：

資料擷取前命令 > *VSS 暫止* > *資料擷取* > *VSS 繼續* > *資料擷取後命令*

使用資料擷取事前/事後命令，您可以暫停和繼續與 VSS 不相容的資料庫或應用程式。由於資料擷取所需時間很短，因此資料庫或應用程式的閒置時間也會縮到最短。

資料擷取事前命令

指定要在資料擷取之前執行的命令/批次檔案

1. 啟用 **[資料擷取之前執行命令]** 開關。
2. 在 **[命令...]** 欄位中輸入命令，或瀏覽至批次檔案。本程式不支援互動式命令，即需要使用者輸入的命令 (例如「pause」)。
3. 在 **[工作目錄]** 欄位中，指定將執行命令/批次檔案所在目錄的路徑。
4. 如有需要，請在 **[引數]** 欄位中指定該命令的執行引數。
5. 依據您要獲得的結果，選擇下表所述的相應選項。
6. 按一下 **[完成]**。

核取方塊	**選擇**			
若命令執行失敗，則放棄備份*	已選擇	已清除	已選擇	已清除
命令執行完成後再執行資料擷取	已選擇	已選擇	已清除	已清除
結果				
	預設 僅在成功執行命令後執行資料擷取。若命令執行失敗，則放棄備份。	執行命令後執行資料擷取，無論命令執行是否成功。	不適用	執行命令的同時執行資料擷取，無論命令執行的結果如何。

* 命令的結束碼如果不等於零便視為失敗。

注意事項
如果指令碼因為在 Linux 中發生與所需程式庫版本相關的衝突而失敗，請在指令碼中加入以下幾行，以排除 LD_LIBRARY_PATH 和 LD_PRELOAD 環境變數：

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

資料擷取事後命令

指定要在資料擷取之後執行的命令/批次檔案

1. 啟用 **[資料擷取之後執行命令]** 開關。
2. 在 **[命令...]** 欄位中輸入命令，或瀏覽至批次檔案。本程式不支援互動式命令，即需要使用者輸入的命令 (例如「pause」)。
3. 在 **[工作目錄]** 欄位中，指定將執行命令/批次檔案所在目錄的路徑。
4. 如有需要，請在 **[引數]** 欄位中指定該命令的執行引數。
5. 依據您要獲得的結果，選擇下表所述的相應選項。
6. 按一下**[完成]**。

核取方塊	**選擇**			
若命令執行失敗，則放棄備份*	已選擇	已清除	已選擇	已清除
命令執行完成後再備份	已選擇	已選擇	已清除	已清除
結果				
	預設 僅在成功執行命令後繼續備份。	執行命令後繼續備份，無論命令執行是否成功。	不適用	執行命令的同時繼續備份，無論命令執行的結果如何。

* 命令的結束碼如果不等於零便視為失敗。

排程

此選項會定義備份是完全按計劃開始或稍有延誤，以及同時要備份的虛擬機器數目。

如需有關如何設定備份排程的詳細資訊，請參閱 "按計劃執行備份" (第 373 頁)。

預設為：**在時間視窗內分配備份開始時間**。**最長延遲**：**30 分鐘**。

您可以選擇下列其中一項：

- **完全按排程開始所有備份**

  實體機器的備份會完全按照排程時間開始進行。虛擬機器則會逐個備份。
- **在時間視窗內分配開始時間**

  實體機器的備份開始時間會比原訂排程時間稍晚。每台機器的延誤的時間是隨機選定的，範圍從 0 到您指定的最大時間值。您可以想在將多台電腦備份到網路位置時使用此設定，以避免網路負載過大。每部電腦的延遲值在保護計劃套用至電腦時即已決定，並會保留相同的值，直到您編輯保護計劃並變更最大延遲值為止。

  虛擬機器則會逐個備份。
- **限制同時執行備份的數目**

  使用此選項管理在 Hypervisor 層級備份的虛擬機器平行備份 (無代理程式備份)。

  選擇此選項的保護計劃可以與相同代理程式同時操作的其他保護計劃一起執行。當您選擇此選項時，必須指定每個計劃的平行備份數量。所有計劃同時備份的電腦總數為每個代理程式 10 部。若要瞭解如何變更預設限制，請參閱 "限制同時備份的虛擬機器總數。" (第 629 頁)。

  未選擇此選項的保護計劃將依序執行備份作業，一部虛擬機器之後再另一部虛擬機器。

逐一磁區備份

此選項僅對磁碟層級備份有效。

此選項會定義是否在實體層級建立磁碟或磁碟區的精確複本。

預設為：**[已停用]**。

若啟用此選項，就會備份所有磁碟或磁碟區的磁區，包括未配置空間以及那些尚未儲存資料的磁區。所產生的備份將與正在備份的磁碟大小相同 (如果 [壓縮程度] 選項設定為 **[無]**)。在備份具有無法識別或不支援檔案系統的磁碟時，軟體會自動切換至「逐一磁區」模式。

注意事項
您無法從在逐一磁區模式下建立的備份，復原應用程式資料。

分割

此選項可讓您選取將較大備份分割成數個較小檔案的方法。

注意事項
在使用雲端儲存空間作為備份位置的保護計劃中，無法使用分割。

預設為：

- 如果備份位置為本機或網路 (SMB) 資料夾，而且備份格式為 12 版：**固定大小 - 200 GB**

  此設定允許軟體在 NTFS 檔案系統上使用大量資料，而不會因為檔案分散程度造成負面影響。
- 其他情況：**自動**

以下是可用的設定：

- **自動**

  若超過檔案系統可支援的檔案大小上限，就會切割備份。

- **固定大小**
  輸入所需的檔案大小或從下拉式清單中選擇。

工作失敗處理

已排定的保護計劃執行失敗時，或者您的電腦在備份執行時重新啟動，此選項會決定程式的行為。當保護計劃為手動啟動時，此選項無效。

若啟用此選項，程式會再次嘗試執行保護計劃。您可以指定嘗試次數，以及每次嘗試的時間間隔。嘗試成功完成或指定的嘗試次數執行後 (視哪一個先發生而定)，程式即停止嘗試。

如果停用此選項，而且您的電腦在備份執行時重新啟動，則備份作業將不會失敗。重新啟動後幾分鐘之內，備份作業將會自動繼續，並完成缺少資料的備份檔案。在此使用案例中，**[嘗試間隔]** 選項不相關。

預設為：**[啟用]**。

注意事項
此選項在鑑識備份中無效。

工作開始條件

此選項在 Windows 和 Linux 作業系統下均有效。

此選項會確定工作即將開始 (排程時間已到或發生排程中指定的事件)，但不符合條件 (或多個條件中的任何一個) 時的程式行為。如需條件的詳細資訊，請參閱 "開始條件" (第 378 頁)。

預設為：**等到符合排程中的條件。**

等到符合排程中的條件

在此設定下，條件一旦符合，排程器即開始監視條件並啟動工作。若一直不符合條件，工作就不會開始。

處理長時間未符合條件，進而延遲工作的情況有一定風險，您可設定時間間隔，在此時間間隔以後無論是否符合條件，工作都將執行。請選擇 **[無論如何，在此時間後執行工作]** 核取方塊，並指定時間間隔。工作將在條件符合或最長遲延時間後開始，視哪一個先發生而定。

略過工作執行

延遲工作可能無法接受，例如，您可能必須在指定的時間內嚴格執行工作。因此，應略過工作，而不是等待符合條件，尤其是工作較常發生時。

磁碟區陰影複製服務 (VSS)

此選項僅適用於 Windows 作業系統。

它會定義如果一或多個磁碟區陰影複製服務 (VSS) 編寫器失敗，備份是否會成功，以及哪個提供者必須通知 VSS 感知應用程式備份即將開始。

使用磁碟區陰影複製服務可確保應用程式使用的所有資料狀態一致;尤其是在備份軟體擷取資料快照時,可確保完成所有資料庫交易。而另一方面來說,資料一致性也能確保應用程式復原至正確的狀態,且在復原後隨即可正常運作。

快照僅用於備份作業期間,而且在備份作業完成後會自動刪除。不會保留任何暫存檔。

您也可以使用資料擷取事前/事後命令來確保資料備份的狀態一致。例如,指定資料擷取事前命令可暫停資料庫並清除所有快取,以確保完成所有交易,然後指定資料擷取事後命令可在擷取快照後繼續資料庫作業。

注意事項
系統將不會備份在 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** 登錄機碼中指定的檔案與資料夾。特別是,離線的 Outlook 資料檔案 (.ost) 將不會備份,因為它們已經在此鍵值中指定於 **OutlookOST**。

忽略失敗的 VSS 編寫器

您可以選擇下列其中一項:

- **忽略失敗的 VSS 編寫器**
  透過此選項,即是一或多個 VSS 編寫器失敗,備份也會成功。

  重要事項
  如果應用程式專用的編寫器失敗,應用程式感知備份一律也會失敗。例如,如果您正在對 SQL Server 資料進行應用程式感知備份,而且 **SqlServerWriter** 失敗,則備份作業也將失敗。

  啟用此選項時,將會對 VSS 快照連續嘗試三次。
  第一次嘗試時,需要所有 VSS 編寫器。如果此次嘗試失敗,將會重複嘗試。如果第二次嘗試也失敗,失敗的 VSS 編寫器將排除在備份作業的範圍之外,然後會進行第三次嘗試。如果第三次嘗試成功,備份將會完成,並出現有關失敗的 VSS 編寫器的警告。如果第三次嘗試不成功,備份將會失敗。

- **需要所有 VSS 編寫器皆處理成功**
  如果任何 VSS 編寫器失敗,備份作業也將失敗。

選擇快照提供者

您可以選擇下列其中一項:

- **自動選擇快照提供者**
  自動選擇硬體快照提供者、軟體快照提供者或 Microsoft 軟體陰影複製提供者。

  注意事項
  建議您盡可能使用自動選擇快照提供者。

- **使用 Microsoft 軟體陰影複製提供者**

如果您有其他不想使用的協力廠商 VSS 提供者，且受保護的工作負載不包含叢集共用磁碟區，則建議您強制使用 Microsoft 軟體陰影複製提供者。

警告！
僅在明確需要使用 Microsoft 軟體陰影複製提供者時，才強制使用它，因為在叢集共用磁碟區和 Microsoft 軟體陰影複製提供者不支援的其他磁碟區環境中，可能會導致備份失敗。

啟用 VSS 完整備份

如果啟用此選項，Microsoft Exchange Server 及其他 VSS 感知應用程式 (除 Microsoft SQL Server 外) 的記錄將於每次成功進行完整、增量或差異磁碟層級備份後遭到截斷。

預設為：**[已停用]**。

在以下情況中，請將此選項保持停用：

- 如果您使用 Exchange 用代理程式或第三方軟體來備份 Exchange Server 資料。這是因為記錄截斷會干擾連續交易記錄備份。
- 如果您使用第三方軟體來備份 SQL Server 資料。這是因為第三方軟體會將產生的磁碟層級備份當作其特有的完整備份。因此，下一次的 SQL Server 資料差異備份將會失敗。備份將會持續失敗，直到第三方軟體下一次建立其特有的完整備份為止。
- 如果電腦上有其他的 VSS 感知應用程式正在執行，且您因故需要保留其記錄。

重要事項
啟用此選項並不會造成 Microsoft SQL Server 記錄截斷。若要於備份後截斷 SQL Server 記錄，請啟用 [記錄截斷] 備份選項。

虛擬機器的磁碟區陰影複製服務 (VSS)

此選項會判斷是否擷取虛擬機器的靜止快照。

預設為：**[啟用]**。

停用此選項時，會擷取非靜止快照。虛擬機器會以「衝突一致性」狀態來進行備份。

啟用此選項時，則會完成虛擬機器中執行的所有 VSS 感知應用程式的交易，然後擷取靜止快照。

如果在 [錯誤處理] 選項中指定重新嘗試次數後無法擷取靜止快照，且已啟用應用程式備份，則備份將會失敗。

如果在 [錯誤處理] 選項中指定重新嘗試次數後無法擷取靜止快照，且已停用應用程式備份，則會建立當機一致的備份。若要使備份失敗而不是建立當機一致的備份，請選擇 **[如果無法擷取靜止快照，備份將會失敗]** 核取方塊。

下表摘要說明可用的設定及其結果。

設定	已成功擷取靜止快照		未擷取靜止快照	
	已啟用應用程式備份	已停用應用程式備份	已啟用應用程式備份	已停用應用程式備份
已啟用 **[虛擬機器的磁碟區陰影複製服務 (VSS)]** 未選擇 **[如果無法擷取靜止快照，備份將會失敗]**	已擷取靜止快照。已建立應用程式一致的備份。	已擷取靜止快照。已建立應用程式一致的備份。	備份失敗。	已擷取非靜止快照。已建立當機一致的備份。
已啟用 **[虛擬機器的磁碟區陰影複製服務 (VSS)]** 已選擇 **[如果無法擷取靜止快照，備份將會失敗]**	已擷取靜止快照。已建立應用程式一致的備份。	已擷取靜止快照。已建立應用程式一致的備份。	備份失敗。	備份失敗。
已停用 **[虛擬機器的磁碟區陰影複製服務 (VSS)]**	已擷取非靜止快照。已建立當機一致的備份。	已擷取非靜止快照。已建立當機一致的備份。	已擷取非靜止快照。已建立當機一致的備份。	已擷取非靜止快照。已建立當機一致的備份。

啟用 **[虛擬機器的磁碟區陰影複製服務 (VSS)]** 也會在備份的虛擬機器上，觸發您可能擁有的凍結前和解除凍結後指令碼。如需有關這些指令碼的詳細資訊，請參閱 "自動執行凍結前和解除凍結後指令碼" (第 621 頁)。

若要擷取靜止快照，備份軟體會分別使用 VMWare Tools、Hyper-V 整合服務、Virtuozzo Guest Tools、Red Hat Virtualization Guest Tools 或 QEMU Guest Tools，將 VSS 套用到虛擬機器內。

注意事項

對於 Red Hat Virtualization (oVirt) 虛擬機器，建議您安裝 QEMU Guest Tools 而非 Red Hat Virtualization Guest Tools。有些 Red Hat Virtualization Guest Tools 版本不支援應用程式一致的快照。

此選項不會影響 Scale Computing HC3 虛擬機器。對於它們而言，靜止取決於 Scale Tools 是否安裝在虛擬機器上。

每週備份

此選項會判斷在保留規則與備份配置中，哪些備份應為「每週」進行。「每週」備份是每一週開始後所建立的第一個備份。

預設為：**[週一]**。

Windows 事件日誌

此選項僅在 Windows 作業系統下有效。

此選項定義代理程式是否必須在 Windows 的應用程式事件記錄檔中記錄備份作業事件 (若要查看此記錄，請執行 eventvwr.exe 或選擇 **[控制台]** > **[系統管理工具]** > **[事件檢視器]**)。您可以篩選要記錄的事件。

預設為：**[已停用]**。

復原

復原快速鍵清單

下表摘述可用的復原方法。使用此表格來選擇最適合您需求的復原方法。

注意事項

您無法在 Cyber Protect 主控台中，為 [合規] 模式下的租用戶復原備份。如需有關如何復原此類備份的詳細資訊，請參閱 "在合規模式下復原租用戶的備份" (第 981 頁)。

復原內容	復原方法
實體機器 (Windows 或 Linux)	使用 Cyber Protect 主控台 使用可開機媒體
實體機器 (Mac)	使用可開機媒體
虛擬機器 (VMware、Hyper-V、Red Hat Virtualization (oVirt) 或 Scale Computing HC3)	使用 Cyber Protect 主控台 使用可開機媒體
虛擬機器或容器 (Virtuozzo、Virtuozzo Hybrid Server 或 Virtuozzo Hybrid Infrastructure)	使用 Cyber Protect 主控台
ESXi 設定	使用可開機媒體
檔案/資料夾	使用 Cyber Protect 主控台 從雲端儲存下載檔案 使用可開機媒體 從本機備份解壓縮檔案
系統狀態	使用 Cyber Protect 主控台
SQL 資料庫	使用 Cyber Protect 主控台
Exchange 資料庫	使用 Cyber Protect 主控台

Exchange 信箱	使用 Cyber Protect 主控台
網站	使用 Cyber Protect 主控台
Microsoft 365	
信箱 (本機 Microsoft 365 用代理程式)	使用 Cyber Protect 主控台
信箱 (雲端 Microsoft 365 用代理程式)	使用 Cyber Protect 主控台
公用資料夾	使用 Cyber Protect 主控台
OneDrive 檔案	使用 Cyber Protect 主控台
SharePoint Online 資料	使用 Cyber Protect 主控台
Google Workspace	
信箱	使用 Cyber Protect 主控台
Google 雲端硬碟檔案	使用 Cyber Protect 主控台
共用磁碟機檔案	使用 Cyber Protect 主控台

跨平台復原

跨平台復原適用於整部電腦的備份，以及包含作業系統之磁碟的備份。

在下列情況下，會執行跨平台復原：

- 備份是由其中一種代理程式建立，但是由另一種代理程式復原。
- 代理程式型備份是在 Hypervisor 層級復原 (無代理程式復原)，或者無代理程式備份是由代理程式復原 (代理程式型復原)。
- 備份會復原至相異硬體 (包括虛擬硬體)。

注意事項

當您執行跨平台復原時，可能無法正確復原部分週邊裝置，例如印表機。

下表顯示跨平台復原的幾個範例。

跨平台復原	
無代理程式備份	代理程式型復原
代理程式型備份	無代理程式復原

跨平台復原	
由 Windows 用代理程式備份	由 VMware 用代理程式復原
由 VMware 用代理程式備份	由 Hyper-V 用代理程式復原
由安裝在 VMware ESXi 虛擬機器上的 Windows 用代理程式備份 (代理程式型)	由相同 VMware ESXi 主機上的 VMware 用代理程式復原 (無代理程式)
由 Windows 用代理程式備份	由安裝在具有相異硬體的電腦上的 Windows 用代理程式復原
實體機器備份	復原為虛擬機器

Mac 使用者注意事項

- 自 10.11 El Capitan 版本開始，為保護特定系統檔案、資料夾和處理程序，將使用延伸檔案屬性 com.apple.rootless 標記上述項目。此功能稱為「系統完整性保護 (SIP)」。受保護的檔案包括預先安裝的應用程式，以及 /system、/bin、/sbin、/usr 中大部分的資料夾。

  在作業系統下執行復原時，使用者將無法覆寫受保護的檔案和資料夾。若您需要覆寫受保護的檔案，請在可開機媒體的環境下執行復原。
- 從 macOS Sierra 10.12 開始，可透過雲端儲存功能將很少用到的檔案移動至 iCloud。這些檔案的小使用量會存於檔案系統。這些使用量會進行備份，而不是原始檔案。

  將使用量復原至原始位置時，其會與 iCloud 同步，原始檔案即可用。將使用量復原至其他位置時，便無法同步，原始檔案不可用。

安全復原

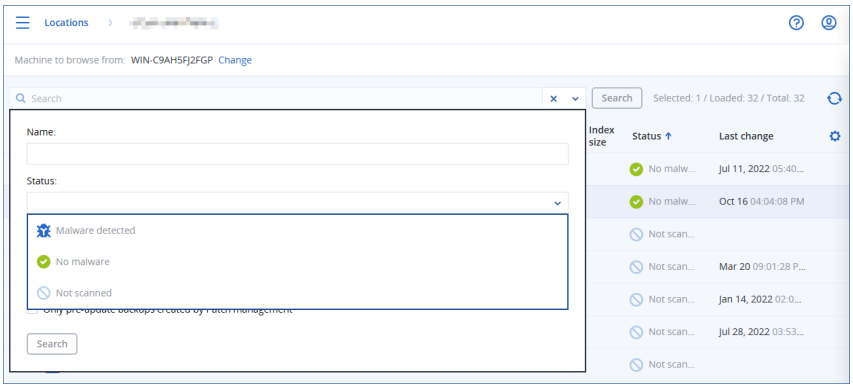
搭配 Windows 工作負載的 **[整部電腦]** 或 **[磁碟/磁碟區]** 備份使用安全復原時，即使備份中包含受感染的檔案，還是可以確保您只復原無惡意軟體的資料。

在安全復原作業期間，會自動掃描備份中是否有惡意軟體。接著，保護代理程式會在目標工作負載上復原備份，並刪除任何受感染的檔案。因此會復原無惡意軟體的備份。

此外，備份會獲指派下列其中一個狀態：

- 偵測到惡意程式碼
- 無惡意程式碼
- 未掃描

您可以使用狀態篩選備份存檔。



限制

- 已安裝保護代理程式的實體和虛擬 Windows 機器支援安全復原。
- **[整部電腦]** 和 **[磁碟/磁碟區]** 備份支援安全復原。
- 只會掃描 NTFS 磁碟區中是否有惡意軟體。非 NTFS 磁碟區將會在不經過防惡意軟體掃描的情況下復原。
- 在存檔中，連續資料保護 (CDP) 備份不支援安全復原。若要從 CDP 備份復原資料，請執行額外的 **[檔案/資料夾]** 復原作業。如需有關 CDP 備份的詳細操作，請參閱 "連續資料保護 (CDP)" (第 363 頁)。

復原電腦

復原實體電腦

本節說明使用 Web 介面來復原實體機器。

如果您要復原下列項目，請使用可開機媒體，而不要使用 Web 介面：

- 執行 macOS 的電腦
- 在合規模式下租用戶中的電腦
- 裸機或離線電腦上的任何作業系統
- 邏輯磁碟區 (Linux 中邏輯磁碟區管理器所建立的磁碟區) 的結構。媒體可讓您自動重新建立邏輯磁碟區結構。

注意事項
您無法將 Intel Mac 的磁碟層級備份復原至使用 Apple 晶片處理器的 Mac，反之亦然。您可以復原檔案和資料夾。

如果要復原實體機器

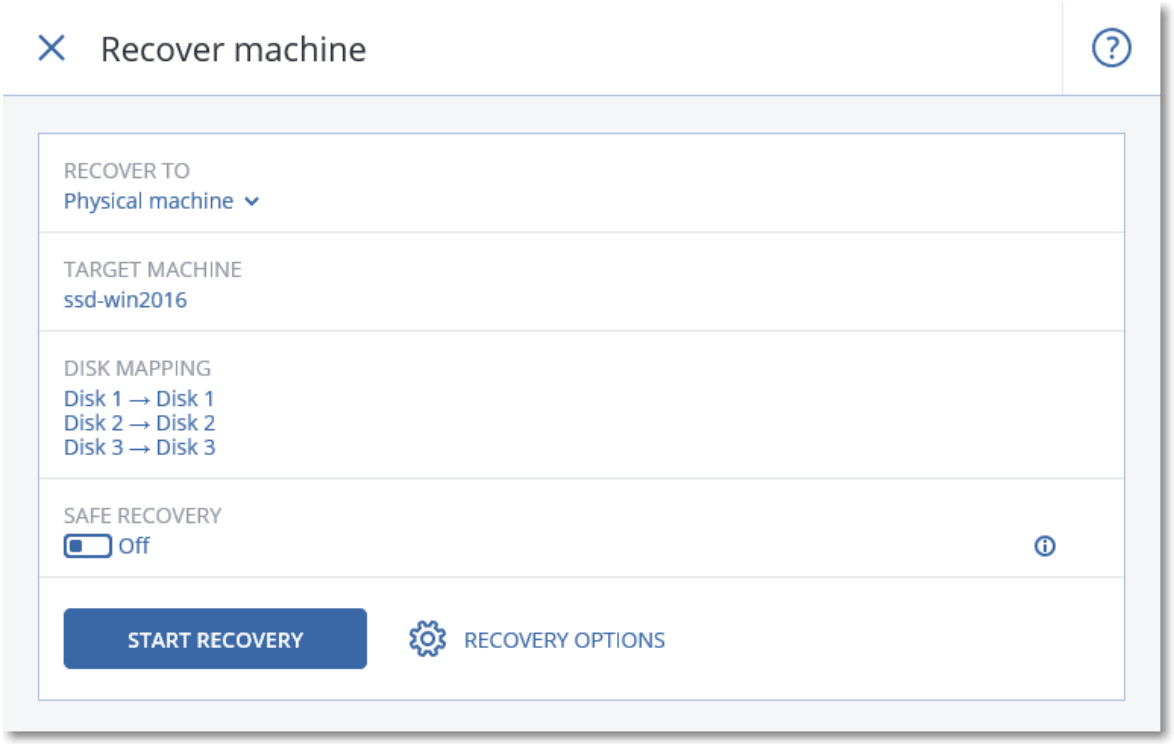
1. 選擇已備份的電腦。
2. 按一下 **[復原]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。
   如果電腦處於離線狀態，復原點就不會顯示。執行下列任何一項作業：

- 如果備份位置是雲端或共用儲存 (即可被其他代理程式存取), 按一下 **[選擇電腦]**, 選擇在線上的目標電腦, 然後選擇復原點。
- 在 [備份儲存] 索引標籤上選擇復原點。
- 如 < 使用可開機媒體復原磁碟 > 所述來復原電腦。

4. 按一下**[復原]** > **[整部機器]**。

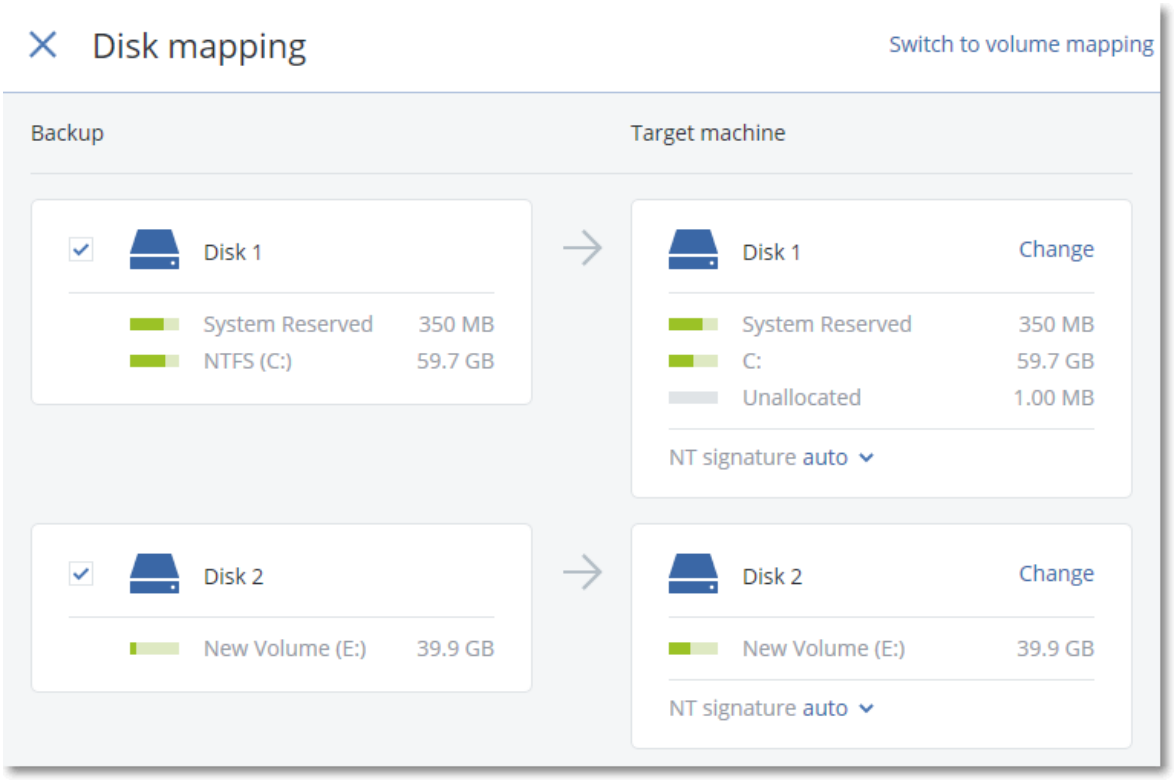
   軟體會自動將備份的磁碟對應到目標電腦的磁碟。

   如果要復原至其他實體機器, 請按一下 **[目標電腦]**, 然後選擇在線上的目標電腦。



5. 如果您不滿意對應結果, 或磁碟對應失敗, 可以按一下 **[磁碟區對應]** 手動重新對應磁碟。

   該對應區段使您還可以選擇要復原的個別磁碟或磁碟區。您可以使用右上角的 **[切換至...]** 連結, 在復原磁碟和磁碟區之間切換。



6. [僅適用於已安裝保護代理程式的 Windows 電腦] 啟用 **[安全復原]** 開關以確保復原的資料中沒有惡意軟體。如需有關安全復原如何運作的詳細資訊，請參閱 "安全復原" (第 444 頁)。
7. 按一下 **[開始復原]**。
8. 確認您要以磁碟的備份版本來覆寫磁碟。選擇是否要自動重新啟動電腦。

復原進度會顯示在 **[活動]** 索引標籤上。

實體機器到虛擬

您可以在其中一個支援的 Hypervisor 上，將實體機器復原至虛擬機器。這也是將實體機器移轉至虛擬機器的機制。如需有關支援的 P2V 移轉路徑的詳細資訊，請參閱「電腦移轉」。

本節說明使用 Web 介面將實體機器復原至虛擬機器。至少在 Acronis Management Server 中為相關的 Hypervisor 安裝並註冊一個代理程式，才能執行此作業。例如，復原至 VMware ESXi 需要在環境中至少安裝並註冊一個 VMware 用代理程式；復原至 Hyper-V 則需要在環境中至少安裝並註冊一個 Hyper-V 用代理程式。

在合規模式下，透過 Web 介面復原不適用於租用戶。

注意事項

您無法將 macOS 虛擬機器復原至 Hyper-V 主機，因為 Hyper-V 不支援 macOS。您可以將 macOS 虛擬機器復原至 Mac 硬體上安裝的 VMware 主機。

此外，您無法將 macOS 實體機器的備份當作虛擬機器復原。

如果要將實體機器復原為虛擬機器

1. 選擇已備份的電腦。
2. 按一下 **[復原]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。

   如果電腦處於離線狀態，復原點就不會顯示。執行下列任何一項作業：

   - 如果備份位置是雲端或共用儲存 (即可被其他代理程式存取)，按一下 **[選擇電腦]**，選擇在線上的電腦，然後選擇復原點。
   - 在 [備份儲存] 索引標籤上選擇復原點。
   - 如 < 使用可開機媒體復原磁碟 > 所述來復原電腦。
4. 按一下 **[復原]** > **[整部機器]**。
5. 在 **[復原至]** 中選擇 **[虛擬機器]**。
6. 按一下 **[目標電腦]**。
   a. 選擇 Hypervisor。

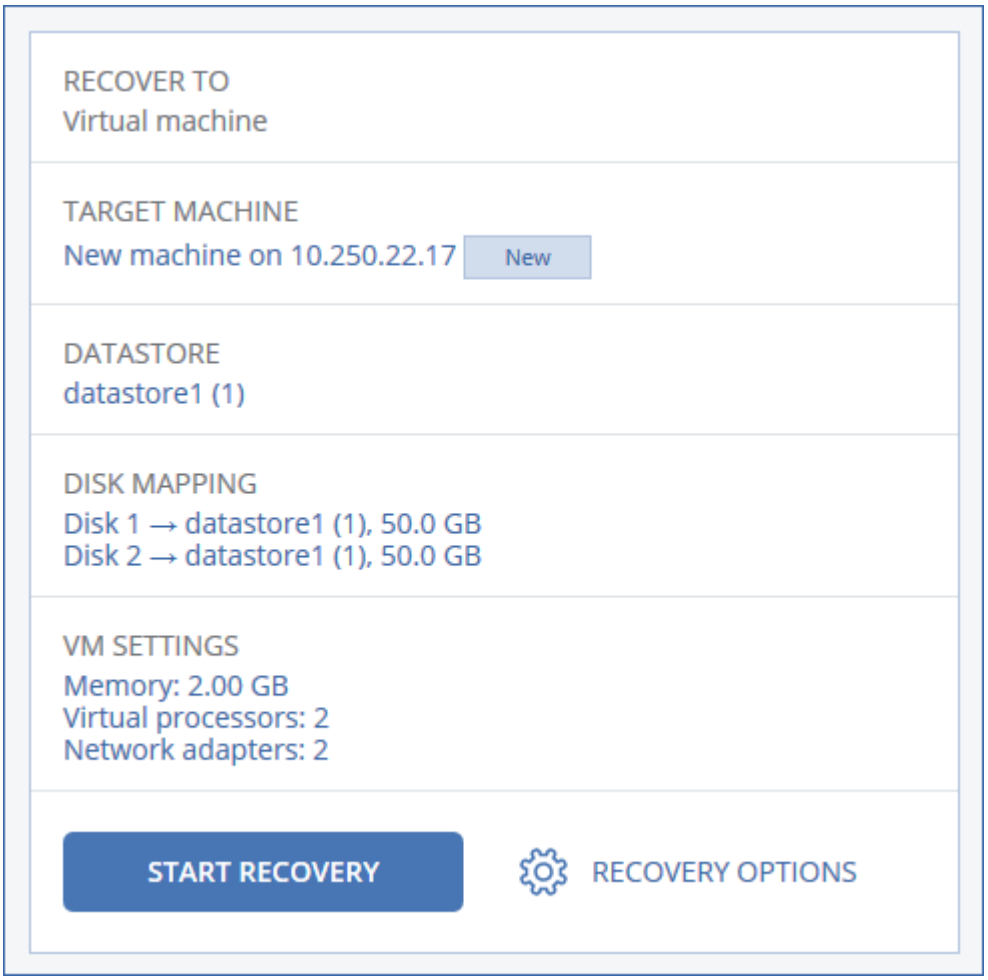
   注意事項
   必須至少在 Acronis Management Server 中為該 Hypervisor 安裝並註冊一個代理程式。

   b. 選擇主機並指定新電腦名稱，或選擇現有目標電腦。最好選擇新電腦，這樣目標電腦的磁碟組態就不需完全符合備份中的磁碟組態。
   c. 選擇主機並指定新電腦名稱，或選擇現有目標電腦。
   d. 按一下 **[確定]**。
7. [若是 Virtuozzo Hybrid Infrastructure] 按一下 **[VM 設定]** 以選擇 **[類別]**。您可以選擇性地變更記憶體大小、處理器數量，以及虛擬機器的網路連線。

   注意事項
   選擇類別是 Virtuozzo Hybrid Infrastructure 的必要步驟。

8. [選用] 設定其他復原選項：
   - [不適用於 Virtuozzo Hybrid Infrastructure] 按一下 **[資料存放區]** (ESXi)，或按一下 **[路徑]** (Hyper-V)，然後選擇虛擬機器的資料存放區 (儲存空間)。
   - 按一下 **[磁碟對映]** 為每個虛擬磁碟選擇資料存放區 (儲存)、介面以及佈建模式。該對映區段使您還可以選擇要復原的個別磁碟。

     若是 Virtuozzo Hybrid Infrastructure，您僅能選擇目標磁碟的儲存原則。方法是，選擇所需的目標磁碟，然後按一下 [變更]。在開啟的刀鋒視窗中，按一下齒輪圖示、選擇儲存原則，然後按一下 [完成]。
   - [若是 VMware ESXi、Hyper-V 和 Red Hat Virtualization/oVirt] 按一下 **[VM 設定]** 以變更記憶體大小、處理器數量，以及虛擬機器的網路連線。



9. [僅適用於已安裝保護代理程式的 Windows 電腦] 啟用 **[安全復原]** 開關以確保復原的資料中沒有惡意軟體。如需有關安全復原如何運作的詳細資訊，請參閱 "安全復原" (第 444 頁)。
10. 按一下 **[開始復原]**。
11. 當復原到現有虛擬機器時，請確認您要覆寫磁碟。

復原進度會顯示在 **[活動]** 索引標籤上。

復原虛擬機器

您可以從其備份復原虛擬機器。

注意事項
您無法在 Cyber Protect 主控台中，為 [合規] 模式下的租用戶復原備份。如需有關如何復原此類備份的詳細資訊，請參閱 "在合規模式下復原租用戶的備份" (第 981 頁)。

必要條件

- 復原至虛擬機器時，此虛擬機器必須為停止狀態。軟體預設不會顯示提示，即停止電腦。復原完成後，您必須手動啟動電腦。您可以使用 VM 電源管理復原選項來變更預設行為 (按一下 **[復原選項]** > **[VM 電源管理]**)。

程序

1. 執行下列其中一項操作：
   - 選擇已備份的電腦，按一下**復原**，然後選擇復原點。
   - 在 [備份儲存] 索引標籤上選擇復原點。
2. 按一下**[復原]** > **[整部機器]**。
3. 如果您想要復原到實體機器，請在**復原至**中選擇**實體機器**。否則，請跳過此步驟。

   只有在目標電腦的磁碟組態完全符合備份中的磁碟組態時，才能復原至實體機器。

   在此情況下，請繼續在「實體機器」中的步驟 4。否則，我們建議您使用可開機媒體來執行 V2P 移轉。
4. [選用] 軟體預設會自動選擇原始電腦做為目標電腦。若要復原到另一部虛擬機器，請按一下**目標機器**然後進行以下操作：
   a. 選擇 Hypervisor (**[VMware ESXi]**、**[Hyper-V]**、**[Virtuozzo]**、**[Virtuozzo Hybrid Infrastructure]**、**[Scale Computing HC3]** 或 **[oVirt]**)。

      只有 Virtuozzo 虛擬機器可復原至 Virtuozzo。如需 V2V 移轉的詳細資訊，請參閱「電腦移轉」。

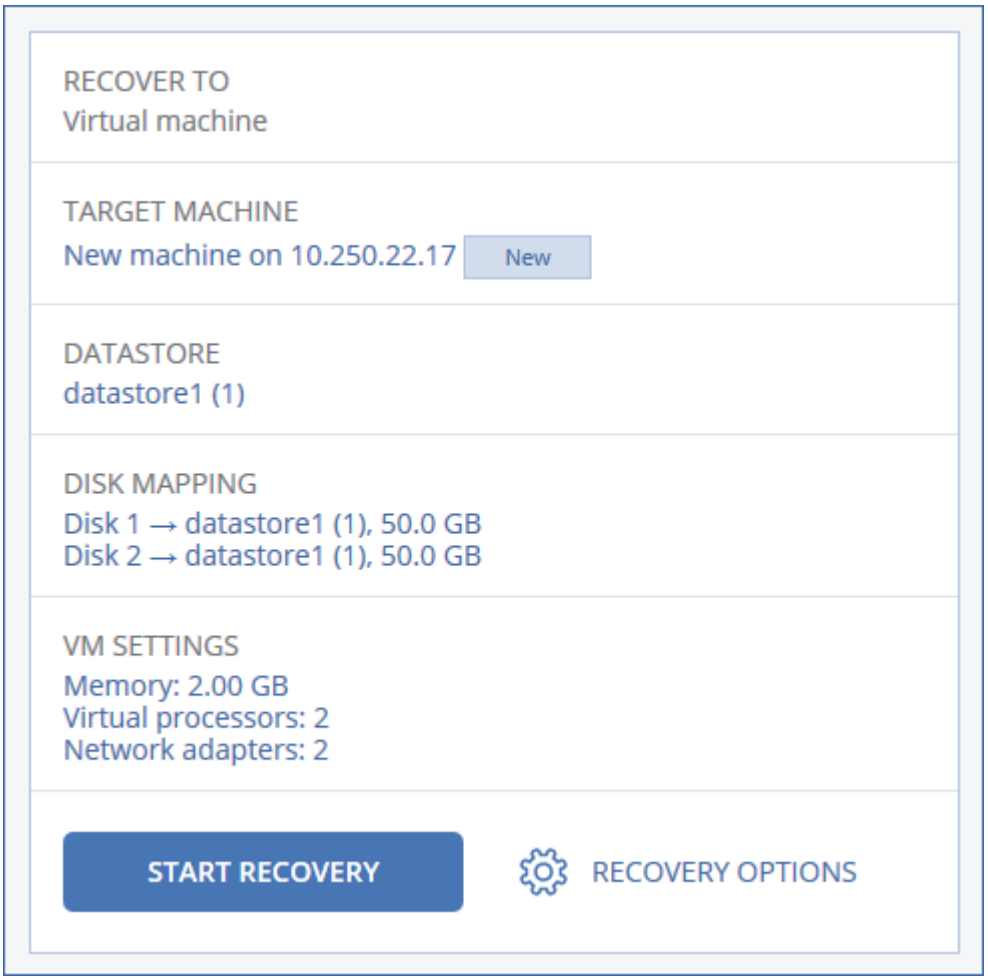
      請注意，選擇 **Microsoft Azure** 作為目標時，您可以選擇相關的 Azure 訂閱、區域和資源群組。
   b. 選擇主機並指定新電腦名稱，或選擇現有目標電腦。
   c. 選擇主機並指定新電腦名稱，或選擇現有目標電腦。
   d. 按一下 **[確定]**。
5. 設定您需要的其他復原選項。
   - [選用] [不適用於 Virtuozzo Hybrid Infrastructure 和 Scale Computing HC3] 若要選擇虛擬機器的資料存放區，按一下 **[資料存放區]** (ESXi)、**[路徑]** (Hyper-V 和 Virtuozzo)，或 **[儲存網域]** (Red Hat Virtualization (oVirt))，然後選擇虛擬機器的資料存放區 (儲存空間)。
   - [選用] 若要檢視每個虛擬磁碟的資料存放區 (儲存空間)、介面以及佈建模式，按一下 **[磁碟對應]**。除非您要復原 Virtuozzo 容器或 Virtuozzo Hybrid Infrastructure 虛擬機器，否則您可以變更這些設定。

     若是 Virtuozzo Hybrid Infrastructure，您僅能選擇目標磁碟的儲存原則。方法是，選擇所需的目標磁碟，然後按一下 **[變更]**。在開啟的刀鋒視窗中，按一下齒輪圖示、選擇儲存原則，然後按一下 **[完成]**。

     該對映區段使您還可以選擇要復原的個別磁碟。

     若是 Microsoft Azure，您可以選擇相關的儲存體類型 (本機備援儲存體 (LRS) 或區域備援儲存體 (ZRS))，以變更每個目標磁碟的儲存體類型。
   - [選用] [適用於 VMware ESXi、Hyper-V 和 Virtuozzo] 若要變更記憶體大小、處理器數量，以及虛擬機器的網路連線，請按一下 **[VM 設定]**。

     [適用於 Microsoft Azure] 若要變更可用性類型和區域、記憶體大小以及虛擬機器的網路連線 (包括子網路和安全性群組)，請按一下 **[VM 設定]**。
   - [若是 Virtuozzo Hybrid Infrastructure] 若要變更虛擬機器的記憶體大小和處理器數量，請選擇 **[類別]**。



6. [僅適用於已安裝保護代理程式的 Windows 電腦] 啟用 **[安全復原]** 開關以確保復原的資料中沒有惡意軟體。如需有關安全復原如何運作的詳細資訊，請參閱 "安全復原" (第 444 頁)。
7. 按一下 **[開始復原]**。
8. 當復原到現有虛擬機器時，請確認您要覆寫磁碟。

復原進度會顯示在 **[活動]** 索引標籤上。

使用重新啟動復原

Windows 和 Linux 電腦支援需要重新啟動的復原。

您可以選擇要自動重新啟動電腦還是為其指派 **[需要互動]** 狀態。復原後的作業系統會自動連線。

當您復原下列項目時需要重新啟動：

- 作業系統

  例如，當您復原整部電腦或電腦的系統磁碟區時。
- 加密的磁碟區

  例如，當您復原使用 BitLocker 加密的磁碟區或使用 CheckPoint 加密的磁碟區時。

重要事項
已備份的加密磁碟區會被當作未加密復原。

系統會在復原後的電腦上自動準備復原環境。當環境準備就緒時，電腦會重新啟動，然後復原環境便會開啟。復原完成後，作業系統隨即啟動。

復原環境

需要重新啟動的復原使用 Linux 復原環境。

注意事項
復原具有加密系統磁碟區的電腦要求相同電腦上至少有一個未加密的磁碟區。

磁碟空間需求

復原環境需要具備用於暫存檔的磁碟空間。需求取決於復原的電腦。

下表摘要說明可用的選項。

開機模式	具有未加密系統磁碟區的電腦	具有加密系統磁碟區的電腦
BIOS	系統磁碟區上有 200 MB	未加密的磁碟區上有 400 MB
UEFI	EFI 系統磁碟分割 (ESP) 上有 200 MB	以下之一： • EFI 系統磁碟分割 (ESP) 上有 400 MB • EFI 系統磁碟分割 (ESP) 上有 200 MB，在開機過程中可存取的未加密磁碟分割上有 200 MB

限制

- 在復原之前，您必須鎖定所有加密的非系統磁碟區。您可以透過開啟位於磁碟區上的檔案來鎖定該磁碟區。如果未鎖定磁碟區，復原將繼續而不重新啟動，且作業系統可能無法辨識該磁碟區。

  您不需要鎖定加密的系統磁碟區。

疑難排解

如果復原失敗且在重新啟動後顯示 [無法從磁碟分割取得檔案] 錯誤，請停用 [安全開機]。如需詳細資訊，請參閱 Microsoft 文件中的停用安全開機。

使用可開機媒體復原磁碟

如需有關如何建立可開機媒體的資訊，請參閱 "建立實體可開機媒體" (第 635 頁)。

注意事項
您無法將 Intel Mac 的磁碟層級備份復原至使用 Apple 晶片處理器的 Mac，反之亦然。您可以復原檔案和資料夾。

使用可開機媒體復原磁碟

1. 使用可開機媒體將目標電腦開機。
2. [僅在復原 Mac 時] 若您要將 APFS 格式化的磁碟/磁碟區復原至非原始電腦或裸機，則會手動重新建立原始磁碟組態：
   a. 按一下 **[磁碟公用程式]**。
   b. 清除目標磁碟並將其格式化為 APFS。如需說明，請參閱 https://support.apple.com/en-us/HT208496#erasedisk。
   c. 重新建立原始磁碟組態。如需說明，請參閱 https://support.apple.com/guide/disk-utility/add-erase-or-delete-apfs-volumes-dskua9e6a110/19.0/mac/10.15。
   d. 按一下 **[磁碟公用程式]** > **[結束磁碟公用程式]**。
3. 按一下 **[在本機管理此電腦]** 或按兩次 **[救援可開機媒體]**，視您使用的媒體類型而定。
4. 如果您的網路中已啟用 Proxy 伺服器，請按一下 **[工具]** > **[Proxy 伺服器]**，然後指定 Proxy 伺服器主機名稱/IP 位址、連接埠和認證。否則，請跳過此步驟。
5. [選用] 復原 Windows 或 Linux 時，按一下 **[工具]** > **[在 Cyber Protection 服務中註冊媒體]**，然後指定您在下載媒體時取得的註冊權杖。如果您這麼做，您將不需要輸入認證或註冊碼，就可以存取雲端儲存空間，如步驟 8 所述。
6. 在歡迎畫面上，按一下 **[復原]**。
7. 按一下 **[選擇資料]**，然後按一下 **[瀏覽]**。
8. 指定備份位置：
   - 若要從雲端儲存進行復原，請選擇 **[雲端儲存]**。輸入已指派備份電腦之帳戶的認證。
     復原 Windows 或 Linux 時，您可以選擇要求註冊碼，並使用該註冊碼代替認證。按一下 **[使用註冊碼]** > **[要求代碼]**。軟體將會顯示註冊連結和註冊碼。您可以複製註冊連結和註冊碼，並在另一部電腦上執行註冊步驟。註冊碼的有效期限為一小時。
   - 若要從本機或網路資料夾進行復原，請瀏覽至 **[本機資料夾]** 或 **[網路資料夾]** 下的資料夾。
   - 若要從公有雲端儲存空間 (例如 Microsoft Azure、Amazon S3、Wasabi 或 S3 相容儲存空間) 上的備份位置復原，請先按一下 **[Cyber Protection 服務中的註冊媒體]**，然後使用 Web 介面設定復原。如需有關透過 Web 介面遠端管理媒體的詳細資訊，請參閱 "可開機媒體的相關遠端作業" (第 650 頁)。

   按一下 **[確定]** 以確認您的選擇。
9. 選擇您要從中復原資料的備份。如果看到提示，請輸入備份的密碼。
10. 在 **[備份內容]** 中，選擇您要復原的磁碟。按一下 **[確定]** 以確認您的選擇。
11. 在 **[復原目標位置]** 下，軟體會自動將已選擇的磁碟對應至目標磁碟。
    如果對應不成功，或如果您不滿意對應結果，您可以手動重新對應磁碟。

    注意事項
    變更磁碟配置可能會影響作業系統的開機能力。除非您有十足的把握會成功，否則請使用原始電腦的磁碟配置。

12. [復原 Linux 時] 如果備份電腦有邏輯磁碟區 (LVM)，而您想要重現原始的 LVM 架構：
    a. 請確保目標電腦磁碟數目和每個磁碟的容量等於或超過原始電腦，然後按一下 **[套用 RAID/LVM]**。
    b. 檢閱磁碟區結構，然後按一下 **[套用 RAID/LVM]** 以建立磁碟區結構。

13. [選用] 按一下 **[復原選項]** 以指定額外的設定。
14. 按一下**[確定]**開始復原。

使用 Universal Restore

最新的作業系統在復原至相異硬體 (包括 VMware 或 Hyper-V 平台) 時，會保持為可開機狀態。如果復原的作業系統無法開機，請使用 Universal Restore 工具來更新對作業系統啟動極為關鍵的驅動程式和模組。

Universal Restore 適用於 Windows 和 Linux。

套用 Universal Restore

1. 從可開機媒體啟動電腦。
2. 按一下 **[套用 Universal Restore]**。
3. 如果電腦上有多個作業系統，系統會提示您選擇要套用 Universal Restore 的目標作業系統。
4. [僅適用於 Windows] 進行其他設定。
5. 按一下 **[確定]**。

Windows 中的 Universal Restore

準備

準備驅動程式

套用 Universal Restore 至 Windows 作業系統前，請先確定已備妥新 HDD 控制器與晶片組的驅動程式。這些驅動程式對開機作業系統至關重要。使用硬體供應商提供的 CD 或 DVD，或者從供應商網站下載驅動程式。驅動程式檔案的副檔名應該是 *.inf。如果下載的驅動程式格式為 *.exe、*.cab 或 *.zip，請使用第三方應用程式進行解壓縮。

最佳的方法是將您組織中使用的所有硬體驅動程式，儲存在按裝置類型或按硬體組態分類的單個存放庫中。您可將存放庫之副本保留在 DVD 或快閃磁碟機上；挑選某些驅動程式並將它們新增至可開機媒體；為您的每個伺服器建立帶有必要驅動程式 (以及必要網路組態) 的自訂可開機媒體。或者，您也可以在每次使用 Universal Restore 時，直接指定存放庫路徑。

檢查是否能在可開機環境中存取驅動程式

請確保您在可開機媒體下工作時，能夠使用驅動程式來存取裝置。如果裝置在 Windows 中可供使用，但無法被 Linux 式媒體偵測到，請使用 WinPE 式媒體。

Universal Restore 設定

驅動程式自動搜尋

指定程式將在何處搜尋硬體抽象層 (HAL)、硬碟控制器驅動程式和網路卡驅動程式：

- 如果驅動程式位於供應商的光碟或其他卸除式媒體上，請開啟 **[搜尋卸除式媒體]**。
- 如果驅動程式位於網路資料夾或可開機媒體上，請按一下 **[新增資料夾]** 指定資料夾路徑。

此外，Universal Restore 將搜尋 Windows 預設驅動程式存放資料夾。其位置是由登錄值 **DevicePath** 所決定，您可以在登錄機碼 **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion** 中找到該值。此存放資料夾通常是 WINDOWS/inf。

Universal Restore 將在所有指定資料夾的子資料夾中執行遞迴搜尋，找出所有可用且最適合的 HAL 和硬碟控制器驅動程式，並將它們安裝至系統。Universal Restore 也會搜尋網路卡驅動程式；已找到的驅動程式路徑將由 Universal Restore 傳輸至作業系統。如果硬體有多個網路介面卡，則 Universal Restore 將嘗試設定所有卡的驅動程式。

仍要安裝的大型存放驅動程式

下列情況需要此設定：

- 硬體配備特定的大型存放控制器，例如 RAID (尤其是 NVIDIA RAID) 或光纖通道介面卡。
- 您將系統移轉至使用 SCSI 硬碟控制器的虛擬機器。使用虛擬化軟體搭售的 SCSI 驅動程式，或是透過軟體製造商網站下載最新版的驅動程式。
- 如果自動驅動程式搜尋無法協助啟動系統，

按一下 **[新增驅動程式]**，指定適當的驅動程式。即使程式找到更合適的驅動程式，仍會安裝此處定義的驅動程式，但會發出相應的警告。

Universal Restore 程序

指定所需的設定後，按一下 **[確定]**。

如果 Universal Restore 在指定的位置找不到相容的驅動程式，會顯示問題裝置提示。執行下列其中一項操作：

- 將驅動程式新增至任何先前指定的任一個位置，然後按一下 **[重試]**。
- 如果您不記得位置，按一下 **[忽略]** 繼續程序。如果結果不甚理想，請重新套用 Universal Restore。設定作業時，請指定必要的驅動程式。

Windows 開機後，系統就會初始化安裝新硬體的標準程序。如果驅動程式具有 Microsoft Windows 簽章，則網路卡驅動程式將自行安裝。否則，Windows 將要求您確認是否安裝未簽章的驅動程式。

之後，您將可以設定網路連線並為顯卡、USB 和其他裝置指定驅動程式。

Linux 中的 Universal Restore

Universal Restore 可以套用至核心版本為 2.6.8 或更新版本的 Linux 作業系統。

Universal Restore 套用至 Linux 作業系統時，會更新稱為初始 RAM 磁碟 (initrd) 的暫存檔系統。這可確保作業系統能在新硬體上啟動。

Universal Restore 會將新硬體的各項模組 (包括裝置驅動程式) 新增至初始 RAM 磁碟。通常，它會在 **/lib/modules** 目錄中尋找必要的模組。如果 Universal Restore 找不到需要的模組，會將模組的檔案名稱寫入記錄中。

Universal Restore 可能會修改 GRUB 開機載入程式的設定。這項程序在某些情況下可能是必要的，例如，當新電腦的磁碟區配置與原本的電腦不同時，可確保系統的開機能力。

Universal Restore 絕對不會修改 Linux 核心。

還原為原始的初始 RAM 磁碟

如有需要，您可以還原成原始的初始 RAM 磁碟。

初始 RAM 磁碟儲存於電腦的一個檔案中。首次更新初始 RAM 磁碟前，Universal Restore 會先將其複本儲存至相同目錄。複本名稱為檔案名稱後接上 **_acronis_backup.img** 尾碼。如果您執行 Universal Restore 一次以上 (例如，新增欠缺的驅動程式後)，複本並不會被覆寫。

若要還原為原始的初始 RAM 磁碟，請執行下列其中一項作業：

- 將複本重新命名為原始的初始 RAM 磁碟名稱。例如，執行類似以下的命令：

  ```
  mv initrd-2.6.16.60-0.21-default_acronis_backup.img initrd-2.6.16.60-0.21-default
  ```

- 在 **GRUB 開機載入程式設定**的 initrd 行指定複本。

復原檔案

在 Cyber Protect 主控台中復原檔案

注意事項
您無法在 Cyber Protect 主控台中，為 [合規] 模式下的租用戶復原備份。如需有關如何復原此類備份的詳細資訊，請參閱 "在合規模式下復原租用戶的備份" (第 981 頁)。

1. 選擇原本存放所要復原之資料的電腦。
2. 按一下 **[復原]**。
3. 選擇復原點。請注意，復原點是依照位置進行篩選。
   如果選擇實體且離線的電腦，則不會顯示復原點。執行下列任何一項作業：
   - [建議] 如果備份位置是雲端或共用儲存 (即可被其他代理程式存取)，按一下 **[選擇電腦]**，選擇在線上的目標電腦，然後選擇復原點。
   - 在 [備份儲存] 索引標籤上選擇復原點。
   - 從雲端儲存下載檔案。
   - 使用可開機媒體。
4. 按一下 **[復原]** > **[檔案/資料夾]**。
5. 瀏覽至所需的資料夾，或使用搜尋列以取得所需檔案和資料夾的清單。
   搜尋與語言無關。

您可以使用一或多個萬用字元 (* 和 ?)。如需有關如何使用萬用字元的詳細資訊，請參閱 "檔案篩選器 (包含/排除)" (第 408 頁)。

注意事項
儲存在雲端儲存空間的磁碟層級備份將無法使用搜尋。

6. 選擇您要復原的檔案。
7. 如果您想要將檔案儲存為 .zip 檔案，請按一下**[下載]**，選擇想要儲存資料的位置，然後按一下**[儲存]**。否則，請跳過此步驟。

   如果您的選取項目含有資料夾，或者所選檔案的大小總計超過 100 MB，則無法下載。若要從雲端擷取更大量的資料，請使用程序 "從雲端儲存下載檔案" (第 458 頁)。
8. 按一下 **[復原]**。

   在 **[復原至]** 中，按一下可選擇復原作業的目標，或保留預設目標。預設目標會根據備份來源而有所不同。

   下列目標可供使用：
   - 來源電腦 (如果保護代理程式安裝在該電腦上)。

     這是原本存放所要復原之檔案的電腦。
   - 安裝保護代理程式的其他機器 (實體機器、虛擬機器)，以及安裝保護代理程式的虛擬化主機，或虛擬裝置。

     您可以將檔案復原至安裝保護代理程式的實體機器、虛擬機器，以及虛擬化主機。您無法將檔案復原至未安裝保護代理程式的虛擬機器 (但 Virtuozzo 虛擬機器除外)。
   - Virtuozzo 容器或虛擬機器。

     您可以將檔案復原至 Virtuozzo 容器和虛擬機器，但有一些限制。如需詳細資訊，請參閱 "復原檔案在 Cyber Protect 主控台中的限制" (第 461 頁)。
9. 在**[路徑]**中，選擇復原目的地。您可以選擇下列其中一項：
   - [復原至原始電腦時] 原始位置。
   - 目標電腦上的本機資料夾或本機連接的存放區。

     注意事項
     不支援符號連結。

   - 可以從目標電腦存取的網路資料夾。

     例如，從 Microsoft Azure 虛擬機器復原檔案時，網路資料夾必須可供虛擬機器上部署的 Azure 用代理程式存取。
10. 按一下 **[開始復原]**。
11. 選擇其中一個檔案覆寫選項：
    - **覆寫現有的檔案**
    - **如果較舊，請覆寫現有的檔案**
    - **不要覆寫現有檔案**

復原進度會顯示在 **[活動]** 索引標籤上。

從雲端儲存下載檔案

在 Web Restore 主控台中，您可以瀏覽雲端儲存，檢視備份內容，以及下載備份的檔案和資料夾。

注意事項
只有在您是客戶 Cyber Protection 系統管理員或客戶租用戶使用者時，才可以存取 Web Restore 主控台。不允許使用合作夥伴層級的使用者角色。

限制

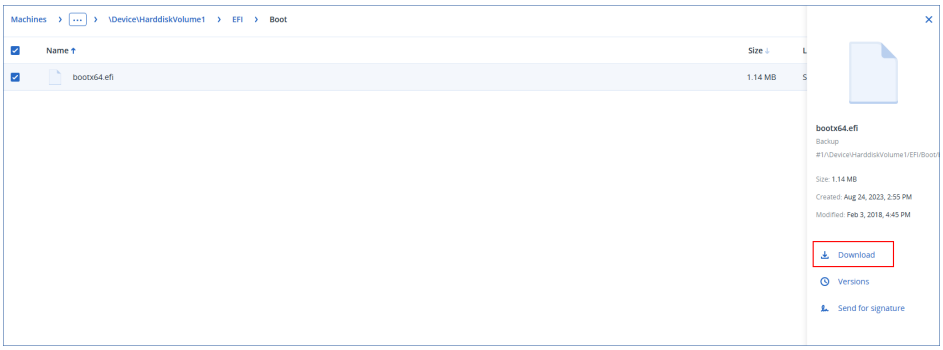
- 您無法下載備份的磁碟、磁碟區或整個復原點。
- 當您瀏覽磁碟層級備份時，不會顯示邏輯磁碟區 (例如 LVM 和 LDM)。
- 您無法瀏覽系統狀態、SQL 資料庫和 Exchange 資料庫的備份。

若要從雲端儲存下載檔案和資料夾

1. 在 Cyber Protection 主控台中，選擇所需的工作負載，然後按一下 **[復原]**。
2. [如果有多個備份位置可供使用] 選擇備份位置，然後按一下 **[更多復原方式]**。
3. 按一下 **[下載檔案]**。
4. 在 **[電腦]** 下，按一下工作負載名稱，然後按一下備份存檔。
   備份存檔包含一個或多個備份 (復原點)。
5. 按一下您要從中下載檔案或資料夾的備份號碼 (復原點)，然後導覽到所需的項目。
6. 選擇您要下載的項目旁的核取方塊。

   注意事項
   如果您選擇多個項目，它們將會以 ZIP 檔案的形式下載。

7. 按一下 **[下載]**。



向 Notary Service 驗證檔案真實性

如果備份期間啟用公證，則可驗證備份檔案的真實性。

要驗證檔案的真實性

1. 選擇檔案，如「使用 Web 介面復原檔案」一節步驟 1-6，或「從雲端儲存空間下載檔案」一節步驟 1-5 中所述。

2. 確保所選檔案標記有下列圖示：  。這表示檔案已公證。
3. 執行下列其中一項操作：
   - 按一下**驗證**。
     軟體會檢查檔案真實性並顯示結果。
   - 按一下**取得憑證**。
     確認檔案公證的憑證會在 Web 瀏覽器視窗中開啟。該視窗還包含了容許您手動驗證檔案真實性的說明。

使用 ASign 簽署檔案

注意事項
此功能適用於 Advanced Backup 套件。

ASign 是允許多人以電子方式簽署檔案的一項服務。此功能僅適用於儲存在雲端儲存中的檔案層級備份。

一次只能簽署一個檔案版本。如果多次備份檔案，則必須選擇要簽署的版本，而且只會簽署該版本。

例如，ASign 可用於以電子方式簽署如下檔案：

- 出租或租用協議
- 銷售合約
- 資產購買協議
- 貸款協議
- 權限名單
- 財務文件
- 保險文件
- 責任拋棄
- 醫療保健文件
- 調查報告
- 真品證明書
- 非公開協議
- 報價書
- 機密性協議
- 獨立承包商協議

要簽署檔案版本

1. 選擇檔案，如「使用 Web 介面復原檔案」一節步驟 1-6，或「從雲端儲存空間下載檔案」一節步驟 1-5 中所述。
2. 確認左面板上已選擇正確的日期與時間。
3. 按一下**簽署此檔案版本**。

4. 指定要在其下儲存備份的雲端儲存帳戶的密碼。提示視窗中會顯示登入帳戶。

   ASign 服務介面會在 Web 瀏覽器視窗中開啟。
5. 透過指定電子郵件地址新增其他簽署人。傳送邀請之後，就無法新增或移除簽署人，因此請確認清單中包含需要其簽章的所有人。
6. 按一下 **[邀請簽署]** 傳送邀請給簽署人。

   各簽署人均收到帶有簽名請求的電子郵件訊息。所有已請求的簽署人簽署檔案後，表示該檔案已透過公證服務完成公證及簽署。

   當每個簽署人簽署檔案且整個流程完成時，您將收到通知。您可以透過按一下所收到的任一電子郵件訊息中的 **[檢視詳細資料]** 來存取 ASign 網頁。
7. 當程序完成時，請前往 ASign 網頁並按一下 **[獲取文件]** 下載 .pdf 文件，其中包含：
   - 收集簽章的簽署憑證頁。
   - 具有活動歷程記錄的「審計存底」頁面：將邀請傳送至簽署人的時間，各簽署人簽署檔案的時間等。

使用可開機媒體復原檔案

如需有關如何建立可開機媒體的資訊，請參閱 < 建立可開機媒體 > 。

如果要使用可開機媒體復原檔案

1. 使用可開機媒體將目標電腦開機。
2. 按一下 **[在本機管理此電腦]** 或按兩次 **[救援可開機媒體]**，視您使用的媒體類型而定。
3. 如果您的網路中已啟用 Proxy 伺服器，請按一下 **[工具]** > **[Proxy 伺服器]**，然後指定 Proxy 伺服器主機名稱/IP 位址、連接埠和認證。否則，請跳過此步驟。
4. [選用] 復原 Windows 或 Linux 時，按一下 **[工具]** > **[在 Cyber Protection 服務中註冊媒體]**，然後指定您在下載媒體時取得的註冊權杖。如果您這麼做，您將不需要輸入認證或註冊碼，就可以存取雲端儲存空間，如步驟 7 所述。
5. 在歡迎畫面上，按一下 **[復原]**。
6. 按一下 **[選擇資料]**，然後按一下 **[瀏覽]**。
7. 指定備份位置：
   - 若要從雲端儲存進行復原，請選擇 **[雲端儲存]**。輸入已指派備份電腦之帳戶的認證。

     復原 Windows 或 Linux 時，您可以選擇要求註冊碼，並使用該註冊碼代替認證。按一下 **[使用註冊碼]** > **[要求代碼]**。軟體將會顯示註冊連結和註冊碼。您可以複製註冊連結和註冊碼，並在另一部電腦上執行註冊步驟。註冊碼的有效期限為一小時。
   - 若要從本機或網路資料夾進行復原，請瀏覽至 **[本機資料夾]** 或 **[網路資料夾]** 下的資料夾。
   - 若要從公有雲端儲存空間 (例如 Microsoft Azure、Amazon S3、Wasabi 或 S3 相容儲存空間) 上的備份位置復原，請先按一下 **[Cyber Protection 服務中的註冊媒體]**，然後使用 Web 介面設定復原。如需有關透過 Web 介面遠端管理媒體的詳細資訊，請參閱 "可開機媒體的相關遠端作業" (第 650 頁)。

   按一下 **[確定]** 以確認您的選擇。
8. 選擇您要從中復原資料的備份。如果看到提示，請輸入備份的密碼。

9. 在 **[備份內容]** 中選擇 **[資料夾/檔案]**。
10. 選擇您要復原的資料。按一下 **[確定]** 以確認您的選擇。
11. 在 **[復原目的地]** 下指定資料夾。或者，您也可禁止覆寫較新版本的檔案或將某些檔案排除在復原之外。
12. [選用] 按一下 **[復原選項]** 以指定額外的設定。
13. 按一下**[確定]**開始復原。

從本機備份解壓縮檔案

您可以瀏覽備份內容並擷取所需的檔案。

需求

- 此功能僅限於 Windows 系統的「檔案總管」使用。
- 備份的檔案系統必須是下列其中一種：FAT16、FAT32、NTFS、ReFS、Ext2、Ext3、Ext4、XFS 或 HFS+。

必要條件

- 您用來瀏覽備份的電腦必須已安裝保護代理程式。
- 備份必須儲存在本機資料夾中，或在網路共用 (SMB/CIFS) 上。

從備份解壓縮檔案

1. 使用檔案總管瀏覽至備份位置。
2. 按兩下備份檔案。檔案名稱是依據下列範本格式：
   `<電腦名稱> - <保護計劃 GUID>`
3. 如果備份已加密，請輸入加密密碼。否則，請跳過此步驟。
   檔案總管會顯示復原點。
4. 按兩下復原點。
   檔案總管會顯示備份的資料。
5. 瀏覽至所需的資料夾。
6. 將所需檔案複製到檔案系統中的任何資料夾。

復原檔案在 Cyber Protect 主控台中的限制

合規模式下的租用戶

您無法在 Cyber Protect 主控台中，為 [合規] 模式下的租用戶復原備份。如需有關如何復原此類備份的詳細資訊，請參閱 "在合規模式下復原租用戶的備份" (第 981 頁)。

復原至 Virtuozzo 容器或 Virtuozzo 虛擬機器

- QEMU 客體代理程式必須安裝在目標虛擬機器上。
- [僅在復原到容器時適用] 容器內的掛載點無法當作復原的目標使用。例如，您無法將檔案復原至掛載到容器的另一個硬碟或 NFS 共用。

- 將檔案復原到 Windows 虛擬機器時，以及已啟用 "檔案層級安全性" (第 466 頁) 復原選項時，存檔位元屬性會設定為已復原的檔案。
- 名稱中包含非 ANSI 字元的檔案在執行 Windows Server 2012 或更舊版本的電腦上，以及執行 Windows 7 或更舊版本的電腦上復原時，其名稱不正確。
- 若要將檔案復原到在 Virtuozzo Hybrid Server 上執行的 CentOS 或 Red Hat Enterprise Linux 虛擬機器，您必須編輯 qemu-ga 檔案，如下所示：
  - 在目標虛擬機器上，導覽至 /etc/sysconfig/，然後開啟 qemu-ga 檔案進行編輯。
  - 導覽至下行，然後刪除等號 (=) 後的所有內容：

    ```
    BLACKLIST_RPC=
    ```

  - 執行下列命令以重新啟動 QEMU 客體代理程式：

    ```
    systemctl restart qemu-guest-agent
    ```

復原系統狀態

注意事項
您無法在 Cyber Protect 主控台中，為 [合規] 模式下的租用戶復原備份。如需有關如何復原此類備份的詳細資訊，請參閱 "在合規模式下復原租用戶的備份" (第 981 頁)。

1. 選擇您要復原系統狀態的電腦。
2. 按一下 **[復原]**。
3. 選擇系統狀態復原點。請注意，復原點是依照位置進行篩選。
4. 按一下 **[復原系統狀態]**。
5. 確認您要以系統狀態的備份版本覆寫系統狀態。

復原進度會顯示在 **[活動]** 索引標籤上。

復原 ESXi 設定

若要復原 ESXi 設定，您需要 Linux 型的可開機媒體。如需有關如何建立可開機媒體的資訊，請參閱 "建立實體可開機媒體" (第 635 頁)。

如果您正在將 ESXi 設定復原至非原始主機，而原始 ESXi 主機仍連線至 vCenter Server，請中斷這部主機與 vCenter Server 的連線並從中移除，以避免復原期間發生意外問題。若要同時保留原始主機與復原主機，您可以在完成復原後將其再次加入。

在主機上執行的虛擬機器未包含在 ESXi 設定備份中。這些虛擬機器可以另行單獨備份和復原。

復原 ESXi 設定

1. 使用可開機媒體將目標電腦開機。
2. 按一下 **[在本機管理這部電腦]**。
3. 在歡迎畫面上，按一下 **[復原]**。
4. 按一下 **[選擇資料]**，然後按一下 **[瀏覽]**。

5. 指定備份位置：
   - 瀏覽至 **[本機資料夾]** 或 **[網路資料夾]**下的資料夾。

   按一下 **[確定]** 以確認您的選擇。
6. 在 **[顯示]** 中，選擇 **[ESXi 設定]**。
7. 選擇您要從中復原資料的備份。如果看到提示，請輸入備份的密碼。
8. 按一下 **[確定]**。
9. 在 **[要用於新資料存放區的磁碟]** 中，執行以下動作：
   - 在 **[將 ESXi 復原至]** 下，選擇將復原主機設定的磁碟。如果您正在將設定復原至原始主機，則會依據預設選擇原始磁碟。
   - [選用] 在 **[用於新資料存放區]** 下，選擇將會建立新資料存放區的磁碟。請格外小心，因為已選擇之磁碟上的所有資料都將遺失。若要保留現有資料存放區中的虛擬機器，請勿選擇任何磁碟。
10. 如果已選擇新資料存放區的任何磁碟，請選擇 **[如何建立新資料存放區]** 中的資料存放區建立方法：**[每個磁碟建立一個資料存放區]** 或 **[在所有已選擇的 HDD 上建立一個資料存放區]**。
11. [選用] 在 **[網路對應]** 中，將存在於備份中之虛擬交換器的自動對應結果，變更為實體網路卡。
12. [選用] 按一下 **[復原選項]** 以指定額外的設定。
13. 按一下**[確定]**開始復原。

復原選項

若要修改復原選項，請在設定復原時按一下**[復原選項]**。

復原選項的可用性

可用的復原選項集取決於：

- 代理程式執行復原作業的環境 (Windows、Linux、Mac OS 或可開機媒體)。
- 復原的資料類型 (磁碟、檔案、虛擬機器、應用程式資料)。

下表總結了復原選項的可用性。

	磁碟			檔案				虛擬機器		SQL 與 Exchange
	Windows	**Linux**	**可開機媒體**	**Windows**	**Linux**	**macOS**	**可開機媒體**	**ESXi、Hyper-V、Scale Computing、oVirt 和 Virtuozzo**	**Azure**	**Windows**
備份驗證	+	+	+	+	+	+	+	+	-	+
開機模式	+	-	-	-	-	-	-	+	-	-
檔案日期	-	-	-	+	+	+	+	-	-	-

與時間										
錯誤處理	+	+	+	+	+	+	+	+	+	+
檔案排除	-	-	-	+	+	+	+	-	-	-
檔案層級安全性	-	-	-	+	-	-	-	-	-	-
Flashback	+	+	+	-	-	-	-	+	-	-
復原完整路徑	-	-	-	+	+	+	+	-	-	-
掛載點	-	-	-	+	-	-	-	-	-	-
效能	+	+	-	+	+	+	-	+	-	+
事前/事後命令	+	+	-	+	+	+	-	+	-	+
SID 變更	+	-	-	-	-	-	-	-	-	-
VM 電源管理	-	-	-	-	-	-	-	+	+	-
Windows 事件日誌	+	-	-	+	-	-	-	僅 Hyper-V	-	+

備份驗證

此選項定義從備份復原資料前，是否驗證備份以確保備份未損毀。此作業是由保護代理程式所執行。

預設為：**[已停用]**。

有關透過總和檢查碼驗證來驗證的詳細資訊，請參閱 "總和檢查碼驗證" (第 202 頁)。

注意事項
視您的服務提供者所選擇的設定而定，可能無法在備份到雲端儲存空間時進行驗證。

開機模式

此選項適用於從含有 Windows 作業系統之磁碟層級備份復原實體機器或虛擬機器。。

此選項可讓您選擇 Windows 在復原後將使用的開機模式 (BIOS 或 UEFI)。如果原始電腦的開機模式與所選開機模式不同，則軟體會：

- 根據所選擇的開機模式 (BIOS 的 MBR、UEFI 的 GPT)，初始化您要復原系統磁碟區的目的地磁碟。
- 調整 Windows 作業系統，讓系統可使用所選開機模式啟動。

預設為:**如同在目標電腦上。**

可選擇以下一個選項:

- **如同在目標電腦上**

  目標電腦上執行的代理程式會偵測 Windows 目前使用的開機模式,並根據偵測到的開機模式進行調整。

  除非下列限制適用,否則這是自動導致可開機系統的最安全值。由於可開機媒體下沒有 **[開機模式]** 選項,因此媒體上的代理程式會一律執行如同選擇此值時的行為。
- **如同在已備份的電腦上**

  目標電腦上執行的代理程式會從備份讀取開機模式,並根據此開機模式進行調整。這有助於在不同電腦上復原系統,即使此電腦使用其他開機模式也行,然後取代已備份電腦中的磁碟。
- **BIOS**

  目標電腦上執行的代理程式會進行調整,以使用 BIOS。
- **UEFI**

  目標電腦上執行的代理程式會進行調整,以使用 UEFI。

一旦設定變更之後,將會重複磁碟對應程序。這需要花費一些時間。

建議

如果您需要在 UEFI 和 BIOS 之間轉換 Windows:

- 復原系統磁碟區所在位置的整個磁碟。如果在現有磁碟區上僅復原系統磁碟區,代理程式將無法正確初始化目標磁碟。
- 請記得,BIOS 不允許使用 2 TB 以上的磁碟空間。

限制

- 下列系統支援在 UEFI 和 BIOS 之間的轉換:
  - 從 Windows 7 開始的 64 位元作業系統
  - 自 Windows Server 2008 SP1 之後的 64 位元 Windows Server 作業系統
- 如果備份儲存在磁帶裝置上,則不支援 UEFI 和 BIOS 之間的轉換。

如果不支援在 UEFI 和 BIOS 之間轉換系統,則代理程式會執行如同已選擇 **[如同在已備份的電腦上]** 設定時的行為。如果目標電腦同時支援 UEFI 與 BIOS 系統,您必須手動啟用與原始電腦對應的開機模式,否則系統將無法啟動。

檔案日期與時間

此選項僅在復原檔案時有效。

此選項定義是從備份復原檔案的日期與時間,還是將目前的日期與時間指派給檔案。

若啟用此選項,會將目前的日期與時間指派給檔案。

預設為:**[啟用]**。

錯誤處理

這些選項可讓您指定如何處理復原期間可能發生的錯誤。

發生錯誤時重新嘗試

預設為：**啟用。嘗試次數:30。嘗試間隔：30 秒。**

如果發生可復原的錯誤，程式將重新嘗試執行未成功的作業。您可以設定時間間隔和嘗試次數。一旦作業成功「或是」已執行指定次數的嘗試後 (以先發生者為準)，軟體將停止嘗試。

處理時不顯示訊息和對話方塊 (無訊息模式)

預設為：**[已停用]**。

啟用無訊息模式後，程式將自動處理需要使用者互動的情形 (如有可能)。如果需要使用者互動方可繼續，則作業將失敗。可在作業記錄中找到作業的詳細記錄，包括錯誤 (若有)。

忽略錯誤

此選項適用於檔案層級復原。

預設為：**[啟用]**。

啟用此選項且檔案復原失敗時，復原作業將針對其餘檔案繼續。在 **[活動]** 畫面上會顯示一個警告。因為未記錄錯誤，因此不會觸發 **[發生錯誤時重新嘗試]** 選項。

停用此選項且檔案復原失敗時，復原作業將失敗。在 **[活動]** 畫面將顯示一個錯誤。

如果使用重新開機復原失敗，請儲存系統資訊。

此選項適用於將磁碟或磁碟區復原至執行 Windows 或 Linux 的實體電腦。

預設為：**[已停用]**。

啟用此選項時，您可以在本機磁碟 (包括連接到目標電腦的快閃磁碟機或 HDD 磁碟機) 或儲存記錄、系統資訊和當機傾印檔案的網路共用上，指定資料夾。此檔案可幫助技術支援人員判別問題所在。

檔案排除

此選項僅在復原檔案時有效。

此選項可定義在復原程序中要略過的檔案及資料夾，以將其排除在復原項目清單之外。

注意事項
排除項目會覆寫要復原的所選資料項目。例如，如果您選擇復原 MyFile.tmp 檔案並排除所有 .tmp 檔案，將不會復原 MyFile.tmp 檔案。

檔案層級安全性

此選項在從 NTFS 格式化磁碟區的磁碟層級和檔案層級備份復原檔案時有效。

此選項定義是否將檔案的 NTFS 權限連同檔案一併復原。

預設為：**[啟用]**。

您可選擇是復原權限，還是讓檔案繼承復原目標資料夾的 NTFS 權限。

Flashback

除 Mac 之外，在實體和虛擬機器上復原磁碟和磁碟區時，此選項會生效。

此選項只有在復原的磁碟的磁碟區配置完全符合目標磁碟的磁碟區配置時才會運作。

若啟用此選項，則只會復原備份中的資料與目標磁碟資料之間的差異部分。這可加速實體和虛擬機器的復原。資料會在資料區塊層級進行比較。

在復原實體機器時，其預設為：**[已停用]**。

在復原虛擬機器時，其預設為：**[啟用]**。

復原完整路徑

只有從檔案層級備份資料時，此選項才能發揮作用。

若啟用此選項，系統會在目標位置中重新建立至檔案的完整路徑。

預設為：**[已停用]**。

掛載點

只有在 Windows 中復原檔案層級備份的資料時，此選項才能發揮作用。

啟用此選項可復原存放在已掛載磁碟區，且於啟用 [掛載點] 選項時進行備份的檔案與資料夾。

預設為：**[已停用]**。

當您選擇資料夾進行復原時，資料夾的階層必須高於掛載點，此選項才能發揮作用。如果您選擇進行復原的資料夾位在掛載點內，或是掛載點本身，則無論 **[掛載點]** 選項的值為何，都會復原選擇的項目。

注意事項
請切記，如果復原時未掛載磁碟區，資料會直接復原至備份時已經是掛載點的資料夾。

效能

此選項會定義作業系統內復原程序的優先順序。

可用設定包括：**[低]**、**[一般]**、**[高]**。

預設為：**[一般]**。

系統中執行程序的優先順序會決定分配給該程序的 CPU 和系統資源多寡。降低復原優先順序，將會釋放更多資源給其他應用程式。提高復原的優先順序，將要求作業系統分配更多資源給執行復原

的應用程式，從而可能加快復原程序的速度。但是，實際效果將取決於 CPU 使用總量和其他因素 (如磁碟 I/O 速度或網路流量)。

事前/事後命令

此選項可讓您定義資料復原之前和之後要自動執行的命令。

事前/事後命令使用方式的範例：

- 啟動 **Checkdisk** 命令，以尋找並修正邏輯檔案系統錯誤、實體錯誤或損壞的磁區，以在復原開始前和復原結束後啟動。

本程式不支援互動式命令，即需要使用者輸入的命令 (例如「pause」)。

如果復原過程將會重新啟動，則復原後命令將不被執行。

復原前命令

指定要在復原程序開始前執行的命令/批次檔案

1. 啟用 **[復原之前執行命令]** 開關。
2. 在 **[命令...]** 欄位中輸入命令，或瀏覽至批次檔案。本程式不支援互動式命令，即需要使用者輸入的命令 (例如「pause」)。
3. 在 **[工作目錄]** 欄位中，指定將執行命令/批次檔案所在目錄的路徑。
4. 如有需要，請在 **[引數]** 欄位中指定該命令的執行引數。
5. 依據您要獲得的結果，選擇下表所述的相應選項。
6. 按一下**[完成]**。

核取方塊	**選擇**			
若命令執行失敗，則放棄復原*	已選擇	已清除	已選擇	已清除
命令執行完成後再復原	已選擇	已選擇	已清除	已清除
結果				
	預設 僅在成功執行命令後執行復原。若命令執行失敗，則放棄復原。	執行命令後執行復原，無論命令執行是否成功。	不適用	執行命令的同時執行復原，無論命令執行的結果如何。

* 命令的結束碼如果不等於零便視為失敗。

復原後命令

指定復原完成後要執行的命令/可執行檔

1. 啟用 **[復原之後執行命令]** 開關。
2. 在 **[命令...]** 欄位中輸入命令，或瀏覽至批次檔案。
3. 在 **[工作目錄]** 欄位中，指定將執行命令/批次檔案所在目錄的路徑。
4. 在 **[引數]** 欄位中指定命令執行引數 (如有需要)。
5. 如果命令成功執行與否很重要，請選取 **[若命令執行失敗，則放棄復原]** 核取方塊。命令的結束碼如果不等於零，命令就視為失敗。如果命令執行失敗，則復原狀態將設為 **[錯誤]**。

   如果未選擇核取方塊，則命令執行結果不會影響復原執行失敗或成功。您可以瀏覽 **[活動]** 標籤，以追蹤命令的執行結果。
6. 按一下**[完成]**。

注意事項
如果復原過程將會重新啟動，則復原後命令將不被執行。

SID 變更

此選項只有在復原 Windows 8.1/Windows Server 2012 R2 或舊版時有效。

VMware 用代理程式、Hyper-V 用代理程式、Scale Computing HC3 用代理程式或 oVirt 用代理程式執行復原至虛擬機器時，此選項不適用。

預設為：**[已停用]**。

軟體可為復原的作業系統產生唯一安全性識別碼 (電腦 SID)。只需要此選項，即可確保第三方軟體可依「電腦 SID」執行作業。

Microsoft 並未正式支援在部署或復原的系統上變更 SID，因此若使用此選項，請自行承擔風險。

VM 電源管理

VMware 用代理程式、Azure 用代理程式、Hyper-V 用代理程式、Virtuozzo 用代理程式、Scale Computing HC3 用代理程式或 oVirt 用代理程式執行復原至虛擬機器時，這些選項均有效。

開始復原時關閉目標虛擬機器

預設為：**[啟用]**。

若現有虛擬機器為連線狀態，即無法復原至該虛擬機器，因此復原一開始，就會自動關閉虛擬機器。使用者會與虛擬機器中斷連線，而任何未儲存的資料會流失。

若您偏好於復原前手動關閉虛擬機器，請清除此選項的核取方塊。

復原完成時開啟目標虛擬機器

預設為：**[已停用]**。

電腦從備份復原至另一台電腦後，網路上可能會顯示現有電腦的複本。基於安全考量，請在採取必要的預防措施後，再手動開啟復原的虛擬機器。

Windows 事件日誌

此選項僅在 Windows 作業系統下有效。

此選項定義代理程式是否必須在 Windows 的應用程式事件記錄檔中記錄復原作業事件 (若要查看此記錄，請執行 eventvwr.exe 或選擇 **[控制台]** > **[系統管理工具]** > **[事件檢視器]**)。您可以篩選要記錄的事件。

預設為：**[已停用]**。

備份的相關作業

備份儲存索引標籤

[備份儲存] 索引標籤可讓您存取所有備份，包括離線電腦的備份、不再登錄在 Cyber Protection 服務中之電腦的備份、公有雲端 (如 Microsoft Azure) 上的備份，以及孤立備份[1]。

透過 acrocmd 建立的備份會被標記為孤立。在產品的 12.5 版中建立的備份也會被識別為孤立。

注意事項
請注意，孤立備份也需要付費。

儲存於共用位置的備份 (如 SMB 或 NFS 共用) 對已讀取位置權限的所有使用者可見。

在 Windows 中，備份檔案會繼承其父資料夾的存取權限。因此，建議您限制此資料夾的讀取權限。

在雲端儲存中，使用者僅能存取他們自己的備份。

系統管理員能夠代表屬於特定單位或公司和其子群組的任何帳戶，透過選擇帳戶的雲端儲存空間，檢視雲端的備份。若要選擇您要用於取得雲端資料的裝置，按一下 **[要瀏覽的電腦]** 列中的 **[變更]**。**[備份儲存]** 索引標籤會顯示曾以所選帳戶登錄之所有電腦的備份。

雲端 Microsoft 365 用代理程式所建立的備份以及 Google Workspace 資料的備份不會顯示在**雲端儲存空間**位置，而是顯示在名稱為 **[雲端應用程式備份]** 的另一個區段。

用於保護計劃的備份位置會自動新增至 **[備份儲存]** 索引標籤。欲新增自訂資料夾 (如卸離式 USB 裝置) 至備份位置清單，請按一下 **[瀏覽]** 然後指定資料夾路徑。

如果您使用檔案管理員新增或移除一些備份，按一下位置名稱旁的齒輪圖示，然後按一下 **[重新整理]**。

警告！
請勿嘗試手動編輯備份檔案，因為這可能會導致檔案損毀，並使備份無法使用。此外，建議您使用備份複寫，而非手動移動備份檔案。

[1]孤立備份是與保護計劃不再有關聯的備份。

如果曾經備份至該位置的所有電腦從 服務中刪除，備份位置 (雲端儲存空間除外) 會從 **[備份儲存]** 索引標籤消失。如此可確保您不必支付此位置中儲存之備份的費用。只要備份至此位置，就會重新加入該位置以及儲存在其中的所有備份。

在 **[備份儲存]** 索引標籤上，您可以在清單中使用下列條件篩選備份：

- **僅搭配鑑識資料** – 只會顯示包含鑑識資料的備份。
- **僅限修補程式管理所建立的預先更新的備份** – 只會顯示修補程式安裝之前，在修補程式管理執行期間所建立的備份。

若要使用 [備份儲存] 索引標籤選擇復原點

1. 在 **[備份儲存]** 索引標籤上，選擇儲存備份的位置。
   軟體會顯示在已選擇的位置裡，您的帳戶可以檢視的所有備份。備份會在群組中合併。群組名稱是依據下列範本：
   <電腦名稱> - <保護計劃名稱>
2. 選擇您要復原其資料的群組。
3. [選用] 請按一下 **[要瀏覽的電腦]** 旁邊的 **[變更]**，然後選擇其他電腦。某些備份僅限特定的代理程式才能瀏覽。例如，要瀏覽 Microsoft SQL Server 資料庫備份，就必須要選擇執行 SQL 用代理程式的電腦。

   重要事項
   請注意，**[要瀏覽的電腦]** 是從實體電腦備份復原的預設目的地。選擇了復原點並按一下 **[復原]** 後，再次檢查 **[目標電腦]** 設定，以確保這是您要復原的特定電腦。欲變更復原目的地，請在 **[要瀏覽的電腦]** 中指定其他電腦。

4. 按一下 **[顯示備份]**。
5. 選擇復原點。

若要為備份新增位置

注意事項
此作業只有在您有線上代理程式時才可以使用。

在 **[備份儲存]** 索引標籤上，按一下 **[新增位置]**。

從以下其中一個位置類型選擇位置，然後按一下 **[完成]**：

- 本機資料夾
- 網路資料夾
- Secure Zone
- NFS 資料夾
- 公有雲端

從備份掛載磁碟區

掛載磁碟層級備份的磁碟區，可讓您如同存取實體磁碟般存取磁碟區。

在讀寫模式下掛載磁碟區可讓您修改備份內容，即儲存、移動、建立、刪除檔案或資料夾，並執行由一個檔案組成的執行檔。在此模式下，軟體會建立增量備份，其中包含您對備份內容所作的變更。請注意，後續的備份都不會包含這些變更。

需求

- 此功能僅限於 Windows 系統的「檔案總管」使用。
- 用來執行掛載作業的電腦必須已安裝 Windows 用代理程式。
- 電腦所執行的 Windows 版本必須支援備份的檔案系統。
- 備份檔案必須儲存在網路共用 (SMB/CIFS) 或 Secure Zone 的本機資料夾中。

使用情境

- 共用資料

  您可以輕易透過網路共用已掛載磁碟區。
- "Band-aid" 資料庫復原解決方案

  掛載一個包含 SQL 資料庫的磁碟區，而該資料庫來自最近發生故障的電腦。如此一來，將可讓您存取該資料庫，直到故障的電腦復原為止。此方法也可以透過 SharePoint Explorer 用於 Microsoft SharePoint 的細微復原。
- 離線病毒移除

  如果電腦受到感染，請先掛載備份，並使用防毒軟體清理病毒 (或尋找最近一個未受到感染的備份)，然後再從該備份復原電腦。
- 錯誤檢查

  如果重新調整大小的磁碟區復原失敗，則可能是備份檔案系統中發生的錯誤所致。請在讀寫模式下掛載備份。接著，使用 `chkdsk /r` 命令檢查已掛載磁碟區是否有錯誤。錯誤修正完成並建立新的增量備份之後，從此備份復原系統。

從備份掛載磁碟區

1. 使用檔案總管瀏覽至備份位置。
2. 按兩下備份檔案。檔案名稱是依據下列範本格式：

   `<電腦名稱> - <保護計劃 GUID>`
3. 如果備份已加密，請輸入加密密碼。否則，請跳過此步驟。

   檔案總管會顯示復原點。
4. 按兩下復原點。

   檔案總管會顯示備份的磁碟區。

   注意事項

   按兩下磁碟區瀏覽內容。您可以從備份將檔案和資料夾複製到檔案系統上的任何資料夾。

5. 以滑鼠右鍵按一下要掛載的磁碟區，然後選擇下列其中一個選項：
   a. **安裝**

      注意事項

      您只能在讀寫模式下，掛載存檔中的最後一個備份 (備份鏈)。

b. **掛載成唯讀模式**。

6. 如果備份儲存在網路共用，請提供存取認證。否則，請跳過此步驟。
   軟體會掛載所選的磁碟區。系統會將第一個未使用的代號指派給磁碟區。

卸載磁碟區

1. 使用檔案總管瀏覽至 [**電腦**] (Windows 8.1 和更新版本會顯示為 [**本機**])。
2. 用滑鼠右鍵按一下已掛載磁碟區。
3. 按一下 [**卸載**]。
4. [選用] 如果先前是在讀寫模式下掛載磁碟區，而其內容經過修改，則請選擇是否要建立包含變更的增量備份。否則，請跳過此步驟。

軟體會卸載所選的磁碟區。

驗證備份

您可以驗證備份以確認您可以復原資料。有關此作業的更多資訊，請參閱 "驗證" (第 201 頁)。

注意事項
此功能適用於當作 Advanced Backup 套件一部分啟用的 **Advanced Backup – 伺服器**或 **Advanced Backup – NAS** 配額的客戶租用戶。

驗證備份

1. 選擇備份的工作負載。
2. 按一下 **[復原]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。
   如果工作負載處於離線狀態，則不會顯示復原點。執行下列任何一項作業：
   - 如果備份位置是雲端或共用儲存空間 (即其他代理程式可存取)，請按一下 **[選擇機器]**，選擇處於連線狀態的目標工作負載，然後選擇復原點。
   - 在 [備份儲存] 索引標籤上選擇復原點。有關在該處備份的更多資訊，請參閱 "備份儲存索引標籤" (第 470 頁)。
4. 按一下齒輪圖示，然後按一下 **[驗證]**。
5. 選擇執行驗證的代理程式。
6. 選擇驗證方式：
7. 如果備份已經過加密，請提供加密密碼。
8. 按一下 **[開始]**。

匯出備份

匯出作業會在您指定的位置建立備份的有效副本。原始備份保持不變。透過匯出備份，您可以從增量備份及差異備份鏈分離特定備份，以便快速復原、寫入抽取式或可拔除媒體或用於其他目的。

注意事項
此功能適用於當作 Advanced Backup 套件一部分啟用的 **Advanced Backup – 伺服器**或 **Advanced Backup – NAS** 配額的客戶租用戶。

匯出作業的結果一律是完整備份。如果要將整個備份鏈複製到其他位置並保留多個復原點，請使用備份複寫計劃。有關系此計劃的更多資訊，請參閱 "備份複寫" (第 198 頁)。

匯出備份的備份檔案名稱與原始備份的備份檔案名稱相同，序號除外。如果相同備份鏈中的多個備份匯出到相同的位置，則會將四位數序號附加到所有備份的檔案名稱，但第一個備份除外。

匯出的備份將繼承原始備份的加密設定和密碼。匯出加密備份時，您必須指定密碼。

若要匯出備份

1. 選擇備份的工作負載。
2. 按一下 **[復原]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。
   如果工作負載處於離線狀態，則不會顯示復原點。執行下列任何一項作業：
   - 如果備份位置是雲端或共用儲存空間(即其他代理程式可存取)，請按一下 **[選擇機器]**，選擇處於連線狀態的目標工作負載，然後選擇復原點。
   - 在 [備份儲存] 索引標籤上選擇復原點。有關在該處備份的更多資訊，請參閱 "備份儲存索引標籤" (第 470 頁)。
4. 按一下齒輪圖示，然後按一下 **[匯出]**。
5. 選擇將執行匯出的代理程式。
6. 如果備份已經過加密，請提供加密密碼。否則，請跳過此步驟。
7. 指定匯出目的地。
8. 按一下 **[開始]**。

刪除備份

備份存檔包含一個或多個備份。您可以刪除存檔中的特定備份 (復原點) 或刪除整個存檔。

刪除備份存檔會刪除其中的所有備份。刪除工作負載的所有備份會刪除包含這些備份的備份存檔。

您可以使用 Cyber Protect 主控台，刪除 **[裝置]** 索引標籤和 **[備份儲存]** 索引標籤上的備份。此外，您可以使用 Web Restore 主控台，從雲端儲存刪除備份。

警告！
如果固定儲存空間遭到停用，則會永久刪除備份的資料，而且無法復原。

若要刪除備份或備份存檔

在 [裝置] 索引標籤上

此程序僅適用於線上工作負載。

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 選擇您要刪除的工作負載備份。
3. 按一下 **[復原]**。
4. [如果有一個以上的備份位置可用] 請選擇備份位置。
5. [若要刪除工作負載的所有備份] 按一下 **[全部刪除]**。
   刪除所有備份也會刪除包含這些備份的備份存檔。
6. [若要刪除特定備份] 選擇您要刪除的備份 (復原點)，然後按一下 **[動作]** > **[刪除]**。
7. [刪除所有備份時] 選擇該核取方塊，然後按一下 **[刪除]** 以確認您的決定。
8. [刪除特定備份時] 按一下 **[刪除]** 以確認您的決定。

在 [備份儲存] 索引標籤上

此程序適用於線上和離線工作負載。

1. 在 Cyber Protect 主控台中，移至 **[備份儲存]**。
2. 選擇您要從中刪除備份的位置。
3. 選擇您要從中刪除備份的備份存檔。
   存檔名稱使用以下範本：
   - 非雲端對雲端備份存檔：<工作負載名稱> - <保護計劃名稱>
   - 雲端對雲端備份存檔：<使用者名稱> 或 <磁碟機名稱> 或 <團隊名稱> - <雲端服務> - <保護計劃名稱>
4. [若要刪除整個備份存檔] 按一下 **[刪除]**。
   刪除備份存檔會刪除該存檔中的所有備份。
5. [若要刪除備份存檔中的特定備份] 按一下 **[顯示備份]**。
   a. 選擇您要刪除的備份 (復原點)。
   b. 按一下 **[動作]** > **[刪除]**。
6. [刪除備份存檔時] 選擇該核取方塊，然後按一下 **[刪除]** 以確認您的決定。
7. [刪除特定備份時] 按一下 **[刪除]** 以確認您的決定。

在 Web Restore 主控台中

此程序僅適用於雲端儲存中的備份存檔。

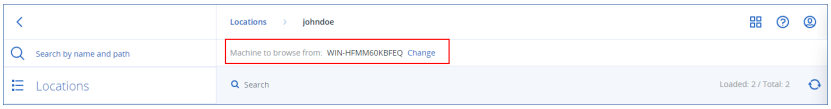
1. 在 Cyber Protection 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 選擇您要刪除的工作負載備份，然後按一下 **[復原]**。
3. [如果有多個備份位置可供使用] 選擇備份位置，然後按一下 **[更多復原方式]**。
4. 按一下 **[下載檔案]**。
   系統會將您重新導向到 Web Restore 主控台。
5. 在 Web Restore 主控台的 **[電腦]** 下，按一下工作負載名稱。
6. 在 **[上一個版本]** 下，按一下日期，然後按一下 **[刪除]**。
   此動作僅適用於備份存檔層級。您無法向下鑽研存檔並從中刪除特定備份。
7. 按一下 **[刪除]** 以確認您的決定。

刪除 Cyber Protect 主控台外的備份

建議您使用 Cyber Protect 主控台刪除備份。如果您使用 Web Restore 主控台刪除雲端儲存中的備份，或使用檔案管理員刪除本機備份，則必須重新整理備份位置，以便將變更同步到 Cyber Protect 主控台。

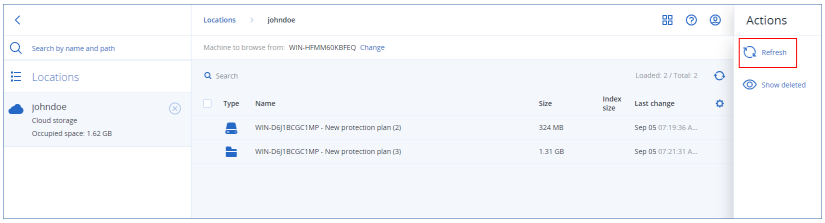
先決條件

- 您必須在 主控台中，選擇可以存取備份位置的線上代理程式作為**要瀏覽的電腦**。



若要重新整理備份位置

1. 在 Cyber Protect 主控台中，移至 **[備份儲存]**。
2. 選擇儲存已刪除備份的備份位置。
3. 在 **[動作]** 窗格中，按一下 **[重新整理]**。



瞭解瓶頸偵測

瓶頸偵測功能透過醒目提示備份或復原程序期間系統中最慢的元件，有助於您瞭解可以在哪些方面提高效能。

在進行任何傳輸時一定會發生瓶頸，因此不一定意味著需要解決瓶頸。您的備份速度可能已經夠快，完全滿足您的備份時段要求，而且符合您的 SLA，因此通常不需要您實際解決任何問題。

您可以在 **[活動詳細資料]** 索引標籤中輕鬆地檢視並追蹤瓶頸。方法是，在 Cyber Protect 主控台中，前往 **[監控] > [活動]**，然後按一下相關的活動。如需有關檢視瓶頸的詳細資訊，請參閱 "檢視瓶頸詳細資料" (第 478 頁) 和 "瓶頸會顯示在哪些工作負載、代理程式和備份位置上？" (第 479 頁)。

什麼是瓶頸？

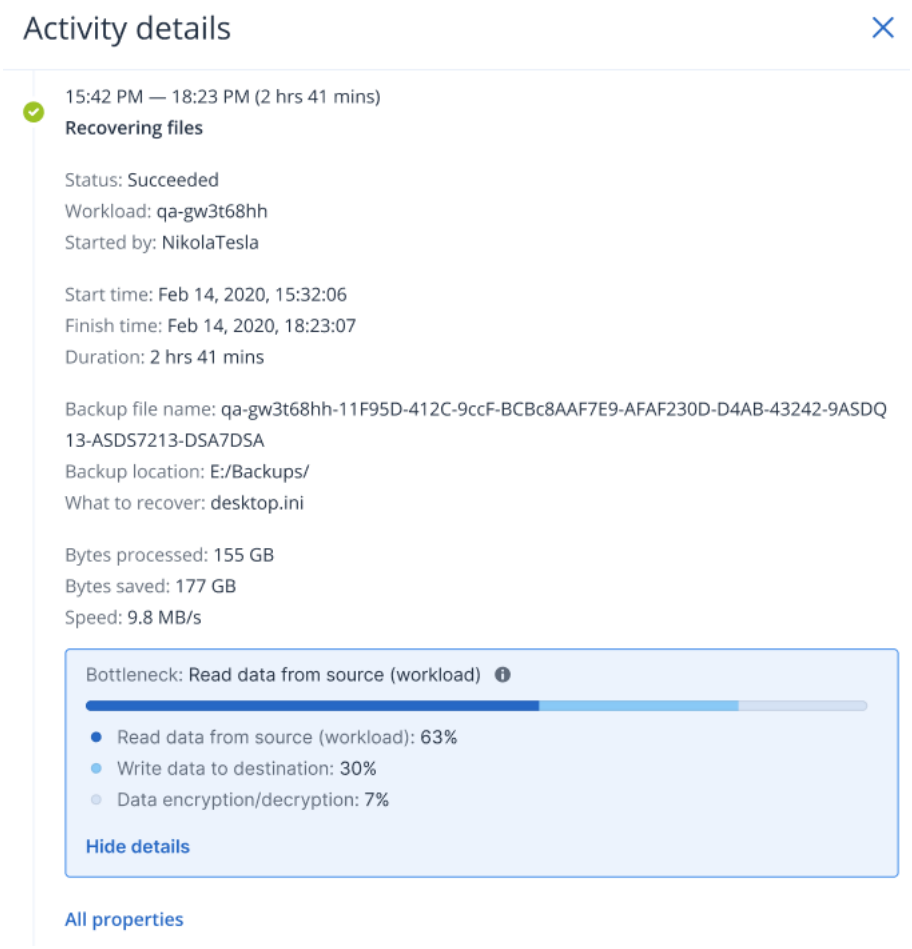
瓶頸通常是因為處理鏈中的元件緩慢 (換句話說，其他元件等待的元件) 所造成。

瓶頸偵測功能可讓您在備份和復原程序期間追蹤這些緩慢的元件，這有助於您瞭解以下哪些元件類型最慢：

- **來源**：您一眼就能確定從備份/復原來源讀取的速度是否造成瓶頸。
- **目的地**：瞭解寫入備份/復原目的地的速度是否影響效能。
- **代理程式**：瞭解代理程式處理資料的速度是否夠快。

瓶頸類型 (無論是來自來源、目的地還是代理程式) 都可能在備份/復原活動期間的不同時間發生變化。以下 **[活動詳細資料]** 索引標籤 **[瓶頸]** 區段中顯示的百分比 (例如，**[從來源讀取資料 (工作負載)：63%]**) 表示遇到此類型瓶頸時的時間百分比。在此案例中，在 63% 的復原活動時間內，瓶頸類型是讀取資料，換句話說，代理程式從備份存檔讀取資料的速度慢。

同樣地，在 30% 的時間內，瓶頸是由於將資料寫入復原目的地的速度慢 (**[將資料寫入目的地：30%]**)。



注意事項

在 **[活動詳細資料]** 索引標籤中查看瓶頸統計資料是正常行為。這些統計資料僅適用於時間長度超過一分鐘的工作。

如何減少瓶頸

如上所提及，瓶頸偵測功能會醒目提示備份元件之間的*讀取*和*寫入*資料流程。*讀取*統計資料是指從資料來源到執行備份/復原作業之代理程式的資料流程，而*寫入*讀取資料則是指代理程式和備份存檔 (目的地) 之間的資料流程。

為減少瓶頸並提高讀取/寫入資料流程效能，您應該分析代理程式和資料來源/備份存檔之間的通道。例如，如果代理程式正在備份一些本機檔案，您可以嘗試對硬碟進行基準測試。

檢視瓶頸詳細資料

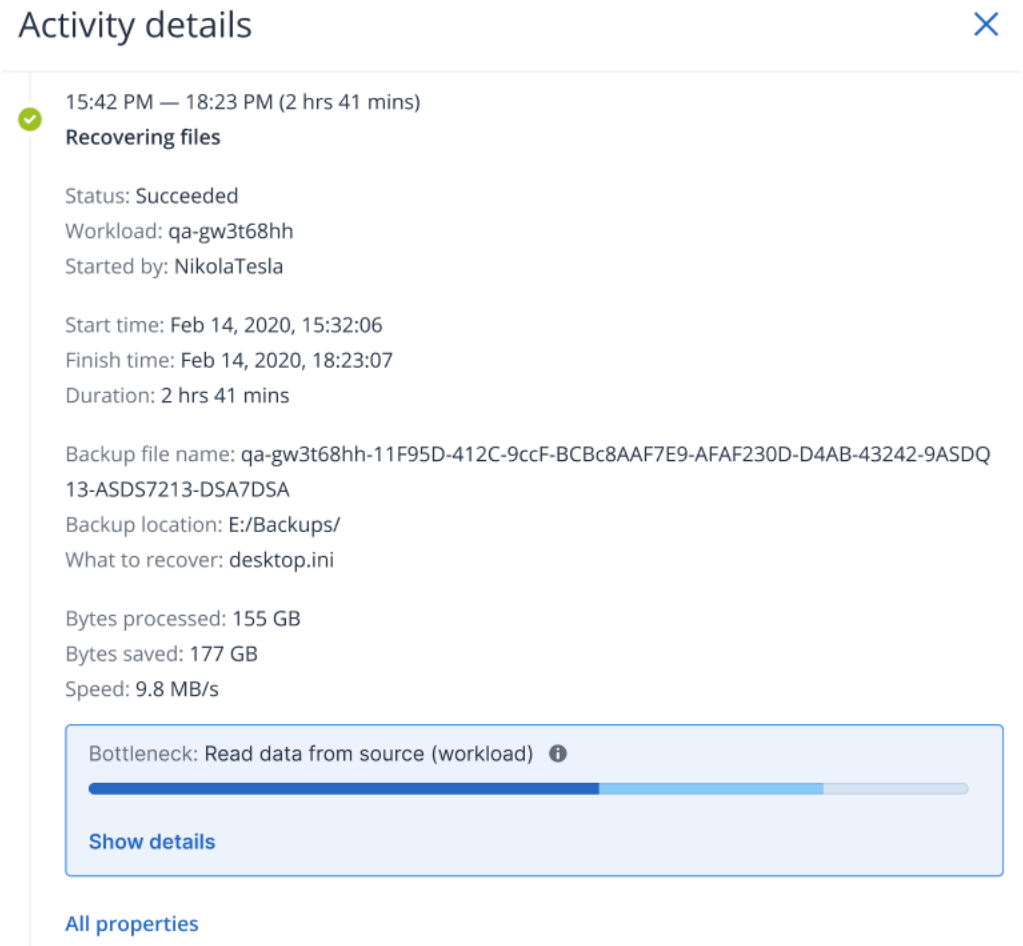
您可以針對任何備份類型、備份複寫或復原程序 (復原至任何類型的目的地資料夾或位置), 包括虛擬機器備份、電腦備份和檔案/資料夾備份, 檢視偵測到的瓶頸。您也可以檢視虛擬機器複寫和容錯回復活動的瓶頸。

如需有關瓶頸類型定義和核心概念的詳細資訊, 請參閱 "瞭解瓶頸偵測" (第 476 頁)。

若要檢視瓶頸詳細資料

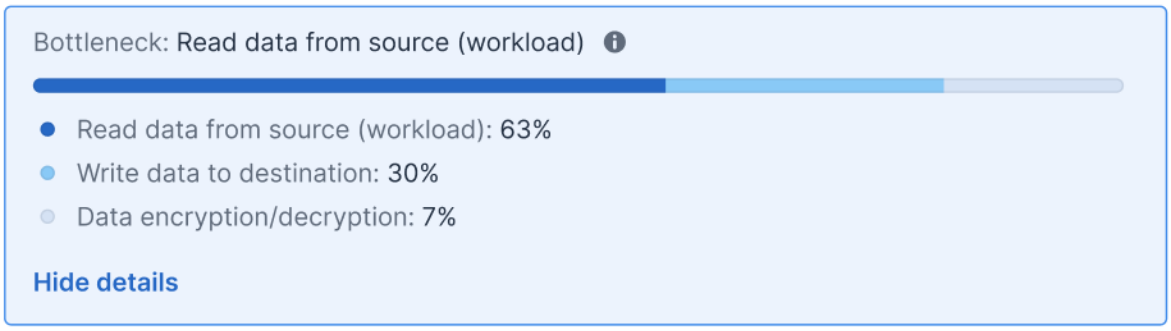
1. 在 Cyber Protect 主控台中, 前往 **[監控] > [活動]**。
2. 按一下相關的活動。

   在 **[活動詳細資料]** 索引標籤中, **[瓶頸]** 區段是以藍色顯示。



3. 按一下 **[顯示詳細資料]** 可在備份/復原作業期間檢視最常遇到的瓶頸。

   [瓶頸] 區段展開可顯示相關瓶頸類型的摘要。



在上述範例中，佔整個操作時間 63% 的瓶頸是由 *[讀取]* 作業 (由代理程式執行) 所造成。

注意事項
瓶頸值會在對應的活動正在執行時，以動態方式每分鐘更新一次。

瓶頸會顯示在哪些工作負載、代理程式和備份位置上？

瓶頸偵測適用於下列類型的工作負載、代理程式和備份位置：

- 磁碟/映像層級備份執行者：
  - Azure 用代理程式
  - Windows 用代理程式
  - Linux 用代理程式
  - Mac 用代理程式
  - VMware 用代理程式 (虛擬裝置和 Windows，包括 VM 複寫以及從複本容錯回復 (從複本還原) 活動)
  - Hyper-V 用代理程式
  - Scale Computing 用代理程式
  - oVirt (KVM) 代理程式
  - Virtuozzo Infrastructure Platform 用代理程式
  - Virtuozzo 用代理程式
  - VMware Cloud Director 用代理程式 (vCD-BA)
- 檔案層級備份
  - Windows 用代理程式
  - Linux 用代理程式
  - Mac 用代理程式
- 應用程式層級備份
  - SQL 用代理程式
  - Exchange 用代理程式
  - MySQL/MariaDB 用代理程式
  - 適用於 Oracle 的代理程式
  - SAP HANA 用代理程式

- 備份位置
  - Acronis 雲端儲存 (包括合作夥伴託管儲存空間)
  - 公有雲端儲存
  - 網路共用 (SMB + NFS)
  - 本機資料夾
  - 指令碼所定義的位置
  - Acronis Secure Zone

將工作負載備份至公有雲端

注意事項
此功能是 [Advanced Backup] 套件的一部分，而後者則是 [資安防護] 服務的一部分。請注意，當您將此功能新增至保護計劃時，您可能需要支付額外費用。

您可以在 Cyber Protect 主控台中選擇公有雲端服務 (例如 Microsoft Azure、Amazon S3 (Simple Storage Service) 和 Wasabi) 作為備份目的地。

若要在公有雲端上設定備份位置，您必須是公司系統管理員或單位系統管理員，或者已在 [資安防護] 服務中定義以下其中一個角色：網路系統管理員、系統管理員或使用者。

在 Microsoft Azure 中定義備份位置

注意事項
若要在 Microsoft Azure 上設定備份位置，您必須已經在資安防護服務中定義以下其中一個角色：公司系統管理員、使用者、網路系統管理員。

若要將工作負載備份至 Microsoft Azure，您需要在 Cyber Protect 主控台中定義 Microsoft Azure 備份位置，然後連線至相關的 Microsoft Azure 訂購授權。這可以透過下列方式完成：

- 建立或編輯保護計劃時。
- 定義和管理備份儲存位置時。

重要事項
系統管理員和非系統管理員使用者都可以將工作負載備份至 Microsoft Azure。

非系統管理員使用者可以新增 Microsoft Azure 訂購授權的存取權 (請參閱 "管理對 Microsoft Azure 訂購授權的存取" (第 492 頁))，但僅能套用備份位置連線至其自行新增之 Microsoft Azure 訂購授權的保護計劃，並針對在 Cyber Protect 主控台中，以其名稱註冊的工作負載套用。

系統管理員可以套用備份位置連線至其自行新增之 Microsoft Azure 訂購授權的保護計劃，並針對在 Cyber Protect 主控台中，以任何使用者身分註冊的工作負載套用。

若要在 Microsoft Azure 中定義備份位置

1. 在 Cyber Protect 主控台中，執行下列其中一項操作：
   - 如果您要建立或編輯保護計劃，請移至 **[裝置]**，然後選擇您要備份至 Microsoft Azure 的相關工作負載。在所選工作負載之保護計劃的 **[備份]** 區段中，按一下 **[備份位置]** 列中的連結。

     如需有關使用保護計劃的詳細資訊，請參閱 "保護計劃和模組" (第 191 頁)。
   - 如果您要管理備份儲存位置，而且想要將 Microsoft Azure 當作新位置新增，請移至 **[備份儲存]**。

     如需有關管理備份儲存位置的詳細資訊，請參閱 "備份儲存索引標籤" (第 470 頁)。
2. 按一下 **[新增位置]**。
3. 從 **[公有雲端]** 下拉式清單中，選擇 **[Microsoft Azure]**。
4. 如果已在 Cyber Protect 主控台中註冊相關的 Microsoft Azure 訂購授權，請從訂購授權清單中選擇該訂購授權。

   如果未在 Cyber Protect 主控台中定義相關的訂購授權，按一下 **[新增]**，然後在顯示的對話方塊中，按一下 **[登入]**。系統會將您重新導向至 Microsoft 登入頁面。如需有關新增和定義 Microsoft Azure 訂購授權存取權的詳細資訊，請參閱 "將存取權新增至 Microsoft Azure 訂購授權" (第 492 頁)。
5. 在 **[儲存體帳戶]** 欄位中，選擇相關的帳戶。

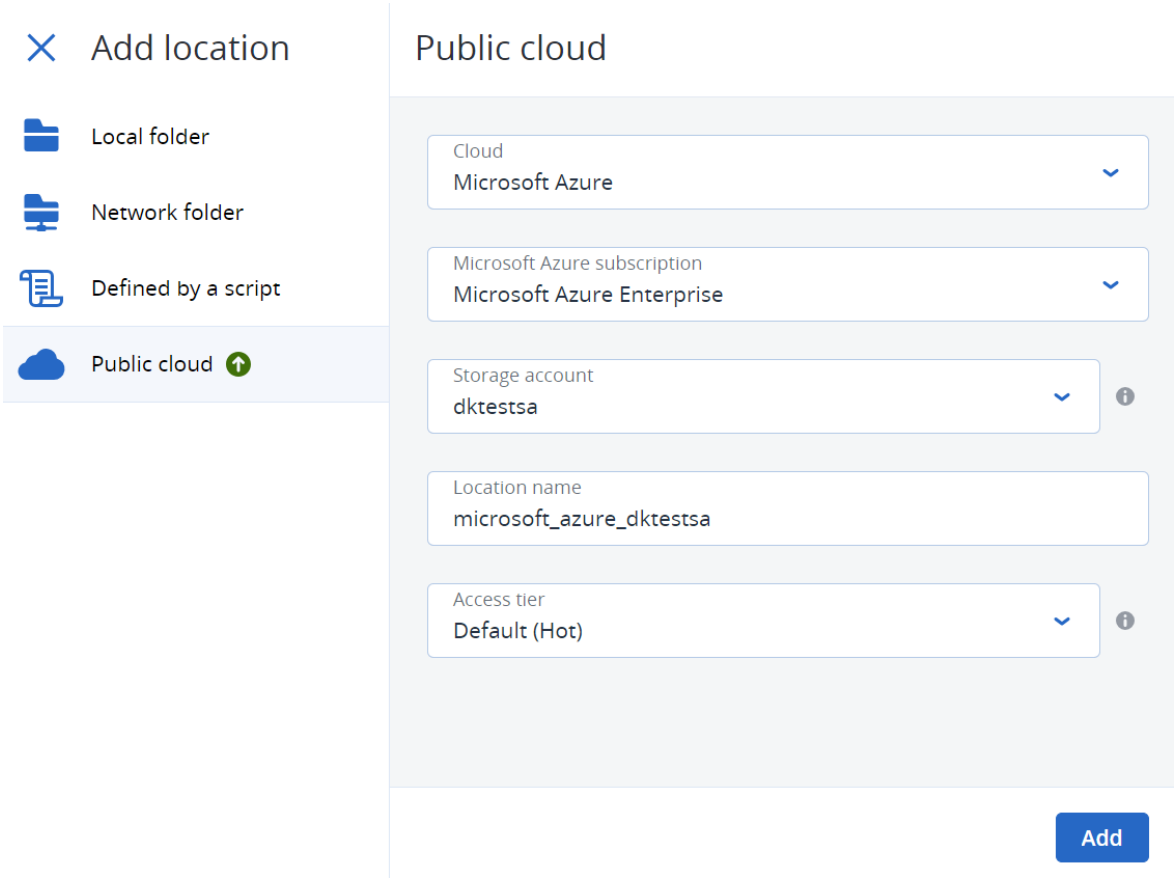
   注意事項

   目前僅支援一般端點尾碼包含 `core.windows.net` 的 Microsoft Azure 儲存體帳戶。此外，所選儲存體帳戶必需是 StorageV2 帳戶類型。

   預設會根據所選儲存體帳戶，自動填入 **[位置名稱]** 和 **[存取層]** 欄位。顯示的位置名稱為 `microsoft_azure_[儲存體帳戶]`，所選存取層則為 **[預設 (即時)]**。兩個欄位都可以視需要修改。

   注意事項

   變更位置名稱時，請輸入唯一的位置名稱 (此名稱對客戶租用戶必須是唯一的)。如果您新增的名稱已存在於儲存體帳戶中，Acronis 會在名稱中新增尾碼編號。例如，如果 **Microsoft Azure Storage** 已存在，該名稱會自動更新為 **Microsoft Azure Storage_01**。



6. 按一下 **[新增]**。

   如果您要建立或編輯保護計劃，Microsoft Azure 備份位置會設定為 **[備份位置]** 中的位置。執行備份 (手動或排程) 時，備份會儲存在已定義的位置。

   如果您要管理備份儲存位置，可以檢視位置詳細資料並視需要更新。定義工作負載的備份位置時，也可以使用 Microsoft Azure 位置。如需詳細資訊，請參閱 "檢視和更新公有雲端備份位置" (第 487 頁)。

在 Amazon S3 中定義備份位置

注意事項

若要在 Amazon S3 上設定備份位置，您必須已經在資安防護服務中定義以下其中一個角色：公司系統管理員、使用者、網路系統管理員。

若要將工作負載備份到 Amazon S3，您必須在 Cyber Protect 主控台中定義 Amazon S3 備份位置，然後連線到相關的 Amazon S3 連線。您可以透過以下方式執行此操作：

- 建立或編輯保護計劃時。
- 定義和管理備份儲存位置時。

重要事項

系統管理員和非系統管理員使用者都可以將工作負載備份至 Amazon S3。

非系統管理員使用者可以新增 Amazon S3 連線的存取權 (請參閱 "管理對其他公有雲端儲存服務的存取權" (第 495 頁)), 但僅能套用備份位置連線至其自行新增之 Amazon S3 連線的保護計劃, 並針對在 Cyber Protect 主控台中, 以其名稱註冊的工作負載套用。

系統管理員可以套用備份位置連線至其自行新增之 Amazon S3 連線的保護計劃, 並針對在 Cyber Protect 主控台中, 以任何使用者身分註冊的工作負載套用。

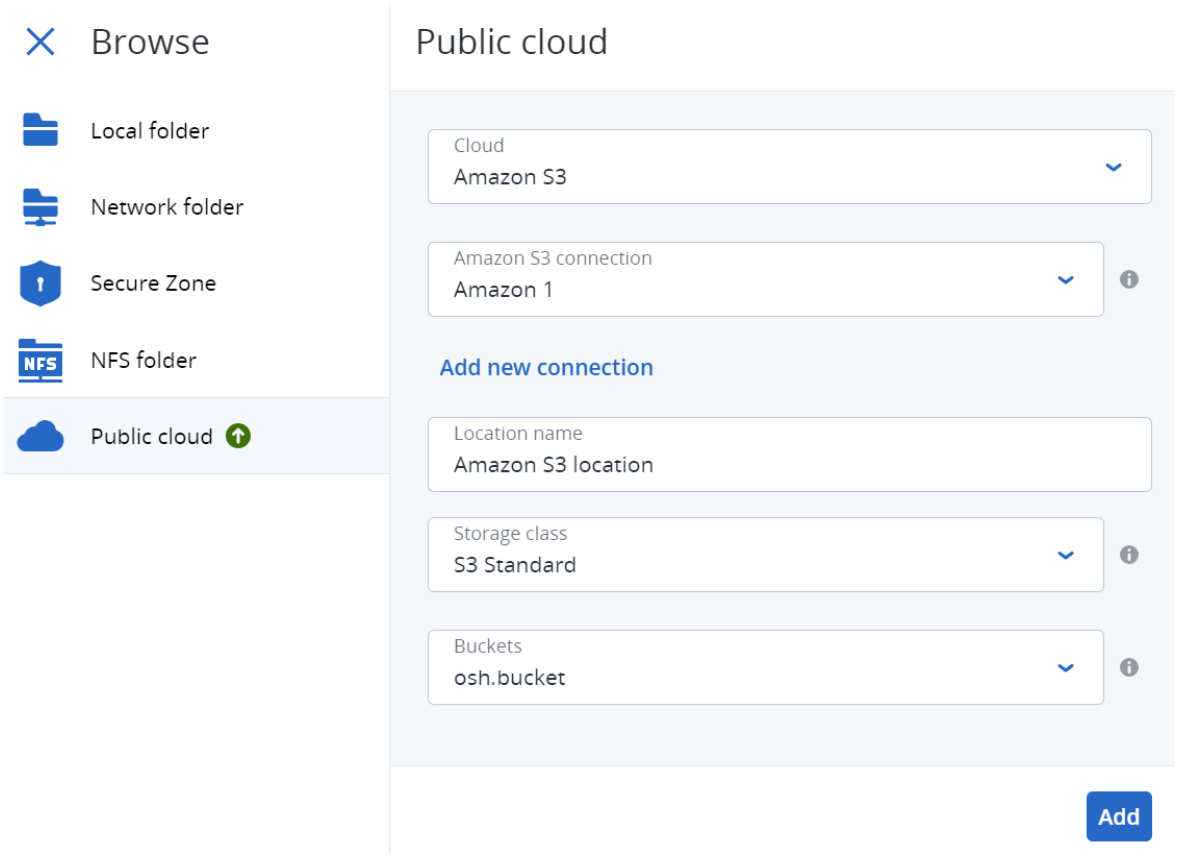
若要在 Amazon S3 中定義備份位置

1. 在 Cyber Protect 主控台中, 執行下列其中一項操作:
   - 如果您要建立或編輯保護計劃, 請移至 **[裝置]**, 然後選擇您要備份至 Amazon S3 的工作負載。在所選工作負載之保護計劃的 **[備份]** 區段中, 按一下 **[備份位置]** 列中的連結。

     如需有關使用保護計劃的詳細資訊, 請參閱 "保護計劃和模組" (第 191 頁)。
   - 如果您要管理備份儲存位置, 而且想要將 Amazon S3 當作新位置新增, 請移至 **[備份儲存]**。

     如需有關管理備份儲存位置的詳細資訊, 請參閱 "備份儲存索引標籤" (第 470 頁)。
2. 按一下 **[新增位置]**。
3. 從 **[公有雲端]** 下拉式清單中, 選擇 **[Amazon S3]**。
4. 如果已在 Cyber Protect 主控台中註冊相關的 Amazon S3 連線, 請從清單中選擇該連線。

   如果沒有在 Cyber Protect 主控台中註冊相關連線, 按一下 **[新增連線]**。如需有關新增和定義對 Amazon S3 連線的存取的詳細資訊, 請參閱 "新增對公有雲端連線的存取權" (第 495 頁)。新增連線後, 請繼續下一步。



5. 定義下列項目：
   - 在 **[位置名稱]** 欄位中，輸入備份位置的名稱。

     注意事項
     位置名稱對於客戶租用戶必須是唯一的。如果您新增的名稱已存在於連線中，Acronis 會為該名稱加上尾碼。例如，如果 **Amazon S3 storage** 已存在，則名稱將自動更新為 **Amazon S3 storage 1**。

   - 在 **[儲存類別]** 欄位中，選擇以下其中一個支援的儲存類別：
     - S3 Standard
     - Standard - 不經常存取 (S3 Standard-IA)
     - One Zone - 不經常存取 (S3 One Zone-IA)
     - S3 Intelligent Tiering
   - 在 **[儲存貯體]** 欄位中，選擇相關的 Amazon S3 儲存貯體。
     如果所選儲存貯體已啟用 [物件鎖定] 和 [物件版本控制] 功能 (這些功能是在 AWS 管理主控台中啟用的)，則會啟用 **[備份不可變期間 (天)]** 核取方塊。接著，您可以定義不可變期間的天數，這可確保在此期間內不會刪除備份的資料，並將其套用至 Acronis 建立的所有備份物件。請注意，當您將不可變期間設為備份位置屬性時，AWS 管理主控台中為儲存貯體定義的預設保留期間將會遭到忽略。如需有關 [物件鎖定] 功能和保留期間的詳細資訊，請參閱 Amazon S3 文件。

注意事項

24.05 版之前的代理程式可以備份至 Amazon S3，但只有 24.05 版或更高版本的代理程式才能將 [物件鎖定] 套用至在 Amazon S3 儲存空間中建立的物件。也就是說，只有更新的代理程式可以確認不可變期間設定為備份位置屬性，並針對所有建立的備份管理此期間。24.05 版之前的代理程式將會忽略此設定，並將預設儲存貯體的 [物件鎖定] 屬性 (在 AWS 管理主控台中或透過 API 定義) 套用到在 Amazon S3 中建立的物件。

6. 按一下 **[新增]**。

   如果您要建立或編輯保護計劃，Amazon S3 備份位置將設定為 **[備份位置]** 列中的位置。執行備份 (手動或按排程) 時，備份將儲存在已定義的位置。

   如果您要管理備份儲存位置，可以檢視位置詳細資料並視需要更新。定義工作負載的備份位置時，也可以使用 Amazon S3 位置。如需詳細資訊，請參閱 "檢視和更新公有雲端備份位置" (第 487 頁)。

在 Wasabi、Impossible Cloud 或 S3 相容儲存空間中定義備份位置

注意事項

若要在 Wasabi、Impossible Cloud 或 S3 相容儲存裝置中設定備份位置，您必須已經在資安防護服務中定義以下其中一個角色：公司系統管理員、使用者、網路系統管理員。

若要將工作負載備份至 Wasabi、Impossible Cloud 或 S3 相容儲存空間，則必須在 Cyber Protect 主控台中定義備份位置，並連線至相關的 Wasabi、Impossible Cloud 或 S3 相容儲存空間連線。您可以使用下列方式進行：

- 建立或編輯保護計劃時。
- 定義和管理備份儲存位置時。

重要事項

系統管理員和非系統管理員使用者都可以將工作負載備份至 Wasabi、Impossible Cloud 或 S3 相容儲存空間。

非系統管理員使用者可以新增 Wasabi、Impossible Cloud 或 S3 相容儲存空間連線的存取權 (請參閱 "管理對其他公有雲端儲存服務的存取權" (第 495 頁))，但僅能套用備份位置連線至其自行新增之 Wasabi、Impossible Cloud 或 S3 相容儲存空間連線的保護計劃，並針對在 Cyber Protect 主控台中，以其名稱註冊的工作負載套用。

系統管理員可以套用備份位置連線至其自行新增之 Wasabi、Impossible Cloud 或 S3 相容儲存空間連線的保護計劃，並針對在 Cyber Protect 主控台中，以任何使用者身分註冊的工作負載套用。

若要在 Wasabi、Impossible Cloud 或 S3 相容儲存空間中定義備份位置

1. 在 Cyber Protect 主控台中，執行下列其中一項操作：
   - 如果您要建立或編輯保護計劃，請移至 **[裝置]**，然後選擇您要備份至 Wasabi、Impossible Cloud 或 S3 相容儲存空間的工作負載。在所選工作負載保護計劃的 **[備份]** 區段中，按一下

[備份位置] 列中的連結。

如需有關使用保護計劃的詳細資訊，請參閱 "保護計劃和模組" (第 191 頁)。

- 如果您要管理備份儲存位置，而且想要將 Wasabi、Impossible Cloud 或 S3 相容儲存空間當作新位置新增，請移至 **[備份儲存]**。

  如需有關管理備份儲存位置的詳細資訊，請參閱 "備份儲存索引標籤" (第 470 頁)。

2. 按一下 **[新增位置]**。
3. 從 **[公有雲端]** 下拉式清單中，選擇下列其中一項：
   - **Wasabi**
   - **S3 相容**
   - **Impossible Cloud**
4. 如果已在 Cyber Protect 主控台中註冊相關連線，請從連線清單中選擇該連線。

   如果沒有在 Cyber Protect 主控台中註冊相關連線，按一下 **[新增連線]**。如需有關新增和定義對 Wasabi、Impossible Cloud 或 S3 相容儲存空間連線的存取的詳細資訊，請參閱 "新增對公有雲端連線的存取權" (第 495 頁)。新增連線後，請繼續進行下一步。

   重要事項

   您無法在 Wasabi 上使用根使用者帳戶的存取金鑰，因為根使用者無法呼叫 AssumeRole。您應該建立一個單獨的非根使用者，並為該使用者產生存取金鑰。

5. 定義下列項目：
   - 在 **[位置名稱]** 欄位中，輸入備份位置的名稱。

     注意事項

     位置名稱對於客戶租用戶必須是唯一的。如果您新增的名稱已存在於連線中，Acronis 會為該名稱加上尾碼。例如，如果 **Wasabi storage** 已存在，則名稱將自動更新為 **Wasabi storage 1**。

   - (僅限 Impossible Cloud) 在 **[區域]** 欄位中，選擇相關區域。
   - 在 **[儲存貯體]** 欄位中，選擇相關的 Wasabi、Impossible Cloud 或 S3 相容儲存空間儲存貯體。

     如果所選儲存貯體已啟用 [物件鎖定] 和 [版本控制] 功能，則會啟用 **[備份不可變期間 (天)]** 核取方塊。接著，您可以定義不可變期間的天數，這可確保在此期間內不會刪除備份的資料，並將其套用至 Acronis 建立的所有備份物件。

     請注意，當您將不可變期間設為備份位置屬性時，為儲存貯體定義的預設保留期間將會遭到忽略。如需有關 [物件鎖定] 功能和保留期間的詳細資訊，請參閱相關文件，如需範例，請參閱 Impossible Cloud 文件。

注意事項

24.06 版之前的代理程式可以備份至 Wasabi、Impossible Cloud 或 S3 相容儲存空間，但只有 24.06 版或更高版本的代理程式才能將 [物件鎖定] 套用至在 Wasabi、Impossible Cloud 或 S3 相容儲存空間中建立的物件。也就是說，只有更新的代理程式可以確認不可變期間設定為備份位置屬性，並針對所有建立的備份管理此期間。24.06 版之前的代理程式將會忽略此設定，並將預設儲存貯體的 [物件鎖定] 屬性套用到在 Wasabi、Impossible Cloud 或 S3 相容儲存空間中建立的物件。

6. 按一下 **[新增]**。

   如果您要建立或編輯保護計劃，Wasabi、Impossible Cloud 或 S3 相容儲存空間備份位置將設定為 **[備份位置]** 列中的位置。執行備份 (手動或按排程) 時，備份將儲存在已定義的位置。

   如果您要管理備份儲存位置，可以檢視位置詳細資料並視需要更新。定義工作負載的備份位置時，也可以使用 Wasabi、Impossible Cloud 或 S3 相容儲存空間位置。如需詳細資訊，請參閱 "檢視和更新公有雲端備份位置" (第 487 頁)。

檢視和更新公有雲端備份位置

您可以檢視和更新您在 **[備份儲存]** 模組中，或在建立或編輯保護計劃時定義的 Microsoft Azure、Amazon S3 和 Wasabi 備份位置。

如需從 Cyber Protect 主控台移除對 Microsoft Azure 訂閱存取權的相關資訊，請參閱 "移除 Microsoft Azure 訂購授權的存取權" (第 494 頁)。如需移除對其他公有雲端連線存取權的相關資訊，請參閱 "管理對其他公有雲端儲存服務的存取權" (第 495 頁)。

注意事項

您無法手動重新整理或刪除 **[備份儲存]** 模組中的公有雲端備份位置。每次備份或復原作業後，都會自動更新備份位置的內容。

若要檢視公有雲端備份位置

1. 在 Cyber Protect 主控台中，移至 **[備份儲存]**。

   備份位置清單隨即顯示，其中包含指派給每個位置的儲存容量和備份數量的詳細資料。

   如需有關使用所列備份位置的詳細資訊，請參閱 "備份儲存索引標籤" (第 470 頁)。
2. 選擇相關的位置。

   系統會列出所選位置的所有目前備份。
3. (選擇性) 按一下某個備份以檢視該備份的詳細資料。

若要更新保護計劃中的公有雲端備份位置

1. 移至相關的保護計劃，然後選擇 **[編輯]**。
2. 按一下 **[備份位置]** 列中的連結。
3. 從現有的備份位置清單中選擇，或按一下 **[新增位置]** 以新增位置。

   如果相關的 Microsoft Azure 訂購授權或公有雲端連線已在 Cyber Protect 主控台中訂閱，請從顯示的清單中選擇它。

如果您要新增 Microsoft Azure 訂閱，您將會收到驗證 Microsoft 帳戶詳細資料的提示 (請參閱 "將存取權新增至 Microsoft Azure 訂購授權" (第 492 頁))。如需有關連線至 Microsoft Azure 時所需權限的詳細資訊，請參閱 Microsoft Azure 連線安全性和稽核 (72684) 一文。

管理公有雲端帳戶存取權

若要在公有雲端平台中啟用 Acronis Cyber Protection 服務，則需要設定對相關公有雲端帳戶的存取權。

例如，使用 Microsoft Azure 時，需要對 Microsoft Azure 訂購授權的存取權。一旦新增到 Cyber Protect 主控台後，當您設定直接備份到 Microsoft Azure 時，就可以選擇訂購授權。同樣地，使用 Amazon S3 和 Wasabi 時，需要與特定備份相關原則相關聯的相關存取金鑰。

對公有雲端的存取權是透過 主控台中的 **[基礎架構]** 功能表管理的。

重要事項
對公有雲端儲存空間上的備份停用備份驗證，以避免過多的出口流量成本。此外，如果公有雲端上的備份位置之前遭到移除，則您目前無法將其「重新附加」到相同或不同的客戶租用戶。如需詳細資訊，請聯絡支援團隊。

備份到公有雲端儲存空間所需的存取需求

直接備份到公有雲端儲存服務時，每個平台都需要考慮許多存取需求：

- Microsoft Azure
- Amazon S3
- S3 相容儲存空間 (包括 Wasabi 和 Impossible Cloud)

備份到 Microsoft Azure

若要連線到 Microsoft Azure 訂購授權，您必須擁有多個權限。如需有關這些權限的詳細資訊，請參閱 Microsoft Azure 連線安全性和稽核 (72684) 一文。

注意事項
您必須在 Microsoft Azure AD 中獲指派以下其中一個角色，才能完成與訂購授權的連線：雲端應用程式系統管理員、應用程式系統管理員或全域系統管理員。您也必須獲指派每個所選訂購授權的擁有者角色。

備份到 Amazon S3

如果您要備份到 Amazon S3，定義 Amazon S3 備份位置時有幾個需求：

- 支援的儲存類別
- 原則權限
- 存取金鑰
- 儲存貯體設定

支援的儲存類別

目前支援以下 Amazon S3 儲存類別：

- S3 Standard
- Standard - 不經常存取 (S3 Standard-IA)
- One Zone - 不經常存取 (S3 One Zone-IA)
- S3 Intelligent Tiering

原則權限

當您備份到 Amazon S3 時，您的 Amazon 帳戶必須套用最低權限，以確保 Acronis 可以將相關的工作負載備份到 Amazon S3。這意味著相關使用者應該可以存取 AWS 管理主控台，並將相關原則套用到其獲指派的群組。

注意事項
針對 Amazon S3 指定的原則權限可供其他 S3 相容儲存空間服務重複使用。如需詳細資訊，請參閱 "備份至 S3 相容儲存空間 (包括 Wasabi 和 Impossible Cloud)" (第 490 頁)。

範例

下列範例原則顯示在備份至特定儲存貯體 (以 [BUCKETNAME] 表示)，並從特定儲存貯體復原時，各種資源所需的一組最低權限。請注意，* 表示所有資源。

```
{ "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]/*" } ] }
```

以下範例原則顯示帳戶中任何儲存貯體的最低權限。請注意，[BUCKETNAME] 應該取代為儲存貯體的名稱。

```
{ "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:::*" } ] }
```

存取金鑰

每個 Amazon S3 連線都需要存取金鑰，而且會在定義 Amazon S3 連線時使用。如需有關產生存取金鑰和存取金鑰 ID 的詳細資訊，請參閱 Amazon S3 文件。

儲存貯體設定

使用 Amazon S3 儲存貯體作為備份位置時，請確認已使用預設設定來設定儲存貯體，包括封鎖所有公開存取 (預設設定為 **[開啟]**)。如需有關使用儲存貯體的詳細資訊，請參閱 Amazon S3 文件。

注意事項

原則權限中的範例包括一組完整的權限。如果您在儲存貯體上不需要使用不可變，則可以排除相關的權限，例如 `s3:GetBucketObjectLockConfiguration` (用於建立和編輯備份位置) 和 `s3:GetObjectRetention` (用於偵測是否需要更新物件鎖定以縮短期間) 權限。

備份至 S3 相容儲存空間 (包括 Wasabi 和 Impossible Cloud)

如果您備份到 S3 相容儲存空間，定義備份位置時需要考慮許多要求：

- 原則權限
- 存取金鑰
- 儲存貯體設定

原則權限

當您在 S3 相容儲存空間中定義備份位置時，請確認相關的原則已套用到相關的群組和使用者。

注意事項

針對 Amazon S3 指定的原則權限 (請參閱上文) 可供其他 S3 相容儲存空間服務重複使用。請注意，`sts:GetFederationToken` 權限僅適用於 Wasabi，而且其他 S3 相容儲存空間服務不需要此權限。

範例

下列範例原則僅適用於 Wasabi，並顯示在備份至特定儲存貯體或從特定儲存貯體 (以 [BUCKETNAME] 表示) 時，各種資源所需的一組最低權限。請注意，* 表示任何資源。此外，請將 `[ACCOUNTID]` 取代為 Wasabi 帳戶的 ID。

```
{ "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]/*" } ] }
```

下列範例原則僅適用於 Wasabi，並顯示帳戶中任何儲存貯體的最低權限。

```
{ "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": "*" } ] }
```

下列範例原則適用於 S3 相容和 Impossible Cloud 儲存空間，並顯示資源範圍有限的有限權限。請注意，[BUCKETNAME] 應取代為儲存貯體的名稱。

```
{ "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]/*" } ] }
```

下列範例原則適用於 S3 相容和 Impossible Cloud 儲存空間，並顯示帳戶中任何儲存貯體的最低權限。

```
{ "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:::*" } ] }
```

存取金鑰

每個 S3 連線都需要存取金鑰，而且會在定義連線時使用。

請注意，無法使用 Wasabi 上根使用者帳戶的存取金鑰，因為根使用者無法呼叫 AssumeRole。您應該建立一個單獨的非根使用者，並為該使用者產生存取金鑰。

如需有關產生存取金鑰和存取金鑰 ID 的詳細資訊，請參閱相關文件。如需範例，請參閱 Wasabi 文件和 Impossible Cloud 文件。

儲存貯體設定

使用儲存貯體作為備份位置時，請確認已使用預設設定來設定儲存貯體。如需有關使用儲存貯體的詳細資訊，請參閱相關文件。如需範例，請參閱 Wasabi 文件和 Impossible Cloud 文件。

管理對 Microsoft Azure 訂購授權的存取

您可以透過連線至 Cyber Protect 主控台中的相關 Microsoft Azure 訂購授權，將相關的工作負載直接備份到 Microsoft Azure。

透過 **[裝置]** 或 **[備份儲存]** 功能表建立備份位置時，可以設定與訂購授權的連線，如 "在 Microsoft Azure 中定義備份位置" (第 480 頁) 中所述。

或者，您可以在 **[公有雲端]** 畫面 (前往 **[基礎架構] > [公有雲端]**) 中設定這些 Microsoft Azure 訂閱。您也可以在此處管理您的訂閱，包括續訂對訂閱的存取權、檢視訂閱屬性和活動，或移除訂閱。請注意，如果您要部署 Azure 用代理程式來執行 Microsoft Azure 虛擬機器的無代理程式備份，則會顯示一個額外的索引標籤，您可以在其中檢視和更新您的部署。如需詳細資訊，請參閱 "檢視及更新已部署的 Azure 用代理程式" (第 145 頁)。

根據您獲指派的使用者角色，您可以管理您組織中其他使用者新增的 Microsoft Azure 訂購授權。例如，如果您是公司系統管理員或單位系統管理員，或者在資安防護服務中獲指派網路系統管理員或系統管理員角色，則可以檢視和管理其他系統管理員所新增的 Microsoft Azure 訂購授權，以及非系統管理員使用者所新增的訂購授權。非系統管理員使用者僅能檢視和存取他們新增到 Cyber Protect 主控台的 Microsoft Azure 訂購授權。

注意事項
合作夥伴可以管理階層中低於其層級的客戶的 Microsoft Azure 訂購授權。不過，當合作夥伴選擇 **[所有客戶]** 時，將無法使用 主控台中的 **[基礎架構]** 功能表。

重要事項
連線至 Microsoft Azure 訂購授權時，Acronis 需要有最低權限，才能連線至訂購授權。如需有關所需權限的詳細資訊，請參閱 Microsoft Azure 連線安全性和稽核 (72684) 一文。

將存取權新增至 Microsoft Azure 訂購授權

透過在 Cyber Protect 主控台中新增 Microsoft Azure 訂購授權，Acronis 可以安全地存取您的訂購授權，並將相關的工作負載直接備份到 Microsoft Azure。

若要將存取權新增至 Microsoft Azure 訂購授權

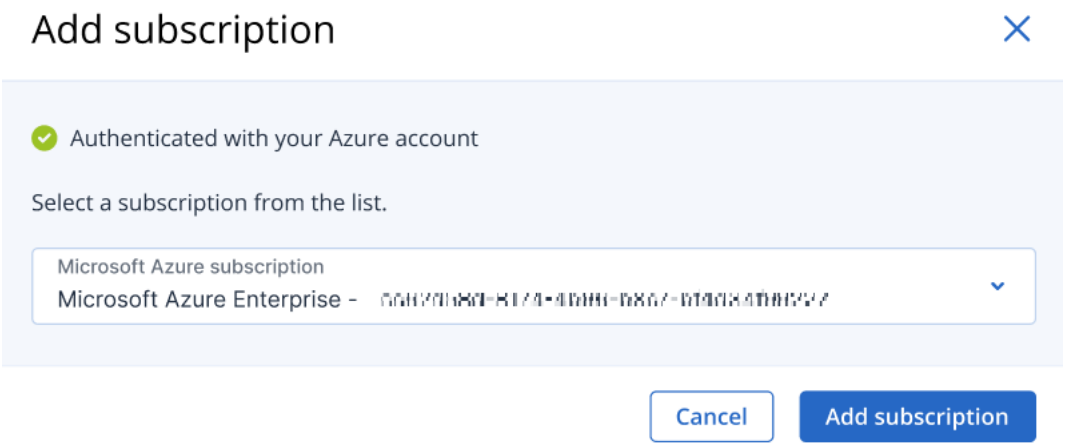
1. 在 Cyber Protect 主控台中，移至 **[基礎架構] > [公有雲端]**。
2. 按一下 **[新增]**，然後從顯示的選項清單中選擇 **[Microsoft Azure]**。
3. 在顯示的對話方塊中，按一下 **[登入]**。系統會將您重新導向至 Microsoft 登入頁面。

注意事項

您必須在 Microsoft Azure AD 中獲指派以下其中一個角色，才能完成與訂購授權的連線：雲端應用程式系統管理員、應用程式系統管理員或全域系統管理員。您也必須獲指派每個所選訂購授權的擁有者角色。

4. 在 Microsoft 登入畫面中，輸入您的登入認證，並接受要求的權限。連線程序隨即開啟，而且可能需要幾分鐘的時間。

   如需有關如何安全地存取 Microsoft Azure 和訂購授權的詳細資訊，請參閱 Microsoft Azure 連線安全性和稽核 (72684) 一文。
5. 當連線完成時，從所顯示的對話方塊中的下拉式清單選擇相關的訂購授權，然後按一下 **[新增訂購授權]**。



訂購授權隨即新增到公有雲端的清單中。

若要續訂訂購授權的每年存取憑證，請參閱 "續訂 Microsoft Azure 訂購授權的存取權" (第 493 頁)。

若要移除訂購授權的存取權，請參閱 "移除 Microsoft Azure 訂購授權的存取權" (第 494 頁)。

注意事項

如果您登入的 Microsoft Azure 帳戶包含對多個 Microsoft Azure AD (包括您以來賓使用者受邀的 AD) 的存取權，則只會選擇預設使用者目錄。如果您要使用您是來賓使用者身分的目錄，則需要在該特定 Microsoft Azure AD 中建立新的使用者。接著，您就可以登入該帳戶，並連線至相關的訂購授權。

續訂 Microsoft Azure 訂購授權的存取權

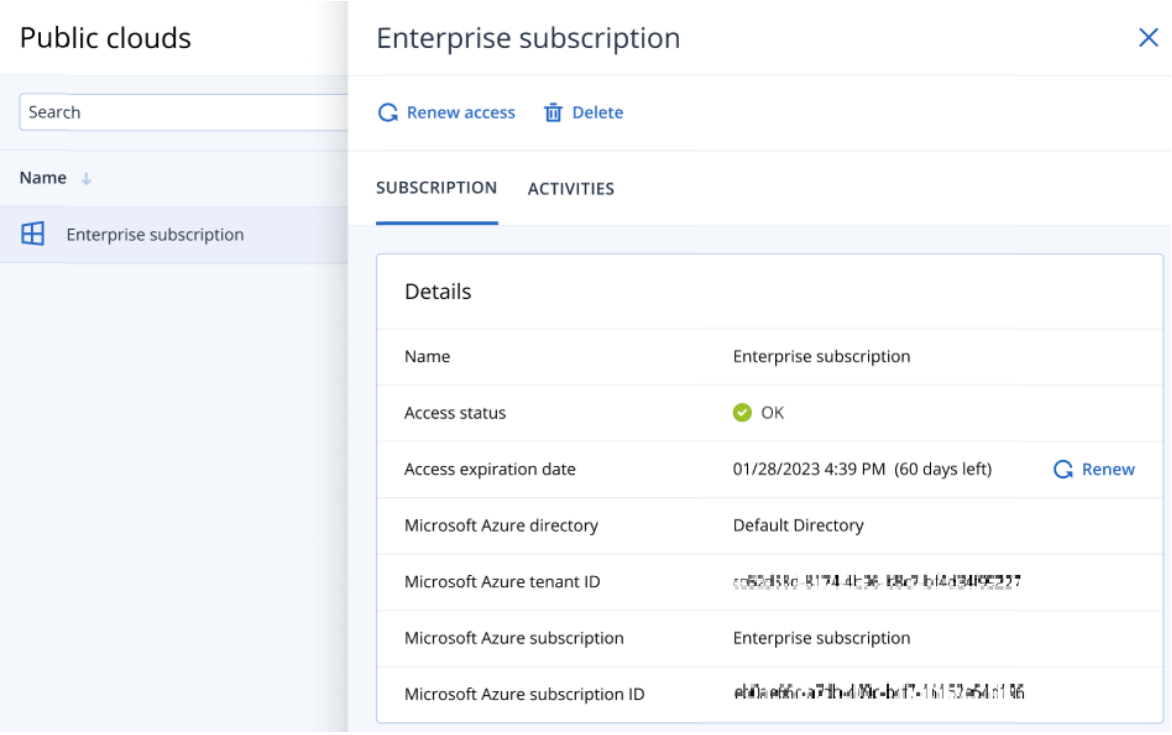
一旦在 Cyber Protect 主控台中註冊之後，Acronis 就可以使用免費且唯一的存取憑證，自動將 Microsoft Azure 訂購授權的存取權設定為續訂一年。當憑證接近其到期日時，您可以快速且輕鬆地續訂該憑證。

若要續訂 Microsoft Azure 訂購授權的存取憑證

1. 在 Cyber Protect 主控台中，移至 **[基礎架構] > [公有雲端]**。
2. 從顯示的清單中，選擇相關的訂購授權。

注意事項
[存取狀態]欄會指出每個訂購授權的存取憑證狀態，並顯示以下其中一個狀態：**[正常]**或 **[已到期]**。

3. 在右窗格中，按一下 **[續訂存取權]**。
   或者，按一下 **[訂購授權]**索引標籤，然後在 **[存取權到期日]**欄位中，按一下 **[續訂]**。



4. 在 Microsoft 登入畫面中，輸入您的登入認證，並接受要求的權限。連線程序隨即開啟，而且可能需要幾分鐘的時間。
   驗證成功後，存取權將自動續訂一年。
   如需有關所需權限的詳細資訊，請參閱 Microsoft Azure 連線安全性和稽核 (72684) 一文。

移除 Microsoft Azure 訂購授權的存取權

如果您不要將工作負載備份至 Microsoft Azure，則應該移除 Microsoft Azure 訂購授權的存取權。

若要移除 Microsoft Azure 訂購授權的存取權

重要事項
如果正在使用某個訂購授權備份至 Microsoft Azure，則無法移除該訂購授權。

1. 在 Cyber Protect 主控台中，移至 **[基礎架構] > [公有雲端]**。
2. 從顯示的清單中，選擇相關的訂購授權。
3. 在右窗格中，按一下 **[刪除]**。

注意事項
您只能移除您新增的訂購授權。如果您是公司系統管理員或單位系統管理員，或者在資安防護服務中獲指派網路系統管理員或系統管理員的角色，則也可以移除訂購授權。

4. 在顯示的確認訊息中，按一下 **[移除]**。

管理對其他公有雲端儲存服務的存取權

注意事項
本節涉及管理對 Microsoft Azure 之外的所有公有雲端儲存服務的存取權，如 "管理對 Microsoft Azure 訂購授權的存取" (第 492 頁) 中所述。

您可以透過連線到 Cyber Protect 主控台中的相關公有雲端帳戶，直接將工作負載備份到相關的公有雲端儲存空間。

您可以在透過 **[裝置]** 或 **[備份儲存]** 功能表建立備份位置時，設定與公有雲端儲存帳戶的連線。或者，您可以在 **[公有雲端]** 畫面中設定公有雲端連線 (前往 **[基礎架構] > [公有雲端]**)。您也可以在此處管理連線，包括更新對連線的存取權、檢視連線內容和活動，或移除連線。

根據您獲指派的使用者角色，您可以管理您組織中其他使用者新增的公有雲端連線。例如，如果您是公司系統管理員或單位系統管理員，或者在資安防護服務中獲指派網路系統管理員或系統管理員角色，則可以檢視和管理其他系統管理員所新增的公有雲端連線，以及非系統管理員使用者所新增的連線。非系統管理員使用者僅能檢視和存取他們新增到 Cyber Protect 主控台的公有雲端連線。

注意事項
合作夥伴可以管理階層中低於其層級的客戶的公有雲端連線。不過，當合作夥伴選擇 **[所有客戶]** 時，將無法使用 主控台中的 **[基礎架構]** 功能表。

重要事項
連線到公有雲端連線時，Acronis 需要一些權限。如需詳細資訊，請參閱 "備份到公有雲端儲存空間所需的存取需求" (第 488 頁)。

新增對公有雲端連線的存取權

在 Cyber Protect 主控台中新增公有雲端連線 (例如 Amazon S3、S3 相容或 Wasabi) 後，可以安全地存取您的雲端資源，並將工作負載直接備份到相關的公有雲端儲存空間。

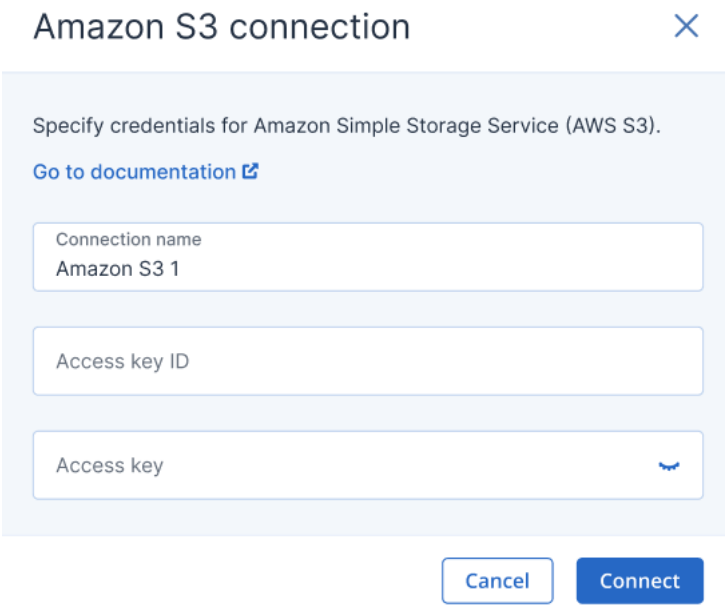
若要新增對公有雲端連線的存取權

1. 在 Cyber Protect 主控台中，移至 **[基礎架構] > [公有雲端]**。
2. 按一下 **[新增]**，然後選擇下列其中一個選項：

   Amazon S3
   在顯示的對話方塊中，定義以下項目：

- **連線名稱**：Amazon S3 連線的名稱。
- **存取金鑰 ID**：Amazon S3 服務的使用者存取金鑰 ID。
- **存取金鑰**：Amazon S3 服務的使用者存取金鑰。

  存取金鑰和存取金鑰 ID 允許存取相關連線的儲存類別和儲存貯體。如需有關存取金鑰和權限的詳細資訊，請參閱 "備份到公有雲端儲存空間所需的存取需求"(第 488 頁)。



注意事項

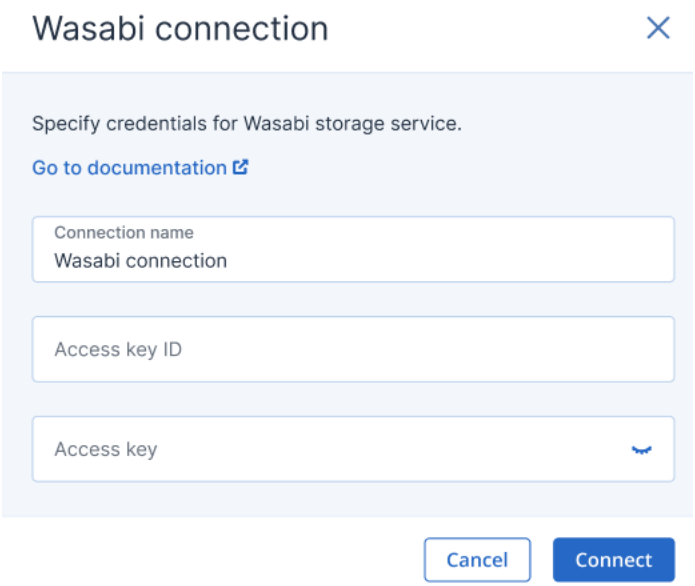
若要成功存取儲存空間，則必須將使用 Amazon S3 儲存空間執行備份和復原作業的代理程式上的系統時間與 NTP 伺服器同步。

Wasabi

在顯示的對話方塊中，定義以下項目：

- **連線名稱**：Wasabi 連線的名稱。
- **存取金鑰 ID**：Wasabi 服務的使用者存取金鑰 ID。
- **存取金鑰**：Wasabi 服務的使用者存取金鑰。

  存取金鑰和存取金鑰 ID 允許存取相關連線的儲存類別和儲存貯體。如需有關存取金鑰和權限的詳細資訊，請參閱 "備份到公有雲端儲存空間所需的存取需求"(第 488 頁)。



注意事項

若要成功存取儲存空間，則必須將使用 Wasabi 儲存空間執行備份和復原作業的代理程式上的系統時間與 NTP 伺服器同步。

S3 相容

注意事項

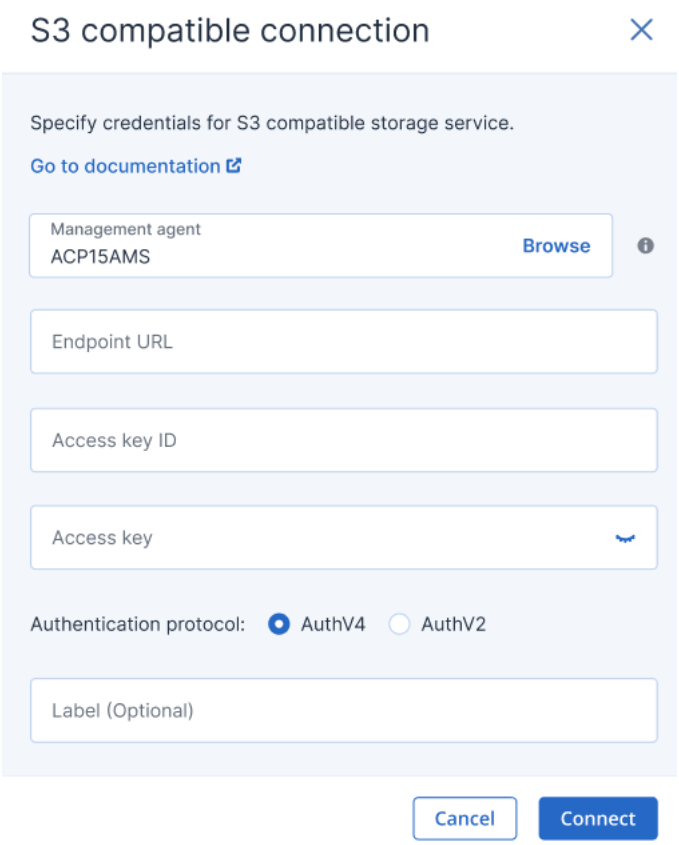
支援私密託管 (指無法透過網際網路存取) 和公開託管的 S3 相容儲存服務。

在顯示的對話方塊中，定義以下項目：

- **管理代理程式**：按一下 **[瀏覽]**，從適當的代理程式清單中選擇管理代理程式。此代理程式將與 S3 相容的儲存空間建立初始通訊。如有需要，您之後可以修改備份位置的參數。

  此管理代理程式可從任何支援的代理程式類型 (包括 Windows/Linux/VMware (虛擬裝置) 用代理程式/Hyper-V/oVirt (但不包括 Azure 用代理程式)) 中選擇，僅在建立或編輯備份位置時使用。代理程式的離線/線上狀態將不會影響其他一般代理程式執行的備份。
- **端點 URL**：請輸入 S3 相容儲存空間廠商共用的端點 URL，以執行儲存空間的相關操作。請注意，此 URL 中指定的端點必須有有效的安全性憑證鏈。不允許使用自我簽署的憑證連線至端點。
- **存取金鑰 ID**：S3 相容儲存空間的使用者存取金鑰 ID。
- **存取金鑰**：S3 相容儲存空間的使用者存取金鑰。

  存取金鑰和存取金鑰 ID 允許存取相關連線的儲存類別和儲存貯體。如需有關存取金鑰和權限的詳細資訊，請參閱 "備份到公有雲端儲存空間所需的存取需求" (第 488 頁)。
- **驗證通訊協定**：選擇儲存端支援的驗證通訊協定版本。預設選擇 **AuthV4**。
- **標籤**：(選擇性) 按需要新增標籤。



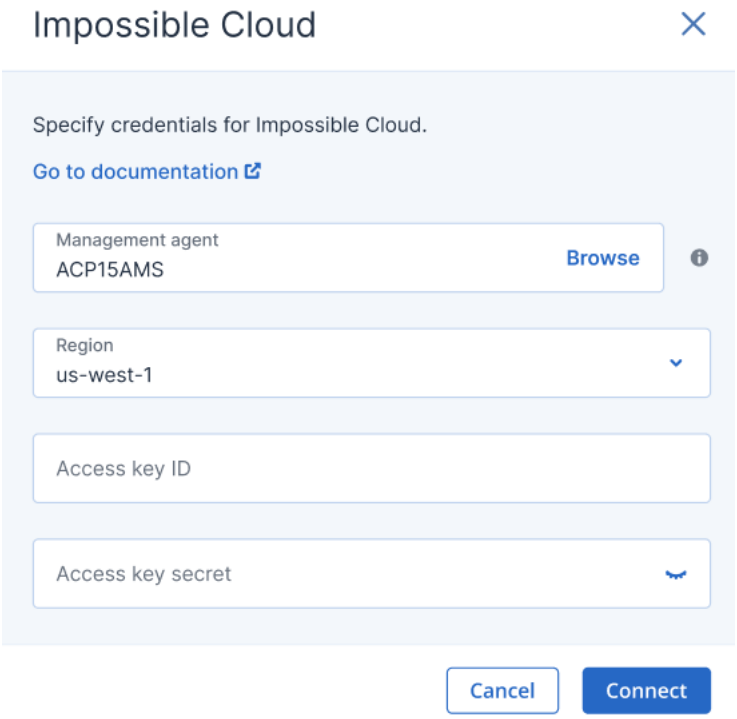
Impossible Cloud

在顯示的對話方塊中，定義以下項目：

- **管理代理程式**：按一下 **[瀏覽]**，從適當的代理程式清單中選擇管理代理程式。此代理程式將與 Impossible Cloud 建立初始通訊。如有需要，您之後可以修改備份位置的參數。

  此管理代理程式可從任何支援的代理程式類型 (包括 Windows/Linux/VMware (虛擬裝置) 用代理程式/Hyper-V/oVirt (但不包括 Azure 用代理程式)) 中選擇，僅在建立或編輯備份位置時使用。代理程式的離線/線上狀態將不會影響其他一般代理程式執行的備份。
- **區域**：選擇相關的區域。
- **存取金鑰 ID**：Impossible Cloud 儲存空間的使用者存取金鑰 ID。
- **存取金鑰**：Impossible Cloud 儲存空間的使用者存取金鑰。

  存取金鑰和存取金鑰 ID 允許存取相關連線的儲存類別和儲存貯體。如需有關存取金鑰和權限的詳細資訊，請參閱 "備份到公有雲端儲存空間所需的存取需求" (第 488 頁)。



注意事項
在代理程式上，使用 Impossible Cloud 儲存空間執行備份與復原作業的系統時間必須與 NTP 伺服器同步，才能成功存取儲存空間。

3. 按一下 **[連線]**。
   連線程序開始，可能需要幾分鐘的時間。完成後，此連線隨即新增到公有雲端清單中。
   若要續訂連線的每年存取憑證，請參閱 "更新對公有雲端連線的存取權"(第 499 頁)。
   若要移除連線的存取權，請參閱 "移除對公有雲端連線的存取權"(第 500 頁)。

更新對公有雲端連線的存取權

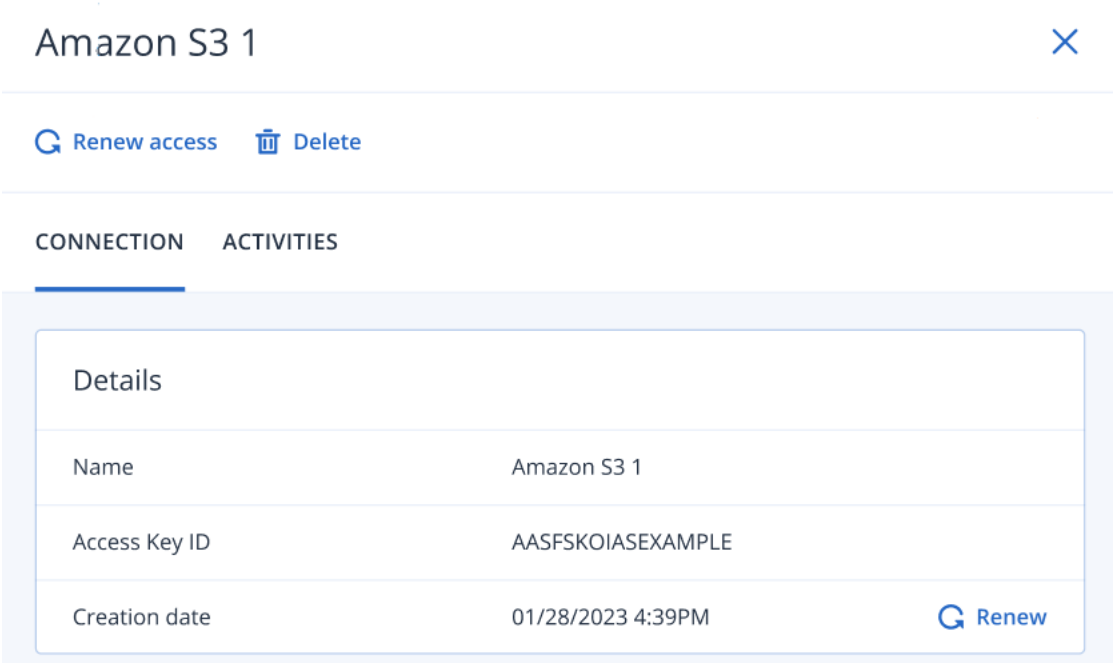
在 Cyber Protect 主控台中註冊公有雲端連線後，Acronis 會自動指派一個免費且唯一的存取憑證，以允許存取公有雲端連線。此憑證有效期限為一年。當憑證接近到期日時，您可以更新。

若要更新公有雲端連線的存取憑證

1. 在 Cyber Protect 主控台中，移至 **[基礎架構] > [公有雲端]**。
2. 從清單中選擇相關的連線。

注意事項
[存取狀態] 欄會指出每個連線目前的存取憑證狀態，並顯示以下其中一個狀態：**[正常]** 或 **[已到期]**。

3. 在右窗格中，按一下 **[續訂存取權]**。
   或者，按一下 **[連線]** 索引標籤，然後在 **[建立日期]** 列中，按一下 **[更新]**。



驗證成功後，存取權將自動續訂一年。

移除對公有雲端連線的存取權

如果您不會將工作負載備份到公有雲端，則應該移除對公有雲端連線的存取權。

若要移除對公有雲端連線的存取權

重要事項
如果連線目前用於備份到公有雲端，則無法移除。

1. 在 Cyber Protect 主控台中，移至 **[基礎架構] > [公有雲端]**。
2. 從清單中選擇連線。
3. 在右窗格中，按一下 **[刪除]**。

注意事項
您只能移除您新增的連線。如果您是公司系統管理員或單位系統管理員，或者在資安防護服務中獲指派網路系統管理員或系統管理員的角色，則也可以移除連線。

4. 在顯示的確認訊息中，按一下 **[刪除]**。

電子郵件存檔

透過電子郵件存檔，Microsoft 365 組織中的所有電子郵件都會保留在雲端儲存的外部存檔中，讓您能夠達到合規性並回應 eDiscovery 要求。新的電子郵件會持續新增至存檔中，因為它們已傳送或接收，且無法修改或手動刪除。

每個使用者信箱中會顯示兩個資料夾的電子郵件 – **[內送]**和 **[外寄]**。在每個資料夾中，電子郵件會依時間順序排序，從最新到最舊。

存檔已使用 AES-256 演算法加密。只有授權的使用者可以根據其存取層級存取存檔，並提供所有動作的稽核追蹤。

除了與法規遵循相關的功能之外，電子郵件存檔還提供備份和復原功能。

您可以執行下列動作：

- 瀏覽存檔
- 使用臨機操作搜尋查詢和已儲存的搜尋查詢來搜尋特定訊息
- 預覽電子郵件，而不復原電子郵件
- 將特定電子郵件、**[內送]** 和 **[外寄]** 資料夾，以及整個信箱復原至原始或非原始信箱
- 下載電子郵件附件

限制

- 存檔中僅包含已授權的信箱。未獲指派授權的共用信箱不包含在存檔中。
- 基於 Microsoft 限制，存檔中可包含的電子郵件大小上限為 150 MB。
- 存檔中不包含草稿電子郵件。
- 您可以將一個存檔計劃套用至一個郵件伺服器。

設定電子郵件存檔

新增郵件伺服器

必要條件

在管理入口網站中，必須為租用戶啟用下列產品項目。

- **電子郵件存檔授權**
- **存檔儲存位置**

若要新增郵件伺服器

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 移至 **[裝置]**，然後按一下 **[新增]** > **[Microsoft 365 商務版 (電子郵件存檔)]**。
   系統會將您重新導向至 Microsoft 365 登入頁面。
3. 在 Microsoft 登入頁面上，以全域系統管理員身分登入。
4. 檢閱所需權限的清單，然後按一下 **[接受]**。

結果，Microsoft 365 電子郵件伺服器隨即出現在 Cyber Protect 主控台的 **[裝置]** > **[電子郵件伺服器]** 索引標籤上。

接著，設定存檔計劃，如 "建立存檔計劃" (第 501 頁) 中所述。

建立存檔計劃

在存檔計劃中，您可以選擇要匯入電子郵件存檔的現有電子郵件。初始匯入僅會影響郵件伺服器上已存在的電子郵件。

將在郵件伺服器新增至 Cyber Protect 主控台後傳送或接收的所有新電子郵件會自動新增至存檔。這不是可設定的設定，且與初始匯入的範圍無關。

您可以將一個存檔計劃套用至一個郵件伺服器。

新郵件伺服器

若要建立存檔計劃

1. 將電子郵件伺服器新增至 Cyber Protect 主控台，如 "新增郵件伺服器" (第 501 頁) 中所述。
   新增伺服器後，**[建立計劃]** 視窗隨即開啟。
2. [選用] 若要變更存檔計劃名稱，請按一下鉛筆圖示，指定新名稱，然後按一下 **[確定]**。
3. 若要設定匯入範圍，按一下 **[要匯入的項目]**。
   您可以調整下列選項。

匯入範圍	日期範圍
所有信箱	全部可用 依電子郵件存留期 依日期
不匯入任何項目	不適用

4. [若已選擇 **[日期範圍]** > **[依電子郵件存留期]**] 指定期間，選擇時間單位，然後按一下 **[完成]**。
   例如，您可以選擇 1 年、2 個月或 300 天。
   只有在指定期間內收到或傳送的電子郵件才會匯入至存檔。
5. [若已選擇 **[日期範圍]** > **[依日期]**] 選擇開始日期和結束日期，然後按一下 **[完成]**。
   只有在指定期間內收到或傳送的電子郵件才會匯入至存檔。
6. 按一下 **[加密]**，指定並確認加密密碼，然後按一下 **[儲存]**。

   警告！
   若您遺失或忘記此密碼，則無法瀏覽存檔並從中復原資料。

7. 按一下 **[建立]**。

現有的郵件伺服器

先決條件

- 已將郵件伺服器新增至 Cyber Protect 主控台，但尚未對其套用任何存檔計劃。

若要建立存檔計劃

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 移至 **[裝置]**，然後選擇您要為其建立計劃的郵件伺服器。
3. 按一下省略符號圖示 (...)，然後選擇 **[保護]**。
4. [選用] 若要變更存檔計劃名稱，請按一下鉛筆圖示，指定新名稱，然後按一下 **[確定]**。
5. 若要設定匯入範圍，按一下 **[要匯入的項目]**。
   您可以調整下列選項。

匯入範圍	日期範圍
所有信箱	全部可用 依電子郵件存留期 依日期
不匯入任何項目	不適用

6. [若已選擇 **[日期範圍]** > **[依電子郵件存留期]**] 指定期間，選擇時間單位，然後按一下 **[完成]**。
   例如，您可以選擇 1 年、2 個月或 300 天。
   只有在指定期間內收到或傳送的電子郵件才會匯入至存檔。
7. [若已選擇 **[日期範圍]** > **[依日期]**] 選擇開始日期和結束日期，然後按一下 **[完成]**。
   只有在指定期間內收到或傳送的電子郵件才會匯入至存檔。
8. 按一下 **[加密]**，指定並確認加密密碼，然後按一下 **[儲存]**。

   警告！
   若您遺失或忘記此密碼，則無法瀏覽存檔並從中復原資料。

9. 按一下 **[建立]**。

結果，電子郵件存檔計劃隨即建立並套用至郵件伺服器，並建立電子郵件存檔。

初始匯入將會花費一些時間，端視所選匯入範圍和期間而定。傳送或接收電子郵件時，所有新的電子郵件將會持續新增至存檔中。

存檔計劃的其他操作

您可以編輯、套用和刪除存檔計劃。

編輯

若要編輯存檔計劃

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 移至 **[管理]** > **[存檔計劃]**，然後按一下 **[存檔計劃]**。
3. 按一下計劃名稱旁的省略符號圖示 (...)，然後按一下 **[編輯]**。
4. 若要變更計劃名稱，請按一下鉛筆圖示，指定新名稱，然後按一下 **[確定]**。
5. 若要變更匯入範圍，按一下 **[要匯入的項目]**。
6. 編輯範圍或日期範圍，然後按一下 **[完成]**。
7. 按一下 **[儲存]**。

結果，若已擴大匯入範圍，會將其他電子郵件訊息匯入存檔。

若已縮小匯入範圍，則不會採取任何動作，且不會刪除已匯入電子郵件存檔的電子郵件。

套用

先決條件

- 您的租用戶中必須至少存在一個存檔計劃。

若要套用存檔計劃

注意事項
只有在尚未將存檔計劃套用至郵件伺服器時，才可以使用此操作。您只能將一個存檔計劃套用至郵件伺服器。

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 移至 **[裝置]** > **[郵件伺服器]**。
3. 按一下電子郵件伺服器名稱旁的省略符號圖示 (...)，然後選擇 **[保護]**。
4. 選擇現有的存檔計劃，然後按一下 **[套用]**。

結果，電子郵件存檔計劃隨即套用至郵件伺服器，並建立電子郵件存檔。

初始匯入將會花費一些時間，端視所選匯入範圍和期間而定。傳送或接收電子郵件時，所有新的電子郵件將會持續新增至存檔中。

刪除

若要刪除存檔計劃

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 移至 **[管理]** > **[存檔計劃]**，然後按一下 **[存檔計劃]**。
3. 按一下計劃名稱旁的省略符號圖示 (...)，然後按一下 **[刪除]**。
4. 選擇核取方塊以確認您的決定，然後按一下 **[刪除]**。

結果，將不再更新套用此計劃的郵件伺服器存檔。已匯入存檔的電子郵件將不會遭到刪除。

建立已儲存的搜尋查詢

您可以使用搜尋查詢，在存檔中尋找特定的電子郵件，然後儲存查詢以供之後使用。

若要建立已儲存的搜尋查詢

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 移至 **[備份儲存]** > **[雲端應用程式備份]**，然後選擇您要搜尋的電子郵件存檔。
3. 按一下 **[瀏覽存檔]**。
4. [如果顯示隱私權警告] 在 **[隱私權警告]** 對話方塊中，按一下 **[繼續]**。
5. 在 **[加密密碼]** 對話方塊中，指定密碼，然後按一下 **[繼續]**。
6. 選擇您要執行搜尋所在的層級。
   您可以選擇 **[所有電子郵件]**、使用者信箱或使用者信箱中的 **[內送]** 或 **[外寄]** 資料夾。
7. 按一下 **[搜尋]**，指定搜尋查詢，然後按一下 **[搜尋]**。
   您可以使用一個或多個單字。若要搜尋特定字詞，請用引號括住字詞。不支援萬用字元。
   搜尋將在下列欄位中執行：
   - 寄件者
   - 收件者
   - 副本

- 密件副本
- 主旨

8. [選用] 若要僅在特定欄位 (例如 **[寄件者]**、**[收件者/副本/密件副本]**、**[主旨包含]**) 中搜尋，或指定其他搜尋條件，請按一下 **[篩選]**。
   a. 設定您的搜尋條件。
      例如，您可以僅搜尋包含附件的電子郵件，或在特定日期傳送或接收的電子郵件。
   b. 按一下**[套用]**。
9. 按一下 **[另存新檔]**。
10. 在 **[搜尋查詢標籤]** 中，指定名稱。
11. 按一下 **[儲存]**。

結果，符合搜尋查詢的電子郵件隨即列出。系統會建立新的已儲存搜尋查詢，並顯示在電子郵件存檔樹狀目錄上方的 **[已儲存的搜尋查詢]** 區段。

每次將已儲存的搜尋查詢重新套用至存檔時，就會更新搜尋結果。

已儲存的搜尋查詢的其他操作

您可以編輯和刪除已儲存的搜尋查詢。

編輯

若要編輯搜尋查詢

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 移至 **[管理]** > **[存檔計劃]**，然後按一下 **[搜尋查詢]**。
3. 按一下查詢名稱旁的省略符號圖示 (...)，然後按一下 **[編輯]**。
4. 編輯搜尋查詢，然後按一下 **[儲存]**。

刪除

若要刪除搜尋查詢

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 移至 **[管理]** > **[存檔計劃]**，然後按一下 **[搜尋查詢]**。
3. 按一下查詢名稱旁的省略符號圖示 (...)，然後按一下 **[刪除]**。
4. 選擇核取方塊以確認您的決定，然後按一下 **[刪除]**。

移除郵件伺服器

您可以移除已新增至 Cyber Protect 主控台的郵件伺服器。

若要移除郵件伺服器

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 移至 **[裝置]** > **[郵件伺服器]**。
3. 按一下電子郵件伺服器名稱旁的省略符號圖示 (...)，然後按一下 **[刪除]**。
4. 若要確認您的選擇，請按一下 **[刪除]**。

結果，郵件伺服器隨即從 Cyber Protect 主控台中移除。系統將保留電子郵件存檔，但不再進行更新。

從電子郵件存檔復原資料

搜尋電子郵件

您可以在存檔中搜尋特定的電子郵件，方法是，使用下列層級的搜尋查詢：

- 電子郵件存檔 (**所有電子郵件**)
- 使用者信箱
- 使用者信箱中的 **[內送]** 或 **[外寄]** 資料夾

若要搜尋電子郵件

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 移至 **[備份儲存]** > **[雲端應用程式備份]**，然後選擇您要搜尋的電子郵件存檔。
3. 按一下 **[瀏覽存檔]**。
4. [如果顯示隱私權警告] 在 **[隱私權警告]** 對話方塊中，按一下 **[繼續]**。
5. 在 **[加密密碼]** 對話方塊中，指定密碼，然後按一下 **[繼續]**。
6. 選擇您要執行搜尋所在的層級。
   您可以選擇 **[所有電子郵件]**、使用者信箱或使用者信箱中的 **[內送]** 或 **[外寄]** 資料夾。
7. 按一下 **[搜尋]**，指定搜尋查詢，然後按一下 **[搜尋]**。
   您可以使用一個或多個單字。若要搜尋特定字詞，請用引號括住字詞。不支援萬用字元。
   搜尋將在下列欄位中執行：
   - 寄件者
   - 收件者
   - 副本
   - 密件副本
   - 主旨
8. [選用] 若要僅在特定欄位 (例如 **[寄件者]**、**[收件者/副本/密件副本]**、**[主旨包含]**) 中搜尋，或指定其他搜尋條件，請按一下 **[篩選]**。
   a. 設定您的搜尋條件。
      例如，您可以僅搜尋包含附件的電子郵件，或在特定日期傳送或接收的電子郵件。
   b. 按一下**[套用]**。

結果，符合搜尋查詢的電子郵件隨即列出。

預覽電子郵件

您可以在不先復原存檔電子郵件的情況下預覽。

若要預覽電子郵件

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 移至 **[備份儲存]** > **[雲端應用程式備份]**，然後選擇您要搜尋的電子郵件存檔。
3. 按一下 **[瀏覽存檔]**。
4. [如果顯示隱私權警告] 在 **[隱私權警告]** 對話方塊中，按一下 **[繼續]**。
5. 在 **[加密密碼]** 對話方塊中，指定密碼，然後按一下 **[繼續]**。
6. 搜尋您要預覽的電子郵件。
   您可以使用臨機操作搜尋查詢和已儲存的搜尋查詢。如需詳細資訊，請參閱 "搜尋電子郵件" (第 506 頁)。
7. 選擇您要預覽的電子郵件。

結果，電子郵件隨即顯示，而且您可以檢查其內容和中繼資料。

復原電子郵件、資料夾和信箱

您可以將電子郵件、資料夾和信箱復原至原始或非原始信箱。

電子郵件

若要復原電子郵件

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 移至 **[備份儲存]** > **[雲端應用程式備份]**，然後選擇要從中復原資料的電子郵件存檔。
3. 按一下 **[瀏覽存檔]**。
4. [如果顯示隱私權警告] 在 **[隱私權警告]** 對話方塊中，按一下 **[繼續]**。
5. 在 **[加密密碼]** 對話方塊中，指定密碼，然後按一下 **[繼續]**。
6. [選用] 搜尋您要復原的電子郵件。
   您可以使用臨機操作搜尋查詢和已儲存的搜尋查詢。如需詳細資訊，請參閱 "搜尋電子郵件" (第 506 頁)。
7. 選擇您要復原的電子郵件，然後按一下 **[復原電子郵件]**。
8. [若已將多個郵件伺服器新增至 Cyber Protect 主控台] 選擇要復原資料的組織。
   a. 在 **[組織]** 中，按一下 **[選擇]**。
   b. 選擇組織，然後按一下 **[選擇]**。
9. 在 **[復原位置]** 中，選擇您要復原電子郵件的位置。
10. [若選擇 **[新位置]**] 選擇目標信箱。
    a. 在 **[復原至]** 中，按一下 **[選擇]**。
    b. 選擇目標信箱，然後按一下 **[選擇]**。
11. 按一下 **[開始復原]**。

結果，來自所選信箱的內送電子郵件將復原到目標信箱的 **[收件匣]** 資料夾，而來自所選信箱的外寄電子郵件將復原到目標信箱的 **[寄件備份]** 資料夾。

資訊夾

若要復原資料夾

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 移至 **[備份儲存]** > **[雲端應用程式備份]**，然後選擇要從中復原資料的電子郵件存檔。
3. 按一下 **[瀏覽存檔]**。
4. [如果顯示隱私權警告] 在 **[隱私權警告]** 對話方塊中，按一下 **[繼續]**。
5. 在 **[加密密碼]** 對話方塊中，指定密碼，然後按一下 **[繼續]**。
6. 選擇要復原的 **[內送]** 或 **[外寄]** 資料夾，然後按一下 **[復原資料夾]**。
7. [若已將多個郵件伺服器新增至 Cyber Protect 主控台] 選擇要復原資料的組織。
   a. 在 **[組織]** 中，按一下 **[選擇]**。
   b. 選擇組織，然後按一下 **[選擇]**。
8. 在 **[復原位置]** 中，選擇您要復原資料的位置。
9. [若選擇 **[新位置]**] 選擇目標信箱。
   a. 在 **[復原至]** 中，按一下 **[選擇]**。
   b. 選擇目標信箱，然後按一下 **[選擇]**。
10. 按一下 **[開始復原]**。

結果，來自所選信箱的內送電子郵件將復原到目標信箱的 **[收件匣]** 資料夾，而來自所選信箱的外寄電子郵件將復原到目標信箱的 **[寄件備份]** 資料夾。

信箱

復原信箱

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 移至 **[備份儲存]** > **[雲端應用程式備份]**，然後選擇要從中復原資料的電子郵件存檔。
3. 按一下 **[瀏覽存檔]**。
4. [如果顯示隱私權警告] 在 **[隱私權警告]** 對話方塊中，按一下 **[繼續]**。
5. 在 **[加密密碼]** 對話方塊中，指定密碼，然後按一下 **[繼續]**。
6. 選擇您要復原的信箱，然後按一下 **[復原使用者電子郵件]**。
7. [若已將多個郵件伺服器新增至 Cyber Protect 主控台] 選擇要復原資料的組織。
   a. 在 **[組織]** 中，按一下 **[選擇]**。
   b. 選擇組織，然後按一下 **[選擇]**。
8. 在 **[復原位置]** 中，選擇您要復原資料的位置。
9. [若選擇 **[新位置]**] 選擇目標信箱。
   a. 在 **[復原至]** 中，按一下 **[選擇]**。
   b. 選擇目標信箱，然後按一下 **[選擇]**。
10. 按一下 **[開始復原]**。

結果，來自所選信箱的內送電子郵件將復原到目標信箱的 **[收件匣]** 資料夾，而來自所選信箱的外寄電子郵件將復原到目標信箱的 **[寄件備份]** 資料夾。

下載附件

您可以下載存檔中一或多封電子郵件的附件。

若要下載附件

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 移至 **[備份儲存]** > **[雲端應用程式備份]**，然後選擇電子郵件存檔。
3. 按一下 **[瀏覽存檔]**。
4. [如果顯示隱私權警告] 在 **[隱私權警告]** 對話方塊中，按一下 **[繼續]**。
5. 在 **[加密密碼]** 對話方塊中，指定密碼，然後按一下 **[繼續]**。
6. [選用] 搜尋包含您要下載之附件的電子郵件。
   您可以使用臨機操作搜尋查詢和已儲存的搜尋查詢。如需詳細資訊，請參閱 "搜尋電子郵件" (第 506 頁)。
7. 選擇包含您要下載之附件的電子郵件，然後按一下 **[下載附件]**。

結果，所選電子郵件的附件隨即下載到您的電腦中。

下載多個項目時，附件會以 ZIP 檔案下載。

保護 Microsoft 應用程式

保護 Microsoft SQL Server 和 Microsoft Exchange Server

注意事項
僅在 NFTS、REFS 和 FAT32 檔案系統上執行的資料庫才支援 Microsoft SQL 備份。不支援 ExFat。

有兩種方法可以保護 Microsoft 應用程式：

- **資料庫備份**
  這是資料庫及與其相關聯之中繼資料的檔案層級備份。資料庫可以復原至即時應用程式或復原為檔案。
- **應用程式感知備份**
  這是也會收集應用程式之中繼資料的磁碟層級備份。此中繼資料可讓您瀏覽和復原應用程式資料，而不需復原整個磁碟或磁碟區。您也可以復原整個磁碟或磁碟區。也就是說，單一解決方案和單一保護計劃可同時用於災難復原和資料保護用途。

對於 Microsoft Exchange Server，您可以選擇**信箱備份**。這是透過 Exchange Web 服務通訊協定執行的單獨信箱備份。信箱或信箱項目可以復原至即時 Exchange Server 或 Microsoft 365。Microsoft Exchange Server 2010 Service Pack 1 (SP1) 更新版本支援信箱備份。

保護 Microsoft SharePoint

Microsoft SharePoint 伺服器陣列包含執行 SharePoint 服務的前端伺服器、執行 Microsoft SQL Server 的資料庫伺服器，以及 (可選) 從前端伺服器卸下部分 SharePoint 服務的負擔之應用程式伺服器。部分前端和應用程式伺服器兩者可能是相同的。

若要保護整個 SharePoint 伺服器陣列：

- 使用應用程式感知備份來備份所有資料庫伺服器。
- 使用一般磁碟層級備份來備份所有唯一的前端伺服器和應用程式伺服器。

所有伺服器的備份應以相同的排程完成。

若只要保護內容，您可另行單獨備份內容資料庫。

保護網域控制站

您可以使用應用程式感知備份來保護執行 Active Directory 網域服務的電腦。如果網域包含一個以上的網域控制站，而您復原了其中之一，則會執行非權威還原，且在復原後 USN 回復將不會發生。

復原應用程式

下表摘述可用的應用程式復原方法。

	從資料庫備份	從應用程式感知備份	從磁碟備份
Microsoft SQL Server	資料庫至即時 SQL Server 執行個體 資料庫做為檔案	整部電腦 資料庫至即時 SQL Server 執行個體 資料庫做為檔案	整部電腦
Microsoft Exchange Server	資料庫至即時 Exchange 資料庫做為檔案 細微復原至即時 Exchange 或 Microsoft 365*	整部電腦 資料庫至即時 Exchange 資料庫做為檔案 細微復原至即時 Exchange 或 Microsoft 365*	整部電腦
Microsoft SharePoint 資料庫伺服器	資料庫至即時 SQL Server 執行個體 資料庫做為檔案 使用 SharePoint Explorer 的細微復原	整部電腦 資料庫至即時 SQL Server 執行個體 資料庫做為檔案 使用 SharePoint Explorer 的細微復原	整部電腦
Microsoft SharePoint 前端 Web 伺服器	-	-	整部電腦
Active Directory 網域服務	-	整部電腦	-

* 從信箱備份復原也提供細微復原。如果在本機安裝 Microsoft 365 用代理程式，則支援將 Exchange 資料項目復原至 Microsoft 365，反之亦然。

必要條件

在設定應用程式備份之前，請先確保符合以下列出的需求。

若要檢查 VSS 編寫器狀態，請使用 `vssadmin list writers` 命令。

一般需求

若是 Microsoft SQL Server，請確保：

- 至少已啟動一個 Microsoft SQL Server 執行個體。
- 已開啟 VSS 的 SQL 編寫器。

若是 Microsoft Exchange Server，請確保：

- 已啟動 Microsoft Exchange 資訊儲存庫服務。
- 已安裝 Windows PowerShell。若是 Exchange 2010 或更新版本，Windows PowerShell 版本至少必須是 2.0。
- 已安裝 Microsoft .NET Framework。

  若是 Exchange 2007，Microsoft .NET Framework 版本至少必須是 2.0。

  若是 Exchange 2010 或更新版本，Microsoft .NET Framework 版本至少必須是 3.5。
- VSS 的 Exchange 編寫器已開啟。

注意事項

Exchange 用代理程式需要臨時存放區才能運作。暫存檔預設位於 `%ProgramData%\Acronis\Temp`。請確定 `%ProgramData%` 資料夾所在磁碟區的可用空間應至少等於 Exchange 資料庫大小的 15%。或者，您可以先變更暫存檔的位置，再建立 Exchange 備份，如變更暫存檔和資料夾位置 (40040) 中所述。

在網域控制站上，請確保：

- 已開啟 VSS 的 Active Directory 編寫器。

建立保護計劃時，請確保：

- 若是實體電腦以及其中已安裝代理程式的電腦，啟用 [磁碟區陰影複製服務 (VSS)] 備份選項。
- 若是虛擬機器，請確保已啟用 [虛擬機器的磁碟區陰影複製服務 (VSS)] 備份選項。

應用程式感知備份的額外需求

建立保護計劃時，請確保已選擇 **[整部電腦]** 進行備份。保護計劃中必須停用 **[逐一磁區]** 備份選項，否則將無法從這類備份中復原應用程式資料。如果計劃是因為自動切換到 **[逐一磁區]** 模式而在此模式下執行的，也將無法復原應用程式資料。

ESXi 虛擬機器的需求

如果應用程式是在透過 VMware 用代理程式備份的虛擬機器上執行，請確保：

- 要備份的虛擬機器符合以下 VMware 文件的「Windows 備份實作」一文中列出之應用程式一致的備份和還原需求：https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html。
- 已在電腦上安裝 VMware Tools 且為最新版。

- 已在電腦上停用使用者帳戶控制 (UAC)。如果您不想要停用 UAC，您必須在啟用應用程式備份時提供內建網域系統管理員 (DOMAIN\Administrator) 的認證。
  如果您不想要停用 UAC，您必須在啟用應用程式備份時提供內建網域系統管理員 (DOMAIN\Administrator) 的認證。

  注意事項
  使用建立網域時設定的內建網域系統管理員帳戶。不支援之後建立的帳戶。

Hyper-V 虛擬機器的需求

如果應用程式是在透過 Hyper-V 用代理程式備份的虛擬機器上執行，請確保：

- 客體作業系統為 Windows Server 2008 或更新版本。
- 若是 Hyper-V 2008 R2：客體作業系統為 Windows Server 2008/2008 R2/2012。
- 虛擬機器沒有動態磁碟。
- 在 Hyper-V 主機和客體作業系統之間存在網路連線。若要在虛擬機器內部執行遠端 WMI 查詢，則這是必要的。
- 已在電腦上停用使用者帳戶控制 (UAC)。如果您不想要停用 UAC，您必須在啟用應用程式備份時提供內建網域系統管理員 (DOMAIN\Administrator) 的認證。
  如果您不想要停用 UAC，您必須在啟用應用程式備份時提供內建網域系統管理員 (DOMAIN\Administrator) 的認證。

  注意事項
  使用建立網域時設定的內建網域系統管理員帳戶。不支援之後建立的帳戶。

- 虛擬機器設定符合下列準則：
  - 已安裝 Hyper-V 整合服務且為最新版。重大更新為 https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines
  - 在虛擬機器設定中，**[管理]** > **[整合服務]** > **[備份 (磁碟區檢查點)]** 選項為啟用狀態。
  - 若是 Hyper-V 2012 和更新版本：虛擬機器沒有檢查點。
  - 若是 Hyper-V 2012 R2 和更新版本：虛擬機器有一個 SCSI 控制器 (核取 **[設定]** > **[硬體]**)。

資料庫備份

在備份資料庫前，請確保已符合「必要條件」中列出的需求。

如下所述選擇資料庫，然後視需要指定保護計劃的其他設定。

選擇 SQL 資料庫

SQL 資料庫備份包含資料庫檔案 (.mdf、.ndf)、記錄檔 (.ldf)，以及其他相關檔案。系統會透過 SQL 寫入器服務協助檔案備份。磁碟區陰影複製服務 (VSS) 要求備份或復原時，此服務必須處於執行狀態。

SQL 交易記錄檔在每次成功備份後都會遭到截斷。您可以在保護計劃選項中停用 SQL 記錄截斷。

選擇 SQL 資料庫

1. 按一下**裝置** > **Microsoft SQL**。

   軟體顯示 SQL Server Always On 可用性群組 (AAG)、執行 Microsoft SQL Server 的電腦、SQL Server 執行個體和資料庫的樹形結構。
2. 瀏覽至您要備份的資料。

   在該樹狀目錄右邊的清單中，展開樹狀節點或按兩下其中的項目。
3. 選擇您要備份的資料。您可選擇 AAG、執行 SQL Server 的電腦、SQL Server 執行個體或個別資料庫。
   - 如果選擇 AAG，將備份包含在所選 AAG 中的所有資料庫。如需有關備份 AAG 或個別 AAG 資料庫的詳細資訊，請參閱「保護 Always On 可用性群組 (AAG)」。
   - 如果選擇執行 SQL Server 的電腦，將備份連接到所有 SQL Server 執行個體 (在所選機器上執行) 的所有資料庫。
   - 如果選擇 SQL Server 執行個體，將備份連接到所選執行個體的所有資料庫。
   - 如果您直接選擇資料庫，則系統將只會備份所選的資料庫。
4. 按一下 **[保護]**。若畫面顯示提示，請提供認證以存取 SQL Server 資料。

   如果您使用的是 Windows 驗證，帳戶必須是電腦上的 **[Backup Operators]** 或 **[Administrators]** 群組成員，而且必須是您將備份之各執行個體上的 **[系統管理員 (sysadmin)]** 角色成員。

   如果您使用的是 SQL Server 驗證，帳戶必須是您將備份之各執行個體上的 **[系統管理員 (sysadmin)]** 角色成員。

選擇 Exchange Server 資料

下表摘述可讓您選擇備份的 Microsoft Exchange Server 資料，以及備份該資料所需具備的最低使用者權限。

Exchange 版本	資料項目	使用者權限
2007	儲存群組	**Exchange Organization Administrators** 角色群組的成員資格
2010/2013/2016/2019	資料庫，資料庫可用性群組 (DAG)	**伺服器管理**角色群組的成員資格。

完整備份包含所有選取的 Exchange Server 資料。

增量備份包含已變更的資料庫檔案區塊、檢查點檔案，以及時間比對應資料庫檢查點更近的少量記錄檔。由於備份會涵蓋資料庫檔案的變更記錄，因此無須備份自上次備份以來的所有交易記錄。只有時間比檢查點更近的記錄才需要在復原後重新執行。這可以讓復原速度更快，並且確保能成功完成資料庫備份，即使已啟用循環記錄也不會有影響。

交易記錄檔在每次成功備份後都會遭到截斷。

選擇 Exchange Server 資料

1. 按一下**[裝置]** > **Microsoft Exchange**。

   軟體會顯示 Exchange Server 資料庫可用性群組 (DAG)、執行 Microsoft Exchange Server 的電腦和 Exchange Server 資料庫的樹狀目錄。如果您依照 "信箱備份" (第 519 頁) 中所述設定 Exchange 用代理程式，則此樹狀目錄中也會顯示信箱。
2. 瀏覽至您要備份的資料。

   在該樹狀目錄右邊的清單中，展開樹狀節點或按兩下其中的項目。
3. 選擇您要備份的資料。
   - 如果選擇 DAG，將會備份每個叢集資料庫的一個副本。如需有關備份 DAG 的詳細資訊，請參閱 "保護資料庫可用性群組 (DAG)" (第 515 頁)。
   - 如果選擇執行 Microsoft Exchange Server 的電腦，將備份安裝至 Exchange Server(執行於所選機器上) 的所有資料庫。
   - 如果您直接選擇資料庫，則系統將只會備份所選的資料庫。
   - 如果您依照 "信箱備份" (第 519 頁) 中所述設定 Exchange 用代理程式，則可以選擇要備份的信箱。

   如果您選擇納入多個資料庫，會一次處理兩個。當第一個群組備份完成時，將會開始下一組備份。
4. 若畫面顯示提示，請提供認證以存取資料。
5. 按一下 **[保護]**。

保護 Always On 可用性群組 (AAG)

注意事項
此功能適用於 Advanced Backup 套件。

SQL Server高可用性解決方案概觀

Windows Server 容錯移轉叢集 (WSFC) 功能可讓您透過執行個體層級 (容錯移轉叢集執行個體，FCI) 或資料庫層級 (AlwaysOn 可用性群組，AAG) 備援，設定高可用性 SQL Server。您也可以結合兩種方式。

在容錯移轉叢集執行個體中，SQL 資料庫會位於共用存放區。只能從活動叢集節點存取此儲存。如果使用中節點失敗，會發生容錯移轉，另一個節點將會成為使用中節點。

在可用性群組中，每個資料庫複本會位於不同的節點。如果主要複本無法使用，會將主要角色指派給位於不同節點的次要複本。

因此，叢集本身已經具有災難復原解決方案的功能。不過，可能也有叢集解決方案無法提供資料保護的時候：例如，資料庫邏輯損毀，或整個叢集停擺等狀況。此外，叢集解決方案也無法防止有害的內容變更，因為內容變更通常會立即複寫至所有叢集節點。

支援的叢集組態

此備份軟體*僅*支援 SQL Server 2012 或更新版本的 Always On 可用性群組 (AAG)。*不*支援其他叢集設定(如容錯移轉叢集執行個體、資料庫鏡像和記錄傳送) 。

叢集資料備份和復原需要多少代理程式?

若要成功備份和復原叢集的資料，就必須在 WSFC 叢集的每個節點上安裝 SQL 用代理程式。

備份 AAG 中包含的資料庫

1. 在每個 WSFC 叢集的節點上安裝 SQL 用代理程式。
2. 如「選擇 SQL 資料庫」所述，選擇要備份的 AAG。

   您必須選擇 AAG 本身，才能備份 AAG 的所有資料庫。若要備份一組資料庫，請在 AAG 的所有節點中定義這組資料庫。

   警告！
   在所有節點中的資料庫組必須完全相同。即使只有一組不同，或未在所有節點上定義，則叢集備份將無法正確運作。

3. 設定「叢集備份模式」備份選項。

復原 AAG 中包含的資料庫

1. 選擇要復原的資料庫，然後選擇要從其復原資料庫的復原點。

   在**[裝置]** > **[Microsoft SQL]** > **[資料庫]**，下選擇叢集資料庫，然後按一下 **[復原]**後，軟體僅顯示與備份資料庫選定副本的時間相對應的復原點。

   檢視叢集資料庫所有復原點的最簡單方法是在 [備份儲存] 索引標籤上選擇整個 AAG 的備份。AAG 備份的名稱是以下列範本為基礎：<AAG 名稱> - <保護計劃名稱>，且有一個特殊圖示。
2. 若要設定復原，請遵循「復原 SQL 資料庫」中描述的步驟，從第 5 步開始。

   軟體會自動定義資料復原目標叢集節點。該節點的名稱會顯示在 **[復原至]** 欄位中。您可以手動變更目標節點。

   重要事項
   包含在 Always On 可用性群組中的資料庫無法在復原期間遭到覆寫，因為 Microsoft SQL Server 禁止此作業。您需要在復原前從 AAG 排除目標資料庫。或者，您可逕將資料庫復原為新的非 AAG 資料庫。完成復原時，您可以在重建原始 AAG 設定。

保護資料庫可用性群組 (DAG)

注意事項
此功能適用於 Advanced Backup 套件。

Exchange 伺服器 [叢集] 概觀

Exchange 叢集的主要優勢，是藉由快速容錯移轉與零資料遺失等特點，來提高資料庫的可用性。通常，這是透過在叢集成員 (叢集節點) 上建立資料庫或儲存群組的一或多個副本來達成。如果裝載主動資料庫副本的叢集節點故障，或主動資料庫副本本身出現問題，其他裝載被動副本的節點會自動接手故障節點的作業，讓使用者可以存取 Exchange 服務，將停機時間降到最低。因此，叢集本身已經具有災難復原解決方案的功能。

不過，可能也有容錯移轉叢集解決方案無法提供資料保護的時候：例如，資料庫邏輯損毀、叢集中的特定資料庫沒有副本 (複本)，或整個叢集停擺等狀況。此外，叢集解決方案也無法防止有害的內容變更，因為內容變更通常會立即複寫至所有叢集節點。

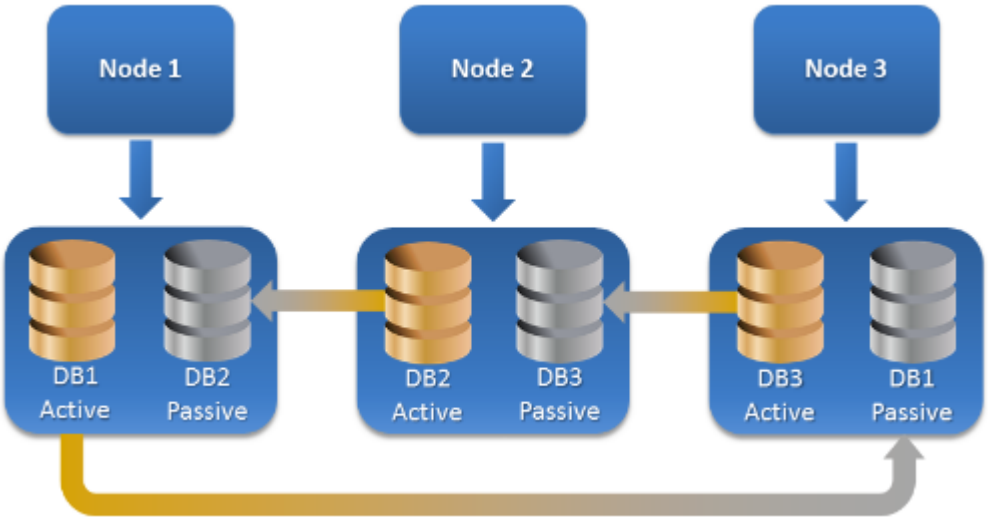
叢集感知備份

藉助叢集感知備份，您只能備份叢集資料的副本。若資料在叢集內的位置改變了 (由於伺服器轉換或容錯移轉)，軟體仍然會追蹤此資料所有變更的位置，並安全地為其備份。

支援的叢集組態

叢集感知備份*僅*在 Exchange Server 2010 或更新版本的資料庫可用性群組 (DAG) 中受支援。*不*支援其他叢集組態，如適用於 Exchange 2007 的單一副本叢集 (SCC) 和叢集連續複寫 (CCR)。

DAG 是由最多 16 部 Exchange 信箱伺服器組成的群組。任何節點都可以裝載來自其他任何節點的信箱資料庫副本。每個節點都可以裝載被動和主動資料庫副本。最多可以為每個資料庫建立 16 個副本。



叢集感知備份和復原需要多少個代理程式?

若要成功備份和復原叢集資料庫，就必須在 Exchange 叢集的每個節點上安裝 Exchange 用代理程式。

注意事項
在其中一個節點上安裝該代理程式後，Cyber Protect 主控台將在 **[裝置]** > **[Microsoft Exchange]** > **[資料庫]** 下顯示 DAG 及其節點。若要在剩餘節點上安裝適用於 Exchange的代理程式，請選擇 DAG，按一下 **[詳細資料]**然後按一下每個節點旁邊的**[安裝代理程式]**。

備份 Exchange 叢集資料

1. 建立保護計劃時，選擇 DAG，如 "選擇 Exchange Server 資料" (第 513 頁) 中所述。
2. 設定 "叢集備份模式" (第 405 頁) 備份選項。
3. 視需要指定保護計劃的其他設定。

重要事項

對於叢集感知備份，務必選擇 DAG 本身。如果您選擇 DAG 內的個別節點或資料庫，則將僅備份所選項目並忽略**叢集備份模式**選項。

復原 Exchange 叢集資料

1. 請選擇您要復原之資料庫的復原點。不能選擇整個叢集進行復原。

   在 **[裝置]** > **[Microsoft Exchange]** > **[資料庫]** > <叢集名稱> > <節點名稱> 下選擇叢集資料庫副本，並按一下 **[復原]** 後，軟體僅顯示與此副本備份時間相對應的復原點。

   檢視叢集資料庫所有復原點的最簡單方法是在 [備份儲存] 索引標籤上選擇其備份。
2. 依照 "復原 Exchange 資料庫" (第 528 頁) 中所述的步驟，從步驟 5 開始。

   軟體會自動定義資料復原目標叢集節點。該節點的名稱會顯示在 **[復原至]** 欄位中。您可以手動變更目標節點。

應用程式感知備份

應用程式感知磁碟層級備份適用於個別實體機器、ESXi 虛擬機器和 Hyper-V 虛擬機器，不適用於裝置群組。

當您備份執行 Microsoft SQL Server、Microsoft Exchange Server 或 Active Directory 網域服務的電腦時，請啟用 **[應用程式備份]**，以獲得這些應用程式資料的額外保護。

為何使用應用程式感知備份？

透過使用應用程式感知備份，您可以確保：

- 應用程式會以一致的狀態進行備份，如此一來，在電腦復原後即可立刻使用。
- 您可以復原 SQL 和 Exchange 資料庫、信箱及信箱項目，而不需復原整部電腦。
- SQL 交易記錄檔在每次成功備份後都會遭到截斷。您可以在保護計劃選項中停用 SQL 記錄截斷。只會在虛擬機器上截斷 Exchange 交易記錄。若要在實體機器上截斷 Exchange 交易記錄，您可以啟用「VSS 完整備份選項」。
- 如果網域包含一個以上的網域控制站，而您復原了其中之一，則會執行非權威還原，且在復原後 USN 回復將不會發生。

使用應用程式感知備份時需要什麼？

在實體機器上，除了 Windows 用代理程式，還必須安裝 SQL 用代理程式和/或 Exchange 用代理程式。

在虛擬機器上，不需安裝代理程式；其假定該電腦已透過 VMware 用代理程式 (Windows) 或 Hyper-V 用代理程式備份。

注意事項

執行 Windows Server 2022 的 Hyper-V 和 VMware ESXi 虛擬機器不支援無代理程式應用程式感知備份。若要保護這些機器上的 Microsoft 應用程式，請在客體作業系統中安裝保護代理程式。如需詳細資訊，請參閱 "在 Windows Server 2022 虛擬機器上設定應用程式感知備份" (第 518 頁)。

VMware 用代理程式 (虛擬裝置) 可以建立應用程式感知備份，但無法從那些備份復原應用程式資料。若要從此代理程式建立的備份復原應用程式資料，在存取備份儲存位置的電腦上，必須有 VMware 用代理程式 (Windows)、SQL 用代理程式或 Exchange 用代理程式。設定應用程式資料的復原時，請在 **[備份儲存]** 索引標籤上選擇復原點，然後在 **[要瀏覽的電腦]** 中選擇此電腦。

< 必要條件 > 和 < 需要的使用者權限 > 章節已列出其他需求。

注意事項

如果在高負載下於主機執行備份，可能會因為 Windows Management Instrumentation 沒有回應或延遲回應，導致 Hyper-V 虛擬機器應用程式感知備份失敗並出現「WMI 'ExecQuery' 無法執行查詢。」或「無法透過 WMI 建立新程序」等錯誤。請在主機負載較低的時段重試備份。

在 Windows Server 2022 虛擬機器上設定應用程式感知備份

若要在執行 Windows Server 2022 的 Hyper-V 和 VMware ESXi 虛擬機器上執行應用程式感知備份，則必須使用代理程式型備份。如需有關備份模式的詳細資訊，請參閱 "代理程式型和無代理程式備份" (第 56 頁)。

	代理程式型備份	無代理程式備份
應用程式感知備份	支援	不支援
Cyber Protect 主控台中的虛擬機器圖示		

若要在代理程式型模式下設定應用程式感知備份

1. 在虛擬機器的客體作業系統中安裝保護代理程式 (例如，Windows 用代理程式、SQL 用代理程式或 Exchange 用代理程式)。
2. 在 Cyber Protect 主控台中，選擇您要安裝保護代理程式的電腦。
3. 在新的保護計劃中設定應用程式感知備份。
4. 將保護計劃套用到虛擬機器。
5. 執行保護計劃。

因此，將建立包含應用程式感知備份的備份存檔。

應用程式感知備份所需的使用者權限

應用程式感知備份包含磁碟上的 VSS 感知應用程式中繼資料。欲存取此中繼資料，代理程式需要有適當權限的帳戶，如下所列。系統會提示您在啟用應用程式備份時，指定此帳戶。

- 針對 SQL Server：
  帳戶必須是電腦上的 **[Backup Operators]** 或 **[系統管理員]** 群組成員，並且必須是您將備份之各執行個體的 **[系統管理員 (sysadmin)]** 角色成員。

  注意事項
  僅支援 Windows 驗證。

- 針對 Exchange Server：
  Exchange 2007：帳戶必須是電腦上 **Administrators** 群組的成員，以及 **Exchange Organization Administrators** 角色群組的成員。
  Exchange 2010 及更新版本：帳戶必須是電腦上 **Administrators** 群組的成員，以及 **Organization Management** 角色群組的成員。
- 對於 Active Directory：
  帳戶必須是網域系統管理員。

虛擬機器的其他需求

如果應用程式是在透過 VMware 用代理程式或 Hyper-V 用代理程式備份的虛擬機器上執行，請確保已在電腦上停用使用者帳戶控制 (UAC)。

如果您不想要停用 UAC，您必須在啟用應用程式備份時提供內建網域系統管理員 (DOMAIN\Administrator) 的認證。

注意事項
使用建立網域時設定的內建網域系統管理員帳戶。不支援之後建立的帳戶。

執行 Windows 的電腦的其他需求

針對所有 Windows 版本，您必須停用使用者帳戶控制 (UAC) 原則以允許應用程式感知備份。

如果您不想要停用 UAC，您必須在啟用應用程式備份時提供內建網域系統管理員 (DOMAIN\Administrator) 的認證。

注意事項
使用建立網域時設定的內建網域系統管理員帳戶。不支援之後建立的帳戶。

若要在 Windows 中停用 UAC 原則

1. 在登錄編輯程式中，找出以下登錄機碼：
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`
2. 將 **EnableLUA** 值變更為 **0**。
3. 重新啟動電腦。

信箱備份

Microsoft Exchange Server 2010 Service Pack 1 (SP1) 更新版本支援信箱備份。

如果在管理伺服器上註冊至少一個 Exchange 用代理程式，則會提供信箱備份。代理程式必須安裝在與 Microsoft Exchange Server 屬於相同 Active Directory 樹系的電腦上。

在備份信箱之前，您必須將 Exchange 用代理程式連線到用於執行 Microsoft Exchange Server 的 **[用戶端存取]** 伺服器角色 (CAS) 的電腦。在 Exchange 2016 和更新版本中，CAS 角色無法當做個別的安裝選項提供。它會自動安裝為信箱伺服器角色的一部分。因此，您可以將代理程式連線至執行 **[信箱角色]** 的任何伺服器。

注意事項

您也可以從資料庫備份和應用程式感知備份復原信箱和信箱項目。如需詳細資訊，請參閱 "復原 Exchange 信箱和信箱項目" (第 530 頁)。您無法使用資料庫備份和應用程式感知備份建立個別信箱的保護計劃。

將 Exchange 用代理程式連線到 CAS

1. 按一下 **[裝置]** > **[新增]**。
2. 按一下 [**Microsoft Exchange Server**]。
3. 按一下 **[Exchange 信箱]**。
   如果沒有在管理伺服器上註冊任何 Exchange 用代理程式，則軟體會要求您安裝一個代理程式。安裝完成後，從步驟 1 重複此程序。
4. [選用] 若在管理伺服器上註冊多個 Exchange 用代理程式，則按一下 **[代理程式]**，然後變更將執行備份的代理程式。
5. 在 **用戶端存取伺服器** 中，指定完全符合網域名稱 (FQDN) 的電腦，其中已啟用 Microsoft Exchange Server 的 **[用戶端存取]** 角色。
   在 Exchange 2016 和更新版本中，用戶端存取服務會自動安裝為信箱伺服器角色的一部分。因此，您可以指定執行 **[信箱角色]** 的任何伺服器。之後，我們在本節中會將此伺服器稱為 CAS。
6. 在 **[驗證類型]** 中，選擇 CAS 使用的驗證類型。您可以選擇 **Kerberos** (預設值) 或 **[基本]**。
7. \[僅適用於基本驗證] 選擇要使用的協定。您可以選擇 **HTTPS** (預設值) 或 **HTTP**。
8. [僅適用於採用 HTTPS 通訊協定的基本驗證] 如果 CAS 使用從認證機構獲得的 SSL 憑證，且您希望連接到 CAS 時軟體檢查該憑證，請選取 **[檢查 SSL 憑證]** 核取方塊。否則，請跳過此步驟。
9. 請指定將用於存取 CAS 的帳戶認證。此帳戶的需求會列在 < 需要的使用者權限 > 中。
10. 按一下 **[新增]**。

然後，信箱會顯示在 **[裝置]** > **[Microsoft Exchange]** > **[信箱]** 下方。

選擇 Exchange Server 信箱

如下所述選擇信箱，然後視需要指定保護計劃的其他設定。

選擇 Exchange 信箱

1. 按一下 **[裝置]** > **Microsoft Exchange**。
   軟體顯示 Exchange 資料庫和信箱的樹狀結構。
2. 按一下 **[信箱]**，然後選擇要備份的信箱。
3. 按一下 **[保護]**。

所需的使用者權限

若要存取信箱，Exchange 用代理程式需要有適當權限的帳戶。系統會提示您在設定信箱的各種操作時，指定此帳戶。

在 **[組織管理]** 角色群組內的帳戶成員資格可存取任何信箱，包括未來將會建立的信箱。

所需的最低使用者權限如下：

- 帳戶必須是 **[伺服器管理]** 和 **[收件者管理]** 角色群組的成員。
- 針對代理程式將會存取其信箱之所有使用者或使用者群組，必須啟用帳戶的 **ApplicationImpersonation** 管理角色。
  如需設定 **ApplicationImpersonation** 管理角色的資訊，請參閱下列 Microsoft 知識庫文章：https://msdn.microsoft.com/en-us/library/office/dn722376.aspx。

復原 SQL 資料庫

您可以從資料庫備份和應用程式感知備份還原 SQL 資料庫。如需有關兩種備份類型間差異的詳細資訊，請參閱 "保護 Microsoft SQL Server 和 Microsoft Exchange Server" (第 509 頁)。

您可以將 SQL 資料庫復原到原始電腦、原始電腦上的不同執行個體，或非原始電腦上的執行個體。當您執行復原到非原始電腦時，必須在目標電腦上安裝 SQL 用代理程式。

此外，您可以將資料庫當作檔案復原。

如果您為 SQL 執行個體使用 Windows 驗證，您必須在電腦上提供 **[Backup Operators]** 或 **[Administrators]** 群組成員所屬帳戶的認證，並在目標執行個體上提供 **[系統管理員 (sysadmin)]** 角色成員所屬帳戶的認證。如果您使用的是 SQL Server 驗證，您必須在目標執行個體上提供 **[系統管理員 (sysadmin)]** 角色成員所屬帳戶的認證。

系統資料庫會當作使用者資料庫復原，但有一些區別。若要深入瞭解這些區別，請參閱 "復原系統資料庫" (第 527 頁)。

復原期間，您可以在 Cyber Protect 主控台的 **[監控]** > **[活動]** 索引標籤上檢查作業進度。

將 SQL 資料庫復原到原始電腦

您可以將 SQL 資料庫復原到其原始電腦、原始電腦上的不同執行個體，或非原始目標電腦上的執行個體。

若要將 SQL 資料庫復原到原始電腦

從資料庫備份

1. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[Microsoft SQL]**。
2. 選擇 SQL Server 執行個體，或按一下執行個體以選擇您要復原的特定資料庫，然後按一下 **[復原]**。
   如果電腦處於離線狀態，就不會顯示復原點。若要將資料復原到非原始電腦，請參閱 "將 SQL 資料庫復原到非原始電腦" (第 523 頁)。

3. 選擇復原點

   復原點是依照位置篩選的。
4. 按一下 **[復原]** > **[資料庫至執行個體]**。

   根據預設，執行個體和資料庫都會復原到原始資料庫。您也可以將原始資料庫復原到新資料庫。
5. [復原到相同電腦上的非原始執行個體時] 按一下 **[目標 SQL Server 執行個體]**、選擇目標執行個體，然後按一下 **[完成]**。
6. [將資料庫復原為新資料庫時] 按一下資料庫名稱，然後在 **[復原到]** 中，選擇 **[新資料庫]**。
   - 指定新資料庫的名稱。
   - 指定新資料庫路徑。
   - 指定記錄路徑。
7. [選用] [不適用於將資料庫復原為新資料庫時] 若要在復原後變更資料庫狀態，按一下資料庫名稱、選擇以下其中一個狀態，然後按一下 **[完成]**。
   - **已可使用 (有恢復之復原)** (預設)

     復原完成後，資料庫將可供使用。使用者會擁有該資料庫的完整存取權限。軟體將會回復交易記錄中針對復原後的資料庫儲存的所有未認可交易。您將無法從原生 Microsoft SQL 備份復原其他交易記錄。
   - **不可正常運作 (無恢復之復原)**

     復原完成後，資料庫將無法操作。使用者不會有該資料庫的存取權限。軟體將會保留復原後的資料庫的所有未認可交易。您將能夠從原生 Microsoft SQL 備份復原其他交易記錄，從而到達所需的復原點。
   - **唯讀 (等候之復原)**

     復原完成後，使用者會擁有該資料庫的唯讀存取權限。軟體將會復原任何未認可交易。然而，它會將復原動作儲存在暫存待命檔案中，以便能還原復原的影響。

     此值主要用以偵測 SQL Server 錯誤發生時間點。
8. 按一下 **[開始復原]**。

從應用程式感知備份

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 選擇原本存放所要復原之資料的電腦，然後按一下 **[復原]**。

   如果電腦處於離線狀態，就不會顯示復原點。若要將資料復原到非原始電腦，請參閱 "將 SQL 資料庫復原到非原始電腦" (第 523 頁)。
3. 選擇復原點

   復原點是依照位置篩選的。
4. 按一下 **[復原]** > **[SQL 資料庫]**。
5. 選擇 SQL Server 執行個體，或按一下執行個體以選擇您要復原的特定資料庫，然後按一下 **[復原]**。

   根據預設，執行個體和資料庫都會復原到原始資料庫。您也可以將原始資料庫復原到新資料庫。
6. [復原到相同電腦上的非原始執行個體時] 按一下 **[目標 SQL Server 執行個體]**、選擇目標執行個體，然後按一下 **[完成]**。

7. [將資料庫復原為新資料庫時] 按一下資料庫名稱，然後在 **[復原到]** 中，選擇 **[新資料庫]**。
   - 指定新資料庫的名稱。
   - 指定新資料庫路徑。
   - 指定記錄路徑。
8. [選用] [不適用於將資料庫復原為新資料庫時] 若要在復原後變更資料庫狀態，按一下資料庫名稱、選擇以下其中一個狀態，然後按一下 **[完成]**。
   - **已可使用 (有恢復之復原)** (預設)

     復原完成後，資料庫將可供使用。使用者會擁有該資料庫的完整存取權限。軟體將會回復交易記錄中針對復原後的資料庫儲存的所有未認可交易。您將無法從原生 Microsoft SQL 備份復原其他交易記錄。
   - **不可正常運作 (無恢復之復原)**

     復原完成後，資料庫將無法操作。使用者不會有該資料庫的存取權限。軟體將會保留復原後的資料庫的所有未認可交易。您將能夠從原生 Microsoft SQL 備份復原其他交易記錄，從而到達所需的復原點。
   - **唯讀 (等候之復原)**

     復原完成後，使用者會擁有該資料庫的唯讀存取權限。軟體將會復原任何未認可交易。然而，它會將復原動作儲存在暫存待命檔案中，以便能還原復原的影響。

     此值主要用以偵測 SQL Server 錯誤發生時間點。
9. 按一下 **[開始復原]**。

將 SQL 資料庫復原到非原始電腦

您可以將應用程式感知備份和資料庫備份復原到安裝 SQL 用代理程式所在非原始目標電腦上的 SQL Server 執行個體。備份必須位於目標電腦可以存取的雲端儲存空間或共用儲存空間。

目標電腦上的 SQL Server 版本必須與來源電腦上的版本相同或更新。

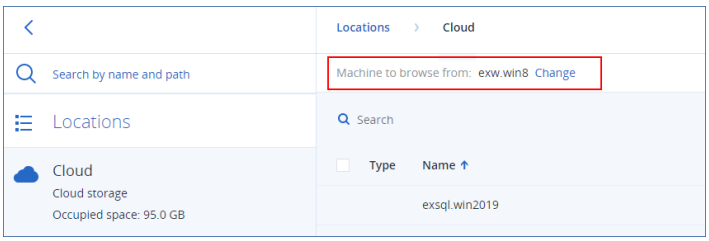
若要將 SQL 資料庫復原到非原始電腦

從備份儲存

此程序適用應用程式感知備份和資料庫備份。

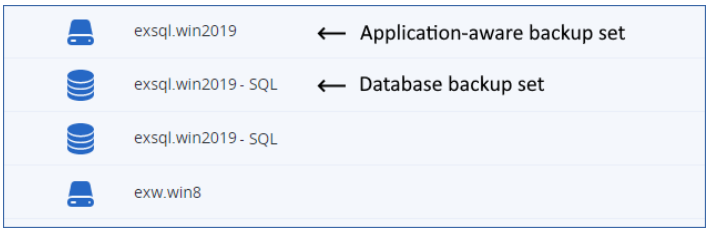
1. 在 Cyber Protect 主控台中，移至 **[備份儲存]**。
2. 選擇您要從中復原資料的備份集的位置。
3. 在 **[要瀏覽的電腦]** 中，選擇目標電腦。

   這是您將資料復原到的電腦。目標電腦必須處於連線狀態。



4. 選擇備份集，然後按一下 **[動作]** 窗格中的 **[顯示備份]**。

   應用程式感知備份集和資料庫備份集的圖示不同。



5. 選擇您要從中復原資料的復原點。
6. [對於資料庫備份] 按一下 **[復原 SQL 資料庫]**。
7. [對於應用程式感知備份] 按一下 **[復原]** > **[SQL 資料庫]**。
8. 選擇 SQL Server 執行個體，或按一下執行個體以選擇您要復原的特定資料庫，然後按一下 **[復原]**。
9. [如果在目標電腦上有多個 SQL 執行個體] 按一下 **[目標 SQL Server 執行個體]**、選擇目標執行個體，然後按一下 **[完成]**。
10. 按一下資料庫名稱、指定新資料庫路徑，然後按一下 **[完成]**。
    您可以在兩個欄位中指定相同的路徑，例如：

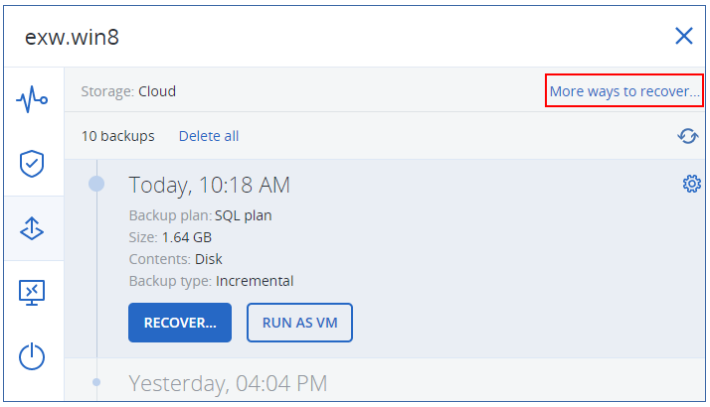
    ```
    C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
    ```

11. 按一下 **[開始復原]**。

從裝置

此程序僅適用於應用程式感知備份。

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 選擇原本存放所要復原之資料的電腦，然後按一下 **[復原]**。
3. [如果來源電腦處於連線狀態] 按一下 **[更多復原方式]**。



4. 按一下 **[選擇電腦]** 以選取目標電腦，然後按一下 **[確定]**。
   這是您將資料復原到的電腦。目標電腦必須處於連線狀態。
5. 選擇復原點
   復原點是依照位置篩選的。
6. 按一下 **[復原]** > **[SQL 資料庫]**。
7. 選擇 SQL Server 執行個體，或按一下執行個體以選擇您要復原的特定資料庫，然後按一下 **[復原]**。

8. [如果在目標電腦上有多個 SQL 執行個體] 按一下 **[目標 SQL Server 執行個體]**、選擇目標執行個體，然後按一下 **[完成]**。
9. 按一下資料庫名稱、指定新資料庫路徑，然後按一下 **[完成]**。
   您可以在兩個欄位中指定相同的路徑，例如：

   ```
   C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
   ```

10. 按一下 **[開始復原]**。

將 SQL 資料庫當作檔案復原

您可以將資料庫當作檔案復原。如果您需要擷取資料以供資料採礦、稽核或使用第三方工具進一步處理，此選項即可派上用場。若要瞭解如何將 SQL 資料庫檔案附加到 SQL Server 執行個體，請參閱 "附加 SQL Server 資料庫" (第 527 頁)。

您可以將資料庫當作檔案，復原到安裝 SQL 用代理程式所在的原始電腦或非原始目標電腦。當您將資料復原到非原始電腦時，備份必須位於雲端儲存空間或目標電腦可以存取的共用儲存空間。

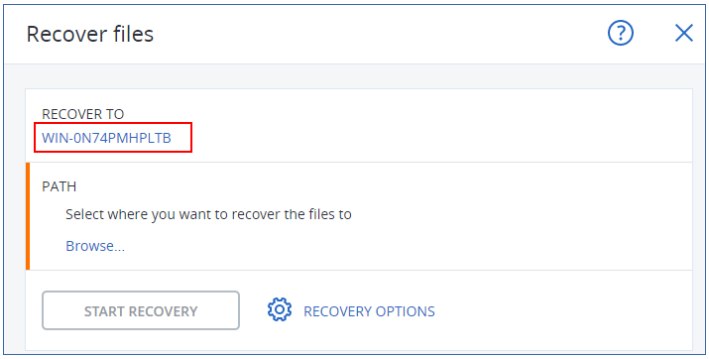
注意事項
如果您使用 VMware 用代理程式 (Windows)，將資料庫當作檔案復原是唯一的復原方法。您無法使用 VMware 用代理程式 (虛擬裝置) 復原資料庫。

將資料庫作為檔案復原

從資料庫備份

此程序適用於線上來源電腦。

1. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[Microsoft SQL]**。
2. 選擇您要復原的資料庫，然後按一下 **[復原]**。
3. 選擇復原點
   復原點是依照位置篩選的。
4. 請按一下 **[復原]** > **[資料庫作為檔案]**。
5. [復原到非原始電腦時] 在 **[復原到]** 中，選擇目標電腦。
   這是您將資料復原到的電腦。目標電腦必須處於連線狀態。
   若要變更選取項目，按一下電腦名稱、選擇其他電腦，然後按一下 **[確定]**。



6. 在 **[路徑]** 中，按一下 **[瀏覽]**、選擇要將檔案儲存到其中的本機或網路資料夾，然後按一下 **[完成]**。
7. 按一下 **[開始復原]**。

從應用程式感知備份

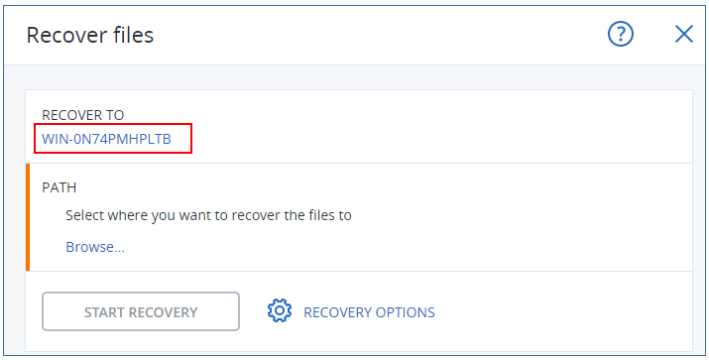
此程序適用於線上來源電腦。

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 選擇原本存放所要復原之資料的電腦，然後按一下 **[復原]**。
3. 選擇復原點

   復原點是依照位置篩選的。
4. 按一下 **[復原]** > **[SQL 資料庫]**、選擇要復原的資料庫，然後按一下 **[作為檔案復原]**。
5. [復原到非原始電腦時] 在 **[復原到]** 中，選擇目標電腦。

   這是您將資料復原到的電腦。目標電腦必須處於連線狀態。

   若要變更選取項目，按一下電腦名稱、選擇其他電腦，然後按一下 **[確定]**。



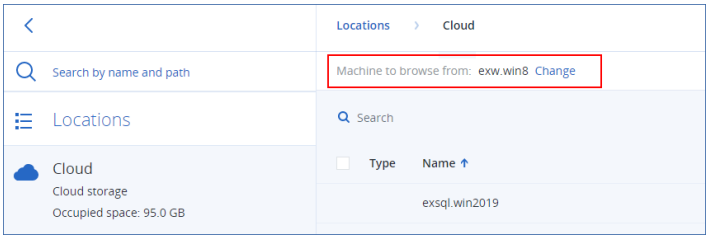
6. 在 **[路徑]** 中，按一下 **[瀏覽]**、選擇要將檔案儲存到其中的本機或網路資料夾，然後按一下 **[完成]**。
7. 按一下 **[開始復原]**。

從離線電腦上的備份

此程序適用於離線來源電腦上的應用程式感知備份和資料庫備份。

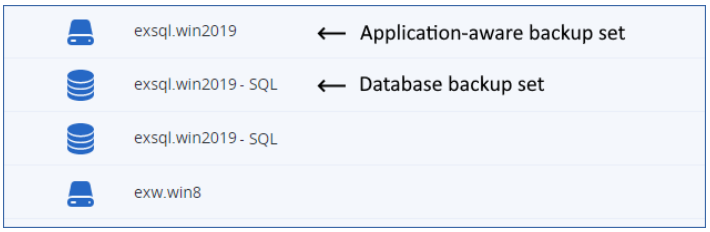
1. 在 Cyber Protect 主控台中，移至 **[備份儲存]**。
2. 選擇您要從中復原資料的備份集的位置。
3. 在 **[要瀏覽的電腦]** 中，選擇目標電腦。

   這是您將資料復原到的電腦。目標電腦必須處於連線狀態。



4. 選擇備份集，然後按一下 **[動作]** 窗格中的 **[顯示備份]**。

   應用程式感知備份集和資料庫備份集的圖示不同。



5. 選擇您要從中復原資料的復原點。
6. [對於資料庫備份] 按一下 **[復原 SQL 資料庫]**。
7. [對於應用程式感知備份] 按一下 **[復原]** > **[SQL 資料庫]**。
8. 選擇 SQL Server 執行個體，或按一下執行個體以選擇您要復原的特定資料庫，然後按一下 **[作為檔案復原]**。
9. 在 **[路徑]** 中，按一下 **[瀏覽]**、選擇要將檔案儲存到其中的本機或網路資料夾，然後按一下 **[完成]**。
10. 按一下 **[開始復原]**。

復原系統資料庫

系統會立即復原執行個體的所有系統資料庫。復原系統資料庫時，軟體會自動以單一使用者模式重新啟動目的地執行個體。復原完成後，軟體會重新啟動執行個體並復原其他資料庫 (如果有的話)。

復原系統資料庫時應考量的其他事項：

- 系統資料庫只能復原至與原始執行個體版本相同的執行個體。
- 系統資料庫一律會在「已可使用」狀態中復原。

復原 master 資料庫

系統資料庫包含 **master** 資料庫。**master** 資料庫會記錄執行個體之所有資料庫的相關資訊。因此，備份中的 **master** 資料庫包含備份時存在於執行個體中之資料庫的相關資訊。復原 **master** 資料庫後，您可能需要進行下列任何作業：

- 執行個體無法看到備份完成後出現在執行個體中的資料庫。如果要使這些資料庫恢復執行，請使用 SQL Server Management Studio 手動將其連接至執行個體。
- 備份完成後刪除的資料庫會在執行個體中顯示為離線。請使用 SQL Server Management Studio 刪除這些資料庫。

附加 SQL Server 資料庫

本節說明如何使用 SQL Server Management Studio 在 SQL Server 中附加資料庫。一次只能附加一個資料庫。

如需附加資料庫，需要以下任一權限：**[建立資料庫]**、**[建立任一資料庫]** 或 **[變更任一資料庫]**。一般狀況下，這些權限會獲授予執行個體的 **sysadmin** 角色。

若要附加資料庫

1. 執行 Microsoft SQL Server Management Studio。
2. 連線至所要的 SQL Server 執行個體，然後展開執行個體。

3. 用滑鼠右鍵按一下 **[資料庫]**，然後按一下 **[附加]**。
4. 按一下 **[新增]**。
5. 在 **[尋找資料庫檔案]** 對話方塊中，尋找並選擇資料庫的 .mdf 檔案。
6. 在 **[資料庫詳細資料]** 區段中，確定已找到其他的資料庫檔案 (.ndf 和 .ldf 檔案)。

   詳細資料。在以下情況中，可能無法自動找到 SQL Server 資料庫檔案：
   - 檔案不在預設位置，或不在主要資料庫檔案 (.mdf) 所在的相同資料夾。解決方法：在 **[目前的檔案路徑]** 欄中，手動指定所需檔案的路徑。
   - 您復原了一組不完整的資料庫檔案。解決方法：從備份復原遺失的 SQL Server 資料庫檔案。
7. 當所有檔案都已找到時，按一下 **[確定]**。

復原 Exchange 資料庫

本節說明如何從資料庫備份和應用程式感知備份復原。

您可以將 Exchange Server 資料復原為作用中的線上 Exchange Server；有可能是原始的 Exchange Server，或是在使用完整網域名稱 (FQDN) 的電腦中執行的同版本 Exchange Server。目標電腦必須安裝有 Exchange 用代理程式。

下表摘述可讓您選擇復原的 Exchange Server 資料，以及復原該資料所須具備的最低使用者權限。

Exchange 版本	資料項目	使用者權限
2007	儲存群組	**Exchange Organization Administrators** 角色群組的成員資格。
2010/2013/2016/2019	資料庫	**伺服器管理**角色群組的成員資格。

或者，您可以將資料庫 (儲存群組) 做為檔案復原。系統會從備份檔將資料庫檔案和交易記錄檔擷取到您指定的資料夾。如果您需要擷取資料以供稽核或使用第三方工具進一步處理，或者復原作業因某些原因而失敗，而您要尋找手動掛載資料庫的解決方法，這項功能即可派上用場。

若您只使用 VMware 用代理程式 (Windows)，則將資料庫當做檔案復原是唯一可用的復原方法。您無法使用 VMware 用代理程式 (虛擬裝置) 復原資料庫。

在以下程序中，我們會以「資料庫」指稱資料庫和儲存群組。

將 Exchange 資料庫復原至即時 Exchange

1. 執行下列其中一項操作：
   - 從應用程式感知備份復原時，在**[裝置]**下，選擇原本存放所要復原之資料的電腦。
   - 若要從資料庫備份復原，請按一下 **[裝置]** > **[Microsoft Exchange]** > **[資料庫]**，然後選擇要復原的資料庫。
2. 按一下 **[復原]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。

   如果電腦處於離線狀態，復原點就不會顯示。執行下列其中一項操作：
   - [僅從應用程式感知備份復原時]如果備份位置是雲端或共用儲存 (即可被其他代理程式存取)，按一下 **[選擇電腦]**，選擇有 Exchange 用代理程式的線上電腦，然後選擇復原點。
   - 在 [備份儲存] 索引標籤上選擇復原點。

透過以上任一瀏覽動作所選的電腦，將會成為 Exchange 資料復原的目標電腦。

4. 執行下列其中一項操作：
   - 從應用程式感知備份復原時，按一下 **[復原]** > **[Exchange 資料庫]**，選擇要復原的資料庫，然後按一下 **[復原]**。
   - 從資料庫備份復原時，請按一下 **[復原]**> **[將資料庫復原為 Exchange 伺服器]**。
5. 依預設，資料庫會復原為原始資料庫。如果原始資料庫不存在，系統會重新建立資料庫。

   若要復原為其他資料庫，請執行下列步驟：
   a. 按一下資料庫名稱。
   b. 從 [**復原至**] 中選擇 [**新資料庫**]。
   c. 指定新資料庫的名稱。
   d. 指定新資料庫的路徑和記錄路徑。指定的資料夾不得包含原始資料庫和記錄檔案。
6. 按一下 **[開始復原]**。

復原進度會顯示在 [活動] 索引標籤上。

將 Exchange 資料庫作為檔案復原

1. 執行下列其中一項操作：
   - 從應用程式感知備份復原時，在**[裝置]**下，選擇原本存放所要復原之資料的電腦。
   - 若要從資料庫備份復原，請按一下 **[裝置]** > **[Microsoft Exchange]** > **[資料庫]**，然後選擇要復原的資料庫。
2. 按一下 **[復原]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。

   如果電腦處於離線狀態，復原點就不會顯示。執行下列其中一項操作：
   - [僅從應用程式感知備份復原時] 如果備份位置是雲端或共用儲存 (即可被其他代理程式存取)，按一下 **[選擇電腦]**，選擇有 Exchange 用代理程式或 VMware 用代理程式的線上電腦，然後選擇復原點。
   - 在 [備份儲存] 索引標籤上選擇復原點。

   透過以上任一瀏覽動作所選的電腦，將會成為 Exchange 資料復原的目標電腦。
4. 執行下列其中一項操作：
   - 從應用程式感知備份復原時，按一下 **[復原]** > **[Exchange 資料庫]**，選擇要復原的資料庫，然後按一下 **[做為檔案復原]**。
   - 從資料庫備份復原時，請按一下 **[復原]** **[將資料庫復原為檔案]**。
5. 按一下 **[瀏覽]**，選擇要用於儲存檔案的本機或網路資料夾。
6. 按一下 **[開始復原]**。

復原進度會顯示在 [活動] 索引標籤上。

掛載 Exchange Server 資料庫

復原資料庫檔案後，您可以掛載資料庫來使其上線。您可以使用 Exchange 管理主控台、Exchange 系統管理員或 Exchange 管理命令介面來執行掛載。

復原的資料庫將會處於「不正常關機」狀態。如果將處於「不正常關機」狀態的資料庫復原至其原始位置 (即 Active Directory 中有原始資料庫的相關資訊), 就可以由系統執行掛載。將資料庫復原至其他位置 (例如新的資料庫或復原資料庫) 時, 您需要使用 `Eseutil /r <Enn>` 命令, 使其成為「正常關機」狀態, 否則無法掛載該資料庫。`<Enn>` 會指定您需要在其中套用交易記錄檔之資料庫 (或包含該資料庫的儲存群組) 的記錄檔首碼。

您必須為用於附加資料庫的帳戶委派 Exchange Server 系統管理員角色, 以及目標伺服器的本機 Administrators 群組。

如需有關如何掛載資料庫的詳細資訊, 請參閱下列文章:

- Exchange 2010 或更新版本: http://technet.microsoft.com/en-us/library/aa998871.aspx
- Exchange 2007: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.80).aspx

復原 Exchange 信箱和信箱項目

您可以從以下備份復原 Exchange 信箱和信箱項目:

- 資料庫備份
- 應用程式感知備份
- 信箱備份

您可以復原下列項目:

- 信箱 (封存信箱除外)
- 公用資料夾

> **注意事項**
> 僅可從資料庫備份取得。請參閱 "選擇 Exchange Server 資料" (第 513 頁)。

- 公用資料夾項目
- 電子郵件資料夾
- 電子郵件訊息
- 行事曆事件
- 工作
- 連絡人
- 日誌項目
- 記事

您可以使用搜尋找出這些項目。

信箱或信箱項目可以復原至即時 Exchange Server 或 Microsoft 365。

復原至 Exchange Server

細微復原功能僅限於 Microsoft Exchange Server 2010 Service Pack 1 (SP1) 及更新版本中執行。來源備份可包含任何 Exchange 支援版本的資料庫或信箱。

細微復原可由 Exchange 用代理程式或 VMware 用代理程式 (Windows) 執行。執行代理程式的目標 Exchange Server 和電腦必須屬於同一個 Active Directory 樹系。

將信箱復原至現有的信箱時，系統會覆寫 ID 相符的現有項目。

信箱項目復原不會造成任何覆寫。而是會在目標資料夾中重新建立信箱項目的完整路徑。

對於使用者帳戶的要求

從備份復原的信箱必須在 Active Directory 中具有一個相關聯的使用者帳戶。

只有在相關聯的使用者帳戶*為啟用狀態*時，才能復原使用者信箱及其中的內容。共用、會議室和設備信箱僅在其相關聯使用者帳戶*為停用狀態*時，才能復原。

系統執行復原時會直接略過不符合上述條件的信箱。

如果系統略過某些信箱，復原會成功，但也會出現警告。如果系統略過所有信箱，復原將會失敗。

復原至 Microsoft 365

如果在本機安裝 Microsoft 365 用代理程式，則支援將 Exchange 資料項目復原至 Microsoft 365，反之亦然。

復原功能可在 Microsoft Exchange Server 2010 及更新版本的備份中執行。

將信箱復原至現有的 Microsoft 365 信箱時，現有項目會保持原樣，且復原的項目會放置在其旁邊。

復原單一信箱時，您需要選擇目標 Microsoft 365 信箱。在一次復原作業過程中復原數個信箱時，軟體嘗試將每個信箱復原至相同名稱使用者的信箱。若找不到使用者，則會略過信箱。如果系統略過某些信箱，復原會成功，但會出現警告。如果系統略過所有信箱，復原將會失敗。

如需有關復原至 Microsoft 365 的詳細資訊，請參閱 "保護 Microsoft 365 資料" (第 542 頁)。

復原信箱

若要從應用程式感知備份或資料庫備份復原信箱

1. [僅在從資料庫備份復原至 Microsoft 365 時] 如果 Microsoft 365 用代理程式未安裝在已備份且執行 Exchange Server 的電腦上，請執行下列其中一項作業：
   - 如果組織中沒有 Microsoft 365 用代理程式，則在已備份的電腦 (或在具有相同 Microsoft Exchange Server 版本的另一部電腦) 上安裝 Microsoft 365 用代理程式。
   - 如果組織中已安裝 Microsoft 365 用代理程式，則從已備份的電腦 (或在具有相同 Microsoft Exchange Server 版本的另一部電腦) 上，將程式庫複製到裝有 Microsoft 365 用代理程式的電腦中，如「複製 Microsoft Exchange 程式庫」中所述。
2. 執行下列其中一項操作：
   - 從應用程式感知備份復原時：在 **[裝置]** 下，選擇原本存放所要復原之資料的電腦。
   - 從資料庫備份復原時，按一下 **[裝置]** > **[Microsoft Exchange]** > **[資料庫]**，然後選擇原本存放所要復原之資料的資料庫。
3. 按一下 **[復原]**。
4. 選擇復原點請注意，復原點是依照位置進行篩選。

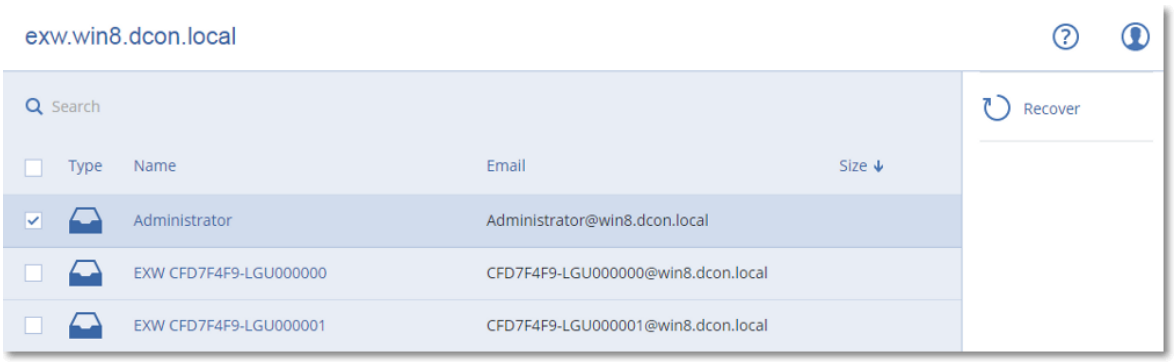
如果電腦處於離線狀態，復原點就不會顯示。請使用其他復原方式：

- [僅從應用程式感知備份復原時] 如果備份位置是雲端或共用儲存 (即可被其他代理程式存取)，按一下 **[選擇電腦]**，選擇有 Exchange 用代理程式或 VMware 用代理程式的線上電腦，然後選擇復原點。
- 在 [備份儲存] 索引標籤上選擇復原點。

復原作業會由透過上述任一動作所選來瀏覽的電腦執行，而非由離線的原始電腦執行。

5. 依序按一下 **[復原]** > **[Exchange 信箱]**。
6. 選擇您要復原的信箱。

   您可以按名稱搜尋信箱。不支援萬用字元。



7. 按一下 **[復原]**。
8. [僅在復原至 Microsoft 365 時]：
   a. 在 **[復原至]** 中，選擇 **[Microsoft 365]**。
   b. [若只選擇步驟 6 中的一個信箱] 在 **目標信箱** 中，指定目標信箱。
   c. 按一下 **[開始復原]**。

   此程序無需執行更多步驟。

   按一下 **[具有 Microsoft Exchange Server 的目標電腦]** 以選擇或變更目標電腦。此步驟可允許非執行 Exchange 用代理程式的電腦進行復原。

   指定電腦的完整網域名稱 (FQDN)，其中已啟用 **[用戶端存取]** 角色 (在 Microsoft Exchange Server 2010/2013 中)，或 **[信箱角色]** (在 Microsoft Exchange Server 2016 或更新版本中)。電腦所屬的 Active Directory 樹系必須與執行復原之機器所屬的樹系相同。
9. 若顯示提示，請指定將用於存取電腦的帳戶認證。此帳戶的需求會列在 < 需要的使用者權限 > 中。
10. [選用] 按一下 **[重新建立任何遺失信箱的資料庫]** 以變更自動選擇的資料庫。
11. 按一下 **[開始復原]**。

復原進度會顯示在 **[活動]** 索引標籤上。

若要從信箱備份復原信箱

1. 按一下 **[裝置]** > **[Microsoft Exchange]** > **[信箱]**。
2. 選擇要復原的信箱，然後按一下**[復原]**。

   您可以按名稱搜尋信箱。不支援萬用字元。

   如果信箱遭到刪除，在 [備份儲存] 索引標籤中選擇此信箱，然後按一下 **[顯示備份]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。

4. 請按一下**[復原]** > **[信箱]**。
5. 執行以上程序的步驟 8-11。

復原信箱項目

若要從應用程式感知備份或資料庫備份復原信箱項目

1. [僅在從資料庫備份復原至 Microsoft 365 時] 如果 Microsoft 365 用代理程式未安裝在已備份且執行 Exchange Server 的電腦上，請執行下列其中一項作業：
   - 如果組織中沒有 Microsoft 365 用代理程式，則在已備份的電腦 (或在具有相同 Microsoft Exchange Server 版本的另一部電腦) 上安裝 Microsoft 365 用代理程式。
   - 如果組織中已安裝 Microsoft 365 用代理程式，則從已備份的電腦 (或在具有相同 Microsoft Exchange Server 版本的另一部電腦) 上，將程式庫複製到裝有 Microsoft 365 用代理程式的電腦中，如「複製 Microsoft Exchange 程式庫」中所述。
2. 執行下列其中一項操作：
   - 從應用程式感知備份復原時：在 **[裝置]** 下，選擇原本存放所要復原之資料的電腦。
   - 從資料庫備份復原時，按一下 **[裝置]** > **[Microsoft Exchange]** > **[資料庫]**，然後選擇原本存放所要復原之資料的資料庫。
3. 按一下 **[復原]**。
4. 選擇復原點請注意，復原點是依照位置進行篩選。

   如果電腦處於離線狀態，復原點就不會顯示。請使用其他復原方式：
   - [僅從應用程式感知備份復原時] 如果備份位置是雲端或共用儲存 (即可被其他代理程式存取)，按一下 **[選擇電腦]**，選擇有 Exchange 用代理程式或 VMware 用代理程式的線上電腦，然後選擇復原點。
   - 在 [備份儲存] 索引標籤上選擇復原點。

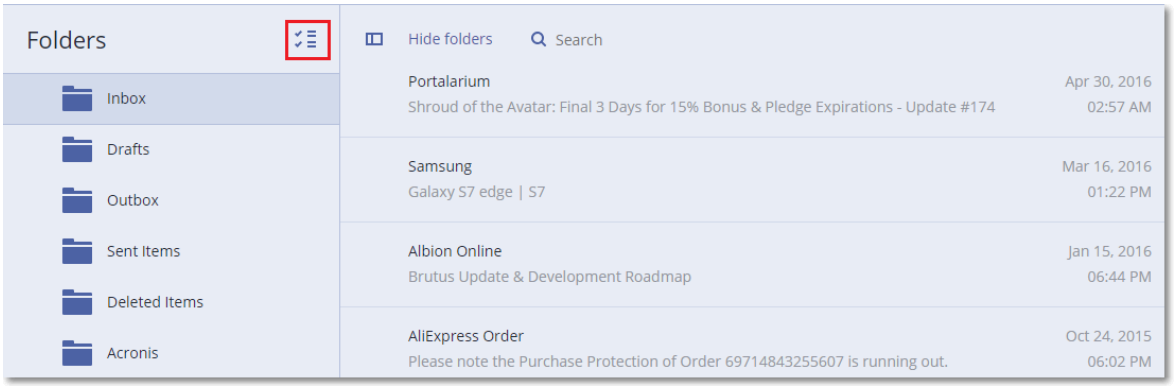
   復原作業會由透過上述任一動作所選來瀏覽的電腦執行，而非由離線的原始電腦執行。
5. 依序按一下 **[復原]** > **[Exchange 信箱]**。
6. 按一下最初具有您想要復原之項目的信箱。
7. 選擇您要復原的項目。

   您可以選取下列搜尋選項。不支援萬用字元。
   - 電子郵件訊息：依主題、寄件者、收件者及日期搜尋。
   - 事件：依主題及日期搜尋。
   - 工作：依主題及日期搜尋。
   - 連絡人：依姓名、電子郵件地址和電話號碼搜尋。

   選擇了電子郵件訊息後，按一下 **[顯示內容]** 以檢視其內容和附件。

   注意事項
   要下載附加檔案，請按一下名稱。

   若要能夠選擇資料夾，請按一下復原資料夾圖示。



8. 按一下 **[復原]**。
9. 若要復原至 Microsoft 365，請在 **[復原至]** 中，選擇 **[Microsoft 365]**。

   若要復原至 Exchange Server，保留**復原至**中的 **Microsoft Exchange** 預設值。

   [僅在復原至 Exchange Server 時]按一下 **[具有 Microsoft Exchange Server 的目標電腦]** 以選擇或變更目標電腦。此步驟可允許非執行 Exchange 用代理程式的電腦進行復原。

   指定電腦的完整網域名稱 (FQDN)，其中已啟用 **[用戶端存取]** 角色 (在 Microsoft Exchange Server 2010/2013 中)，或 **[信箱角色]** (在 Microsoft Exchange Server 2016 或更新版本中)。電腦所屬的 Active Directory 樹系必須與執行復原之機器所屬的樹系相同。
10. 若顯示提示，請指定將用於存取電腦的帳戶認證。此帳戶的需求會列在 < 需要的使用者權限 > 中。
11. **[目標信箱]** 可以檢視、變更或指定目標信箱。

    原始信箱預設為選取狀態。如果此信箱不存在或選取了非原始目標電腦，則必須指定目標信箱。
12. [僅恢復電子郵件訊息時] 在**目標資料夾**中，查看或變更目標信箱中的目標資料夾。根據預設，已選取 **[已復原項目]** 資料夾。由於 Microsoft Exchange 的限制，無論指定任何不同的**目標資料夾**，事件、工作、記事和聯絡人都會還原到其原始位置。
13. 按一下 **[開始復原]**。

復原進度會顯示在 **[活動]** 索引標籤上。

若要從信箱備份復原信箱項目

1. 按一下 **[裝置]** > **[Microsoft Exchange]** > **[信箱]**。
2. 按一下最初具有您想要復原之項目的信箱，然後按一下**[復原]**。

   您可以按名稱搜尋信箱。不支援萬用字元。

   如果信箱遭到刪除，在 [備份儲存] 索引標籤中選擇此信箱，然後按一下 **[顯示備份]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。
4. 按一下**[復原]** > **[電子郵件訊息]**。
5. 選擇您要復原的項目。

   您可以選取下列搜尋選項。不支援萬用字元。
   - 電子郵件訊息：依主題、寄件者、收件者及日期搜尋。
   - 事件：依主題及日期搜尋。
   - 工作：依主題及日期搜尋。
   - 連絡人：依姓名、電子郵件地址和電話號碼搜尋。

選擇了電子郵件訊息後，按一下 **[顯示內容]** 以檢視其內容和附件。

注意事項
要下載附加檔案，請按一下名稱。

選擇電子郵件訊息後，您可按一下**[以電子郵件傳送]**，向電子郵件地址傳送訊息。訊息便會從您的管理員帳戶的電子郵件地址傳送。

若要能夠選擇資料夾，請按一下 [復原資料夾] 圖示： 

6. 按一下 **[復原]**。
7. 執行以上程序的步驟 9-13。

複製 Microsoft Exchange Server 程式庫

將 Exchange 信箱或信箱項目復原至 Microsoft 365 時，您可能需要從已備份的電腦 (或具有相同 Microsoft Exchange Server 版本的另一部電腦) 上，將下列程式庫複製到已安裝 Microsoft 365 用代理程式的電腦中。

根據已備份的 Microsoft Exchange Server 版本，複製下列檔案。

Microsoft Exchange Server 版本	程式庫	預設位置
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

程式庫應該位於 %ProgramData%\Acronis\ese 資料夾中。如果此資料夾不存在，請手動建立。

變更 SQL Server 或 Exchange Server 存取認證

您可以變更 SQL Server 或 Exchange Server 的存取認證，而無需重新安裝代理程式。

若要變更 SQL Server 或 Exchange Server 存取認證

1. 按一下 **[裝置]**，然後按一下 **Microsoft SQL** 或 **Microsoft Exchange**。
2. 選擇您要變更其存取認證的 [Always On 可用性群組]、[資料庫可用性群組]、SQL Server 執行個體或 Exchange Server。

3. 按一下 **[指定認證]**。
4. 指定新的存取認證，然後按一下 **[確定]**。

若要變更信箱備份的 Exchange Server 存取認證

1. 按一下 **[裝置]** > **Microsoft Exchange**，然後展開 **[信箱]**。
2. 選擇您要變更其存取認證的 Exchange Server。
3. 按一下 **[設定]**。
4. 在**Exchange 系統管理員帳戶**下，指定新的存取認證，然後按一下 **[儲存]**。

保護行動裝置

Acronis Cyber Protect 應用程式可讓您將行動資料備份到雲端儲存空間，然後在遺失或損毀時將其復原。請注意，備份至雲端儲存空間需要有一個帳戶以及雲端訂購授權。

支援的行動裝置

您可以在執行下列其中一個作業系統的行動裝置上安裝 Acronis Cyber Protect 應用程式：

- iOS 15 至 iOS 17 (iPhone、iPod、iPad)
- Android 10 至 Android 14

可備份的內容

- 聯絡人 (姓名、電話號碼和電子郵件)
- 照片 (保留照片的原始大小及格式)
- 影片
- 行事曆
- 提醒訊息 (僅適用於 iOS 裝置)

須知事項

- 您只能將資料備份到雲端儲存。
- 每次開啟應用程式時，都會看到資料變更摘要，而且您可以手動啟動備份。
- **[連續備份]** 功能預設為啟用狀態。如果開啟此設定，Acronis Cyber Protect 應用程式會自動即時偵測新資料並將其上傳到雲端。
- **[僅使用 Wi-Fi]** 選項在應用程式設定中預設為啟用狀態。如果開啟此設定，則只會在有 Wi-Fi 連線時，Acronis Cyber Protect 應用程式才會備份資料。如果失去 Wi-Fi 連線，備份程序將不會開始。若要讓應用程式也使用行動數據連線，請將此選項關閉。
- 裝置上的電池最佳化功能可能會使 Acronis Cyber Protect 應用程式無法正常運作。若要準時執行備份，您應該停止應用程式的電池最佳化功能。
- 您有兩種節省能源的方法：
  - **[充電時備份]** 功能預設為停用狀態。如果此設定已開啟，則只會在您的裝置連線到電源時，Acronis Cyber Protect 應用程式才會備份資料。當裝置在連續備份過程中與電源中斷連線，備份將會暫停。

- **[省電模式]** 預設為啟用狀態。如果已開啟此設定，則只會在您的裝置電池電力充足時，Acronis Cyber Protect 應用程式才會備份資料。當裝置電池電力不足時，連續備份將會暫停。
- 您可以使用註冊在您帳戶之下的任何行動裝置存取備份資料。這有助於您將資料從舊的行動裝置移轉到新裝置。Android 裝置和 iOS 裝置上的連絡人和相片可以相互移轉復原。您也可以使用 Cyber Protect 主控台，將相片、影片或聯絡人下載到任何裝置。
- 從用您的帳戶登錄的行動裝置備份的資料僅可在此帳戶下 使用。其他人無法檢視或復原您的資料。
- 在 Acronis Cyber Protect 應用程式中，您只能復原最新的資料版本。如果您需要從特定的備份版本復原，請在平板電腦或電腦上使用 Cyber Protect 主控台。
- 保留規則不適用於行動裝置備份。
- [僅適用於 Android 裝置] 如果備份期間裝有 SD 卡，系統也會一併備份儲存在這張卡上的資料。資料將會復原到 SD 卡上；如果復原期間裝有 SD 卡，則會復原到 **[備份復原]** 資料夾；或者應用程式將會要求將資料復原到其他位置。

何處取得 Acronis Cyber Protect 應用程式

根據您的行動裝置而定，從 App Store 或 Google Play 安裝應用程式。

如何開始備份資料

1. 開啟應用程式。
2. 使用您的帳戶登入。
3. 點選 **[設定]** 可建立備份。請注意，只有在您沒有行動裝置備份時，才會顯示此按鈕。
4. 選擇您要備份的資料類別。系統預設為全選所有類別。
5. [選擇性步驟] 啟用 **[加密備份]** 可透過加密保護備份。在這個案例中，您也將需要：
   a. 輸入加密密碼兩次。

      注意事項
      請務必記住密碼，因為永遠無法還原或變更忘記的密碼。

   b. 點選 **[加密]**。
6. 點選**[備份]**。
7. 允許應用程式存取您的個人資料。如果您拒絕存取某些資料類別，便不會對它們進行備份。

備份開始。

如何將資料復原至行動裝置

警告！
若要復原行動資料，您必須使用使用者帳戶。

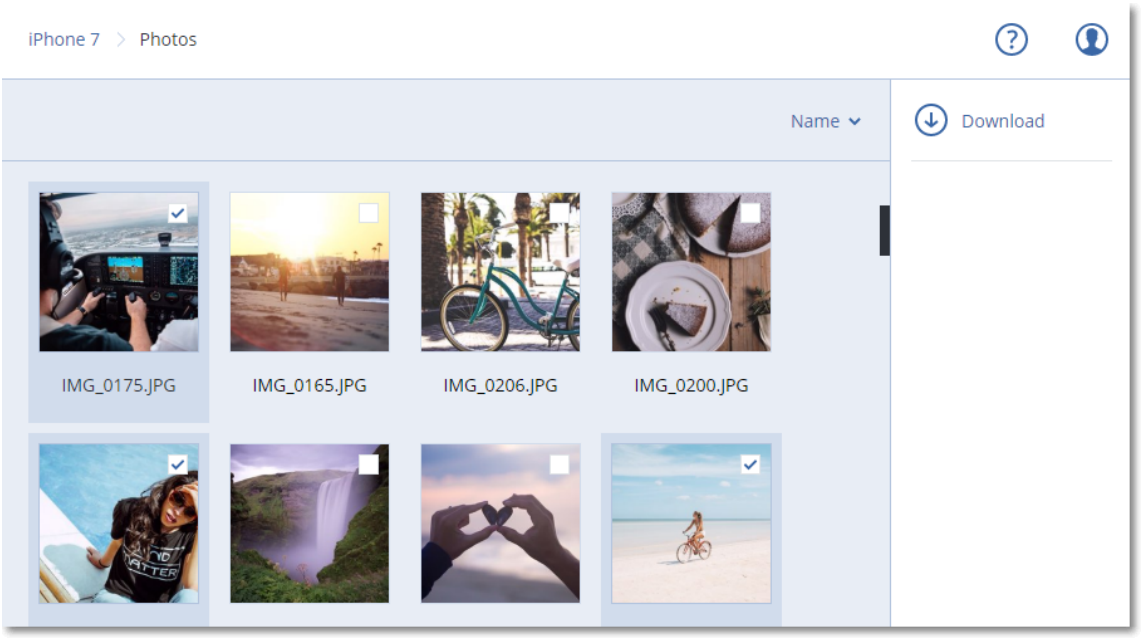
1. 開啟 Acronis Cyber Protect 應用程式。
2. 點選 **[瀏覽]**。
3. 點選裝置名稱。

4. 執行下列其中一項操作：
   - 若要復原所有備份的資料，點選 **[復原全部]**。您不需要再進行任何動作。
   - 若要復原一個或多個資料類別，點選 **[選擇]**，然後點選所需資料類別的核取方塊。點選 **[復原]**。您不需要再進行任何動作。
   - 若要復原屬於同一資料類別的一個或多個資料項目，點選資料類別。繼續進行後續步驟。
5. 執行下列其中一項操作：
   - 若要復原單一資料項目，請點選此項目。
   - 若要復原多個資料項目，點選 **[選擇]**，然後點選所需資料項目的核取方塊。
6. 點選 **[復原]**。

如何透過 Cyber Protect 主控台檢閱資料

1. 在電腦上開啟瀏覽器，並輸入 Cyber Protect 主控台 URL。
2. 使用您的帳戶登入。
3. 在 **[所有裝置]** 中，按一下行動裝置名稱底下的 **[復原]**。
4. 執行下列任何一項作業：
   - 若要下載所有相片、影片、連絡人、行事曆或提醒，選擇相應的資料類別。按一下 **[下載]**。

   - 若要下載個別相片、影片、連絡人、行事曆或提醒，按一下相應的資料類別名稱，然後選擇所需資料項目的核取方塊。按一下 **[下載]**。



- 若要預覽相片或聯絡人，按一下相應的資料類別名稱，然後按一下所需的資料項目。

保護託管的 Exchange 資料

哪些項目可以備份？

您可以備份使用者信箱、共用信箱和群組信箱。或者，您可以選擇備份所選信箱的封存信箱 (**就地封存**)。

可以復原哪些項目？

下列項目可以從信箱備份復原：

- 信箱
- 電子郵件資料夾
- 電子郵件訊息
- 行事曆事件
- 工作
- 連絡人
- 日誌項目
- 記事

您可以使用搜尋找出這些項目。

復原信箱、信箱項目、公用資料夾和公用資料夾項目時，您可以選擇是否要覆寫目標位置中的項目。

將信箱復原至現有的信箱時，系統會覆寫 ID 相符的現有項目。

信箱項目復原不會造成任何覆寫。而是會在目標資料夾中重新建立信箱項目的完整路徑。

選擇 Exchange Online 信箱

如下所述選擇信箱，然後視需要指定保護計劃的其他設定。

若要選取 Exchange Online 信箱

1. 按一下 **[裝置] > [託管的 Exchange]**。
2. 如果多個託管的 Exchange 組織新增到 Cyber Protection 服務，請選擇您要備份其使用者資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
   - 若要備份所有使用者信箱和所有共用信箱 (包括之後建立的信箱)，展開 **[使用者]** 節點、選取 **[所有使用者]**，然後按一下 **[群組備份]**。
   - 若要備份個別的使用者信箱或共用信箱，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要備份其信箱的使用者，然後按一下 **[備份]**。
   - 若要備份所有群組的信箱 (包括之後建立之群組的信箱)，展開 **[群組]** 節點、選取 **[所有群組]**，然後按一下 **[群組備份]**。
   - 若要備份個別的群組信箱，展開 **[群組]** 節點、選取 **[所有群組]**、選取您要備份其信箱的群組，然後按一下 **[備份]**。

復原信箱和信箱項目

復原信箱

1. 按一下 **[裝置] > [託管的 Exchange]**。
2. 如果多個託管的 Exchange 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
   - 若要復原使用者信箱，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原其信箱的使用者，然後按一下 **[復原]**。
   - 若要復原共用信箱，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原的共用信箱，然後按一下 **[復原]**。
   - 若要復原群組信箱，展開 **[群組]** 節點、選取 **[所有群組]**、選取您要復原其信箱的群組，然後按一下 **[復原]**。
   - 如果使用者、群組或共用信箱遭到刪除，請在 [備份儲存] 索引標籤的 **[雲端應用程式備份]** 區段中選取該項目，然後按一下 **[顯示備份]**。

   您可以按名稱搜尋使用者和群組。不支援萬用字元。
4. 選擇復原點
5. 按一下 **[復原] > [整個信箱]**。
6. 如果多個託管的 Exchange 組織新增到 Cyber Protection 服務，按一下 **[託管的 Exchange 組織]** 可檢視、變更或指定目標組織。

   預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
7. 在 **[復原至信箱]** 中，檢視、變更或指定目標信箱。

原始信箱預設為選取狀態。如果此信箱不存在或選取了非原始組織，則必須指定目標信箱。

8. 按一下 **[開始復原]**。
9. 選取其中一個覆寫選項：
   - **覆寫現有項目**
   - **不要覆寫現有項目**
10. 按一下 **[繼續]** 可確認您的決定。

復原信箱項目

1. 按一下 **[裝置] > [託管的 Exchange]**。
2. 如果多個託管的 Exchange 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
   - 若要從使用者信箱復原項目，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取其信箱原本包含您要復原之項目的使用者，然後按一下 **[復原]**。
   - 若要復原共用信箱中的項目，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取原本包含您要復原之項目的共用信箱，然後按一下 **[復原]**。
   - 若要從群組信箱復原項目，展開 **[群組]** 節點、選取 **[所有群組]**、選取其信箱原本包含您要復原之項目的群組，然後按一下 **[復原]**。
   - 如果使用者、群組或共用信箱遭到刪除，請在 [備份儲存] 索引標籤的 **[雲端應用程式備份]** 區段中選取該項目，然後按一下 **[顯示備份]**。

   您可以按名稱搜尋使用者和群組。不支援萬用字元。
4. 選擇復原點
5. 按一下 **[復原] > [電子郵件訊息]**。
6. 瀏覽到所需的資料夾，或使用搜尋以取得所需項目的清單。

   您可以使用下列搜尋選項。不支援萬用字元。
   - 電子郵件訊息：依主旨、寄件者、收件者、附件名稱及日期搜尋。
   - 事件：依主題及日期搜尋。
   - 工作：依主題及日期搜尋。
   - 連絡人：依姓名、電子郵件地址和電話號碼搜尋。
7. 選擇您要復原的項目。若要能夠選擇資料夾，請按一下 [復原資料夾] 圖示： 

   此外，您可以執行下列任何一項作業：
   - 選取項目後，按一下 **[顯示內容]** 可檢視其內容，包括附件。若要下載附加檔案，請按一下其名稱。
   - 選取電子郵件訊息或行事曆項目後，按一下 **[以電子郵件傳送]**，可將該項目傳送到指定的電子郵件地址。您可以選取寄件者，並撰寫要加入至轉寄項目的文字。
   - 只有在備份未經加密、使用搜尋，並在搜尋結果中選取單一項目時：按一下 **[顯示版本]** 來選取要復原的項目版本。您可以選取早於或晚於所選復原點的任何備份版本。
8. 按一下 **[復原]**。

9. 如果多個託管的 Exchange 組織新增到 Cyber Protection 服務，按一下 **[託管的 Exchange 組織]** 可檢視、變更或指定目標組織。

   預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
10. 在 **[復原至信箱]** 中，檢視、變更或指定目標信箱。

    原始信箱預設為選取狀態。如果此信箱不存在或選取了非原始組織，則必須指定目標信箱。
11. [僅在復原至使用者信箱或共用信箱時] 在 **[路徑]** 中，檢視或變更目標信箱中的目標資料夾。根據預設，已選取 **[已復原項目]** 資料夾。

    群組信箱項目一律復原至 **[收件匣]** 資料夾。
12. 按一下 **[開始復原]**。
13. 選取其中一個覆寫選項：
    - **覆寫現有項目**
    - **不要覆寫現有項目**
14. 按一下 **[繼續]** 可確認您的決定。

保護 Microsoft 365 資料

為什麼要備份 Microsoft 365 資料？

即使 Microsoft 365 是一組雲端服務，但定期備份可提供一層額外的保護，防止使用者出錯及故意的惡意操作。即使 Microsoft 365 的保留期過期後，您仍可從備份復原已刪除的項目。另外，如需遵守法規規定，您可以保留 Exchange Online 信箱的本機複本。

備份資料會自動壓縮，並且在備份位置上使用的空間比原始位置更少。雲端到雲端備份的壓縮層級是固定的，對應於非雲端到雲端備份的 **一般** 層級。有關這些層級的詳細資訊，請參閱 "壓縮層級" (第 406 頁)。

雲端代理程式和本機代理程式

Microsoft 365 工作負載可使用以下兩種代理程式：

- 雲端代理程式

  雲端代理程式提供擴充的備份功能，您可以在 Cyber Protect 主控台中直接存取該功能。不需要安裝。如需詳細資訊，請參閱 "使用雲端 Microsoft 365 用代理程式" (第 550 頁)。
- 本機代理程式

  本機代理程式僅提供 Exchange Online 信箱的備份。此代理程式必須安裝在已連線至網際網路的 Windows 電腦上。如需詳細資訊，請參閱 "使用本機安裝的 Office 365 用代理程式" (第 546 頁)。

兩種代理程式均支援 Azure 資訊保護 (AIP)。

注意事項

對於合規模式下的租用戶，僅能使用本機代理程式。這些租用戶僅能備份 Microsoft 365 信箱。他們無法使用雲端代理程式提供的擴充功能。

下表摘要說明這兩種代理程式的功能。

	本機代理程式	雲端代理程式
可以備份的資料項目	**Exchange Online:** 使用者信箱和共用信箱 (包括 Kiosk 計劃上的使用者信箱和訴訟保留信箱)	• **Exchange Online**: ◦ 使用者信箱和共用信箱 (包括 Kiosk 計劃上的使用者信箱和訴訟保留信箱) ◦ 群組信箱 ◦ 公用資料夾 • **OneDrive**: 使用者檔案和資料夾 • **SharePoint Online**: ◦ 傳統網站集合 ◦ 群組 (小組) 網站 ◦ 通訊網站 ◦ 個別資料項目 • **Microsoft 365 Teams**: ◦ 整個小組 ◦ 小組頻道 ◦ 頻道檔案 ◦ 小組信箱 ◦ 小組信箱中的檔案和電子郵件訊息 ◦ 會議 ◦ 小組網站 • **OneNote 筆記本**: 作為 OneDrive、SharePoint Online 和 Microsoft 365 Teams 備份的一部分
封存信箱備份 (**就地封存**)	否	是
備份排程	使用者定義的	每天最多六次*
備份位置	雲端儲存、本機資料夾、網路資料夾	僅限雲端儲存 (包括合作夥伴託管的儲存空間)
自動保護新的 Microsoft 365 使用者、群組、網站和小組	否	是, 透過將保護計劃套用至 **[所有使用者]**、**[所有群組]**、**[所有網站]**、**[所有小組]** 群組
保護多個 Microsoft 365 組織	否	是
精細復原	是	是
復原至相同 Microsoft 365 組織中的另一位使用者	是	是
復原至相同租用戶中的另一	否	是

	本機代理程式	雲端代理程式
個 Microsoft 365 組織		
復原至內部部署 Microsoft Exchange Server	否	否
可以備份但不會降低效能的項目數上限	備份到雲端儲存空間時：每個公司 5,000 個信箱 備份到其他目的地時：每個保護計劃 2,000 個信箱 (每個公司的信箱數量則沒有限制)	每家公司最多 50,000 個受保護的工作負載**
可執行的手動備份數目上限	否	一小時內手動執行 10 次
同時復原作業數目上限	否	10 個作業，包括 Google Workspace 復原作業

* 預設選項為**一天一次**。使用 Advanced Backup 套件，即可每天排程最多六個備份。備份會以近似間隔開始，該間隔根據目前服務資料中心內多個客戶的雲端代理程式負載而定。這能確保一天中的負載均衡，且所有客戶都獲得同等的服務品質。

注意事項

保護排程可能會受到第三方服務作業的影響，例如，Microsoft 365 伺服器的可存取性、Microsoft 伺服器的調節設定等等。另請參閱 https://docs.microsoft.com/en-us/graph/throttling。

** 工作負載的最大數目取決於工作負載類型，如下所示：50,000 個信箱或 10,000 個團隊或 10,000 個 SharePoint 網站或 5,000 個 OneDrive。

若要計算支援的組合，請使用下列公式：

```
10 mailboxes = 2 teams = 2 sites = 1 OneDrive
```

例如：

- 50,000 個信箱
- 40,000 個信箱和 1,000 個 OneDrive
- 40,000 個信箱和 2,000 個網站
- 40,000 個信箱和 2,000 個團隊
- 30,000 個信箱、1,000 個 OneDrive、1,000 個網站和 1,000 個團隊
- 30,000 個信箱、2,000 個網站和 2,000 個團隊

建議您依照下列順序逐步備份工作負載：

1. 信箱。
2. 所有信箱都備份之後，請繼續進行 OneDrives。
3. OneDrive 備份完成後，請繼續進行 Teams 備份。
4. Teams 備份完成後，請繼續進行 SharePoint 網站備份。

初次完整備份可能需要數天的時間，端視受保護項目的數目及其大小而定。

所需的使用者權限

在 Cyber Protection 中

本機代理程式必須以公司系統管理員帳戶的身分註冊，並在客戶租用戶層級使用。單位層級的公司系統管理員、單位系統管理員和使用者無法備份或復原 Microsoft 365 資料。

雲端代理程式可以同時在客戶租用戶層級和單位層級使用。如需有關這些層級及其個別系統管理員的詳細資訊，請參閱 "管理在不同層級新增的 Microsoft 365 組織" (第 551 頁)。

在 Microsoft 365 中

您的帳戶必須獲指派 Microsoft 365 中的全域系統管理員角色。

若要探索、備份和復原 Microsoft 365 公用資料夾，至少其中一個 Microsoft 365 系統管理員帳戶必須有一個信箱，而且必須有您要備份之公用資料夾的讀取/寫入權限。

- 本機代理程式會使用此帳戶登入 Microsoft 365。若要啟用代理程式存取所有信箱的內容，此帳戶便會被指派 **ApplicationImpersonation** 管理角色。如果您變更帳戶密碼，請在 Cyber Protect 主控台中更新密碼，如 "變更 Microsoft 365 存取認證" (第 548 頁) 中所述。
- 雲端代理程式無法登入 Microsoft 365。您需要以全域系統管理員的身分登入 Microsoft 365 一次，才能為雲端代理程式授予其操作所需的權限。

  Microsoft 365 中需要以下權限：
  - 登入和讀取使用者設定檔
  - 讀取和寫入所有網站集合中的檔案
  - 讀取和寫入所有使用者的完整設定檔
  - 讀取和寫入所有群組
  - 讀取目錄資料
  - 讀取所有頻道訊息
  - 讀取和寫入受管理中繼資料
  - 讀取和寫入所有網站集合中的項目和清單
  - 完全控制所有網站集合
  - 讀取和寫入所有網站集合中的項目
  - 使用可完整存取所有信箱的 Exchange Web 服務
- 雲端代理程式不會儲存您的帳戶認證，也不會將這些帳戶認證用於執行備份和復原。變更認證、停用帳戶或刪除帳戶都不會影響雲端代理程式的操作。

限制

- 透過本機代理程式，您最多可以保護 5,000 個工作負載。透過雲端代理程式，您最多可以保護 50,000 個工作負載。

- 擁有信箱或 OneDrive 的所有使用者都會顯示在 Cyber Protect 主控台，包含沒有 Microsoft 365 授權的使用者，還有遭封鎖而無法登入 Microsoft 365 服務的使用者。
- 信箱備份僅包含使用者看得到的資料夾。**[可復原的項目]** 資料夾及其子資料夾 (**[刪除]**、**[版本]**、**[清除]**、**[稽核]**、**[DiscoveryHold]**、**[行事曆記錄]**) 不包含在信箱備份中。
- 無法在復原期間自動建立使用者、公用資料夾、群組或網站。例如，如果您要復原已經刪除的 SharePoint Online 網站，請先手動建立一個新網站，然後將其指定為復原期間的目標網站。
- 即使您可以從搜尋結果中選擇這類項目，也無法同時從不同的復原點復原這些項目。
- 在備份期間，將會保留套用到內容的所有敏感度標籤。因此，如果要將敏感內容復原到非原始位置，且其使用者的存取權限不同，則可能不會顯示該內容。
- 您只能將一個個別的備份計劃套用到工作負載。
- 當單獨備份計劃和群組備份計劃套用到相同工作負載時，單獨計劃中的設定具有更高優先順序。

Microsoft 365 授權報告

公司系統管理員可以下載受保護 Microsoft 365 授權的報告。此報告採用 CSV 格式，其中包含各授權的授權狀態以及使用授權的原因等資訊。此報告也包含受保護的授權名稱、相關聯的電子郵件、群組、Microsoft 365 組織、受保護工作負載的名稱和類型。

此報告僅適用於註冊 Microsoft 365 組織所在的租用戶。

若要下載 Microsoft 365 授權報告

1. 以公司系統管理員的身分，登入 Cyber Protect 主控台。
2. 按一下右上角的帳戶圖示。
3. 按一下 **[Microsoft 365 授權報告]**。

記錄

檢視已備份電子郵件的內容、下載附件或檔案、將電子郵件復原到非原始信箱，或將其當作電子郵件傳送等使用雲端對雲端資源的動作可能會違反使用者隱私權。這些動作會記錄在管理入口網站的 **[監控]** > **[稽核記錄]** 中。

使用本機安裝的 Office 365 用代理程式

新增 Microsoft 365 組織

新增 Microsoft 365 組織

1. 以公司系統管理員的身分，登入 Cyber Protect 主控台。
2. 按一下右上角的帳戶圖示，然後按一下 **[下載]** > **[Office 365 用代理程式]**。
3. 在已連線至網際網路的 Windows 電腦上下載及安裝代理程式。
4. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[Microsoft Office 365](本機代理程式)**。
5. 在開啟的視窗中，輸入您的應用程式 ID、應用程式密碼，以及 Microsoft 365 租用戶 ID。如需有

關如何尋找這些資訊的詳細資訊，請參閱 "取得應用程式 ID 和應用程式密碼" (第 547 頁)。

6. 按一下 **[確定]**。

因此，貴組織的資料項目會出現在 Cyber Protect 主控台，位於 **[Microsoft Office 365](本機代理程式)** 索引標籤上。

重要事項
組織 (公司群組) 內只能有一個本機安裝的 Office 365 用代理程式。

取得應用程式 ID 和應用程式密碼

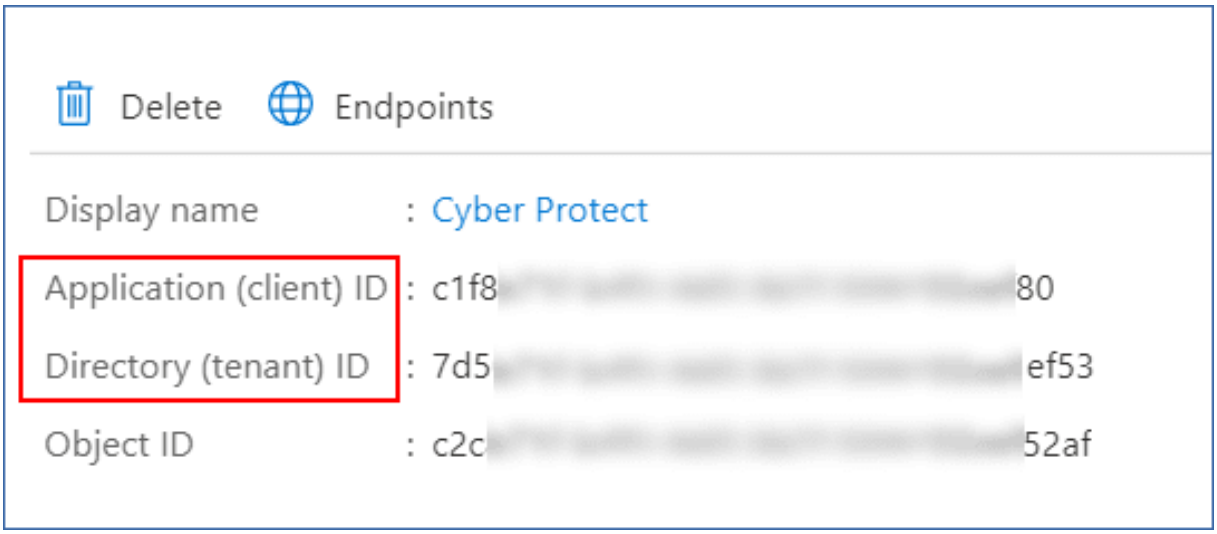
若要為 Office 365 使用新型驗證，您需要在 Entra 管理中心建立自訂應用程式，並為其授予特定的 API 權限。因此，您將取得您需要在 主控台中輸入的**應用程式 ID**、**應用程式密碼**以及**目錄 (租用戶) ID**。

注意事項
在已安裝 Office 365 用代理程式的電腦上，確認允許透過連接埠 443 存取 graph.microsoft.com。

若要在 Entra 管理中心建立應用程式

1. 以系統管理員身分，登入 Entra管理中心。
2. 瀏覽至 **[Azure Active Directory]** > **[應用程式註冊]**，然後按一下 **[新註冊]**。
3. 為您的自訂應用程式指定一個名稱，例如 Cyber Protection。
4. 在 **[支援的帳戶類型]** 中，選擇 **[僅在此組織目錄中的帳戶]**。
5. 按一下 **[註冊]**。

您的應用程式現在已經建立。在 Entra 管理中心，瀏覽至應用程式的 **[概觀]** 頁面，然後檢查您的應用程式 (用戶端) ID 與目錄 (租用戶) ID。



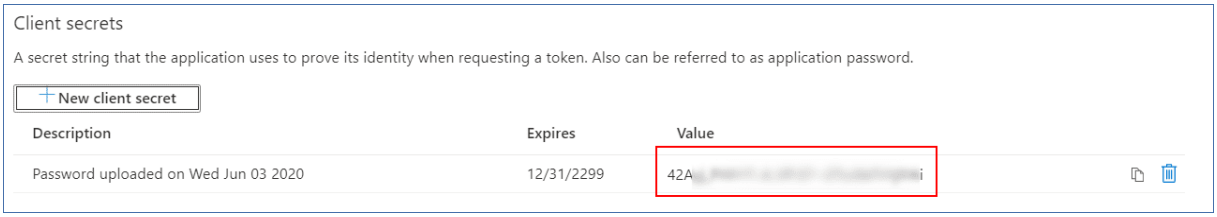
如需有關如何在 Entra 管理中心建立應用程式的詳細資訊，請參閱 Microsoft 文件。

若要為您的應用程式授予所需的 API 權限

1. 在 Entra 管理中心，瀏覽至應用程式的 **[API 權限]**，然後按一下 **[新增權限]**。
2. 選擇 **[我的組織使用的 API]** 索引標籤，然後搜尋 **Office 365 Exchange Online**。
3. 按一下 **[Office 365 Exchange Online]**，然後按一下 **[應用程式權限]**。
4. 選擇 **[full_access_as_app]** 核取方塊，然後按一下 **[新增權限]**。
5. 在 **[API 權限]** 中，按一下 **[新增權限]**。
6. 選擇 **[Microsoft Graph]**。
7. 選擇 **[應用程式權限]**。
8. 展開 **[目錄]** 索引標籤，然後選擇 **[Directory.Read.All]** 核取方塊。按一下 **[新增權限]**。
9. 核取所有權限，然後按一下 **[為 <您應用程式的名稱> 授予系統管理員同意]**。
10. 按一下 **[是]**，確認您的選擇。

若要建立應用程式密碼

1. 在 Entra 管理中心，瀏覽至您應用程式的 **[憑證和密碼]** > **[新增用戶端密碼]**。
2. 在開啟的對話方塊中，選擇 [到期日]:**[永不]**，然後按一下 **[新增]**。
3. 在 **[值]** 欄位中檢查您的應用程式密碼，然後確認您記住該密碼。



如需有關應用程式密碼的詳細資訊，請參閱 Microsoft 文件。

變更 Microsoft 365 存取認證

您可以變更 Microsoft 365 的存取認證，而無需重新安裝代理程式。

變更 Microsoft 365 存取認證

1. 按一下 **[裝置]** > **[Microsoft Office 365 (本機代理程式)]**。
2. 選擇 Microsoft 365 組織。
3. 按一下 **[指定認證]**。
4. 輸入您的應用程式 ID、應用程式密碼，以及 Microsoft 365 租用戶 ID。如需有關如何尋找這些資訊的詳細資訊，請參閱 "取得應用程式 ID 和應用程式密碼" (第 547 頁)。
5. 按一下 **[確定]**。

保護 Exchange Online 信箱

哪些項目可以備份？

您可以備份使用者信箱和共用信箱。群組信箱和封存信箱 **(就地封存)** 無法進行備份。

可以復原哪些項目？

下列項目可以從信箱備份復原：

- 信箱
- 電子郵件資料夾
- 電子郵件訊息
- 行事曆事件
- 工作
- 連絡人
- 日誌項目
- 記事

您可以使用搜尋找出各項目。

將信箱復原至現有的信箱時，系統會覆寫 ID 相符的現有項目。

信箱項目復原不會造成任何覆寫。而是會在目標資料夾中重新建立信箱項目的完整路徑。

選擇 Microsoft 365 信箱

如下所述選擇信箱，然後視需要指定保護計劃的其他設定。

選取信箱

1. 按一下 **[Microsoft Office 365 (本機代理程式)]**。
2. 選擇您要備份的信箱。
3. 按一下 **[備份]**。

復原信箱和信箱項目

復原信箱

1. 按一下 **[Microsoft Office 365 (本機代理程式)]**。
2. 選擇要復原的信箱，然後按一下**[復原]**。
   您可以按名稱搜尋信箱。不支援萬用字元。
   如果信箱遭到刪除，在 [備份儲存] 索引標籤中選擇此信箱，然後按一下 **[顯示備份]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。
4. 請按一下**[復原]** > **[信箱]**。
5. **[目標信箱]** 可以檢視、變更或指定目標信箱。
   原始信箱預設為選取狀態。如果此信箱不存在，則必須指定目標信箱。
6. 按一下 **[開始復原]**。

復原信箱項目

1. 按一下 **[Microsoft Office 365 (本機代理程式)]**。
2. 按一下最初具有您想要復原之項目的信箱，然後按一下**[復原]**。
   您可以按名稱搜尋信箱。不支援萬用字元。
   如果信箱遭到刪除，在 [備份儲存] 索引標籤中選擇此信箱，然後按一下 **[顯示備份]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。

4. 按一下**[復原]** > **[電子郵件訊息]**。
5. 選擇您要復原的項目。

   您可以選取下列搜尋選項。不支援萬用字元。

   - 電子郵件訊息：依主旨、寄件者、收件者、附件名稱及日期搜尋。
   - 事件：依主題及日期搜尋。
   - 工作：依主題及日期搜尋。
   - 連絡人：依姓名、電子郵件地址和電話號碼搜尋。

   選擇了電子郵件訊息後，按一下 **[顯示內容]** 以檢視其內容和附件。

   注意事項
   要下載附加檔案，請按一下名稱。

   選擇電子郵件訊息後，您可按一下**[以電子郵件傳送]**，向電子郵件地址傳送訊息。訊息便會從您的管理員帳戶的電子郵件地址傳送。

   若要能夠選擇資料夾，請按一下 [復原資料夾] 圖示： 
6. 按一下 **[復原]**。
7. **[目標信箱]** 可以檢視、變更或指定目標信箱。

   原始信箱預設為選取狀態。如果此信箱不存在，則必須指定目標信箱。
8. 按一下 **[開始復原]**。
9. 確認選項無誤。

信箱項目必定復原至目標信箱中的 **[已復原項目]** 資料夾。

使用雲端 Microsoft 365 用代理程式

新增 Microsoft 365 組織

系統管理員可以將一或多個 Microsoft 365 組織新增到客戶租用戶或單位。

公司系統管理員可將組織新增至客戶租用戶。單位系統管理員和單位層級的客戶系統管理員可將組織新增至單位。

新增 Microsoft 365 組織

1. 根據您需要新增組織之處，以公司系統管理員或單位系統管理員的身分，登入 Cyber Protect 主控台。
2. [適用於單位層級的公司系統管理員] 在管理入口網站中，瀏覽至所需的單位。
3. 按一下 **[裝置]** > **[新增]** > **[Microsoft 365 商務版]**。

   此軟體會將您重新導向至 Microsoft 365 登入頁面。
4. 使用 Microsoft 365 全域系統管理員認證登入。

   Microsoft 365 會顯示備份和復原貴組織資料所需權限的清單。
5. 確認您為 Cyber Protection 服務授予這些權限。

結果，您的 Microsoft 365 組織出現在 主控台的 **[裝置]** 索引標籤底下。

有用的提示

- 雲端代理程式從組織新增至 Cyber Protection 服務開始，每 24 小時會與 Microsoft 365 同步一次。如果您新增或移除使用者、群組或網站，將不會在 Cyber Protect 主控台中立即看到這個變更。若要立即同步變更，請在 **[Microsoft 365]** 頁面上選取組織，然後按一下 **[重新整理]**。
  如需有關同步 Microsoft 365 組織和 Cyber Protect 主控台資源的詳細資訊，請參閱 "探索 Microsoft 365 資源" (第 552 頁)。
- 如果您已經將保護計劃套用到 **[所有使用者]**、**[所有群組]** 或 **[所有網站]** 群組，則只有在同步後，新增的項目才會包含在備份中。
- 根據 Microsoft 原則，當使用者、群組或網站從 Microsoft 365 圖形化使用者介面移除之後，仍然可以透過 API 使用幾天。在這段時間內，已移除的項目在 Cyber Protect 主控台中為非作用中 (呈灰色) 狀態，而且將不會進行備份。當已移除的項目變成無法透過 API 使用時，就會從 Cyber Protect 主控台中消失。其備份 (如果有的話) 可以在 **[備份儲存]** > **[雲端應用程式備份]** 中找到。

管理在不同層級新增的 Microsoft 365 組織

公司系統管理員對於新增至客戶租用戶層級的 Microsoft 365 組織，擁有完整的存取權。

公司系統管理員對於新增至單位的組織，擁有限制的存取權。在這些組織 (以括號中的單位名稱顯示) 中，公司系統管理員可以執行下列操作：

- 從備份中復原資料。
  公司系統管理員可以將資料復原到租用戶中的所有組織 (無論在哪個層級新增這些組織)。
- 瀏覽備份中的備份與復原點。
- 刪除備份中的備份與復原點。
- 檢視警示與活動。

客戶租用戶層級的公司系統管理員無法執行下列操作：

- 將 Microsoft 365 組織新增至單位。
- 從單位刪除 Microsoft 365 組織。
- 同步新增至單位的 Microsoft 365 組織。
- 在新增至單位的 Microsoft 365 組織中，檢視、建立、編輯、刪除、套用、執行或撤銷資料項目的保護計劃。

單位系統管理員和單位層級的公司系統管理員對於新增至單位的組織，擁有完整的存取權。但是，他們無法存取父客戶租用戶中的任何資源，包括在其中建立的保護計劃。

刪除 Microsoft 365 組織

刪除 Microsoft 365 組織不會影響此組織資料的現有備份。如果您不再需要這些備份，請先刪除它們，然後再刪除 Microsoft 365 組織。否則，備份仍將使用可能會計費的雲端儲存空間。

如需有關如何刪除備份的詳細資訊，請參閱 "若要刪除備份或備份存檔" (第 474 頁)。

刪除 Microsoft 365 組織

1. 根據新增組織所在位置，以公司系統管理員或單位系統管理員的身分，登入 Cyber Protect 主控台。
2. [適用於單位層級的公司系統管理員] 在管理入口網站中，瀏覽至所需的單位。
3. 前往 **[裝置]** > **[Microsoft 365]**。
4. 選擇組織，然後按一下 **[刪除群組]**。

結果，套用至此群組的備份計劃將會遭到撤銷。

但是，您還應該手動撤銷 Backup Service 應用程式對 Microsoft 365 組織資料的存取權限。

若要撤銷存取權限

1. 以全域系統管理員的身分登入 Microsoft 365。
2. 前往 **[系統管理中心]** > **[Azure Active Directory]** > **[企業應用程式]** > **[所有應用程式]**。
3. 選擇 **[Backup Service]** 應用程式並向下鑽研。
4. 前往 **[屬性]** 索引標籤，然後按一下動作面板上的 **[刪除]**。
5. 確認刪除作業。

結果，Microsoft 365 組織資料的存取權限將從 Backup Service 應用程式撤銷。

探索 Microsoft 365 資源

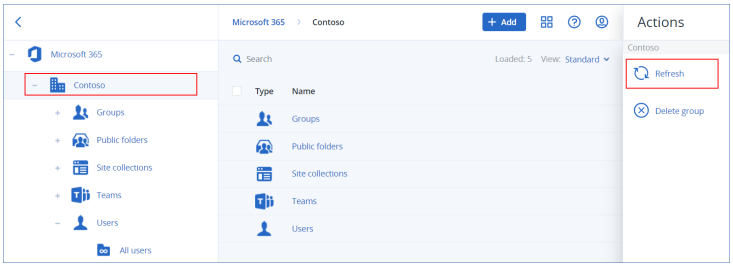
當您將 Microsoft 365 組織新增至 Cyber Protection 服務時，此組織中的資源 (例如信箱、OneDrive 儲存空間、Microsoft Teams 和 SharePoint 網站) 會同步到 Cyber Protect 主控台中。此作業稱為探索，且其記錄在 **[監控]** > **[活動]** 中。

探索作業完成後，您可以在 主控台的 **[裝置]** > **[Microsoft 365]** 索引標籤上，查看 Microsoft 365 組織的資源，而且您可以在其中套用備份計劃。

自動探索作業會每天執行一次，以便在 Cyber Protect 主控台中保留最新的資源清單。您也可以視需要，透過手動重新執行探索作業來同步此清單。

若要手動執行探索作業

1. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[Microsoft 365]**。
2. 選擇您的 Microsoft 365 組織，然後在 **[動作]** 窗格中，按一下 **[重新整理]**。



注意事項

每小時可以手動執行探索作業高達 10 次。達到此次數後，允許的執行會重設為每小時一次，然後每小時可以額外執行一次，直到再次達到每小時總共執行 10 次為止。

設定 Microsoft 365 備份的頻率

依預設值，Microsoft 365 備份每天會執行一次，且無法使用其他排程選項。

如果租用戶中啟用了 Advanced Backup 套件，您就能更頻繁設定備份。您可以選擇每天備份數，但無法設定備份開始時間。備份會以近似間隔自動開始，該間隔根據目前服務資料中心內多個客戶的雲端代理程式負載而定。這能確保一天中的負載均衡，且所有客戶都獲得同等的服務品質。

您可以調整下列選項。

排程選項	每次備份間的近似間隔
一天一次	24 小時
一天兩次 (預設)	12 小時
一天 3 次	8 小時
一天 6 次	4 小時

注意事項

依雲端代理程式以及 Microsoft 365 可能的調節而定，備份可能會比排程還晚執行，或需要更長時間才能完成。如果備份比兩次備份平均間隔還長，將重新排定下次備份，這可能導致每天備份數比所選次數還少。例如，就算選擇每天六次，每天也可能只能完成兩次備份。

一天只能執行一次群組信箱備份。

保護 Exchange Online 資料

哪些項目可以備份？

您可以備份使用者信箱、共用信箱和群組信箱。或者，您可以選擇備份所選信箱的線上封存信箱 (**就地封存**)。

從 Cyber Protection 服務 8.0 版開始，您可以備份公用資料夾。如果貴組織在 8.0 版發行前新增至 Cyber Protection 服務，您需要重新新增組織以取得此功能。請不要刪除組織，只要重複 "新增 Microsoft 365 組織" (第 550 頁) 中所述的步驟即可。因此，Cyber Protection 服務會取得使用對應 API 的權限。

可以復原哪些項目？

下列項目可以從信箱備份復原：

- 信箱
- 電子郵件資料夾
- 電子郵件訊息
- 行事曆事件
- 工作

- 連絡人
- 日誌項目
- 記事

下列項目可以從公用資料夾備份復原：

- 子資料夾
- 貼文
- 電子郵件訊息

您可以使用搜尋找出這些項目。

復原信箱、信箱項目、公用資料夾和公用資料夾項目時，您可以選擇是否要覆寫目標位置中的項目。

選取信箱

如下所述選擇信箱，然後視需要指定保護計劃的其他設定。

若要選取 Exchange Online 信箱

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選取您要備份其使用者資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
   - 若要備份所有使用者信箱和所有共用信箱 (包括之後建立的信箱)，展開 **[使用者]** 節點、選取 **[所有使用者]**，然後按一下 **[群組備份]**。
   - 若要備份個別的使用者信箱或共用信箱，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要備份其信箱的使用者，然後按一下 **[備份]**。
   - 若要備份所有群組的信箱 (包括之後建立之群組的信箱)，展開 **[群組]** 節點、選取 **[所有群組]**，然後按一下 **[群組備份]**。
   - 若要備份個別的群組信箱，展開 **[群組]** 節點、選取 **[所有群組]**、選取您要備份其信箱的群組，然後按一下 **[備份]**。

     注意事項
     雲端 Microsoft 365 用代理程式使用具有適當權限的帳戶存取群組信箱。因此，若要備份群組信箱，至少要有其中一個群組擁有者必須是擁有信箱的獲授權 Microsoft 365 使用者。如果是私有群組或擁有隱藏會員資格的群組，則擁有者必須也是群組成員。

4. 在保護計劃面板上：
   - 請確認在 **[要備份的內容]** 中已選擇 **[Microsoft 365 信箱]** 項目。
     如果部分個別選擇的使用者沒有在其 Microsoft 365 計劃中包含 Exchange 服務，您將無法選擇此選項。
     如果部分針對群組備份選擇的使用者沒有在其 Microsoft 365 計劃中包含 Exchange 服務，您將可以選擇此選項，但是保護計劃將不會套用到這些使用者。
   - 如果您不想要備份封存信箱，停用 **[封存信箱]** 開關。

選擇公用資料夾

如下所述選擇公用資料夾，然後視需要指定保護計劃的其他設定。

注意事項
公用資料夾會耗用 Microsoft 365 授權的備份配額中的授權。

若要選取 Exchange Online 公用資料夾

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請展開您要備份其資料的組織。否則，請跳過此步驟。
3. 展開 **[公用資料夾]** 節點，然後選取 **[所有公用資料夾]**。
4. 執行下列其中一項操作：
   - 若要備份所有公用資料夾 (包括之後建立的公用資料夾)，請按一下 **[群組備份]**。
   - 若要備份個別的公用資料夾，選取您要備份的公用資料夾，然後按一下 **[備份]**。
5. 在保護計劃面板上，請確認在 **[要備份的內容]** 中已選擇 **[Microsoft 365 信箱]** 項目。

復原信箱和信箱項目

復原信箱

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
   - 若要復原使用者信箱，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原其信箱的使用者，然後按一下 **[復原]**。
   - 若要復原共用信箱，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原的共用信箱，然後按一下 **[復原]**。
   - 若要復原群組信箱，展開 **[群組]** 節點、選取 **[所有群組]**、選取您要復原其信箱的群組，然後按一下 **[復原]**。
   - 如果使用者、群組或共用信箱遭到刪除，請在 [備份儲存] 索引標籤的 **[雲端應用程式備份]** 區段中選取該項目，然後按一下 **[顯示備份]**。

   您可以按名稱搜尋使用者和群組。不支援萬用字元。
4. 選擇復原點

   注意事項
   若只要查看含有信箱的復原點，請在 **[依內容篩選]** 中選取 **[信箱]**。

5. 按一下 **[復原]** > **[整個信箱]**。
6. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。

預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。

7. 在 **[復原至信箱]** 中，檢視、變更或指定目標信箱。

   原始信箱預設為選取狀態。如果此信箱不存在或選取了非原始組織，則必須指定目標信箱。

   您無法在復原期間建立新的目標信箱。若要將信箱復原為新的信箱，首先需要在 Microsoft 365 組織中建立目標信箱，然後讓雲端代理程式同步變更。雲端代理程式每 24 小時自動與 Microsoft 365 同步一次。若要立即同步變更，請在 Cyber Protect 主控台中，選擇 **[Microsoft 365]** 頁面上的組織，然後按一下 **[重新整理]**。
8. 按一下 **[開始復原]**。
9. 選取其中一個覆寫選項：
   - **覆寫現有項目**
   - **不要覆寫現有項目**
10. 按一下 **[繼續]** 可確認您的決定。

復原信箱項目

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
   - 若要從使用者信箱復原項目，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取其信箱原本包含您要復原之項目的使用者，然後按一下 **[復原]**。
   - 若要復原共用信箱中的項目，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取原本包含您要復原之項目的共用信箱，然後按一下 **[復原]**。
   - 若要從群組信箱復原項目，展開 **[群組]** 節點、選取 **[所有群組]**、選取其信箱原本包含您要復原之項目的群組，然後按一下 **[復原]**。
   - 如果使用者、群組或共用信箱遭到刪除，請在 [備份儲存] 索引標籤的 **[雲端應用程式備份]** 區段中選取該項目，然後按一下 **[顯示備份]**。

   您可以按名稱搜尋使用者和群組。不支援萬用字元。
4. 選擇復原點

   注意事項
   若只要查看含有信箱的復原點，請在 **[依內容篩選]** 中選取 **[信箱]**。
5. 按一下 **[復原]** > **[電子郵件訊息]**。
6. 瀏覽到所需的資料夾，或使用搜尋以取得所需項目的清單。

   您可以使用下列搜尋選項。不支援萬用字元。
   - 電子郵件訊息：依主旨、寄件者、收件者、附件名稱及日期搜尋。您可以選擇開始日期或結束日期 (包括兩者)，或同時選擇兩者以便在某個時間範圍內進行搜尋。
   - 事件：依主題及日期搜尋。
   - 工作：依主題及日期搜尋。
   - 連絡人：依姓名、電子郵件地址和電話號碼搜尋。

7. 選擇您要復原的項目。若要能夠選擇資料夾，請按一下 [復原資料夾] 圖示： 

   您無法在復原期間建立新的目標信箱。若要將新的信箱項目復原為新的信箱，首先需要在 Microsoft 365 組織中建立新的目標信箱，然後讓雲端代理程式同步變更。雲端代理程式每 24 小時自動與 Microsoft 365 同步一次。若要立即同步變更，請在 Cyber Protect 主控台中，選擇 **[Microsoft 365]** 頁面上的組織，然後按一下 **[重新整理]**。

   此外，您可以執行下列任何一項作業：

   - 選取項目後，按一下 **[顯示內容]** 可檢視其內容，包括附件。若要下載附加檔案，請按一下其名稱。
   - 選取電子郵件訊息或行事曆項目後，按一下 **[以電子郵件傳送]**，可將該項目傳送到指定的電子郵件地址。您可以選取寄件者，並撰寫要加入至轉寄項目的文字。
   - 只有在備份未經加密、使用搜尋，並在搜尋結果中選取單一項目時：按一下 **[顯示版本]** 來選取要復原的項目版本。您可以選取早於或晚於所選復原點的任何備份版本。
8. 按一下 **[復原]**。
9. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。

   預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
10. 在 **[復原至信箱]** 中，檢視、變更或指定目標信箱。

    原始信箱預設為選取狀態。如果此信箱不存在或選取了非原始組織，則必須指定目標信箱。
11. [僅在復原至使用者信箱或共用信箱時] 在 **[路徑]** 中，檢視或變更目標信箱中的目標資料夾。根據預設，已選取 **[已復原項目]** 資料夾。

    群組信箱項目一律復原至 **[收件匣]** 資料夾。
12. 按一下 **[開始復原]**。
13. 選取其中一個覆寫選項：
    - **覆寫現有項目**
    - **不要覆寫現有項目**
14. 按一下 **[繼續]** 可確認您的決定。

將整個信箱復原到 PST 資料檔案

注意事項

您可以使用 **[復原] > [電子郵件訊息]** 選項，將就地封存中的電子郵件或資料夾復原為個別的信箱項目。如需詳細資訊，請參閱 "復原信箱項目" (第 556 頁)。當您使用 **[復原] > [整個信箱]** 或 **[復原] > [為 PST 檔案]** 選項時，不會復原就地封存。

復原信箱

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：

- 若要將使用者信箱復原至 PST 資料檔案，請展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原的信箱，然後按一下 **[復原]**。
- 若要將共用信箱復原至 PST 資料檔案，請展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原的信箱，然後按一下 **[復原]**。
- 若要將群組信箱復原至 PST 資料檔案，請展開 **[群組]** 節點、選取 **[所有群組]**、選取您要復原信箱的群組，然後按一下 **[復原]**。

您可以按名稱搜尋使用者和群組。不支援萬用字元。

如果使用者、群組或共用的 Outlook 資料檔案被刪除，請在 [備份儲存空間] 索引標籤的 **[雲端應用程式備份]** 區段選取項目，然後按一下 **[顯示備份]**。

4. 按一下 **[復原]** > **[為 PST 檔案]**。
5. 設定密碼使用 PST 檔案加密存檔。

   密碼必須至少包含一個符號。
6. 確認密碼，然後按一下 **[完成]**。
7. 選定的信箱項目將復原為 PST 資料檔並以 ZIP 格式存檔。PST 檔案的最大限制為 2 GB，因此，如果要復原的資料超過 2 GB，將被拆分成多個 PST 檔案。ZIP 存檔將使用您設定的密碼進行保護。
8. 您將收到一封電子郵件，其中的連結指向 ZIP 存檔，並包含建立的 PST 檔案。
9. 系統管理員將收到您已執行復原程式的電子郵件通知。

注意事項

信箱復原至 PST 檔案可能很花時間，因為這不只包含資料傳輸，還包含使用複雜演算法將資料轉換。

使用 PST 檔案下載存檔並完全復原

1. 執行下列其中一項操作：
   - 若要從電子郵件下載存檔，請依照 **[下載檔案]** 連結進行。

     存檔將保留 96 小時。若要在 96 小時期限後下載存檔，請重複復原程序。
   - 從 Cyber Protect 主控台下載存檔：
     a. 前往 **[備份儲存]** > **[PST 檔案]**。
     b. 選擇最新醒目提示的存檔。
     c. 在右窗格按一下 **[下載]**。

   存檔將下載到您電腦的預設下載目錄。
2. 使用您設定適合加密存檔的密碼從存檔提取 PST 檔案。
3. 使用 Microsoft Outlook 開啟 PST 檔案。

   產生的 PST 檔案的大小可能比原始信箱小得多。這是正常的。

   重要事項

   請不要使用 **[匯入和匯出精靈]**，將這些檔案匯入至 Microsoft Outlook。

   若要開啟這些檔案，請按兩下這些檔案，或以滑鼠右鍵按一下這些檔案，然後在內容功能表中，選取 **[開啟方式...]** > **[Microsoft Outlook]**。

復原信箱項目到 PST 檔案

注意事項

您可以使用 **[復原] > [電子郵件訊息]** 選項，將就地封存中的電子郵件或資料夾復原為個別的信箱項目。如需詳細資訊，請參閱 "復原信箱項目" (第 556 頁)。當您使用 **[復原] > [整個信箱]** 或 **[復原] > [為 PST 檔案]** 選項時，不會復原就地封存。

復原信箱項目

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
   - 若要從使用者信箱復原項目，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取其信箱原本包含您要復原之項目的使用者，然後按一下 **[復原]**。
   - 若要復原共用信箱中的項目，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取原本包含您要復原之項目的共用信箱，然後按一下 **[復原]**。
   - 若要從群組信箱復原項目，展開 **[群組]** 節點、選取 **[所有群組]**、選取其信箱原本包含您要復原之項目的群組，然後按一下 **[復原]**。
   - 如果使用者、群組或共用信箱遭到刪除，請在 [備份儲存] 索引標籤的 **[雲端應用程式備份]** 區段中選取該項目，然後按一下 **[顯示備份]**。

   您可以按名稱搜尋使用者和群組。不支援萬用字元。
4. 按一下 **[復原] > [電子郵件訊息]**。
5. 瀏覽到所需的資料夾，或使用搜尋以取得所需項目的清單。

   您可以使用下列搜尋選項。不支援萬用字元。
   - 電子郵件訊息：依主旨、寄件者、收件者、附件名稱及日期搜尋。
   - 事件：依主題及日期搜尋。
   - 工作：依主題及日期搜尋。
   - 連絡人：依姓名、電子郵件地址和電話號碼搜尋。
6. 選擇您要復原的項目。若要能夠選擇資料夾，請按一下 [復原資料夾] 圖示： 

   此外，您可以執行下列任何一項作業：
   - 選取項目後，按一下 **[顯示內容]** 可檢視其內容，包括附件。若要下載附加檔案，請按一下其名稱。
   - 選取電子郵件訊息或行事曆項目後，按一下 **[以電子郵件傳送]**，可將該項目傳送到指定的電子郵件地址。您可以選取寄件者，並撰寫要加入至轉寄項目的文字。
   - 只有在備份未經加密、使用搜尋，並在搜尋結果中選取單一項目時：按一下 **[顯示版本]** 來選取要復原的項目版本。您可以選取早於或晚於所選復原點的任何備份版本。
7. 按一下 **[復原 PST 檔案]**。
8. 設定密碼使用 PST 檔案加密存檔。

密碼應包含至少一個符號。

9. 確認密碼，然後按一下 **[完成]**。

選定的信箱項目將復原為 PST 資料檔並以 ZIP 格式存檔。PST 檔案的最大限制為 2 GB，因此，如果要復原的資料超過 2 GB，將被拆分成多個 PST 檔案。ZIP 存檔將使用您設定的密碼進行保護。

您將收到一封電子郵件，其中的連結指向 ZIP 存檔，其中包含建立的 PST 檔案。

系統管理員將收到您已執行復原程式的電子郵件通知。

使用 PST 檔案下載存檔並完全復原

1. 執行下列其中一項操作：
   - 若要從電子郵件下載存檔，請依照 **[下載檔案]** 連結進行。
     存檔將保留 96 小時。若要在 96 小時期限後下載存檔，請重複復原程序。
   - 從 Cyber Protect 主控台下載存檔：
     a. 前往 **[備份儲存]** > **[PST 檔案]**。
     b. 選擇最新醒目提示的存檔。
     c. 在右窗格按一下 **[下載]**。

   存檔將下載到您電腦的預設下載目錄。
2. 使用您設定適合加密存檔的密碼從存檔提取 PST 檔案。
3. 使用 Microsoft Outlook 開啟 PST 檔案。
   產生的 PST 檔案的大小可能比原始信箱小得多。這是正常的。

重要事項
請不要使用 **[匯入和匯出精靈]**，將這些檔案匯入至 Microsoft Outlook。
若要開啟這些檔案，請按兩下這些檔案，或以滑鼠右鍵按一下這些檔案，然後在內容功能表中，選取 **[開啟方式...]** > **[Microsoft Outlook]**。

復原公用資料夾和資料夾項目

若要復原公用資料夾或公用資料夾項目，目標 Microsoft 365 組織至少有一個系統管理員必須擁有目標公用資料夾的 **[擁有者]** 權限。如果復原失敗並出現拒絕存取的錯誤，請在目標資料夾內容中指派這些權限、在 Cyber Protect 主控台中選擇目標組織、按一下 **[重新整理]**，然後重複復原。

若要復原公用資料夾或資料夾項目

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請展開您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
   - 展開 **[公用資料夾]** 節點、選取 **[所有公用資料夾]**、選取您要復原的公用資料夾或原本包含您要復原之項目的公用資料夾，然後按一下 **[復原]**。
   - 如果公用資料夾遭到刪除，請在 [備份儲存] 索引標籤的 **[雲端應用程式備份]** 區段中選取該公用資料夾，然後按一下 **[顯示備份]**。

   您可以按名稱搜尋公用資料夾。不支援萬用字元。

4. 選擇復原點
5. 按一下 **[復原資料]**。
6. 瀏覽到所需的資料夾，或使用搜尋以取得所需項目的清單。
   您可以依主旨、寄件者、收件者及日期搜尋電子郵件訊息和貼文。不支援萬用字元。
7. 選擇您要復原的項目。若要能夠選擇資料夾，請按一下 [復原資料夾] 圖示： 
   此外，您可以執行下列任何一項作業：
   - 選取電子郵件訊息或貼文後，按一下 **[顯示內容]** 可檢視其內容，包括附件。若要下載附加檔案，請按一下其名稱。
   - 選取電子郵件訊息或貼文後，按一下 **[以電子郵件傳送]**，可將該項目傳送到指定的電子郵件地址。您可以選取寄件者，並撰寫要加入至轉寄項目的文字。
   - 只有在備份未經加密、使用搜尋，並在搜尋結果中選取單一項目時：按一下 **[顯示版本]** 來選取要復原的項目版本。您可以選取早於或晚於所選復原點的任何備份版本。
8. 按一下 **[復原]**。
9. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。
   預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
10. 在 **[復原至公用資料夾]** 中，檢視、變更或指定目標公用資料夾。
    原始資料夾根據預設已經選取。如果此資料夾不存在或選取了非原始組織，則必須指定目標資料夾。
    您無法在復原期間建立新的公用資料夾。若要將公用資料夾復原為新的公用資料夾，首先需要在所需的 Microsoft 365 組織中建立目標公用資料夾，然後讓雲端代理程式同步變更。雲端代理程式每 24 小時自動與 Microsoft 365 同步一次。若要立即同步變更，請在 Cyber Protect 主控台中，選擇 **[Microsoft 365]** 頁面上的組織，然後按一下 **[重新整理]**。
11. 在 **[路徑]** 中，檢視或變更目標公用資料夾中的目標子資料夾。預設將會重新建立原始路徑。
12. 按一下 **[開始復原]**。
13. 選取其中一個覆寫選項：

選項	描述
覆寫現有項目	目的地位置中的所有現有檔案都會遭到覆寫。
不要覆寫現有項目	如果目的地位置中包含相同名稱的檔案，該檔案不會遭到覆寫，而且來源檔案不會儲存到目的地位置。

14. 按一下 **[繼續]** 可確認您的決定。

保護 OneDrive 檔案

哪些項目可以備份？

您可以備份整個 OneDrive 或個別的檔案和資料夾。

備份計劃的個別選項可啟用 OneNote 筆記本的備份。

檔案會與其共用權限一起備份。進階權限層級 (**[設計]**、**[完整]**、**[提供]**) 不會進行備份。

有些檔案可能含有機密資訊，而且 Microsoft 365 中的資料洩漏防禦 (DLP) 規則可能會封鎖對它們的存取。這些檔案未備份，而且備份作業完成後也不會顯示任何警告。

限制

共用信箱不支援備份 OneDrive 內容。若要備份此內容，請將共用信箱轉換為一般使用者帳戶，並確認已針對該帳戶啟用 OneDrive。

可以復原哪些項目？

您可以復原整個 OneDrive 或已備份的任何檔案或資料夾。

您可以使用搜尋找出這些項目。

您可以選擇要復原共用權限，還是讓檔案繼承復原目標資料夾的權限。

檔案與資料夾的共用連結不會復原。

選取 OneDrive 檔案

如下所述選擇檔案，然後視需要指定保護計劃的其他設定。

若要選取 OneDrive 檔案

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選取您要備份其使用者資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
   - 若要備份所有使用者 (包括之後建立的使用者) 的檔案，展開 **[使用者]** 節點、選取 **[所有使用者]**，然後按一下 **[群組備份]**。
   - 若要備份個別使用者的檔案，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要備份其檔案的使用者，然後按一下 **[備份]**。
4. 在保護計劃面板上：
   - 確認在 **[要備份的內容]** 中，選擇 **[OneDrive]** 項目。

     如果部分個別選擇的使用者沒有在其 Microsoft 365 計劃中包含 OneDrive 服務，您將無法選擇此選項。

     如果部分針對群組備份選擇的使用者沒有在其 Microsoft 365 計劃中包含 OneDrive 服務，您將可以選擇此選項，但是保護計劃將不會套用到這些使用者。
   - 在 **[要備份的項目]** 中，執行下列其中一項操作：
     - 保留預設設定 **[全部]** (所有檔案)。
     - 新增檔案和資料夾的名稱或路徑來指定要備份的檔案和資料夾。

       您可以使用萬用字元 (*、** 和 ?)。如需有關指定路徑和使用萬用字元的詳細資訊，請參閱「檔案篩選器」。
     - 瀏覽來指定要備份的檔案和資料夾。

       只有在建立單一使用者的保護計劃時，才可以使用 **[瀏覽]** 連結。

- [選用] 在 **[要備份的項目]** 中，按一下 **[顯示排除項目]** 來指定要在備份期間略過的檔案和資料夾。

  檔案排除項目會覆寫檔案選項，亦即，如果您在兩個欄位中指定相同的檔案，將會在備份期間略過這個檔案。
- [選用] 若要備份 OneNote 筆記本，請啟用 **[包括 OneNote]** 開關。

復原 OneDrive 和 OneDrive 檔案

復原整個 OneDrive

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原其 OneDrive 的使用者，然後按一下 **[復原]**。

   如果使用者遭到刪除，請在 [備份儲存] 索引標籤的 **[雲端應用程式備份]** 區段中選取該使用者，然後按一下 **[顯示備份]**。

   您可以按名稱搜尋使用者。不支援萬用字元。
4. 選擇復原點

   注意事項

   若只要查看含有 OneDrive 檔案的復原點，請在 **[依內容篩選]** 中選取 **[OneDrive]**。
5. 按一下 **[復原]** > **[整個 OneDrive]**。
6. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。

   預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。

   您無法在復原期間建立新的 OneDrive 目標。若要將 OneDrive 復原為新的 OneDrive，首先需要在 Microsoft 365 組織中建立目標 OneDrive，然後讓雲端代理程式同步變更。雲端代理程式每 24 小時自動與 Microsoft 365 同步一次。若要立即同步變更，請在 Cyber Protect 主控台中，選擇 **[Microsoft 365]** 頁面上的組織，然後按一下 **[重新整理]**。
7. 在 **[復原至磁碟機]** 中，檢視、變更或指定目標使用者。

   預設會選取原始使用者。如果此使用者不存在或選取了非原始組織，則必須指定目標使用者。
8. 選取是否要復原檔案的共用權限。
9. 按一下 **[開始復原]**。
10. 選取其中一個覆寫選項：

選項	描述
如果較舊，請覆寫現有的檔案	如果在目的地位置有一個具有相同名稱的檔案，且其比來源檔案還舊，則會將來源檔案儲存在目的地位置，取代較舊的版本。
覆寫現有的檔案	無論上次修改日期為何，目的地位置中的所有現有檔案都會遭到覆寫。

選項	描述
不要覆寫現有檔案	如果目的地位置中包含具有相同名稱的檔案，則不會對其套用任何變更，而且來源檔案不會儲存到目的地位置。

注意事項
當您復原 OneNote 筆記本時，**[如果檔案較舊請覆寫現有檔案]** 以及 **[覆寫現有檔案]** 都將導致現有的 OneNote 筆記本遭覆寫。

11. 按一下 **[繼續]** 可確認您的決定。

復原 OneDrive 檔案

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原其 OneDrive 檔案的使用者，然後按一下 **[復原]**。
   如果使用者遭到刪除，請在 [備份儲存] 索引標籤的 **[雲端應用程式備份]** 區段中選取該使用者，然後按一下 **[顯示備份]**。
   您可以按名稱搜尋使用者。不支援萬用字元。
4. 選擇復原點

注意事項
若只要查看含有 OneDrive 檔案的復原點，請在 **[依內容篩選]** 中選取 **[OneDrive]**。

5. 按一下 **[復原]** > **[檔案/資料夾]**。
6. 瀏覽至所需的資料夾，或使用搜尋以取得所需檔案和資料夾的清單。
7. 選擇您要復原的檔案。
   如果備份未經加密而且您選擇單一檔案，您可以按一下 **[顯示版本]** 來選取要復原的檔案版本。您可以選取早於或晚於所選復原點的任何備份版本。
8. 如果您要下載檔案，請選擇該檔案，按一下 **[下載]**，選擇儲存資料的位置，然後按一下 **[儲存]**。否則，請跳過此步驟。
9. 按一下 **[復原]**。
10. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。
    預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
    您無法在復原期間建立新的 OneDrive。若要將檔案復原為新的 OneDrive，首先需要在所需的 Microsoft 365 組織中建立目標 OneDrive，然後讓雲端代理程式同步變更。雲端代理程式每 24 小時自動與 Microsoft 365 同步一次。若要立即同步變更，請在 Cyber Protect 主控台中，選擇 **[Microsoft 365]** 頁面上的組織，然後按一下 **[重新整理]**。
11. 在 **[復原至磁碟機]** 中，檢視、變更或指定目標使用者。
    預設會選取原始使用者。如果此使用者不存在或選取了非原始組織，則必須指定目標使用者。

12. 在 **[路徑]** 中，檢視或變更目標使用者 OneDrive 中的目標資料夾。預設會選取原始位置。
13. 選取是否要復原檔案的共用權限。
14. 按一下 **[開始復原]**。
15. 選擇其中一個檔案覆寫選項：

選項	描述
如果較舊，請覆寫現有的檔案	如果在目的地位置有一個具有相同名稱的檔案，且其比來源檔案還舊，則會將來源檔案儲存在目的地位置，取代較舊的版本。
覆寫現有的檔案	無論上次修改日期為何，目的地位置中的所有現有檔案都會遭到覆寫。
不要覆寫現有檔案	如果目的地位置中包含具有相同名稱的檔案，則不會對其套用任何變更，而且來源檔案不會儲存到目的地位置。

注意事項
當您復原 OneNote 筆記本時，**[如果檔案較舊請覆寫現有檔案]** 以及 **[覆寫現有檔案]** 都將導致現有的 OneNote 筆記本遭覆寫。

16. 按一下 **[繼續]** 可確認您的決定。

保護 SharePoint Online 網站

哪些項目可以備份？

您可以備份 SharePoint 傳統網站集合、群組 (新型團隊) 網站和通訊網站。此外，您也可以選擇個別的子網站、清單和程式庫以進行備份。

備份計劃的個別選項可啟用 OneNote 筆記本的備份。

備份期間會*略過*下列項目：

- **[外觀與風格]** 網站設定 (但**標題、描述和標誌**除外)。
- 網站頁面註解與頁面註解設定 (註解**開啟/關閉**)。
- **[網站功能]** 網站設定。
- Web 組件頁面和 wiki 頁面中內嵌的 Web 組件 (基於 SharePoint Online API 限制)。
- 已簽出的檔案—已手動簽出以供編輯的檔案以及已在程式庫中建立或上傳的所有檔案，其中已啟用 **[需要簽出]** 選項。若要備份這些檔案，請先簽入這些檔案。
- 外部資料和受管理中繼資料類型的欄。
- 預設網站集合 "domain-my.sharepoint.com"。這是所有組織使用者 OneDrive 檔案所在的集合。
- 資源回收筒的內容。

限制

- 如果標題/描述的大小超過 10,000 個位元組，則在備份期間，網站/子網站/清單/欄的標題和描述會遭到截斷。
- 您無法備份在 SharePoint Online 中建立的舊版檔案。只有最新版的檔案受到保護。

- 您無法備份文件保留庫。
- 您無法備份使用 Microsoft 365 前置項 Business Productivity Online Suite (BPOS) 建立的網站。
- 您無法針對使用受管理路徑 `/portals` 的網站備份設定 (例如，`https://<tenant>.sharepoint.com/portals/...`)。
- 只有在目標 Microsoft 365 組織中啟用資訊版權管理 (IRM) 的情況下，才能復原清單或文件庫的 IRM 設定。

可以復原哪些項目？

下列項目可以從網站備份復原：

- 整個網站
- 子網站
- 清單
- 清單項目
- 文件庫
- 文件
- 清單項目附件
- 網站頁面和 wiki 頁面

您可以使用搜尋找出這些項目。

項目可以復原到原始或非原始的網站。已復原項目的路徑與原始項目路徑相同。˙如果路徑不存在，則會建立一個路徑。

您可以選擇要復原共用權限，還是讓項目在復原後繼承父物件的權限。

無法復原哪些項目？

- 以 **Visio 程序存放庫**範本為基礎的子網站。
- 以下類型的清單：**調查清單**、**工作清單**、**圖片庫**、**連結**、**行事曆**、**討論板**、**外部**和**匯入試算表**。
- 啟用多個內容類型的清單。

選擇 SharePoint Online 資料

如下所述選擇資料，然後視需要指定保護計劃的其他設定。

若要選擇 SharePoint Online 資料

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選取您要備份其使用者資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
   - 若要備份組織中的所有傳統 SharePoint 網站 (包括之後建立的網站)，展開 **[網站集合]** 節點、選擇 **[所有網站集合]**，然後按一下 **[群組備份]**。
   - 若要備份個別的傳統網站，展開 **[網站集合]** 節點、選取 **[所有網站集合]**、選取您要備份的網站，然後按一下 **[備份]**。

- 若要備份所有群組 (新型團隊) 網站 (包括之後建立的網站), 展開 **[群組]** 節點、選擇 **[所有群組]**, 然後按一下 **[群組備份]**。
- 若要備份個別的群組 (新型團隊) 網站, 展開 **[群組]** 節點、選擇 **[所有群組]**、選擇您要備份其網站的群組, 然後按一下 **[備份]**。

4. 在保護計劃面板上:
   - 確認在 **[要備份的內容]** 中, 選擇 **[SharePoint 網站]** 項目。
   - 在 **[要備份的項目]** 中, 執行下列其中一項操作:
     - 保留預設設定 **[全部]** (所選網站的所有項目)。
     - 新增子網站、清單和程式庫的名稱或路徑來指定要備份的子網站、清單和程式庫。

       若要備份子網站或最上層網站清單/程式庫, 請使用下列格式指定其顯示名稱:`/display name/**`

       若要備份子網站清單/程式庫, 請使用下列格式指定其顯示名稱:`/subsite display name/list display name/**`

       子網站、清單和程式庫的顯示名稱會顯示在 SharePoint 網站或子網站的 **[網站內容]** 頁面上。
     - 瀏覽來指定要備份的子網站。

       只有在建立單一網站的保護計劃時, 才可以使用 **[瀏覽]** 連結。
   - [選用] 在 **[要備份的項目]** 中, 按一下 **[顯示排除項目]** 來指定要在備份期間略過的子網站、清單和程式庫。

     項目排除項目會覆寫項目選項, 亦即, 如果您在兩個欄位中指定相同的子網站, 將會在備份期間略過這個子網站。
   - [選用] 若要備份 OneNote 筆記本, 請啟用 **[包括 OneNote]** 開關。

復原 SharePoint Online 資料

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務, 請選擇您要復原其已備份資料的組織。否則, 請跳過此步驟。
3. 執行下列其中一項操作:
   - 若要從群組 (新型團隊) 網站復原資料, 展開 **[群組]** 節點、選擇 **[所有群組]**、選擇其網站原本包含您要復原之項目的群組, 然後按一下 **[復原]**。
   - 若要從傳統網站復原資料, 展開 **[網站集合]** 節點、選取 **[所有網站集合]**、選取原本包含您要復原之項目的網站, 然後按一下 **[復原]**。
   - 如果網站遭到刪除, 請在 [備份儲存] 索引標籤的 **[雲端應用程式備份]** 區段中選取該網站, 然後按一下 **[顯示備份]**。

   您可以按名稱搜尋群組和網站。不支援萬用字元。
4. 選擇復原點

   注意事項

   若只要查看含有 SharePoint 網站的復原點, 請在 **[依內容篩選]** 中選取 **[SharePoint 網站]**。
5. 按一下 **[復原 SharePoint 檔案]**。

6. 瀏覽到所需的資料夾，或使用搜尋以取得所需資料項目的清單。
7. 選擇您要復原的項目。

   如果備份未經加密、使用搜尋，並在搜尋結果中選取單一項目，您可以按一下 **[顯示版本]** 來選取要復原的項目版本。您可以選取早於或晚於所選復原點的任何備份版本。
8. [選用] 若要下載項目，請選取項目，按一下 **[下載]**，然後選取要儲存的位置，按一下 **[儲存]**。
9. 按一下 **[復原]**。
10. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。

    預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
11. 在 **[復原至網站]** 中，檢視、變更或指定目標網站。

    您無法在復原期間建立新的 SharePoint 網站。若要將 SharePoint 網站復原為新的 SharePoint 網站，首先需要在所需的 Microsoft 365 組織中建立目標網站，然後讓雲端代理程式同步變更。雲端代理程式每 24 小時自動與 Microsoft 365 同步一次。若要立即同步變更，請在 Cyber Protect 主控台中，選擇 **[Microsoft 365]** 頁面上的組織，然後按一下 **[重新整理]**。
12. 選取是否要復原已復原項目的共用權限。
13. 按一下 **[開始復原]**。
14. 選取其中一個覆寫選項：

選項	描述
如果較舊，請覆寫現有的檔案	如果在目的地位置有一個具有相同名稱的檔案，且其比來源檔案還舊，則會將來源檔案儲存在目的地位置，取代較舊的版本。
覆寫現有的檔案	無論上次修改日期為何，目的地位置中的所有現有檔案都會遭到覆寫。
不要覆寫現有檔案	如果目的地位置中包含具有相同名稱的檔案，則不會對其套用任何變更，而且來源檔案不會儲存到目的地位置。

   注意事項

   當您復原 OneNote 筆記本時，**[如果檔案較舊請覆寫現有檔案]** 以及 **[覆寫現有檔案]** 都將導致現有的 OneNote 筆記本遭覆寫。
15. 按一下 **[繼續]** 可確認您的決定。

保護 Microsoft 365 Teams

哪些項目可以備份？

您可以備份整個小組。這包括小組名稱、小組成員清單、小組頻道及其內容、小組信箱和會議，以及小組網站。

備份計劃的個別選項可啟用 OneNote 筆記本的備份。

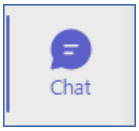
可以復原哪些項目？

- 整個小組
- 小組頻道
- 頻道檔案
- 小組信箱
- 小組信箱中的電子郵件資料夾
- 小組信箱中的電子郵件訊息
- 會議
- 小組網站

您無法復原小組頻道中的對話，但是您可以將這些對話下載為單一 html 檔案。

限制

系統不會備份下列項目：

- 一般頻道的設定 (仲裁喜好設定) – 由於 Microsoft Teams 測試版 API 的限制。
- 自訂頻道的設定 (仲裁喜好設定) – 由於 Microsoft Teams 測試版 API 的限制。
- 會議記錄。
- 聊天區段 

中的訊息。此區段包含私人一對一聊天和群組聊天。
- 貼圖和稱讚。

下列頻道索引標籤支援備份和復原：

- Word
- Excel
- PowerPoint
- PDF
- 文件庫

選擇小組

如下所述選擇小組，然後視需要指定保護計劃的其他設定。

若要選擇小組

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要備份其小組的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
   - 若要備份組織中的所有小組 (包括之後建立的小組)，展開 **[小組]** 節點、選擇 **[所有小組]**，然後按一下 **[群組備份]**。

- 若要備份個別的小組，展開 **[小組]** 節點、選擇 **[所有小組]**、選擇您要備份的小組，然後按一下 **[備份]**。

  您可以按名稱搜尋小組。不支援萬用字元。

4. 在保護計劃面板上：
   - 請確認已在 **[要備份的內容]** 中，選擇 **[Microsoft Teams]** 項目。
   - [選用] 在 **[保留時間]** 中，設定清理選項。
   - [選用] 如果您要加密備份，請啟用 **[加密]** 開關，然後設定密碼並選擇加密演算法。
   - [選用] 若要備份 OneNote 筆記本，請啟用 **[包括 OneNote]** 開關。

復原整個小組

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份小組的組織。否則，請跳過此步驟。
3. 展開 **[小組]** 節點、選擇 **[所有小組]**、選擇您要復原的小組，然後按一下 **[復原]**。

   您可以按名稱搜尋小組。不支援萬用字元。
4. 選擇復原點
5. 按一下 **[復原]** > **[整個小組]**。

   如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。

   預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
6. 在 **[復原到團隊]** 中，查看目標團隊或選擇另一個目標團隊。

   預設選取原始團隊。如果此團隊不存在(例如，已刪除)或您選擇的組織未包含原始團隊，則必須從下拉清單中選擇目標團隊。

   您只能將團隊復原到現有團隊。您無法在復原作業期間建立團隊。
7. 按一下 **[開始復原]**。
8. 選取其中一個覆寫選項：
   - **若現有內容較舊則加以覆寫**
   - **覆寫現有內容**
   - **不要覆寫現有內容**

   注意事項

   當您復原 OneNote 筆記本時，**[若現有內容較舊則加以覆寫]** 以及 **[覆寫現有內容]** 兩個選項都將導致現有的 OneNote 筆記本遭覆寫。
9. 按一下 **[繼續]** 可確認您的決定。

當您在 Microsoft Teams 的圖形介面中刪除頻道時，該頻道不會立即從系統移除。因此，當您復原整個小組時，無法使用此頻道的名稱，而且該名稱將會加上一個後置。

對話在頻道的 **[檔案]** 索引標籤中，會復原為單一 html 檔案。您可以在根據下列模式命名的資料夾中找到此檔案：<小組名稱>_<頻道名稱>_conversations_backup_<復原日期>T<復原時間>Z。

注意事項
復原小組或小組頻道之後，前往 Microsoft Teams，選擇所復原的頻道，然後按一下其 **[檔案]** 索引標籤。否則，這些頻道之後的備份將不會包含此索引標籤的內容 – 由於 Microsoft Teams 測試版 API 的限制。

復原小組頻道或小組頻道中的檔案

若要復原小組頻道

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份小組的組織。否則，請跳過此步驟。
3. 展開 **[小組]** 節點、選擇 **[所有小組]**、選擇您要復原其頻道的小組，然後按一下 **[復原]**。
4. 選擇復原點
5. 按一下 **[復原]** > **[頻道]**。
6. 選擇您要復原的頻道，然後按一下 **[復原]**。若要在主窗格中選擇頻道，請選擇其名稱前方的核取方塊。

   下列搜尋選項可供使用：
   - 若是 **[對話]**：傳送者、主旨、內容、語言、附件名稱、日期或日期範圍。
   - 若是 **[檔案]**：檔案名稱或資料夾名稱、檔案類型、大小、上次變更的日期或日期範圍。

   注意事項
   您也可在本機下載檔案，而非復原它們。
7. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。

   預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
8. 在 **[復原至小組]** 中，檢視、變更或指定目標小組。

   預設會選取原始小組。如果此小組不存在或選取了非原始組織，則必須指定目標小組。
9. 在 **[復原至頻道]** 中，檢視、變更或指定目標頻道。
10. 按一下 **[開始復原]**。
11. 選取其中一個覆寫選項：
    - **若現有內容較舊則加以覆寫**
    - **覆寫現有內容**
    - **不要覆寫現有內容**

    注意事項
    當您復原 OneNote 筆記本時，**[若現有內容較舊則加以覆寫]** 以及 **[覆寫現有內容]** 兩個選項都將導致現有的 OneNote 筆記本遭覆寫。
12. 按一下 **[繼續]** 可確認您的決定。

對話在頻道的 **[檔案]** 索引標籤中，會復原為單一 html 檔案。您可以在根據下列模式命名的資料夾中找到此檔案：<小組名稱>_<頻道名稱>_conversations_backup_<復原日期>T<復原時間>Z。

注意事項
復原小組或小組頻道之後，前往 Microsoft Teams，選擇所復原的頻道，然後按一下其 **[檔案]** 索引標籤。否則，這些頻道之後的備份將不會包含此索引標籤的內容 – 由於 Microsoft Teams 測試版 API 的限制。

復原團隊頻道的檔案

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份小組的組織。否則，請跳過此步驟。
3. 展開 **[小組]** 節點、選擇 **[所有小組]**、選擇您要復原其頻道的小組，然後按一下 **[復原]**。
4. 選擇復原點
5. 按一下 **[復原]** > **[頻道]**。
6. 選擇所需的頻道，然後開啟 **[檔案]** 資料夾。
   瀏覽到所需的項目，或使用搜尋以取得所需項目的清單。可使用以下搜尋選項：檔案名稱或資料夾名稱，檔案類型，大小，上次變更日期或日期範圍。
7. [選用] 若要下載項目，請選取項目，按一下 **[下載]**，然後選取要儲存的位置，按一下 **[儲存]**。
8. 選擇您要復原的項目，然後按一下 **[復原]**
9. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 [Microsoft 365 組織] 可檢視、變更或指定目標組織。
   預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
10. 在 **[復原至小組]** 中，檢視、變更或指定目標小組。
    預設會選取原始小組。如果此小組不存在或選取了非原始組織，則必須指定目標小組。
11. 在 **[復原至頻道]** 中，檢視、變更或指定目標頻道。
12. 選取是否要復原已復原項目的共用權限。
13. 按一下 **[開始復原]**。
14. 選取其中一個覆寫選項：
    - **若現有內容較舊則加以覆寫**
    - **覆寫現有內容**
    - **不要覆寫現有內容**

    注意事項
    當您復原 OneNote 筆記本時，**[若現有內容較舊則加以覆寫]** 以及 **[覆寫現有內容]** 兩個選項都將導致現有的 OneNote 筆記本遭覆寫。
15. 按一下 **[繼續]** 可確認您的決定。

您無法復原個別的對話。在主窗格中，您僅能瀏覽 **[對話]** 資料夾或將其內容下載為單一 html 檔案。方法是，按一下 [復原資料夾] 圖示  、選擇所需的 **[對話]** 資料夾，然後按一下 **[下載]**。

您可以在 **[對話]** 資料夾中，按照下列條件，搜尋訊息：

- 寄件者
- 內容
- 附件名稱
- 日期

復原小組信箱

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份小組的組織。否則，請跳過此步驟。
3. 展開 **[小組]** 節點、選擇 **[所有小組]**、選擇您要復原其信箱的小組，然後按一下 **[復原]**。
   您可以按名稱搜尋小組。不支援萬用字元。
4. 選擇復原點
5. 按一下 **[復原]** > **[電子郵件訊息]**。
6. 按一下 [復原資料夾] 圖示  、選擇根信箱資料夾，然後按一下 **[復原]**。

   注意事項
   您也可以從所選信箱復原個別的資料夾。

7. 按一下 **[復原]**。
8. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。
   預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
9. 在 **[復原至信箱]** 中，檢視、變更或指定目標信箱。
   原始信箱預設為選取狀態。如果此信箱不存在或選取了非原始組織，則必須指定目標信箱。
10. 按一下 **[開始復原]**。
11. 選取其中一個覆寫選項：
    - **覆寫現有項目**
    - **不要覆寫現有項目**
12. 按一下 **[繼續]** 可確認您的決定。

將團隊信箱項目復原到 PST 檔案

復原團隊信箱項目

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 您可以按名稱搜尋使用者和群組。不支援萬用字元。
4. 展開 **[團隊]** 節點、選取 **[所有團隊]**、針對信箱原來包含要復原的項目選取團隊，然後按一下 **[復原]**。
5. 按一下 **[復原]** > **[電子郵件訊息]**。
6. 瀏覽到所需的資料夾，或使用搜尋以取得所需項目的清單。

您可以使用下列搜尋選項。不支援萬用字元。

- 電子郵件訊息：依主旨、寄件者、收件者、附件名稱及日期搜尋。
- 事件：依主題及日期搜尋。
- 工作：依主題及日期搜尋。
- 連絡人：依姓名、電子郵件地址和電話號碼搜尋。

7. 選擇您要復原的項目。若要能夠選擇資料夾，請按一下 [復原資料夾] 圖示： 

   此外，您可以執行下列任何一項作業：

   - 選取項目後，按一下 **[顯示內容]** 可檢視其內容，包括附件。若要下載附加檔案，請按一下其名稱。
   - 選取電子郵件訊息或行事曆項目後，按一下 **[以電子郵件傳送]**，可將該項目傳送到指定的電子郵件地址。您可以選取寄件者，並撰寫要加入至轉寄項目的文字。
   - 當備份未加密時，使用搜尋並從搜尋結果選取單一項目：按一下 **[顯示版本]** 來檢視版本項目。您可選取任何備份版本，無論該版本早於或晚於選取的復原點。
8. 按一下 **[復原為 PST 檔案]**。
9. 設定密碼使用 PST 檔案加密存檔。

   密碼應包含至少一個符號。
10. 確認密碼，然後按一下 **[完成]**。

選定的信箱項目將復原為 PST 資料檔並以 ZIP 格式存檔。PST 檔案的最大限制為 2 GB，因此，如果要復原的資料超過 2 GB，將被拆分成多個 PST 檔案。ZIP 存檔將使用您設定的密碼進行保護。

您將收到一封電子郵件，其中的連結指向 ZIP 存檔，並包含建立的 PST 檔案。

系統管理員將收到您已執行復原程式的電子郵件通知。

使用 PST 檔案下載存檔並完全復原

1. 執行下列其中一項操作：
   - 若要從電子郵件下載存檔，請點選 **[下載檔案]** 連結。

     可在 24 小時內下載存檔。如果連結過期，請重複復原程式。
   - 從 Cyber Protect 主控台下載存檔：
     a. 前往 **[備份儲存]** > **[PST 檔案]**。
     b. 選擇最新醒目提示的存檔。
     c. 在右窗格按一下 **[下載]**。

   存檔將下載到您電腦的預設下載目錄。
2. 使用您設定適合加密存檔的密碼從存檔提取 PST 檔案。
3. 在 Microsoft Outlook 中開啟或匯入 PST 檔案。想了解如何操作，請參閱 Microsoft 文件。

復原電子郵件訊息和會議

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份小組的組織。否則，請跳過此步驟。

3. 展開 **[小組]** 節點、選擇 **[所有小組]**、選擇您要復原其電子郵件訊息或會議的小組，然後按一下 **[復原]**。
   您可以按名稱搜尋小組。不支援萬用字元。
4. 選擇復原點
5. 按一下 **[復原]** > **[電子郵件訊息]**。
6. 瀏覽到所需的項目，或使用搜尋以取得所需項目的清單。
   下列搜尋選項可供使用：
   - 電子郵件訊息：依主題、寄件者、收件者及日期搜尋。
   - 若是會議：依事件名稱和日期搜尋。
7. 選擇您要復原的項目，然後按一下 **[復原]**。

   注意事項
   您可以在 **[行事曆]** 資料夾中找到會議。

   此外，您可以執行下列任何一項作業：
   - 選取項目後，按一下 **[顯示內容]** 可檢視其內容，包括附件。要下載附加檔案，請按一下名稱。
   - 選取電子郵件訊息或會議後，按一下 **[以電子郵件傳送]** 可將該項目傳送到指定的電子郵件地址。您可以選取寄件者，並撰寫要加入至轉寄項目的文字。
8. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。
   預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
9. 在 **[復原至信箱]** 中，檢視、變更或指定目標信箱。
   原始信箱預設為選取狀態。如果此信箱不存在或選取了非原始組織，則必須指定目標信箱。
10. 按一下 **[開始復原]**。
11. 選取其中一個覆寫選項：
    - **覆寫現有項目**
    - **不要覆寫現有項目**
12. 按一下 **[繼續]** 可確認您的決定。

復原小組網站或特定的網站項目

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份小組的組織。否則，請跳過此步驟。
3. 展開 **[小組]** 節點、選擇 **[所有小組]**、選擇您要復原其網站的小組，然後按一下 **[復原]**。
   您可以按名稱搜尋小組。不支援萬用字元。
4. 選擇復原點
5. 按一下 **[復原]** > **[小組網站]**。
6. 瀏覽到所需的項目，或使用搜尋以取得所需項目的清單。
7. [選用] 若要下載項目，請選取項目，按一下 **[下載]**，然後選取要儲存的位置，按一下 **[儲存]**。
8. 選擇您要復原的項目，然後按一下 **[復原]**。

9. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。

   預設會選取原始組織和小組。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
10. 在 **[復原至小組]** 中，檢視、變更或指定目標小組。

    預設會選取原始小組。如果此小組不存在或選取了非原始組織，則必須指定目標網站。
11. 選取是否要復原已復原項目的共用權限。
12. 按一下 **[開始復原]**。
13. 選取其中一個覆寫選項：
    - **若現有內容較舊則加以覆寫**
    - **覆寫現有內容**
    - **不要覆寫現有內容**

    注意事項

    當您復原 OneNote 筆記本時，**[若現有內容較舊則加以覆寫]** 以及 **[覆寫現有內容]** 兩個選項都將導致現有的 OneNote 筆記本遭覆寫。
14. 按一下 **[繼續]** 可確認您的決定。

保護 OneNote 筆記型電腦

根據預設，OneNote 筆記本包含在 OneDrive 檔案、Microsoft Teams 和 SharePoint 網站的備份中。

若要從這些備份中排除 OneNote 筆記本，請在個別的備份計劃中停用 **[包括 OneNote]** 開關。

復原備份的 OneNote 筆記本

若要瞭解如何復原備份 OneNote 筆記本，請參閱對應的主題：

- 有關 OneDrive 備份，請參閱 "復原整個 OneDrive" (第 563 頁) 或 "復原 OneDrive 檔案" (第 564 頁)。
- 有關 Teams 備份，請參閱 "復原整個小組" (第 570 頁)、"復原小組頻道或小組頻道中的檔案" (第 571 頁) 或 "復原小組網站或特定的網站項目" (第 575 頁)。
- 有關 SharePoint 網站備份，請參閱 "復原 SharePoint Online 資料" (第 567 頁)。

支援的版本

- OneNote(OneNote 2016 及更新版本)
- Windows 10 版 OneNote

限制及已知問題

- OneDrive 或 SharePoint 當中儲存的 OneNote 筆記本上限為 2 GB。您無法將更大的 OneNote 筆記本復原至 OneDrive 或 SharePoint 目標。
- 不支援具有區段群組的 OneNote 筆記本。

- 對於備份 OneNote 筆記本包含非預設名稱的區段，第一區段會以預設名稱顯示(例如 [新區段] 或 [無標題區段])。這可能會影響具有多個區段的筆記本區段順序。
- 當您復原 OneNote 筆記本時，**[若現有內容較舊則加以覆寫]** 以及 **[覆寫現有內容]** 兩個選項都將導致現有的 OneNote 筆記本遭覆寫。
- 當您復原整個小組、小組網站或小組網站的網站資產資料夾，且選擇 **[若現有內容較舊則加以覆寫]** 或 **[覆寫現有內容]** 選項時，將不會覆寫小組的預設 OneNote 筆記本。成功復原，但出現警告 *無法更新「/sites/<Team name>/SiteAssets/<OneNote notebook name>」檔案的屬性*。

保護 Microsoft 365 協同作業應用程式授權

您可以使用 Advanced Email Security 套件，為 Microsoft 365、Google Workspace 或 Open-Xchange 信箱提供即時保護：

- 反惡意程式碼和防垃圾郵件
- 電子郵件內的 URL 掃描
- DMARC 分析
- 防網路釣魚
- 模擬保護
- 附件掃描
- 消除內容的傷害力並重建
- 信任圖

您也可以啟用 Microsoft 365 協同作業應用程式授權，如此可保護 Microsoft 365 雲端協同作業應用程式免受內容傳播的安全性威脅。這些應用程式包括 OneDrive、SharePoint 和 Teams。

Advanced Email Security 可以按工作負載或按 GB 啟用，而且將影響您的授權模型。

若要從 Cyber Protect Cloud 主控台將 Advanced Email Security 上線

1. 按一下 **[裝置]** > **[Microsoft 365]**。
2. 按一下 **[使用者]** 節點，然後按一下右上方的 **[移至 Email Security]** 連結。

在Advanced Email Security 規格書中深入瞭解Advanced Email Security。

如需設定指示，請參閱採用 Perception Point 技術的Advanced Email Security。

保護 Google Workspace 資料

注意事項
在合規模式下，此功能不適用於租用戶。如需詳細資訊，請參閱 "合規模式" (第 980 頁)。

Google Workspace 保護是什麼意思？

- Google Workspace 使用者資料 (Gmail 信箱、行事曆、聯絡人、Google 雲端硬碟) 與 Google Workspace 共用磁碟機的雲端對雲端備份和復原。
- 電子郵件、檔案、聯絡人和其他項目的細微復原。

- 對數個 Google Workspace 組織和跨組織復原的支援。
- 選擇性地透過 Ethereum 區塊鏈資料庫公證備份檔案。啟用時，您可以證明檔案在備份後即是真實和未變更的。
- 選擇性的全文檢索。啟用時，您可以依電子郵件內容來搜尋電子郵件。
- 每個公司最多有 5,000 個項目 (信箱、Google 雲端硬碟和共用磁碟機) 可以受到保護，而不會降低效能。
- 備份資料會自動壓縮，並且在備份位置上使用的空間比原始位置更少。雲端到雲端備份的壓縮層級是固定的，對應於非雲端到雲端備份的 **一般** 層級。有關這些層級的詳細資訊，請參閱 "壓縮層級" (第 406 頁)。

所需的使用者權限

在 Cyber Protection 中

在 Cyber Protection 中，您必須是客戶租用戶層級的公司系統管理員。單位層級的公司系統管理員、單位系統管理員和使用者無法備份或復原 Google Workspace 資料。

在 Google Workspace 中

若要將 Google Workspace 組織新增到 Cyber Protection 服務，您必須使用已啟用 API 存取的 Super Admin 身分登入 (在 Google Admin 主控台中的 **[安全性]** > **[API 參照]** > **[啟用 API 存取]**)。

Super Admin 密碼不會儲存在任何地方，也不會用於執行備份和復原。在 Google Workspace 中變更此密碼不會影響 Cyber Protection 服務作業。

如果新增 Google Workspace 組織的 Super Admin 從 Google Workspace 刪除，或者獲指派權限較低的角色，則備份將會失敗，並出現「拒絕存取」之類的錯誤。在此情況下，請重複 "新增 Google Workspace 組織" (第 579 頁) 中所述的程序，並指定有效的 Super Admin 認證。為避免此情況，建議您建立專用的 Super Admin 使用者，以供備份和復原之用。

關於備份排程

雲端代理程式可服務多個客戶，因此它會針對每個保護計劃，自行決定開始時間，以確保一天中的負載均衡，且所有客戶都獲得同等的服務品質。

每個保護計劃每天都會在相同的時間執行。

預設選項為**一天一次**。使用 Advanced Backup 套件，即可每天排程最多六個備份。備份會以近似間隔開始，該間隔根據目前服務資料中心內多個客戶的雲端代理程式負載而定。這能確保一天中的負載均衡，且所有客戶都獲得同等的服務品質。

限制

- Cyber Protect 主控台僅會顯示擁有獲指派 Google Workspace 授權和信箱或 Google 雲端硬碟的使用者。

- 在變更其狀態後的探索操作之後，已存檔或已暫停的 Google Workspace 使用者在 Cyber Protect 主控台中會顯示為非作用中 (變為灰色)。您無法將新的備份計劃套用到非作用中使用者。現有的備份計劃在 72 小時內將保持有效。

  在 72 小時期限後的探索操作之後，已存檔或已暫停的使用者會從 Cyber Protect 主控台中移除，且不再備份其資料。現有的備份仍然可用。
- 遭刪除 Google Workspace 使用者帳戶的備份不會自動從雲端儲存空間中刪除。這些備份會按所使用的儲存空間收取費用。
- 原生 Google 格式的文件會備份為一般 Office 文件，並以不同的副檔名顯示在 Cyber Protect 主控台中，例如 .docx 或 .pptx。在復原期間，這些文件會轉換為其原始格式。
- 每小時您可以手動執行最多 10 個備份。如需詳細資訊，請參閱 "手動執行雲端對雲端備份" (第 211 頁)。
- 您可以同時執行最多 10 個雲端對雲端復原作業。此數字包括 Microsoft 365 和 Google Workspace 復原作業。
- 即使您可以從搜尋結果中選擇這類項目，也無法同時從不同的復原點復原這些項目。
- 您只能將一個個別的備份計劃套用到工作負載。
- 當單獨備份計劃和群組備份計劃套用到相同工作負載時，單獨計劃中的設定具有更高優先順序。

記錄

檢視已備份電子郵件的內容、下載附件或檔案、將電子郵件復原到非原始信箱，或將其當作電子郵件傳送等使用雲端對雲端資源的動作可能會違反使用者隱私權。這些動作會記錄在管理入口網站的 **[監控]** > **[稽核記錄]** 中。

新增 Google Workspace 組織

若要將 Google Workspace 組織新增至 Cyber Protection 服務，您需要專用的個人 Google Cloud 專案。如需有關如何建立並設定這種專案的詳細資訊，請參閱 "建立個人 Google Cloud 專案" (第 580 頁)。

使用專用的個人 Google Cloud 專案新增 Google Workspace 組織

1. 以公司系統管理員的身分，登入 Cyber Protect 主控台。
2. 按一下 **[裝置]** > **[新增]** > **[Google Workspace]**。
3. 輸入 Google Workspace 帳戶超級系統管理員的電子郵件地址。
   對於此程序，無論是否針對超級系統管理員電子郵件帳戶啟用 2 步驟驗證，都無關緊要。
4. 瀏覽包含您在 Google Cloud 專案中建立之服務帳戶私密金鑰的 JSON 檔案。
   您也可以將檔案內容當作文字貼上。
5. 按一下 **[確認]**。

結果，您的 Google Workspace 組織出現在 主控台的 **[裝置]** 索引標籤底下。

有用的提示

- 新增 Google Workspace 組織之後，將會備份主要網域和所有次要網域 (如果有的話) 中的使用者資料與共用磁碟機。已備份的資源將會顯示在一個清單中，而且將不會依其網域分組。
- 雲端代理程式從組織新增至 Cyber Protection 服務開始，每 24 小時會與 Google Workspace 同步一次。如果您新增或移除使用者或共用磁碟機，將不會在 Cyber Protect 主控台中立即看到這個變更。若要立即同步變更，請在 **[Google Workspace]** 頁面上選取組織，然後按一下 **[重新整理]**。如需有關同步 Google Workspace 組織和 Cyber Protect 主控台資源的詳細資訊，請參閱 "探索 Google Workspace 資源" (第 583 頁)。
- 如果您已經將保護計劃套用到 **[所有使用者]** 或 **[所有共用磁碟機]** 群組，則只有在同步後，新增的項目才會包含在備份中。
- 根據 Google 原則，當使用者或共用磁碟機從 Google Workspace 圖形化使用者介面移除之後，仍然可以透過 API 使用幾天。在這段時間內，已移除的項目在 Cyber Protect 主控台中為非作用中 (呈灰色) 狀態，而且將不會進行備份。當已移除的項目變成無法透過 API 使用時，就會從 Cyber Protect 主控台中消失。其備份 (如果有的話) 可以在 **[備份儲存]** > **[雲端應用程式備份]** 中找到。

建立個人 Google Cloud 專案

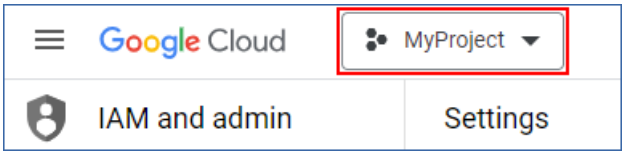
若要使用專用的 Google Cloud 專案將 Google Workspace 組織新增至 Cyber Protection 服務，您需要執行下列操作：

1. 建立新的 Google Cloud 專案。
2. 啟用此專案所需的 API。
3. 設定此專案的認證：
   a. 設定 OAuth 同意畫面。
   b. 為 Cyber Protection 服務建立並設定服務帳戶。
4. 為您的 Google Workspace 帳戶授予新的專案存取權。

注意事項
本主題包含第三方使用者介面的描述，如有變更，恕不另行通知。

建立新的 Google Cloud 專案

1. 以超級系統管理員的身分，登入 Google Cloud Platform (console.cloud.google.com)。
2. 在 Google Cloud Platform 主控台中，按一下左上角的專案選擇器。



3. 在開啟的畫面中，選擇組織，然後按一下 **[新增專案]**。

4. 為您的新專案指定一個名稱。
5. 按一下 **[建立]**。

   結果，您的新 Google Cloud 專案隨即建立。

啟用此專案所需的 API

1. 在 Google Cloud Platform 主控台中，選取您的新專案。
2. 從導覽功能表中，選取 **[API 和服務]** > **[已啟用的 API 和服務]**。
3. 逐一停用在此專案中預設啟用的所有 API：
   a. 向下捲動 **[已啟用的 API 和服務]** 頁面，然後按一下已啟用之 API 的名稱。
      所選 API 的 **[API/服務詳細資料]** 頁面隨即開啟。
   b. 按一下 **[停用 API]**，然後按一下 **[停用]**，確認您的選擇。
   c. [如果出現提示] 按一下 **[確認]**，確認您的選擇。
   d. 返回 **[API 和服務]** > **[已啟用的 API 和服務]**，然後停用下一個 API。
4. 從導覽功能表中，選取 **[API 和服務]** > **[程式庫]**。
5. 在 API 程式庫中，逐一啟用下列 API：
   - Admin SDK API
   - Gmail API
   - Google Calendar API
   - Google Drive API
   - Google People API

   使用搜尋列尋找所需的 API。若要啟用 API，請按一下其名稱，然後按一下 **[啟用]**。若要搜尋下一個 API，從導覽功能表中，選取 **[API 和服務]** > **[程式庫]** 以返回 API 程式庫。

設定 OAuth 同意畫面

1. 從 Google Cloud Platform 的導覽功能表中，選取 **[API 和服務]** > **[OAuth 同意畫面]**。
2. 在開啟的視窗中，選取 **[內部]** 作為使用者類型，然後按一下 **[建立]**。
3. 在 **[應用程式名稱]** 欄位中，為您的應用程式指定一個名稱。
4. 在 **[使用者支援電子郵件]** 欄位中，輸入超級系統管理員電子郵件。
5. 在 **[開發人員聯絡資訊]** 欄位中，輸入超級系統管理員電子郵件。
6. 將其他所有欄位留空，然後按一下 **[儲存並繼續]**。
7. 在 **[範圍]** 頁面上，按一下 **[儲存並繼續]**，而不必變更任何內容。
8. 在 **[摘要]** 頁面上，確認您的設定，然後按一下 **[返回資訊主頁]**。

為 Cyber Protection 服務建立並設定服務帳戶

1. 從 Google Cloud Platform 的導覽功能表中，選取 **[IAM 與管理]** > **[服務帳戶]**。
2. 按一下 **[建立服務帳戶]**。
3. 指定服務帳戶的名稱。
4. [選用] 指定服務帳戶的說明。
5. 按一下 **[建立並繼續]**。

6. 請勿變更 **[將專案存取權授予這個服務帳戶]** 和 **[將這個服務帳戶的存取權授予使用者]** 步驟中的任何內容。
7. 按一下**[完成]**。

   [服務帳戶] 頁面隨即開啟。
8. 在 **[服務帳戶]** 頁面上，選取新的服務帳戶，然後在 **[動作]** 底下，按一下 **[管理金鑰]**。
9. 在 **[金鑰]** 底下，按一下 **[新增金鑰]** > **[建立新的金鑰]**，然後選取 **[JSON]** 金鑰類型。
10. 按一下 **[建立]**。

    結果，含有服務帳戶私密金鑰的 JSON 檔案會自動下載到您的電腦。安全地儲存此檔案，因為在您將 Google Workspace 組織新增到 Cyber Protection 服務時，將需要這個檔案。

為您的 Google Workspace 帳戶授予新的專案存取權

1. 從 Google Cloud Platform 的導覽功能表中，選取 **[IAM 與管理]** > **[服務帳戶]**。
2. 在清單中，找出您建立的服務帳戶，然後複製顯示在 **[OAuth 2.0 用戶端 ID]** 欄´中的用戶端 ID。
3. 以超級系統管理員的身分，登入 Google Admin 主控台 (admin.google.com)。
4. 從導覽功能表中，選取 **[安全性]** > **[存取和資料控制]** > **[API 控制項]**。
5. 向下捲動 **[API 控制項]** 頁面，然後在 **[全網域委派]** 底下，按一下 **[管理全網域委派]**。

   [全網域委派] 頁面隨即開啟。
6. 在 **[全網域委派]** 頁面上，按一下 **[新增]**。

   [新增用戶端 ID] 視窗隨即開啟。
7. 在 **[用戶端編號]** 欄位中，輸入您服務帳戶用戶端的用戶端編號。
8. 在 **[OAuth 範圍]** 欄位中，複製並貼上以下逗號分隔的範圍清單：

   ```
   https://mail.google.com,https://www.googleapis.com/auth/contacts,https://www.googlea
   pis.com/auth/calendar,https://www.googleapis.com/auth/admin.directory.user.readonly,
   https://www.googleapis.com/auth/admin.directory.domain.readonly,https://www.googleap
   is.com/auth/drive,https://www.googleapis.com/auth/gmail.modify
   ```

   或者，您可以每行新增一個範圍：
   - 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. 按一下 **[授權]**。

結果，您的新 Google Cloud 專案可以存取您 Google Workspace 帳戶中的資料。若要備份資料，您需要將此專案連結到 Cyber Protection 服務。如需有關操作方式的詳細資訊，請參閱 "使用專用的個人 Google Cloud 專案新增 Google Workspace 組織" (第 579 頁)。

如果您需要撤銷 Google Workspace 帳戶對 Google Cloud 專案的存取權，以及對 Cyber Protection 服務的存取權，請刪除您專案使用的 API 用戶端。

撤銷對 Google Workspace 帳戶的存取權

1. 在 Google Admin 主控台 (admin.google.com) 中，以超級系統管理員的身分登入。
2. 從導覽功能表中，選擇 **[安全性]** > **[存取和資料控制]** > **[API 控制項]**。
3. 向下捲動 **[API 控制項]** 頁面，然後在 **[全網域委派]** 底下，按一下 **[管理全網域委派]**。
   [全網域委派] 頁面隨即開啟。
4. 在 **[全網域委派]** 頁面上，選取您專案所使用的 API 用戶端，然後按一下 **[刪除]**。
   結果，您的 Google Cloud 專案和 Cyber Protection 服務將無法存取您的 Google Workspace 帳戶並備份其中的資料。

探索 Google Workspace 資源

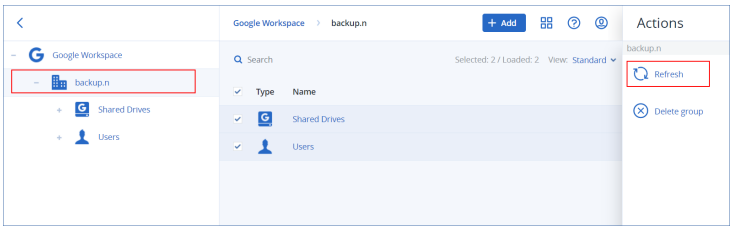
當您將 Google Workspace 組織新增至 Cyber Protection 服務時，此組織中的資源 (例如信箱和 Google 雲端硬碟) 會同步到 Cyber Protect 主控台中。此作業稱為探索，且其記錄在 **[監控]** > **[活動]** 中。

探索作業完成後，您可以在 主控台的 **[裝置]** > **[Google Workspace]** 索引標籤上，查看 Google Workspace 組織的資源，而且您可以在其中套用備份計劃。

自動探索作業會每天執行一次，以便在 Cyber Protect 主控台中保留最新的資源清單。您也可以視需要，透過手動重新執行探索作業來同步此清單。

若要手動執行探索作業

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[Google Workspace]**。
2. 選擇您的 Google Workspace 組織，然後在 **[動作]** 窗格中，按一下 **[重新整理]**。



注意事項
每小時可以手動執行探索作業高達 10 次。達到此次數後，允許的執行會重設為每小時一次，然後每小時可以額外執行一次，直到再次達到每小時總共執行 10 次為止。

設定 Google Workspace 備份的頻率

依預設值，Google Workspace 備份每天會執行一次，且無法使用其他排程選項。

如果租用戶中啟用了 Advanced Backup 套件，您就能更頻繁設定備份。您可以選擇每天備份數，但無法設定備份開始時間。備份會以近似間隔自動開始，該間隔根據目前服務資料中心內多個客戶的雲端代理程式負載而定。這能確保一天中的負載均衡，且所有客戶都獲得同等的服務品質。

您可以調整下列選項。

排程選項	每次備份間的近似間隔
一天一次	24 小時
一天兩次 (預設)	12 小時
一天 3 次	8 小時
一天 6 次	4 小時

注意事項
依雲端代理程式以及 Google Workspace 可能的調節而定，備份可能會比排程還晚執行，或需要更長時間才能完成。如果備份比兩次備份平均間隔還長，將重新排定下次備份，這可能導致每天備份數比所選次數還少。例如，就算選擇每天六次，每天也可能只能完成兩次備份。

保護 Gmail 資料

哪些項目可以備份？

您可以備份 Gmail 使用者的信箱。信箱備份也包括行事曆和聯絡人資料。或者，您可以選擇備份共用行事曆。

備份期間會*略過*下列項目：

- **[生日]**、**[提醒]**、**[任務]** 行事曆
- 連接至行事曆活動的資料夾
- [聯絡人] 中的 **[目錄]** 資料夾

系統會因為 Google Calendar API 的限制，而*略過*下列行事曆項目：

- 預約時段
- 活動的會議欄位
- 行事曆設定 **[全天活動通知]**
- 行事曆設定 **[自動接受邀請]** (在行事曆中，用於房間或共用空間)

系統會因為 Google People API 的限制，而*略過*下列聯絡人項目：

- **[其他聯絡人]** 資料夾
- 聯絡人的外部設定檔 (**目錄設定檔**、**Google 設定檔**)
- 聯絡人欄位 **[歸檔為]**

可以復原哪些項目？

下列項目可以從信箱備份復原：

- 信箱
- 電子郵件資料夾 (根據 Google 詞彙，「標籤」。**標籤**在備份軟體中會顯示為資料夾，以便與其他資料顯示保持一致)。
- 電子郵件訊息

- 行事曆事件
- 連絡人

您可以使用搜尋來找出備份中的項目。

復原信箱和信箱項目時，您可以選擇是否要覆寫目標位置中的項目。

限制

- 無法復原聯絡人相片
- **[不在辦公室]** 行事曆項目會因為 Google Calendar API 的限制而復原為一般行事曆活動

選擇 Gmail 信箱

如下所述選擇信箱，然後視需要指定保護計劃的其他設定。

若要選擇 Gmail 信箱

1. 按一下 **[Google Workspace]**。
2. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，請選取您要備份其使用者資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
   - 若要備份所有使用者的信箱 (包括之後建立的信箱)，展開 **[使用者]** 節點、選取 **[所有使用者]**，然後按一下 **[群組備份]**。
   - 若要備份個別的使用者信箱，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要備份其信箱的使用者，然後按一下 **[備份]**。
4. 在保護計劃面板上：
   - 確認在 **[要備份的內容]** 中，選擇 **[Gmail]** 項目。
   - 如果您要備份與所選使用者共用的行事曆，請啟用 **[包括共用行事曆]** 開關。
   - 決定您是否需要全文檢索已備份的電子郵件訊息。若要存取此選項，按一下齒輪圖示 > **[備份選項]** > **[全文檢索]**。

復原信箱和信箱項目

復原信箱

1. 按一下 **[Google Workspace]**。
2. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，請選取您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原其信箱的使用者，然後按一下 **[復原]**。
   如果使用者遭到刪除，請在 [備份儲存] 索引標籤的 **[雲端應用程式備份]** 區段中選取該使用者，然後按一下 **[顯示備份]**。
   您可以按名稱搜尋使用者和群組。不支援萬用字元。
4. 選擇復原點

注意事項
若只要查看含有信箱的復原點，請在 **[依內容篩選]** 中選取 **[Gmail]**。

5. 按一下 **[復原]** > **[整個信箱]**。
6. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，按一下 **[Google Workspace 組織]** 可檢視、變更或指定目標組織。
   預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須從可用的已登錄組織中選擇一個新的目標組織。
7. 在 **[復原至信箱]** 中，檢視、變更或指定目標信箱。
   原始信箱預設為選取狀態。如果此信箱不存在或選取了非原始組織，則必須指定目標信箱。
   您無法在復原期間建立新的目標信箱。若要將某個信箱復原到新的信箱，首先您需要在所需的 Google Workspace 組織中建立目標信箱，然後讓雲端代理程式同步變更。雲端代理程式每 24 小時會自動與 Google Workspace 同步一次。若要立即同步變更，請在 Cyber Protect 主控台的 **[Google Workspace]** 頁面上選擇組織，然後按一下 **[重新整理]**。
8. 按一下 **[開始復原]**。
9. 選取其中一個覆寫選項：
   - **覆寫現有項目**
   - **不要覆寫現有項目**
10. 按一下 **[繼續]** 可確認您的決定。

復原信箱項目

1. 按一下 **[Google Workspace]**。
2. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，請選取您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取其信箱原本包含您要復原之項目的使用者，然後按一下 **[復原]**。
   如果使用者遭到刪除，請在 [備份儲存] 索引標籤的 **[雲端應用程式備份]** 區段中選取該使用者，然後按一下 **[顯示備份]**。
   您可以按名稱搜尋使用者和群組。不支援萬用字元。
4. 選擇復原點

注意事項
若只要查看含有信箱的復原點，請在 **[依內容篩選]** 中選取 **[Gmail]**。

5. 按一下 **[復原]** > **[電子郵件訊息]**。
6. 瀏覽至所需的資料夾。如果備份未經過加密，您可以使用搜尋以取得所需項目的清單。
   您可以使用下列搜尋選項。不支援萬用字元。
   - 電子郵件訊息：依主旨、寄件者、收件者、日期、附件名稱和訊息內容搜尋。
     依日期搜尋時，您可以選擇開始日期或結束日期 (包括兩者)，或同時選擇兩者以便在某個時間範圍內進行搜尋。

只有在備份期間啟用了 **[全文檢索]** 選項的情況下，依附件名稱搜尋或在郵件內容中搜尋才會產生結果。您可以指定將當作其他參數搜尋之郵件片段的語言。

- 事件：依主題及日期搜尋。
- 連絡人：依姓名、電子郵件地址和電話號碼搜尋。

7. 選擇您要復原的項目。若要能夠選擇資料夾，請按一下 [復原資料夾] 圖示： 

   此外，您可以執行下列任何一項作業：

   - 選取項目後，按一下 **[顯示內容]** 可檢視其內容，包括附件。若要下載附加檔案，請按一下其名稱。
   - 只有在備份未經加密、使用搜尋，並在搜尋結果中選取單一項目時：按一下 **[顯示版本]** 來選取要復原的項目版本。您可以選取早於或晚於所選復原點的任何備份版本。
8. 按一下 **[復原]**。
9. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，按一下 **[Google Workspace 組織]** 可檢視、變更或指定目標組織。

   預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須從可用的已登錄組織中選擇一個新的目標組織。
10. 在 **[復原至信箱]** 中，檢視、變更或指定目標信箱。

    原始信箱預設為選取狀態。如果此信箱不存在或選取了非原始組織，則必須指定目標信箱。
11. 在 **[路徑]** 中，檢視或變更目標信箱中的目標資料夾。原始資料夾根據預設已經選取。
12. 按一下 **[開始復原]**。
13. 選取其中一個覆寫選項：
    - **覆寫現有項目**
    - **不要覆寫現有項目**
14. 按一下 **[繼續]** 可確認您的決定。

保護 Google 雲端硬碟檔案

哪些項目可以備份？

您可以備份整個 Google 雲端硬碟或個別的檔案和資料夾。檔案會與其共用權限一起備份。

重要事項
系統不會備份下列項目：

- **[與我共用]** 資料夾
- **[電腦]** 資料夾 (由備份和同步用戶端所建立)

限制

非 Google 專屬檔案格式、Google 文件、Google 試算表和 Google 簡報都完整支援備份和復原。其他 Google 專屬格式可能未受到完整支援或可能完全不受支援，例如，Google 繪圖檔案會復原為 `.svg` 檔案、Google 協作平台網站會復原為 `.txt` 檔案、Google Jamboard 檔案會復原為 `.pdf` 檔案，而 Google 我的地圖檔案在備份期間則會被略過。

注意事項
非 Google 專屬的檔案格式 (例如 .txt、.docx、.pptx、.pdf、.jpg、.png、.zip) 則完整支援備份和復原。

可以復原哪些項目?

您可以復原整個 Google 雲端硬碟或已備份的任何檔案或資料夾。

您可以選擇要復原共用權限, 還是讓檔案繼承復原目標資料夾的權限。

限制

- 系統不會復原檔案中的註解。
- 檔案與資料夾的共用連結不會復原。
- 復原期間, 無法變更共用檔案的唯讀 **[擁有者設定]** (**[防止編輯者變更存取權並加入新的人員]** 以及 **[為註解者和檢視者停用下載、列印和複製的選項]**)。
- 如果為此資料夾啟用 **[防止編輯者變更存取權並加入新的人員]** 選項, 則在復原期間, 無法變更共用資料夾的所有權。此設定會防止 Google Drive API 列出資料夾權限。系統會正確地復原資料夾中檔案的所有權。

選擇 Google 雲端硬碟檔案

如下所述選擇檔案, 然後視需要指定保護計劃的其他設定。

若要選擇 Google 雲端硬碟檔案

1. 按一下 **[Google Workspace]**。
2. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務, 請選取您要備份其使用者資料的組織。否則, 請跳過此步驟。
3. 執行下列其中一項操作:
   - 若要備份所有使用者 (包括之後建立的使用者) 的檔案, 展開 **[使用者]** 節點、選取 **[所有使用者]**, 然後按一下 **[群組備份]**。
   - 若要備份個別使用者的檔案, 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要備份其檔案的使用者, 然後按一下 **[備份]**。
4. 在保護計劃面板上:
   - 確認在 **[要備份的內容]** 中, 選擇 **[Google 雲端硬碟]** 項目。
   - 在 **[要備份的項目]** 中, 執行下列其中一項操作:
     - 保留預設設定 **[全部]** (所有檔案)。
     - 新增檔案和資料夾的名稱或路徑來指定要備份的檔案和資料夾。
       您可以使用萬用字元 (*、** 和 ?)。如需有關指定路徑和使用萬用字元的詳細資訊, 請參閱「檔案篩選器」。
     - 瀏覽來指定要備份的檔案和資料夾。
       只有在建立單一使用者的保護計劃時, 才可以使用 **[瀏覽]** 連結。

- [選用] 在 **[要備份的項目]** 中，按一下 **[顯示排除項目]** 來指定要在備份期間略過的檔案和資料夾。

  檔案排除項目會覆寫檔案選項，亦即，如果您在兩個欄位中指定相同的檔案，將會在備份期間略過這個檔案。
- 如果您要對選定備份的所有檔案啟用公證，請啟用 **[公證]** 開關。如需公證的詳細資訊，請參閱「公證」。

復原 Google 雲端硬碟和 Google 雲端硬碟檔案

復原整個 Google 雲端硬碟

1. 按一下 **[Google Workspace]**。
2. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，請選取您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原其 Google 雲端硬碟的使用者，然後按一下 **[復原]**。

   如果使用者遭到刪除，請在 [備份儲存] 索引標籤的 **[雲端應用程式備份]** 區段中選取該使用者，然後按一下 **[顯示備份]**。

   您可以按名稱搜尋使用者。不支援萬用字元。
4. 選擇復原點

   注意事項

   若只要查看含有 Google 雲端硬碟檔案的復原點，請在 **[依內容篩選]** 中選取 **[Google 雲端硬碟]**。
5. 按一下 **[復原]** > **[整個雲端硬碟]**。
6. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，按一下 **[Google Workspace 組織]** 可檢視、變更或指定目標組織。

   預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須從可用的已登錄組織中選擇一個新的目標組織。
7. 在 **[復原至磁碟機]** 中，檢視、變更或指定目標使用者或目標共用磁碟機。

   預設會選取原始使用者。如果此使用者不存在或選取了非原始組織，則必須指定目標使用者或目標共用磁碟機。

   如果備份中含有共用檔案，則檔案將會復原到目標磁碟機的 root 資料夾。
8. 選取是否要復原檔案的共用權限。
9. 按一下 **[開始復原]**。

10. 選取其中一個覆寫選項：

選項	描述
如果較舊，請覆寫現有的檔案	如果在目的地位置有一個具有相同名稱的檔案，且其比來源檔案還舊，則會將來源檔案儲存在目的地位置，取代較舊的版本。
覆寫現有的檔案	無論上次修改日期為何，目的地位置中的所有現有檔案都會遭到覆寫。
不要覆寫現有檔案	如果目的地位置中包含具有相同名稱的檔案，則不會對其套用任何變更，而且來源檔案不會儲存到目的地位置。

11. 按一下 **[繼續]** 可確認您的決定。

復原 Google 雲端硬碟檔案

1. 按一下 **[Google Workspace]**。
2. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，請選取您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原其 Google 雲端硬碟檔案的使用者，然後按一下 **[復原]**。

   如果使用者遭到刪除，請在 [備份儲存] 索引標籤的 **[雲端應用程式備份]** 區段中選取該使用者，然後按一下 **[顯示備份]**。

   您可以按名稱搜尋使用者。不支援萬用字元。
4. 選擇復原點

   注意事項

   若只要查看含有 Google 雲端硬碟檔案的復原點，請在 **[依內容篩選]** 中選取 **[Google 雲端硬碟]**。
5. 按一下 **[復原]** > **[檔案/資料夾]**。
6. 瀏覽至所需的資料夾，或使用搜尋以取得所需檔案和資料夾的清單。
7. 選擇您要復原的檔案。

   如果備份未經加密而且您選擇單一檔案，您可以按一下 **[顯示版本]** 來選取要復原的檔案版本。您可以選取早於或晚於所選復原點的任何備份版本。
8. 如果您要下載檔案，請選擇該檔案，按一下 **[下載]**，選擇儲存資料的位置，然後按一下 **[儲存]**。否則，請跳過此步驟。
9. 按一下 **[復原]**。
10. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，按一下 **[Google Workspace 組織]** 可檢視、變更或指定目標組織。

    預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須從可用的已登錄組織中選擇一個新的目標組織。
11. 在 **[復原至磁碟機]** 中，檢視、變更或指定目標使用者或目標共用磁碟機。

    預設會選取原始使用者。如果此使用者不存在或選取了非原始組織，則必須指定目標使用者或目標共用磁碟機。

12. 在 **[路徑]** 中，檢視或變更目標使用者 Google 雲端硬碟或目標共用磁碟機中的目標資料夾。預設會選取原始位置。
13. 選取是否要復原檔案的共用權限。
14. 按一下 **[開始復原]**。
15. 選擇其中一個檔案覆寫選項：

選項	描述
如果較舊，請覆寫現有的檔案	如果在目的地位置有一個具有相同名稱的檔案，且其比來源檔案還舊，則會將來源檔案儲存在目的地位置，取代較舊的版本。
覆寫現有的檔案	無論上次修改日期為何，目的地位置中的所有現有檔案都會遭到覆寫。
不要覆寫現有檔案	如果目的地位置中包含具有相同名稱的檔案，則不會對其套用任何變更，而且來源檔案不會儲存到目的地位置。

16. 按一下 **[繼續]** 可確認您的決定。

保護共用磁碟機檔案

哪些項目可以備份？

您可以備份整個共用磁碟機或個別的檔案和資料夾。檔案會與其共用權限一起備份。

重要事項
[與我共用] 資料夾不會備份。

限制

- 由於 Google Drive API 的限制，無法備份不含成員的共用磁碟機。
- 非 Google 專屬檔案格式、Google 文件、Google 試算表和 Google 簡報都完整支援備份和復原。其他 Google 專屬格式可能未受到完整支援或可能完全不受支援，例如，Google 繪圖檔案會復原為 `.svg` 檔案、Google 協作平台網站會復原為 `.txt` 檔案、Google Jamboard 檔案會復原為 `.pdf` 檔案，而 Google 我的地圖檔案在備份期間則會被略過。

  注意事項
  非 Google 專屬的檔案格式 (例如 `.txt`、`.docx`、`.pptx`、`.pdf`、`.jpg`、`.png`、`.zip`) 則完整支援備份和復原。

可以復原哪些項目？

您可以復原整個共用磁碟機或已備份的任何檔案或資料夾。

您可以選擇要復原共用權限，還是讓檔案繼承復原目標資料夾的權限。

系統不會復原下列項目：

- 如果目標共用磁碟機中停用了在組織外部共用，則不會復原與組織外部使用者共用之檔案的共用權限。

- 如果目標共用磁碟機中停用了 **[與非成員共用]**，則不會復原與非目標共用磁碟機成員的使用者共用之檔案的共用權限。

限制

- 系統不會復原檔案中的註解。
- 檔案與資料夾的共用連結不會復原。

選擇共用磁碟機檔案

如下所述選擇檔案，然後視需要指定保護計劃的其他設定。

若要選擇共用磁碟機檔案

1. 按一下 **[Google Workspace]**。
2. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，請選取您要備份其使用者資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
   - 若要備份所有共用磁碟機 (包括之後建立的共用磁碟機) 的檔案，展開 **[共用磁碟機]** 節點、選取 **[所有共用磁碟機]**，然後按一下 **[群組備份]**。
   - 若要備份個別共用磁碟機的檔案，展開 **[共用磁碟機]** 節點、選取 **[所有共用磁碟機]**、選取您要備份的共用磁碟機，然後按一下 **[備份]**。
4. 在保護計劃面板上：
   - 在 **[要備份的項目]** 中，執行下列其中一項操作：
     - 保留預設設定 **[全部]** (所有檔案)。
     - 新增檔案和資料夾的名稱或路徑來指定要備份的檔案和資料夾。

       您可以使用萬用字元 (*、** 和 ?)。如需有關指定路徑和使用萬用字元的詳細資訊，請參閱「檔案篩選器」。
     - 瀏覽來指定要備份的檔案和資料夾。

       只有在建立單一共用磁碟機的保護計劃時，才可以使用 **[瀏覽]** 連結。
   - [選用] 在 **[要備份的項目]** 中，按一下 **[顯示排除項目]** 來指定要在備份期間略過的檔案和資料夾。

     檔案排除項目會覆寫檔案選項，亦即，如果您在兩個欄位中指定相同的檔案，將會在備份期間略過這個檔案。
   - 如果您要對選定備份的所有檔案啟用公證，請啟用 **[公證]** 開關。如需公證的詳細資訊，請參閱「公證」。

復原共用磁碟機和共用磁碟機檔案

復原整個共用磁碟機

1. 按一下 **[Google Workspace]**。
2. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，請選取您要復原其已備份資料的組織。否則，請跳過此步驟。

3. 展開 **[共用磁碟機]** 節點、選取 **[所有共用磁碟機]**、選取您要復原的共用磁碟機，然後按一下 **[復原]**。

   如果共用磁碟機遭到刪除，請在 [備份儲存] 索引標籤的 **[雲端應用程式備份]** 區段中選取該共用磁碟機，然後按一下 **[顯示備份]**。

   您可以按名稱搜尋共用磁碟機。不支援萬用字元。
4. 選擇復原點
5. 按一下 **[復原]** > **[整個共用磁碟機]**。
6. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，按一下 **[Google Workspace 組織]** 可檢視、變更或指定目標組織。

   預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須從可用的已登錄組織中選擇一個新的目標組織。
7. 在 **[復原至磁碟機]** 中，檢視、變更或指定目標共用磁碟機或目標使用者。如果您指定某個使用者，資料將會復原到此使用者的 Google 雲端硬碟。

   預設會選取原始共用磁碟機。如果此共用磁碟機不存在或選取了非原始組織，則必須指定目標共用磁碟機或目標使用者。
8. 選取是否要復原檔案的共用權限。
9. 按一下 **[開始復原]**。
10. 選取其中一個覆寫選項：

選項	描述
如果較舊，請覆寫現有的檔案	如果在目的地位置有一個具有相同名稱的檔案，且其比來源檔案還舊，則會將來源檔案儲存在目的地位置，取代較舊的版本。
覆寫現有的檔案	無論上次修改日期為何，目的地位置中的所有現有檔案都會遭到覆寫。
不要覆寫現有檔案	如果目的地位置中包含具有相同名稱的檔案，則不會對其套用任何變更，而且來源檔案不會儲存到目的地位置。

11. 按一下 **[繼續]** 可確認您的決定。

復原共用磁碟機檔案

1. 按一下 **[Google Workspace]**。
2. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，請選取您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 展開 **[共用磁碟機]** 節點、選取 **[所有共用磁碟機]**、選取包含您要復原之檔案的共用磁碟機，然後按一下 **[復原]**。

   如果共用磁碟機遭到刪除，請在 [備份儲存] 索引標籤的 **[雲端應用程式備份]** 區段中選取該共用磁碟機，然後按一下 **[顯示備份]**。

   您可以按名稱搜尋共用磁碟機。不支援萬用字元。
4. 選擇復原點
5. 按一下 **[復原]** > **[檔案/資料夾]**。
6. 瀏覽至所需的資料夾，或使用搜尋以取得所需檔案和資料夾的清單。

7. 選擇您要復原的檔案。

   如果備份未經加密而且您選擇單一檔案，您可以按一下 **[顯示版本]** 來選取要復原的檔案版本。您可以選取早於或晚於所選復原點的任何備份版本。
8. 如果您要下載檔案，請選擇該檔案，按一下 **[下載]**，選擇儲存資料的位置，然後按一下 **[儲存]**。否則，請跳過此步驟。
9. 按一下 **[復原]**。
10. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，按一下 **[Google Workspace 組織]** 可檢視、變更或指定目標組織。

    預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須從可用的已登錄組織中選擇一個新的目標組織。
11. 在 **[復原至磁碟機]** 中，檢視、變更或指定目標共用磁碟機或目標使用者。如果您指定某個使用者，資料將會復原到此使用者的 Google 雲端硬碟。

    預設會選取原始共用磁碟機。如果此共用磁碟機不存在或選取了非原始組織，則必須指定目標共用磁碟機或目標使用者。
12. 在 **[路徑]** 中，檢視或變更目標共用磁碟機或目標使用者 Google 雲端硬碟中的目標資料夾。預設會選取原始位置。
13. 選取是否要復原檔案的共用權限。
14. 按一下 **[開始復原]**。
15. 選擇其中一個檔案覆寫選項：

選項	描述
如果較舊，請覆寫現有的檔案	如果在目的地位置有一個具有相同名稱的檔案，且其比來源檔案還舊，則會將來源檔案儲存在目的地位置，取代較舊的版本。
覆寫現有的檔案	無論上次修改日期為何，目的地位置中的所有現有檔案都會遭到覆寫。
不要覆寫現有檔案	如果目的地位置中包含具有相同名稱的檔案，則不會對其套用任何變更，而且來源檔案不會儲存到目的地位置。

16. 按一下 **[繼續]** 可確認您的決定。

公證

公證讓您證明檔案在備份後即是真實和未變更的。建議您在備份法律檔案或需要證明真實性的任何其他檔案時啟用公證。

公證僅適用於 Google 雲端硬碟檔案和 Google Workspace 共用磁碟機檔案的備份。

如何使用公證

若要對選定備份的所有檔案啟用公證，建立保護計劃時，請啟用 **[公證]** 開關。

在設定復原時，公證檔將標記有特殊圖示，並且您可以 [驗證檔案真實性]。

運作原理

在備份過程中，代理程式會計算備份檔案的雜湊代碼，組建雜湊樹狀結構 (基於資料夾結構)，儲存備份中的樹狀結構，然後將雜湊樹狀結構根部發送給公證服務。公證服務將雜湊樹狀結構根部儲存在 Ethereum 區塊鏈資料庫中，以確保此值不會變更。

在驗證檔案真實性時，代理程式會計算檔案雜湊，然後將其與儲存在備份內雜湊樹狀結構中的雜湊相比較。若這些雜湊不相符，則檔案被視為不真實。否則，由雜湊樹狀結構保證檔案的真實性。

若要驗證雜湊樹狀結構自身未受損，代理程式會將雜湊樹狀結構根部發送給公證服務。公證服務將其與儲存在區塊鏈資料庫中的雜湊相比較。若雜湊相符，則所選檔案保證為真實的。否則，軟體會顯示一則訊息，指示檔案不真實。

向 Notary Service 驗證檔案真實性

如果備份期間啟用公證，則可驗證備份檔案的真實性。

要驗證檔案的真實性

1. 執行下列其中一項操作：
   - 若要驗證 Google 雲端硬碟檔案的真實性，請選擇檔案，如「復原 Google 雲端硬碟檔案」一節的步驟 1-7 所述。
   - 若要驗證 Google Workspace 共用磁碟機檔案的真實性，請選擇檔案，如「復原共用磁碟機檔案」一節的步驟 1-7 所述。
2. 確保所選檔案標記有下列圖示：  。這表示檔案已公證。
3. 執行下列其中一項操作：
   - 按一下**驗證**。

     軟體會檢查檔案真實性並顯示結果。
   - 按一下**取得憑證**。

     確認檔案公證的憑證會在 Web 瀏覽器視窗中開啟。該視窗還包含了容許您手動驗證檔案真實性的說明。

在雲端對雲端備份中搜尋

復原資料時，您可以搜尋特定的備份項目，而不是瀏覽備份存檔。

在未加密的備份中，一律可以使用搜尋。只支援增強的 (以索引為基礎) 搜尋。

以索引為基礎的搜尋更快速，而且提供其他選項，例如，顯示已備份項目的版本、在附件名稱中搜尋，以及在 Gmail 備份中進行全文檢索。

全文檢索

全文檢索僅適用於 Gmail 備份，且預設為啟用狀態。透過此功能，您可以在備份的電子郵件內文中進行搜尋。如果此選項遭到停用，您只能依主旨，寄件者，收件者和日期進行搜尋。

全文檢索索引佔用了 Gmail 備份儲存空間的 10 到 30%。沒有全文檢索的索引明顯小很多。為了節省儲存空間，您可以停用全文檢索，並清除包含全文檢索資料的索引部分。

搜尋索引

索引可在雲端對雲端備份存檔中提供增強的搜尋功能。

每次備份作業後，存檔就會自動編列索引。編列索引過程不會影響備份效能，因為編列索引和備份是由不同的軟體元件所完成。

索引編列作業完成後即可顯示搜尋結果，最多可能需要 24 小時。為第一個備份 (即完整備份) 編列索引通常比為後續的增量備份編列索引需要更長的時間。

所有索引均包含支援主要搜尋功能 (依主旨、寄件者、收件者或日期搜尋) 的中繼資料。如果啟用全文檢索，則 Gmail 備份的索引將包含額外的資料。

檢查搜尋索引的大小

搜尋索引會隨著時間而變得越來越大。啟用全文檢索的備份存檔的索引最多可能佔用存檔大小的 30%。

若要檢查搜尋索引的大小

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 在 **[備份儲存]** 索引標籤上，按一下 **[雲端應用程式備份]**。
3. 檢查 **[索引大小]** 欄的值。

更新、重建或刪除索引

若要在雲端對雲端備份中對搜尋相關問題進行疑難排解，您可以更新、重建或刪除搜尋索引。

注意事項
建議您在更新、重建或刪除索引之前，聯絡支援團隊。

若要更新、重建或刪除索引

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 在 **[備份儲存]** 索引標籤上，按一下 **[雲端應用程式備份]**。
   選擇您想要更新、重建或刪除其索引的存檔。
   這些動作是否可用取決於系統管理員層級和角色，如下所示：

帳戶層級	角色	可以更新索引	可以重建索引	可以刪除索引
合作夥伴租用戶	公司系統管理員	+	+	+
	Protection 網路系統管理員	+	-	-
	Protection 系統管理員	+	-	-
	Protection 唯讀系統管理員	-	-	-
客戶租用戶	公司系統管理員	+	-	-
	Protection 系統管理員	+	-	-
	Protection 唯讀系統管理員	-	-	-
單位	單位系統管理員	+	-	-
	Protection 系統管理員	+	-	-
	Protection 唯讀系統管理員	-	-	-

3. 在 **[動作]** 窗格中，選擇您要執行的動作：
   - **更新索引** — 檢查存檔中的復原點，並新增缺少的索引。
   - **重建索引** —刪除存檔中所有復原點的索引，然後再次建立索引。
   - **刪除索引** —刪除存檔中所有復原點的索引。
4. 選擇動作的範圍，然後按一下 **[確定]**。
   根據存檔和所選動作，以下可能有一個或多個選項可供使用：
   - **僅限中繼資料**
   - **僅限內容**
   - **中繼資料和內容搜尋**

停用 Gmail 備份的全文檢索

全文檢索僅適用於 Gmail 備份，且預設為啟用狀態。透過此功能，您可以在備份的電子郵件內文中進行搜尋。如果此選項遭到停用，您只能依主旨，寄件者，收件者和日期進行搜尋。

如果您需要保持最小搜尋索引的大小，可能需要停用全文檢索。

若要停用全文檢索

1. 建立或編輯備份計劃時，按一下右上角的齒輪圖示。
2. 在 **[全文檢索]** 索引標籤上，停用開關。
3. 按一下**[完成]**。
4. [建立計劃時] 按一下 **[套用]**。
5. [編輯計劃時] 按一下 **[儲存設定]**。

注意事項
如果您重新啟用全文檢索，此備份計劃建立的所有存檔將再次編列索引。這是一個耗時的作業。

保護 Oracle 資料庫

注意事項
此功能適用於 Advanced Backup 套件。

對 Oracle Database 的保護詳述於另一個文件中：https://dl.managed-protection.com/u/pdf/OracleBackup_whitepaper_en-US.pdf

保護 SAP HANA

注意事項
此功能適用於 Advanced Backup 套件。

SAP HANA 的保護詳述於可在 https://dl.managed-protection.com/u/pdf/SAP_HANA_backup_whitepaper_en-US.pdf 取得的另一份文件

保護 MySQL 和 MariaDB 資料

您可以使用應用程式感知備份來保護 MySQL 或 MariaDB 資料。它會收集應用程式中繼資料，並允許在執行個體、資料庫或資料表層級上的細微復原。

注意事項
MySQL 或 MariaDB 資料的應用程式感知備份可在 Advanced Backup 套件取得。

若要使用應用程式感知備份來保護執行 MySQL 或 MariaDB 執行個體的實體或虛擬機器，您必須在此電腦上安裝 MySQL/MariaDB 用代理程式。MySQL/MariaDB 用代理程式是與 Linux 用代理程式 (64 位元) 一起搭售，因此僅能安裝在 64 位元的 Linux 作業系統上。請參閱 "支援的作業系統和環境" (第 22 頁)。

若要下載 Linux 用代理程式 (64 位元) 安裝檔案

1. 登入 Cyber Protect 主控台。
2. 按一下右上角的帳戶圖示，然後選擇 **[下載]**。
3. 按一下 **[Linux 用代理程式 (64 位元)]**。

   安裝檔案會下載到您的電腦中。若要安裝代理程式，請依照 "在 Linux 中安裝保護代理程式" (第 74 頁) 或 "在 Linux 中安裝和解除安裝保護代理程式" (第 93 頁) 中的描述繼續進行。確認您選擇 MySQL/MariaDB 用代理程式，這是一個選擇性元件。

   若要將資料庫和資料表復原至執行中的執行個體，則 MySQL/MariaDB 用代理程式需要臨時存放區才能運作。預設會使用 `/tmp` 目錄。您可以透過設定 `ACRONIS_MYSQL_RESTORE_DIR` 環境變數來變更此目錄。

限制

- 不支援 MySQL 或 MariaDB 叢集。
- 不支援 Docker 容器中執行的 MySQL 或 MariaDB 執行個體。
- 不支援在使用 BTRFS 檔案系統之作業系統上執行的 MySQL 或 MariaDB 執行個體。
- 系統資料庫 (`sys`、`mysql`、`information-schema` 和 `performance_schema`) 和不包含任何資料表的資料庫無法復原至執行中的執行個體。不過，當復原整個執行個體時，這些資料庫可以復原為檔案。
- 復原僅支援與備份執行個體相同版本或更新版本的目標執行個體，並有以下限制：
  - 不支援從 MySQL 5.x 執行個體復原至 MySQL 8.x 執行個體。
  - 只有透過將整個執行個體復原為檔案的方式，才支援復原至更新的 MySQL 5.x 版本 (包括次要版本)。在嘗試復原之前，請參考官方 MySQL 升級指南以瞭解目標版本，例如 MySQL 5.7 升級指南。
- 不支援從儲存在 Secure Zone 上的備份復原。
- 在已安裝 AppArmor 的電腦上執行的 MySQL/MariaDB 用代理程式無法復原資料庫和資料表。您仍然可將執行個體復原為檔案，或整個電腦。
- 不支援復原至使用符號連結設定的目標資料庫。您可將備份資料庫復原為新資料庫，方法是變更其名稱。

已知問題

如果在從密碼保護的 Samba 共用復原資料時碰到問題，請登出 Cyber Protect 主控台，然後再登入回去。選擇想要的復原點，然後按一下 **[MySQL/MariaDB 資料庫]**。請勿按下 **[整部電腦]** 或 **[檔案/資料夾]**。

設定應用程式感知備份

必要條件

- 所選電腦上至少必須執行一個 MySQL 或 MariaDB 執行個體。
- 在執行 MySQL 或 MariaDB 執行個體的電腦上，保護代理程式必須在 root 使用者下啟動。
- 只有在保護計劃選擇 **[整部電腦]** 作為備份來源時，才可使用應用程式感知備份。
- 保護計劃中務必停用 **[逐一磁區]** 備份選項。否則，無法復原應用程式資料。

若要設定應用程式感知備份

1. 在 Cyber Protect 主控台中，選擇一或多部執行 MySQL 或 MariaDB 執行個體的電腦。
   每部電腦上可以有一或多個執行個體。
2. 在啟用備份模組的情況下，建立一個保護計劃。
3. 在 **[要備份的內容]** 中選擇 **[整部電腦]**。
4. 按一下 **[應用程式備份]**，然後啟用 **[MySQL/MariaDB Server]** 旁邊的開關。
5. 選擇如何指定 MySQL 或 MariaDB 執行個體：

- **對於所有工作負載**

  如果您在多部伺服器上執行具有相同設定的執行個體，請使用此選項。所有執行個體都將使用相同的連線參數和存取認證。
- **針對特定工作負載**

  使用此選項來指定每個執行個體的連線參數和存取認證。

6. 按一下 **[新增執行個體]** 以設定連線參數和存取認證。
   a. 選擇連線類型，然後指定下列各項：
      - [針對 TCP 通訊端] IP 位址和連接埠。
      - [針對 Unix 通訊端] 通訊端路徑。
   b. 指定具備下列執行個體權限的使用者帳戶認證：
      - `FLUSH_TABLES` 或 `RELOAD`，針對所有資料庫和資料表 (`*.*`)
      - `SELECT`，針對 `information_schema.tables`
   c. 按一下 **[確定]**。
7. 按一下**[完成]**。

從應用程式感知備份復原資料

您可以從應用程式感知備份復原 MySQL 或 MariaDB 執行個體、資料庫和資料表。您還可復原執行執行個體的整個伺服器，或從此伺服器復原檔案和資料夾。

下表摘要所有復原選項。

復原內容	復原為	復原至
MySQL Server MariaDB Server	整部電腦	已安裝 Linux 用代理程式的電腦*
MySQL Server MariaDB Server	檔案或資料夾	已安裝 Linux 用代理程式的電腦*
執行個體	檔案	已安裝 MySQL/MariaDB 用代理程式的電腦*
資料庫	相同資料庫 新資料庫	已安裝 MySQL/MariaDB 用代理程式的電腦* • 原始執行個體 • 其他執行個體 • 原始資料庫 • 新資料庫
Table	相同資料表 新資料表	已安裝 MySQL/MariaDB 用代理程式的電腦* • 原始執行個體 • 其他執行個體 • 原始資料庫 • 原始資料表

復原內容	復原為	復原至
		• 新資料表

* 從備份觀點來看，內部具有代理程式的虛擬機器會被視為實體機器。

復原整個伺服器

若要瞭解如何復原正在執行 MySQL 或 MariaDB 執行個體的整個伺服器，請參閱 "復原電腦" (第 445 頁)。

復原執行個體

您可以從應用程式感知備份，將 MySQL 或 MariaDB 執行個體復原為檔案。

若要復原執行個體

1. 在 Cyber Protect 主控台中，選擇原本存放所要復原之資料的電腦。
2. 按一下 **[復原]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。
   如果電腦處於離線狀態，復原點就不會顯示。執行下列其中一項操作：
   - 如果備份位置是雲端或共用儲存 (即可被其他代理程式存取)，按一下 **[選擇電腦]**，選擇有 MySQL/MariaDB 用代理程式的線上電腦，然後選擇復原點。
   - 在 **[備份儲存]** 索引標籤上選擇復原點。

   依照上述動作任一而選擇瀏覽的電腦，將成為復原的目標電腦。
4. 按一下 **[復原]** > **[MySQL/MariaDB 資料庫]**。
5. 選擇您要復原的執行個體，然後按一下 **[復原為檔案]**。
6. 在 **[路徑]** 底下，選擇將要復原檔案的目標目錄。
7. 按一下 **[開始復原]**。

復原資料庫

您可以從應用程式感知備份，將資料庫復原至執行中的 MySQL 或 MariaDB 執行個體。

1. 在 Cyber Protect 主控台中，選擇原本存放所要復原之資料的電腦。
2. 按一下 **[復原]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。
   如果電腦處於離線狀態，復原點就不會顯示。執行下列其中一項操作：
   - 如果備份位置是雲端或共用儲存 (即可被其他代理程式存取)，按一下 **[選擇電腦]**，選擇有 MySQL/MariaDB 用代理程式的線上電腦，然後選擇復原點。
   - 在 **[備份儲存]** 索引標籤上選擇復原點。

   依照上述動作任一而選擇瀏覽的電腦，將成為復原的目標電腦。
4. 按一下 **[復原]** > **[MySQL/MariaDB 資料庫]**。
5. 按一下所需的執行個體名稱，以向下鑽研至其資料庫。

6. 請選擇您要復原的一或多個資料庫。
7. 按一下 **[復原]**。
8. 按一下 **[目標 MySQL/MariaDB 執行個體]** 以指定目標執行個體的連線參數和存取認證。
   - 驗證您要復原資料的目標執行個體。預設會選擇原始執行個體。
   - 指定可存取目標執行個體的使用者帳戶認證。此使用者帳戶必須具備為所有資料庫和資料表 (*.*) 指派的下列權限：
     - INSERT
     - CREATE
     - DROP
     - LOCK_TABLES
     - ALTER
     - SELECT
   - 按一下 **[確定]**。
9. 驗證目標資料庫。

   預設會選擇原始資料庫。

   若要將資料庫復原為新資料庫，請按一下目標資料庫名稱，然後加以變更。此動作僅適用於復原單一資料庫時。
10. 在 **[覆寫現有的資料庫]** 底下，選擇覆寫模式。

    依預設，會啟用覆寫，而且備份資料庫會取代名稱相同的目標資料庫。

    如果停用覆寫，在復原作業期間會略過備份資料庫，而且不會取代名稱相同的目標資料庫。
11. 按一下 **[開始復原]**。

復原資料表

您可以從應用程式感知備份，將資料表復原至執行中的 MySQL 或 MariaDB 執行個體。

1. 在 Cyber Protect 主控台中，選擇原本存放所要復原之資料的電腦。
2. 按一下 **[復原]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。

   如果電腦處於離線狀態，復原點就不會顯示。執行下列其中一項操作：
   - 如果備份位置是雲端或共用儲存 (即可被其他代理程式存取)，按一下 **[選擇電腦]**，選擇有 MySQL/MariaDB 用代理程式的線上電腦，然後選擇復原點。
   - 在 **[備份儲存]** 索引標籤上選擇復原點。

   依照上述動作任一而選擇瀏覽的電腦，將成為復原的目標電腦。
4. 按一下 **[復原]** > **[MySQL/MariaDB 資料庫]**。
5. 按一下所需的執行個體名稱，以向下鑽研至其資料庫。
6. 按一下所需的資料庫名稱，以向下鑽研至其資料表。
7. 請選擇您要復原的一或多個資料表。
8. 按一下 **[復原]**。
9. 按一下 **[目標 MySQL/MariaDB 執行個體]** 以指定目標執行個體的連線參數和存取認證。

- 驗證您要復原資料的目標執行個體。預設會選擇原始執行個體。
- 指定可存取目標執行個體的使用者帳戶認證。此使用者帳戶必須具備為所有資料庫和資料表 (*.*) 指派的下列權限：
  - INSERT
  - CREATE
  - DROP
  - LOCK_TABLES
  - ALTER
  - SELECT
- 按一下 **[確定]**。

10. 驗證目標資料表。

    預設會選擇原始資料表。

    若要將資料表復原為新資料表，請按一下目標資料表名稱，然後加以變更。此動作僅適用於復原單一資料表時。

11. 在 **[覆寫現有的資料表]** 下方，選擇覆寫模式。

    依預設，會啟用覆寫，而且備份資料表會取代名稱相同的目標資料表。

    如果停用覆寫，在復原作業期間會略過備份資料表，而且不會取代名稱相同的目標資料表。

12. 按一下 **[開始復原]**。

復原預存常式

當您復原整個 MySQL 執行個體時，會自動復原預存常式。

當您將個別的資料庫復原到非原始執行個體，或將其當作新資料庫復原時，不會自動復原預存常式。您可以手動復原預存常式，只要在 SQL 檔案中匯出預存常式，然後將其新增到復原的資料庫中即可。

若要匯出預存常式並將其新增至復原的資料庫

1. 在具有原始 MySQL 執行個體的電腦上，開啟終端機。
2. 執行以下命令來匯出預存常式。
3. ```
   mysqldump -p [source_database_name] --routines --no-create-info --no-data >
   [exported_db_routines.sql]
   ```
4. 在復原資料庫的電腦上，開啟 MySQL 命令列用戶端。
5. 執行以下命令，將常式新增到復原的資料庫中。

   ```
   mysql>  use [recovered_database_name];
   ```

   ```
   mysql>  source [path_to_exported_db_routines.sql];
   ```
   ```

保護網站和託管伺服器

保護網站

未經授權的存取或惡意程式碼攻擊，可能導致網站損毀。如果希望在發生損毀狀況時輕鬆還原其健康狀態，請備份您的網站。

備份網站需要什麼？

網站必須能透過 SFTP 或 SSH 通訊協定存取。您不需要安裝代理程式，只要按本節稍後所述新增網站即可。

哪些項目可以備份？

您可備份下列項目：

- **網站內容檔案**
  您針對 SFTP 或 SSH連線所指定的帳戶可存取的所有檔案。
- **MySQL 伺服器上已連結的資料庫 (如果有的話)。**
  您指定的 MySQL 帳戶可存取的所有資料庫。

如果您的網站採用資料庫，我們建議您備份檔案和資料庫，以便將它們復原為一致的狀態。

限制

- 網站備份可用的唯一備份位置是雲端儲存空間。
- 您可以將數個保護計劃套用至一個網站，但其中只有一個保護計劃可以依排程執行。其他計劃必須手動啟動。
- 唯一可用的備份選項為 [備份檔案名稱]。
- 網站保護計劃不會顯示在 **[管理]** > **[保護計劃]** 索引標籤上。

備份網站

若要新增網站

1. 按一下 **[裝置]** > **[新增]**。
2. 按一下**[網站]**。
3. 為網站設定下列存取設定：
   - 在 **[網站名稱]** 中，建立及輸入網站名稱。此名稱將顯示在 Cyber Protect 主控台中。
   - 在 **[主機]** 中，指定要用來透過 SFTP 或 SSH 存取網站的主機名稱或 IP 位址。例如，`my.server.com` 或 `10.250.100.100`。
   - 在 **[連接埠]**，指定連接埠號碼。
   - 在 **[使用者名稱]** 和 **[密碼]** 中，指定可用來透過 SFTP 或 SSH 存取網站的帳戶的認證。

重要事項
只會備份指定帳戶可存取的檔案。

除了密碼，也可以指定私密 SSH 金鑰。若要這麼做，請選擇 **[使用 SSH 私密金鑰而非密碼]** 核取方塊，然後指定金鑰。

4. 按 **[下一步]**。
5. 如果您的網站使用 MySQL資料庫，請設定資料庫的存取設定。否則，請按一下 **[略過]**。
   a. 在 **[連線類型]** 中，選則如何從雲端存取資料庫：
      - **[透過 SSH 來源主機]**— 將透過步驟 3 終止定的主機存取資料庫。
      - **[直接連線]**— 直接存取資料庫。僅當可從網際網路存取資料庫時，才選擇此設定。
   b. 在 **[主機]** 中，指定執行 MySQL 伺服器的主機的名稱或 IP 位址。
   c. 在 **[連接埠]** 中，指定與伺服器的 TCP/IP 連線的連接埠號碼。預設的連接埠號碼是 3306。
   d. 在 **[使用者名稱]** 及 **[密碼]** 中指定 MySQL 帳戶認證。

   重要事項
   只會備份指定帳戶可存取的資料庫。

   e. 按一下 **[建立]**。

   此網站將會出現在 Cyber Protect 主控台的 **[裝置]** > **[網站]** 底下。

若要變更連線設定

1. 在 **[裝置]** > **[網站]** 下選擇網站。
2. 按一下**[詳細資料]**。
3. 按一下網站或資料庫連線設定旁的鉛筆圖示。
4. 進行必要的變更，然後按一下 **[儲存]**。

建立網站的保護計劃

1. 在 **[裝置]** > **[網站]** 下選擇一個或數個網站。
2. 按一下 **[保護]**。
3. [選用] 啟用資料庫備份。

   如果選擇數個網站，則預設會停用資料庫備份。
4. [選用] 變更保留規則。
5. [選用] 啟用備份的加密。
6. [選用] 按一下齒輪圖示以編輯 **[備份檔案名稱]** 選項。這在兩個情況下是可行的：
   - 如果您稍早備份此網站，而且想要繼續現有的備份順序
   - 如果您想要在 **[備份儲存]** 索引標籤上看到自訂名稱
7. 按一下**[套用]**。

您可以按照與電腦相同的方式，編輯、撤消和刪除網站的保護計劃。這些作業將詳述於「保護計劃相關操作」中。

復原網站

若要復原網站

1. 執行下列其中一項操作：
   - 在 **[裝置]** > **[網站]** 下選擇您要復原的網站，然後按一下 **[復原]**。
     您可以按名稱搜尋網站。不支援萬用字元。
   - 如果網站遭到刪除，請在 [備份儲存] 索引標籤的 **[雲端應用程式備份]** 區段中選取該網站，然後按一下 **[顯示備份]**。
     若要復原已刪除的網站，您必須將目標網站當做裝置新增。
2. 選擇復原點。
3. 按一下 **[復原]**，然後選擇您要復原哪些內容：**[整個網站]**、**[資料庫]**(如果有的話)，或 **[檔案/資料夾]**。
   為確保您的網站處於一致狀態，建議您同時復原檔案和資料庫，順序不限。
4. 視您的選擇而定，請遵照以下所述的其中一個程序。

若要復原整個網站

1. 在 **[復原到網站]** 中，檢視或變更目標網站。
   預設會選取原始網站。如果原始網站不存在，您必須選取目標網站。
2. 選取是否要復原已復原項目的共用權限。
3. 按一下 **[開始復原]**，然後確認動作。

若要復原資料庫

1. 請選擇您要復原的資料庫。
2. 如果您要將資料庫當做檔案下載，請按一下 **[下載]**，選擇儲存檔案的位置，然後按一下 **[儲存]**。
   否則，請跳過此步驟。
3. 按一下 **[復原]**。
4. 在 **[復原到網站]** 中，檢視或變更目標網站。
   預設會選取原始網站。如果原始網站不存在，您必須選取目標網站。
5. 按一下 **[開始復原]**，然後確認動作。

若要復原網站檔案/資料夾

1. 選擇您要復原的檔案/資料夾。
2. 如果您要儲存檔案，請按一下 **[下載]**，選擇儲存檔案的位置，然後按一下 **[儲存]**。否則，請跳過此步驟。
3. 按一下 **[復原]**。
4. 在 **[復原到網站]** 中，檢視或變更目標網站。
   預設會選取原始網站。如果原始網站不存在，您必須選取目標網站。
5. 選取是否要復原已復原項目的共用權限。
6. 按一下 **[開始復原]**，然後確認動作。

保護 Web 託管伺服器

您可以保護執行 Plesk、cPanel、DirectAdmin、VirtualMin 或 ISPManager 控制面板的 Linux 型 Web 託管伺服器。執行其他廠商的 Web 託管控制面板的伺服器會當作一般工作負載受到保護。

配額

執行 Plesk、cPanel、DirectAdmin、VirtualMin 或 ISPManager 控制面板的伺服器會被視為 Web 託管伺服器。每部備份的 Web 託管伺服器都會耗用 **Web 託管伺服器**配額。如果此配額遭到停用，或超過此配額的超額，將會按如下方式指派配額，或者備份將會失敗：

- 如果是實體伺服器，將會使用**伺服器**配額。如果此配額遭到停用，或超過此配額的超額，備份將會失敗。
- 如果是虛擬伺服器，將會使用**虛擬機器**配額。如果此配額遭到停用，或超過此配額的超額，備份將會失敗。

DirectAdmin、cPanel 和 Plesk 的整合

使用 DirectAdmin、Plesk 或 cPanel 的 Web 託管系統管理員可以將這些控制台與 Cyber Protection 服務整合在一起，以獲得數個強大功能，包括：

- 使用磁碟層級備份，將整部 Web 託管伺服器備份到雲端儲存空間
- 復原整部伺服器，包括所有網站和帳戶
- 針對帳戶、網站、個別檔案、信箱或資料庫，執行細微復原和下載
- 讓經銷商和客戶對自己的資料，執行自助復原

若要執行整合，您需要使用 Cyber Protection 服務擴充功能。如需詳細資訊，請參閱對應的整合指南：

- DirectAdmin 整合指南
- WHM 和 cPanel 整合指南
- Plesk 整合指南

虛擬機器的特殊作業

從備份執行虛擬機器(立即復原)

您可以從含有作業系統的磁碟層級備份執行虛擬機器。此作業又稱為立即還原，可讓您在數秒間加速虛擬伺服器。系統可直接從備份模擬虛擬磁碟，因此不會占用資料存放區的空間 (儲存空間)。儲存空間僅需要保留變更至虛擬磁碟。

建議您讓這個臨時虛擬機器最多執行三天。然後可以完全移除或轉換為一般虛擬機器 (最終化) 毋需停機時間。

只要臨時虛擬機器存在，該電腦所使用的備份就不適用保留規則。原始電腦的備份可以繼續執行。

使用範例

- **災難復原**

  立即讓故障電腦複本上線。
- **測試備份**

  從備份執行電腦並確保客體 OS 和應用程式均運作正常。
- **存取應用程式資料**

  在電腦執行時，使用應用程式原生管理工具存取和擷取所需的資料。

必要條件

- 必須至少有一個 VMware 用代理程式或 Hyper-V 用代理程式在 Cyber Protection 服務中註冊。
- 備份可以儲存在網路資料夾或已安裝 VMware 用代理程式或 Hyper-V 用代理程式的電腦本機資料夾中。如果您選擇網路資料夾，則必須可以從該電腦存取。虛擬機器亦可從儲存在雲端儲存的備份執行，但速度較慢，因為這項作業需要從備份進行密集隨機存取讀取。
- 備份必須包含足以讓作業系統啟動的整個電腦或是所有磁碟區。
- 實體機器和虛擬機器的備份均可以使用。Virtuozzo 容器的備份不可使用。
- 含有 Linux 邏輯磁碟區 (LVM) 的備份必須透過 VMware 用代理程式或 Hyper-V 用代理程式建立。虛擬機器與原始電腦 (ESXi 或 Hyper-V) 的類型必須相同。

執行電腦

1. 執行下列其中一項操作：
   - 選擇已備份的電腦，按一下**復原**，然後選擇復原點。
   - 在 [備份儲存] 索引標籤上選擇復原點。
2. 按一下 **[以 VM 的身分執行]**。

   軟體會自動選擇主機與其他所需的參數。
3. [選用] 按一下 **[目標電腦]**，然後變更虛擬機器類型 (ESXi 或 Hyper-V)、主機或虛擬機器名稱。
4. [選用] 為 ESXi 按一下 **[資料存放區]**，或為 Hyper-V 按一下 **[路徑]**，然後選擇虛擬機器的資料存放區。

   電腦執行時，虛擬磁碟的變更會累積。請確定選擇的資料存放區有足夠的可用空間。如果您打算透過設為永久虛擬機器來保留這些變更，請選取適合實際執行電腦的資料存放區。
5. [選用] 按一下 **[VM 設定]** 來變更虛擬機器的記憶體大小與網路連線。
6. [選用] 選擇 VM 電源狀態 (**[開啟]**/**[關閉]**)。
7. 按一下 **[立即執行]**。

如此一來，電腦會顯示在 Web 介面中，並具有下列其中一個圖示：  或 

。您不能選擇備份這類虛擬機器。

注意事項

您可以使用 Microsoft Azure 中的備份，執行 [以虛擬機器身分執行] (Instant Restore) 作業。但是，此作業會產生大量出口流量，這些流量將會新增至您的 Microsoft Azure 訂購授權帳單。對於從 Microsoft Azure 備份執行的 Windows 電腦，其典型出口流量約為從虛擬機器啟動到登入的 5 GB。

刪除電腦

建議您不要直接在 vSphere/Hyper-V 中刪除臨時虛擬機器，這可能會導致在 Web 介面中產生成品。此外，執行電腦的備份可能會暫時鎖住 (無法藉由保留規則加以刪除)。

欲刪除從備份執行的虛擬機器

1. 在 **[所有裝置]** 索引標籤上，選擇從備份執行的電腦。
2. 請按一下 **[刪除]**。

電腦已從 Web 介面中移除。同時也從 vSphere 或 Hyper-V 詳細目錄和資料存放區 (儲存空間) 移除。所有在電腦執行時的資料變更都遺失了。

最終化電腦

從備份執行虛擬機器時，虛擬磁碟的內容為直接取自該備份。因此，如果失去與備份位置或是保護代理程式的連線，電腦將變成無法存取，甚至損壞。

您可以選擇讓此電腦變成永久電腦，亦即，將其所有虛擬磁碟，以及在電腦執行時發生的變更，復原至儲存這些變更的資料存放區。此過程就叫做最終化。

執行最終化時，不需停機時間。在最終化期間，虛擬機器將*不會*關閉。

最終虛擬磁碟的位置是在 **[以 VM 的身分執行]** 作業的參數中定義的 (**[資料存放區]** (用於 ESXi) 或 **[路徑]** (用於 Hyper-V))。在開始最終化之前，請確認此資料存放區的可用空間、共用功能及效能適合執行實際運作的電腦。

注意事項

在 Windows Server 2008/2008 R2 和 Microsoft Hyper-V Server 2008/2008 R2 中執行的 Hyper-V 不支援最終化，因為在這些 Hyper-V 版本中缺少所需的 API。

欲最終化從備份執行的電腦

1. 在 **[所有裝置]** 索引標籤上，選擇從備份執行的電腦。
2. 按一下 **[最終化]**。
3. [選用] 請指定新的電腦名稱。
4. [選用] 請變更磁碟的佈建模式。預設設定為 **[精簡]**。
5. 按一下 **[最終化]**。

電腦名稱立即變更。復原進度會顯示在 **[活動]** 索引標籤上。復原完成後，電腦圖示將變更為一般虛擬機器圖示。

最終化須知

最終化與一般復原

最終化程序比一般復原慢的原因如下：

- 在最終化期間，代理程式會對備份的不同部分執行隨機存取。當整部電腦正在復原時，代理程式會循序讀取備份中的資料。
- 如果虛擬機器在最終化期間運作，代理程式會更常讀取備份中的資料，以同時維持兩個處理程序。在一般復原期間，虛擬機器將會停止。

從雲端備份執行電腦最終化

由於密集存取備份資料的緣故，最終化速度將與備份位置和代理程式之間的頻寬息息相關。相較於本機備份，雲端備份的最終化比較慢。如果網際網路連線非常慢或不穩定，從雲端備份執行的電腦最終化可能會失敗。如果您打算執行最終化而且可以選擇，建議您從本機備份執行虛擬機器。

注意事項
最終化速度取決於代理程式是連線到 VMware ESXi 主機還是 vCenter，如 "設定虛擬裝置" (第 123 頁) 的步驟 3 所述。基於 VMware API 的特殊性，連線到 VMware vCenter 可能會減緩最終化作業。若要加快最終化作業速度，請使用單獨的 VMware 用代理程式執行 **[以 VM 的身分執行]** 作業，然後再進行最終化，此時此代理程式將會連線到 ESXi 主機而非 vCenter。

於 VMware vSphere 中進行作業

本節介紹特定於 VMware vSphere 環境的作業。

虛擬機器的複寫

複寫僅限 VMware ESXi 虛擬機器。

複寫是建立虛擬機器的精確複本(複本)，然後維持複本與原始電腦同步之過程。經由複寫關鍵的虛擬機器，您將隨時擁有此電腦在準備啟動狀態的複本。

複寫可以手動啟動，或是在您指定的排程中。第一個複寫是完整複寫 (複製整台電腦)。除非停用此選項，否則所有後續複寫均為增量複寫，且與 [Changed Block Tracking] 同時執行。

複寫與備份之比較

與已排程備份不同的是，複本僅保留虛擬機器的最新狀態。複本耗用資料存放區空間，而備份則可以保留在更便宜的存放區。

不過，啟動複本會比啟動復原快速，從備份執行虛擬機器也快速許多。啟動複本比從備份執行 VM 快速，且不會增加 VMware 用代理程式的負載。

使用範例

- **將虛擬機器複寫至遠端站台。**

  藉著從主要網站到次要網站複製虛擬機器的方式，複寫可以承擔資料中心部份或全部故障。次要網站通常位於遠端設備中，不可能受到環境、基礎架構，或是會造成主要網站故障的其他因素所影響。
- **在單一站台中複寫虛擬機器 (從一個主機/資料存放區到另一個)。**

  現場複寫適用於高可用性和災難復原等情況。

複本可以執行的動作

- **測試複本**

  將啟動複本進行測試。使用 vSphere Client 或其他工具檢查複本是否正確運作。在測試進行中，將暫停複寫。
- **容錯移轉至複本**

  容錯移轉是將工作量從原始虛擬機器移轉至其複本。在容錯移轉進行中，將暫停複寫。
- **備份複本**

  備份和複寫均需要存取虛擬磁碟，因此會影響執行虛擬機器的主機之效能。如果想同時擁有虛擬機器的複本和備份，卻不想增加生產主機額外的負載，請複寫電腦至不同主機，並設定複本的備份。

限制

- 下列類型的虛擬機器無法複寫：
  - 在 ESXi 5.5 或更早版本上執行的容錯機器。
  - 從備份執行的電腦。
  - 虛擬機器的複本。
- 部分硬體變更 (例如將網路介面卡 (NIC) 新增至 ESXi 主機或從中移除 NIC) 會導致變更主機的內部 ID。此變更會影響 VM 複寫計劃。進行此類變更後，您必須重新建立 VM 複寫計劃，其中選擇 ESXi 主機作為來源或目標。否則，VM 複寫計劃將會失敗。

建立複寫計劃

您必須為每台電腦分別建立複寫計劃。目前無法將現有的計劃套用到其他電腦。

建立複寫計劃

1. 選擇要複寫的虛擬機器。
2. 按一下 **[複寫]**。

   軟體會顯示新的複寫計劃範本。
3. 選用：若要修改複寫計劃名稱，請按一下預設名稱。
4. 按一下 **[目標電腦]**，然後執行下列操作：
   a. 選擇建立新的複本或是使用原始電腦的現有複本。
   b. 選擇 ESXi 主機並指定新複本名稱，或是選擇現有的複本。

新複本的預設名稱為 **[原始電腦名稱]_replica**。

c. 按一下 **[確定]**。

5. [僅適用於複寫到新電腦] 按一下 **[資料存放區]**，然後選擇虛擬機器的資料存放區。
6. [選用] 按一下 **[排程]** 以變更複寫排程。

   依預設，系統會將複寫排程為星期一到星期五每日執行。您可以選擇複寫執行的時間。

   若想變更複寫頻率，請移動滑桿，然後指定排程。

   您也可以執行下列步驟：

   - 設定排程啟用時間的日期範圍。選擇 **[在日期範圍內執行計劃]** 核取方塊，然後指定日期範圍。
   - 停用排程。若是選用此項目，需要複寫時可手動執行。
7. [選用] 按一下齒輪圖示以修改複寫選項。
8. 按一下**[套用]**。
9. [選用] 若要手動執行計劃，請按一下計劃面板上的 **[立即執行]**。

由於執行複寫計劃的關係，虛擬機器複本會出現在 **[所有裝置]** 清單中，並顯示下列圖示： 

測試複本

準備測試複本

1. 選擇要測試的複本。
2. 按一下 **[測試複本]**。
3. 按一下 **[開始測試]**。
4. 選擇是否要將啟動的複本連接至網路。依預設，複本不會連線至網路。
5. [選用] 如果您要將複本連線到網路，請選擇 **[停止原始虛擬機器]** 核取方塊，即可在啟動複本之前停止原始電腦。
6. 按一下 **[開始]**。

停止測試複本

1. 選擇正在進行測試的複本。
2. 按一下 **[測試複本]**。
3. 按一下 **[停止測試]**。
4. 確認選項無誤。

容錯至複本

機器容錯移轉至複本

1. 選擇容錯移轉的複本。
2. 按一下 **[複本動作]**。
3. 按一下 **[容錯移轉]**。
4. 選擇是否要將啟動的複本連接至網路。根據預設，複本會連接到與原始機器相同的網路。

5. [選用] 若您選擇將複本連接到網路，請先清除 **[停止原始虛擬機器]** 核取方塊，以保持原始機器的連線狀態。
6. 按一下 **[開始]**。

複本處於容錯移轉狀態時，您可以選擇執行下列任一動作：

- **停止容錯移轉**

  若原始電腦已修正，則會停止容錯移轉。系統會關閉複本。系統將恢復執行複寫。
- **對複本執行永久容錯移轉**

  此作業會立即移除虛擬機器中的 [複本] 旗標，如此即無法再複寫該機器。若要恢復執行複寫，請編輯複寫計劃，選取此機器做為來源。
- **容錯回復**

  若容錯移轉至非預定用於持續作業的網站，則執行容錯回復。複本會復原為原始電腦或新的虛擬機器。一旦復原為原始電腦的作業完成後，系統就會開機並恢復執行複寫。若要選擇復原為新的機器，請編輯複寫計劃，選取此機器做為來源。

停止容錯移轉

停止容錯移轉

1. 選擇處於容錯移轉狀態的複本。
2. 按一下 **[複本動作]**。
3. 按一下 **[停止容錯移轉]**。
4. 確認選項無誤。

執行永久容錯移轉

執行永久容錯移轉

1. 選擇處於容錯移轉狀態的複本。
2. 按一下 **[複本動作]**。
3. 按一下 **[永久容錯移轉]**。
4. [選用] 變更虛擬機器的名稱。
5. [選用] 選擇 **[停止原始虛擬機器]** 核取方塊。
6. 按一下 **[開始]**。

容錯回復

從複本容錯回復

1. 選擇處於容錯移轉狀態的複本。
2. 按一下 **[複本動作]**。
3. 按一下 **[從複本容錯回復]**。

   軟體會自動選擇原始電腦做為目標電腦。
4. [選用] 按一下 **[目標電腦]**，然後執行下列操作：

a. 選擇容錯回復為新電腦或現有的電腦。
b. 選擇 ESXi 主機並指定新電腦名稱，或是選擇現有的電腦。
c. 按一下 **[確定]**。

5. 選用：若選擇容錯回復為新電腦，您也可以執行下列動作：
   - 按一下 **[資料存放區]**，選擇虛擬機器的資料存放區。
   - 按一下 **[VM 設定]**，變更記憶體大小、處理器數量，以及虛擬機器的網路連線。
6. [選用] 按一下 **[復原選項]**，以修改容錯回復選項。
7. 按一下 **[開始復原]**。
8. 確認選項無誤。

複寫選項

欲修改複寫選項，請按一下複寫計劃名稱旁邊的齒輪圖示，然後按一下 **[複寫選項]**。

Changed block tracking (CBT)

此選項與備份選項 [Changed block tracking (CBT)] 類似。

磁碟佈建

此選項會定義複本的磁碟佈建設定。

預設為：**精簡佈建**。

您可以選取下列值：**精簡佈建**、**密集佈建**和**保留原始設定**。

錯誤處理

此選項與備份選項 [錯誤處理] 類似。

事前/事後命令

此選項與備份選項 [事前/事後命令] 類似。

虛擬機器的磁碟區陰影複製服務 VSS

此選項與備份選項 [虛擬機器的磁碟區陰影複製服務 VSS] 類似。

容錯回復選項

若要修改容錯回復選項，請在設定容錯回復時按一下 **[復原選項]**。

錯誤處理

此選項與「錯誤處理」復原選項類似。

效能

此選項與「效能」復原選項類似。

事前/事後命令

此選項與「事前/事後命令」復原選項類似。

VM 電源管理

此選項與「VM 電源管理」復原選項類似。

初始複本種子

為了加速複寫至遠端位置並節省網路頻寬，您可以執行複本種子。

重要事項
若要執行複本植入，必須在目標 ESXi 上執行 VMware 用代理程式 (虛擬裝置)。

欲初始複本種子

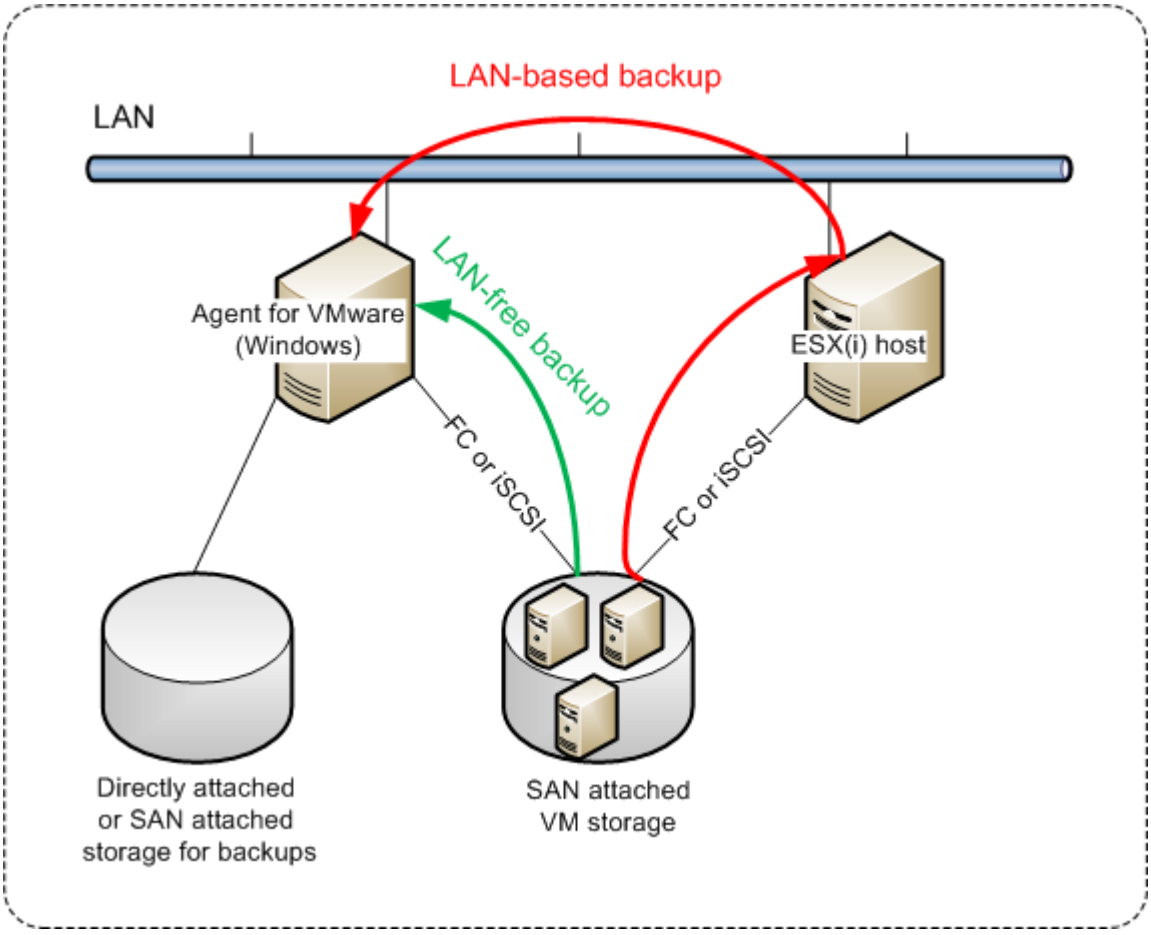
1. 執行下列其中一項操作：
   - 若可以關閉原始的虛擬機器，請將之關閉，然後跳到步驟 4。
   - 若無法關閉原始的虛擬機器，請繼續下一個步驟。
2. 建立複寫計劃。
   建立計劃時，請在 **[目標電腦]** 中選擇 **[新的複本]** 以及託管原始電腦的 ESXi。
3. 執行計劃一次。
   複本已建立在原始的 ESXi 上。
4. 匯出虛擬機器 (或複本) 檔案至外接硬碟。
   a. 連結外接硬碟至執行 vSphere 用戶端的電腦。
   b. 連結 vSphere 用戶端至原始的 vCenter\ESXi。
   c. 選擇詳細目錄中最新建立的複本。
   d. 按一下 **[檔案]** > **[匯出]** > **[匯出 OVF 範本]**。
   e. 在 **[目錄]** 中指定外接式硬碟上的資料夾。
   f. 按一下 **[確定]**。
5. 移轉硬碟至遠端位置。
6. 匯入複本至目標 ESXi。
   a. 連結外接硬碟至執行 vSphere 用戶端的電腦。
   b. 連結 vSphere 用戶端至目標 vCenter\ESXi。
   c. 按一下 **[檔案]** > **[部署 OVF 範本]**。
   d. 在 **[從檔案或 URL 部署]** 中，指定您在步驟 4 匯出的範本。
   e. 完成匯入程序。
7. 編輯您在步驟 2 中建立的複寫計劃。在 **[目標電腦]** 中選擇 **[現有的複本]**，然後選擇已匯入的複本。

如此一來，軟體將會繼續更新複本。所有複寫將會增量。

VMware 用代理程式 - 不透過 LAN 備份

如果您的 ESXi 使用 SAN 連接儲存裝置，請將代理程式安裝在連線至相同 SAN 的電腦上。代理程式將會直接從儲存裝置備份虛擬機器，而不是透過 ESXi 主機和 LAN。此功能稱為「不透過 LAN 備份」。

下方圖表說明透過 LAN 與不透過 LAN 的備份方式。如果您有光纖通道 (FC) 或 iSCSI 儲存區域網路，就可以不透過 LAN 存取虛擬機器。若要完全停用透過 LAN 傳送備份資料，請將備份儲存在代理程式電腦的本機磁碟上，或 SAN 附加存放區上。



啟用代理程式直接存取資料存放區

1. 在可經由網路存取 vCenter Server 的 Windows 電腦上安裝 VMware 用代理程式。
2. 將託管資料存放區的邏輯單元編號 (LUN) 連線至電腦。考慮以下情況：
   - 使用資料存放區連線至 ESXi 所用的相同協定 (即 iSCSI 或 FC)。
   - LUN *不得*進行初始化，但須在**[磁碟管理]**中顯示為「離線」磁碟。如果 Windows 對 LUN 進行初始化，則其可能會損毀並且無法被 VMware vSphere 讀取。

因此，代理程式會使用 SAN 傳輸模式存取虛擬磁碟，即其會讀取 iSCSI/FC 上的原始 LUN 磁區，而不識別 VMFS 檔案系統（Windows 不會感知到這種行為）。

限制

- 在 vSphere 6.0 及更新版本中，如果部分 VM 磁碟在 VMware 虛擬磁碟區 (VVol)，部分不在，代理程式便無法使用 SAN 傳輸模式。此類虛擬機器的備份便會失敗。
- 即使您為代理程式設定了 SAN 傳輸模式，VMware vSphere 6.5 中提供的加密虛擬機器仍會透過 LAN 進行備份。由於 VMware 不支援採用 SAN 傳輸備份加密虛擬磁碟，所以代理程式會回復至 NBD 傳輸。

範例

如果您使用 iSCSI SAN，在執行 Windows 並安裝 VMware 用代理程式的電腦上設定 iSCSI 起始端。

設定 SAN 原則。

1. 以系統管理員身分登入、開啟命令提示字元、輸入 `diskpart`，然後按 **Enter**。
2. 輸入 `san`，然後按 **Enter**。確保 **SAN 原則：將顯示全部離線**。
3. 如果有設定 SAN 原則的另一個值：
   a. 輸入 `san policy=offlineall`。
   b. 按一下 **Enter**。
   c. 要檢查是否有正確套用設定，請執行步驟 2。
   d. 重新啟動機器。

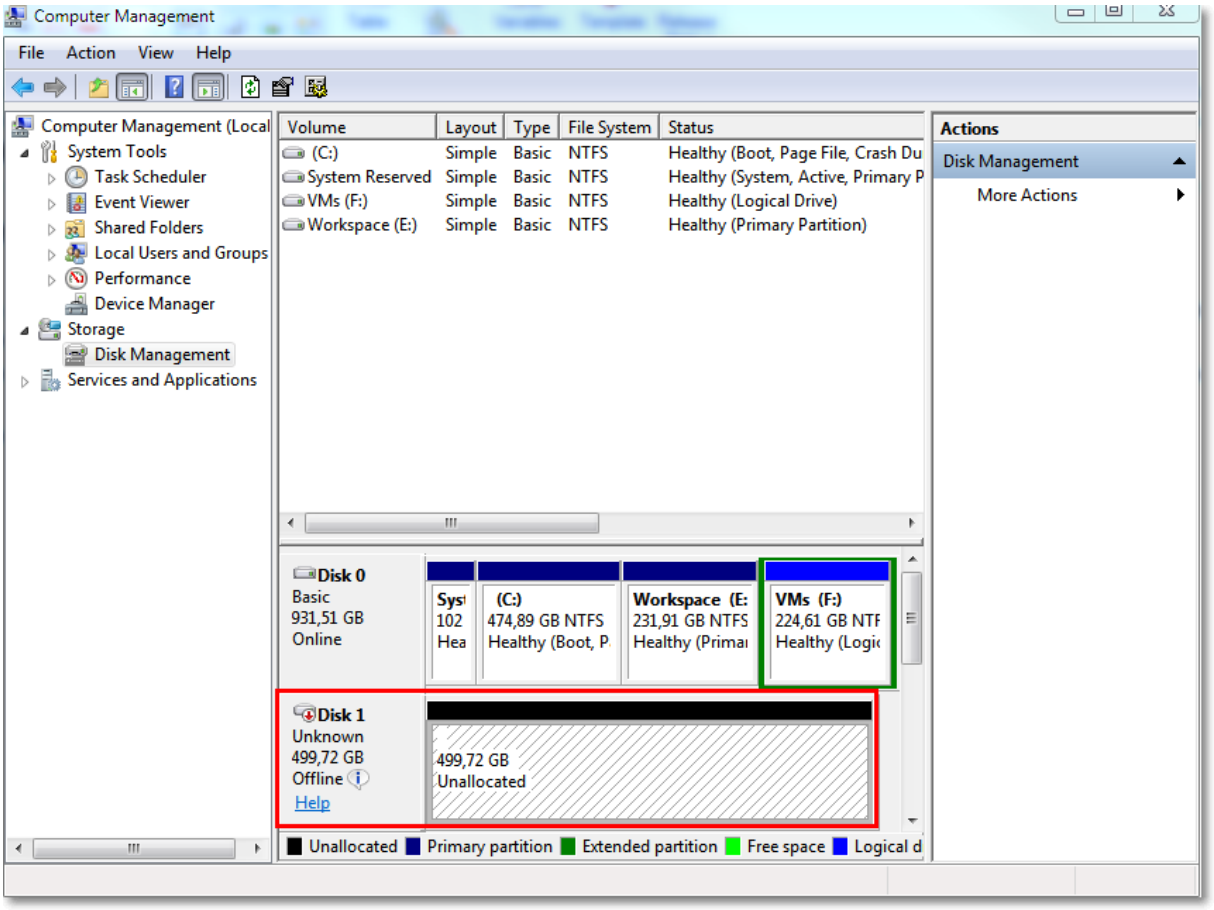
設定 iSCSI 起始端

1. 移至 **[控制台]** > **[管理工具]** > **[iSCSI 起始端]**。

   注意事項
   若要尋找 **[管理工具]** 小程式，您或需將 **[控制台]** 視圖變更為 **[首頁]** 或 **[類別]** 以外的項目，或使用搜尋。

2. 如果這是第一次發佈 Microsoft iSCSI 起始端，請確認您要啟動 Microsoft iSCSI 起始端服務。
3. 在**[目標]**索引標籤，輸入目標 SAN 裝置的完整網域名稱 (FQDN) 或 IP 位址，然後按一下**[快速連線]**。
4. 選擇託管資料存放區的 LUN，然後按一下**[連線]**。
   如果 LUN 未顯示，請確保 iSCSI 目標的分區允許執行代理程式的電腦存取 LUN。電腦必須新增至此目標上已允許的 iSCSI 起始端清單。
5. 按一下 **[確定]**。

就緒的 SAN LUN 應顯示在下方螢幕擷取畫面所示的**[磁碟管理]**中。



使用本機附加的存放區

您可以將額外的磁碟附加到 VMware 用代理程式 (虛擬裝置)，讓代理程式可以備份到這個本機附加的存放區。這種方法減少了代理程式與備份位置之間的網路流量。

藉助備份虛擬機器執行於相同主機或叢集的虛擬裝置可以直接存取電腦所在的資料存放區。這意味著該裝置可以透過使用 HotAdd 傳輸來連接備份磁碟，因此，備份流量是由一個本端磁碟導向至另一個本端磁碟。若資料存放區是連線作為**磁碟/LUN**，而不是 **NFS**，則備份將完全 不用 LAN 。在 NFS 資料存放區的情況下，資料存放區與主機之間將會存在網路流量。

使用本機附加的存放區，即假設代理程式一律會備份相同的電腦。如果有多個代理程式於 vSphere 中運作，且其中一或多個代理程式使用本機附加的存放區，則您需要手動將每個代理程式繫結至所有其必須備份的電腦。否則，如果由管理伺服器重新分配電腦給代理程式，則可能發生一部電腦的備份分散到多個存放區的情形。

您可以將存放區新增到運作中的代理程式，亦可在從 OVF 範本部署代理程式時新增存放區。

若要將存放區附加至運作中的代理程式

1. 在 VMware vSphere 詳細目錄中，用滑鼠右鍵按一下 [VMware 用代理程式 (虛擬裝置)]。
2. 編輯虛擬機器的設定，以新增磁碟。磁碟大小必須至少為 10 GB。

警告！
新增現有的磁碟時請務必小心。存放區一旦建立，此磁碟上所有先前含有的資料都將喪失。

3. 前往虛擬裝置主控台。您可以在畫面底部找到**建立存放區**連結。如果找不到此連結，請按一下**重新整理**。
4. 按一下**建立存放區** 連結，選擇磁碟並為其指定標籤。由於檔案系統限制，標籤長度的限制為 16 個字元。

若要選擇本機附加的存放區作為備份目的地

- 建立保護計劃時，於 **[備份目標位置]** 中，選擇 **[本機資料夾]**，然後輸入對應到本機連接存放區的代號，例如 **D:**。

注意事項
本機連接的儲存裝置 (LAS) 專為相對較小且具有單一代理程式 (虛擬裝置) 的環境而設計。我們已經測試了容量高達 5 TB 的本機連接的儲存裝置。您可以連接更大的磁碟，但風險由您自行承擔，但不支援此類組態。對於超過 5TB 的備份資料，建議您使用其他類型的儲存裝置。例如，您可以建立 VMware 虛擬磁碟並將其連接到任何隨機的虛擬機器，並在其上建立網路共用，然後將其當作備份目的地而非 LAS 使用。

虛擬機器繫結

本節概述 Cyber Protection 服務如何在 VMware vCenter 內組織多個代理程式的作業。

下列分配演算法適用於安裝在 Windows 的虛擬裝置和代理程式。

分配演算法

虛擬機器將自動平均分佈於 VMware 用代理程式之間。所謂的平均，是指每個代理程式會管理相同數量的虛擬機器。虛擬機器所佔用的儲存空間則不會納入計算。

然而，為虛擬機器選擇代理程式時，軟體會嘗試最佳化整體系統效能。軟體特別會考量代理程式與虛擬機器的位置。管理伺服器會優先選擇裝載於相同主機的代理程式。如果相同的主機上沒有代理程式，則會優先選擇來自相同叢集的代理程式。

虛擬機器一旦指定給某個代理程式後，此虛擬機器的所有備份都會交由此代理程式負責進行。

重新分配

每當既定的平衡被破壞時 (更精確地說，當代理程式間負載不平衡的情況達到百分之 20 的程度時)，就會進行重新分配。當您新增或移除虛擬機器或代理程式、將虛擬機器移轉到不同的主機或叢集，或手動將虛擬機器繫結到代理程式時，就可能會發生這種情形。如果發生此情形，Cyber Protection 服務會使用相同的演算法重新分配電腦。

例如，您發現需要更多代理程式來增進處理能力，以及部署額外的虛擬裝置到叢集。Cyber Protection 服務會指派最適合的電腦給新的代理程式。舊代理程式的負載將會減少。

當您從 Cyber Protection 服務移除代理程式時，指派給代理程式的電腦會分配給剩餘的代理程式。不過，如果代理程式損毀，或者未從 vSphere 手動刪除，這就不會發生。只有當您從 Web Interface 移除此類代理程式後，才會開始重新分配。

檢視分配結果

您可檢視自動分配的結果：

- 在 **[所有裝置]** 區段上，每部虛擬機器的 **[代理程式]** 欄中
- 在**設定** > **代理程式**區段中選擇代理程式後，在**詳細資料**窗格的**已指派虛擬機器**中

手動繫結

[VMware 用代理程式繫結] 可讓您指定一個固定的代理程式來備份某部虛擬機器，將該虛擬機器自上述分配程序中排除。整體平衡將保持不變，僅在原代理程式已移除的情況下，才可將特定電腦轉給不同的代理程式。

將虛擬機器與代理程式建立繫結

1. 選擇電腦。
2. 按一下**[詳細資料]**。
   在**已指派代理程式**區段中，軟體顯示當前管理所選電腦的代理程式。
3. 按一下**變更**。
4. 選擇**手動**。
5. 選擇電腦要繫結到的代理程式。
6. 按一下 **[儲存]**。

解除電腦與代理程式的繫結

1. 選擇電腦。
2. 按一下**[詳細資料]**。
   在**已指派代理程式**區段中，軟體顯示當前管理所選電腦的代理程式。
3. 按一下**變更**。
4. 選擇**自動**。
5. 按一下 **[儲存]**。

正在停用代理程式的自動指派

您可以停用 VMware 用代理程式的自動指派，以透過指定該代理程式必須備份之電腦清單將其從分發過程中排除。將維持其他代理程式之間的整體平衡。

如果無其他登錄的代理程式，或者如果停用所有其他代理的自動指派，則無法停用代理程式的自動指派。

要停用代理程式的自動指派

1. 請按一下**[設定]** > **[代理程式]**。
2. 選擇要通用自動指派的 VMware 用代理程式。

3. 按一下**[詳細資料]**。
4. 停用**自動指派**開關。

使用範例

- 如果您希望以 VMware 用代理程式 (Windows) 透過光纖通道來備份一部特定 (相當大型) 的虛擬機器，而其他虛擬機器則由虛擬裝置來備份，手動繫結即可派上用場。
- 如果代理程式具有本機連接存放區，則需將 VM 繫結到代理程式。
- 停用自動指派讓您能夠確保可根據您指定的排程對特定電腦進行預測備份。排程時間到來時，僅備份一台 VM 的代理程式無法正常備份其他 VM。
- 如果您有多台在地理上分離的 ESXi 主機，則停用自動指派非常有用。如果停用自動指派，然後將每台主機上的 VM 繫結到在同一主機上執行的代理程式，則可確保代理程式不會備份在遠端 ESXi 主機上執行的任何電腦，從而節省網路流量。

自動執行凍結前和解除凍結後指令碼

您可以透過 VMware Tools，在您使用無代理程式模式備份的虛擬機器上，自動執行自訂的凍結前和解除凍結後指令碼。因此，例如，您可以執行自訂的 quiescing 指令碼，並針對執行非 VSS 感知應用程式的虛擬機器，建立應用程式一致的備份。

必要條件

凍結前和解除凍結後指令碼必須位於虛擬機器上的特定資料夾。

- 若是 Windows 虛擬機器，此資料夾的位置取決於主機的 ESXi 版本。
  例如，若是在 ESXi 6.5 主機上執行的虛擬機器，此資料夾為 `C:\Program Files\VMware\VMware Tools\backupScripts.d\`。您必須手動建立 `backupScritps.d` 資料夾。請不要在此資料夾中儲存其他類型的檔案，因為這可能會使 VMware Tools 變得不穩定。
  如需有關其他 ESXi 版本的凍結前和解除凍結後指令碼位置的詳細資訊，請參閱 VMware 文件。
- 若是 Linux 虛擬機器，請將您的指令碼分別複製到 `/usr/sbin/pre-freeze-script` 和 `/usr/sbin/post-thaw-script` 目錄。當您建立快照時，會執行 `/usr/sbin/pre-freeze-script` 中的指令碼；當快照最終化時，會執行 `/usr/sbin/post-thaw-script` 中的指令碼。這些指令碼必須可由 VMware Tools 使用者執行。

若要自動執行凍結前和解除凍結後指令碼

1. 請確認 VMware Tools 已安裝在虛擬機器上。
2. 在虛擬機器上，將您的自訂指令碼放到所需的資料夾中。
3. 在此機器的保護計劃中，啟用 **[虛擬機器的磁碟區陰影複製服務 (VSS)]** 選項。
   如此會在啟用 **[靜止客體檔案系統]** 選項時，建立 VMware 快照，然後觸發虛擬機器內的凍結前和解除凍結後指令碼。

您不需要在執行 VSS 感知應用程式 (例如 Microsoft SQL Server 或 Microsoft Exchange) 的虛擬機器上執行自訂的 quiescing 指令碼。若要針對這類機器建立應用程式一致的備份，請在保護計劃中啟用 **[虛擬機器的磁碟區陰影複製服務 (VSS)]** 選項。

支援虛擬機器移轉

本節包含虛擬機器在 vSphere 環境中移轉的相關資訊，包括 vSphere 叢集所屬 ESXi 主機之間的移轉。

vMotion 允許將虛擬機器的狀態和組態移至其他主機，而電腦磁碟則保持在共用儲存空間的相同位置。Storage vMotion 允許將虛擬機器磁碟從一個資料存放區移至另一個資料存放區。

- 執行 VMware 用代理程式 (虛擬裝置) 的虛擬機器不支援使用 vMotion 遷移，包括 Storage vMotion，且必須在裝置部署後停用。您應該將此虛擬機器新增到在 vSphere 叢集組態中的 VM 覆寫清單，才能避免跨 vSphere 叢集節點遷移裝置虛擬機器。
- 開始備份虛擬機器時，會自動停用使用 vMotion (包括 Storage vMotion) 進行移轉。此虛擬機器會暫時新增至 vSphere 叢集設定的 **[VM 覆寫]** 清單中。備份完成後，系統會將 **[VM 覆寫]** 設定自動還原至其先前的狀態。
- 正在使用 vMotion (包括 Storage vMotion) 進行虛擬機器移轉時，無法開始該虛擬機器的備份。當此虛擬機器的移轉完成後，就會開始該機器的備份。

保護虛擬化環境

在 Cyber Protect 主控台中，您可以使用原生的呈現方式檢視 vSphere、Hyper-V 和 Virtuozzo 環境。安裝並註冊對應的代理程式後，**VMware**、**Hyper-V** 或 **Virtuozzo** 索引標籤會出現在 **[裝置]** 下。

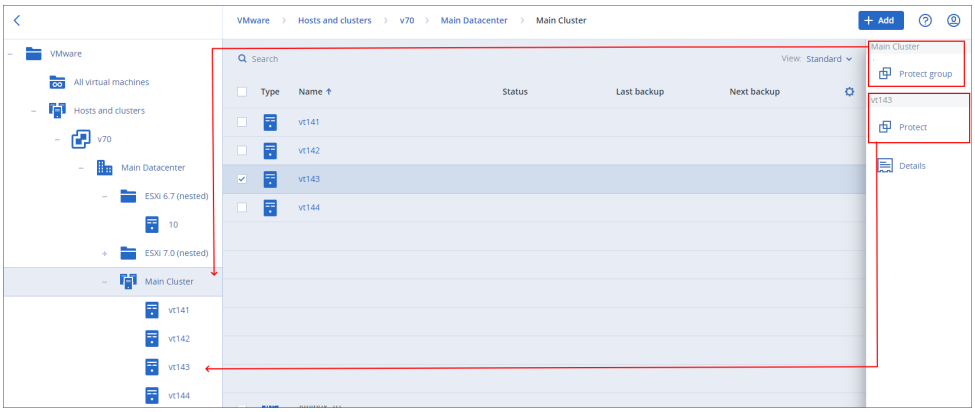
例如，在 **[VMware]** 索引標籤上，您可以備份下列 vSphere 基礎架構物件：

- vCenter
- 資料中心
- 資料夾
- 叢集
- ESXi 主機
- 資源集區
- 虛擬機器

若要將計劃套用到所選基礎架構物件，按一下 **[保護]**。所有子物件都將備份。

若要將計劃套用到所選基礎結構物件的父物件，按一下 **[保護群組]**。父物件的所有子物件都將備份。

例如，如果您將計劃套用到 ESXi 主機，則該主機上的所有虛擬機器都會備份。如果您將計劃套用到父叢集，則此叢集中所有主機上的所有虛擬機器都會備份。



在 vSphere Client 中檢視備份狀態

您可以在 vSphere Client 中檢視虛擬機器的備份狀態以及上次備份時間。

此資訊會顯示在虛擬機器摘要 (**[摘要]** > **[自訂屬性]/[註解]/[備註]** 中，視用戶端類型和 vSphere 版本而定)。您也可以針對任何主機、資料庫、資料夾、資源集區，或整個 vCenter Server，在 **[虛擬機器]** 索引標籤上啟用 **[上次備份]** 和 **[備份狀態]** 欄。

若要提供這些屬性，VMware 用代理程式除了「VMware 用代理程式 - 必要權限」中所述的權限之外，還要具備下列權限：

- **[全域]** > **[管理自訂屬性]**
- **[全域]** > **[設定自訂屬性]**

VMware 用代理程式所需的權限

注意事項

若要啟用虛擬機器備份，請在 ESXi 主機上安裝 vStorage API。如需詳細資訊，請參閱本知識庫文章。

VMware 用代理程式會透過在代理部署期間指定的使用者帳戶，向 vCenter 或 ESXi 主機進行驗證。使用者帳戶必須具備包含下表中列出的權限的角色。建議您使用專用帳戶和角色，而不是使用擁有系統管理員角色的現有帳戶。

使用者帳戶必須獲授予權限，才能存取所有層級的 vSphere 基礎架構，例如 vCenter、資料中心、叢集、ESXi 主機、資源集區和虛擬機器。若要瞭解如何在 vCenter 層級新增權限並將其傳播到其他層級，請參閱 "授予使用者帳戶的存取權限" (第 627 頁)。

您可以變更 VMware 用代理程式使用的使用者帳戶，而無需重新部署代理程式。若要瞭解如何變更帳戶，請參閱 "變更 VMware 用代理程式的使用者帳戶" (第 627 頁)。

物件	權限	作業			
		備份 VM	復原至新 VM	復原至現有 VM	從備份執行 VM
密碼編譯作業 (從 vSphere 6.5 開始)					
	新增磁碟	+*			
	直接存取	+*			
資料存放區					
	配置空間		+	+	+
	瀏覽資料存放區				+
	設定資料存放區	+	+	+	+
	低階檔案作業				+
全域					
	停用方式	+	+	+	
	啟用方式	+	+	+	
	授權	+	+	+	+
	管理自訂屬性	+	+	+	
	設定自訂屬性	+	+	+	
主機 > 組態					
	儲存磁碟分割組態				+
	修改叢集				
主機 > 本機作業					
	建立虛擬機器				+
	刪除虛擬機器				+
	重新設定虛擬機器				+
網路					

物件	權限	作業			
		備份 VM	復原至新 VM	復原至現有 VM	從備份執行 VM
	指派網路		+	+	+
資源					
	將虛擬機器指派給資源集區		+	+	+
虛擬機器 > 變更組態					
	取得磁碟租賃	+		+	
	新增現有磁碟	+	+		+
	新增新磁碟		+	+	+
	新增或移除裝置		+		+
	進階組態	+	+	+	
	變更 CPU 數量		+		
	變更記憶體		+		
	變更設定		+	+	+
	變更資源	+	+		
	修改裝置設定	+	+		
	移除磁碟	+	+	+	+
	重新命名		+		
	設定註解				+
	切換磁碟變更追蹤	+		+	
虛擬機器 > 客體作業					
	客體作業修改	+**			
	客體作業程式執行	+**			
	客體作業查詢	+**			
虛擬機器 > 互動					

物件	權限	作業			
		備份 VM	復原至新 VM	復原至現有 VM	從備份執行 VM
	取得客體控制票證 (適用於 vSphere 4.1 及 5.0)				+
	設定 CD 媒體		+	+	
	由 VIX API 執行客體作業系統管理 (適用於 vSphere 5.1 及更新版本)				+
	關閉電源			+	+
	開啟電源		+	+	+
虛擬機器 > 清查					
	建立自現有		+	+	+
	新建		+	+	+
	登錄				+
	移除		+	+	+
	取消登錄				+
虛擬機器 > 佈建					
	允許磁碟存取		+	+	+
	允許唯讀磁碟存取	+		+	
	允許虛擬機器下載	+	+	+	+
虛擬機器 > 狀態 **虛擬機器 > 快照管理** (vSphere 6.5 及更高版本)					
	建立快照	+		+	+
	移除快照	+		+	+
vApp					
	新增虛擬機器				+

***** 僅備份加密電腦時需要這項權限。

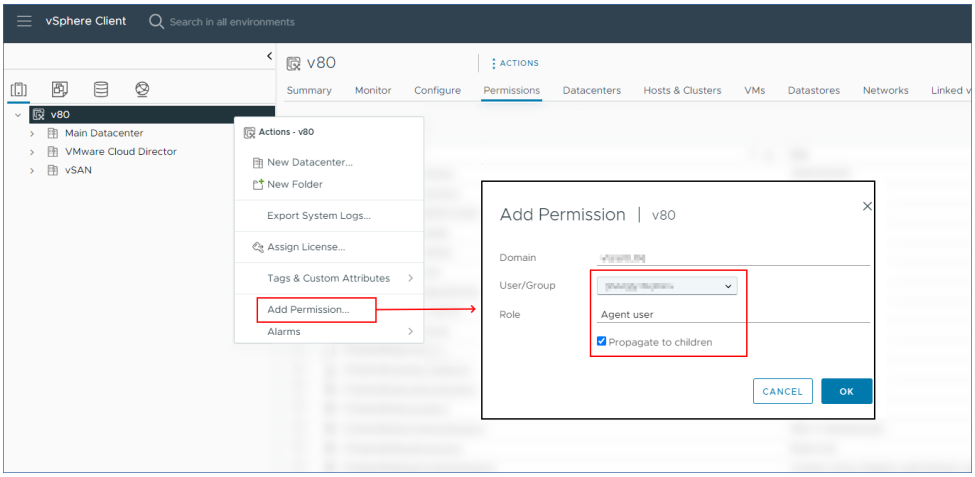
** 僅應用程式感知備份需要這項權限。

授予使用者帳戶的存取權限

VMware 用代理程式所使用的使用者帳戶必須能夠存取所有層級的 vSphere 基礎架構，例如 vCenter、資料中心、叢集、ESXi 主機、資源集區和虛擬機器。

若要授予使用者帳戶的存取權限

1. 在 vSphere Client 中，移至 **[清查]**。
2. 以滑鼠右鍵按一下您要授予權限的 **vCenter** 物件，然後按一下 **[新增權限]**。
3. 在 **[新增權限]** 對話方塊中，選擇使用者帳戶和角色。
   此角色必須包含 "VMware 用代理程式所需的權限" (第 623 頁) 中列出的權限。
4. 選擇 **[傳播至子項]** 核取方塊。
5. 按一下 **[確定]**。



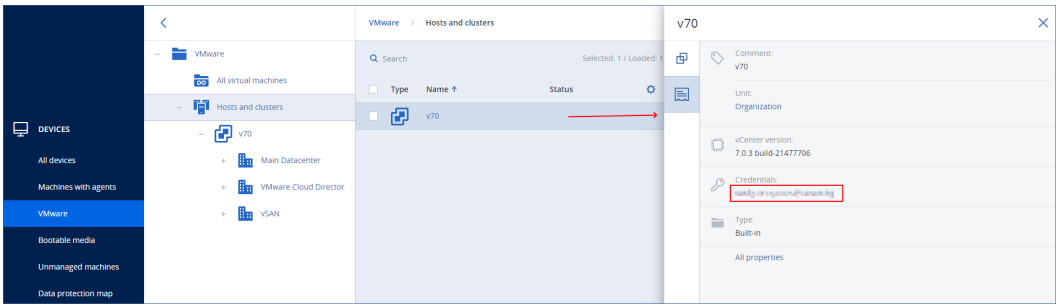
變更 VMware 用代理程式的使用者帳戶

在 Cyber Protect 主控台中，您可以變更 vCenter 或 ESXi 主機上個別代理程式或所有代理程式的使用者帳戶。

若要變更 VMware 用代理程式的使用者帳戶

對於所有代理程式

1. 在 Cyber Protect 主控台中，移至 **[裝置]** > **[VMware]**。
2. 按一下 **[主機與叢集]**。
3. 在主面板中，按一下 vCenter 或獨立 ESXi 主機名稱旁的空白空間。
4. 在右側面板上，按一下 **[詳細資料]**。
5. 在 **[認證]** 下，按一下使用者帳戶。

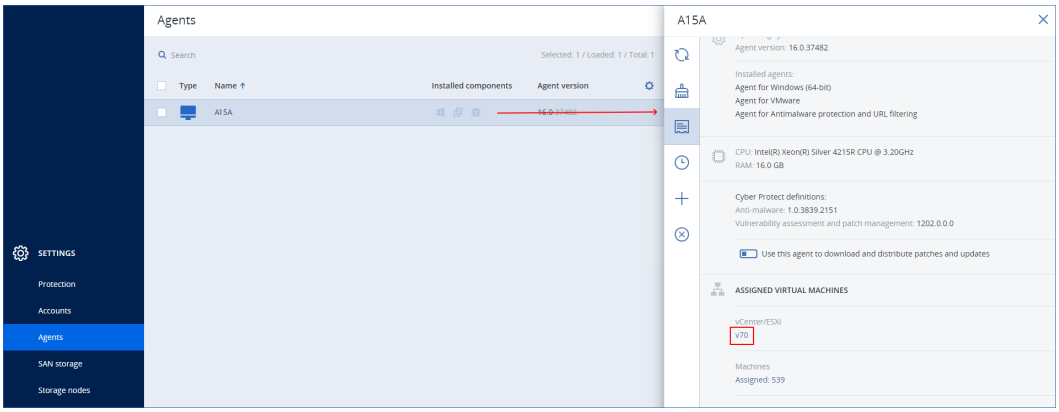


6. 指定新的使用者帳戶和該帳戶的密碼。
7. 按一下 **[確定]**。

因此，此 vCenter 或 ESXi 主機上的所有代理程式都將使用新的使用者帳戶。

對於個別代理程式

1. 在 Cyber Protect 主控台中，移至 **[設定]** > **[代理程式]**。
2. 選擇代理程式。
3. 在右側面板上，按一下 **[詳細資料]**。
4. 在 **[已指派的虛擬機器]** 下，按一下 vCenter/ESXi 名稱。



5. 在 **[新增 VMware vCenter 或 ESXi 主機]** 畫面中，指定新的使用者帳戶以及該帳戶的密碼。
6. 按一下 **[設定]**。

備份叢集 Hyper-V 虛擬機器

在 Hyper-V 叢集中，虛擬機器可以在不同的叢集節點之間移轉。請依照以下建議，設定正確的叢集 Hyper-V 虛擬機器備份：

1. 無論虛擬機器移轉的目的地節點為何，都必須可供備份。為了確保 Hyper-V 用代理程式可以存取任何節點上的電腦，代理程式服務必須以在各叢集節點上具有系統管理權限的網域使用者帳戶身分執行。

   建議您在 Hyper-V 用代理程式安裝期間，為代理程式服務指定上述帳戶。
2. 在叢集的每個節點上安裝 Hyper-V 用代理程式。
3. 在 Cyber Protection 服務中註冊所有代理程式。

已復原虛擬機器的高可用性

當您將備份的磁碟復原至*現有的* Hyper-V 虛擬機器時，虛擬機器的 [高可用性] 屬性將保持原樣。

當您將備份的磁碟復原至*新的* Hyper-V 虛擬機器時，所產生的虛擬機器將不具有高可用性。它會視為備用虛擬機器，而且電源通常會關閉。如果您需要在實際執行環境中使用該虛擬機器，可以從**容錯移轉叢集管理**嵌入式管理單元中，將其設定為具有 [高可用性]。

限制同時備份的虛擬機器總數。

在 **[排程]** 備份選項中，您可以限制每個保護計劃同時備份虛擬機器的數量。

當代理程式同時執行多個計劃時，同時備份的機器數量會增加。這可能會影響備份效能，並使主機和虛擬機器儲存空間超載。您可以設定代理程式層級的限制來避免這類問題。

若要限制代理程式層級同時備份的數量

VMware 用代理程式 (Windows)

1. 在已安裝代理程式的電腦上，建立新文字文件，然後在文字編輯器中開啟該文件。
2. 複製以下幾行並貼到檔案中。

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. 將 `00000001` 取代為您想要設定之限制的十六進位值。
   例如，`00000001` 為 1，而 `0000000A` 為 10。
4. 將文件儲存為 **limit.reg**。
5. 以系統管理員身份執行檔案。
6. 確認您要編輯 Windows 登錄。
7. 重新啟動代理程式。
   a. 在 **[開始]** 功能表中，按一下 **[執行]**。
   b. 輸入 **cmd**，然後按一下 **[確定]**。
   c. 在命令列上，執行下列命令：

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

Hyper-V 用代理程式

1. 在已安裝代理程式的電腦上，建立新文字文件，然後在文字編輯器中開啟該文件。
2. 複製以下幾行並貼到檔案中。

```
Windows Registry Editor Version 5.00

```

```
[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. 將 `00000001` 取代為您想要設定之限制的十六進位值。

   例如，`00000001` 為 1，而 `0000000A` 為 10。
4. 將文件儲存為 **limit.reg**。
5. 以系統管理員身份執行檔案。
6. 確認您要編輯 Windows 登錄。
7. 重新啟動代理程式。
   a. 在 **[開始]** 功能表中，按一下 **[執行]**。
   b. 輸入 **cmd**，然後按一下 **[確定]**。
   c. 在命令列上，執行下列命令：

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

虛擬裝置

此程序適用於 VMware (虛擬裝置) 用代理程式、Scale Computing 用代理程式、Virtuozzo Hybrid Infrastructure 用代理程式，以及 oVirt 用代理程式。

1. 在虛擬裝置的主控台中，按下 CTRL+SHIFT+F2 以開啟命令列介面。
2. 在文字編輯器中開啟 `/etc/Acronis/MMS.config` 檔案。
3. 找到以下區段：

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. 將 `10` 取代為您想要設定的同時備份數量上限。
5. 儲存檔案。
6. 執行 `reboot` 命令，重新啟動代理程式。

電腦移轉

您可將電腦的備份復原到另一台電腦，進行電腦移轉。

下表摘述可用的移轉選項。

備份電腦類型	可用的復原目的地							
	實體電腦	ESXi 虛擬機器	Hyper-V 虛擬機器	Virtuozzo		Virtuozzo Hybrid Infrastructure 虛擬機器	Scale Computing HC3 虛擬機器	RHV/oVirt 虛擬機器
				虛擬機器	容器			
實體電腦	+	+	+	-	-	+	+*	+
VMware ESXi 虛擬機器	+	+	+	-	-	+	+*	+
Microsoft Azure 虛擬機器	+	+	+	-	-	+	+*	+
Hyper-V 虛擬機器	+	+	+	-	-	+	+*	+
Virtuozzo 虛擬機器	+	+	+	+	-	+	+*	+
Virtuozzo 容器	-	-	-	-	+	-	-	-
Virtuozzo Hybrid Infrastructure 虛擬機器	+	+	+	-	-	+	+*	+
Scale Computing HC3 虛擬機器	+	+	+	-	-	+	+	+
Red Hat Virtualization/ oVirt 虛擬機器	+	+	+	-	-	+	+*	+

*若來源電腦已啟用安全開機，將無法啟動復原的 VM，除非您在復原後停用 VM 主控台中的安全開機。

注意事項

您無法將 macOS 虛擬機器復原至 Hyper-V 主機，因為 Hyper-V 不支援 macOS。您可以將 macOS 虛擬機器復原至 Mac 硬體上安裝的 VMware 主機。

如需有關如何執行遷移作業的詳細資訊，請參閱下列主題：

- 若是實體到虛擬 (P2V) 遷移，請參閱 "實體機器到虛擬" (第 447 頁)。
- 若是虛擬到虛擬 (V2V) 遷移，請參閱 "復原虛擬機器您可以從其備份復原虛擬機器。您無法在 Cyber Protect 主控台中，為 [合規] 模式下的租用戶復原備份。如需有關如何復原此類備份的詳細資訊，請參閱 "在合規模式下復原租用戶的備份" (第 1 頁)。必要條件復原至虛擬機器時，此虛擬機器必須為停止狀態。軟體預設不會顯示提示，即停止電腦。復原完成後，您必須手動啟動電腦。您可以使用 VM 電源管理復原選項來變更預設行為 (按一下 [復原選項] > [VM 電源管理])。程序執行下列其中一項操作：選擇已備份的電腦，按一下復原，然後選擇復原點。在 [備份儲存] 索引標籤上選擇復原點。按一下[復原] > [整部機器]。如果您想要復原到實體機器，請在復原至中選擇實體機器。否則，請跳過此步驟。只有在目標電腦的磁碟組態完全符合備份中的磁碟組態時，才能復原至實體機器。在此情況下，請繼續在「實體機器」中的步驟 4。否則，我們建議您使用可開機媒體來執行 V2P 移轉。[選用] 軟體預設會自動選擇原始電腦做為目標電腦。若要復原到另一部虛擬機器，請按一下目標機器然後進行以下操作：選擇 Hypervisor ([VMware ESXi]、[Hyper-V]、[Virtuozzo]、[Virtuozzo Hybrid Infrastructure]、[Scale Computing HC3] 或 [oVirt])。只有 Virtuozzo 虛擬機器可復原至 Virtuozzo。如需 V2V 移轉的詳細資訊，請參閱「電腦移轉」。請注意，選擇 Microsoft Azure 作為目標時，您可以選擇相關的 Azure 訂閱、區域和資源群組。選擇主機並指定新電腦名稱，或選擇現有目標電腦。選擇主機並指定新電腦名稱，或選擇現有目標電腦。按一下 [確定]。設定您需要的其他復原選項。[不適用於 Virtuozzo Hybrid Infrastructure 和 Scale Computing HC3] 若要選擇虛擬機器的資料存放區，按一下 [資料存放區] (ESXi)、[路徑] (Hyper-V 和 Virtuozzo)，或 [儲存網域] (Red Hat Virtualization (oVirt))，然後選擇虛擬機器的資料存放區 (儲存空間)。若要檢視每個虛擬磁碟的資料存放區 (儲存空間)、介面以及佈建模式，按一下 [磁碟對應]。除非您要復原 Virtuozzo 容器或 Virtuozzo Hybrid Infrastructure 虛擬機器，否則您可以變更這些設定。若是 Virtuozzo Hybrid Infrastructure，您僅能選擇目標磁碟的儲存原則。方法是，選擇所需的目標磁碟，然後按一下 [變更]。在開啟的刀鋒視窗中，按一下齒輪圖示、選擇儲存原則，然後按一下 [完成]。該對映區段使您還可以選擇要復原的個別磁碟。若是 Microsoft Azure，您可以選擇相關的儲存體類型 (本機備援儲存體 (LRS) 或區域備援儲存體 (ZRS))，以變更每個目標磁碟的儲存體類型。[適用於 VMware ESXi、Hyper-V 和 Virtuozzo] 若要變更記憶體大小、處理器數量，以及虛擬機器的網路連線，請按一下 [VM 設定]。[適用於 Microsoft Azure] 若要變更可用性類型和區域、記憶體大小以及虛擬機器的網路連線 (包括子網路和安全性群組)，請按一下 [VM 設定]。[若是 Virtuozzo Hybrid Infrastructure] 若要變更虛擬機器的記憶體大小和處理器數量，請選擇 [類別]。[僅適用於已安裝保護代理程式的 Windows 電腦] 啟用 [安全復原] 開關以確保復原的資料中沒有惡意軟體。如需有關安全復原如何運作的詳細資訊，請參閱 "安全復原" (第 1 頁)。按一下 [開始復原]。當復原到現有虛擬機器時，請確認您要覆寫磁碟。復原進度會顯示在 [活動] 索引標籤上。" (第 1 頁)。
- 若是虛擬到實體 (V2P) 遷移，請參閱 "復原虛擬機器您可以從其備份復原虛擬機器。您無法在 Cyber Protect 主控台中，為 [合規] 模式下的租用戶復原備份。如需有關如何復原此類備份的詳細資訊，請參閱 "在合規模式下復原租用戶的備份" (第 1 頁)。必要條件復原至虛擬機器時，此虛擬機器必須為停止狀態。軟體預設不會顯示提示，即停止電腦。復原完成後，您必須手動啟動電腦。您可以使用 VM 電源管理復原選項來變更預設行為 (按一下 [復原選項] > [VM 電源管理])。程序執行下列其中一項操作：選擇已備份的電腦，按一下復原，然後選擇復原點。在 [備份儲存] 索引標籤上選擇復原點。按一下[復原] > [整部機器]。如果您想要復原到實體機器，請在復原至中選擇實體機器。否則，請跳過此步驟。只有在目標電腦的磁碟組態完全符合備份中的磁碟組態時，才能復原至實體機器。在此情況下，請繼續在「實體機器」中的步驟 4。否則，我們建議您使用可開機媒體來執行 V2P 移轉。[選用] 軟體預設會自動選擇原始電腦做為目標電腦。若要復原到另

一部虛擬機器，請按一下目標機器然後進行以下操作：選擇 Hypervisor ([VMware ESXi]、[Hyper-V]、[Virtuozzo]、[Virtuozzo Hybrid Infrastructure]、[Scale Computing HC3] 或 [oVirt])。只有 Virtuozzo 虛擬機器可復原至 Virtuozzo。如需 V2V 移轉的詳細資訊，請參閱「電腦移轉」。請注意，選擇 Microsoft Azure 作為目標時，您可以選擇相關的 Azure 訂閱、區域和資源群組。選擇主機並指定新電腦名稱，或選擇現有目標電腦。選擇主機並指定新電腦名稱，或選擇現有目標電腦。按一下 [確定]。設定您需要的其他復原選項。[不適用於 Virtuozzo Hybrid Infrastructure 和 Scale Computing HC3] 若要選擇虛擬機器的資料存放區，按一下 [資料存放區] (ESXi)、[路徑] (Hyper-V 和 Virtuozzo)，或 [儲存網域] (Red Hat Virtualization (oVirt))，然後選擇虛擬機器的資料存放區 (儲存空間)。若要檢視每個虛擬磁碟的資料存放區 (儲存空間)、介面以及佈建模式，按一下 [磁碟對應]。除非您要復原 Virtuozzo 容器或 Virtuozzo Hybrid Infrastructure 虛擬機器，否則您可以變更這些設定。若是 Virtuozzo Hybrid Infrastructure，您僅能選擇目標磁碟的儲存原則。方法是，選擇所需的目標磁碟，然後按一下 [變更]。在開啟的刀鋒視窗中，按一下齒輪圖示、選擇儲存原則，然後按一下 [完成]。該對映區段使您還可以選擇要復原的個別磁碟。若是 Microsoft Azure，您可以選擇相關的儲存體類型 (本機備援儲存體 (LRS) 或區域備援儲存體 (ZRS))，以變更每個目標磁碟的儲存體類型。[適用於 VMware ESXi、Hyper-V 和 Virtuozzo] 若要變更記憶體大小、處理器數量，以及虛擬機器的網路連線，請按一下 [VM 設定]。[適用於 Microsoft Azure] 若要變更可用性類型和區域、記憶體大小以及虛擬機器的網路連線 (包括子網路和安全性群組)，請按一下 [VM 設定]。[若是 Virtuozzo Hybrid Infrastructure] 若要變更虛擬機器的記憶體大小和處理器數量，請選擇 [類別]。[僅適用於已安裝保護代理程式的 Windows 電腦] 啟用 [安全復原] 開關以確保復原的資料中沒有惡意軟體。如需有關安全復原如何運作的詳細資訊，請參閱 "安全復原" (第 1 頁)。按一下 [開始復原]。當復原到現有虛擬機器時，請確認您要覆寫磁碟。復原進度會顯示在 [活動] 索引標籤上。" (第 1 頁) 和 "使用可開機媒體復原磁碟" (第 452 頁)。

透過可開機媒體遷移

您可以使用可開機媒體復原電腦，作為在 Cyber Protect 主控台中執行電腦遷移的替代方法。

在下列情況下，建議您使用可開機媒體：

- 執行非原生支援的遷移。
  例如，使用可開機媒體將實體機器或非 Virtuozzo 虛擬機器復原為 Virtuozzo 主機上的 Virtuozzo 虛擬機器。
- 針對包含邏輯磁碟區 (LVM) 的 Linux 電腦執行遷移。
  使用 Linux 用代理程式或可開機媒體建立備份，然後使用可開機媒體復原備份。
- 提供系統開機所必需的特定硬體驅動程式。
  建置可以使用所需驅動程式的可開機媒體。如需詳細資訊，請參閱 "可開機媒體組建" (第 636 頁)。

Microsoft Azure 和 Amazon EC2 虛擬機器

若要備份 Microsoft Azure 或 Amazon EC2 虛擬機器，請在電腦上安裝保護代理程式。對於實體電腦，備份和復原作業是相同的。不過，您設定機器的數量配額時，系統會將該電腦視為虛擬機器。

這和實體機器的差異之處在於 Microsoft Azure 和 Amazon EC2 虛擬機器無法從可開機媒體開機。若您需要復原至新的 Microsoft Azure 或 Amazon EC2 虛擬機器，請依照以下程序執行。

注意事項
下列復原程序僅適用於包含在 Microsoft Azure 中，以原生方式執行所需所有驅動程式之電腦的備份 (Azure VM 建立的備份、Hyper-V 本機電腦，或裝有 Windows Server 2016 和更新版本的來源電腦)。對於跨平台復原，請參閱這篇知識庫文章。

若要將電腦復原為 Microsoft Azure 或 Amazon EC2 虛擬機器

1. 從 Microsoft Azure 或 Amazon EC2 中的影像/範本建立新的虛擬機器。新電腦的磁碟組態必須與您要復原的電腦組態相同。
2. 在新電腦上安裝 Windows 用代理程式或 Linux 用代理程式。
3. 按照「實體機器」一節中所述的程序復原備份電腦。設定復原時，選擇新電腦做為目標電腦。

建立可開機媒體以復原作業系統

可開機媒體是 CD、DVD、USB 快閃磁碟機或其他卸除式媒體，可讓您無需作業系統的協助，即可在 Linux 環境或 Windows 預先安裝環境/Windows 復原環境 (WinPE/WinRE) 中執行保護代理程式。可開機媒體的主要用途是復原無法啟動的作業系統。

注意事項
可開機媒體不支援混合式磁碟機。

自訂或現成的可開機媒體？

您可以使用 Bootable Media Builder，為 Windows、Linux 或 macOS 電腦，建立自訂的可開機媒體 (Linux 型或 WinPE 型)。在 Linux 型和 WinPE/WinRE 型自訂可開機媒體中，您可以進行其他設定，例如，自動註冊、網路設定或 Proxy 伺服器設定。在 WinPE/WinRE 型自訂可開機媒體中，您也可以新增其他磁碟機。

或者，您可以下載現成的可開機媒體 (僅限 Linux 型)。您可以將現成的可開機媒體用於復原作業，以及存取 Universal Restore 功能。

Linux 型或 WinPE/WinRE 型可開機媒體？

Linux

Linux 型可開機媒體包含以 Linux 核心為基礎的保護代理程式。代理程式可在任何 PC 相容硬體上開機並執行作業，包括裸機和含有已損壞或不支援的檔案系統的電腦。

WinPE/WinRE 型

WinPE 型可開機媒體包含一個稱為 Windows 預先安裝環境 (WinPE) 的最小 Windows 系統和 WinPE 用 Cyber Protection 外掛程式，這個外掛程式是保護代理程式的改版，可在預先安裝環境中執行。WinRE 型可開機媒體使用 Windows 復原環境，而且不需要安裝其他 Windows 套件。

WinPE 被證明是用於含有各種硬體的較大環境中最方便的開機解決方案。

優點：

- 相較於使用 Linux 型可開機媒體，在 Windows 預先安裝環境中使用 Cyber Protection 可享有更多功能。開機 PC 相容硬體進入 WinPE 後，您不僅可以使用保護代理程式，而且還可以使用 PE 命令和指令碼，以及已新增到 PE 的其他外掛程式。
- PE 型可開機媒體有助於克服某些與 Linux 相關的可開機媒體問題，如僅支援特定 RAID 控制器或特定層級的 RAID 陣列。以 WinPE 2.x 及更新版本為基礎的媒體允許動態載入所需的裝置驅動程式。

限制：

- 在使用整合可延伸韌體介面 (UEFI) 的電腦上，以舊於 4.0 之 WinPE 版本為基礎的可開機媒體無法開機。

建立實體可開機媒體

強烈建議您在開始使用磁碟層級備份時，立即建立並測試可開機媒體。此外，在保護代理程式的每次主要更新後重新建立媒體，也是相當不錯的作法。

您可以透過使用相同的媒體復原 Windows 或 Linux。若要復原 Mac OS，請在執行 Mac OS 的電腦上另行建立單獨的媒體。

在 Windows 或 Linux 中建立實體可開機媒體

1. 建立自訂的可開機媒體 ISO 檔案或下載現成的 ISO 檔案。
   若要建立自訂 ISO 檔案，請使用 "可開機媒體組建" (第 636 頁)。
   若要下載現成的 ISO 檔案，請在 Cyber Protect 主控台中選擇一部電腦，然後按一下 **[復原]** > **[更多復原方式...]** > **[下載 ISO 映像]**。
2. [選擇性] 在 Cyber Protect 主控台中，產生註冊權杖。當您下載現成的 ISO 檔案時，會自動顯示註冊權杖。
   此權杖允許可開機媒體存取雲端儲存，而不必提示您輸入登入和密碼。
3. 透過下列其中一種方式，建立實體可開機媒體：
   - 將 ISO 檔案燒錄到 CD/DVD。
   - 透過使用 ISO 檔及其中一個可在線上取得的免費工具，來建立可開機 USB 快閃磁碟機。
     如果您需要啟動 UEFI 電腦，請使用 `[ISO 至 USB]` 或 `[RUFUS]`。若是 BIOS 電腦，則請使用 `[Win32DiskImager]`。在 Linux 中，應使用 `dd` 公用程式。

   若是虛擬機器，您可以將 ISO 檔案當作 CD/DVD 光碟機，連接至您要復原的電腦。

在 macOS 中建立實體可開機媒體

1. 在已安裝 Mac 用代理程式的電腦上，按一下 **[應用程式]** > **[Rescue Media Builder]**。
2. 軟體會顯示已連接的卸除式媒體。選擇您要使之成為可開機的那一個媒體。

   警告！
   磁碟上的所有資料將被清除。

3. 按一下 **[建立]**。
4. 等候軟體建立可開機媒體。

可開機媒體組建

Bootable Media Builder 是建立可開機媒體的專用工具。它會當作選用的元件，安裝在安裝保護代理程式所在的電腦上。

為什麼要使用 Bootable Media Builder?

可供在 Cyber Protect 主控台中下載的現成可開機媒體是以 Linux 核心為基礎。與 Windows PE 不同，其不允許即時插入自訂驅動程式。

Bootable Media Builder 可讓您建立自訂的 Linux 型或 WinPE 型可開機媒體影像。

32 位元或 64 位元?

Bootable Media Builder 會建立同時包含 32 位元及 64 位元元件的可開機媒體。在大多數的情況下，使用整合可延伸韌體介面 (UEFI) 的電腦需要有 64 位元的媒體才能開機。

Linux 可開機媒體

若要建立 Linux 可開機媒體

1. 啟動 **Bootable Media Builder**。
2. 在 **[可開機媒體類型]** 中，選擇 **[預設 (Linux 媒體)]**。
3. 選擇表示磁碟區和網路資源的方式：
   - 採用類似 Linux 磁碟區表示方式的可開機媒體，會將磁碟區顯示為以下格式：hda1 和 sdb2。這種媒體在開始復原前，會先嘗試重建 MD 裝置和邏輯磁碟區 (LVM)。
   - 採用類似 Windows 磁碟區表示方式的可開機媒體，會將磁碟區顯示為以下格式：C: 與 D:。這種媒體可讓您存取動態磁碟區 (LDM)。
4. 指定 Linux 核心的參數。使用空格分隔多個參數。

   例如，為了能夠在每次媒體啟動時選擇可開機代理程式的顯示模式，請輸入：**vga=ask**。如需有關可用參數的詳細資訊，請參閱 "核心參數" (第 637 頁)。
5. [選用] 選擇用於可開機媒體的語言。
6. [選用] 選擇 Windows 在復原後將使用的開機模式 (BIOS 或 UEFI)。
7. 選擇要放在媒體上的元件 – Cyber Protection 可開機代理程式。
8. [選用] 指定開機功能表的逾時間隔。如果未進行此設定，載入器將會等待您選擇要啟動作業系統 (如果有) 還是元件。
9. [選用] 如果您想要將可開機代理程式作業自動化，請選擇 **[使用下列指令碼]** 核取方塊。然後，選擇指令碼之一並指定指令碼參數。如需有關指令碼的詳細資訊，請參閱 "可開機媒體中的指令碼" (第 638 頁)。
10. [選用] 選擇在開機時要如何在 Cyber Protection 服務中註冊可開機媒體。如需有關註冊設定的詳細資訊，請參閱 "註冊可開機媒體" (第 646 頁)。
11. 指定已開機電腦網路介面卡的網路設定，或保留自動 DHCP 設定。
12. [選用] 如果您的網路中已啟用 Proxy 伺服器，請指定其主機名稱/IP 位址和連接埠。
13. 選擇已建立之可開機媒體的檔案類型：

- ISO 影像
- ZIP 檔案

14. 指定可開機媒體檔案的檔案名稱。
15. 在摘要畫面中檢查您的設定，然後按一下 **[繼續]**。

核心參數

您可以指定將會在可開機媒體啟動時自動套用的一或多個 Linux 核心參數。這些參數通常在使用可開機媒體遇到問題時使用。一般來說，可將此欄位留空。

您也可以在開機功能表中按下 F11 鍵來指定這些參數中的任何參數。

參數

指定多個參數時，使用空格將它們隔開。

- **acpi=off**
  停用進階組態與電源介面 (ACPI)。遇到特定硬體組態問題時，您可能需要使用此參數。
- **noapic**
  停用進階可程式中斷控制卡 (APIC)。遇到特定硬體組態問題時，您可能需要使用此參數。
- **vga=ask**
  提示可開機媒體的圖形化使用者介面要使用的視訊模式。若沒有 **vga** 參數，則會自動偵測視訊模式。
- **vga=** *mode_number*
  指定可開機媒體的圖形化使用者介面要使用的視訊模式。模式編號由 *mode_number* 以十六進位格式提供，例如：**vga=0x318**
  與某個模式編號相對應的螢幕解析度和顏色數量在不同的電腦上可能會有所不同。建議您先使用 **vga=ask** 參數來選擇 *mode_number* 的值。
- **quiet**
  載入 Linux 核心時停用啟動訊息顯示，並在載入核心後啟動管理主控台。
  此參數是在建立可開機媒體時以隱含的方式指定，但是您可以在開機功能表中移除此參數。
  如果移除此參數，將顯示所有啟動訊息，然後顯示命令提示字元。若要從命令提示字元啟動管理主控台，請執行命令：**/bin/product**
- **nousb**
  停用 USB (通用序列匯流排) 子系統的載入。
- **nousb2**
  停用 USB 2.0 支援。使用此參數，USB 1.1 裝置仍可運作。某些 USB 磁碟機無法在 USB 2.0 模式下運作時，此參數可讓您以 USB 1.1 模式使用這些磁碟機。
- **nodma**
  停用所有 IDE 硬碟機的直接記憶體存取 (DMA)。防止核心在某些硬體上停止回應。
- **nofw**
  停用 FireWire (IEEE1394) 介面支援。
- **nopcmcia**

停用 PCMCIA 硬體偵測。

- **nomouse**
  停用滑鼠支援。
- *module_name* **=off**
  停用 *module_name* 指定之名稱的模組。例如，若要停用 SATA 模組，請指定：**sata_sis=off**
- **pci=bios**
  強制使用 PCI BIOS，而不直接存取硬體裝置。如果電腦使用非標準 PCI 主機橋接器，則您可能需要使用此參數。
- **pci=nobios**
  停用 PCI BIOS，僅允許使用直接硬體存取方式。可開機媒體無法啟動 (可能由 BIOS 造成) 時，您可能需要使用此參數。
- **pci=biosirq**
  使用 PCI BIOS 呼叫，以取得中斷路由表。如果核心無法配置中斷請求 (IRQ) 或無法找到主機板上的次要 PCI 匯流排，則您可能需要使用此參數。
  這些呼叫在部分電腦上可能無法正常運作。但這可能是取得中斷路由表的唯一方法。
- **LAYOUTS=en-US, de-DE, fr-FR, ...**
  指定可開機媒體的圖形化使用者介面可使用的鍵盤配置。
  若沒有此參數，則只能使用兩種配置：英文 (美國) 和對應到媒體開機功能表中所選語言的配置。
  您可以指定以下任一配置：
  比利時文：**be-BE**
  捷克文：**cz-CZ**
  英文：**en-GB**
  英文 (美國)：**en-US**
  法文：**fr-FR**
  法文 (瑞士)：**fr-CH**
  德文：**de-DE**
  德文 (瑞士)：**de-CH**
  義大利文：**it-IT**
  波蘭文：**pl-PL**
  葡萄牙文：**pt-PT**
  葡萄牙文 (巴西)：**pt-BR**
  俄文：**ru-RU**
  塞爾維亞文 (斯拉夫文)：**sr-CR**
  塞爾維亞文 (拉丁文)：**sr-LT**
  西班牙文：**es-ES**
  在可開機媒體下作業時，使用 CTRL + SHIFT 可在可用配置循環。

可開機媒體中的指令碼

如果您希望可開機媒體執行一組預先定義的作業，可以指定指令碼，同時使用 Bootable Media Builder 建立媒體。因此，每次從媒體啟動電腦時，將會執行指定的指令碼，而且不會顯示使用者介

面。

您可按照指令碼處理慣例選取其中一個預先定義的指令碼或建立自訂指令碼。

預先定義腳本

可開機媒體建立程式提供以下預定義腳本：

- 從雲端存放區復原 (**entire_pc_cloud**)
- 從網路共用復原 (**entire_pc_share**)

指令碼位於安裝 Bootable Media Builder 所在電腦上的下列資料夾中：

- 在 Windows 中：**%ProgramData%\Acronis\MediaBuilder\scripts**
- 在 Linux 中：**/var/lib/Acronis/MediaBuilder/scripts/**

從雲端存放區復原

在可開機媒體開機程式中，指定以下腳本參數：

1. 備份檔案名稱。
2. [選用] 指令碼將用於存取加密備份的密碼。

從網路共用復原

在可開機媒體開機程式中，指定以下腳本參數：

- 網路共用的路徑。
- 網絡共用的使用者名稱和密碼。
- 備份檔案名稱。找出備份檔案名稱：
  a. 在 Cyber Protect 主控台中，移至 **[備份儲存]** > **[位置]**。
  b. 選擇網路共用（如果共用未列出，請按一下 **[新增位置]**）。
  c. 選擇備份。
  d. 按一下**[詳細資料]**。檔案名顯示在 **[備份檔案名稱]** 下方。
- [選用] 指令碼將用於存取加密備份的密碼。

自訂指令碼

重要事項
建立自訂指令碼需要瞭解 Bash 命令語言及 JavaScript 物件標記法 (JSON)。如果您不熟悉 Bash，則可以前往以下網址瞭解：http://www.tldp.org/LDP/abs/html。JSON 規格位於以下網址：http://www.json.org

指令碼的檔案

指令碼必須位於安裝可開機媒體建立程式之電腦上的下列目錄中：

- 在 Windows 中：%**ProgramData%\Acronis\MediaBuilder\scripts**
- 在 Linux 中：**/var/lib/Acronis/MediaBuilder/scripts/**

指令碼必須包含至少三個檔案：

- **<script_file>.sh** - 具有 Bash 指令碼的檔案。建立指令碼時，僅使用一組有限的 Shell 命令，這些命令位於：https://busybox.net/downloads/BusyBox.html。系統也可以使用下列命令：
  - `acrocmd` - 用於備份及復原的命令列公用程式
  - `product` - 啟動可開機媒體使用者介面的命令

  此檔案以及指令碼包括之任何其他檔案 (例如，透過使用 dot 命令) 必須位於 **bin** 子資料夾中。在指令碼中，將其他檔案路徑指定為 **/ConfigurationFiles/bin/<some_file>**。
- **自動啟動** - 用於啟動 **<script_file>.sh** 的檔案。檔案內容必須如下所示：

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** - 包含下列項目的 JSON 檔案：
  - 要在可開機媒體建立程式中顯示的指令碼名稱和說明。
  - 要透過可開機媒體建立程式設定之指令碼變數的名稱。
  - 將針對每個變數顯示在可開機媒體建立程式中的控制參數。

autostart.json 的結構

最上層物件

配對		需要	描述
名稱	值類型		
`displayName`	string	是	要在可開機媒體建立程式中顯示的指令碼名稱。
`description`	string	否	要在可開機媒體建立程式中顯示的指令碼說明。
`timeout`	number	否	啟動指令碼之前開機功能表的逾時值 (秒)。如果未指定配對，則逾時值將為 10 秒。
`variables`	物件	否	您要透過可開機媒體建立程式設定之 **<script_file>.sh** 的任何變數。 該值應該是以下一組配對：變數的字串識別碼與變數的物件 (請參閱下表)。

變數物件

配對		需要	描述
名稱	值類型		
displayName	string	是	**<script_file>.sh** 中使用的變數名稱。
type	string	是	可開機媒體建立程式中顯示的控制類型。此控制用於設定變數值。 如需所有受支援的類型，請參閱下表。
description	string	是	可開機媒體建立程式中控制項上方顯示的控制標籤。
default	如果 type 是 string、multiString、password 或 enum，則為字串 如果 type 是 number、spinner 或 checkbox，則為數字	否	控制項的預設值。如果未指定配對，則根據控制類型，預設值將為空字串或零。 核取方塊的預設值可以是 0 (已清除狀態) 或 1 (已選取狀態)。
order	number (非負數)	是	可開機媒體建立程式中的控制命令。該值越高，相對於 **autostart.json** 中定義之其他控制放置的控制越低。起始值必須是 0。
min (僅限 spinner)	number	否	微調方塊中微調控制的最小值。如果未指定配對，則該值將為 0。
max (僅限 spinner)	number	否	微調方塊中微調控制的最大值。如果未指定配對，則該值將為 100。
step (僅限 spinner)	number	否	微調方塊中微調控制的步驟值。如果未指定配對，則該值將為 1。
items (僅限 enum)	字串陣列	是	下拉式清單的值。
required	number	否	指定控制值是可以為空 (0)，還是不可以為空 (1)。如果未指定配對，則控制值可以為空。

(針對 string、multiString、password 和 enum)			

控制類型

名稱	描述
string	用來輸入或編輯短字串的單一行、無限制文字方塊。
multiString	用來輸入或編輯長字串的多行、無限制文字方塊。
password	用來安全地輸入密碼的單一行、無限制文字方塊。
number	用來輸入或編輯數字的單一行、僅限數字的文字方塊。
spinner	用來輸入或編輯數字的單一行、僅限數字且具有微調控制的文字方塊。也稱為微調方塊。
enum	具有一組固定預先確定值的標準下拉清單。
checkbox	具有兩個狀態的核取方塊 - 已清除狀態或已選取狀態。

下方的樣本 **autostart.json** 包含可用來設定 **<script_file>.sh** 之變數的所有可能控制類型。

```
{
        "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
        }
    }
}
```

WinPE 型和 WinRE 型可開機媒體

您不需要任何額外的準備，就可以建立 WinRE 影像，也可以在安裝 Windows 自動化安裝套件 (AIK) 或 Windows 評定及部署套件 (ADK) 後建立 WinPE 影像。

WinRE 影像

下列作業系統支援建立 WinRE 影像：

- Windows 7 (64 位元)
- Windows 8 (32 位元及 64 位元)
- Windows 8.1 (32 位元及 64 位元)
- Windows 10 (32 位元及 64 位元)
- Windows 11 (64 位元)
- Windows Server 2012 (64 位元)
- Windows Server 2016 (64 位元)
- Windows Server 2019 (64 位元)
- Windows Server 2022 (64 位元)

WinPE 影像

安裝 Windows 自動化安裝套件 (AIK) 或 Windows 評定及部署套件 (ADK) 之後，Bootable Media Builder 支援基於下列任何核心的 WinPE 發行版：

- Windows Vista (PE 2.0)
- Windows Vista SP1 和 Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0)，無論是否有 Windows 7 SP1 (PE 3.1) 的補充
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE 10.0.1xxx)
- Windows 11 (PE 10.0.2xxx)

Bootable Media Builder 支援 32 位元及 64 位元的 WinPE 發行版。32 位元的 WinPE 發行版亦可在 64 位元硬體上運作。不過，使用整合可延伸韌體介面 (UEFI) 的電腦需要有 64 位元的發行版才能開機。

注意事項
WinPE 4 及更新版本的 PE 影像需要約 1 GB 的 RAM 才能運作。

建立 WinPE 或 WinRE 可開機媒體

Bootable Media Builder 提供將 Cyber Protection 與 WinPE 和 WinRE 整合在一起的兩種方法：

- 使用 Cyber Protection 外掛程式，從頭開始建立 ISO 檔案。
- 出於未來任何使用目的 (手動建立 ISO、將其他工具新增至影像等)，將 Cyber Protection 外掛程式新增至 WIM 檔案。

建立 WinPE 或 WinRE 可開機媒體

1. 在安裝保護代理程式所在的電腦上，執行 Bootable Media Builder。
2. 在 **[可開機媒體類型]** 中，選取 **[Windows PE]** 或 **[Windows PE (64 位元)]**。使用整合可延伸韌體介面 (UEFI) 的電腦需要有 64 位元的媒體才能開機。
3. 選擇可開機媒體的子類型：**[WinRE]** 或 **[WinPE]**。

   建立 WinRE 可開機媒體不需要安裝其他任何套件。

   若要建立 64 位元 WinPE 媒體，您必須下載 Windows 自動化安裝套件 (AIK) 或 Windows 評定及部署套件 (ADK)。若要建立 32 位元 WinPE 媒體，除了下載 AIK 或 ADK 之外，您還需要執行下列操作：

   a. 按一下 **下載 WinPE(32 位元) 外掛程式**。

   b. 將外掛程式儲存到 **%PROGRAM_FILES%\BackupClient\BootableComponents\WinPE32**。
4. [選用] 選擇用於可開機媒體的語言。
5. [選用] 選擇 Windows 在復原後將使用的開機模式 (BIOS 或 UEFI)。
6. 指定已開機電腦網路介面卡的網路設定，或保留自動 DHCP 設定。
7. [選用] 選擇在開機時要如何在 Cyber Protection 服務中註冊可開機媒體。如需有關註冊設定的詳細資訊，請參閱 "註冊可開機媒體" (第 646 頁)。
8. [選用] 指定要新增至可開機媒體的 Windows 驅動程式。

   電腦開機進入 Windows PE 或 Windows RE 後，驅動程式即可協助您存取備份所在的裝置。如果您使用 32 位元 WinPE 或 WinRE 發行版本，請新增 32 位元驅動程式；如果您使用 64 位元 WinPE 或 WinRE 發行版本，則新增 64 位元驅動程式。

   若要新增驅動程式：

   - 按一下 **[新增]**，然後指定對應 SCSI、RAID、SATA 控制器、網路介面卡、磁帶機或其他裝置所需 .inf 檔案的路徑。
   - 對要包含在所產生 WinPE 或 WinRE 媒體中的每個驅動程式重複此程序。
9. 選擇已建立之可開機媒體的檔案類型：
   - ISO 影像
   - WIM 影像
10. 指定所產生影像檔案的完整路徑，包括檔案名稱。
11. 在摘要畫面中檢查您的設定，然後按一下 **[繼續]**。

從產生的 WIM 檔案建立 PE 影像 (ISO 檔案)

- 以新建立的 WIM 檔案取代 Windows PE 資料夾中的預設 boot.wim 檔案。以上述範例為例，請輸入：

  ```
  copy c:\RecoveryWIMMedia.wim c:\winpe_x86\ISO\sources\boot.wim
  ```

- 使用 **Oscdimg** 工具。以上述範例為例，請輸入：

  ```
  oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
  ```

警告！
請勿複製貼上此範例。請手動輸入命令，否則命令將會失敗。

準備工作：WinPE 2.x 與 3.x

若要能夠建立或修改 PE 2.x 或 3.x 映像，請在相同的電腦上安裝 Bootable Media Builder 和 Windows 自動化安裝套件 (WAIK)。

準備一部電腦

1. 從 Microsoft 網站下載 AIK 映像檔，如下所示：
   - 若是 Windows Vista (PE 2.0)：https://www.microsoft.com/en-us/download/details.aspx?id=10333
   - 若是 Windows Vista SP1 和 Windows Server 2008 (PE 2.1)：https://www.microsoft.com/en-us/download/details.aspx?id=9085
   - 若是 Windows 7 (PE 3.0)：https://www.microsoft.com/en-gb/download/details.aspx?id=5753

     若是 Windows 7 SP1 (PE 3.1)，您也需要 AIK 補充，網址為 https://www.microsoft.com/en-us/download/details.aspx?id=5188
2. 將映像檔燒錄到 DVD 光碟或 USB 隨身碟。
3. 從映像檔中，安裝以下項目：
   - Microsoft .NET Framework (NETFXx86 或 NETFXx64，取決於您的硬體)
   - MSXML (Microsoft XML 剖析器)
   - Windows AIK
4. 在相同電腦上安裝 Bootable Media Builder。

準備工作：WinPE 4.0 及更新版本

若要能夠建立或修改 PE 4 或更新版本映像，請在相同的電腦上安裝 Bootable Media Builder 和 Windows 評定及部署套件 (ADK)。

準備一部電腦

1. 從 Microsoft 網站下載 ADK 安裝程式。

   支援以下 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. 安裝評定及部署套件。
3. 安裝 Bootable Media Builder。

註冊可開機媒體

在 Cyber Protection 服務中註冊可開機媒體後，允許存取雲端儲存進行備份。您可以在建立可開機媒體時預先設定註冊。如果未預先設定註冊，您葛以在使用媒體啟動電腦後註冊。

在 Cyber Protection 服務中預先設定註冊

1. 在 Bootable Media Builder 中，瀏覽至 **[可開機媒體註冊]**。
2. 在 **[服務 URL]** 中，指定 Cyber Protection 服務位址。
3. [選用] 在 **[顯示名稱]** 中，指定已開機電腦的名稱。
4. 若要在 Cyber Protection 服務中設定自動註冊，選擇 **[自動註冊可開機媒體]** 核取方塊，然後選擇自動註冊層級：
   - **開機時要求註冊權杖**
     權杖必須在每次從此可開機媒體啟動電腦時提供。
   - **使用下列權杖**
     從此可開機媒體啟動電腦時，將會自動註冊。

從可開機媒體啟動電腦後註冊

1. 從可開機媒體啟動電腦。
2. 在啟動視窗中，按一下 **[註冊媒體]**。
3. 在 **[伺服器]** 中，指定 Cyber Protection 服務位址。
4. 在 **[註冊權杖]** 中，輸入註冊權杖。
5. 按一下 **[註冊]**。

網路設定

建立可開機媒體時，您可以預先設定將由可開機代理程式使用的網路連線。您可以預先設定下列參數：

- IP 位址
- 子網路遮罩
- 閘道
- DNS 伺服器
- WINS 伺服器

之後可開機代理程式在電腦上啟動時，該設定會套用到電腦的網路介面卡 (NIC)。如果尚未預先設定設定，代理程式將使用 DHCP 自動設定。

當可開機代理程式在電腦上執行時，您也可以手動設定網路設定。

預先設定多個網路連線

您可以為多達 10 個網路介面卡 (NIC) 預先設定 TCP/IP 設定。為確保為每個 NIC 指定適合設定，在相應伺服器上建立將被自訂的媒體。當您在精靈視窗中選擇一個現有的 NIC 時，會選擇其設定並儲存在媒體上。每個現有 NIC 的 MAC 位址也將儲存在該媒體上。

您可以變更 MAC 位址之外的設定；或為不存在的 NIC 進行設定。

一旦可開機代理程式在伺服器上啟動之後，它將擷取可用 NIC 的清單。此清單按 NIC 佔用的插槽排序，最接近處理器的位於最上方。

可開機代理程式會為每個已知的 NIC 指派適合的設定，並透過其 MAC 位址識別 NIC。在設定包含已知 MAC 位址的 NIC 後，將從上部未指派的 NIC 開始，為剩餘的 NIC 指派您為不存在的 NIC 所進行的設定。

您可以為任何電腦自訂可開機媒體，而不僅限於建立媒體所在的電腦。若要進行此作業，根據它們在該電腦上的插槽順序設定 NIC：NIC1 佔用最接近處理器的插槽，NIC2 位於下一個插槽，依此類推。當可開機代理程式在該電腦上啟動時，它將找不到具有已知 MAC 位址的 NIC，因此將採用與您所使用的相同順序設定 NIC。

範例

可開機代理程式可以使用其中一個網路介面卡，透過生產網路與管理主控台通訊。可以自動設定此連線。用於復原且可變更大小的資料可透過第二個 NIC 傳輸，使用靜態 TCP/IP 設定的方式包括在專用備份網路中。

連線到從可開機媒體開機的電腦

本機連線

如果要直接在從可開機媒體開機的電腦上操作，請按一下啟動視窗中的 **[本機管理此電腦]**。

電腦從可開機媒體開機後，電腦終端機將顯示一個啟動視窗，其中包含向 DHCP 取得或根據預先設定的值設定的 IP 位址。

進行網路設定

若要變更目前工作階段的網路設定，請按一下啟動視窗中的 **[設定網路]**。隨即會顯示 **[網路設定]** 視窗，您可在其中為電腦上的每張網路介面卡 (NIC) 進行網路設定。

電腦重新開機後，將會失去在工作階段期間所做的變更。

新增 VLAN

您可以在 **[網路設定]** 視窗中，新增虛擬區域網路 (VLAN)。如果您需要存取包含於特定 VLAN 中的備份位置，可以使用此功能。

VLAN 主要用於將區域網路分為多個區段。連接到交換器 *[存取]* 連接埠的 NIC 一律可以存取連接埠設定中指定的 VLAN。而連接到交換器 *[主幹]* 連接埠的 NIC，則僅在您於網路設定中有指定 VLAN 時，才能存取連接埠設定中允許的 VLAN。

透過主幹連接埠提供 VLAN 存取

1. 按一下 **[新增 VLAN]**。
2. 選擇可供存取包含所需 VLAN 之區域網路的 NIC。
3. 指定 VLAN 識別碼。

當您按下 **[確定]** 之後，網路介面卡清單中會出現新項目。

如果您需要移除 VLAN，請按一下所需的 VLAN 項目，然後按一下 **[移除 VLAN]**。

可開機媒體的相關本機作業

可開機媒體的相關作業與在執行中作業系統下執行的復原作業類似。差異如下：

1. 在以類似 Windows 磁碟區表示的可開機媒體下，磁碟區的磁碟機代號與 Windows 中的磁碟機代號相同。如果磁碟區在 Windows 中沒有磁碟機代號 (例如系統保留磁碟區)，系統會依磁碟區在磁碟中的順序，將可用代號指定給磁碟區。

   如果可開機媒體無法在電腦上偵測到 Windows，或者偵測到一個以上的 Windows，則系統會依磁碟區在磁碟中的順序，將可用代號指派給所有磁碟區，包括沒有磁碟機代號的磁碟區。因此，磁碟區代號可能與 Windows 中看到的不同。例如，D: 磁碟機在可開機媒體下可能對應的是 Windows 中的 E: 磁碟機。

   注意事項
   建議為磁碟區指派唯一的名稱。

2. 以類似 Linux 磁碟區表示的可開機媒體會將本機磁碟和磁碟區顯示為已卸載 (sda1, sda2...)。
3. 無法排程工作。如果您需要重複作業，則需要從頭開始設定。
4. 記錄的存留期僅限於當前工作階段。您可將整份記錄或篩選出來的記錄項目儲存為一個檔案。

設定顯示模式

當您透過 Linux 可開機媒體啟動電腦時，會根據硬體組態 (監視器和圖形卡規格) 自動偵測顯示視訊模式。如果視訊模式偵測錯誤，請執行下列動作：

1. 在開機功能表中，按下 F11。
2. 在命令列上，輸入 **vga=ask**，然後繼續進行開機。
3. 從所支援的視訊模式清單中選擇適當模式，其方法是輸入其編號 (例如 **318**)，然後按 **Enter**。

如果您不想每次在特定硬體組態上開機時都依照此程序執行，請重新建立可開機媒體，並在 **[核心參數]** 欄位中指定適當的模式編號 (在上述範例中為 **vga=0x318**)。

使用內部部署可開機媒體復原

1. 從可開機媒體啟動電腦。
2. 按一下 **[在本機管理這部電腦]**。
3. 按一下 **[復原]**。
4. 在 **[復原內容]** 中，按一下 **[選擇資料]**。
5. 選擇您要復原的來源備份檔案。
6. 在左下方窗格中，選擇您要復原的磁碟機/磁碟區或檔案/資料夾，然後按一下 **[確定]**。
7. 設定覆寫規則。
8. 設定復原排除。
9. 設定復原選項。
10. 檢查您的設定是否正確，然後按一下 **[確定]**。

可開機媒體的相關遠端作業

注意事項
此功能適用於 Advanced Backup 套件。

若要查看 Cyber Protect 主控台中的可開機媒體，首先您需要先註冊，如 "註冊可開機媒體" (第 646 頁) 中所述。

在 Cyber Protect 主控台中註冊媒體之後，該媒體就會出現在 **[裝置]** > **[可開機媒體]** 索引標籤中。當可開機媒體已經離線超過 30 天時，就會從此索引標籤中消失。

您可以在 Cyber Protect 主控台中遠端管理可開機媒體。例如，您可以復原資料、重新啟動或關閉使用媒體開機的電腦，或檢視有關媒體的資訊、活動和警示。

重要事項
您無法在 主控台中的 **[設定]** > **[代理程式]** 索引標籤上，遠端更新可開機媒體。

若要更新可開機媒體，請建立一個，如 "可開機媒體組建" (第 636 頁) 一節中所述。或者，在 主控台中，按一下您的帳戶圖示 > **[下載]** > **[可開機媒體]** 以下載現成的媒體。

若要使用可開機媒體，從遠端復原檔案或資料夾

1. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[可開機媒體]**。
1. 選擇您要用於資料復原的媒體。
2. 按一下 **[復原]**。
3. 選擇位置，然後選擇您需要的備份。請注意，備份是依照位置篩選的。
4. 選擇復原點，然後按一下 **[復原檔案/資料夾]**。
5. 瀏覽至所需的資料夾，或使用搜尋列以取得所需檔案和資料夾的清單。

   搜尋與語言無關。

   您可以使用一或多個萬用字元 (* 和 ?)。如需有關如何使用萬用字元的詳細資訊，請參閱 "檔案篩選器 (包含/排除)" (第 408 頁)。
6. 按一下可選擇您要復原的檔案，然後按一下 **[復原]**。
7. 在**[路徑]**中，選擇復原目的地。
8. [選用] 對於進階復原設定，按一下 **[復原選項]**。如需詳細資訊，請參閱 "復原選項" (第 463 頁)。
9. 按一下 **[開始復原]**。
10. 選擇其中一個檔案覆寫選項：
    - **覆寫現有的檔案**
    - **如果較舊，請覆寫現有的檔案**
    - **不要覆寫現有檔案**

    選擇是否要自動重新啟動電腦。
11. 按一下 **[繼續]** 開始復原。復原進度會顯示在 **[活動]** 索引標籤上。

若要使用可開機媒體，從遠端復原磁碟、磁碟區或整部電腦

1. 在 **[裝置]** 索引標籤上，前往 **[可開機媒體]** 群組，然後選擇您要用於資料復原的媒體。
2. 按一下 **[復原]**。
3. 選擇位置，然後選擇您需要的備份。請注意，備份是依照位置篩選的。
4. 選擇復原點，然後按一下 **[復原]** > **[整部電腦]**。

   如有必要，請設定目標電腦和磁碟區對應，如 "復原實體電腦本節說明使用 Web 介面來復原實體機器。如果您要復原下列項目，請使用可開機媒體，而不要使用 Web 介面：執行 macOS 的電腦在合規模式下租用戶中的電腦裸機或離線電腦上的任何作業系統邏輯磁碟區（Linux 中邏輯磁碟區管理器所建立的磁碟區）的結構。媒體可讓您自動重新建立邏輯磁碟區結構。您無法將 Intel Mac 的磁碟層級備份復原至使用 Apple 晶片處理器的 Mac，反之亦然。您可以復原檔案和資料夾。如果要復原實體機器選擇已備份的電腦。按一下 [復原]。選擇復原點請注意，復原點是依照位置進行篩選。如果電腦處於離線狀態，復原點就不會顯示。執行下列任何一項作業：如果備份位置是雲端或共用儲存 (即可被其他代理程式存取)，按一下 [選擇電腦]，選擇在線上的目標電腦，然後選擇復原點。在 [備份儲存] 索引標籤上選擇復原點。如 < 使用可開機媒體復原磁碟 > 所述來復原電腦。按一下[復原] > [整部機器]。軟體會自動將備份的磁碟對應到目標電腦的磁碟。如果要復原至其他實體機器，請按一下 [目標電腦]，然後選擇在線上的目標電腦。如果您不滿意對應結果，或磁碟對應失敗，可以按一下 [磁碟區對應] 手動重新對應磁碟。該對應區段使您還可以選擇要復原的個別磁碟或磁碟區。您可以使用右上角的 [切換至...] 連結，在復原磁碟和磁碟區之間切換。[僅適用於已安裝保護代理程式的 Windows 電腦] 啟用 [安全復原] 開關以確保復原的資料中沒有惡意軟體。如需有關安全復原如何運作的詳細資訊，請參閱 "安全復原" (第 1 頁)。按一下 [開始復原]。確認您要以磁碟的備份版本來覆寫磁碟。選擇是否要自動重新啟動電腦。復原進度會顯示在 [活動] 索引標籤上。" (第 1 頁) 中所述。
5. 對於進階復原設定，按一下 **[復原選項]**。如需詳細資訊，請參閱 "復原選項" (第 463 頁)。
6. 按一下 **[開始復原]**。
7. 確認您要以磁碟的備份版本來覆寫磁碟。選擇是否要自動重新啟動電腦。
8. 復原進度會顯示在 **[活動]** 索引標籤上。

若要從遠端重新啟動已開機的電腦

1. 在 **[裝置]** 索引標籤上，前往 **[可開機媒體]** 群組，然後選擇您要用於資料復原的媒體。
2. 按一下 **[重新開機]**。
3. 確認您想要重新啟動使用媒體開機的電腦。

若要從遠端關閉已開機的電腦

1. 在 **[裝置]** 索引標籤上，前往 **[可開機媒體]** 群組，然後選擇您要用於資料復原的媒體。
2. 按一下 **[關機]**。
3. 確認您想要關閉使用媒體開機的電腦。

若要檢視可開機媒體的相關資訊

1. 在 **[裝置]** 索引標籤上，前往 **[可開機媒體]** 群組，然後選擇您要用於資料復原的媒體。
2. 按一下 **[詳細資料]**、**[活動]** 或 **[警示]** 以查看對應的資訊。

若要從遠端刪除可開機媒體

1. 在 **[裝置]** 索引標籤上，前往 **[可開機媒體]** 群組，然後選擇您要用於資料復原的媒體。
2. 按一下 **[刪除]**，從 Cyber Protect 主控台刪除可開機媒體。
3. 確認您要刪除可開機媒體。

Startup Recovery Manager

Startup Recovery Manager 是位於硬碟上的可開機元件。您可以利用 Startup Recovery Manager 啟動可開機救援公用程式，而無須使用個別的可開機媒體。

若發生故障，請重新啟動電腦，等待提示 **[按下 F11，執行 Acronis Startup Recovery Manager]** 出現，然後按下 F11 或從開機功能表選擇 Startup Recovery Manager (如果您使用的是 GRUB 開機載入程式)。Startup Recovery Manager 隨即啟動，您現在可以執行復原。

Windows 和 Linux 電腦支援 Startup Recovery Manager。

重要事項
* 在具有加密系統磁碟區的電腦上啟用 Startup Recovery Manager 要求相同電腦上至少有一個未加密的磁碟區。

磁碟空間需求

Startup Recovery Manager 需要具備用於暫存檔的磁碟空間。需求會根據啟用 Startup Recovery Manager 所在的電腦而有所不同。

下表摘要說明可用的選項。

開機模式	沒有 Secure Zone 的電腦		具有 Secure Zone 的電腦
	具有未加密的系統磁碟區	具有加密的系統磁碟區	具有加密或未加密的系統磁碟區
BIOS	系統磁碟區上有 200 MB	未加密的磁碟區上有 400 MB	Secure Zone 上有 400 MB
UEFI	EFI 系統磁碟分割 (ESP) 上有 200 MB	以下之一： • EFI 系統磁碟分割 (ESP) 上有 400 MB • EFI 系統磁碟分割 (ESP) 上有 200 MB，在開機過程中可存取的未加密磁碟分割上有 200 MB	Secure Zone 上有 400 MB

注意事項
需要重新啟動的復原需要額外的磁碟空間。若要確認需要多少額外空間，請參閱 "磁碟空間需求" (第 452 頁)。

限制

- [不適用於安裝到主開機記錄的 GRUB] 啟用 Startup Recovery Manager 可使用自己的開機碼覆寫主開機記錄 (MBR)。因此，您可能需要在啟用後重新啟用任何第三方開機載入程式。
- [不適用於 GRUB] 在 Linux 中啟用 Startup Recovery Manager 前，建議您將開機載入程式安裝到根磁碟分割的開機記錄或 /boot 磁碟分割的開機記錄，而不是將其安裝到主開機記錄。否則，請在啟用後，手動重新設定開機載入程式。

啟動 Startup Recovery Manager

若要啟用開機過程中的提示 **[按下 F11，執行 AcronisStartup Recovery Manager]** (或者將 **Startup Recovery Manager** 項目新增至 GRUB 功能表)，您必須啟用 Startup Recovery Manager。

注意事項
如果未啟用 Startup Recovery Manager，建立單鍵復原備份的備份作業將會失敗。

若要啟用 Startup Recovery Manager

在具有代理程式的電腦上

1. 在 Cyber Protect 主控台中，選擇您要啟用 Startup Recovery Manager 的電腦。
2. 按一下**[詳細資料]**。
3. 啟用 **Startup Recovery Manager** 開關。

在沒有代理城市的電腦上

1. 使用可開機媒體將電腦開機。
2. 在可開機媒體圖形化介面中，按一下 **[工具]** > **[啟用 Startup Recovery Manager]**。
3. 選擇 **[啟用]**。
4. 按一下 **[確定]**。
5. 在 **[詳細資料]** 索引標籤上，檢查 **[結果]** 列以確認啟用是否成功。
6. 按一下**[關閉]**。

停用 Startup Recovery Manager

停用會停用開機過程中的提示 **[按下 F11，執行 Acronis Startup Recovery Manager]** (或從 GRUB 功能表移除 **Startup Recovery Manager** 項目)。

如果未啟用 Startup Recovery Manager，您仍然可以使用另一個可開機媒體來復原無法開機的電腦。

注意事項
如果未啟用 Startup Recovery Manager，建立單鍵復原備份的備份作業將會失敗。

若要停用 Startup Recovery Manager

在具有代理程式的電腦上

1. 在 Cyber Protect 主控台中，選擇您要停用 Startup Recovery Manager 的電腦。
2. 按一下**[詳細資料]**。
3. 停用 **Startup Recovery Manager** 開關。

在沒有代理城市的電腦上

1. 使用可開機媒體將電腦開機。
2. 在可開機媒體圖形化介面中，按一下 **[工具]** > **[停用 Startup Recovery Manager]**。
3. 選擇 **[停用]**。
4. 按一下 **[確定]**。
5. 在 **[詳細資料]** 索引標籤上，檢查 **[結果]** 列以確認停用是否成功。
6. 按一下**[關閉]**。

實作災難復原

注意事項
此功能不支援 Microsoft Azure 備份位置。

關於 Cyber Disaster Recovery Cloud

Cyber Disaster Recovery Cloud (DR) 是 Cyber Protection 的一部分，可提供災難復原即服務 (DRaaS)。Cyber Disaster Recovery Cloud 可為您提供一個快速且穩定的解決方案，以便在雲端站台上啟動確切的電腦複本，並在發生人為或自然災害時，將工作負載從損毀的原始電腦切換到雲端的復原伺服器。

主要功能

注意事項
部分功能可能需要額外的授權，端視適用的授權模型而定。

- 從單一主控台管理 Cyber Disaster Recovery Cloud 服務
- 使用安全的 VPN 通道，將最多 23 個區域網路延伸至雲端
- 建立與雲端站台的連線，而不需要部署任何 VPN 設備[1] (僅雲端模式)
- 建立本機站台[2]和雲端站台的點對站台連線
- 使用雲端的復原伺服器[3]保護您的電腦
- 使用雲端的主要伺服器[4]保護應用程式和裝置
- 為加密的備份執行自動災難復原作業
- 在隔離的網路中執行測試容錯移轉
- 使用 Runbook[5] 在雲端啟動實際執行環境

軟體需求

支援的作業系統

使用復原伺服器的保護，已針對下列作業系統進行測試：

- CentOS 6.6, 7.x, 8.x
- Debian 9.x, 10.x, 11.x

---

[1][災難復原] 特殊的虛擬機器，可透過安全的 VPN 通道，在區域網路和雲端站台之間連線。VPN 設備是在本機站台上部署的。
[2][災難復原] 在公司內部部署上部署的本機基礎架構。
[3][災難復原] 原始電腦的 VM 複本，以儲存在雲端的受保護伺服器備份為基礎。復原伺服器在發生災難時，用於從原始伺服器切換工作負載。
[4][災難復原] 在本機站台 (例如，復原伺服器) 上沒有連結電腦的虛擬機器。主要伺服器用於保護應用程式或執行各種輔助服務 (例如，網頁伺服器)。
[5][災難復原] 計劃的案例，其中包含可自動執行災難復原動作的可設定步驟。

- Red Hat Enterprise Linux 6.6, 7.x, 8.x
- Ubuntu 16.04, 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 – 所有安裝選項，Nano Server 除外
- Windows Server 2019 – 所有安裝選項，Nano Server 除外
- Windows Server 2022 – 所有安裝選項，Nano Server 除外

軟體可能可搭配其他 Windows 作業系統或 Linux 版本使用，但不提供保證。

注意事項

使用復原伺服器的保護，已針對安裝下列作業系統的 Microsoft Azure VM 進行測試。

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – 所有安裝選項，Nano Server 除外
- Windows Server 2019 – 所有安裝選項，Nano Server 除外
- Windows Server 2022 – 所有安裝選項，Nano Server 除外
- Ubuntu Server 20.04 LTS - Gen2 (Canonical)。如需有關存取復原伺服器主控台的詳細資訊，請參閱 https://kb.acronis.com/content/71616。

支援的虛擬化平台

使用復原伺服器的虛擬機器保護，已針對下列虛擬化平台進行測試：

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- 帶 Hyper-V 的 Windows Server 2008 R2
- 帶 Hyper-V 的 Windows Server 2012/2012 R2
- Windows Server 2016 with Hyper-V – 所有安裝選項，Nano Server 除外
- Windows Server 2019 與 Hyper-V – 所有安裝選項，Nano Server 除外
- Windows Server 2022 with Hyper-V – 所有安裝選項，Nano Server 除外
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- 核心虛擬機器 (KVM) — 僅限完全虛擬化的客體 (HVM)。不支援半虛擬化的客體 (PV)。
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2

VPN 設備已針對下列虛擬化平台進行測試：

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- 帶 Hyper-V 的 Windows Server 2008 R2
- 帶 Hyper-V 的 Windows Server 2012/2012 R2

- Windows Server 2016 with Hyper-V – 所有安裝選項，Nano Server 除外
- Windows Server 2019 與 Hyper-V – 所有安裝選項，Nano Server 除外
- Windows Server 2022 with Hyper-V – 所有安裝選項，Nano Server 除外
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

支援從客體作業系統進行無代理程式備份且具有˙邏輯磁碟區管理員 (LVM) 組態之磁碟區的 Linux 工作負載。

支援從客體作業系統進行無代理程式備份並且有動態磁碟 (LDM) 組態的 Windows 工作負載。

軟體可能可搭配其他虛擬化平台或版本使用，但無法保證。

限制

在 Cyber Disaster Recovery Cloud 中不支援下列平台和設定：

1. 不支援的平台：
   - Virtuozzo 用代理程式
   - macOS
   - 由於 Microsoft 產品條款的緣故，不支援 Windows 桌面作業系統。
   - Windows Server Azure Edition

     Azure Edition 是專門建置的 Windows Server 特殊版本，可在 Azure 中當作 Azure IaaS 虛擬機器 (VM) 執行，或在 Azure Stack HCI 叢集上當作 VM 執行。與 Standard 和 Datacenter Edition 不同的是，Azure Edition 未獲授權，無法在裸機硬體、Windows 用戶端 Hyper-V、Windows Server Hyper-V、第三方虛擬機器 Hypervisor 或第三方雲端中執行。
2. 不支援的設定：

   Microsoft Windows
   - 不支援 Windows 桌面作業系統 (由於 Microsoft 產品條款的緣故)。
   - 不支援具有 FRS 複寫的 Active Directory 服務。
   - 不支援非 GPT 或 MBR 格式 (所謂的「超級軟碟」) 的卸除式媒體。

   Linux
   - 不含磁碟分割表的檔案系統。
   - 使用客體 OS 的代理程式備份，而且擁有包含下列進階邏輯磁碟區管理員 (LVM) 設定之磁碟區的 Linux 工作負載：等量磁碟區、鏡像磁碟區、RAID 0、RAID 4、RAID 5、RAID 6 或 RAID 10 磁碟區。

   注意事項

   不支援已安裝多個作業系統的工作負載。
3. 不支援的備份類型：

- 連續資料保護 (CDP) 復原點不相容。

  重要事項
  如果您從擁有 CDP 復原點的備份建立復原伺服器，則在容錯回復或建立復原伺服器備份期間，您將失去 CDP 復原點中所包含的資料。

- 鑑識備份無法用於建立復原伺服器。

復原伺服器擁有一個網路介面。如果原始電腦有數個網路介面，則只模擬一個。

雲端伺服器未加密。

使用 Microsoft Azure 虛擬機器進行操作

注意事項
部分功能可能需要額外的授權，端視適用的授權模型而定。

您可以將 Microsoft Azure 虛擬機器容錯移轉至 Acronis Cyber Protect Cloud。如需詳細資訊，請參閱 "執行容錯移轉" (第 711 頁)。

之後，您可以從 Acronis Cyber Protect Cloud 容錯回復到 Azure 虛擬機器。容錯回復程序與容錯回復至實體機器的程序相同。如需詳細資訊，請參閱 "執行代理程式型容錯回復 (透過可開機媒體)" (第 716 頁)。

注意事項
若要登錄新的 Azure 虛擬機器進行容錯回復，您可以使用 Azure 中提供的 Acronis Backup VM 擴充功能。

您可以在 Acronis Cyber Protect Cloud 和 Azure VPN 閘道之間設定多站台 IPsec VPN 連線。如需詳細資訊，請參閱 "設定多站台 IPsec VPN" (第 674 頁)。

Cyber Disaster Recovery Cloud 試用版產品

您可以使用 Acronis Cyber Disaster Recovery Cloud 的試用版產品 30 天。在此情況下，災難復原對於合作夥伴租用戶具備下列限制：

- 復原伺服器和主要伺服器無法存取公用網際網路。您無法將公共 IP 位址指派給伺服器。
- IPsec 多站台 VPN 無法使用。

使用異地備援雲端儲存時的限制

異地備援雲端儲存為您的備份資料提供次要位置。次要位置位於地理上與主要存位置不同的區域。區域的地理區隔可確保發生影響其中一個區域並導致備份資料無法復原的災難時，另一個區域將不會受到影響，而且操作將繼續。

重要事項
如果備份儲存位置從主要位置切換到異地備援次要位置，則不支援災難復原服務。

災難復原與加密軟體的相容性

災難復原與下列磁碟層級加密軟體相容：

- Microsoft BitLocker Drive Encryption
- McAfee 端點加密
- PGP 全磁碟加密

注意事項

- 對於具有磁碟層級加密的工作負載，建議您在工作負載的客體作業系統中安裝保護代理程式，並執行代理程式型備份。
- 加密工作負載的無代理程式備份不支援故障移轉和故障回復。

如需有關 Cyber Protection 與加密軟體相容性的詳細資訊，請參閱 "與加密軟體的相容性" (第 39 頁)。

自動刪除雲端站台上未使用的客戶環境

災難復原服務會追蹤針對災難復原用途而建立之客戶環境的使用狀況，並在未使用時自動刪除。

下列準則用於定義客戶租用戶是否作用中：

- 目前至少有一部雲端伺服器，或者在過去七天有雲端伺服器。
  或者
- 已啟用 **[本機站台的 VPN 存取]** 選項，且已建立站台對站台 OpenVPN 通道，或在過去 7 天有從 VPN 設備回報的資料。

其餘所有的租用戶都會被視為非使用中租用戶。系統會針對這類租用戶執行下列操作：

- 刪除 VPN 閘道以及與租用戶相關的所有雲端資源。
- 取消登錄 VPN 設備。

非作用中的租用戶會回復到其連線設定前的狀態。

使用災難復原雲端

注意事項

部分功能可能需要額外的授權，端視適用的授權模型而定。

使用災難復原的基本工作流程如下：

1. 以下列其中一種方式建立要保護的工作負載的復原伺服器：
   - a. 建立一個保護計劃，其中包括 **[災難復原]** 模組和 **[備份]** 模組，並將 **[備份內容]** 設定為 **[整部電腦]** 或系統和開機磁碟區。
   b. 將計劃套用至您的裝置。這將會自動設定預設的災難復原基礎架構。如需詳細資訊，請參

閱建立災難復原保護計劃。

- 手動設定災難復原雲端基礎架構並控制每個步驟。請參閱 "建立復原伺服器" (第 694 頁)。

2. 設定與雲端站台的連線。
   - 僅雲端模式
   - 站台對站台 OpenVPN 連線
   - 多站台 IPsec VPN 連線
   - 點對站台連線
3. 設定自動測試容錯移轉。
4. 執行測試容錯移轉。
5. [發生災難時] 執行實際執行容錯移轉。
6. [發生災難後] 執行容錯回復至本機站台。
7. [選用] 設定 Runbook。

建立災難復原保護計劃

災難復原保護計劃是啟用 **[災難復原]** 模組的保護計劃。

在您啟用災難復原功能並將計劃套用至您的裝置之後，就會建立雲端網路基礎架構。如需詳細資訊，請參閱 "預設雲端網路基礎架構" (第 662 頁)。

注意事項

- 套用災難復原保護計劃只有在復原雲端網路基礎架構不存在時才會加以建立。系統不會變更或重新建立現有的雲端網路。
- 在設定災難復原之後，您將能夠從針對裝置建立復原伺服器之後產生的任何復原點，執行測試或實際執行容錯移轉。在裝置受到災難復原保護之前產生的復原點 (備份) (例如，在建立復原伺服器之前) 無法用於容錯移轉。
- 如果無法偵測裝置的 IP 位址，無法啟用災難復原保護計劃。例如，虛擬機器無代理程式備份且未指派 IP 位址時。
- 當您套用保護計劃時，系統會在雲端站台中指派相同的網路和 IP 位址。IPsec VPN 連線要求雲端站台和本機站台的網路區段不要重疊。如果已設定多站台 IPsec VPN 連線，且您之後將保護計劃套用至一或數個裝置，則您必須另外更新雲端網路，並重新指派雲端伺服器的 IP 位址。如需詳細資訊，請參閱 "重新指派 IP 位址" (第 688 頁)。

建立災難復原保護計劃

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 選擇您要保護的電腦。
3. 按一下 **[保護]**，然後按一下 **[建立計劃]**。
   保護計劃預設設定隨即開啟。
4. 設定備份選項。
   若要使用災難復原功能，此計劃必須在雲端儲存空間備份整部電腦，或僅備份開機及提供必要服務所需的磁碟。
5. 按一下模組名稱旁邊的開關，以啟用 **[災難復原]** 模組。

6. 按一下 **[建立]**。
   已建立計劃並套用至所選電腦。已使用預設參數建立預設網路基礎架構和復原伺服器。如需詳細資訊，請參閱 "編輯復原伺服器的預設設定" (第 661 頁) 和 "預設雲端網路基礎架構" (第 662 頁)。

後續步驟

- 您可以編輯復原伺服器的預設設定。如需詳細資訊，請參閱 "編輯復原伺服器的預設設定" (第 661 頁)。
- 您可以編輯預設網路設定。如需詳細資訊，請參閱 "連線和網路" (第 662 頁)。

編輯復原伺服器的預設設定

當您建立並套用災難復原保護計劃時，會使用預設設定建立復原伺服器。必要時，您可以編輯這些預設設定。

注意事項
´復原伺服器只有在不存在時才會建立。系統不會變更或重新建立現有的復原伺服器。

若要編輯復原伺服器的預設設定

1. 移至 **[裝置]** > **[所有裝置]**。
2. 選擇一個裝置，然後按一下 **[災難復原]**。
3. 編輯復原伺服器的預設設定。
   下表描述復原伺服器設定。

設定	預設值	描述
CPU 和 RAM	自動	復原伺服器的虛擬 CPU 數量和 RAM 數量。系統將會根據原始裝置的 CPU 和 RAM 設定，自訂決定預設設定。
雲端網路	自動	將與伺服器連線的雲端網路。如需有關如何設定雲端網路的詳細資訊，請參閱雲端網路基礎架構。
實際執行網路中的 IP 位址	自動	伺服器將在實際執行網路中具備的 IP 位址。依預設，會設定原始電腦的 IP 位址。
測試 IP 位址	已停用	測試 IP 位址可讓您有能力在隔離的測試網路中測試容錯移轉，並在測試容錯移轉期間，透過 RDP 或 SSH 連線到復原伺服器。在測試容錯移轉模式中，VPN 閘道將會使用 NAT 通訊協定，將測試 IP 位址取代為實際執行 IP 位址。如果未指定測試 IP 位址，則在測試容錯移轉期間只能使用主控台存取伺服器。
網際網路存取	已啟用	可讓復原伺服器在實際或測試容錯移轉期間存取網際網路。預設拒絕 TCP 連接埠 25，以供輸出連

		線使用。
使用公共位址	已停用	具有公共 IP 位址可在容錯移轉或測試容錯移轉期間，讓復原伺服器從網際網路使用。如果您沒有使用公共 IP 位址，則只能在您的實際執行網路中使用該伺服器。若要使用公共 IP 位址，您必須啟用網際網路存取。公共 IP 位址將在您完成設定之後顯示。預設開放 TCP 連接埠 443，以供輸入連線使用。
設定 RPO 閾值	已停用	RPO 閾值會定義上次復原點和目前時間之間的最大可允許時間間隔。此值可以設定在 15 – 60 分鐘、1 – 24 小時、1 – 14 天內。

預設雲端網路基礎架構

將災難復原保護計劃套用至您的工作負載時自動建立的雲端網路基礎架構包含下列元件：

- 每個受保護裝置的復原伺服器。
  復原伺服器是雲端中所選裝置複本的虛擬機器。
  針對每個所選裝置會在 **[待機]** 狀態 (虛擬機器未執行) 下建立具有預設設定的復原伺服器。復原伺服器的大小會依受保護裝置的 CPU 和 RAM 自動調整。
- 雲端站台上的 VPN 閘道。
- 復原伺服器連線的雲端網路。

系統會檢查裝置 IP 位址，如果沒有 IP 位址適用的現有雲端網路，就會自動建立適合的雲端網路。如果您已經有復原伺服器 IP 位址適用的現有雲端網路，將不會變更或重新建立現有的雲端網路。

- 如果您沒有現有的雲端網路或者您是第一次設定災難復原設定，將會根據您裝置的 IP 位址範圍，使用 IANA 建議的最大範圍建立私人用途的雲端網路 (10.0.0.0/8、172.16.0.0/12、192.168.0.0/16)。您可以透過編輯網路遮罩來縮小網路的範圍。
- 如果在多個區域網路上都有您的裝置，則雲端站台上的網路將會變成區域網路的超集。您可以在 **[連線]** 區段中重新設定網路。請參閱 "管理站台對站台 OpenVPN 的網路" (第 670 頁)。
- 如果您需要設定站台對站台的 OpenVPN 連線，請下載並設定 VPN 裝置。請參閱 "設定站台對站台 OpenVPN" (第 668 頁)。請確認您的雲端網路範圍符合連線到 VPN 裝置的區域網路範圍。
- 若要變更預設網路設定，請導覽至 **[災難復原]** > **[連線]**，或在保護計劃的 **[災難復原]** 模組中，按一下 **[移至連線]**。

如果您撤銷、刪除或關閉保護計劃的 **[災難復原]** 模組，將不會自動刪除復原伺服器和雲端網路。如有需要，您可以手動移除災難復原基礎架構。

連線和網路

注意事項
部分功能可能需要額外的授權，端視適用的授權模型而定。

您可以透過 Cyber Disaster Recovery Cloud，定義下列雲端站台的連線類型：

- **僅雲端模式**

  這種類型的連線不需要在本機站台上部署 VPN 設備。

  區域網路和雲端網路是兩個獨立的網路。這種類型的連線意味著容錯移轉所有本機站台受保護的伺服器，或部分容錯移轉不需要與本機站台通訊的獨立伺服器。

  雲端站台上的雲端伺服器可以透過點對站台 VPN，以及公共 IP 位址 (如果已指派) 存取。
- **站台對站台 OpenVPN 連線**

  這種類型的連線必須在本機站台上部署 VPN 設備。

  站台對站台 OpenVPN 連線允許將您的網路延伸至雲端，並保留 IP 位址。

  您的區域網路會透過安全的 VPN 通道連線至雲端站台。如果您在本機站台上有緊密相依的伺服器 (例如，網頁伺服器和資料庫伺服器)，則適合這種類型的連線。如果發生部分容錯移轉，當您在雲端重建這些伺服器中的其中一部伺服器，而其他伺服器則保留在本機站台上時，它們將仍然能夠透過 VPN 通道，與彼此通訊。

  雲端站台上的雲端伺服器可以透過區域網路、點對站台 VPN，以及公共 IP 位址 (如果已指派) 存取。
- **多站台 IPsec VPN 連線**

  此類型的連線需要有支援 IPsec IKE v2 的本機 VPN 裝置。

  當您開始設定多站台 IPsec VPN 連線時，Cyber Disaster Recovery Cloud 會使用公共 IP 位址，自動建立一個雲端 VPN 閘道。

  使用多站台 IPsec VPN 時，您的本機站台會透過安全的 IPsec VPN 通道連線至雲端站台。

  當您有一或數個本機站台主控重要工作負載或緊密相依的服務時，此類型的連線適用於災難復原情境。

  如果其中一部伺服器發生部分容錯移轉，系統會在雲端站台上重新建立該伺服器，而其他伺服器則保留在本機站台上，而且這些伺服器仍然能夠透過 IPsec VPN 通道，與彼此通訊。

  如果其中一個本機站台發生部分容錯移轉，其餘的本機站台則維持運作，而且將仍然能夠透過 IPsec VPN 通道，與彼此通訊。
- **點對站台遠端 VPN 存取**

  使用端點裝置，從外部進行雲端和本機站台工作負載的安全點對站台遠端 VPN 存取。

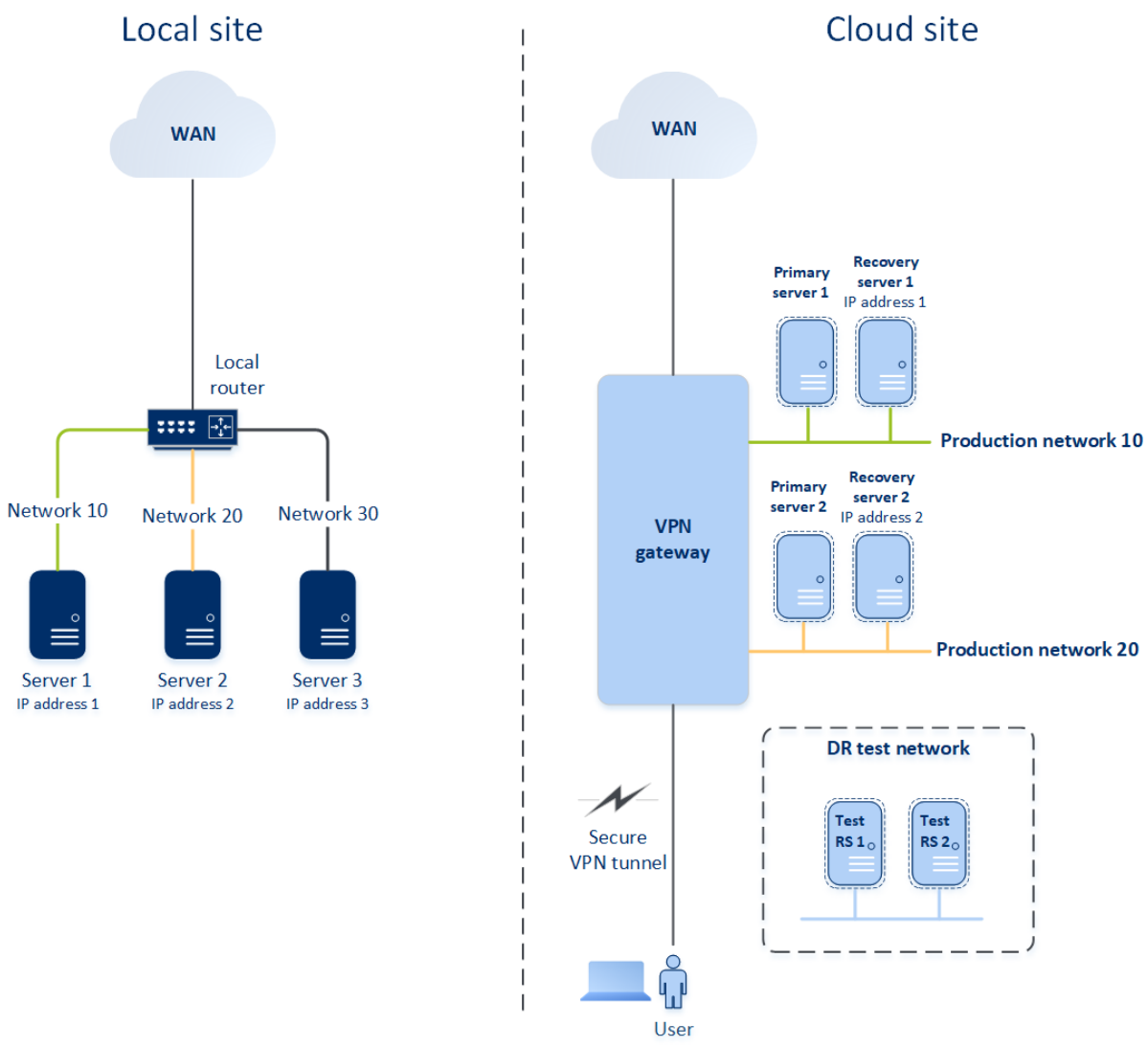
  對於本機站台存取，這種類型的連線必須在本機站台上部署 VPN 設備。

僅雲端模式

僅雲端模式不需要在本機站台上部署 VPN 設備。這意味著您有兩個獨立網路：一個在本機站台上，另一個在雲端站台上。路由是使用路由器，在雲端站台上執行的。

路由的運作方式

如果已建立僅雲端模式，則會使用雲端站台上的路由器執行路由，讓不同雲端網路的伺服器可以彼此通訊。



設定僅雲端模式

僅雲端模式是將災難復原計劃套用至工作負載時自動建立的預設連線類型。

若要在僅雲端模式下設定連線

1. 在 Cyber Protect 主控台中，移至 **[災難復原]** > **[連線]**。
2. 選取 **[僅雲端]**，然後按一下 **[設定]**。

   因此，將會在雲端站台上部署具有已定義之位址和遮罩的 VPN 閘道與雲端網路。

在僅限雲端模式下管理網路

您在雲端最多可以新增和管理 23 個網路。

新增網路

若要新增雲端網路

1. 移至 **[災難復原]** > **[連線]**。
2. 在 **[雲端站台]** 上，按一下 **[新增雲端網路]**。
3. 定義雲端網路參數：網路位址和遮罩，然後按一下 **[完成]**。

因此，將會在雲端站台上建立具有已定義之位址和遮罩的其他雲端網路。

刪除網路

必要條件

要刪除的網路中的所有雲端伺服器都會遭到刪除。

若要刪除雲端網路

1. 移至 **[災難復原]** > **[連線]**。
2. 在 **[雲端站台]** 上，按一下您要刪除的網路位址。
3. 按一下 **[刪除]** 以確認作業。

變更參數

若要變更雲端網路參數

1. 移至 **[災難復原]** > **[連線]**。
2. 在 **[雲端站台]** 上，按一下您要編輯的網路位址。
3. 按一下 **[編輯]**。
4. 定義網路位址和遮罩，然後按一下 **[完成]**。

站台對站台 OpenVPN 連線

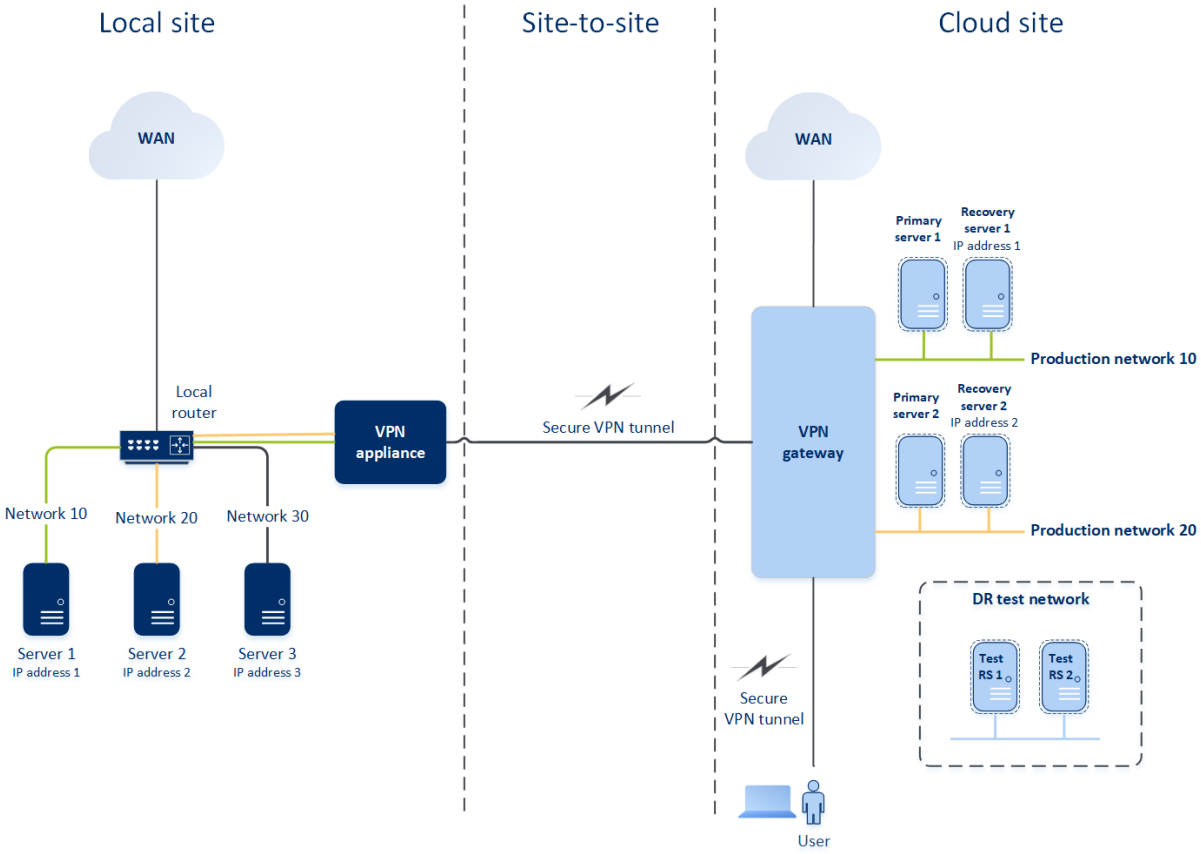
注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

為瞭解網路在 Cyber Disaster Recovery Cloud 中運作的方式，我們將考慮當您有三個網路時，每個本機站台都有一部電腦的情況。您將為下列兩個網站設定災難防護：網路 10 和網路 20。

在以下的圖表中，您可以看到託管電腦所在的本機站台，以及發生災難時啟動雲端伺服器所在的雲端站台。

您可以使用 Cyber Disaster Recovery Cloud，將所有工作負載從本機站台中損毀的電腦容錯移轉至雲端的雲端伺服器。

您在雲端最多可以新增和管理 23 個網路。



若要在本機站台和雲端站台之間建立站台對站台 OpenVPN 連線，會使用 **VPN 裝置**和 **VPN 閘道**。

當您開始在 Cyber Protect 主控台中設定站台對站台 OpenVPN 連線時，會在雲端站台中自動部署 VPN 閘道。

部署 VPN 閘道器後，您必須執行下列動作：

- 在本機站台上部署 VPN 裝置。
- 新增要受保護的網路。
- 在雲端註冊 VPN 裝置。

Cyber Disaster Recovery Cloud 會在雲端建立您的區域網路複本。VPN 裝置與 VPN 閘道之間將會建立一個安全的 VPN 通道。此 VPN 通道可讓您的區域網路延伸至雲端。雲端的實際執行網路將與您的區域網路進行橋接。本機伺服器與雲端伺服器將透過此 VPN 通道進行通訊，就像它們都在相同的乙太網路區段中一樣。路由將由您的本機路由器執行。

對於要保護的每部來源電腦，您必須在雲端站台上建立一部復原伺服器。發生容錯移轉事件之前，其會維持在 **[待命]** 狀態。如果發生災難，而且您開始容錯移轉程序 (在**實際執行模式**下)，將會在雲端啟動代表您受保護電腦確切複本的復原伺服器。其可能會獲指派與來源電腦相同的 IP 位址，而且其可以在相同的乙太網路區段中啟動。您的用戶端將繼續使用伺服器，而不會注意到任何背景變更。

您也可以在**測試模式**下啟動容錯移轉程序。也就是說，來源電腦仍在運作中，同時，擁有相同 IP 位址的個別復原伺服器將會在雲端啟動。若要防止 IP 位址發生衝突，將會在雲端建立一個特殊的虛擬網路 – **測試網路**。測試網路會加以隔離，以防某個乙太網路區段中的來源電腦 IP 位址重複。若要

在測試容錯移轉模式下存取復原伺服器，當您建立復原伺服器時，必須將 **[測試 IP 位址]** 指派給該復原伺服器。您也可以設定復原伺服器的其他參數。

路由的運作方式

建立站台對站台連線時，本機路由器會在雲端網路之間執行路由。VPN 伺服器不會在不同雲端網路中的雲端伺服器間執行路由。如果某個網路中的雲端伺服器想要與另一個雲端網路中的伺服器通訊，流量會通過 VPN 通道到達本機站台上的本機路由器，接著本機路由器會將其路由傳送到另一個網路，然後再通過該通道到達雲端站台上的目的地伺服器。

VPN 閘道

VPN 閘道是允許在本機站台和雲端站台間通訊的主要元件。這是雲端中安裝特殊軟體，並專門設定網路所在的虛擬機器。VPN 閘道具備下列功能：

- 在 L2 模式下，連線雲端中區域網路和實際執行網路的乙太網路區段。
- 提供 iptables 和 ebtables 規則。
- 當做預設路由器和 NAT 使用，以供測試和實際執行網路中的電腦使用。
- 當做 DHCP 伺服器使用。實際執行與測試網路中的所有電腦都會透過 DHCP 取得網路設定 (IP 位址、DNS 設定)。每次雲端伺服器都將從 DHCP 伺服器取得相同的 IP 位址。如果您需要設定自訂 DNS 設定，應該連絡支援小組。
- 當做快取 DNS 使用。

VPN 閘道網路設定

VPN 閘道有數個網路介面：

- 外部介面，連線至網際網路
- 實際執行介面，連線至實際執行網路
- 測試介面，連線至測試網路

此外，系統會新增兩個虛擬介面，分別供點對站台連線和站台對站台連線使用。

部署並初始化 VPN 閘道時，系統會建立橋接 (一個供外部介面使用，一個供用戶端和實際執行介面使用)。雖然用戶端實際執行橋接和測試介面使用相同的 IP 位址，但是 VPN 閘道可以使用特定技術，正確路由傳送套件。

VPN 設備

VPN 裝置是本機站台上已安裝 Linux 的一部虛擬機器，其中安裝了特殊軟體，而且具有特殊網路設定。此裝置允許在本機站台和雲端站台之間進行通訊。

啟用站台對站台連線

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

在下列情況下，您可以啟用站台對站台連線：

- 如果您需要雲端站台上的雲端伺服器與本機站台上的伺服器通訊。
- 容錯移轉至雲端之後，會復原本機基礎架構，而且您會想要將伺服器容錯回復至本機站台。

若要啟用站台對站台連線

1. 移至 **[災難復原]** > **[連線]**。
2. 按一下 **[顯示屬性]**，然後啟用 **[站台對站台連線]** 選項。

因此會在本機站台和雲端站台之間啟用站台對站台 VPN 連線。Cyber Disaster Recovery Cloud 服務會從 VPN 設備取得網路設定，並將區域網路延伸至雲端站台。

設定站台對站台 OpenVPN

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

VPN 裝置的需求

系統需求

- 1 顆 CPU
- 1 GB RAM
- 8 GB 磁碟空間

連接埠

- TCP 443 (輸出) - 用於 VPN 連線
- TCP 80 (輸出) - 用於自動更新設備

請確認您的防火牆以及您網路安全性系統的其他元件允許透過這些連接埠連線到任何 IP 位址。

設定站台對站台 OpenVPN 連線

VPN 設備會將您的區域網路透過安全的 VPN 通道延伸至雲端。此類連線通常稱為「站台對站台」(S2S) 連線。您可以依照下方的程序或觀看影片教學。

透過 VPN 設備設定連線

1. 在 Cyber Protect 主控台中，移至 **[災難復原]** > **[連線]**。
2. 選擇 **[站台對站台 OpenVPN 連線]**，然後按一下 **[設定]**。
   系統會開始在雲端部署 VPN 閘道。這需要花費一些時間。此時，您可以繼續進行下一個步驟。

   注意事項
   VPN 閘道不會另外收費。如果未使用災難復原功能，則會將它刪除，也就是說，雲端會有七天沒有主要伺服器或復原伺服器。

3. 在 **[VPN 設備]** 區塊中，按一下 **[下載並部署]**。根據您所使用的虛擬化平台，下載使用,下載適用於 VMware vSphere 或 Microsoft Hyper-V 的 VPN 設備。

4. 部署設備，並將其連線至實際執行網路。

   在 vSphere 中，確認已啟用 **[混合模式]** 和 **[偽造傳輸]**，並針對將 VPN 設備連線到實際執行網路的所有虛擬交換器，設定為 **[接受]**。若要存取這些設定，請在 vSphere Client 中選取主機 > **[摘要]** > **[網路]**，然後選取交換器 > **[編輯設定...]** > **[安全性]**。

   在 Hyper-V 中，建立具有 1024 MB 記憶體的**第 1 代**虛擬機器。此外，建議您為該電腦啟用 **[動態記憶體]**。建立電腦之後，前往 **[設定]** > **[硬體]** > **[網路卡]** > **[進階功能]** 並選取 **[啟用 MAC 位址詐騙]** 核取方塊。
5. 開啟設備電源。
6. 開啟設備主控台，並以 "admin"/"admin" 使用者名稱和密碼登入。
7. [選用] 變更密碼。
8. [選用] 如有需要，變更網路設定。定義將當做網際網路連線的 WAN 介面使用的介面。
9. 使用公司系統管理員的認證，在 Cyber Protection 服務中登錄設備。

   這些認證僅能用於擷取憑證一次。資料中心 URL 是預先定義的。

   注意事項

   如果為您的帳戶設定雙重驗證機制，系統也將提示您輸入 TOTP 代碼。如左已啟用雙重驗證機制，但尚未為您的帳戶是定，則您無法登錄 VPN 設備。首先，您必須移至 Cyber Protect 主控台登入頁面，並為您的帳戶完成雙重驗證機制設定。如需有關雙重驗證機制的更多詳細資訊，請參閱《管理入口網站系統管理員指南》。

設定完成之後，該設備將顯示 **[線上]** 狀態。此設備會連線到 VPN 閘道，並開始將網路相關資訊從所有作用中介面回報到 Cyber Disaster Recovery Cloud 服務。Cyber Protect 主控台會根據來自 VPN 裝置的資訊，顯示介面。

管理 VPN 設備設定

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

在 **[災難復原]** > **[連線]** 索引標籤上，您可以：

- 下載記錄檔。
- 取消登錄裝置 (如果您需要重設 VPN 裝置設定或切換到僅雲端模式)。

若要存取這些設定，請按一下 **[VPN 裝置]** 區塊中的 **i** 圖示。

在 VPN 設備主控台中，您可以：

- 變更設備的密碼。
- 檢視/變更網路設定，並定義將當做網際網路連線的 WAN 使用的介面。
- 註冊/變更註冊帳戶 (透過重複註冊)。
- 重新啟動 VPN 服務。
- 重新啟動 VPN 設備。
- 執行 Linux 殼層命令 (僅適用於進階疑難排解情況)。

管理站台對站台 OpenVPN 的網路

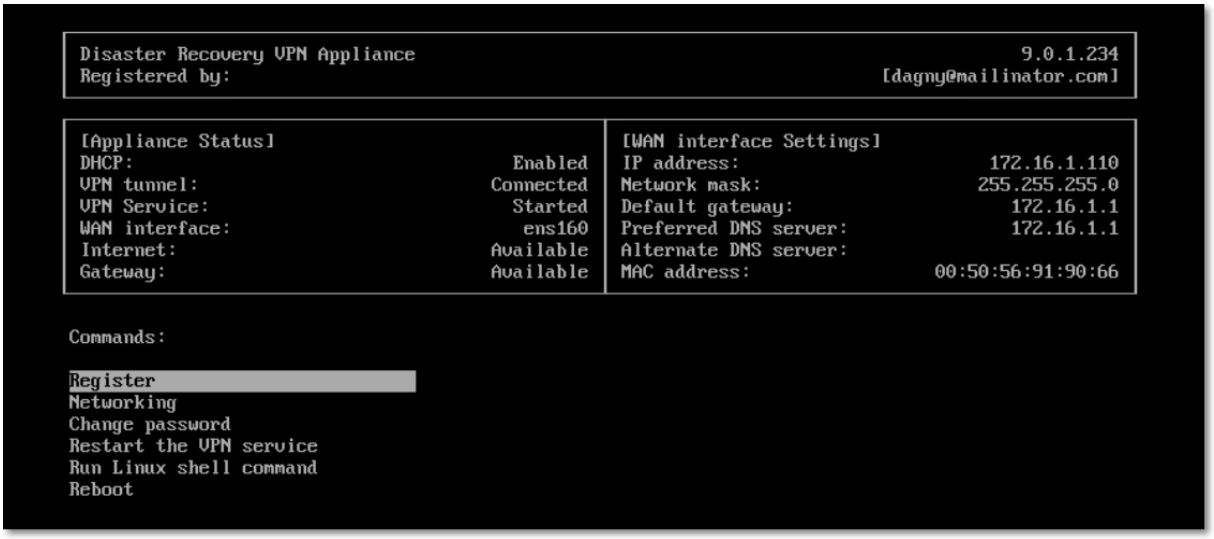
注意事項
部分功能可能需要額外的授權，端視適用的授權模型而定。

您在雲端最多可以新增和管理 23 個網路。

新增網路

若要在本機站台上新增網路，並將其延伸到雲端

1. 在 VPN 設備上，使用您要在雲端延伸的區域網路，設定新的網路介面。
2. 登入 VPN 設備主控台。
3. 在 **[網路]** 區段中，設定新介面的網路設定。



VPN 設備會開始將網路相關資訊從所有作用中介面回報到 Cyber Disaster Recovery Cloud。Cyber Protect 主控台會根據來自 VPN 裝置的資訊，顯示介面。

刪除網路

若要刪除延伸至雲端的網路

1. 登入 VPN 設備主控台。
2. 在 **[網路]** 區段中，選取您要刪除的介面，然後按一下 **[清除網路設定]**。
3. 確認作業。

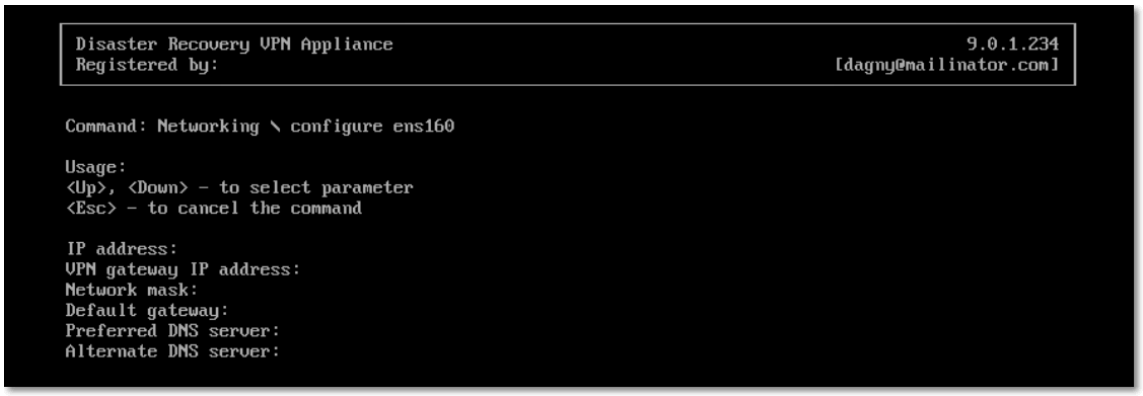
因此，透過安全的 VPN 通道延伸至雲端的區域網路將會遭到停止。此網路將會當做獨立的雲端區段運作。如果使用此介面從雲端站台傳遞流量或將流量傳遞到雲端站台，將會中斷與雲端站台的所有網路連線。

變更參數

若要變更網路參數

1. 登入 VPN 設備主控台。
2. 在 **[網路]** 區段中，選取您要編輯的介面。
3. 按一下 **[編輯網路設定]**。
4. 選擇其中一個選項：
   - 若要透過 DHCP 自動設定網路，按一下 **[使用 DHCP]**，然後確認操作。
   - 若要手動設定網路，按一下 **[設定靜態 IP 位址]**，進行設定，然後按一下 **Enter**。

設定	描述
IP 位址	區域網路中介面的 IP 位址。
VPN 閘道 IP 位址	為網路的雲端區段保留的特殊 IP 位址，可讓 Cyber Disaster Recovery Cloud 服務正常運作。
網路遮罩	區域網路的網路遮罩。
預設閘道	本機站台上的預設閘道。
慣用的 DNS 伺服器	本機站台上的主要 DNS 伺服器。
替代的 DNS 伺服器	本機站台上的次要 DNS 伺服器。



允許透過 L2 VPN 的 DHCP 流量

如果本機站台上的裝置是從 DHCP 伺服器取得其 IP 位址，您可以使用災難復原保護 DHCP 伺服器，將其容錯移轉至雲端，然後允許 DHCP 流量透過 L2 VPN 執行。因此，您的 DHCP 伺服器將在雲端上執行，但會繼續將 IP 位址指派給本機裝置。

必要條件

必須設定雲端的站台對站台 L2 VPN 連線類型。

若要允許透過 L2 VPN 連線的 DHCP 流量

1. 移至 **[災難復原]** > **[連線]** 索引標籤。
2. 按一下 **[顯示屬性]**。
3. 啟用 **[允許透過 L2 VPN 的 DHCP 流量]** 開關。

從站台對站台 OpenVPN 切換至多站台 IPsec VPN

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以輕鬆地從站台對站台 OpenVPN 連線切換到多站台 IPsec VPN 連線，也可以輕鬆地從多站台 IPsec VPN 連線切換到站台對站台 OpenVPN 連線。

當您切換連線類型時，作用中的 VPN 連線會遭到刪除，但是會保留雲端伺服器和網路設定。但是，您仍然需要重新指派雲端網路和伺服器的 IP 位址。

下表比交站台對站台 OpenVPN 連線與多站台 IPsec VPN 連線的基本特性。

	站台對站台 OpenVPN	**多站台 IPsec VPN**
本機站台支援	單一	單一、多個
VPN 閘道模式	L2 Open VPN	L3 IPsec VPN
網路區段	將區域網路延伸到雲端網路	區域網路區段和雲端網路區段不應重疊
支援本機站台的點對站台存取	是	否
支援雲端站台的點對站台存取	是	是
需要公共 IP 產品項目	否	是

從站台對站台 OpenVPN 連線切換到多站台 IPsec VPN 連線

1. 在 Cyber Protect 主控台中，移至 **[災難復原]** > **[連線]**。
2. 按一下 **[顯示屬性]**。
3. 按一下 **[切換到多站台 IPsec VPN]**。
4. 按一下 **[重新設定]**。
5. 針對雲端網路和雲端伺服器，重新指派 IP 位址。
6. 設定多站台 IPsec 連線設定。

停用站台對站台連線

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

如果您不需要雲端站台上的雲端伺服器與本機站台上的伺服器通訊，您可以停用站台對站台連線。

若要停用站台對站台連線

1. 移至 **[災難復原]** > **[連線]**。
2. 按一下 **[顯示屬性]**，然後停用 **[站台對站台連線]** 選項。

因此，本機站台將與雲端站台中斷連線。

多站台 IPsec VPN 連線

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以使用多站台 IPsec VPN 連線來連線單一本機站台，或透過安全的 L3 IPsec VPN 連線，將多個本機站台連線到 Cyber Disaster Recovery Cloud。

如果您有下列其中一個使用案例，此連線類型適用於災難復原情境：

- 您有一個本機站台主控重要工作負載。
- 您有多個本機站台主控重要工作負載，例如不同地點的辦公室。
- 您使用第三方軟體站台或受管理服務供應商站台，並透過 IPsec VPN 通道，連線到這些站台。

若要在本機站台和雲端站台之間建立多站台 IPsec VPN 通訊，會使用 **VPN 閘道**。當您開始在 Cyber Protect 主控台中設定多站台 IPsec VPN 連線時，會在雲端站台中自動部署 VPN 閘道。您應該設定雲端網路區段，並確認這些區段沒有與區域網路區段重疊。系統會在本機站台和雲端站台之間建立一個安全的 VPN 通道。本機伺服器和雲端伺服器可以透過此 VPN 通道通訊，如同它們全都位於相同的乙太網路區段。

對於要保護的每部來源電腦，您必須在雲端站台上建立一部復原伺服器。它會維持在 **[待命]** 狀態，直到發生生容錯移轉事件為止。如果發生災難，而且您開始容錯移轉程序 (在**實際執行模式**下)，會在雲端啟動代表您受保護電腦確切複本的復原伺服器。您的用戶端可以繼續使用伺服器，而不會注意到任何背景變更。

您也可以在**測試模式**下啟動容錯移轉程序。也就是說，來源電腦仍在運作中，同時，個別復原伺服器會在雲端中建立之特殊虛擬網路中的雲端啟動 – **測試網路**。測試網路會加以隔離，以防其他雲端網路區段中的 IP 位址重複。

VPN 閘道

允許在本機站台和雲端站台間通訊的主要元件為 **VPN 閘道**。這是雲端中安裝特殊軟體，並專門設定網路所在的虛擬機器。VPN 閘道提供下列功能：

- 在 L3 IPsec 模式下，連線雲端中區域網路和實際執行網路的乙太網路區段。
- 當做預設路由器和 NAT 使用，以供測試和實際執行網路中的電腦使用。
- 當做 DHCP 伺服器使用。實際執行與測試網路中的所有電腦都會透過 DHCP 取得網路設定 (IP 位址、DNS 設定)。每次雲端伺服器都將從 DHCP 伺服器取得相同的 IP 位址。
  如果您希望，可以設定自訂 DNS 設定。如需詳細資訊，請參閱 "設定自訂 DNS 伺服器" (第 689 頁)。
- 當做快取 DNS 使用。

路由的運作方式

使用雲端站台上的路由器執行雲端網路之間的路由，讓不同雲端網路的伺服器可以彼此通訊。

設定多站台 IPsec VPN

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以透過下列兩種方式，設定多站台 IPsec VPN 連線：

- 從 **[災難復原]** > **[連線]** 索引標籤。
- 在一或數個裝置上套用保護計劃，然後從自動建立的站台對站台 OpenVPN 連線，自動切換到多站台 IPsec VPN 連線、設定多站台 IPsec VPN 設定，並重新指派 IP 位址。

[連線] 索引標籤

從 [連線] 標籤設定多站台 IPsec VPN 連線

1. 在 Cyber Protect 主控台中，移至 **[災難復原]** > **[連線]**。
2. 在 **[多站台 VPN 連線]** 區段中，按一下 **[設定]**。
   VPN 閘道是在雲端站台上部署的。
3. 設定多站台 IPsec VPN 設定。

保護計劃

從保護計劃設定多站台 IPsec VPN 連線

1. 在 Cyber Protect 主控台中，移至 **[裝置]**。
2. 將保護計劃套用到清單中的一或多個裝置。
   系統會針對站台對站台的 OpenVPN 連線，自動設定復原伺服器和雲端基礎架構設定。
3. 移至 **[災難復原]** > **[連線]**。
4. 按一下 **[顯示屬性]**。
5. 按一下 **[切換到多站台 IPsec VPN]**。
6. 設定多站台 IPsec VPN 設定。
7. 針對雲端網路和雲端伺服器，重新指派 IP 位址。

設定多站台 IPsec VPN 設定

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

設定多站台 IPsec VPN 之後，您必須在 **[災難復原]** > **[連線]** 索引標籤上設定雲端站台和本機站台設定。

必要條件

- 已設定多站台 IPsec VPN 連線。如需有關設定多站台 IPsec VPN 連線的詳細資訊，請參閱 "設定多站台 IPsec VPN" (第 674 頁)。
- 每個本機 IPsec VPN 閘道都有一個公共 IP 位址。
- 您的雲端網路具備足夠的 IP 位址，可供作為受保護電腦複本的雲端伺服器 (在實際執行網路中) 以及復原伺服器 (根據您的需求，擁有一或兩個 IP 位址) 使用。
- [如果您在本機站台和雲端站台之間使用防火牆] 在本機站台上要允許下列 IP 通訊協定和 UDP 連接埠：IP 通訊協定 ID 50 (ESP)、UDP 連接埠 500 (IKE) 和 UDP 連接埠 4500。
- 本機站台上的 NAT-T 設定遭到停用。

設定多站台 IPsec VPN 連線

1. 將一或多個網路新增到雲端站台。
   a. 按一下 **[新增網路]**。

      注意事項
      新增雲端網路時，系統將會自動新增擁有相同網路位址和遮罩的對應測試網路，以執行測試容錯移轉。測試網路中的雲端伺服器與雲端實際執行網路中的雲端伺服器擁有相同的 IP 位址。如果您需要在測試容錯移轉期間，從實際執行網路存取雲端伺服器，請在建立復原伺服器時，為其指派另一個測試 IP 位址。

   b. 在 **[網路位址]** 欄位中，輸入網路的 IP 位址。

      注意事項
      請確認雲端網路沒有與您環境中的任何區域網路重疊。否則，無法建立通道。

   c. 在 **[網路遮罩]** 欄位中，輸入網路的遮罩。
   d. 按一下 **[新增]**。
2. 依照適用於本機站台的建議，為您希望連線到雲端站台的每個本機站台進行設定。如需有關這些建議的詳細資訊，請參閱 "對於本機站台的一般建議" (第 676 頁)。
   a. 按一下 **[新增連線]**。
   b. 輸入本機 VPN 閘道的名稱。
   c. 輸入本機 VPN 閘道的公共 IP 位址。
   d. [選用] 輸入本機 VPN 閘道的描述。
   e. 按 **[下一步]**。
   f. 在 **[預先共用金鑰]** 欄位中，輸入預先共用金鑰，或按一下 **[產生新的預先共用金鑰]**，使用自動產生的值。

      注意事項
      您必須為本機和雲端 VPN 閘道使用相同的預先共用金鑰。

   g. 按一下 **[IPsec/IKE 安全性設定]** 以進行設定。如需有關您可以進行之設定的詳細資訊，請參閱 "IPsec/IKE 安全性設定" (第 676 頁)。

注意事項
您可以使用自動填入的預設設定，或使用自訂值。僅支援 IKEv2 通訊協定連線。建立 VPN 時的預設 **[啟動動作]** 為 **[新增]**(您的本機 VPN 閘道會起始連線)，但是您可以將其變更為 **[啟動]**(雲端 VPN 閘道會起始連線)或 **[路由]**(適用於支援路由選項的防火牆)。

h. 設定 **[網路政策]**。
網路政策會指定 IPsec VPN 所連線的網路。使用 CIDR 格式，輸入網路的 IP 位址和遮罩。區域網路區段和雲端網路區段不應重疊。

i. 按一下 **[儲存]**。

對於本機站台的一般建議

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

當您為多站台 IPsec VPN 連線設定本機站台時，請考慮下列建議：

- 針對每個 IKE 階段，請為下列參數設定至少一個在雲端站台中設定的值：加密演算法、雜湊演算法以及 Diffie-Hellman 群組號碼。
- 針對為 IKE 階段 2 在雲端站台中設定的 Diffie-Hellman 群組號碼，使用至少其中一個值，啟用 [完整轉寄密碼]。
- 針對 IKE 階段 1 和 IKE 階段 2，設定與雲端站台中相同的 **[存留時間]** 值。
- 不支援使用 NAT 周遊 (NAT-T) 的設定。停用本機站台上的 NAT-T 設定。否則，無法交涉其他 UDP 封裝。
- **[啟動動作]** 設定可定義哪一端起始連線。預設值 **[新增]** 意指本機站台起始連線，而雲端站台正在等待連線起始。如果您希望雲端站台起始連線，請將值變更為 **[啟動]**；如果您希望兩端都能夠起始連線 (適用於支援路由選項的防火牆)，則將該值變更為 **[路由]**。

如需詳細資訊以及不同解決方案的設定範例，請參閱：

- 本系列的知識庫文章
- 本影片範例

IPsec/IKE 安全性設定

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

下表提供有關 IPsec/IKE 安全性參數的詳細資訊。

參數	描述
加密演算法	將用於確保在傳輸中無法檢視資料的加密演算法。預設會選擇所有演算法。您必須在本機閘道裝置上，針對每個 IKE 階段設定至少其中一個所選演算

參數	描述
	法。
雜湊演算法	將用於驗證資料完整性和真實性的雜湊演算法。預設會選擇所有演算法。您必須在本機閘道裝置上，針對每個 IKE 階段設定至少其中一個所選演算法。
Diffie-Hellman 群組號碼	Diffie-Hellman 群組號碼可定義網際網路金鑰交換 (IKE) 程序中使用之金鑰的強度。 群組號碼越高越安全，但是需要額外的時間讓金鑰運算。 預設會選擇所有群組。您必須在本機閘道裝置上，針對每個 IKE 階段設定至少其中一個所選群組。
存留時間 (秒)	存留時間值可透過使用者封包的一組加密/驗證金鑰，決定從成功交涉到過期的連線執行個體持續時間。 階段 1 的範圍：900-28800 秒，預設為 28800。 階段 2 的範圍：900-3600 秒，預設為 3600。 階段 2 的存留時間必須小於階段 1 的存留時間。 連線會在過期之前，透過金鑰處理通道進行重新交涉，請參閱**重設金鑰寬限時間**。如果本機和遠端的存留時間不一致，則存留時間較長的那一端將會發生替換連線的混亂情況。另請參閱**重設金鑰寬限時間**和**重設金鑰模糊資料**。
重設金鑰寬限時間 (秒)	連線過期或金鑰處理通道過期之前的寬限時間，在此期間內，VPN 連線的本機端會嘗試交涉替換。系統會根據**重設金鑰模糊資料**的值，隨機選擇重設金鑰的確切時間。僅在本機相關，遠端無需對此達成共識。範圍：900-3600 秒。預設值為 3600。
重新執行視窗大小 (封包)	此連線的 IPsec 重新執行視窗大小。 預設值 -1 使用在 strongswan.conf 檔案中，以 charon.replay_window 設定的值。 只有在使用 Netlink 後端時，才支援大於 32 的值。 值為 0 時，會停用 IPsec 重新執行保護。
重設金鑰模糊資料 (%)	隨機增加寬限位元組、寬限封包和寬限時間的百分比上限以隨機選擇重設金鑰間隔 (對於具有許多連線的主機很重要)。 重設金鑰模糊資料值可以超過 100%。marginTYPE 的值在隨機增加之後，不得超過 lifeTYPE，其中 TYPE 是其中一個位元組 (封包或時間)。

參數	描述
	值為 0% 時，會停用隨機選擇。僅在本機相關，遠端無需對此達成共識。
DPD 逾時 (秒)	發生無作用對等偵測 (DPD) 逾時前等待的時間。您可以將值指定為 30 或更高。預設值為 30。
無作用對等偵測 (DPD) 逾時動作	無作用對等偵測 (DPD) 逾時發生後採取的動作。 **重新啟動** - DPD 逾時發生時，重新啟動工作階段。 **清除** - DPD 逾時發生時，結束工作階段。 **無** - DPD 逾時發生時，不採取任何動作。
啟動動作	決定哪一端起始連線，並為 VPN 連線建立通道。 **新增** - 您的本機 VPN 閘道會起始連線。 **啟動** - 雲端 VPN 閘道會起始連線。 **路由** - 適用於支援路由選項的 VPN 閘道。只有在存在從本機 VPN 閘道或雲端 VPN 閘道起始的流量時，通道才會啟動。

從多站台 IPsec VPN 切換至站台對站台 OpenVPN

您可以輕鬆地從多站台 IPsec VPN 連線切換到站台對站台 OpenVPN 連線。

當您切換連線類型時，作用中的 VPN 連線會遭到刪除，但是會保留雲端伺服器和網路設定。但是，您仍然需要重新指派雲端網路和伺服器的 IP 位址。

下表比交站台對站台 OpenVPN 連線與多站台 IPsec VPN 連線的基本特性。

	站台對站台 OpenVPN	多站台 IPsec VPN
本機站台支援	單一	單一、多個
VPN 閘道模式	L2 Open VPN	L3 IPsec VPN
網路區段	將區域網路延伸到雲端網路	區域網路區段和雲端網路區段不應重疊
支援本機站台的點對站台存取	是	否
支援雲端站台的點對站台存取	是	是
需要公共 IP 產品項目	否	是

若要從多站台 IPsec VPN 連線切換到站台對站台 OpenVPN 連線

1. 在 Cyber Protect 主控台中，移至 **[災難復原]** > **[連線]**。
2. 按一下 **[顯示屬性]**。
3. 按一下 **[切換到站台對站台 OpenVPN]**。
4. 按一下 **[重新設定]**。
5. 針對雲端網路和雲端伺服器，重新指派 IP 位址。
6. 設定切換站台對站台連線設定。

疑難排解 IPsec VPN 設定

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

當您設定或使用 IPsec VPN 連線時，可能會遇到問題。

您可以在 IPsec 記錄檔中深入瞭解您所遇到的問題，並查閱「疑難排解 IPsec VPN 設定問題」主題，以找出部分可能會發生的常見問題的可能解決方案。

疑難排解 IPsec VPN 設定問題

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

下表描述最常發生的 IPsec VPN 設定問題，並說明其疑難排解方式。

問題	可能的解決方案
我看到下列錯誤訊息：**IKE 第 1 階段交涉錯誤。請檢查雲端和本機站台上的 IPsec IKE 設定。**	按一下 **[重試]**，然後確認是否出現更具體的錯誤訊息。例如，更具體的錯誤訊息可能是關於演算法不相符或預先共用金鑰不正確的錯誤訊息。 **注意事項** 基於安全性，下列限制適用於 IPsec VPN 連線： • 在 RFC8247 中需要取代 IKEv1，而且因為安全性風險的緣故而不受支援。僅支援 IKEv2 通訊協定連線。 • 下列加密演算法不被視為安全，因此不受支援：DES 與 3DES。 • 下列雜湊演算法不被視為安全，因此不受支援：SHA1 與 MD5。 • Diffie-Hellman 群組號碼 2 不被視為安全，因此不受支援。
我的本機站台和雲端站台之間的連線維持在 **[正在連線]** 狀態。	檢查： • 是否已開放 UDP 連接埠 500 (當您使用防火牆時)。

問題	可能的解決方案
	• 本機站台和雲端站台之間的連線。 • 本機站台的 IP 位址是否正確。
我的本機站台和雲端站台之間的連線維持在 **[正在等候連線]** 狀態。	當雲端站台的 **[啟動動作]** 設定為 **[新增]** (亦即，雲端站台正在等候本機站台起始連線) 時，您會看到這個狀態。 從本機站台起始連線。
我的本機站台和雲端站台之間的連線維持在 **[正在等候流量]** 狀態。	當雲端站台的 **[啟動動作]** 設定為 **[路由]** 時，您會看到這個狀態。 如果您希望從本機站台起始連線，請執行下列操作： • 嘗試從本機站台 Ping 雲端站台中的虛擬機器。這是為某些裝置建立通道所需的標準行為，例如 Cisco ASA。(路由模式) • 請確認本機站台已透過將本機站台的 **[啟動動作]** 設定為 **[啟動]** 來建立通道。
我的本機站台和雲端站台之間的連線已建立，但是我可以看到其中一或多個網路政策已關閉。	此問題可能是由於下列原因所造成： • 雲端 IPsec 站台的網路對應與本機站台的網路對應不同。 請確認本機站台和雲端站台的網路對應和網路政策順序完全相符。 • 當本機站台和/或雲端站台的 **[啟動動作]** 設定為 **[路由]** (例如，在 Cisco ASA 裝置上)，而且目前沒有流量時，此狀態是正確的。您可以嘗試 Ping 以確認是否已建立通道。如果 Ping 沒有作用，請檢查本機站台和雲端站台的網路對應。
我想要重新啟動特定的 IPsec 連線。	重新啟動特定的 IPsec 連線： 1. 在 **[災難復原]** > **[連線]** 畫面中，按一下 IPsec 連線。 2. 按一下 **[停用連線]**。 3. 再按一下 IPsec 連線。 4. 按一下 **[啟用連線]**。

下載 IPsec VPN 記錄檔

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以在 VPN 伺服器上的記錄檔中，找到 IPsec 連線的其他資訊。記錄檔會壓縮成您可以下載並解壓縮的 .zip 存檔。

必要條件

已設定多站台 IPsec VPN 連線。

下載包含記錄檔的 .zip 存檔

1. 在 Cyber Protect 主控台中，移至 **[災難復原]** > **[連線]**。
2. 按一下雲端站台 VPN 閘道旁的齒輪圖示。
3. 按一下 **[下載記錄檔]**。
4. 按一下**[完成]**。
5. 當 .zip 存檔準備就緒可供下載時，請按一下**下載記錄**，然後將其儲存在本機。

多站台 IPSec VPN 記錄檔

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

下列清單描述 zip 存檔中的 IPsec VPN 記錄檔及其包含的資訊。

- `ip.txt` - 此檔案包含網路介面設定中的記錄。您必須看到兩個 IP 位址：公共 IP 位址和本機 IP 位址。如果您在記錄中看不到這些 IP 位址，則表示有問題。請聯絡支援小組。

  注意事項
  公共 IP 位址的遮罩必須是 32。

- `swanctl-list-loaded-config.txt` - 此檔案包含所有 IPsec 站台的相關資訊。
  如果您在檔案中看不到站台，則表示未套用 IPsec 設定。請嘗試更新設定並加以儲存，或聯絡支援小組。
- `swanctl-list-active-sas.txt` - 此檔案包含處於作用中或正在連線狀態的連線和政策。

點對站台遠端 VPN 存取

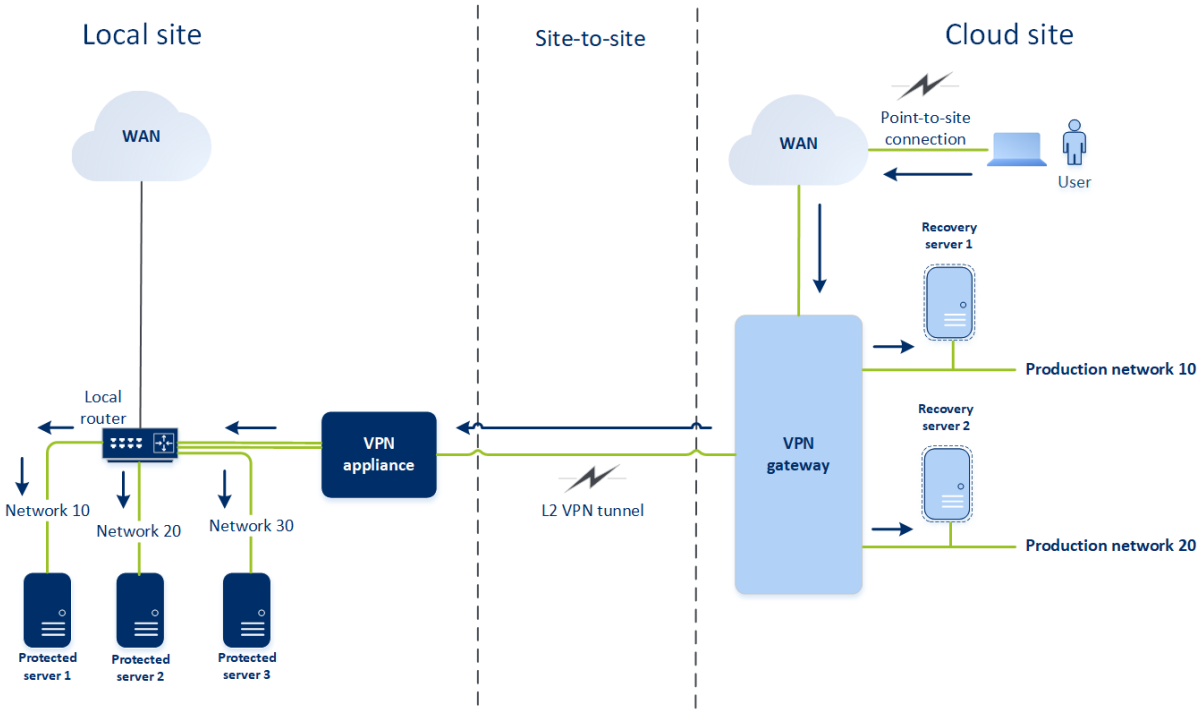
注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

點對站台連線是一種使用端點裝置 (例如電腦或筆記型電腦)，從外部透過 VPN 對雲端站台和本機站台進行的安全連線。在您建立與 Cyber Disaster Recovery Cloud 站台的站台對站台 OpenVPN 連線之後，即可供使用。此類型的連線在下列情況中非常有用：

- 在許多公司中，僅能從公司網路取得公司服務和 Web 資源。您可以使用點對站台連線，安全地連線到本機站台。
- 如果發生災難，當工作負載切換到雲端站台，且您的區域網路斷線時，您可能需要直接存取雲端伺服器。這可以透過雲端站台的點對站台連線完成。

對於本機站台的點對站台連線，您需要在本機站台上安裝 VPN 設備、設定站台對站台連線，然後設定本機站台的點對站台連線。因此，您的遠端員工將透過 L2 VPN 存取公司網路。

以下配置顯示本機站台、雲端站台，以及以綠色醒目提示的伺服器間的通訊。L2 VPN 通道可連線本機站台和雲端站台。當使用者建立點對站台連線時，會透過雲端站台對本機站台執行通訊。



點對站台設定會使用憑證向 VPN 用戶端進行驗證。此外，使用者認證用於驗證。請注意有關本機站台的點對站台連線的下列資訊：

- 使用者應該使用其 Cyber Protect Cloud 認證，在 VPN 用戶端中進行驗證。他們必須具備「公司系統管理員」或「網路保護」使用者角色。
- 如果您重新產生 OpenVPN 設定，則您必須將更新的設定提供給使用點對站連線與雲端站台連線的所有使用者。

設定點對站台遠端 VPN 存取

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

如果您需要從遠端連線到本機站台，可以設定本機站台的點對站台連線。您可以依照下方的程序或觀看影片教學。

必要條件

- 已設定站台到站台 OpenVPN 連線。
- 已在本機站台上安裝 VPN 裝置。

設定本機站台的點對站台連線

1. 在 Cyber Protect 主控台中，移至 **[災難復原]** > **[連線]**。
2. 按一下 **[顯示屬性]**。

3. 啟用 **[本機站台的 VPN 存取]** 選項。
4. 確認需要建立本機站台的點對站台連線的使用者：
   - 在 Cyber Protect Cloud 中擁有使用者帳戶。這些認證在 VPN 用戶端中用於驗證。否則，請在 Cyber Protect Cloud 中建立使用者帳戶。
   - 具備「公司系統管理員」或「網路保護」使用者角色。
5. 設定 OpenVPN 用戶端：
   a. 從下列位置下載 OpenVPN 用戶端 2.4.0 版或更新版本：https://openvpn.net/community-downloads/。

      注意事項
      不支援 OpenVPN Connect 用戶端。

   b. 將 OpenVPN 用戶端安裝在您要連線到本機站台的來源電腦上。
   c. 按一下 **[下載 OpenVPN 的設定]**。設定檔適用於貴組織中擁有「公司系統管理員」或「網路保護」使用者角色的使用者。
   d. 將已下載的設定匯入 OpenVPN 用戶端。
   e. 使用 Cyber Protect Cloud 使用者認證，登入 OpenVPN 用戶端 (請參閱上述的步驟 4)。
   f. [選用] 如果針對貴組織啟用雙重驗證機制，則您應該提供產生的一次性 TOTP 代碼。

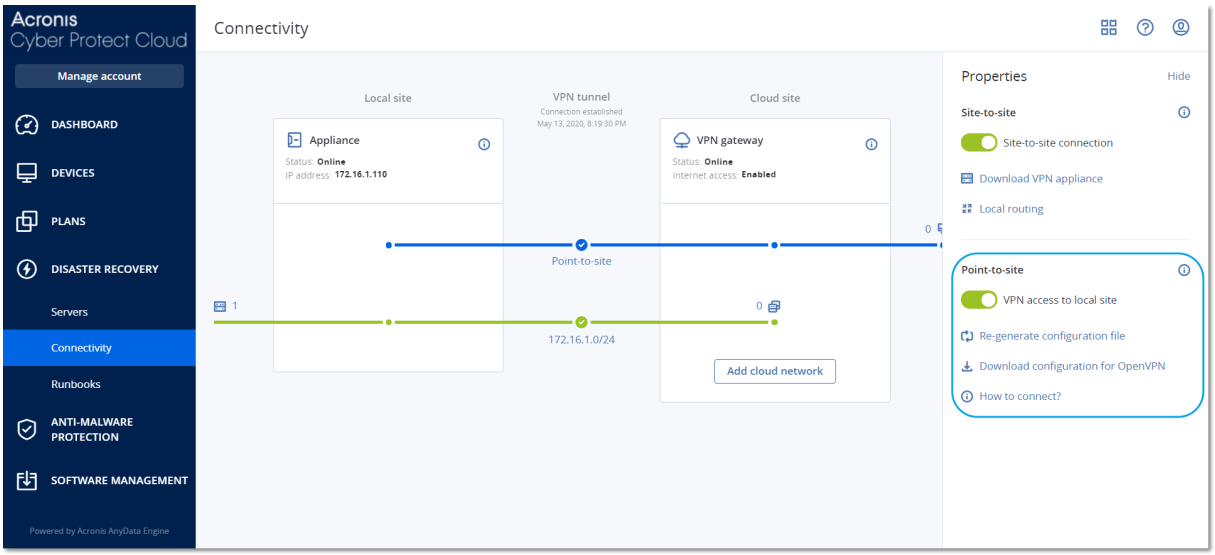
重要事項
如果為您的帳戶啟用雙重驗證機制，您需要重新產生設定檔，並為您現有的 OpenVPN 用戶端更新設定檔。使用者必須重新登入 Cyber Protect Cloud，才能為其帳戶設定雙重驗證機制。

因此，您將可以連線到本機站台上的電腦。

管理點對站台連線設定

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

在 Cyber Protect 主控台中，移至 **[災難復原]** > **[連線]**，然後按一下右上角的 **[顯示屬性]**。



本機站台的 VPN 存取

此選項用於管理對本機站台的 VPN 存取。預設為啟用狀態。如果遭到停用，將不允許對本機站台的點對站台存取。

下載 OpenVPN 的設定

這會下載 OpenVPN 用戶端的設定檔。若要建立與雲端站台的點對站台連線，需要這個檔案。

重新產生設定

您可以重新產生 OpenVPN 用戶端的設定檔。

在下列情況下，這是必要的：

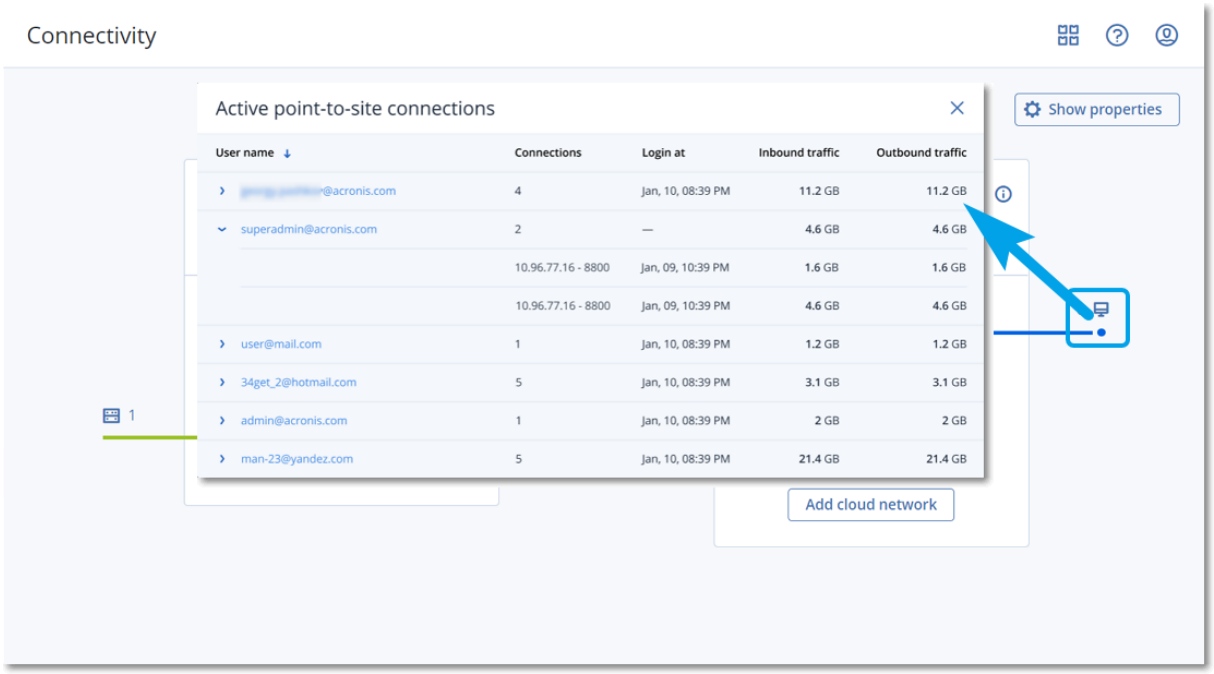
- 如果您懷疑設定檔已損壞。
- 如果您的帳戶已啟用雙重驗證機制。

當設定檔更新之後，將無法透過舊的設定檔連線。確認將新檔案散發給獲允許使用點對站台連線的使用者。

作用中的點對站台連線

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以在 **[災難復原]** > **[連線]** 中檢視所有作用中的點對站台連線。按一下**點對站台**藍線上的電腦圖示，您將會看到依使用者名稱分組的作用中點對站台連線的詳細資訊。



對於 Active Directory 網域服務可用性的建議

如果受保護的工作負載需要在網域控制站中進行驗證，建議您在災難復原站台擁有 Active Directory 網域控制站 (AD DC) 執行個體。

適用於 L2 OpenVPN 連線的 Active Directory 網域控制站

使用 L2 OpenVPN 連線時，受保護工作負載的 IP 位址在測試容錯移轉或實際執行容錯移轉期間，會保留在雲端站台中。因此，測試容錯移轉或實際執行容錯移轉期間的 AD DC 與本機站台的 AD DC 具有相同的 IP 位址。

您可以透過自訂 DNS，為所有雲端伺服器設定您自己的自訂 DNS 伺服器。如需詳細資訊，請參閱 "設定自訂 DNS 伺服器" (第 689 頁)。

適用於 L3 IPsec VPN 連線的 Active Directory 網域控制站

使用 L3 IPsec VPN 連線時，受保護工作負載的 IP 位址不會保留在雲端站台中。因此，建議您在執行實際執行容錯移轉之前，先具備其他專用的 AD DC 執行個體，作為雲端站台中的主要伺服器。

對於設定為雲端站台中主要伺服器的專用 AD DC 執行個體，其建議如下：

- 關閉 Windows 防火牆。
- 將主要伺服器加入至 Active Directory 服務。
- 確認主要伺服器可存取網際網路。
- 新增 Active Directory 功能。

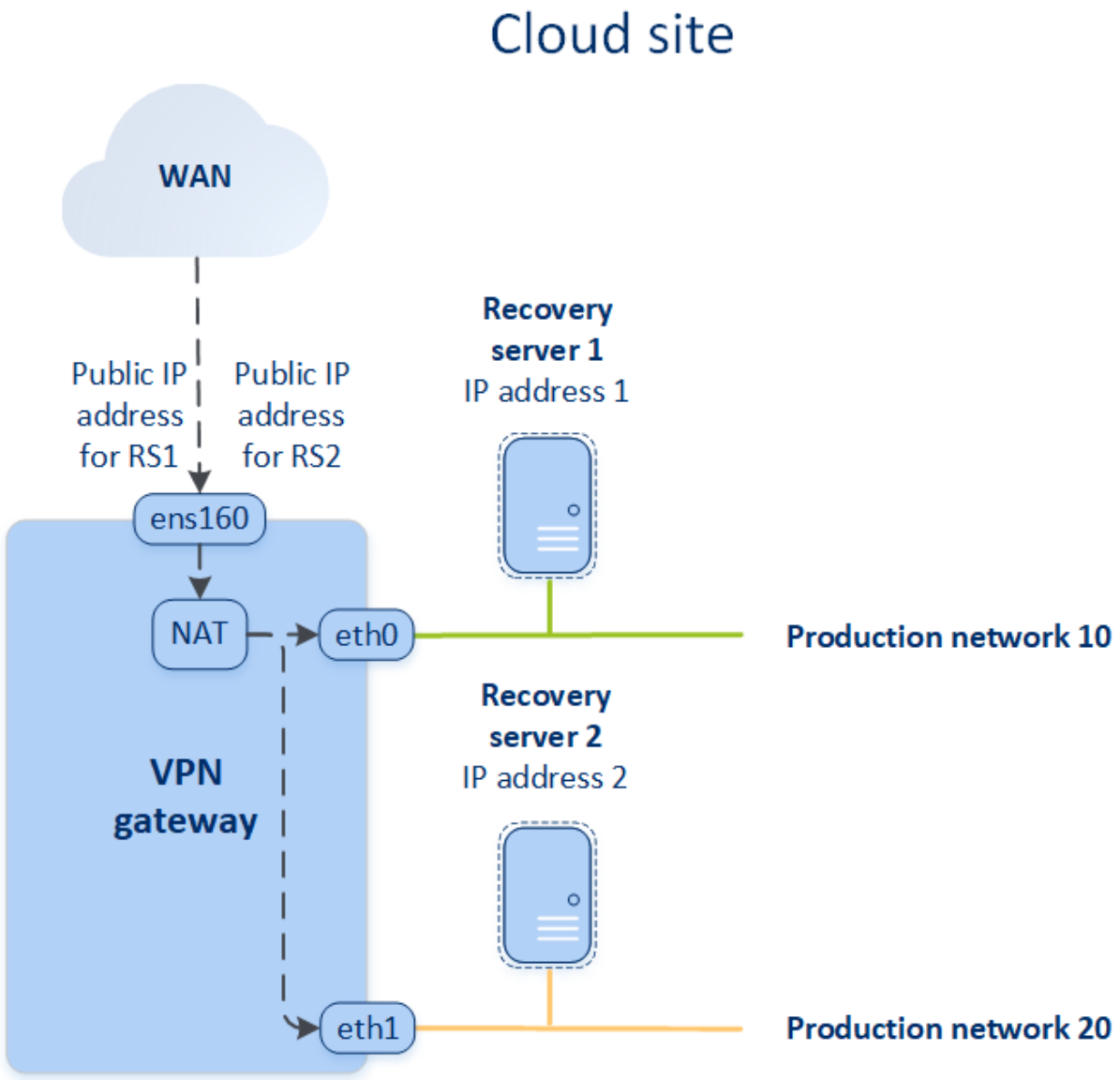
您可以透過自訂 DNS，為所有雲端伺服器設定您自己的自訂 DNS 伺服器。如需詳細資訊，請參閱 "設定自訂 DNS 伺服器" (第 689 頁)。

網路管理

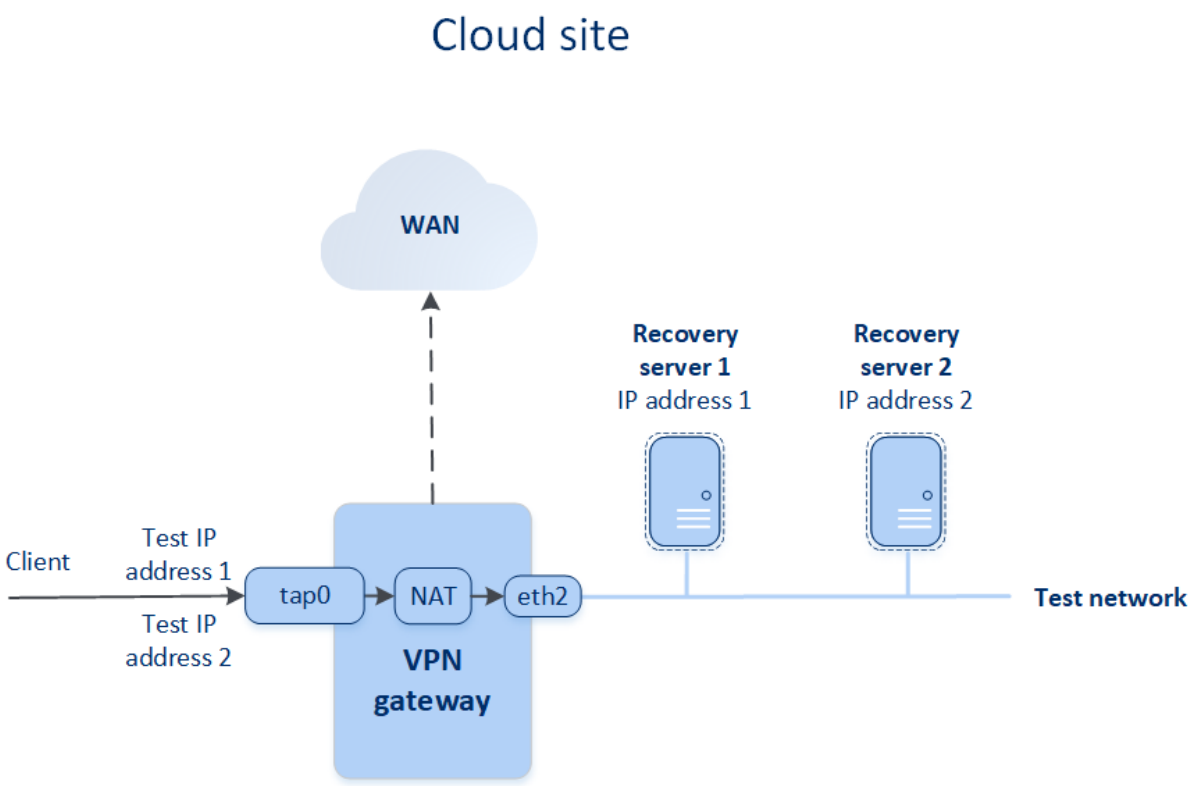
本節描述網路管理案例。

公用和測試 IP 位址

如果您在建立復原伺服器時指派公共 IP 位址，則復原伺服器會變成可以透過此 IP 位址，從網際網路使用。當具有目的地公共 IP 位址的封包來自網際網路時，VPN 閘道會使用 NAT，將其重新對應到個別的實際執行 IP 位址，然後將其傳送至對應的復原伺服器。



如果您在建立復原伺服器時指派測試 IP 位址，則復原伺服器會變成可以透過此 IP 位址，在測試網路中使用。如果您執行測試容錯移轉，當具有相同 IP 位址的復原伺服器在雲端的測試網路中啟動的同時，原始電腦仍在執行中。IP 位址不會發生衝突，因為測試網路遭到隔離。測試網路中的復原伺服器可透過其測試 IP 位址聯繫，這些 IP 位址會透過 NAT，重新對應到實際執行 IP 位址。



如需有關站台對站台 OpenVPN 的詳細資訊，請參閱 "站台對站台 OpenVPN - 其他資訊" (第 986 頁)。

IP 位址重新設定

為獲得適當的災難復原效能，指派給本機伺服器和雲端伺服器的 IP 位址必須一致。如果 IP 位址有任何不一致或不相符，您將會在 **[災難復原]** > **[連線]** 中對應網路的旁邊看到一個驚嘆號。

IP 位址不一致的部分常見原因列在下方：

1. 復原伺服器是從一個網路移轉到另一個網路，或者雲端網路的網路遮罩遭到變更。因此，雲端伺服器的 IP 位址來自未連線的網路。
2. 連線類型從沒有站台對站台連線切換到站台對站台連線。因此，本機伺服器置於不同於針對雲端站台上的復原伺服器而建立的網路。
3. 連線類型從站台對站台 OpenVPN 切換到多站台 IPsec VPN，或從多站台 IPsec VPN 切換到站台對站台 OpenVPN。如需有關此案例的詳細資訊，請參閱切換連線、"從多站台 IPsec VPN 切換至站台對站台 OpenVPN" (第 678 頁)和重新指派 IP 位址。
4. 在 VPN 設備站台上編輯下列網路參數：
   - 透過網路設定新增介面
   - 透過介面設定手動編輯網路遮罩
   - 透過 DHCP 編輯網路遮罩
   - 透過介面設定手動編輯網位址和路遮罩
   - 透過 DHCP 編輯網路遮罩和位址

上列動作的結果是，雲端站台上的網路可能會變成區域網路的子集或超集，或者 VPN 設備介面可能會針對不同的介面回報相同的網路設定。

若要解決網路設定的問題

1. 按一下需要 IP 位址重新設定的網路。
   您將會看到所選網路中伺服器、其狀態以及 IP 位址的清單。其網路設定不一致的伺服器會以驚嘆號標示。
2. 若要變更伺服器的網路設定，按一下 **[前往伺服器]**。若要一次變更所有伺服器的網路設定，按一下通知區塊中的 **[變更]**。
3. 如有需要，請在 **[新 IP]** 和 **[新的測試 IP]** 欄位中進行變更，以變更 IP 位址。
4. 準備就緒後，按一下 **[確認]**。

將伺服器移至合適的網路

當您建立災難復原保護計劃，並將其套用到所選裝置時，系統會檢查裝置 IP 位址，如果沒有 IP 位址適用的現有雲端網路，就會自動建立雲端網路。預設會使用 IANA 建議的最大範圍，設定私人用途的雲端網路 (10.0.0.0/8、172.16.0.0/12、192.168.0.0/16)。您可以透過編輯網路遮罩來縮小網路的範圍。

如果選取的裝置位於多個區域網路上，則雲端站台上的網路可能會變成區域網路的超集。在此情況下，若要重新設定雲端網路：

1. 按一下需要重新設定網路大小的雲端網路，然後按一下 **[編輯]**。
2. 使用正確的設定，重新設定網路大小。
3. 建立其他所需的網路。
4. 按一下連線到網路的裝置數量旁邊的通知圖示。
5. 按一下 **[移至合適的網路]**。
6. 選擇您想要移至合適網路的伺服器，然後按一下 **[移動]**。

重新指派 IP 位址

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

在下列情況下，您必須重新指派雲端網路和雲端伺服器的 IP 位址以完成設定：

- 從站台對站台 OpenVPN 切換到多站台 IPsec VPN，或從多站台 IPsec VPN 切換到站台對站台 OpenVPN 之後。
- 套用保護計劃之後 (如果已設定多站台 IPsec VPN 連線)。

雲端網路

重新指派雲端網路的 IP 位址

1. 在 **[連線]** 索引標籤中，按一下雲端網路的 IP 位址。
2. 在 **[網路]** 快顯視窗中，按一下 **[編輯]**。

3. 輸入新的網路位址和網路遮罩。
4. 按一下**[完成]**。

重新指派雲端網路的 IP 位址之後，您必須重新指派屬於重新指派之雲端網路的雲端伺服器。

雲端伺服器

重新指派伺服器的 IP 位址

1. 在 **[連線]** 索引標籤中，按一下伺服器在雲端網路中的 IP 位址。
2. 在 **[伺服器]** 快顯視窗中，按一下 **[變更 IP 位址]**。
3. 在 **[變更 IP 位址]** 快顯視窗中，輸入伺服器的新 IP 位址，或使用自動產生的 IP 位址 (重新指派的雲端網路一部分)。

   注意事項
   Cyber Disaster Recovery Cloud 會將雲端網路中的 IP 位址自動指派給雲端網路所屬的所有雲端伺服器，然後再重新指派網路 IP 位址。您可以使用建議的 IP 位址，一次重新指派所有雲端伺服器的 IP 位址。

4. 按一下 **[確認]**。

重新安裝 VPN 閘道

如果有您無法解決的 VPN 閘道問題，您可能需要重新安裝 VPN 閘道。可能的問題包括：

- VPN 閘道處於 **[錯誤]** 狀態。
- VPN 閘道長時間處於 **[等候中]** 狀態。
- VPN 閘道狀態長時間未確定。

重新安裝 VPN 閘道程序包括下列自動動作：完全刪除現有的 VPN 閘道虛擬機器、從範本安裝新的虛擬機器，然後在新的虛擬機器上套用先前 VPN 閘道的設定。

必要條件：

必須設定雲端站台的其中一個連線類型。

若要重新安裝 VPN 閘道

1. 在 Cyber Protect 主控台中，移至 **[災難復原]** > **[連線]**。
2. 按一下 VPN 閘道的齒輪圖示，然後選擇 **[重新安裝 VPN 閘道]**。
3. 在 **[重新安裝 VPN 閘道]** 對話方塊中，輸入您的登入資料。
4. 按一下 **[重新安裝]**。

設定自訂 DNS 伺服器

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

當您設定連線時，Cyber Disaster Recovery Cloud 會建立雲端網路基礎架構。雲端 DHCP 伺服器會將預設 DNS 伺服器自動指派給復原伺服器和主要伺服器，但是您可以變更預設設定，並設定自訂 DNS 伺服器。新的 DNS 設定將在下次對 DHCP 伺服器提出要求時套用。

必要條件

必須設定雲端站台的其中一個連線類型。

設定自訂 DNS 伺服器

1. 在 Cyber Protect 主控台中，移至 **[災難復原]** > **[連線]**。
2. 按一下 **[顯示屬性]**。
3. 按一下 **[預設 (雲端站台所提供)]**。
4. 選擇 **[自訂伺服器]**。
5. 輸入 DNS 伺服器的 IP 位址。
6. [選用] 如果您想要新增其他 DNS 伺服器，按一下 **[新增]**，然後輸入 DNS 伺服器 IP 位址。

   注意事項
   新增自訂 DNS 伺服器之後，您也可以新增預設 DNS 伺服器。如此一來，如果自訂 DNS 伺服器無法使用，Cyber Disaster Recovery Cloud 將使用預設 DNS 伺服器。

7. 按一下**[完成]**。

刪除自訂 DNS 伺服器

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以從自訂 DNS 清單刪除 DNS 伺服器。

必要條件：

已設定自訂 DNS 伺服器。

刪除自訂 DNS 伺服器

1. 在 Cyber Protect 主控台中，移至 **[災難復原]** > **[連線]**。
2. 按一下 **[顯示屬性]**。
3. 按一下 **[自訂伺服器]**。
4. 按一下 DNS 伺服器旁的刪除圖示。

注意事項
只有一個自訂 DNS 伺服器可用時，才會停用刪除作業。如果您要刪除所有自訂 DNS 伺服器，選擇 **[預設 (雲端站台所提供)]**。

5. 按一下**[完成]**。

設定本機路由

除了透過 VPN 設備延伸到雲端的區域網路之外，您可以擁有未在 VPN 設備中登錄，但其中的伺服器必須與雲端伺服器通訊的其他區域網路。若要建立這類本機伺服器和雲端伺服器間的連線，您需要設定本機路由設定。

若要設定本機路由

1. 移至 **[災難復原]** > **[連線]**。
2. 按一下 **[顯示屬性]**，然後按一下 **[本機路由]**。
3. 以 CIDR 標記法指定區域網路。
4. 按一下 **[儲存]**。

因此，來自指定之區域網路的伺服器可以與雲端伺服器通訊。

下載 MAC 位址

您可以下載 MAC 位址清單，然後加以解壓縮並匯入您自訂 DHCP 伺服器的組態中。

必要條件：

- 必須設定雲端站台的其中一個連線類型。
- 至少必須設定一個具有 MAC 位址的主要或復原伺服器。

若要下載 MAC 位址清單

1. 在 Cyber Protect 主控台中，移至 **[災難復原]** > **[連線]**。
2. 按一下 **[顯示屬性]**。
3. 按一下 **[下載 MAC 位址清單]**，然後儲存 CSV 檔案。

使用記錄

災難復原會收集 VPN 設備和 VPN 閘道的記錄。這些記錄會以.txt 檔案形式儲存，這些檔案會壓縮在 .zip 存檔中。您可以下載並解壓縮存檔，然後使用該資訊進行疑難排解或監視。

下列清單描述 .zip 存檔中的記錄檔及其包含的資訊。

`dnsmasq.config.txt` - 該檔案包含有關提供 DNS 及 DHCP 位址之服務設定的資訊。

`dnsmasq.leases.txt` - 該檔案包含有關目前 DHCP 位址租用的資訊。

`dnsmasq_log.txt` - 該檔案包含 dnsmasq 服務的記錄。

`ebtables.txt` - 該檔案包含有關防火牆資料表的資訊。

`free.txt` - 該檔案包含有關可用記憶體的資訊。

`ip.txt` - 該檔案包含網路介面設定的記錄，包括可在進行**擷取網路封包**設定時使用的名稱。

`NetworkManager_log.txt` - 該檔案包含 NetworkManager 服務的記錄。

`NetworkManager_status.txt` - 該檔案包含有關 NetworkManager 服務狀態的資訊。

`openvpn@p2s_log.txt` - 該檔案包含 OpenVPN 服務的記錄。

`openvpn@p2s_status.txt` - 該檔案包含有關 VPN 通道狀態的資訊。

`ps.txt` - 該檔案包含有關目前在 VPN 閘道或 VPN 設備上執行的處理程序的資訊。

`resolf.conf.txt` - 該檔案包含有關 DNS 伺服器設定的資訊。

`routes.txt` - 該檔案包含有關網路路由的資訊。

`uname.txt` - 該檔案包含有關作業系統核心之目前版本的資訊。

`uptime.txt` - 該檔案包含有關尚未重新啟動作業系統之期間長度的資訊。

`vpnserver_log.txt` - 該檔案包含 VPN 服務的記錄。

`vpnserver_status.txt` - 該檔案包含有關 VPN 伺服器狀態的資訊。

如需有關 IPsec VPN 連線之特定記錄檔的詳細資訊，請參閱 "多站台 IPSec VPN 記錄檔" (第 681 頁)。

下載 VPN 設備的記錄

您可以下載並解壓縮包含 VPN 設備記錄的存檔，然後使用該資訊進行疑難排解或監視。

若要下載 VPN 設備的記錄，請執行下列動作

1. 在**連線**頁面上，按一下 VPN 設備旁的齒輪圖示。
2. 按一下**下載記錄**。
3. [選用] 選擇**擷取網路封包**，然後進行設定。如需詳細資訊，請參閱 "擷取網路封包" (第 693 頁)。
4. 按一下**[完成]**。
5. 當 .zip 存檔準備就緒可供下載時，請按一下**下載記錄**，然後將其儲存在本機。

下載 VPN 閘道的記錄

您可以下載並解壓縮包含 VPN 閘道記錄的存檔，並使用該資訊進行疑難排解或監視。

若要下載 VPN 閘道的記錄，請執行下列動作

1. 在**連線**頁面上，按一下 VPN 閘道旁的齒輪圖示。
2. 按一下**下載記錄**。
3. [選用] 選擇**擷取網路封包**，然後進行設定。如需詳細資訊，請參閱 "擷取網路封包" (第 693 頁)。
4. 按一下**[完成]**。
5. 當 .zip 存檔準備就緒可供下載時，請按一下**下載記錄**，然後將其儲存在本機。

擷取網路封包

若要對本機生產站台與主要或復原伺服器之間的通訊進行疑難排解及分析，您可以選擇以收集 VPN 閘道或 VPN 設備上的網路封包。

收集 32,000 個網路封包或達到時間限制後，網路封包擷取即會停止，而結果會寫入 .libpcap 檔案，且該檔案會新增至記錄的 .zip 存檔。

下表提供有關您可以設定之**擷取網路封包**設定的詳細資訊。

設定	描述
網路介面名稱	擷取網路封包所在的網路介面。如果要擷取所有網路介面上的網路封包，請選擇**任何**。
時間限制 (秒)	擷取網路封包的時間限制。您可以設定的最大值為 1800。
篩選	要在擷取的網路封包上套用的額外篩選條件。 您可以輸入包含通訊協定、連接埠、方向及其組合的字串，並以空格分隔，例如："and"、"or"、"not"、" ("、") "、"src"、"dst"、"net"、"host"、"port"、"ip", "tcp"、"udp"、"icmp"、"arp"、"esp”。 如果要使用括弧，請在前後加上空格。您也可以輸入 IP 位址及網路位址，例如："icmp or arp" 及 "port 67 or 68"。 如需有關您可以輸入的值的詳細資訊，請參閱 Linux tcpdump 說明。

雲端伺服器

您可以透過災難復原，使用兩種類型的雲端伺服器：主要和復原。

主要伺服器是未與本機站台上的電腦連結的虛擬機器。您可以使用主要伺服器來保護特定應用程式或執行各種輔助服務 (例如網頁伺服器)。

復原伺服器是原始電腦 (受保護伺服器) 複本的虛擬機器。復原伺服器是以儲存在雲端的受保護伺服器備份為基礎。發生災難時，復原伺服器用於從原始伺服器切換工作負載。

設定復原伺服器

復原伺服器：原始電腦的一個複本，以儲存在雲端的受保護伺服器備份為基礎。復原伺服器在發生災難時，用於從原始伺服器切換工作負載。

建立復原伺服器時，您必須指定下列網路參數：

參數	描述
雲端網路	(必填) 將與復原伺服器連線的雲端網路。
實際執行網路中的 IP 位址	(必填) 將啟動復原伺服器之虛擬機器所使用的 IP 位址。此位址同時用於實際執行網路和測試網路。啟動前，系統會設定虛擬機器以透過 DHCP 取得 IP 位址。
測試 IP 位址	(選填) 在測試容錯移轉期間，從用戶端實際執行網路存取復原伺服器所使用的 IP 位址，以防實際執行 IP 位址在相同網路中重複。此 IP 位址不同於實際執行網路中的 IP 位址。本機站台中的伺服器可以在測試容錯移轉期間，透過測試 IP 位址聯繫復原伺服器，但是無法反向進行存取。如果在復原伺服器建立期間選取 **[網際網路存取]** 選項，則可以在測試網路中從復原伺服器進行網際網路存取。
公用 IP 位址	(選填) 從網際網路存取復原伺服器所使用的 IP 位址。如果伺服器沒有公用 IP 位址，則僅能從區域網路聯繫該伺服器。
網際網路存取	(選填) 可讓復原伺服器存取網際網路 (在實際執行和測試容錯移轉的情況下)。

建立復原伺服器

若要建立將成為工作負載副本的復原伺服器，請遵循以下程序進行。您還可以觀看演示過程的 影片教學。

重要事項
當您執行容錯移轉時，您僅能選取建立復原伺服器之後所建立的復原點。

必要條件

- 保護計劃必須套用到您要保護的原始電腦。此計劃必須在雲端儲存空間備份整部電腦，或僅備份開機及提供必要服務所需的磁碟。
- 必須設定雲端站台的其中一個連線類型。

建立復原伺服器

1. 在 **[所有裝置]** 索引標籤上，選取您要保護的電腦。
2. 按一下 **[災難復原]**，然後按一下 **[建立復原伺服器]**。
3. 選取虛擬核心數量和 RAM 大小。

   注意事項
   您可以查看每個選項的計算點。計算點的數量會反應復原伺服器每小時的執行成本。如需詳細資訊，請參閱 "計算點" (第 706 頁)。

4. 指定將與伺服器連線的雲端網路。
5. 選擇 **[DHCP]** 選項。

DHCP 選項	描述
雲端站台所提供	預設設定。伺服器的 IP 位址將由雲端中自動設定的 DHCP 伺服器提供。
自訂	伺服器的 IP 位址將由雲端中您自己的 DHCP 伺服器提供。

6. [選用] 指定 **[MAC 位址]**。

   MAC 位址是指派給伺服器網路介面卡的唯一識別碼。如果使用自訂 DHCP，您可以將其設定為一律指派特定的 IP 位址給特定的 MAC 位址。如此一來，您將確保復原伺服器一律取得相同的 IP 位址。您可以執行具有以 MAC 位址註冊之授權的應用程式。
7. 指定伺服器將在實際執行網路中具備的 IP 位址。依預設，會設定原始電腦的 IP 位址。

   注意事項

   如果您使用 DHCP 伺服器，請將此 IP 位址新增至伺服器排除清單，以避免 IP 位址發生衝突。

   如果使用自訂 DHCP 伺服器，您必須在 **[實際執行網路中的 IP 位址]** 中指定與 DHCP 伺服器中設定的 IP 位址相同的 IP 位址。否則，測試容錯移轉將無法正常運作，而且無法透過公用 IP 位址存取伺服器。
8. [選用] 選取 **[測試 IP 位址]** 核取方塊，然後指定 IP 位址。

   這可讓您有能力在隔離的測試網路中測試容錯移轉，並在測試容錯移轉期間，透過 RDP 或 SSH 連線到復原伺服器。在測試容錯移轉模式中，VPN 閘道將會使用 NAT 通訊協定，將測試 IP 位址取代為實際執行 IP 位址。

   如果您未選取該核取方塊，則在測試容錯移轉期間只能使用主控台存取伺服器。

   注意事項

   如果您使用 DHCP 伺服器，請將此 IP 位址新增至伺服器排除清單，以避免 IP 位址發生衝突。

   您可以選擇建議的 IP 位址其中之一或輸入不同的位址。
9. [選用] 選取 **[網際網路存取]** 核取方塊。

   這將可讓復原伺服器在實際或測試容錯移轉期間存取網際網路。預設開放 TCP 連接埠 25，以供與公用 IP 位址的輸出連線使用。
10. [選用] 設定 **[RPO 閾值]**。

    RPO 閾值會定義上次適合容錯移轉的復原點和目前時間之間允許的最大時間間隔。此值可以設定在 15 – 60 分鐘、1 – 24 小時、1 – 14 天內。
11. [選用] 選取 **[使用公共 IP 位址]** 核取方塊。

    具有公共 IP 位址可在容錯移轉或測試容錯移轉期間，讓復原伺服器從網際網路使用。如果您未選取該核取方塊，則只能在您的實際執行網路中使用該伺服器。

    [使用公用 IP 位址] 選項需要啟用 **[網際網路存取]** 選項。

    公共 IP 位址將在您完成設定之後顯示。預設開放 TCP 連接埠 443，以供與公用 IP 位址的輸入連線使用。

    注意事項

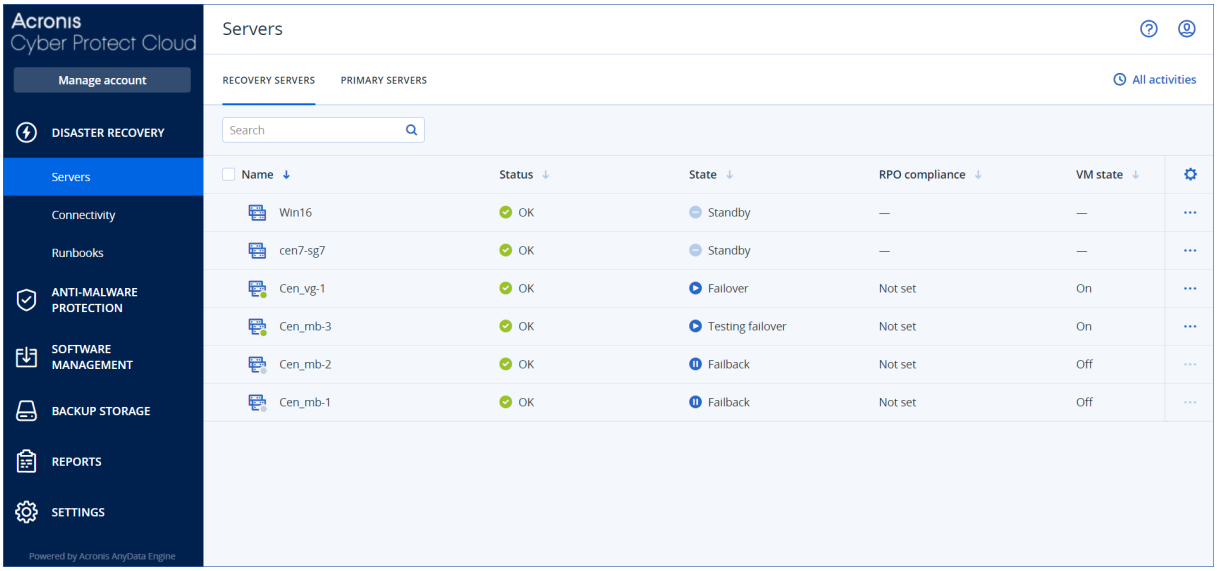
    如果您清除 **[使用公用 IP 位址]** 核取方塊，或刪除復原伺服器，將不會保留其公用 IP 位址。

12. [選擇性] [如果所選電腦的備份是使用加密作為電腦屬性來加密的], 請指定從加密備份建立用於復原伺服器的虛擬機器時將會自動使用的密碼。
    a. 按一下 **[指定]**, 然後輸入加密備份的密碼, 並定義認證的名稱。
       根據預設, 您將會在清單中看到最新的備份。
    b. [選用] 若要檢視所有備份, 選取 **[顯示所有備份]**。
    c. 按一下**[完成]**。

    注意事項
    雖然您指定的密碼將會儲存在安全的認證存放區中, 但儲存密碼可能會違反您的合規義務。

13. [選用] 變更復原伺服器名稱。
14. [選用] 輸入復原伺服器的描述。
15. [選用] 按一下 **[雲端防火牆規則]** 索引標籤以編輯預設防火牆規則。如需詳細資訊, 請參閱 "設定雲端伺服器的防火牆規則" (第 703 頁)。
16. 按一下 **[建立]**。

復原伺服器將會出現在 Cyber Protect 主控台的 **[災難復原]** > **[伺服器]** > **[復原伺服器]** 索引標籤中。您可以選取原始機器並按一下 **[災難復原]** 來檢視其設定。



次要伺服器的操作

在 Cyber Protect 主控台中, 主要伺服器會顯示在 **[災難復原]** > **[伺服器]** > **[復原伺服器]** 索引標籤上。

開啟電源

若要開啟復原伺服器電源

1. 在 **[復原伺服器]** 索引標籤上, 按一下復原伺服器。
2. 按一下 **[開啟電源]**。

關閉電源

若要關閉復原伺服器電源

1. 在 **[復原伺服器]** 索引標籤上，按一下復原伺服器。
2. 按一下 **[關閉電源]**。
3. 在 **[關閉伺服器電源]** 畫面中，按一下 **[關閉電源]**。

強制關閉電源

若要強制關閉復原伺服器電源

1. 在 **[復原伺服器]** 索引標籤上，按一下復原伺服器。
2. 按一下 **[關閉電源]**。
3. 在 **[關閉伺服器電源]** 畫面中，選擇 **[強制關閉伺服器]**，然後按一下 **[關閉電源]**。

停止

若要停止復原伺服器

1. 在 **[復原伺服器]** 索引標籤上，按一下復原伺服器。
2. 按一下 **[停止]**。

編輯設定

若要編輯復原伺服器的設定

1. 在 **[復原伺服器]** 索引標籤上，按一下復原伺服器。
2. 按一下 **[停止]**。
3. 按一下 **[編輯]**，然後編輯設定。

套用保護計劃

若要將計劃套用到主要伺服器

1. 在 **[主要伺服器]** 索引標籤上，按一下主要伺服器。
2. 在 **[計劃]** 索引標籤上，按一下 **[建立]**。
   您將會看到預先定義的保護計劃，您只能在其中變更排程和保留規則。如需詳細資訊，請參閱「備份雲端伺服器」。

使用加密備份

您可以從加密備份建立復原伺服器。您可以在容錯移轉至復原伺服器期間，對加密備份設定自動套用密碼，以供您方便之用。

建立復原伺服器時，您可以指定要用於自動災難復原作業的密碼。此密碼將會儲存到認證儲存區，這是一個安全的認證儲存區，可以在 **[設定]** > **[認證]** 區段中找到。

一個認證可以連結到數個備份。

若要在認證儲存區中管理已儲存的密碼

1. 移至 **[設定]** > **[認證]**。
2. 若要管理特定的認證，請按一下最後一欄‘中的圖示。您可以檢視連結至此認證的項目。

- 若要從所選認證取消連結備份，請按一下備份附近的 [資源回收筒] 圖示。因此，您必須在容錯移轉至復原伺服器期間，手動指定密碼。
- 若要編輯認證，按一下 **[編輯]**，然後指定名稱或密碼。
- 若要刪除認證，按一下 **[刪除]**。請注意，您必須在容錯移轉至復原伺服器期間，手動指定密碼。

設定主要伺服器

主要伺服器是一部虛擬機器，相較於復原伺服器，在本機站台上沒有連結的機器。主要伺服器用於透過複寫保護應用程式，或用於執行各種輔助服務 (例如，網頁伺服器)。

一般而言，主要伺服器用於執行重要應用程式之伺服器之間的即時資料複寫。您應使用應用程式的原生工具，自行設定複寫。例如：可以在本機伺服器和主要伺服器之間設定 Active Directory 複寫或 SQL 複寫。

或者，主要伺服器可以包含在 AlwaysOn 可用性群組 (AAG) 或資料庫可用性群組 (DAG) 中。

這兩種方法都需要深入瞭解應用程式和系統管理員權限。主要伺服器會持續消耗快速災難復原儲存空間上的計算資源與空間。它需要您那一端的維護：監控複寫、安裝軟體更新以及備份。其優點是最小的 RPO 和 RTO，以及實際執行環境的最小負載 (相較於將整個伺服器備份到雲端而言)。

主要伺服器一律僅在實際執行網路中啟動，而且有下列網路參數：

參數	描述
雲端網路	(必填) 將與主要伺服器連線的雲端網路。
實際執行網路中的 IP 位址	(必填) 主要伺服器將在實際執行網路中具備的 IP 位址。根據預設，會設定您實際執行網路中的第一個可用 IP 位址。
公用 IP 位址	(選填) 從網際網路存取主要伺服器所使用的 IP 位址。如果伺服器沒有公用 IP 位址，則僅能從區域網路 (而無法透過網際網路) 聯繫該伺服器。
網際網路存取	(選填) 可讓主要伺服器存取網際網路。

建立主要伺服器

必要條件

- 必須設定雲端站台的其中一個連線類型。

建立主要伺服器

1. 移至 **[災難復原]** > **[伺服器]** > **[主要伺服器]** 索引標籤 。
2. 按一下 **[建立]**。
3. 為新的虛擬機器選取範本。
4. 選擇設定類別 (虛擬核心數目以及 RAM 大小)。下表顯示每個類別的磁碟空間總數上限 (GB)。

類型	vCPU	RAM (GB)	磁碟空間總數上限 (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

注意事項

您可以查看每個選項的計算點。計算點的數量會反應主要伺服器每小時的執行成本。如需詳細資訊，請參閱 "計算點" (第 706 頁)。

5. [選用] 變更虛擬磁碟大小。如果您需要一個以上的硬碟，請按一下 **[新增磁碟]**，然後指定新的磁碟大小。目前您可以針對主要伺服器新增不超過 10 個磁碟。
6. 指定主要伺服器將包含在內的雲端網路。
7. 選擇 **[DHCP]** 選項。

DHCP 選項	描述
雲端站台所提供	預設設定。伺服器的 IP 地址將由雲端中自動設定的 DHCP 伺服器提供。
自訂	伺服器的 IP 地址將由雲端中您自己的 DHCP 伺服器提供。

8. [選用] 指定 **[MAC 位址]**。

   MAC 位址是指派給伺服器網路介面卡的唯一識別碼。如果使用自訂 DHCP，您可將它設定為一律指派特定的 IP 位址給特定的 MAC 位址。如此可確保主要伺服器一定會獲得相同的 IP 位址。您可以執行具有以 MAC 位址註冊之授權的應用程式。
9. 指定伺服器將在實際執行網路中具備的 IP 位址。根據預設，會設定您實際執行網路中的第一個可用 IP 位址。

注意事項

如果您使用 DHCP 伺服器，請將此 IP 位址新增至伺服器排除清單，以避免 IP 位址發生衝突。

如果使用自訂 DHCP 伺服器，您必須在 **[實際執行網路中的 IP 位址]** 中指定與 DHCP 伺服器中設定的 IP 位址相同的 IP 位址。否則，測試容錯移轉將無法正常運作，而且無法透過公用 IP 位址存取伺服器。

10. [選用] 選取 **[網際網路存取]** 核取方塊。

    這將可讓主要伺服器存取網際網路。預設開放 TCP 連接埠 25，以供與公用 IP 位址的輸出連線使用。

11. [選用] 選取 **[使用公共 IP 位址]** 核取方塊。

    具有公共 IP 位址可讓主要伺服器從網際網路使用。如果您未選取該核取方塊，則只能在您的實際執行網路中使用該伺服器。

    公共 IP 位址將在您完成設定之後顯示。預設開放 TCP 連接埠 443，以供與公用 IP 位址的輸入連線使用。

    注意事項

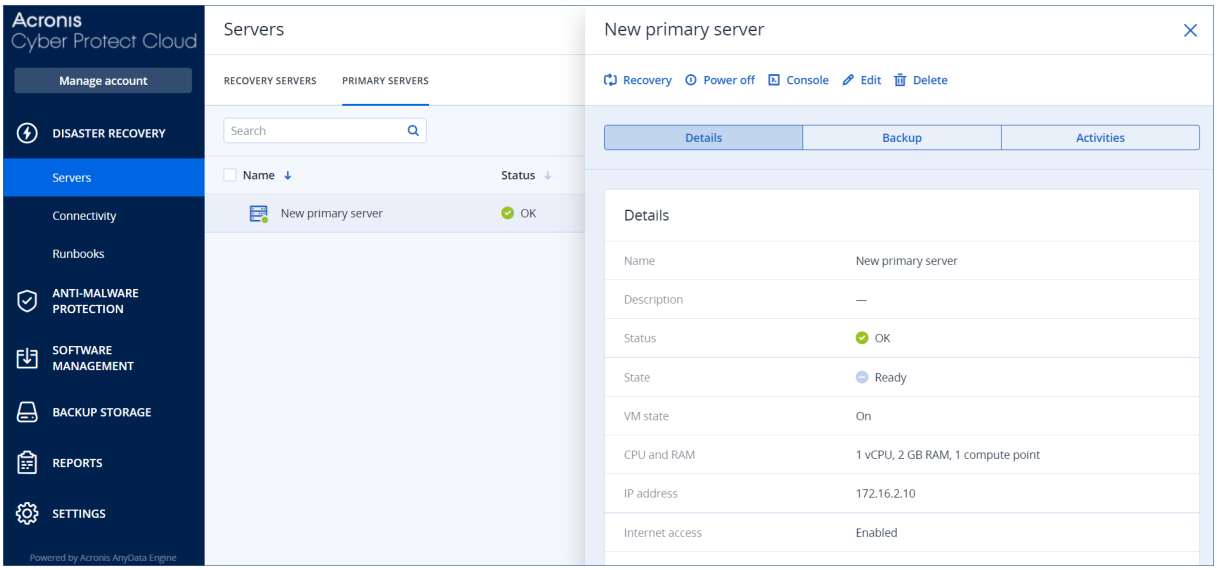
    如果您清除 **[使用公用 IP 位址]** 核取方塊，或刪除復原伺服器，將不會保留其公用 IP 位址。

12. [選用] 選擇 **[設定 RPO 閾值]**。

    RPO 閾值會定義上次復原點和目前時間之間的最大可允許時間間隔。此值可以設定在 15 – 60 分鐘、1 – 24 小時、1 – 14 天內。

13. 定義主要伺服器名稱。
14. [選用] 指定主要伺服器的描述。
15. [選用] 按一下 **[雲端防火牆規則]** 索引標籤以編輯預設防火牆規則。如需詳細資訊，請參閱 "設定雲端伺服器的防火牆規則" (第 703 頁)。
16. 按一下 **[建立]**。

主要伺服器便可在實際執行網路中使用。您可以使用伺服器的主控台、RDP、SSH 或 TeamViewer 來管理伺服器。



主要伺服器的操作

在 Cyber Protect 主控台中，主要伺服器會顯示在 **[災難復原]** > **[伺服器]** > **[主要伺服器]** 索引標籤上。

開啟電源

若要開啟主要伺服器電源

1. 在 **[主要伺服器]** 索引標籤上，按一下主要伺服器。
2. 按一下 **[開啟電源]**。

關閉電源

若要關閉主要伺服器電源

1. 在 **[主要伺服器]** 索引標籤上，按一下主要伺服器。
2. 按一下 **[關閉電源]**。
3. 在 **[關閉伺服器電源]** 畫面中，按一下 **[關閉電源]**。

強制關閉電源

若要強制關閉主要伺服器電源

1. 在 **[主要伺服器]** 索引標籤上，按一下主要伺服器。
2. 按一下 **[關閉電源]**。
3. 在 **[關閉伺服器電源]** 畫面中，選擇 **[強制關閉伺服器]**，然後按一下 **[關閉電源]**。

停止

若要停止主要伺服器

1. 在 **[主要伺服器]** 索引標籤上，按一下主要伺服器。
2. 按一下 **[停止]**。

編輯設定

若要編輯主要伺服器的設定

1. 在 **[主要伺服器]** 索引標籤上，按一下主要伺服器。
2. 按一下 **[停止]**。
3. 按一下 **[編輯]**，然後編輯設定。

套用保護計劃

若要將計劃套用到主要伺服器

1. 在 **[主要伺服器]** 索引標籤上，按一下主要伺服器。
2. 在 **[計劃]** 索引標籤上，按一下 **[建立]**。
   您將會看到預先定義的保護計劃，您只能在其中變更排程和保留規則。如需詳細資訊，請參閱「備份雲端伺服器」。

檢視有關雲端伺服器的詳細資料

若要檢視雲端伺服器的詳細資料，請移至 **[災難復原]** > **[伺服器]**。該處有兩個索引標籤：**[復原伺服器]** 和 **[主要伺服器]**。若要顯示表格中的所有選用欄，請按一下齒輪圖示。

您可以透過選取每部雲端伺服器，找到該伺服器的下列相關資訊。

欄名稱	描述

名稱	您定義的雲端伺服器名稱
狀態	反映雲端伺服器最嚴重問題的狀態 (根據作用中警示)
狀態	雲端伺服器狀態
VM 狀態	與雲端伺服器相關之虛擬機器的電源狀態
使用中的位置	託管雲端伺服器所在的位置。例如，**雲端**。
RPO 閾值	上次適合容錯移轉的復原點和目前時間之間允許的最大時間間隔。此值可以設定在 15-60 分鐘、1-24 小時、1-14 天內。
RPO 合規	RPO 合規是實際 RPO 和 RPO 閾值之間的比率。如果 RPO 閾值已經過定義，則會顯示 RPO 合規。 其計算方式如下： **RPO 合規 = 實際 RPO/RPO 閾值** 其中： **實際 RPO = 目前時間 – 上次復原點時間** **RPO 合規狀態** 根據實際 RPO 和 RPO 閾值間比率的值，會使用下列狀態： • **合規**。RPO 合規 < 1x。伺服器符合 RPO 閾值。 • **超過**。RPO 合規 <= 2x。伺服器違反 RPO 閾值。 • **嚴重超過**。RPO 合規 <= 4x。伺服器違反 RPO 閾值超過 2x 次。 • **極度超過**。RPO 合規 > 4x。伺服器違反 RPO 閾值超過 4x 次。 • **擱置中 (無備份)**。伺服器受到保護計劃保護，但備份正在建立，而且還未完成。
實際 RPO	自上次建立復原點後經過的時間
上次復原點	建立上次復原點的日期與時間

雲端伺服器的備份

主要伺服器和復原伺服器是無代理程式備份在雲端站台上。這些備份具有以下限制。

- 唯一的備份位置是雲端儲存。主要伺服器會備份到**主要伺服器備份**儲存空間。

  注意事項
  不支援 Microsoft Azure 備份位置。

- 備份計劃無法套用到多個伺服器。每個伺服器必須有自己的備份計劃，即使所有備份計劃具有相同設定也一樣。
- 只有一個備份計劃可以套用到網站。
- 不支援應用程式感知備份。

- 加密不可使用。
- 備份選項不可使用。

當您刪除主要伺服器時，也同時刪除其備份。

復原伺服器僅在容錯移轉狀態中才會備份。其備份會繼續原始伺服器的備份順序。執行容錯回復時，原始伺服器會繼續此備份順序。因此，復原伺服器的備份只能以手動方式刪除，或當做套用保留規則的結果。當刪除復原伺服器時，其備份一律會保留。

注意事項
雲端伺服器的備份計劃是根據 UTC 時間執行的。

雲端伺服器的防火牆規則

您可以將防火牆規則設定為控制雲端站台上，主要伺服器和復原伺服器的輸入及輸出流量。

您可以在佈建雲端伺服器的公用 IP 位址後設定輸入規則。預設允許 TCP 連接埠 443，並拒絕其他所有輸入連線。您可以變更預設防火牆規則，並新增或移除輸入例外。如果未佈建公用 IP，您僅能檢視輸入規則，但無法進行設定。

您可以在佈建雲端伺服器的網際網路存取後設定輸出規則。預設拒絕 TCP 連接埠 25，並允許其他所有輸出連線。您可以變更預設防火牆規則，並新增或移除輸出例外。如果未佈建網際網路存取，您僅能檢視輸出規則，但無法進行設定。

注意事項
基於安全性原因，有一些預先定義且您無法變更的防火牆規則。

針對輸入和輸出連線：

- 允許 Ping：ICMP echo-request (type 8, code 0) and ICMP echo-reply (type 0, code 0)
- Permit ICMP need-to-frag (type 3, code 4)
- Permit TTL exceeded (type 11, code 0)

僅針對輸入連線：

- 無法設定的部分：全部拒絕

僅針對輸出連線：

- 無法設定的部分：全部拒絕

設定雲端伺服器的防火牆規則

您可以針對雲端的主要伺服器和復原伺服器編輯預設防火牆規則。

若要編輯雲端站台上伺服器的防火牆規則

1. 在 Cyber Protect 主控台中，移至 **[災難復原]** > **[伺服器]**。
2. 如果您要編輯復原伺服器的防火牆規則，按一下 **[復原伺服器]** 索引標籤。或者，如果您要編輯主要伺服器的防火牆規則，按一下 **[主要伺服器]** 索引標籤。

3. 按一下伺服器，然後按一下 **[編輯]**。
4. 按一下 **[雲端防火牆規則]** 索引標籤。
5. 如果您要變更輸入連線的預設動作：
   a. 在 **[輸入]** 下拉式欄位中，選擇預設動作。

動作	描述
全部拒絕	拒絕任何輸入流量。 您可以新增例外，並允許來自特定 IP 位址、通訊協定和連接埠的流量。
全部允許	允許所有輸入 TCP 和 UDP 流量。 您可以新增例外，並拒絕來自特定 IP 位址、通訊協定和連接埠的流量。

注意事項
變更預設動作會使現有輸入規則的設定失效並加以移除。

   b. [選用] 如果您要儲存現有的例外，請在確認視窗中，選擇 **[儲存填入的例外]**。
   c. 按一下 **[確認]**。
6. 如果您要新增例外：
   a. 按一下 **[新增例外]**。
   b. 指定防火牆參數。

防火牆參數	描述
通訊協定	選擇用於連線的通訊協定。支援下列選項： • **TCP** • **UDP** • **TCP+UDP**
伺服器連接埠	選擇要套用規則的連接埠。您可以指定： • 特定連接埠號碼 (例如，2298) • 連接埠號碼範圍 (例如，6000-6700) • 任何連接埠號碼。如果您希望將規則套用到任何連接埠號碼，請使用 *。
用戶端 IP 位址	選擇要套用規則的 IP 位址。您可以指定： • 特定 IP 位址 (例如，192.168.0.0) • 使用 CIDR 標記法的 IP 位址範圍 (例如，192.168.0.0/24) • 任何 IP 位址。如果您希望將規則套用到任何 IP 位址，請使用 *。

7. 如果您要移除現有的輸入例外，按一下旁邊的垃圾桶圖示。
8. 如果您要變更輸出連線的預設動作：

a. 在 **[輸出]** 下拉式欄位中，選擇預設動作。

動作	描述
全部拒絕	拒絕任何輸出流量。 您可以新增例外，並允許前往特定 IP 位址、通訊協定和連接埠的流量。
全部允許	允許所有輸出流量。 您可以新增例外，並拒絕來自特定 IP 位址、通訊協定和連接埠的流量。

注意事項
變更預設動作會使現有輸出規則的設定失效並加以移除。

b. [選用] 如果您要儲存現有的例外，請在確認視窗中，選擇 **[儲存填入的例外]**。

c. 按一下 **[確認]**。

9. 如果您要新增例外：

a. 按一下 **[新增例外]**。

b. 指定防火牆參數。

防火牆參數	描述
通訊協定	選擇用於連線的通訊協定。支援下列選項： • **TCP** • **UDP** • **TCP+UDP**
伺服器連接埠	選擇要套用規則的連接埠。您可以指定： • 特定連接埠號碼 (例如，2298) • 連接埠號碼範圍 (例如，6000-6700) • 任何連接埠號碼。如果您希望將規則套用到任何連接埠號碼，請使用 *。
用戶端 IP 位址	選擇要套用規則的 IP 位址。您可以指定： • 特定 IP 位址 (例如，192.168.0.0) • 使用 CIDR 標記法的 IP 位址範圍 (例如，192.168.0.0/24) • 任何 IP 位址。如果您希望將規則套用到任何 IP 位址，請使用 *。

10. 如果您要移除現有的輸出例外，按一下旁邊的垃圾桶圖示。

11. 按一下 **[儲存]**。

檢查雲端防火牆活動

雲端伺服器防火牆規則設定更新後，更新活動記錄會出現在 Cyber Protect 主控台中。您可以檢視記錄並檢查下列資訊：

- 更新設定之使用者的使用者名稱
- 更新的日期和時間
- 輸入和輸出連線的防火牆設定
- 輸入和輸出連線的預設動作
- 輸入和輸出連線例外的通訊協定、連接埠和 IP 位址

若要檢視有關雲端防火牆規則設定變更的詳細資訊

1. 在 Cyber Protect 主控台中，按一下 **[監控]** > **[活動]**。
2. 按一下對應的活動，然後按一下 **[所有屬性]**。
   活動的描述應該是 **[正在更新雲端伺服器設定]**。
3. 在 **[內容]** 欄位中，檢查您感興趣的資訊。

計算點

在 [災難復原] 中，計算點在測試容錯移轉和實際執行容錯移轉期間用於主要伺服器及復原伺服器。計算點會反映在雲端執行伺服器 (虛擬機器) 所使用的計算資源。

計算點在災難復原期間的耗用量取決於伺服器的參數，以及伺服器處於容錯移轉狀態期間的持續時間。伺服器越強大且時間越長，耗用的計算點越多。此外，耗用的計算點越多，您要支付的價格就越高。

在 Acronis Cloud 中執行的所有伺服器，無論其狀態為開啟或關閉，都將根據計算點設定的類別收費。

處於 [待命] 狀態的復原伺服器不會耗用計算點，也不會產生計算點費用。

在下表中，您可以看到雲端中 8 部不同類別伺服器的範例，及其每小時耗用的對應計算點。您可以在 **[詳細資料]** 索引標籤中變更伺服器的類別。

類型	CPU	RAM	計算點
F1	1 個 vCPU	2 GB	1
F2	1 個 vCPU	4 GB	2
F3	2 個 vCPU	8 GB	4
F4	4 個 vCPU	16 GB	8
F5	8 個 vCPU	32 GB	16
F6	16 個 vCPU	64 GB	32
F7	16 個 vCPU	128 GB	64
F8	16 個 vCPU	256 GB	128

您可以使用表格中的資訊，輕鬆地估計一部伺服器 (虛擬機器) 將耗用的計算點數量。

例如，如果您要使用 [災難復原] 保護一部擁有 4 個 vCPU* 16 GB RAM 的虛擬機器，以及一部擁有 2 個 vCPU 8 GB RAM 的虛擬機器，則第一部虛擬機器每小時將耗用 8 個計算點，第二部虛擬機器每小時將耗用 4 個計算點。如果兩部虛擬機器都處於容錯移轉狀態，則總耗用量將為每小時 12 個計算點，或整天 288 個計算點 (12 個計算點 x 24 小時 = 288 個計算點)。

* vCPU 指的是指派給虛擬機器的實體中央處理器 (CPU)，而且是與時間相關的實體。

注意事項
如果達到**計算點**配額的超額，所有主要伺服器和復原伺服器都將關閉。在下一個計費週期開始之前，或在您增加配額之前，將無法使用這些伺服器。預設計費週期是一整個月。

測試容錯移轉

執行測試容錯移轉指的是在與您工作網路分開的測試 VLAN 中，啟動復原伺服器。您一次可以測試數部復原伺服器，並檢查其互動。在測試網路中，伺服器會使用其實際執行 IP 位址進行通訊，但它們無法啟動與您區域網路內工作負載的 TCP 或 UDP 連線。

在測試容錯移轉期間，虛擬機器 (復原伺服器) 並未最終化。代理程式會直接從備份讀取虛擬磁碟的內容，並隨機存取備份的不同部分。這可能會使處於測試容錯移轉狀態的復原伺服器的效能比其正常效能慢。

執行測試容錯移轉

雖然執行測試容錯移轉是選擇性的，但我們建議您就成本和安全考量，以適當頻率定期執行。有一個好作法是建立 Runbook，也就是一組說明如何在雲端啟動實際執行環境的指示。

重要事項
您必須事先建立復原伺服器以保護您的裝置免受災難影響。

您只能從建立裝置的復原伺服器後所建立的復原點 (備份) 執行容錯移轉。

容錯移轉至復原伺服器之前，必須至少建立一個復原點。支援的復原點數量上限為 100。

執行測試容錯移轉

1. 選取原始電腦或選取您要測試的復原伺服器。
2. 按一下 **[災難復原]**。
   接著會開啟復原伺服器的說明。
3. 按一下 **[容錯移轉]**。
4. 選取容錯移轉類型 **[測試容錯移轉]**。
5. 選擇復原點 (備份)，然後按一下 **[開始]**。
6. 如果您選擇的備份是使用加密作為機器屬性加密的：

a. 輸入備份集的加密密碼。

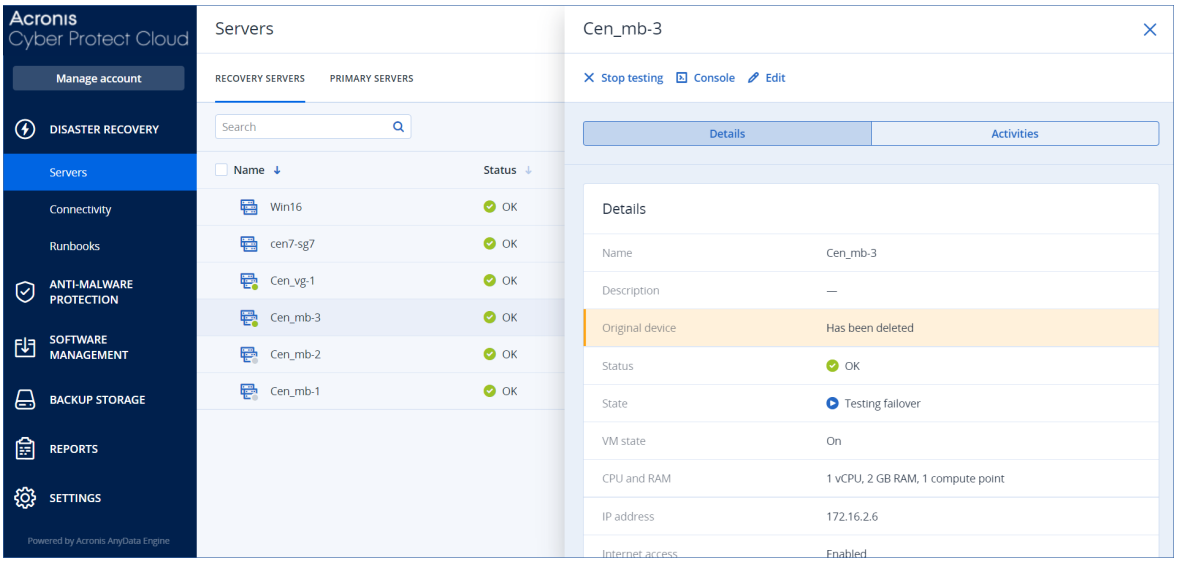
注意事項
此密碼僅會暫時儲存，而且將僅用於目前的測試容錯移轉作業。在測試容錯移轉停止時或測試容錯移轉作業完成後，此密碼會自動從認證存放區中刪除。

b. [選用] 若要儲存備份集的密碼並將其用於後續的容錯移轉作業，請選擇 **[將密碼儲存在安全的認證存放區中...]** 核取方塊，然後在 **[認證名稱]** 欄位中，輸入認證的名稱。

重要事項
密碼將儲存在安全的認證存放區中，而且將在後續的容錯移轉作業中自動套用。但是，儲存密碼可能會與法規遵循義務相衝突。

c. 按一下**[完成]**。

當復原伺服器啟動時，其狀態會變更為 **[正在測試容錯移轉]**。



7. 使用下列任何一個方法測試復原伺服器：
   - 在 **[災難復原]** > **[伺服器]** 中，選取復原伺服器，然後按一下 **[主控台]**。
   - 使用 RDP 或 SSH，以及您在建立復原伺服器時指定的測試 IP，連線到復原伺服器。在實際執行網路內部和外部皆嘗試連線 (如「點對站台連線」中所述)。
   - 在復原伺服器內執行指令碼。
     指令碼可檢查登入畫面、應用程式是否啟動、網際網路連線，以及其他電腦連線到復原伺服器的能力。
   - 如果復原伺服器具備網際網路存取權和公共 IP 位址，您可能會想使用 TeamViewer。
8. 當測試完成時，按一下 **[停止測試]**。
   復原伺服器隨即停止。在測試容錯移轉期間針對復原伺服器所做的變更都不會保留。

注意事項
在 Runbook 中，或在手動啟動測試容錯移轉時，**[啟動伺服器]** 和 **[停止伺服器]** 動作都不適用於測試容錯移轉作業。如果您嘗試執行此種動作，將會失敗，並出現下列錯誤訊息：
失敗：此動作不適用於目前的伺服器狀態。

自動測試容錯移轉

使用自動測試容錯移轉，每月自動測試復原伺服器一次，無需任何手動互動。

自動測試容錯移轉程序包含下列部分：

1. 從最後一個復原點建立虛擬機器
2. 擷取虛擬機器的螢幕擷取畫面
3. 分析虛擬機器的作業系統是否啟動成功
4. 通知您有關測試容錯移轉狀態

注意事項
自動測試容錯移轉會使用計算點。

您可以在復原伺服器的設定中設定自動測試容錯移轉。如需詳細資訊，請參閱 "設定自動測試容錯移轉" (第 709 頁)。

請注意，在極少數情況下，自動測試容錯移轉可能會被跳過，而且可能不會在排程時間執行。這是因為生產故障容錯移轉的優先順序高於自動測試容錯移轉，因此配置給自動測試容錯移轉的硬體資源 (CPU 和 RAM) 可能會暫時受限，以確保有足夠資源用於並行的生產容錯移轉。

如果出於某種原因而跳過自動測試容錯移轉，則會發出警示。

注意事項
如果原始機器的反斜線使用加密作為機器屬性進行加密，並且在創建復原後的磁碟區序列化程式時未指定加密傳遞磁碟，則自動化測試容錯回復將會失敗。有關指定加密傳遞磁碟的更多資訊，請參見"建立復原伺服器" (第 694 頁)。

設定自動測試容錯移轉

透過設定自動測試容錯移轉，可以每月測試您的復原伺服器，無需執行任何手動動作。

若要設定自動測試容錯移轉

1. 在主控台中，移至 **[災難復原]** > **[伺服器]** > **[復原伺服器]**，然後選擇復原伺服器。
2. 按一下 **[編輯]**。
3. 在 **[自動測試容錯移轉]** 區段的 **[排程]** 欄位中，選擇 **[每月]**。
4. [選用] 在 **[螢幕擷取畫面逾時]** 中，變更系統嘗試執行自動測試容錯移轉的最長時間預設值 (以分鐘為單位)。
5. [選用] 如果您想要將 **[螢幕擷取畫面逾時]** 值儲存為預設值，並在啟用其他復原伺服器的自動測

試容錯移轉時將其自動填入，請選擇 **[設為預設逾時]**。

6. 按一下 **[儲存]**。

檢視自動測試容錯移轉狀態

您可以檢視完整的自動測試容錯移轉詳細資料，例如狀態、開始時間、結束時間、持續時間，以及虛擬機器的螢幕擷取畫面。

注意事項
虛擬機器的螢幕擷取畫面會保留，直到自動測試容錯移轉再次執行並產生新的螢幕擷取畫面為止。

若要檢視復原伺服器的自動測試容錯移轉狀態

1. 在主控台中，移至 **[災難復原]** > **[伺服器]** > **[復原伺服器]**，然後選擇復原伺服器。
2. 在 **[自動測試容錯移轉]** 區段中，查看上次自動測試容錯移轉的詳細資料。
3. 若要檢視虛擬機器的螢幕擷取畫面，請按一下 **[顯示螢幕擷取畫面]**。

停用自動測試容錯移轉

如果想要節省資源，或者某個復原伺服器不需要執行自動測試容錯移轉，您可以停用自動測試容錯移轉。

若要停用自動測試容錯移轉

1. 在主控台中，移至 **[災難復原]** > **[伺服器]** > **[復原伺服器]**，然後選擇復原伺服器。
2. 按一下 **[編輯]**。
3. 在 **[自動測試容錯移轉]** 區段的 **[排程]** 欄位中，選擇 **[永不]**。
4. 按一下 **[儲存]**。

實際執行容錯移轉

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

復原伺服器建立時，它會維持在 **[待命]** 狀態。在開始容錯移轉之前，對應的虛擬機器不存在。開始容錯移轉程序之前，您必須為原始電腦建立至少一個磁碟映像備份 (含可開機磁碟區)。

開始容錯移轉程序時，您要選擇原始電腦的復原點 (備份)，您將會從該復原點使用預先定義的參數建立虛擬機器。容錯移轉作業會使用「從備份執行 VM」功能。復原伺服器的過渡狀態為 **[最終化]**。此程序意味著將伺服器的虛擬磁碟從備份儲存空間 (「冷」儲存) 傳送到災難復原儲存空間 (「熱」儲存)。

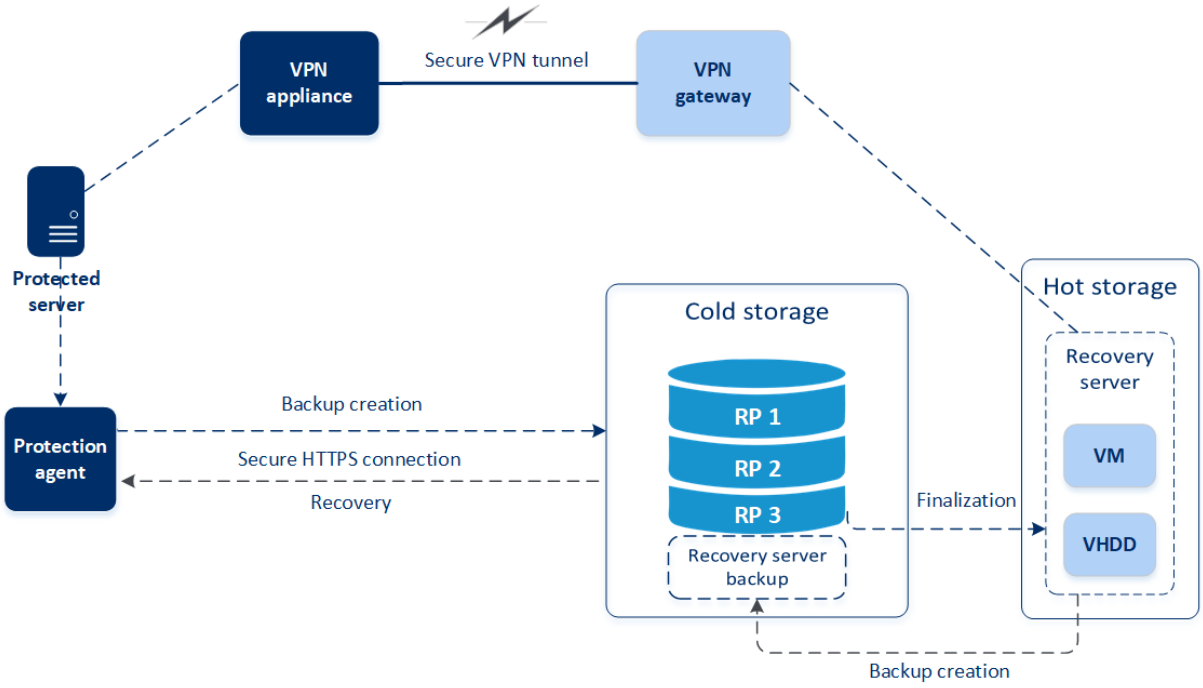
注意事項

在 **[最終化]** 期間，雖然效能低於正常狀態，但仍然可以存取和操作。您可以按一下 **[主控台就緒]** 連結來開啟伺服器主控台。此連結可在 **[災難復原]** > **[伺服器]** 畫面上的 **[VM 狀態]** 欄中，以及伺服器的 **[詳細資料]** 檢視中取得。

當 **[最終化]** 完成後，伺服器效能就會達到其正常值。伺服器狀態會變更為 **[容錯移轉]**。工作負載現在會從原始電腦切換到雲端站台中的復原伺服器。

如果復原伺服器內部有保護代理程式，則會停止代理程式服務，以避免干擾 (例如開始備份或將過期的狀態報告至備份元件)。

在以下的圖表中，您可以同時看到容錯移轉和容錯回復程序。



執行容錯移轉

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

容錯移轉是從您本機將工作負載移到雲端的程序，也是工作負載保留在雲端的狀態。

當您開始容錯移轉時，復原伺服器會在實際執行網路中啟動。為避免干擾和不必要的問題，請確保原始工作負載不在線上且無法透過 VPN 存取。

為了避免對同一個雲端存檔的備份干擾，請手動撤銷目前處於**容錯移轉**狀態之工作負載的保護計劃。如需有關撤銷計劃的詳細資訊，請參閱撤銷保護計劃。

重要事項
您必須事先建立復原伺服器以保護您的裝置免受災難影響。

您只能從建立裝置的復原伺服器後所建立的復原點 (備份) 執行容錯移轉。

容錯移轉至復原伺服器之前，必須至少建立一個復原點。支援的復原點數量上限為 100。

您可以依照下方的程序或觀看影片教學。

執行容錯移轉

1. 確認原始電腦在網路上無法使用。
2. 在 Cyber Protect 主控台中，移至 **[災難復原]** > **[伺服器]** > **[復原伺服器]**，然後選擇復原伺服器。
3. 按一下 **[容錯移轉]**。
4. 選擇 **[實際執行容錯移轉]**。
5. 選擇復原點 (備份)，然後按一下 **[開始]**。
6. [如果您選擇的備份是使用加密作為機器屬性加密的]
   a. 輸入備份集的加密密碼。

      注意事項
      此密碼僅會暫時儲存，而且將僅用於目前的容錯移轉作業。在容錯移轉作業完成且伺服器回復到 **[待命]** 狀態時，此密碼會自動從認證存放區中刪除。

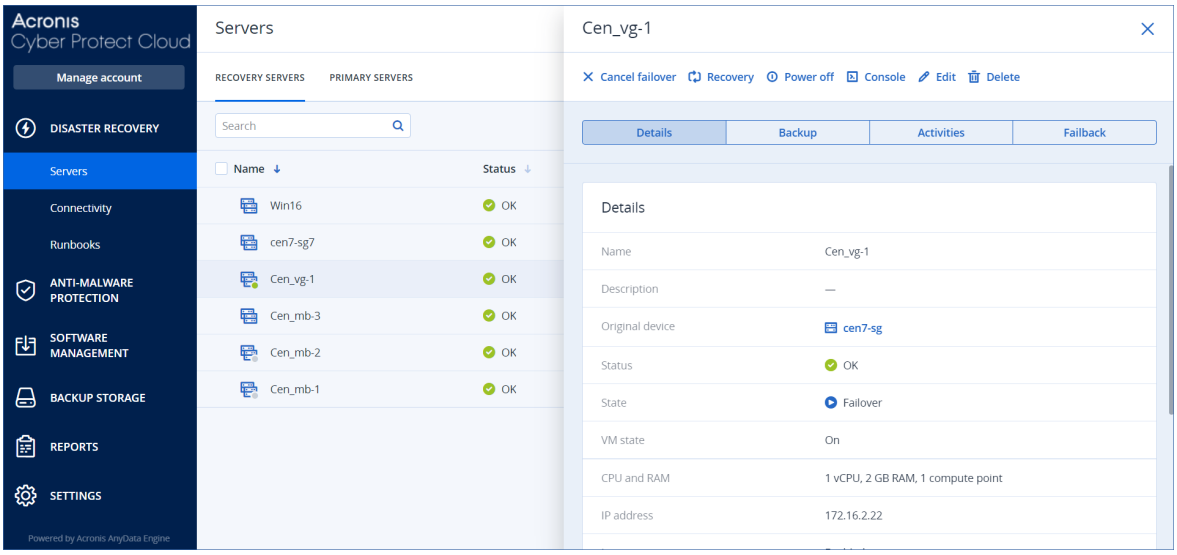
   b. [選用] 若要儲存備份集的密碼並將其用於後續的容錯移轉作業，請選擇 **[將密碼儲存在安全的認證存放區中...]** 核取方塊，然後在 **[認證名稱]** 欄位中，輸入認證的名稱。

      重要事項
      密碼將儲存在安全的認證存放區中，而且將在後續的容錯移轉作業中自動套用。但是，儲存密碼可能會與法規遵循義務相衝突。

   c. 按一下 **[完成]**。

   當復原伺服器啟動時，其狀態會變更為 **[最終化]**，一段時間後則會變更為 **[容錯移轉]**。

   重要事項
   瞭解伺服器 **[最終化]** 和 **[容錯移轉]** 這兩種狀態下都可以使用至關重要。在 **[最終化]** 狀態期間，您可以按一下 **[主控台就緒]** 連結來存取伺服器主控台。此連結可在 **[災難復原]** > **[伺服器]** 畫面上的 **[VM 狀態]** 欄中，以及伺服器的 **[詳細資料]** 檢視中取得。



7. 透過檢視其主控台，確認復原伺服器已啟動。按一下 **[災難復原]** > **[伺服器]**、選取復原伺服器，然後按一下 **[主控台]**。
8. 確認可使用您在建立復原伺服器時指定的實際執行 IP 位址存取復原伺服器。

復原伺服器最終化之後，會自動建立新的保護計劃並套用至復原伺服器。此保護計劃是以用來建立復原伺服器的保護計劃為基礎，其有特定限制。在此計劃中，您可以變更的只有排程和保留規則。如需詳細資訊，請參閱 < 備份雲端伺服器 > 。

如何使用本機 DNS 執行伺服器的容錯移轉

如果您使用本機站台上的 DNS 伺服器解析電腦名稱，則在容錯移轉對應依賴 DNS 之電腦的復原伺服器之後，將因為雲端中使用的 DNS 伺服器不同而無法通訊。根據預設，雲端站台的 DNS 伺服器用於新建立的雲端伺服器。如果您需要套用自訂 DNS 設定，請連絡支援小組。

如何執行 DHCP 伺服器的容錯移轉

您本機基礎架構的 DHCP 伺服器可能位於 Windows 或 Linux 主機。當這種主機容錯移轉至雲端站台時，會發生 DHCP 伺服器重複問題，因為雲端中的 VPN 閘道也會執行 DHCP 角色。若要解決這個問題，請執行下列其中一項操作：

- 如果只有 DHCP 主機容錯移轉至雲端，雖然其餘的雲端伺服器仍在本機站台，但您還是必須登入雲端的 DHCP 主機，並關閉其上的 DHCP 伺服器。因此，將不會發生衝突，而且只有 VPN 閘道將會當做 DHCP 伺服器。
- 如果您的雲端伺服器已經從 DHCP 主機取得 IP 位址，則您必須登入雲端的 DHCP 主機，並關閉其上的 DHCP 伺服器。您也必須登入雲端伺服器並更新 DHCP 租賃，以指派從正確的 DHCP 伺服器 (在 VPN 閘道上託管) 配置的新 IP 位址。

注意事項

當您的雲端 DHCP 伺服器設定為 **[自訂 DHCP]** 選項時，這些指示無效，而且某些復原或主要伺服器會從此 DHCP 伺服器獲得其 IP 位址。

停止容錯移轉

您可以在處理程序的每個階段，隨時停止實際執行容錯移轉。

注意事項
停止容錯移轉會還原從容錯移轉開始執行時所做的所有變更，但復原伺服器備份除外。

若要停止實際執行容錯移轉

1. 在 Cyber Protect 主控台中，前往 **[災難復原]** > **[伺服器]** > **[復原伺服器]**。
2. 選擇處於**[容錯移轉]** 狀態的復原伺服器。
3. 按一下復原伺服器。
4. 按一下 **[停止容錯移轉]**。
5. 在出現的確認視窗中，選擇核取方塊，然後按一下 **[停止容錯移轉]**。
   容錯移轉隨即停止。復原伺服器會回復至 **[待機]** 狀態。

容錯回復

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

容錯回復是從雲端將工作負載移回您本機站台上的實體或虛擬機器的程序。您可以在**容錯移轉**狀態下對復原伺服器執行容錯回復，並在本機站台上繼續使用伺服器。

您可以對本機站台上的虛擬或實體目標機器執行自動容錯移轉。在容錯回復期間，您可以在雲端的虛擬機器繼續執行時，將備份資料傳輸到本機站台。此技術有助於達到非常短的停機期間，且此停機期間可以估算並顯示在 Cyber Protect 主控台中。您可以檢視此停機期間，並使用這項資訊規劃您的活動，必要時，對您的用戶端提出停機期間即將到來的警告。如果您透過可開機媒體執行代理程式型容錯回復，停機時間甚至更短，因為只有差異變更將傳輸到本機站台。

若要容錯回復至目標實體機器，您可以透過可開機媒體使用代理程式型容錯回復。如需詳細資訊，請參閱 "執行代理程式型容錯回復 (透過可開機媒體)" (第 716 頁)。

若要容錯回復至目標虛擬機器，您可以透過可開機媒體使用代理程式型容錯回復，或透過 Hypervisor 代理程式使用無代理程式容錯回復。如需詳細資訊，請參閱 "執行代理程式型容錯回復 (透過可開機媒體)" (第 716 頁) 和 "執行無代理程式容錯回復 (透過 Hypervisor 代理程式)" (第 719 頁)。

在您無法使用自動容錯回復程序的特定情況下，可以執行手動容錯回復。如需詳細資訊，請參閱 "手動容錯回復" (第 722 頁)。

注意事項
Runbook 作業僅支援手動模式下的容錯回復。也就是說，如果您透過執行包含**容錯回復伺服器**步驟的 Runbook 來開始容錯回復程序，此程序將需要手動互動：您必須手動復原機器，並從 **[災難復原]** > **[伺服器]** 索引標籤確認或取消容錯回復程序。

代理程式型容錯回復 (透過可開機媒體)

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

代理程式型容錯回復 (透過可開機媒體) 程序已經過最佳化，可容錯回復至原始實體或虛擬機器。在此程序中，僅將增量變更傳輸至本機站台。

透過可開機媒體至目標實體或虛擬機器的代理程式型容錯回復 (透過可開機媒體) 程序包括下列階段：

1. **規劃**。在此階段期間，您要在本機站台還原 IT 基礎架構 (例如，主機和網路設定)、設定容錯回復參數，以及規劃開始資料傳輸的時間。
2. **資料傳輸**。在此階段期間，資料會在雲端的虛擬機器繼續執行時，從雲端站台傳輸到本機站台。您可以在資料傳輸階段期間，隨時開始下一個階段 (轉換)，但是您應該考慮下列關係。

   您維持在資料傳輸階段的時間越長，
   - 雲端的虛擬機器繼續執行的時間越長，
   - 傳輸到本機站台的資料越多，
   - 您將支付的成本越高 (您花費的計算點越多)。
   - 您在轉換階段經歷的停機期間越短。

   如果您要將停機時間減至最少，請在超過 90% 的資料傳輸到本機站台之後，就開始轉換階段。

   如果您可以承受經歷較長的停機期間，而且不想要花費更多的計算點執行雲端的虛擬機器，您可以更早開始轉換階段。

   注意事項
   資料傳輸程序使用 Flashback 技術。此技術會比較目標電腦上存在的資料與虛擬機器在雲端的資料。如果目標電腦上已存在部分資料，則不會再次傳輸這些資料。此技術會加快資料傳輸階段的速度。
   因此，建議您將伺服器還原到您本機站台上的原始電腦。

3. **轉換**。此階段期間會關閉雲端的虛擬機器，而且包括上次備份增量在內的剩餘資料會傳輸到本機站台。如果在復原伺服器上未套用任何備份計劃，將會在轉換階段期間自動執行備份，這會減慢該程序。
4. **驗證**。在此階段期間，本機站台上的實體機器已準備就緒，您可以使用 Linux 可開機媒體將其重新開機。您可以確認虛擬機器正確運作，而且：
   - 如果一切如預期般運作，請確認容錯回復。容錯回復確認之後，雲端的虛擬機器就會遭到刪除，且復原伺服器會回復到**待命**狀態。這是容錯回復程序的結尾。
   - 如果發生問題，您可以取消容錯移轉，並返回規劃階段。

注意事項

可開機媒體重新開機後，您將無法再次使用它。如果在驗證階段發生問題，則您必須註冊新的可開機媒體，並再次開始容錯回復程序。

但是在使用 Flashback 技術時，將不會再次傳輸本機站台上已經存在的資料，因此容錯回復程序將會快很多。

執行代理程式型容錯回復 (透過可開機媒體)

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以對本機站台上的目標實體或虛擬機器，透過可開機媒體執行代理程式型容錯回復。

注意事項

資料傳輸程序使用 Flashback 技術。此技術會比較目標電腦上存在的資料與虛擬機器在雲端的資料。如果目標電腦上已存在部分資料，則不會再次傳輸這些資料。此技術會加快資料傳輸階段的速度。

因此，建議您將伺服器還原到您本機站台上的原始電腦。

必要條件

- 您將用於執行容錯回復的代理程式已連線，且目前未用於其他容錯回復作業。
- 您的網際網路連線穩定。
- 已註冊的可開機媒體可供使用。如需詳細資訊，請參閱《Cyber Protection 使用指南》中的「建立可開機媒體以復原作業系統」。
- 目標機器是本機站台上的原始機器，或者與原始機器擁有相同的韌體。
- 雲端至少有一個虛擬機器的完整備份。

對實體機器執行容錯回復

1. 在 Cyber Protect 主控台中，移至 **[災難復原]** > **[伺服器]**。
2. 選擇處於**[容錯移轉]** 狀態的復原伺服器。
3. 按一下 **[容錯回復]** 索引標籤。
4. 在 **[容錯回復類型]** 欄位中，選擇 **[代理程式型 (透過可開機媒體)]**。
5. 在 **[目標可開機媒體]** 欄位中，按一下 **[指定]**，選擇可開機媒體，然後按一下 **[完成]**。

   注意事項

   建議您使用已設定的現成可開機媒體。如需詳細資訊，請參閱《Cyber Protection 使用指南》中的「建立可開機媒體以復原作業系統」。

6. [選用] 若要變更預設磁碟對應，請在 **[磁碟對應]** 欄位中，按一下 **[指定]**，將備份的磁碟對應到目標電腦的磁碟，然後按一下 **[完成]**。
7. 按一下 **[開始資料傳輸]**，然後在確認視窗中，按一下 **[開始]**。

注意事項

如果雲端中沒有虛擬機器的備份，系統將在資料傳輸階段之前自動執行備份。

資料傳輸階段隨即開始。主控台會顯示以下資訊：

欄位	描述
進度	此參數會顯示已經傳輸到本機站台的資料量以及必須傳輸的總資料量。 總資料量包括資料傳輸階段開始前最後備份的資料，以及新產生資料的備份 (備份增量)，因為虛擬機器在資料傳輸階段期間會繼續執行。因此，**[進度]** 值會隨著時間而增加。 由於系統在資料傳輸期間使用 Flashback 技術，且不傳輸目標電腦上已存在的資料，因此進度可能比主控台最初計算的速度更快。
停機時間預估	此參數會顯示如果您現在開始轉換階段，將無法使用雲端的虛擬機器的時間。這個值是根據 **[進度]** 參數的值計算得來，而且會隨著時間而減少。 由於系統在資料傳輸期間使用 Flashback 技術，且不傳輸目標電腦上已存在的資料，因此停機時間可能比主控台中最初顯示的值短很多。

8. 按一下 **[轉換]**，然後在確認視窗中，再按一下 **[轉換]**。

   轉換階段隨即開始。主控台會顯示以下資訊：

欄位	描述
進度	此參數會顯示在本機站台上還原電腦的進度。
估計的完成時間	此參數會顯示將完成轉換階段，而且您將能夠啟動本機站台上電腦的大約時間。

注意事項

如果雲端虛擬機器上未套用任何備份計劃，將會在轉換階段期間自動執行備份，從而導致停機時間較長。

9. **轉換**階段完成後，請使用可開機媒體重新開機，然後驗證本機站台上的實體機器是否如預期般運作。

   如需詳細資訊，請參閱《Cyber Protection 使用指南》中的「使用可開機媒體復原磁碟」。

10. 按一下 **[確認容錯回復]**，然後在確認視窗中，按一下 **[確認]** 以結束程序。

    雲端的虛擬機器會遭到刪除，且復原伺服器會回復到**待命**狀態。

注意事項

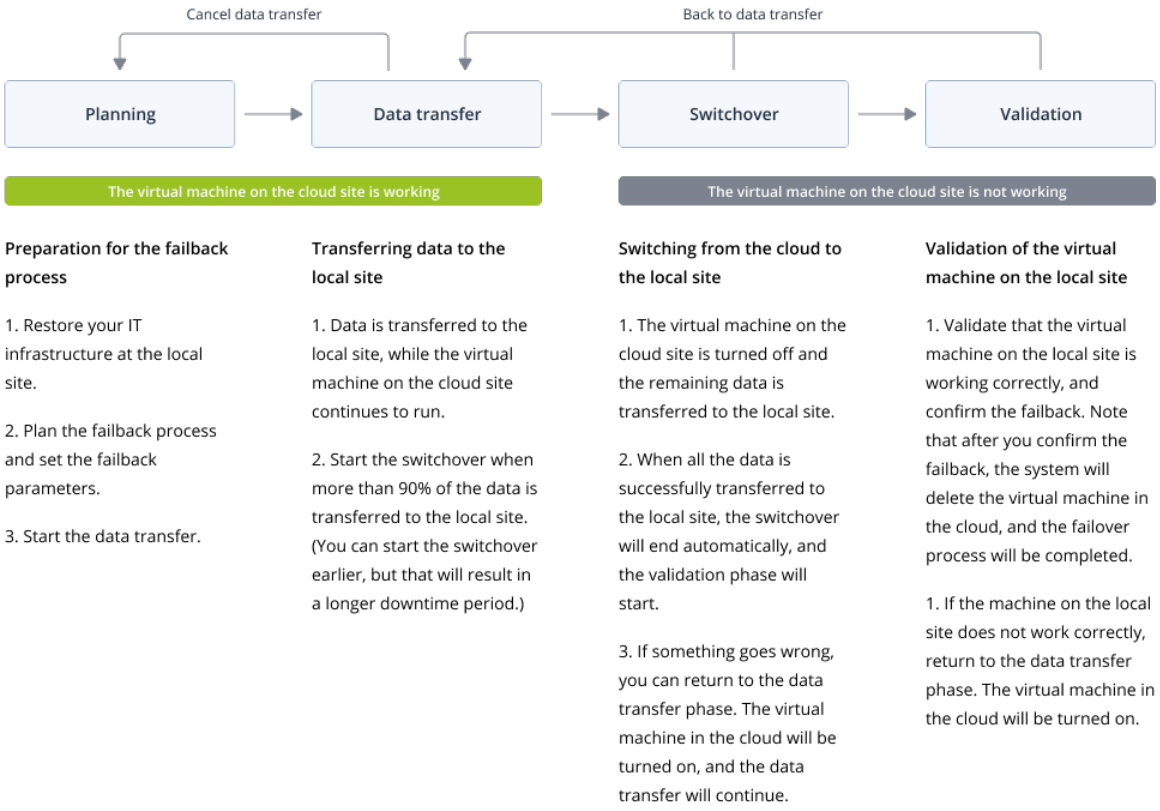
在復原的伺服器上套用保護計劃不是容錯回復程序的一部分。在容錯回復程序完成之後，在復原的伺服器上套用保護計劃以確保其再次受到保護。您可以套用在原始伺服器上套用的相同保護計劃，也可以套用已啟用 **[災難復原]** 模組的新保護計劃。

無代理程式容錯回復 (透過 Hypervisor 代理程式)

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

無代理程式容錯回復 (透過 Hypervisor 代理程式) 程序已經過最佳化，可容錯回復至新的虛擬機器。若要容錯回復至原始虛擬機器，請依照代理程式型容錯回復 (透過可開機媒體) 的程序執行。

無代理程式容錯回復 (透過 Hypervisor 代理程式) 包括四個階段。



1. **規劃**。在此階段期間，您要在本機站台還原 IT 基礎架構 (例如，主機和網路設定)、設定容錯回復參數，以及規劃開始資料傳輸的時間。

   注意事項
   為將容錯回復程序的全部時間減至最少，建議您在設定本機伺服器後立即開始資料傳輸階段，然後在資料傳輸階段期間，繼續設定網路以及其餘的本機基礎架構。

2. **資料傳輸**。在此階段期間，資料會在雲端的虛擬機器繼續執行時，從雲端站台傳輸到本機站台。您可以在資料傳輸階段期間，隨時開始下一個階段 (轉換)，但是您應該考慮下列關係。
   您維持在資料傳輸階段的時間越長，
   - 雲端的虛擬機器繼續執行的時間越長，
   - 傳輸到本機站台的資料越多，

- 您將支付的成本越高 (您花費的計算點越多)。
- 您在轉換階段經歷的停機期間越短。

如果您要將停機時間減至最少，請在超過 90% 的資料傳輸到本機站台之後，就開始轉換階段。

如果您可以承受經歷較長的停機期間，而且不想要花費更多的計算點執行雲端的虛擬機器，您可以更早開始轉換階段。

如果您在資料傳輸階段期間取消容錯回復程序，已傳輸的資料將不會從本機站台刪除。為避免可能的問題，請先手動刪除已傳輸的資料，然後再開始新的容錯回復程序。下列資料傳輸程序將從頭開始。

3. **轉換**。此階段期間會關閉雲端的虛擬機器，而且包括上次備份增量在內的剩餘資料會傳輸到本機站台。如果在復原伺服器上未套用任何備份計劃，將會在轉換階段期間自動執行備份，這會減慢該程序。

   您可以在 Cyber Protect主控台中，檢視完成此階段的估計時間 (停機期間)。當所有資料都傳輸到本機站台 (不會失去任何資料，而且本機站台上的虛擬機器為雲端虛擬機器完全相符的複本) 時，轉換階段便完成。系統會復原本機站台上的虛擬機器，而且會自動開始驗證階段。
4. **驗證**。在此階段期間，本機站台上的虛擬機器已準備就緒，並已自動啟動。您可以確認虛擬機器正確運作，而且：
   - 如果一切如預期般運作，請確認容錯回復。容錯回復確認之後，雲端的虛擬機器就會遭到刪除，且復原伺服器會回復到**待命**狀態。這是容錯回復程序的結尾。
   - 如果發生問題，您可以取消轉換，並返回資料傳輸階段。

執行無代理程式容錯回復 (透過 Hypervisor 代理程式)

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以透過 Hypervisor 代理程式，在本機站台對目標虛擬機器執行無代理程式容錯回復。

必要條件

- 您將用於執行容錯回復的代理程式已連線，且目前未用於其他容錯回復作業。
- 您的網際網路連線穩定。
- 雲端至少有一個虛擬機器的完整備份。

若要透過 Hypervisor 代理程式對虛擬機器執行無代理程式容錯回復

1. 在 Cyber Protect 主控台中，移至 **[災難復原]** > **[伺服器]**。
2. 選擇處於**[容錯移轉]** 狀態的復原伺服器。
3. 按一下 **[容錯回復]** 索引標籤。
4. 在 **[容錯回復參數]** 區段的 **[容錯回復類型]** 欄位中，選擇 **[無代理程式 (透過 Hypervisor 代理程式)]**，然後設定其他參數。

   請注意，部分 **[容錯回復參數]** 預設會自動填入建議的值，但是您可以加以變更。

   下表提供有關 **[容錯回復參數]** 的詳細資訊。

參數	描述
備份大小	在容錯回復程序期間傳輸到本機站台的資料量。 在您開始容錯回復到目標虛擬機器的程序之後，**[備份大小]** 將會在 [資料傳輸] 階段增加，因為雲端的虛擬機器將繼續執行並產生新資料。 若要計算容錯回復至目標虛擬機器程序期間的預估停機期間，請使用 10% 的 **[備份大小]** 值 (因為我們建議您在 90% 的資料傳輸到本機站台之後再開始 [轉換] 階段)，並將其除以您網際網路速度的值。 **注意事項** 當您同時執行數個容錯回復程序時，網際網路速度的值將會減少。
目標電腦位置	容錯回復位置：VMware ESXi 主機或 Microsoft Hyper-V 主機。 您可以從裝有已向網路保護服務註冊之代理程式的所有主機選擇。
代理程式	將執行容錯回復作業的代理程式。 您可以同時使用一個代理程式執行一個容錯回復作業。 您可以選擇已連線且目前未用於其他容錯回復程序、具備支援容錯回復功能的版本，以及擁有存取備份權限的代理程式。 請注意，您可以在 VMware ESXi 主機上安裝數個代理程式，並使用每一個代理程式開始一個個別的容錯回復程序。這些容錯回復程序可以同時執行。
目標電腦設定	虛擬機器設定： • **虛擬處理器**。選擇虛擬裝置的數量。 • **記憶體**。選擇虛擬機器將具備的記憶體數量。 • **單位**。選擇記憶體的單位。 • [選用] **網路介面卡**。若要新增網路介面卡，按一下 **[新增]**，然後在 **[網路]** 欄位中選擇一個網路。 當您準備好進行變更時，按一下 **[完成]**。
路徑	(適用於 Microsoft Hyper-V 主機) 將存放您電腦所在主機上的資料夾。 請確認電腦的主機上有足夠的可用記憶體空間。
資料存放區	(適用於 VMware ESXi 主機) 將存放您電腦所在主機上的資料存放區。 請確認電腦的主機上有足夠的可用記憶體空間。
佈建模式	虛擬磁碟配置的方法。 若是 Microsoft Hyper-V 主機： • **動態擴充** (預設值)。 • **固定大小**。 若是 Microsoft Hyper-V 主機： • **精簡** (預設值)。 • **密集**。
目標	目標電腦的名稱。根據預設，目標電腦名稱與復原伺服器名稱相同。

參數	描述
電腦名稱	目標電腦名稱在所選**目標電腦位置**上必須是唯一的。

5. 按一下 **[開始資料傳輸]**，然後在確認視窗中，按一下 **[開始]**。

注意事項
如果雲端中沒有虛擬機器的備份，系統將在資料傳輸階段之前自動執行備份。

資料傳輸階段隨即開始。主控台會顯示以下資訊：

欄位	描述
進度	此參數會顯示已經傳輸到本機站台的資料量以及必須傳輸的總資料量。 總資料量包括資料傳輸階段開始前最後備份的資料，以及新產生資料的備份 (備份增量)，因為虛擬機器在資料傳輸階段期間會繼續執行。因此，**[進度]** 參數的這兩個值會隨著時間而增加。
停機時間預估	此參數會顯示如果您現在開始轉換階段，將無法使用雲端的虛擬機器的時間。這個值是根據 **[進度]** 參數的值計算得來，而且會隨著時間而減少。

6. 按一下 **[轉換]**，然後在確認視窗中，再按一下 **[轉換]**。
轉換階段隨即開始。主控台會顯示以下資訊：

欄位	描述
進度	此參數會顯示在本機站台上還原電腦的進度。
估計的完成時間	此參數會顯示將完成轉換階段，而且您將能夠啟動本機站台上電腦的大約時間。

注意事項
如果雲端虛擬機器上未套用任何備份計劃，將會在轉換階段期間自動執行備份，從而導致停機時間較長。

7. **轉換**階段完成且本機站台上的虛擬機器自動啟動後，驗證是否如預期般運作。
8. 按一下 **[確認容錯回復]**，然後在確認視窗中，按一下 **[確認]** 以結束程序。
雲端的虛擬機器會遭到刪除，且復原伺服器會回復到**待命**狀態。

注意事項
在復原的伺服器上套用保護計劃不是容錯回復程序的一部分。在容錯回復程序完成之後，在復原的伺服器上套用保護計劃以確保其再次受到保護。您可以套用在原始伺服器上套用的相同保護計劃，也可以套用已啟用 **[災難復原]** 模組的新保護計劃。

手動容錯回復

注意事項
建議您僅在支援團隊建議時，才在手動模式下使用容錯回復程序。

您也可以在手動模式下開始容錯回復程序。在此情況下，資料將不會自動從雲端的備份傳輸到本機站台。此程序必須在雲端的虛擬機器關閉之後手動完成。這會使手動模式下的容錯回復程序慢很多，因此您應該預期停機時間會更長。

手動模式下的容錯回復程序包括下列階段：

1. **規劃**。在此階段期間，您要在本機站台還原 IT 基礎架構 (例如，主機和網路設定)、設定容錯回復參數，以及規劃開始資料傳輸的時間。
2. **轉換**。此階段期間會關閉雲端的虛擬機器，並備份新產生的資料。如果在復原伺服器上未套用任何備份計劃，將會在轉換階段期間自動執行備份，這會減慢該程序。備份完成後，您要手動將電腦復原到本機站台。您可以使用可開機媒體復原磁碟，或從雲端備份儲存空間復原整部電腦。
3. **驗證**。在此階段期間，您要確認本機站台的實體或虛擬機器正確運作並確認容錯回復。確認之後，雲端站台的虛擬機器會遭到刪除，且復原伺服器會回復到**待命**狀態。

執行手動容錯回復

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以對本機站台上的目標實體或虛擬機器執行手動容錯回復。

若要執行手動容錯回復

1. 在 Cyber Protect 主控台中，移至 **[災難復原]** > **[伺服器]**。
2. 選擇處於**[容錯移轉]** 狀態的復原伺服器。
3. 按一下 **[容錯回復]** 索引標籤。
4. 在 **[目標]** 欄位中，選擇 **[實體機器]**。
5. 按一下齒輪圖示，然後啟用 **[使用手動模式]** 開關。
6. [選用] 將 **[備份大小]** 值除以您網際網路速度的值，以計算容錯回復程序期間的預估停機期間。

   注意事項
   當您同時執行數個容錯回復程序時，網際網路速度的值將會減少。

7. 按一下 **[轉換]**，然後在確認視窗中，再按一下 **[轉換]**。
   雲端站台上的虛擬機器隨即關閉。

   注意事項
   如果雲端虛擬機器上未套用任何備份計劃，將會在轉換階段期間自動執行備份，從而導致停機時間較長。

8. 將伺服器從雲端備份復原到本機站台上的實體或虛擬機器。如需詳細資訊，請參閱《Cyber Protection 使用指南》中的「復原機器」。
9. 確認復原已完成且復原的電腦正常運作，然後按一下 **[電腦已還原]**。
10. 如果一切如預期般運作，按一下 **[確認容錯回復]**，然後在確認視窗中，再按一下 **[確認]**。
    復原伺服器和復原點會變成準備就緒供下次容錯移轉之用。若要建立新的復原點，請將保護計劃套用到新的本機伺服器。

注意事項
在復原的伺服器上套用保護計劃不是容錯回復程序的一部分。在容錯回復程序完成之後，在復原的伺服器上套用保護計劃以確保其再次受到保護。您可以套用在原始伺服器上套用的相同保護計劃，也可以套用已啟用 **[災難復原]** 模組的新保護計劃。

編排 (Runbook)

注意事項
部分功能可能需要額外的授權，端視適用的授權模型而定。

Runbook 是一組指令，用來描述如何在雲端啟動實際執行環境。您可以在 Cyber Protect 主控台中建立 Runbook。

透過 Runbook，您可以：

- 自動容錯移轉一或多部伺服器。
- Ping 伺服器 IP 位址並檢查您指定之連接埠的連線，以便自動檢查容錯移轉結果。
- 針對執行分散式應用程式的伺服器，設定操作順序。
- 在工作流程中包含手動作業。
- 在測試模式下執行 Runbook，以確認災難復原解決方案的完整性。

若要存取 **[Runbook]** 畫面，請選擇 **[災難復原]** > **[Runbook]**。

建立 Runbook

Runbook 包含連續執行的步驟。步驟則包含同時開始的動作。

若要建立 Runbook，請依照下列程序或影片教學課程中的指示進行。

若要建立 Runbook

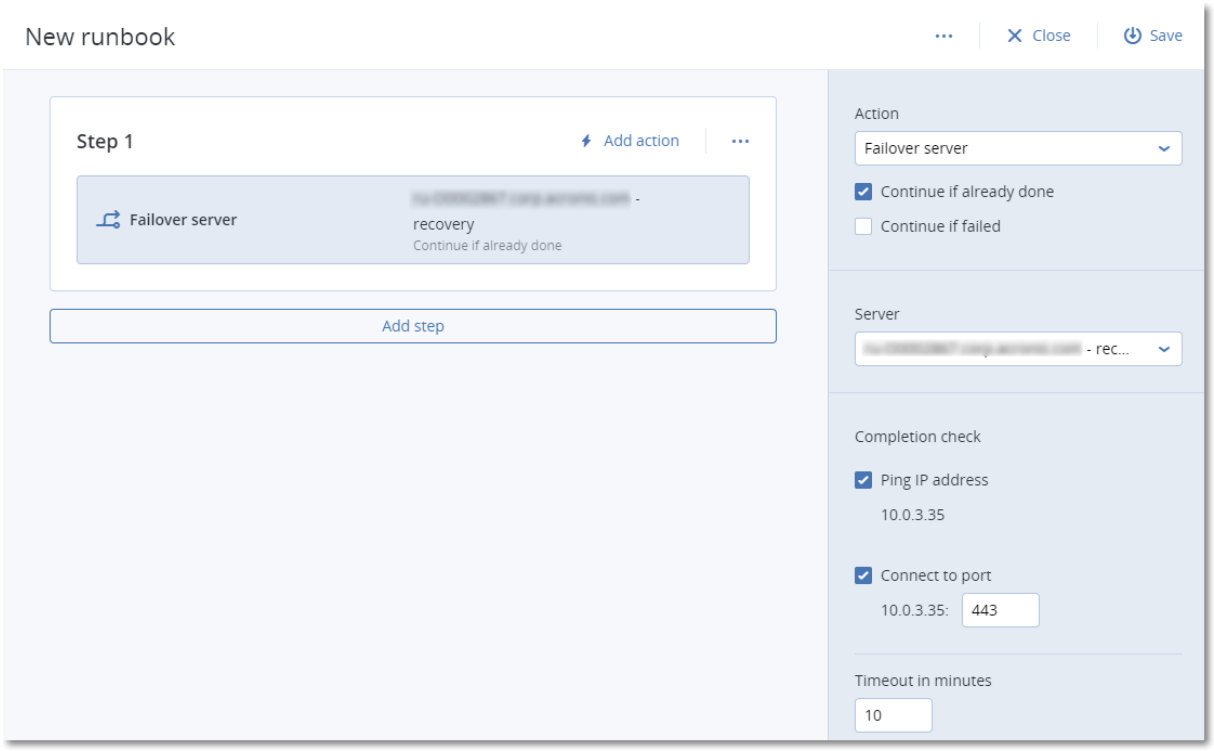
1. 在 Cyber Protection 主控台中，移至 **[災難復原]** > **[Runbook]**。
2. 按一下 **[建立 Runbook]**。
3. 按一下 **[新增步驟]**。
4. 按一下 **[新增動作]**，然後選擇您想要新增到步驟中的動作。

動作	描述
容錯移轉伺服器	執行雲端伺服器的容錯移轉。若要定義此動作，您必須選擇一部雲端伺服器，並

動作	描述
	設定可用於此動作的 Rrunbook 參數。如需有關這些參數的詳細資訊，請參閱 "Runbook 參數" (第 725 頁)。 **注意事項** 如果您選擇的伺服器備份是使用加密作為機器屬性加密的，則 **[容錯移轉伺服器]** 動作將會遭到暫停，而且將自動變更為 **[需要互動]**。若要繼續執行 Runbook，您必須提供加密備份的密碼。
容錯回復伺服器	執行雲端伺服器的容錯回復。若要定義此動作，您必須選擇一部雲端伺服器，並設定可用於此動作的 Rrunbook 參數。如需有關這些設定的詳細資訊，請參閱 "Runbook 參數" (第 725 頁)。 **注意事項** Runbook 作業僅支援手動模式下的容錯回復。也就是說，如果您透過執行包含**容錯回復伺服器**步驟的 Runbook 來開始容錯回復程序，此程序將需要手動互動：您必須手動復原機器，並從 **[災難復原]** > **[伺服器]** 索引標籤確認或取消容錯回復程序。
啟動伺服器	啟動雲端伺服器。若要定義此動作，您必須選擇一部雲端伺服器，並設定可用於此動作的 Rrunbook 參數。如需有關這些設定的詳細資訊，請參閱 "Runbook 參數" (第 725 頁)。 **注意事項** **[啟動伺服器]** 動作不適用於 Runbook 中的測試容錯移轉作業。如果您嘗試執行此類動作，將會出現以下的錯誤訊息： 失敗：此動作不適用於目前的伺服器狀態。
停止伺服器	停止雲端伺服器。若要定義此動作，您必須選擇一部雲端伺服器，並設定可用於此動作的 Rrunbook 參數。如需有關這些設定的詳細資訊，請參閱 "Runbook 參數" (第 725 頁)。 **注意事項** **[停止伺服器]** 動作不適用於 Runbook 中的測試容錯移轉作業。如果您嘗試執行此類動作，將會出現以下的錯誤訊息： 失敗：此動作不適用於目前的伺服器狀態。
手動作業	手動作業需要使用者的互動。若要定義此動作，您必須輸入描述。 當 Runbook 順序達到手動作業時，該 Runbook 將會遭到暫停，而且在使用者執行所需的手動作業 (例如，按一下確認按鈕) 之前不會繼續執行。
執行 Runbook	執行另一個 Runbook。若要定義此動作，您必須選擇一個 Runbook。 一個 Runbook 僅能包含一個指定 Runbook 的執行。例如，如果您新增「執行 Runbook A」動作，您可以新增「執行 Runbook B」動作，但無法新增另一個「執行 Runbook A」動作。

5. 為動作定義 Runbook 參數。如需有關這些參數的詳細資訊，請參閱 "Runbook 參數" (第 725 頁)。

6. [選用] 若要新增步驟的描述：
   a. 按一下省略符號圖示，然後按一下 **[描述]**。
   b. 輸入步驟的描述。
   c. 按一下**[完成]**。
7. 重複步驟 3-6，直到您建立所需的步驟和動作順序為止。
8. [選用] 若要變更 Runbook 的預設名稱：
   a. 按一下省略符號圖示。
   b. 輸入 Runbook 的名稱。
   c. 輸入 Runbook 的描述。
   d. 按一下**[完成]**。
9. 按一下 **[儲存]**。
10. 按一下**[關閉]**。



Runbook 參數

Runbook 參數是您必須設定，才能定義 Runbook 動作的特定設定。Runbook 參數有兩種類型：動作參數和完成檢查參數。

動作參數會根據動作的初始狀態或結果，定義 Runbook 行為。

完成檢查參數可確保伺服器可供使用，並提供所需的服務。如果完成檢查失敗，則會將該動作視為失敗。

下表描述每個動作可設定的 Runbook 參數。

Runbook 參數	類別	可用於動作	描述
完成時繼續	動作參數	• **容錯移轉伺服器** • **啟動伺服器** • **停止伺服器** • **容錯回復伺服器**	此參數會定義所需動作已經完成時的 Runbook 行為 (例如，已經執行容錯移轉或伺服器已經在執行)。啟用時，Runbook 會發出警告並繼續。停用時，動作和 Runbook 都將失敗。 根據預設，此參數為啟用狀態。
失敗時繼續	動作參數	• **容錯移轉伺服器** • **啟動伺服器** • **停止伺服器** • **容錯回復伺服器**	此參數會定義所需動作失敗時的 Runbook 行為。啟用時，Runbook 會發出警告並繼續。停用時，動作和 Runbook 都將失敗。 根據預設，此參數為停用狀態。
Ping IP 位址	完成檢查	• **啟動伺服器**	此軟體將會 Ping 雲端伺服器的實際運作 IP 位址，直到伺服器回覆或逾時到期為止 (以先到者為準)。
連線到連接埠 (預設為 443)	完成檢查	• **容錯移轉伺服器** • **啟動伺服器**	此軟體將會嘗試使用其實際運作 IP 位址和您指定的連接埠，連線至雲端伺服器，直到建立連線或逾時到期為止 (以先到者為準)。如此一來，您就可以確認接聽指定之連接埠的應用程式是否正在執行。
逾時 (分鐘)	完成檢查	• **容錯移轉伺服器** • **啟動伺服器**	預設逾時為 10 分鐘。

Runbook 的相關作業

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

若要存取作業清單，請將滑鼠暫留在 Runbook 上，然後按一下省略符號圖示。當 Runbook 沒有在執行時，可以使用下列作業：

- **執行**
- **編輯**
- **複製**
- **刪除**

執行 Runbook

每次按一下 **[執行]** 時，都會收到執行參數的提示。這些參數適用於 Runbook 中包含的所有容錯移轉和容錯回復作業。在 **[執行 Runbook]** 作業中指定的 Runbook 會從主要 Runbook 繼承這些參數。

- **容錯移轉和容錯回復模式**

  選擇您要執行測試容錯移轉 (預設) 還是實際 (實際運作) 容錯移轉。容錯回復模式將對應到選擇的容錯移轉模式。
- **容錯移轉復原點**

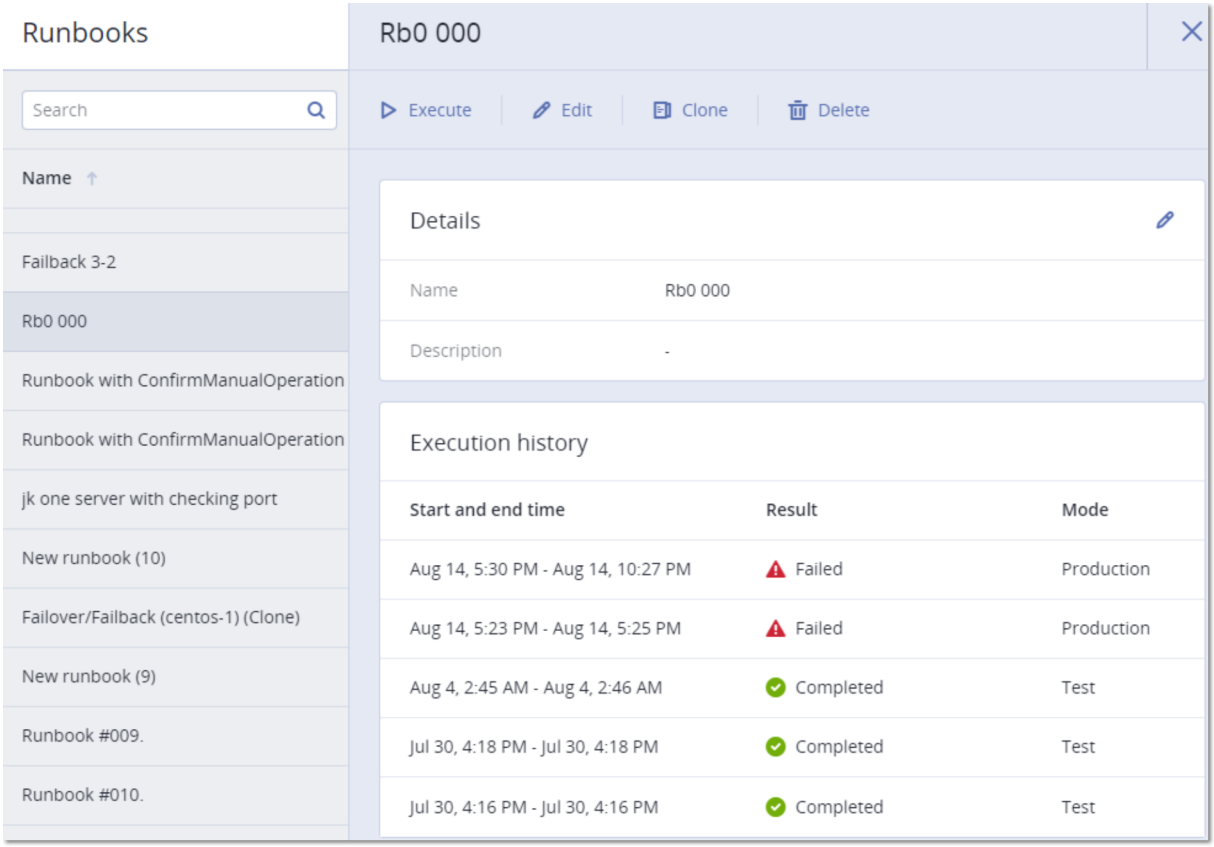
  選擇最近的復原點 (預設) 或選取過去的時間點。如果是後者，將會為每部伺服器選取最接近指定之日期和時間前的復原點。

停止 Runbook 執行

在 Runbook 執行期間，您可以選取作業清單中的 **[停止]**。此軟體將會完成所有已經開始的動作，但需要使用者互動的動作除外。

檢視執行歷程記錄

在 **[Runbook]** 索引標籤上選取 Runbook 時，此軟體會顯示 Runbook 詳細資料以及執行歷程記錄。按一下對應到特定執行的行可檢視執行記錄。



移除災難復原網站

您可以移除災難復原網站。此動作將會自動刪除 VPN 閘道、VPN 連線以及在網站上設定的所有 Runbook。

必要條件

災難復原網站上沒有可用的雲端伺服器。

若要移除災難復原網站

1. 在 Cyber Protect 主控台中，移至 **[災難復原]** > **[連線]**。
2. 按一下 **[顯示屬性]**。
3. 按一下 **[移除災難復原網站]**。
4. 在確認視窗中，按一下 **[移除]**。

設定防毒和防惡意程式保護

注意事項
在 Windows 電腦上，防惡意軟體防護功能需要安裝防惡意軟體防護用代理程式，URL 篩選功能則需要安裝 URL 篩選用代理程式。如果在其保護計劃中啟用 **[防毒和防惡意軟體防護]** 和/或 **[URL 篩選]** 模組，則會自動為受保護的工作負載安裝這些代理程式。

Cyber Protection 中的反惡意程式碼保護可為您提供下列優點：

- 所有階段的頂級保護：預防性、主動性和反應性。
- 內部的四種不同反惡意程式碼技術可提供同類最佳的多層保護。
- Microsoft Security Essentials 和 Microsoft Defender 防毒軟體的管理。

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

重要事項
只有在保護計劃中啟用 **[進階反惡意程式碼]** 選項時，才會偵測到 EICAR 測試檔案。但是，偵測不到 EICAR 檔案也不會影響 Cyber Protection 的反惡意程式碼功能。

支援防毒和防惡意軟體防護的作業系統

下列平台支援 Active Protection、防毒和防惡意軟體功能。

作業系統	版本/發行版本
Windows	Windows 7 Service Pack 1 和更新版本 Windows Server 2008 R2 Service Pack 1 和更新版本 **注意事項** 若是 Windows 7，您必須先安裝以下 Microsoft 更新，然後再安裝保護代理程式。 • Windows 7 Extended Security Updates (ESU) • KB4474419 • KB4490628 有關所需更新的詳細資訊，請參閱本知識庫文章。
Linux	Red Hat Linux 7.x, 8.x, 9.x CloudLinux 6.10, 7.x, 8.x CentOS 6.5 和更新的 6.x、7.x、8.x 版本 Ubuntu 16.04, 18.04, 20.04, 22.04, 22.10 Debian 8.x, 9.x, 10,x, 11.x

作業系統	版本/發行版本
	Oracle Linux 7.x, 8.x, 9.x SUSE Enterprise Linux 15.x openSUSE Leap 15.x
macOS	macOS 10.13.x 及更新版本

每個平台支援的功能

注意事項

進階防惡意軟體套件提供適用於 Linux 和 macOS 的防惡意軟體防護。

功能集	Windows	Linux	macOS
防毒和反惡意程式碼保護			
完全整合的 Active Protection 功能	是	否	否
即時反惡意軟體防護	是	是，含進階防惡意軟體套件	是，含進階防惡意軟體套件
包含本機特徵比對偵測的進階即時反惡意程式碼保護	是	是	是
針對可攜式可執行檔進行靜態分析	是	否	是*
按需反惡意程式碼掃描	是	是**	是
網路資料夾保護	是	是	否
伺服器端保護	是	否	否
掃描存檔檔案	是	否	是
掃描卸除式磁碟機	是	否	是
僅掃描新的和已變更的檔案	是	否	是
檔案/資料夾排除	是	是	是***
程序排除	是	否	是
行為分析引擎	是	否	是
漏洞利用防禦	是	否	否
隔離	是	是	是

功能集	Windows	Linux	macOS
防毒和反惡意程式碼保護			
隔離區自動清理	是	是	是
URL 篩選 (http/https)	是	否	否
全公司的白名單	是	否	是
防火牆管理****	是	否	否
Microsoft Defender 防毒軟體管理*****	是	否	否
Microsoft Security Essentials 管理	是	否	否
透過 Windows Security Center 註冊並管理防毒和反惡意程式碼保護	是	否	否
如需有關支援的作業系統及其版本的詳細資訊，請參閱 "支援防毒和防惡意軟體防護的作業系統" (第 729 頁)。			

* 只有在 macOS 上的排程掃描才支援針對可攜式可執行檔進行靜態分析。

** Linux 上的按需掃描不支援開始條件。

*** 只有在 macOS 上指定即時保護或排程掃描將不會掃描的檔案和資料夾時，才支援檔案/資料夾排除。

**** Windows 8 和更新版本支援防火牆管理。不支援 Windows Server。

***** Windows 8.1 和更新版本支援 Microsoft Defender 防毒軟體管理。

功能集	Windows	Linux	macOS
Active Protection			
程序插入偵測	是	否	否
從本機快取自動復原受影響的檔案	是	是	是
Acronis 備份檔案的自我防衛	是	否	否
Acronis 軟體的自我防衛	是	否	是 (僅限 Active Protection 和防惡意程式碼元件)
受信任/遭到封鎖的程序管理	是	否	是
程序/資料夾排除	是	是	是

功能集	Windows	Linux	macOS
Active Protection			
根據程序行為 (基於 AI) 進行勒索軟體偵測	是	是	是
根據程序行為進行加密採礦程序偵測	是	否	否
外接磁碟機保護 (HDD、快閃磁碟機、SD 卡)	是	否	是
網路資料夾保護	是	是	是
伺服器端保護	是	否	否
Zoom、Cisco Webex、Citrix Workspace 和 Microsoft Teams 保護	是	否	否
如需有關支援的作業系統及其版本的詳細資訊，請參閱 "支援防毒和防惡意軟體防護的作業系統" (第 729 頁)。			

防毒和防惡意程式保護

注意事項
部分功能可能需要額外的授權，端視適用的授權模型而定。

[防毒和防惡意程式保護] 模組可保護您的 Windows、Linux 和 macOS 電腦，免受所有最近的惡意程式碼威脅的影響。查看 "支援防毒和防惡意軟體防護的作業系統" (第 729 頁) 中支援之防惡意軟體功能的完整清單。

Windows Security Center 支援並登錄防毒和防惡意程式保護。

反惡意程式碼功能

- 在即時保護和按需模式下偵測檔案中的惡意程式碼
- 偵測處理程序中的惡意行為 (適用於 Windows)
- 封鎖對惡意 URL 的存取 (適用於 Windows)
- 將危險的檔案置入隔離區
- 將受信任的公司應用程式新增到允許名單中

掃描類型

您可以將防毒和防惡意程式保護設定為持續在背景執行或視需要執行。

即時保護

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

即時保護會檢查正在電腦上執行或開啟的所有檔案，以防止惡意程式碼威脅。

為防止潛在的相容性和效能問題，即時保護無法與也使用即時保護功能的其他防毒解決方案同時執行。其他已安裝的防毒解決方案的狀態是透過 Windows Security Center 判斷的。如果 Windows 電腦已受到其他防毒解決方案的保護，就會自動關閉即時保護。

若要啟用即時保護，請停用或解除安裝其他防毒解決方案。即時保護可以自動取代 Microsoft Defender 即時保護。

注意事項
在執行 Windows Server 作業系統的電腦上啟用即時保護時，將不會自動關閉 Microsoft Defender。系統管理員必須手動關閉 Microsoft Defender 以避免潛在的相容性問題。

您可以選擇以下其中一個掃描模式：

- **智慧型主動即時掃描**偵測是指反惡意程式碼程式在背景執行，並在系統開機的整個持續時間內，主動且不斷地掃描電腦系統中是否有病毒和其他惡意威脅。當檔案正在執行時，以及檔案的各種操作 (例如，開啟檔案以供讀取或編輯) 期間，系統將會偵測惡意程式碼。
- **執行時**偵測是指只有在可執行檔執行時才會進行掃描，以確保可執行檔未受感染，而且將不會對電腦或資料造成任何損害。複製受感染的檔案將不會引起注意。

排程掃描

反惡意程式碼掃描是根據排程執行的。

您可以選擇以下其中一個掃描模式。

- **快速掃描**—僅檢查工作負載系統檔案。
- **完整掃描**—檢查工作負載上的所有檔案。
- **自訂掃描**—檢查系統管理員新增至保護計劃的檔案/資料夾。

防惡意程式碼掃描完成之後，您可以在 **[監控]** > **[概觀]** > [最近受影響] 桌面小工具中查看受威脅影響的工作負載的詳細資料。

防毒和防惡意程式保護設定

本節描述您可以在保護計劃中的 **[防毒和防惡意軟體防護]** 模組中設定的功能。若要瞭解如何建立保護計劃，請參閱 "建立保護計劃" (第 192 頁)。

您可以在保護計劃的 [防毒和防惡意軟體防護] 模組中設定下列功能：

- "Active Protection" (第 734 頁)
- "進階反惡意程式碼" (第 734 頁)
- "網路資料夾保護" (第 735 頁)
- "伺服器端保護" (第 735 頁)
- "自我保護" (第 736 頁)
- "加密採礦程序偵測" (第 737 頁)
- "隔離設定" (第 737 頁)

- "行為引擎" (第 738 頁)
- "漏洞利用防禦" (第 738 頁)
- "即時保護" (第 740 頁)
- "排程掃描" (第 741 頁)
- "保護排除項目" (第 743 頁)

注意事項
並非所有作業系統都支援防毒和防惡意軟體防護功能。如需有關支援的作業系統和功能的詳細資訊，請參閱 "支援防毒和防惡意軟體防護的作業系統" (第 729 頁)。部分功能需要特定授權才能在您的保護計劃中使用。

Active Protection

Active Protection 可保護系統免受被稱為勒索軟體的惡意軟體入侵，此類軟體會將檔案加密，並要求贖金才會提供加密金鑰。

預設設定：**[啟用]**。

注意事項
保護代理程式必須安裝在受保護的電腦上。如需有關支援的作業系統及功能的詳細資訊，請參閱 "支援防毒和防惡意軟體防護的作業系統" (第 729 頁)。

若要設定 Active Protection

1. 在 **[建立保護計劃]** 視窗中，展開 **[防毒和防惡意軟體防護]** 模組。
2. 按一下 **[Active Protection]**。
3. 在 **[與偵測相關的動作]** 區段中，選擇其中一個可用的選項：
   預設設定：**使用快取還原**
   - **僅通知** — 軟體會針對懷疑有勒索軟體活動的程序產生警示。
   - **停止程序** — 軟體產生警示並停止懷疑有勒索軟體活動的程序。
   - **使用快取還原** — 軟體會產生警示、停止程序，並使用服務快取來還原檔案變更。
4. 按一下 **[完成]**，將所選選項套用至保護計劃。

進階反惡意程式碼

此引擎使用增強的病毒特徵資料庫提高快速掃描和完整掃描的防惡意軟體偵測效率。

重要事項
此作業只有在您已啟用 Advanced Security 保護套件時才可以使用。如需詳細資訊，請參閱 https://www.acronis.com/en-us/products/cloud/cyber-protect/security/

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

若要設定進階防惡意軟體

1. 在 **[建立保護計劃]** 視窗中，展開 **[防毒和防惡意軟體防護]** 模組。
2. 在 **[進階反惡意程式碼]** 區段中，使用切換啟用本機特徵比對引擎。

注意事項
macOS 與 Linux 用防毒和防惡意程式保護也需要使用本機特徵比對引擎。對於 Windows，防毒和防惡意程式保護則不一定要搭配此引擎使用。

網路資料夾保護

[網路資料夾保護] 功能會定義防毒和防惡意軟體防護是否會保護對應為本機磁碟機的網路資料夾。此保護適用於透過 SMB 或 NFS 通訊協定共用的資料夾。

若要設定網路資料夾保護

1. 在 **[建立保護計劃]** 視窗中，展開 **[防毒和防惡意軟體防護]** 模組。
2. 按一下 **[網路資料夾保護]**。
3. 新增您要備份網路資料夾所在位置的檔案：
   - 例如，如果您的工作負載為 Windows，請在 **[Windows]** 欄位中，輸入您要備份網路資料夾所在 Windows 檔案的路徑。預設值：C:\ProgramData\Acronis\Restored Network Files。
   - 例如，如果您的工作負載為 macOS，請在 **[macOS]** 欄位中，輸入您要備份網路資料夾所在 macOS 檔案的路徑。預設值：/Library/Application Support/Acronis/Restored Network Files/。

   注意事項
   輸入本機資料夾的路徑。不支援網路資料夾 (包括對應磁碟機的資料夾) 作為網路資料夾的備份目的地。
4. 按一下 **[完成]**，將所選選項套用至保護計劃。

伺服器端保護

此功能會定義 Active Protection 是否會保護您從外部傳入連線共用的網路資料夾，免受網路中可能帶來威脅的其他伺服器的攻擊。

預設設定：**關閉**。

注意事項
Linux 不支援伺服器端保護。

若要設定受信任的連線

1. 在 **[建立保護計劃]** 視窗中，展開 **[防毒和防惡意軟體防護]** 模組。
2. 按一下 **[伺服器端保護]**。
3. 使用 **[伺服器端保護]** 切換啟用它。
4. 選擇 **[受信任]** 索引標籤。
5. 在 **[受信任的連線]** 欄位中，按一下 **[新增]** 以定義將可以修改資料的連線。

6. 在 **[電腦名稱/帳戶]** 欄位中，輸入安裝保護代理程式所在電腦的電腦名稱和帳戶。例如，`MyComputer\TestUser`。
7. 在 **[主機名稱]** 欄位中，輸入可以使用保護代理程式連線至電腦的電腦主機名稱。
8. 按一下右側的核取標記以儲存連線定義。
9. 按一下**[完成]**。

若要設定封鎖的連線

1. 在 **[建立保護計劃]** 視窗中，展開 **[防毒和防惡意軟體防護]** 模組。
2. 按一下 **[伺服器端保護]**。
3. 使用 **[伺服器端保護]** 切換啟用它。
4. 選擇 **[封鎖]** 索引標籤。
5. 在 **[封鎖的連線]** 欄位中，按一下 **[新增]** 以定義將無法修改資料的連線。
6. 在 **[電腦名稱/帳戶]** 欄位中，輸入安裝保護代理程式所在電腦的電腦名稱和帳戶。例如，`MyComputer\TestUser`。
7. 在 **[主機名稱]** 欄位中，輸入可以使用保護代理程式連線至電腦的電腦主機名稱。
8. 選擇右側的核取方塊以儲存連線定義。
9. 按一下**[完成]**。

自我保護

自我保護可防止對軟體自身的程序、登錄檔記錄、可執行檔與組態檔，以及位於本機資料夾的備份進行未經授權的變更。

系統管理員可以在不啟用 **[Active Protection]** 的情況下啟用 **[自我保護]**。

預設設定：**開啟**。

注意事項
Linux 不支援自我保護。

若要啟用自我保護

1. 在 **[建立保護計劃]** 視窗中，展開 **[防毒和防惡意軟體防護]** 模組。
2. 按一下 **[自我保護]**。
3. 使用 **[自我保護]** 切換啟用它。

若要啟用密碼保護

1. 一旦啟用 **[自我保護]** 功能之後，您可以使用切換啟用 **[密碼保護]** 功能。
2. 按一下 **[產生新密碼]** 以產生修改或刪除本機代理程式的密碼。
3. 按一下 **[複製]**，然後將其貼在安全的位置，因為當您想要在本機修改元件清單時，將會要求此密碼。

重要事項
關閉視窗後，密碼將無法使用。若要將此密碼套用至裝置，必須儲存保護計劃設定。

4. 按一下**[關閉]**。

密碼保護可防止未經授權的使用者或軟體解除安裝 Windows 用代理程式或修改其元件。只有使用系統管理員可以提供的密碼才能執行這些動作。

下列動作永遠不需要密碼：

- 在本機執行安裝程式以更新安裝
- 使用 Cyber Protect 主控台更新安裝
- 修復安裝

預設設定：**已停用**

如需有關如何啟用**密碼保護**的詳細資訊，請參閱防止未經授權者解除安裝或修改代理程式。

加密採礦程序偵測

加密採礦惡意軟體會使有用應用程式的效能降低、增加電費，而且可能造成系統當機，甚至因為濫用而導致硬體損壞。**[加密採礦程序偵測]** 功能可保護您的裝置免受加密採礦惡意軟體攻擊，以防止未經許可使用電腦資源。

系統管理員可以在不啟用 **[Active Protection]** 的情況下啟用 **[加密採礦程序偵測]**。預設設定：**[啟用]**。

注意事項
Linux 不支援加密採礦程序偵測。

若要設定網路資料夾保護

1. 在 **[建立保護計劃]** 視窗中，展開 **[防毒和防惡意軟體防護]** 模組。
2. 按一下 **[加密採礦程序偵測]**。
3. 使用 **[偵測加密採礦程序]** 切換啟用或停用此功能。
4. 選擇如何處理懷疑有加密採礦活動的程序：

   預設設定：**停止程序**

   - **僅通知** — 軟體會產生警示。
   - **停止程序** — 軟體會產生警示並停止程序。
5. 按一下 **[完成]**，將所選選項套用至保護計劃。

隔離設定

隔離是一個資料夾，用於隔離可疑 (可能受感染) 或可能危險的檔案。

若要設定隔離

1. 在 **[建立保護計劃]** 視窗中，展開 **[防毒和防惡意軟體防護]** 模組。
2. 按一下 **[隔離]**。
3. 在 **[在下列時間後移除隔離的檔案]** 欄位中，您可以定義將移除隔離的檔案前經過的天數。
   預設設定：**30 天**
4. 按一下**[完成]**。

如需有關此功能的詳細資訊，請參閱隔離。

行為引擎

[行為引擎] 功能使用行為啟發方式找出惡意程序，以保護系統免受惡意軟體攻擊。

預設設定：**[啟用]**。

注意事項
Linux 不支援行為引擎。

若要設定網路資料夾保護

1. 在 **[建立保護計劃]** 視窗中，展開 **[防毒和防惡意軟體防護]** 模組。
2. 按一下 **[行為引擎]**。
3. 使用 **[行為引擎]** 切換啟用或停用此功能。
4. 在 **[與偵測相關的動作]** 區段中，選擇當偵測到惡意軟體活動時，軟體將執行的動作：
   預設設定：**隔離**
   - **僅通知** — 軟體會針對懷疑有惡意軟體活動的程序產生警示。
   - **停止程序** — 軟體會產生警示並停止懷疑有惡意軟體活動的程序。
   - **隔離** — 軟體會產生警示、停止程序，然後將可執行檔移到隔離資料夾。
5. 按一下 **[完成]**，將所選選項套用至保護計劃。

漏洞利用防禦

重要事項
此作業只有在您已啟用 Advanced Security 保護套件時才可以使用。如需詳細資訊，請參閱 https://www.acronis.com/zh-tw/products/cloud/cyber-protect/security/

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

漏洞利用防禦可偵測受感染的程序並防止其散播並利用系統上的軟體弱點。偵測到漏洞利用時，此軟體可以產生警示並停止懷疑有漏洞利用活動的程序。

漏洞利用防禦僅適用於代理程式 12.5.23130 (21.08, 2020 年 8 月發行) 版或更新版本。

預設設定：**啟用**新建立的保護計劃，並**停用**使用舊版代理程式建立的現有保護計劃。

注意事項
Linux 不支援漏洞攻擊防護。

您可以選擇偵測到漏洞利用時，程式要採取的動作，以及程式要套用的漏洞利用防禦方法。

若要設定漏洞利用防禦

1. 在 **[建立保護計劃]** 視窗中，展開 **[防毒和防惡意軟體防護]** 模組。
2. 按一下 **[漏洞利用防禦]**。
3. 在 **[與偵測相關的動作]** 區段中，選擇其中一個可用的選項：
   預設設定：**停止程序**
   - **僅通知**
     軟體將會針對懷疑有漏洞利用活動的程序產生警示。
   - **停止程序**
     軟體將會產生警示並停止懷疑有漏洞利用活動的程序。
4. 在 **[啟用漏洞利用防禦技術]** 區段中，從您要套用的可用選項中選擇：
   預設設定：**已啟用所有方法**
   - **記憶體保護**
     偵測並防止記憶體頁面執行權限的可疑修改。惡意程序會套用對頁面屬性的這類修改，以便從非可執行記憶體區域 (例如堆疊和堆積) 執行 shell 程式碼。
   - **傳回導向程式設計 (ROP) 保護**
     偵測並防止使用 ROP 漏洞技術的嘗試。
   - **權限提升保護**
     偵測並防止未經授權的程式碼或應用程式所進行的權限提升嘗試。惡意程式碼會使用權限提升獲得受攻擊電腦的完整存取權，然後執行重要和敏感的工作。未經授權的程式碼無法存取重要的系統資源或修改系統設定。
   - **程式碼插入保護**
     偵測並防止惡意程式碼插入遠端程序。程式碼插入用於將應用程式的惡意意圖隱藏在未受感染或良性的程序後面，以逃避反惡意程式碼產品的偵測。
5. 按一下 **[完成]**，將所選選項套用至保護計劃。

注意事項
系統將不會掃描 [排除] 清單中列為受信任程序的程序中是否有漏洞利用。

允許程序修改備份

只有在啟用 **[自我保護]** 設定時，才能使用 **[允許特定程序修改備份]** 設定。

此選項適用於副檔名為 .tibx、.tib、.tia，且位於本機資料夾中的檔案。

此設定可讓您指定修改備份檔案的程序，即使這些檔案受到自我保護的保護，也是如此。這很實用，例如，當您使用指令碼移除備份檔案，或將其移至其他位置時。

如果停用此設定，則只有備份軟體廠商簽署的程序可以修改備份檔案。如此可讓軟體套用保留規則，並在使用者從 Web 介面提出要求時，移除備份。其他程序 (無論是否可疑) 都無法修改備份。

如果啟用此設定，您可以允許其他程序修改備份。指定程序執行檔的完整路徑，並以磁碟機代號開頭。

預設設定：**[已停用]**。

即時保護

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

除非電腦使用者暫停，否則**即時保護**會在系統開機期間，持續檢查電腦系統中是否有病毒和其他惡意威脅。

預設設定：**[啟用]**。

重要事項
此作業只有在您已啟用 Advanced Security 保護套件時才可以使用。如需詳細資訊，請參閱 https://www.acronis.com/en-us/products/cloud/cyber-protect/security/

若要設定即時保護

1. 在 **[建立保護計劃]** 視窗中，展開 **[防毒和防惡意軟體防護]** 模組。
2. 按一下 **[即時保護]**。
3. 在 **[與偵測相關的動作]** 下拉式清單中，選擇其中一個可用的選項：
   預設設定：**隔離**
   - **僅通知**
     此軟體會針對懷疑有勒索軟體活動的程序產生警示。
   - **封鎖並通知**
     此軟體將會封鎖程序，並針對懷疑有惡意程式碼活動的程序產生警示。
   - **隔離**
4. 此軟體會產生警示、停止程序，然後將可執行檔移到隔離資料夾。
5. 在 **[掃描模式]** 區段中，選擇當偵測到病毒或其他惡意威脅時，軟體將執行的動作：
   預設設定：**智慧型主動即時掃描**
   - **智慧型主動即時掃描** — 監視所有系統活動，並在存取檔案以供讀取或寫入時，或在啟動程式時，自動掃描這些檔案。
   - **執行時掃描** — 只會在啟動可執行檔時自動掃描，以確保可執行檔未受感染，而且將不會對電腦或資料造成任何損害。
6. 按一下**[完成]**。

排程掃描

按需掃描會根據指定的排程，檢查電腦系統中是否有病毒。完整掃描會檢查電腦上的所有檔案，而快速掃描只會檢查電腦的系統檔案。

若要設定排程掃描

預設設定：

- **[自訂掃描]** 為停用狀態。
- 已排程 **[快速]** 和 **[完整]** 掃描。

1. 在 **[建立保護計劃]** 視窗中，展開 **[防毒和防惡意軟體防護]** 模組。
2. 按一下 **[排程掃描]**。
3. 使用切換啟用您要為電腦套用的掃描類型。

可用的掃描類型：

- **完整** — 相較於快速掃描，所需的時間更長，因為每個檔案都將經過檢查。
- **快速** — 僅掃描電腦上通常會駐留惡意軟體的一般區域。
- **自訂** — 檢查 保護 計劃的系統管理員選擇的檔案/資料夾。

> **注意事項**
> 您可以在一個保護計劃中排程全部三種掃描：**[快速]**、**[完整]** 和 **[自訂]**。

若要設定自訂掃描

- 使用 **[自訂掃描切換]** 啟用或停用此類型的掃描。
- 在 **[與偵測相關的動作]** 下拉式清單中，選擇其中一個可用的選項：

預設設定：**隔離**

隔離

此軟體會產生警示，然後將可執行檔移到隔離資料夾。

僅通知

此軟體會針對懷疑有惡意程式碼的程序產生警示。

欄位	描述
使用下列事件，排程工作執行	此設定會定義執行工作的時間。 您可以選取下列值： • **依時間排程** – 這是預設設定。工作將會根據指定的時間執行。 • **當使用者登入系統時** – 根據預設，任何使用者的登入都將觸發工作。您可以修改此設定，因此只有特定使用者帳戶能夠觸發工作。 • **當使用者登出系統時** – 根據預設，任何使用者的登出都將觸發工作。您可以修改此設定，因此只有特定使用者帳戶能夠觸發工作。

欄位	描述
	注意事項 工作將不會在系統關機時執行。關機和登出在排程設定上是不同的動作。 • **在系統啟動時** – 工作將會在作業系統啟動時執行。 • **在系統關機時** – 工作將會在作業系統關機時執行。
排程類型	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[依時間排程]**，此欄位將會出現。 您可以選取下列值： • **每月** – 選擇執行工作的月份以及該月的週數或日期。 • **每天** – 這是預設設定。選擇工作將在一週的哪幾天執行。 • **每小時** – 選擇工作將在一週的哪幾天執行、重複次數以及時間間隔。
開始時間	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[依時間排程]**，此欄位將會出現 選擇執行工作的明確時間。
在日期範圍內執行	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[依時間排程]**，此欄位將會出現。 設定一個範圍，已設定的排程將在該範圍內生效。
指定使用者帳戶，該帳戶登入作業系統時將啟動工作	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[當使用者登入系統時]**，此欄位將會出現。 您可以選取下列值： • **任何使用者** - 如果您希望任何使用者登入時都能觸發工作，請使用此選項。 • **下列使用者** - 如果您僅希望在特定使用者帳戶登入時觸發工作，請使用此選項。
指定使用者帳戶，該帳戶登出作業系統時將啟動工作	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[當使用者登出系統時]**，此欄位將會出現。 您可以選取下列值： • **任何使用者** - 如果您希望任何使用者登出時都能觸發工作，請使用此選項。 • **下列使用者** - 如果您僅希望在特定使用者帳戶登出時觸發工作，請使用此選項。
開始條件	定義必須同時符合，工作才能執行的所有條件。 防惡意軟體掃描的開始條件與 **[備份]** 模組的開始條件類似，其詳述於「開始條件」中。 您可以定義下列額外的開始條件：

欄位	描述
	• **在時間視窗中分配工作開始時間** – 此選項可讓您設定工作的時間範圍，以避免網路瓶頸。您可以以小時或分鐘，指定延遲時間。例如，如果預設開始時間為上午 10:00，且延遲為 60 分鐘，則工作將會在上午 10:00 到上午 11:00 之間開始。 • **如果電腦關閉，則在電腦啟動時執行遺漏的工作** • **防止在工作執行期間進入睡眠或休眠模式** – 此選項僅適用於執行 Windows 的電腦。 • **如果未符合開始條件，請無論如何在此時間後執行工作** – 指定無論開始條件為何，將會在其後執行工作的時段。 **注意事項** Linux 不支援開始條件。

- 如果您僅要掃描新建立和修改的檔案，請選擇 **[僅掃描新的和變更的檔案]** 核取方塊。

預設設定：**啟用**

- 僅針對 **[自訂掃描]** 和 **[完整掃描]** 顯示的兩個額外選項：

1. **掃描存檔檔案**

   預設設定：**[啟用]**。

   遞迴深度上限

   預設設定：**16**

   可以掃描多少層級的嵌入式存檔。例如，MIME 文件 > ZIP 存檔 > Office 存檔 > 文件內容。

   大小上限

   預設設定：**100**

   要掃描之存檔檔案的大小上限。

2. **掃描卸除式磁碟機**

預設設定：**已停用**

- **對應的 (遠端) 網路磁碟機**
- **USB 儲存裝置** (例如，隨身碟和外接式硬碟)
- **CD/DVD**

注意事項
Linux 不支援掃描卸除式磁碟機。

保護排除項目

保護排除項目可讓您在受信任的程式被視為勒索軟體或惡意軟體時消除誤報。若要定義信任項目和封鎖項目，您可以將其新增至保護排除項目清單。

在信任項目清單中，您可以新增檔案、程序和資料夾，以便將其視為系統中的安全項目，並防止之後偵測到這些內容。

在封鎖項目清單中，您可以新增程序和雜湊。此選項可保證這些程序將會遭到封鎖，而且您的工作負載將安全無虞。

保護排除項目	已封鎖	受信任
雜湊	當雜湊新增到封鎖項目清單時，系統將會根據提供的雜湊，停止程序。 例如，當您新增這個 MD5 雜湊 (938c2cc0dcc05f2b68c4287040cfcf71) 時，與此雜湊相關聯的程序將會遭到封鎖。	當雜湊新增到信任項目清單時，系統將會根據提供的雜湊，知道必須透過監控略過的程序。 例如，當您新增這個 MD5 雜湊 (938c2cc0dcc05f2b68c4287040cfcf71) 時，與此雜湊相關聯的程序將會受到信任並從監控中排除。
程序	當程序新增到封鎖項目清單時，系統將會知道必須監控這些程序，因此這些程序一律會遭到封鎖。 例如，如果您將此路徑 C:\Users\user1\application\nppInstaller.exe 新增到封鎖項目清單中，這個特定程序將會遭到封鎖，因此當您嘗試開啟該程序時，將無法啟動它。	當程序新增到信任項目清單時，系統將會知道這些程序必須從監控中排除。 **注意事項** 由 Microsoft 簽署的程序一律受到信任。 例如，如果您新增此路徑 C:\Users\user1\application\nppInstaller.exe，這個特定程序將會從監控中排除，因此防毒軟體將不會干擾此程序。
檔案/資料夾		當檔案或資料夾新增到信任項目清單時，系統將會知道這些檔案或資料夾應該一律被視為安全無虞，因此不需要掃描/監控它們。

若要指定將一律受到信任的項目

1. 開啟保護計劃。
2. 展開 **[防毒和反惡意程式碼保護]** 模組。
3. 選擇 **[排除項目]** 選項。
   [保護排除項目] 視窗隨即開啟。
4. 在 **[信任項目]** 區段中，按一下 **[新增]** 可從可用選項中選擇：
   - 若要信任檔案、資料夾或程序，選擇 **[檔案/資料夾/程序]** 選項。**[新增檔案/資料夾/程序]** 視窗隨即開啟。

- 在 **[檔案/資料夾/程序]** 欄位中新的一行上，輸入每個程序、資料夾或檔案的路徑。在 **[描述]** 區段中輸入簡短描述，讓您可以在信任項目清單中辨識您的變更。
- 選擇 **[新增為檔案/資料夾]** 核取方塊以信任檔案/資料夾。
  資料夾描述的範例：D:\folder\、/home/Folder/folder2、F:\
- 選擇 **[新增為程序]** 核取方塊以信任程序。所選程序將從監控中排除。

注意事項
指定程序執行檔的完整路徑，並以磁碟機代號開頭。例如，
`C:\Windows\Temp\er76s7sdkh.exe`。

注意事項
支援區域網路路徑，例如：\\localhost\folderpath\file.exe

- 選擇 **[雜湊]** 選項可將 MD5 雜湊新增至信任項目清單中。**[新增雜湊]** 視窗隨即開啟。
  - 在此，您可以在個別行上插入 MD5 雜湊，以便納入為 [保護排除項目] 清單中的受信任項目。根據這些雜湊，Cyber Protection 將排除 MD5 雜湊所述的程序，使其不受監控。

預設設定：預設沒有定義任何排除項目。

若要指定將一律遭到封鎖的項目

1. 開啟保護計劃。
2. 展開 **[防毒和防惡意程式保護]** 模組。
3. 選擇 **[保護排除項目]** 選項。**[保護排除項目]** 視窗隨即開啟。

   在 **[封鎖項目]** 區段中，按一下 **[新增]** 可從可用選項中選擇：
- 若要封鎖程序，選擇 **[程序]** 選項。**[新增程序]** 視窗隨即開啟。
  - 在 **[程序]** 欄位中新的一行上，輸入每個程序的路徑。在 **[描述]** 欄位中輸入簡短描述，讓您可以在封鎖項目清單中辨識您的變更。

注意事項
只要在電腦上啟用了 Active Protection，這些程式就無法啟動。

- 若要封鎖雜湊，選擇 **[雜湊]** 選項。**[新增雜湊]** 視窗隨即顯示。
  - 在 **[雜湊]** 欄位中新的一行上，輸入每個程序的雜湊。在 **[描述]** 欄位中輸入簡短描述，讓您可以在封鎖項目清單中辨識您的變更。

預設設定：預設沒有定義任何排除項目。

萬用字元

指定資料夾時，您可以使用萬用字元 * 與 ?。星號 (*) 可代替零個或多個字元。問號 (?)可代替一個字元。無法使用環境變數，例如 `%AppData%`。

您可以使用萬用字元 (*)，將項目新增到排除清單。

- 萬用字元可以用於描述中間或結尾。

描述中接受的萬用字元範例：

C:*.pdf

D:\folders\file.*

C:\Users*\AppData\Roaming

- 萬用字元無法用於描述開頭。

描述中不接受的萬用字元範例：

*.docx

*:\folder\

變數

您也可以使用變數，將項目新增到 [保護排除項目] 清單，但限制如下：

- 若是 Windows，僅支援 SYSTEM 變數。不支援使用者專用的變數 (例如 %USERNAME%、%APPDATA%)。不支援包含 {username} 的變數。如需詳細資訊，請參閱 https://ss64.com/nt/syntax-variables.html。
- 若是 macOS，不支援環境變數。
- 若是 Linux，不支援環境變數。

支援的格式的範例：

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

描述

您可以使用 **[描述]** 欄位，記下您在 [保護排除項目] 清單中新增的排除項目。您可以記下的一些內容建議：

- 排除的原因和目的。
- 雜湊排除項目的實際檔案名稱。
- 時間戳記。

如果在單一項目中新增了多個項目，則只能針對多個項目擷取 1 個註解。

Cyber Backup Standard 版本中的 Active Protection

在 Cyber Backup Standard 版本中，Active Protection 是保護計劃中的獨立模組。因此其可以單獨設定，並套用至不同的裝置或裝置群組。

在其他所有版本的資安防護服務中，Active Protection 是保護計劃的 **[防毒和防惡意軟體]** 模組的一部分。

預設設定：**[啟用]**。

注意事項
保護代理程式必須安裝在受保護的電腦上。如需有關支援的作業系統及功能的詳細資訊，請參閱 "支援防毒和防惡意軟體防護的作業系統" (第 729 頁)。

運作原理

Active Protection 會在受保護的機器上監控所執行的程式。當第三方程序嘗試加密檔案或進行加密貨幣採礦時，Active Protection 會產生警示，並執行額外的動作，如保護計劃中所指定。

此外，Active Protection 可避免對備份軟體自身的程序、登錄檔記錄、可執行檔與組態檔案，以及位於本機資料夾的備份進行未經授權的變更。

Active Protection 採用行為判別方式來識別惡意程序。Active Protection 將程序執行的動作鏈與惡意行為模式資料庫中記錄的事件鏈進行比較。此方法可讓 Active Protection 透過新惡意軟體的一般行為來進行偵測。

Cyber Backup Standard 中的 Active Protection 設定

在 Cyber Backup Standard 版本中，您可以設定下列 Active Protection 功能：

- 與偵測相關的動作
- 自我保護
- 網路資料夾保護
- 伺服器端保護
- 加密採礦程序偵測
- 排除

注意事項
Linux 用 Active Protection 支援以下設定：偵測到時採取的動作、網路資料夾保護，以及排除項目。網路資料夾保護一律處於開啟狀態，而且無法設定。

與偵測相關的動作

在 **[與偵測相關的動作]** 區段中，選擇其中一個可用的選項：

- **僅通知**
  此軟體將會針對懷疑有勒索軟體活動的程序產生警示。
- **停止程序**
  此軟體將會產生警示並停止懷疑有勒索軟體活動的程序。
- **使用快取還原**
  軟體將產生警示、停止程序，並使用服務快取來回復檔案變更。

預設設定：**使用快取還原**。

自我保護可防止對軟體自身的程序、登錄檔記錄、可執行檔與組態檔，以及位於本機資料夾的備份進行未經授權的變更。

系統管理員可以在不啟用 **[Active Protection]** 的情況下啟用 **[自我保護]**。

預設設定：**開啟**。

注意事項
Linux 不支援自我保護。

若要啟用自我保護

1. 在 **[建立保護計劃]** 視窗中，展開 **[防毒和防惡意軟體防護]** 模組。
2. 按一下 **[自我保護]**。
3. 使用 **[自我保護]** 切換啟用它。

若要啟用密碼保護

1. 一旦啟用 **[自我保護]** 功能之後，您可以使用切換啟用 **[密碼保護]** 功能。
2. 按一下 **[產生新密碼]** 以產生修改或刪除本機代理程式的密碼。
3. 按一下 **[複製]**，然後將其貼在安全的位置，因為當您想要在本機修改元件清單時，將會要求此密碼。

   重要事項
   關閉視窗後，密碼將無法使用。若要將此密碼套用至裝置，必須儲存保護計劃設定。

4. 按一下**[關閉]**。

密碼保護可防止未經授權的使用者或軟體解除安裝 Windows 用代理程式或修改其元件。只有使用系統管理員可以提供的密碼才能執行這些動作。

下列動作永遠不需要密碼：

- 在本機執行安裝程式以更新安裝
- 使用 Cyber Protect 主控台更新安裝
- 修復安裝

預設設定：**已停用**

如需有關如何啟用**密碼保護**的詳細資訊，請參閱防止未經授權者解除安裝或修改代理程式。

網路資料夾保護

[保護對應為本機磁碟機的網路資料夾] 設定會定義 Active Protection 是否會保護對應為本機磁碟機的網路資料夾免受本機惡意程序攻擊。

此設定適用於透過 SMB 或 NFS 通訊協定共用的資料夾。

如果檔案原本位於對應的磁碟機，則當 **[使用快取還原]** 動作從快取擷取該檔案時，無法儲存到原始位置。但是會儲存到此設定中指定的資料夾。Windows 的預設資料夾是 `C:\ProgramData\Acronis\Restored Network Files`，以及 macOS 的 `Library/Application Support/Acronis/Restored Network Files/`。如果此資料夾不存在，將建立此資料夾。如果您要變更此路徑，請指定本機資料夾。不支援網路資料夾，包括對應磁碟機的資料夾。

預設設定：**開啟**。

此功能會定義 Active Protection 是否會保護您從外部傳入連線共用的網路資料夾，免受網路中可能帶來威脅的其他伺服器的攻擊。

預設設定：**關閉**。

注意事項
Linux 不支援伺服器端保護。

若要設定受信任的連線

1. 在 **[建立保護計劃]** 視窗中，展開 **[防毒和防惡意軟體防護]** 模組。
2. 按一下 **[伺服器端保護]**。
3. 使用 **[伺服器端保護]** 切換啟用它。
4. 選擇 **[受信任]** 索引標籤。
5. 在 **[受信任的連線]** 欄位中，按一下 **[新增]** 以定義將可以修改資料的連線。
6. 在 **[電腦名稱/帳戶]** 欄位中，輸入安裝保護代理程式所在電腦的電腦名稱和帳戶。例如，`MyComputer\TestUser`。
7. 在 **[主機名稱]** 欄位中，輸入可以使用保護代理程式連線至電腦的電腦主機名稱。
8. 按一下右側的核取標記以儲存連線定義。
9. 按一下**[完成]**。

若要設定封鎖的連線

1. 在 **[建立保護計劃]** 視窗中，展開 **[防毒和防惡意軟體防護]** 模組。
2. 按一下 **[伺服器端保護]**。
3. 使用 **[伺服器端保護]** 切換啟用它。
4. 選擇 **[封鎖]** 索引標籤。
5. 在 **[封鎖的連線]** 欄位中，按一下 **[新增]** 以定義將無法修改資料的連線。
6. 在 **[電腦名稱/帳戶]** 欄位中，輸入安裝保護代理程式所在電腦的電腦名稱和帳戶。例如，`MyComputer\TestUser`。
7. 在 **[主機名稱]** 欄位中，輸入可以使用保護代理程式連線至電腦的電腦主機名稱。
8. 選擇右側的核取方塊以儲存連線定義。
9. 按一下**[完成]**。

加密採礦惡意軟體會使有用應用程式的效能降低、增加電費，而且可能造成系統當機，甚至因為濫用而導致硬體損壞。**[加密採礦程序偵測]** 功能可保護您的裝置免受加密採礦惡意軟體攻擊，以防止未經許可使用電腦資源。

系統管理員可以在不啟用 **[Active Protection]** 的情況下啟用 **[加密採礦程序偵測]**。預設設定：**[啟用]**。

注意事項
Linux 不支援加密採礦程序偵測。

若要設定網路資料夾保護

1. 在 **[建立保護計劃]** 視窗中，展開 **[防毒和防惡意軟體防護]** 模組。
2. 按一下 **[加密採礦程序偵測]**。
3. 使用 **[偵測加密採礦程序]** 切換啟用或停用此功能。
4. 選擇如何處理懷疑有加密採礦活動的程序：

   預設設定：**停止程序**

   - **僅通知** — 軟體會產生警示。
   - **停止程序** — 軟體會產生警示並停止程序。
5. 按一下 **[完成]**，將所選選項套用至保護計劃。

保護排除項目可讓您在受信任的程式被視為勒索軟體或惡意軟體時消除誤報。若要定義信任項目和封鎖項目，您可以將其新增至保護排除項目清單。

在信任項目清單中，您可以新增檔案、程序和資料夾，以便將其視為系統中的安全項目，並防止之後偵測到這些內容。

在封鎖項目清單中，您可以新增程序和雜湊。此選項可保證這些程序將會遭到封鎖，而且您的工作負載將安全無虞。

保護排除項目	已封鎖	受信任
雜湊	當雜湊新增到封鎖項目清單時，系統將會根據提供的雜湊，停止程序。 例如，當您新增這個 MD5 雜湊 (938c2cc0dcc05f2b68c4287040cfcf71) 時，與此雜湊相關聯的程序將會遭到封鎖。	當雜湊新增到信任項目清單時，系統將會根據提供的雜湊，知道必須透過監控略過的程序。 例如，當您新增這個 MD5 雜湊 (938c2cc0dcc05f2b68c4287040cfcf71) 時，與此雜湊相關聯的程序將會受到信任並從監控中排除。
程序	當程序新增到封鎖項目清單時，系統將會知道必須監控這些程序，因此這些程序一律會遭到封鎖。 例如，如果您將此路徑 C:\Users\user1\application\nppInstaller.exe 新增到封鎖項目清單中，這個特定程序將會遭到封鎖，因此當您嘗試開啟該程序	當程序新增到信任項目清單時，系統將會知道這些程序必須從監控中排除。 **注意事項** 由 Microsoft 簽署的程序一律受到信任。 例如，如果您新增此路徑 C:\Users\user1\application\nppInstaller.ex

保護排除項目	已封鎖	受信任
	時，將無法啟動它。	e，這個特定程序將會從監控中排除，因此防毒軟體將不會干擾此程序。
檔案/資料夾		當檔案或資料夾新增到信任項目清單時，系統將會知道這些檔案或資料夾應該一律被視為安全無虞，因此不需要掃描/監控它們。

若要指定將一律受到信任的項目

1. 開啟保護計劃。
2. 展開 **[防毒和反惡意程式碼保護]** 模組。
3. 選擇 **[排除項目]** 選項。
   [保護排除項目] 視窗隨即開啟。
4. 在 **[信任項目]** 區段中，按一下 **[新增]** 可從可用選項中選擇：
   - 若要信任檔案、資料夾或程序，選擇 **[檔案/資料夾/程序]** 選項。**[新增檔案/資料夾/程序]** 視窗隨即開啟。
     - 在 **[檔案/資料夾/程序]** 欄位中新的一行上，輸入每個程序、資料夾或檔案的路徑。在 **[描述]** 區段中輸入簡短描述，讓您可以在信任項目清單中辨識您的變更。
     - 選擇 **[新增為檔案/資料夾]** 核取方塊以信任檔案/資料夾。
       資料夾描述的範例：D:\folder\、/home/Folder/folder2、F:\
     - 選擇 **[新增為程序]** 核取方塊以信任程序。所選程序將從監控中排除。

       注意事項
       指定程序執行檔的完整路徑，並以磁碟機代號開頭。例如，
       `C:\Windows\Temp\er76s7sdkh.exe`。

       注意事項
       支援區域網路路徑，例如：\\localhost\folderpath\file.exe
   - 選擇 **[雜湊]** 選項可將 MD5 雜湊新增至信任項目清單中。**[新增雜湊]** 視窗隨即開啟。
     - 在此，您可以在個別行上插入 MD5 雜湊，以便納入為 [保護排除項目] 清單中的受信任項目。根據這些雜湊，Cyber Protection 將排除 MD5 雜湊所述的程序，使其不受監控。

預設設定：預設沒有定義任何排除項目。

若要指定將一律遭到封鎖的項目

1. 開啟保護計劃。
2. 展開 **[防毒和防惡意程式保護]** 模組。

3. 選擇 **[保護排除項目]** 選項。**[保護排除項目]** 視窗隨即開啟。

   在 **[封鎖項目]** 區段中，按一下 **[新增]** 可從可用選項中選擇：

- 若要封鎖程序，選擇 **[程序]** 選項。**[新增程序]** 視窗隨即開啟。
  - 在 **[程序]** 欄位中新的一行上，輸入每個程序的路徑。在 **[描述]** 欄位中輸入簡短描述，讓您可以在封鎖項目清單中辨識您的變更。

    注意事項
    只要在電腦上啟用了 Active Protection，這些程式就無法啟動。

- 若要封鎖雜湊，選擇 **[雜湊]** 選項。**[新增雜湊]** 視窗隨即顯示。
  - 在 **[雜湊]** 欄位中新的一行上，輸入每個程序的雜湊。在 **[描述]** 欄位中輸入簡短描述，讓您可以在封鎖項目清單中辨識您的變更。

預設設定：預設沒有定義任何排除項目。

萬用字元

指定資料夾時，您可以使用萬用字元 * 與 ?。星號 (*) 可代替零個或多個字元。問號 (?)可代替一個字元。無法使用環境變數，例如 %AppData%。

您可以使用萬用字元 (*)，將項目新增到排除清單。

- 萬用字元可以用於描述中間或結尾。

描述中接受的萬用字元範例：

C:*.pdf

D:\folders\file.*

C:\Users*\AppData\Roaming

- 萬用字元無法用於描述開頭。

描述中不接受的萬用字元範例：

*.docx

*:\folder\

變數

您也可以使用變數，將項目新增到 [保護排除項目] 清單，但限制如下：

- 若是 Windows，僅支援 SYSTEM 變數。不支援使用者專用的變數 (例如 %USERNAME%、%APPDATA%)。不支援包含 {username} 的變數。如需詳細資訊，請參閱 https://ss64.com/nt/syntax-variables.html。
- 若是 macOS，不支援環境變數。
- 若是 Linux，不支援環境變數。

支援的格式的範例：

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

描述

您可以使用 **[描述]** 欄位，記下您在 [保護排除項目] 清單中新增的排除項目。您可以記下的一些內容建議：

- 排除的原因和目的。
- 雜湊排除項目的實際檔案名稱。
- 時間戳記。

如果在單一項目中新增了多個項目，則只能針對多個項目擷取 1 個註解。

URL 篩選

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

惡意程式碼通常是由惡意網站或受感染的網站散佈，並使用所謂的路過式下載感染方法。

「URL 篩選」功能可讓您保護電腦，免受來自網際網路的惡意程式碼和網路釣魚等威脅。您可以透過封鎖對可能含有惡意內容之網站的使用者存取，以保護貴組織。

URL 篩選也可讓您控制網路使用量以符合外部法規和公司內部政策。您可以根據網站的相關類別，設定其存取權。URL 篩選目前支援 44 個網站類別，並允許管理其存取權。

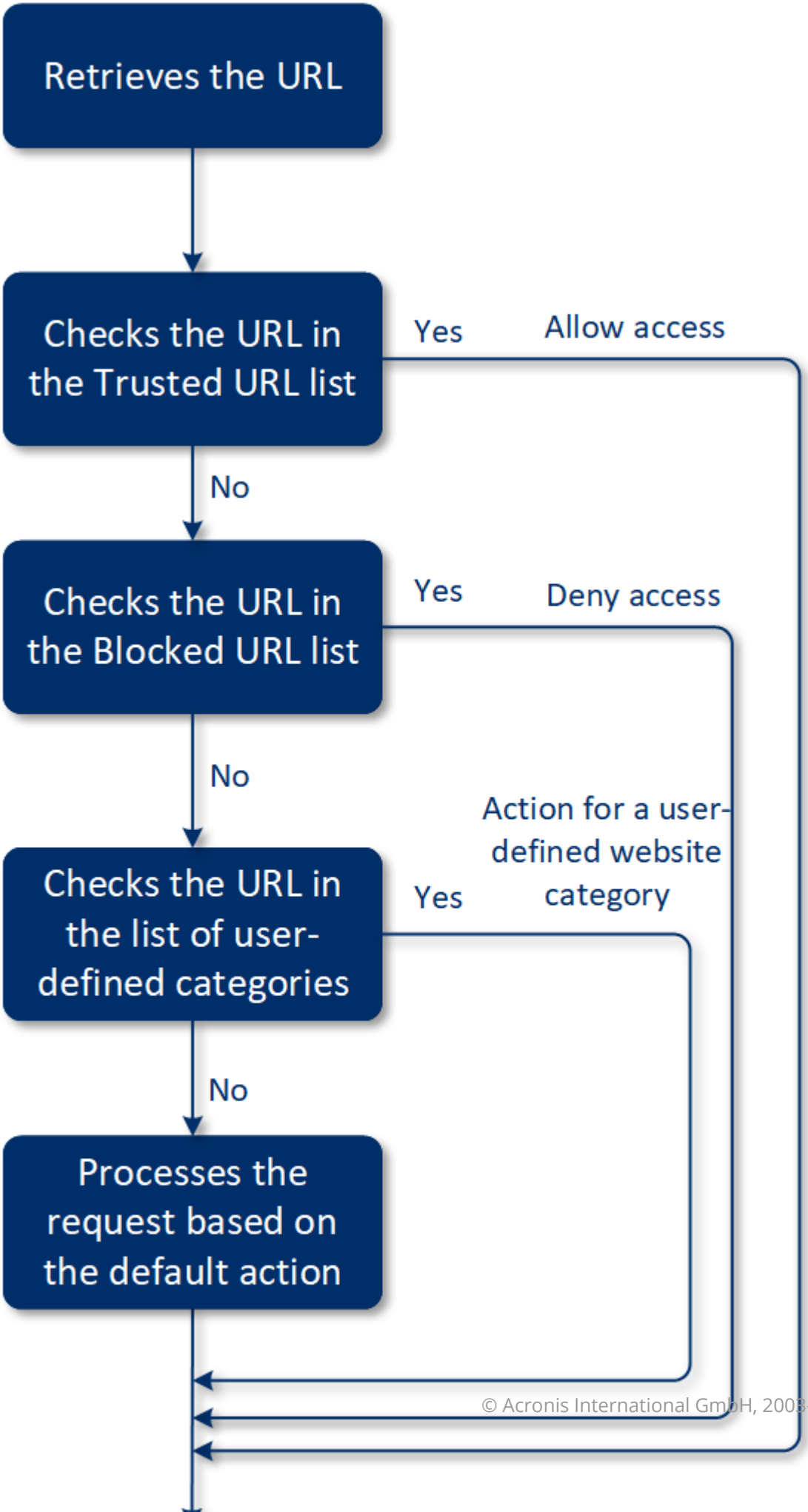
目前，保護代理程式將會檢查 Windows 電腦上的 HTTP/HTTPS 連線。

URL 篩選功能需要有網際網路連線才能運作。

注意事項
為防止可能發生的保護代理程式組建 15.0.26692 (版本 C21.03 HF1) 和更舊版本相容性問題，如果偵測到其他防毒解決方案，或者如果系統上沒有 Windows 資訊安全中心服務，則會自動停用 URL 篩選功能。
在之後的保護代理程式中，相容性問題會獲得解決，因此根據原則，一律啟用 URL 篩選。

運作原理

使用者在瀏覽器中輸入一個 URL 連結。攔截器取得連結，並傳送到保護代理程式中。代理程式取得 URL、進行剖析，然後檢查結果。攔截器將使用者重新導向至含有訊息的頁面，此訊息中含有手動前往所要求頁面的可用動作。

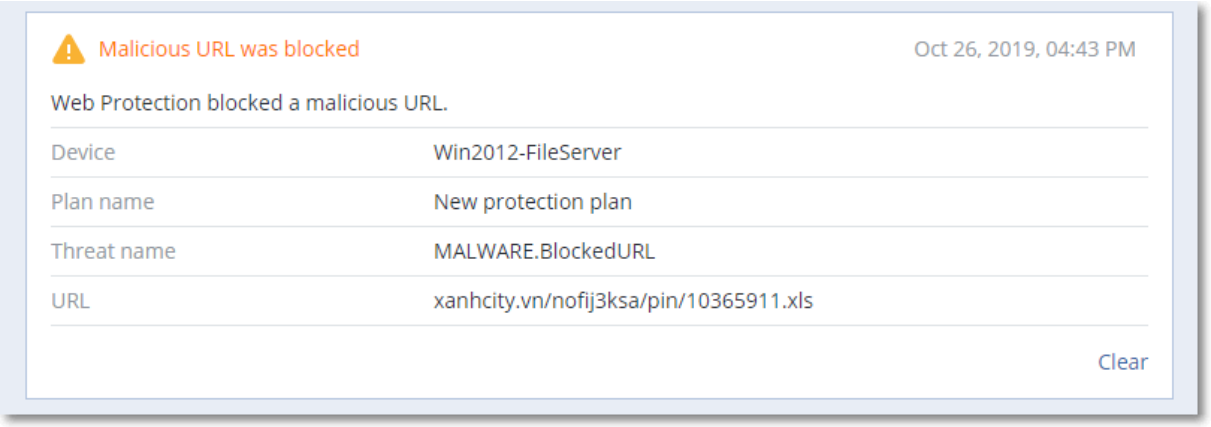


URL 篩選設定工作流程

一般而言，URL 篩選設定包含下列步驟：

1. 在啟用 **[URL 篩選]** 模組的情況下，建立一個保護計劃。
2. 指定 URL 篩選設定 (請參閱以下內容)。
3. 將保護計劃指派給電腦。

若要檢查已遭到封鎖的 URL，請移至 **[監控]** > **[警示]**。



URL 篩選設定

您可以針對 [URL 篩選] 模組指定下列設定。

惡意網站存取

指定當使用者開啟惡意網站時將執行的動作：

- **僅通知** — 軟體會針對懷疑有勒索軟體活動的程序產生警示。
- **封鎖** – 封鎖對惡意網站的存取。使用者將無法存取網站，而且系統將會產生一個警告警示。
- **一律詢問使用者** – 詢問使用者仍要繼續前往網站還是要返回。

要篩選的類別

您可以設定其存取權的網站有 44 個：

- **允許** – 允許存取與所選類別相關的網站。
- **拒絕** – 拒絕存取與所選類別相關的網站。

系統預設允許所有類別。

顯示依類別封鎖之 URL 的所有通知 – 如果啟用，您將收到系統匣中顯示的所有通知 (依類別封鎖的 URL)。如果某個網站有數個子網域，則系統也會為其產生通知，因此通知數量可能很大。

在下表中，您可以找到類別描述：

	網站類別	描述
1	**廣告**	此類別涵蓋其主要用途為提供廣告服務的網域。
2	**留言板**	此類別涵蓋論壇、討論區和問答型網站。此類別未涵蓋公司網站上客戶提出問題的特定部分。
3	**個人網站**	此類別涵蓋個人網站以及所有類型的部落格：個人、團體甚至公司部落格。部落格是在全球資訊網上發佈的一種日誌。其由條目 (「貼文」) 所組成，通常以相反的時間順序顯示，因此最新的貼文最先顯示。
4	**公司/商業網站**	這是一個廣泛的類別，其中涵蓋通常不屬於其他任何類別的公司網站。
5	**電腦軟體**	此類別涵蓋提供電腦軟體的網站，通常是開放原始碼、免費軟體或共享軟體。其可能也涵蓋線上軟體商店。
6	**醫療藥品**	此類別涵蓋與藥品/酒精/煙草相關的網站，其中討論 (合法) 醫療藥品或器材、酒精或煙草產品的使用或銷售。 請注意，非法藥物涵蓋在「毒品」類別中。
7	**教育**	此類別涵蓋屬於正式教育機構的網站，包括 .edu 網域之外的網站。其也包含教育網站，例如 Encyclopedia。
8	**娛樂**	此類別涵蓋提供與藝術活動和博物館相關資訊的網站，以及評論或評價電影、音樂或藝術等內容的網站。
9	**檔案共用**	此類別涵蓋使用者可以在其中上傳檔案並與他人共用的檔案共用網站。其也涵蓋 torrent 共享網站和 torrent 追蹤器。
10	**財務**	此類別涵蓋屬於全球所有提供線上存取的銀行的網站。部分信用合作社和其他金融機構也涵蓋在內。但是，可能不包括部分本地銀行。
11	**賭博**	此類別涵蓋賭博網站。這些是「線上賭場」或「線上樂透彩」類型網站，通常需要先付款，使用者才能在線上輪盤、撲克牌、21 點或類似遊戲中賭博。其中有一些是合法的，也就是有贏的機會；有一些則是欺詐性的，也就是沒有贏的機會。它還會偵測「密技和作弊」網站，其中描述在賭博和線上樂透彩網站上賺錢的方式。
12	**遊戲**	此類別涵蓋提供線上遊戲的網站，這些網站通常是以 Adobe Flash 或 Java Applet。偵測遊戲是免費的還是需要訂購授權並不重要，但是，在「賭博」類別中會偵測賭場形式的網站。 以下類別不涵蓋在內： • 開發電玩遊戲的公司的官方網站 (除非他們製作線上遊戲) • 討論遊戲的討論網站 • 可以下載非線上遊戲的網站 (其中部分屬於「非法」類別) • 要求使用者下載並執行可執行檔的遊戲，例如 《魔獸世界》；可以透過不同方式 (例如，防火牆) 防禦的遊戲
13	**政府機**	此類別涵蓋政府網站，包括政府機構、大使館和辦公室網站。

	構	
14	**駭客入侵**	此類別涵蓋為駭客提供駭客入侵工具、文章和討論平台的網站。其也涵蓋提供常見平台漏洞利用的網站，這些漏洞可導致 Facebook 或 Gmail 帳戶遭到駭客入侵。
15	**非法活動**	此類別是一個與仇恨、暴力和種族主義相關的廣泛類別，旨在封鎖以下類別的網站： • 屬於恐怖組織的網站 • 具有種族主義或仇外心理的網站 • 討論攻擊性運動和/或煽動暴力的網站
16	**健康和健身**	此類別涵蓋與醫療機構相關的網站、與疾病預防和治療相關的網站、提供減重、飲食、類固醇、合成代謝或 HGH 產品相關資訊或產品的網站，以及提供整形外科相關資訊的網站。
17	**嗜好**	此類別涵蓋的網站提供通常在個人空閒時間進行之活動相關的資源，例如收集、手工藝品和騎自行車。
18	**Web 託管**	此類別涵蓋免費商業網站託管服務，該服務允許私人使用者和組織建立及發佈網頁。
19	**非法下載**	此類別涵蓋與軟體盜版相關的網站，包括： • 點對點 (BitTorrent、emule、DC++) 追蹤器網站，眾所周知，這種網站會在未經版權所有人同意的情況下，協助散佈受版權保護的內容 • Warez (盜版商業軟體) 網站和討論區 • 為使用者提供破解，金鑰產生器和序號，有利於非法使用軟體的網站 其中部分網站也可能被偵測為色情或菸酒的網站，因為這些網站經常使用色情或酒類廣告來賺錢。
20	**即時訊息**	此類別涵蓋允許使用者即時聊天的即時訊息和聊天網站。其也會偵測到 yahoo.com 和 gmail.com，因為它們都包含一個嵌入式即時訊息服務。
21	**工作/職業**	此類別涵蓋顯示求職板、工作相關分類廣告和職業機會，以及此類服務彙總器的網站。其未涵蓋人力仲介或常規公司網站上的「工作」頁面。
22	**成人內容**	此類別涵蓋由網站建立者標記為成人對象的內容。其涵蓋從 慾經》和性教育網站到露骨色情內容的各式各樣網站。
23	**毒品**	此類別涵蓋分享娛樂和非法藥物相關資訊的網站。此類別也涵蓋包含開發或成長中藥品的網站。
24	**新聞**	此類別涵蓋提供文字和影片新聞的新聞網站。其致力於涵蓋全球和地方新聞網站；但是，部分小型地方新聞網站可能未包含在內。
25	**線上交友**	此類別涵蓋付費和免費的線上交友網站，使用者可以在其中使用特定條件搜尋其他人。他們也可以張貼其個人資料，以供其他人搜尋。此類別同時包含免費和付費的線上交友網站。 大部分熱門的社交網路都可以當作線上交友網站使用，因此，這個類別也會偵測到 Facebook 之類的熱門網站。建議您使用此類別搭配社群網路類別。

26	**線上支付**	此類別涵蓋提供線上支付或匯款的網站。其會偵測到熱門的支付網站，例如 PayPal 或 Moneybookers。它也會以啟發的方式偵測要求信用卡資訊的一般網站上的網頁，從而偵測到隱藏的、未知的或非法的線上商店。
27	**相片分享**	此類別涵蓋其主要用途是讓使用者上傳和分享相片的相片分享網站。
28	**線上商店**	此類別涵蓋已知的線上商店。如果某個網站在線上銷售商品或服務，就會被視為線上商店。
29	**色情**	此類別涵蓋包含性愛內容和色情內容的網站。其同時包含付費和免費的網站。它涵蓋提供圖片、故事和影片的網站，而且它也會偵測到混合內容網站上的色情內容。
30	**入口網站**	此類別涵蓋的網站彙總來自多個來源和各種網域的資訊，而且通常會提供諸如搜尋引擎、電子郵件、新聞和娛樂資訊之類的功能。
31	**廣播電台**	此類別涵蓋提供網際網路音樂串流服務的網站，從線上廣播電台到提供隨選 (免費或付費) 音訊內容的網站。
32	**宗教**	此類別涵蓋宣傳宗教或宗派的網站。其也涵蓋與一或多個宗教相關的討論區。
33	**搜尋引擎**	此類別涵蓋搜尋引擎網站，例如 Google、Yahoo 和 Bing。
34	**社交網路**	此類別涵蓋社交網路網站。這包括 MySpace.com、Facebook.com、Bebo.com 等等。但是，專業化的社交網路 (例如 YouTube.com) 將會列在「影片/相片」類別中。
35	**運動**	此類別涵蓋提供運動資訊、新聞和教學課程的網站。
36	**自殺**	此類別涵蓋宣傳、提供或倡導自殺的網站。其未涵蓋自殺防治診所。
37	**小報**	此類別主要針對藝術性色情內容和名人八卦網站而設計。許多小報風格的新聞網站可能會在這裡列出子類別。此類別的偵測也是以啟發式方法為主。
38	**浪費時間**	此類別涵蓋個人傾向於花費大量時間的網站。這可能包括其他類別的網站，例如，社交網路或娛樂。
39	**旅遊**	此類別涵蓋顯示旅遊優惠和旅遊裝備以及旅遊目的地評論和評等的網站。
40	**影片**	此類別涵蓋裝載各種影片或相片的網站，這些內容是由使用者上傳或由各種內容提供者所提供。這包括 YouTube、Metacafe、Google Video 之類的網站，以及 Picasa 或 Flickr 之類的相片網站。其也會偵測到其他網站或部落格中內嵌的影片。
41	**暴力卡通**	此類別涵蓋討論、分享和提供暴力卡通或漫畫的網站，這些內容可能會因為暴力、露骨的語言或色情內容而不適合未成年人。 此類別未涵蓋提供 《湯姆貓與傑利鼠》等主流卡通的網站。
42	**武器**	此類別涵蓋提供武器出售或交換、製造或使用的網站。其也涵蓋打獵資源與空氣槍和 BB 槍的使用，以及格鬥武器。
43	**電子郵件**	此類別涵蓋以 Web 應用程式提供電子郵件功能的網站。

44	**Web Proxy**	此類別涵蓋提供 Web Proxy 服務的網站。這是一個當使用者開啟網頁、在表單中輸入所要求的 URL, 然後按一下 [提交] 時的「瀏覽器內的瀏覽器」類型網站。Web Proxy 網站會下載實際的網頁, 並將其顯示在使用者瀏覽器內。 偵測到 (而且可能需要封鎖) 這個類型的原因如下: • 用於匿名瀏覽。由於對目的地網頁伺服器的要求是從 Proxy 網頁伺服器發出的, 因此只能看到其 IP 位址, 而且如果伺服器系統管理員追蹤使用者, 則追蹤將在 Web Proxy 上結束, 這不一定會保留找出原始使用者所需的記錄。 • 用於位置詐騙。使用者 IP 位址通常用於依來源位置分析服務 (部分國家政府網站可能只能從本機 IP 位址存取), 而且這些服務可協助使用者欺騙其真實位置。 • 用於存取禁止的內容。如果使用簡單的 URL 篩選, 將只會看到 Web Proxy URL, 而不會看到使用者所造訪的實際伺服器。 • 用於避免公司監視。公司政策可能會要求監視員工的網際網路使用情況。透過 Web Proxy 存取所有內容時, 使用者可能會逃避將不會提供正確資訊的監視。 SDK 不僅會分析 HTML 網頁 (若有提供), 還會分析 URL, 因此對於某些類別而言, SDK將仍然能夠偵測到內容。但是, 僅使用 SDK 無法避免其他原因。

URL 排除項目

已知為安全的 URL 可以新增到受信任網域的清單中。代表威脅的 URL 可以新增到已封鎖網域的清單中。

若要指定將一律受到信任或遭到封鎖的 URL

1. 在保護計劃的 [URL 篩選] 模組中, 按一下 **[URL 排除項目]**。
   [URL 排除項目] 視窗隨即開啟。
   顯示下列選項:

信任項目 — 按一下 **[新增]** 可從可用選項中選擇:

- **網域** — 當您選擇此選項時, **[新增網域]** 視窗隨即開啟。
  - 在 **[網域]** 欄位中新的一行上, 輸入每個網域。在 **[描述]** 欄位中輸入簡短描述, 讓您可以在信任項目清單中辨識您的變更。
- **程序** — 當您選擇此選項時, **[新增程序]** 視窗隨即顯示。
  - 在 **[程序]** 欄位中新的一行上, 輸入每個程序的路徑。在 **[描述]** 區段中輸入簡短描述, 讓您可以在信任項目清單中辨識您的變更。

封鎖項目 — 按一下 **[新增]**。**[新增網域]** 視窗隨即顯示。

在 **[網域]** 欄位中新的一行上, 輸入每個網域。在 **[描述]** 欄位中輸入簡短描述, 讓您可以在封鎖項目清單中辨識您的變更。

注意事項
支援區域網路路徑。例如, \\localhost\folderpath\file.exe。

描述

您可以使用 **[描述]** 欄位, 記下您在 URL 排除項目清單中新增的排除項目。您可以記下的一些建議:

- 排除的原因和目的。
- 時間戳記。

如果在單一項目中新增了多個項目，則只能針對多個項目擷取 1 個註解。

Microsoft Defender 防毒軟體與 Microsoft Security Essentials

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

Microsoft Defender 防毒軟體

Microsoft Defender 防毒軟體是 Microsoft Windows 從 Windows 8 開始提供的一種內建反惡意程式碼元件。

Microsoft Defender 防毒軟體 (WDA) 模組可讓您透過 Cyber Protect 主控台，設定 Microsoft Defender 防毒軟體安全性原則並追蹤其狀態。

此模組適用於已安裝 Microsoft Defender 防毒軟體的工作負載。

Microsoft Security Essentials

Microsoft Security Essentials 是 Microsoft Windows 在 Windows 8 之前提供的一種內建反惡意程式碼元件。

Microsoft Security Essentials 模組可讓您透過 Cyber Protect 主控台，設定 Microsoft Security Essentials 安全性原則並追蹤其狀態。

此模組適用於已安裝 Microsoft Security Essentials 的工作負載。

Microsoft Security Essentials 的設定與 Microsoft Defender 防毒軟體的設定類似，但是您無法設定即時保護，而且無法透過 Cyber Protect 主控台定義排除項目。

排程掃描

指定排程掃描的排程。

掃描模式：

- **完整** – 除了在快速掃描中掃描的項目之外，完整檢查所有檔案和資料夾。相較於快速掃描，完整掃描需要更多用於執行的電腦資源。
- **快速** – 快速檢查通常會找到惡意程式碼的記憶體內程序和資料夾。快速掃描需要用於執行的電腦資源較少。

定義執行掃描的時間和星期幾。

每日快速掃描 – 定義每日快速掃描的時間。

您可以根據您的需求，設定以下選項：

當電腦開啟但未使用中時，啟動排程掃描

執行排程掃描之前，檢查最新的病毒和間諜軟體定義

進行下列掃描期間，限制 CPU 使用量

如需有關 Microsoft Defender 防毒軟體設定的詳細資訊，請參閱 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings

預設動作

針對偵測到的不同嚴重層級威脅，並易要執行的預設動作：

- **清理** – 清理工作負載上偵測到的惡意程式碼。
- **隔離** – 將偵測到的惡意程式碼放在隔離資料夾中，但不要移除它。
- **移除** – 從工作負載中移除偵測到的惡意程式碼。
- **允許** – 不要移除或隔離偵測到的惡意程式碼。
- **使用者自訂** – 系統將提示使用者指定要對偵測到的惡意程式碼執行的動作。
- **無動作** – 將不採取任何動作。
- **封鎖** – 封鎖偵測到的惡意程式碼。

如需有關 Microsoft Defender 防毒軟體預設動作設定的詳細資訊，請參閱 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings

即時保護

啟用 **[即時保護]** 以偵測惡意程式碼並阻止其在工作負載上安裝或執行。

掃描所有下載 – 如果已選擇，則會針對所有下載的檔案和附件執行掃描。

啟用行為監視 – 如果已選擇，將會啟用行為監視。

掃描網路檔案 – 如果已選擇，將會掃描網路檔案。

允許在對應的網路磁碟機上執行完整掃描 – 如果已選擇，將會完整掃描對應的網路磁碟機。

允許電子郵件掃描 – 如果已啟用，引擎將會根據其特定格式，剖析信箱和郵件檔案，以分析郵件本文和附件。

如需有關 Microsoft Defender 防毒軟體即時保護設定的詳細資訊，請參閱 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings

進階

指定進階掃描設定：

- **掃描存檔檔案** – 將存檔檔案 (例如 .zip 或 .rar 檔案) 包含在掃描中。
- **掃描卸除式磁碟機** – 在完整掃描期間掃描卸除式磁碟機。

- **建立系統還原點** – 在某些情況下，重要檔案或登錄項目可能會被當作「誤報」遭到移除，則您將能夠從還原點復原。
- **在下列時間後移除隔離的檔案** – 定義將移除隔離檔案的期限。
- **需要進一步分析時，自動傳送檔案範例：**
  - **一律提示** – 檔案傳送之前，將會要求您確認。
  - **自動傳送安全範例** – 大多數範例將會自動傳送，但可能包含個人資訊的檔案除外。這類檔案將需要另外確認。
  - **自動傳送所有範例** – 系統將自動傳送所有範例。
- **停用 Windows Defender 防毒軟體 GUI** – 如果已選擇，使用者將無法使用 WDA 使用者介面。您可以透過 Cyber Protect 主控台管理 WDA 原則。
- **MAPS (Microsoft Active Protection Service)** – 可協助您選擇如何回應潛在威脅的線上社群。
  - **我不要加入 MAPS** – 對於偵測到的軟體，將不會傳送任何資訊給 Microsoft。
  - **基本成員資格** – 對於偵測到的軟體，將會傳送基本資訊給 Microsoft。
  - **進階成員資格** – 對於偵測到的軟體，將會傳送更詳細的資訊給 Microsoft。

  如需詳細資訊，請參閱 https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise/

如需有關 Microsoft Defender 防毒軟體進階設定的詳細資訊，請參閱 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings

排除

您可以定義下列要從掃描排除的檔案和資料夾：

- **程序** – 將會從掃描中排除已定義之程序讀取或寫入的任何檔案。您需要定義程序可執行檔的完整路徑。
- **檔案和資料夾** – 指定的檔案和資料夾將從掃描排除。您需要定義資料夾或檔案的完整路徑，或定義副檔名。

如需有關 Microsoft Defender 防毒軟體排除設定的詳細資訊，請參閱 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings

防火牆管理

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

防火牆管理可讓您在受保護的工作負載上輕鬆設定防火牆設定。

系統會透過 Microsoft Windows 的內建 Microsoft Defender 防火牆元件，在 Cyber Protect 中提供這個功能。Microsoft Defender 防火牆會封鎖未經授權流入或流出工作負載的網路流量。

防火牆管理適用於已安裝 Microsoft Defender 防火牆所在的工作負載。

支援的 Windows 作業系統

防火牆管理支援下列 Windows 作業系統：

Windows

- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

不支援 Windows Server。

啟用和停用防火牆管理

您可以在建立保護計劃時啟用防火牆管理。您可以將現有的保護計劃變更為啟用或停用防火牆管理。

若要啟用或停用防火牆管理

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 執行下列其中一項操作以開啟保護計劃面板：
   - 如果您要建立新的保護計劃，選擇要保護的電腦，按一下 **[保護]**，然後按一下 **[建立計劃]**。
   - 如果您要變更現有的保護計劃，選擇受保護的電腦，按一下 **[保護]**，按一下保護計劃名稱旁的省略符號 (...)，然後按一下 **[編輯]**。
3. 在保護計劃面板中，瀏覽至 **[防火牆管理]** 區域，然後啟用或停用 **[防火牆管理]**。
4. 執行下列其中一項操作以套用您的變更：
   - 若要建立保護計劃，按一下 **[建立]**。
   - 若要編輯保護計劃，按一下 **[儲存]**。

根據您啟用還是停用防火牆管理而定，保護計劃的 **[防火牆管理]** 區域中的 **[Microsoft Defender 防火牆狀態]** 會顯示為 **[開啟]** 或 **[關閉]**。

您也可以從 [管理] 索引標籤存取保護計劃面板。但是，此功能無法用於 Cyber Protection 服務的所有版本。

隔離

隔離是受保護裝置硬碟上的一個特殊隔離資料夾。如果防毒和防惡意軟體防護偵測到任何可疑的檔案，則會將其移入 [隔離]，以防止威脅進一步擴散。

在主控台的 **[隔離]** 索引標籤中，您可以從所有受保護的裝置檢閱可疑和可能危險的檔案，並決定要移除還是還原這些檔案。

注意事項
如果裝置從環境中移除，就會自動移除隔離的檔案。

檔案如何進入隔離資料夾?

1. 在保護計劃中，選擇 **[隔離]** 作為受感染或可疑檔案的預設動作。
   若要瞭解如何建立保護計劃，請參閱 "建立保護計劃" (第 192 頁)。
2. 掃描時，[防毒和防惡意軟體防護] 模組會偵測惡意檔案，並將其移至安全的 [隔離] 資料夾。
3. 此模組會更新隔離清單，以新增已移至 [隔離] 的檔案相關資訊。

注意事項
在保護計劃的 **[在下列時間後移除隔離的檔案]** 設定中定義的期限之後，就會從 [隔離] 資料夾自動刪除檔案。請參閱 "隔離設定" (第 737 頁)。

管理隔離的檔案

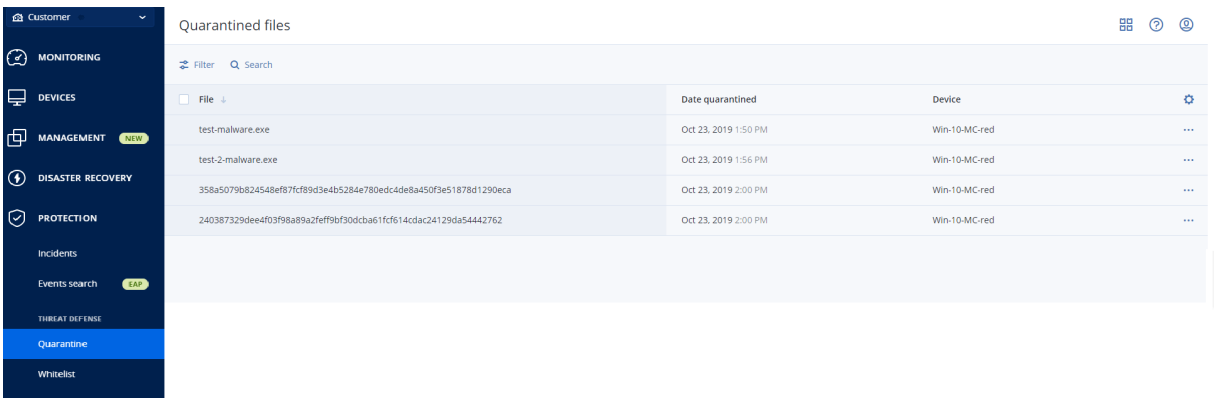
若要管理隔離的檔案，請前往 **[防護]** > **[隔離]**。所有受保護裝置的隔離檔案清單中包含下列資訊。

名稱	描述
檔案	所隔離檔案的名稱。
隔離日期	檔案移入 [隔離] 的日期和時間。
裝置	找到受感染檔案所在的裝置。
威脅名稱	威脅名稱。
保護計劃	將可疑檔案移至 [隔離] 所依據的保護計劃。

您可以對隔離的檔案執行下列動作：

- **刪除** – 從電腦永久移除隔離的檔案。您可以使用相同的檔案雜湊，刪除所有檔案。您可以使用相同的檔案雜湊，還原所有檔案。依雜湊為檔案分組、選擇需要的檔案，然後刪除這些檔案。
- **還原** – 在不進行任何修改的情況下，將隔離的檔案還原到原始位置。如果目前在原始位置中有名稱相同的檔案，則該檔案將會以還原的檔案覆寫。

  注意事項
  系統會將已還原的檔案新增至允許名單中，並在進一步的惡意程式碼掃描期間略過該檔案。



電腦上的隔離位置

以下是每個作業系統的隔離檔案的預設位置清單。

- 若是 Windows 電腦：`%programdata%\Acronis\NGMP\quarantine`
- 若是 Mac 電腦：`/Library/Application Support/Acronis/NGMP/quarantine`
- 若是 Linux 電腦：`/var/lib/Acronis/NGMP/quarantine`

隔離儲存空間受到服務提供者的自我防衛保護。

隨選自助服務自訂資料夾

您可以在工作負載上選擇自訂資料夾，然後直接從內容功能表掃描這些資料夾。

若要在內容功能表中存取使用 Cyber Protect 選項進行掃描

對於已在保護計劃中啟用防毒和反惡意程式碼的工作負載，以滑鼠右鍵按一下您要掃描的檔案/資料夾。

注意事項
此選項僅適用於工作負載的系統管理員。

公司白名單

防毒解決方案可能會將合法的公司專用應用程式視為可疑的應用程式。為防止這些誤報偵測，必須將信任的應用程式手動新增到白名單，這非常耗時。

注意事項
公司白名單不會影響備份的防惡意軟體掃描。

Cyber Protection 可以將此流程自動化：[防毒和防惡意程式保護] 模組會掃描備份，而且會分析掃描的資料，以便將這類應用程式移到白名單，並防止誤報偵測。此外，全公司白名單可提高進一步的防惡意軟體掃描效能。

系統會針對每個客戶，而且僅基於此客戶的資料，建立白名單。

您可以啟用和停用白名單。停用白名單時，會暫時隱藏其中新增的檔案。

注意事項
只有擁有系統管理員角色的帳戶 (例如，Cyber Protection 系統管理員；公司系統管理員；代表公司系統管理員行事的合作夥伴系統管理員；單位系統管理員) 才可以設定和管理白名單。此功能不適用於唯讀系統管理員帳戶或使用者帳戶。

自動新增至白名單

1. 在至少兩部電腦上對備份執行雲端掃描。您可以使用備份掃描計劃達到這個目的。
2. 在白名單設定中，啟用 **[自動產生白名單]** 開關。

手動新增至白名單

即使是在停用 **[自動產生白名單]** 開關時，您還是可以將檔案手動新增到白名單。

1. 在 Cyber Protect 主控台中，移至 **[防惡意軟體防護]** > **[白名單]**。
2. 按一下 **[新增檔案]**。
3. 指定檔案的路徑，然後按一下 **[新增]**。

將隔離的檔案新增到白名單

您可以將隔離的檔案新增到白名單。

1. 在 Cyber Protect 主控台中，移至 **[防惡意軟體防護]** > **[隔離]**。
2. 選擇隔離的檔案，然後按一下 **[新增到白名單]**。

白名單設定

當您啟用 **[自動產生白名單]** 開關時，必須指定下列其中一個啟發式保護的層級：

- **低**
  只有在經過大量時間和檢查之後，才會將公司應用程式新增至白名單。這類應用程式更受信任。不過，這種方法會增加誤報偵測的可能性。將檔案視為未受感染並受信任的條件很高。
- **預設**
  公司應用程式將會根據建議的保護層級，新增到白名單，以減少可能的誤報偵測。將檔案視為未受感染並受信任的條件中等。
- **高**
  公司應用程式將會更快地新增到白名單，以減少可能的誤報偵測。不過，這並不保證該軟體未受感染；它之後可能會被視為可疑或惡意程式碼。將檔案視為未受感染並受信任的條件很低。

檢視白名單中關於項目的詳細資料

您可以按一下白名單中的某個項目，檢視其相關的詳細資訊，並在線上進行分析。

如果您不確定您所新增的項目，可以在 VirtusTotal 分析程式中進行檢查。當您按一下 **[在 VirusTotal 上檢查]** 時，網站會使用您所新增之項目的檔案雜湊，分析可疑的檔案和 URL 以偵測惡意程式碼類型。您可以檢視 **[檔案雜湊 (MD5)]** 字串中的雜湊。

[電腦] 值表示在備份掃描期間找到此種雜湊所在電腦的數目。只有在項目來自備份掃描或隔離區時，才會填入這個值。如果已將檔案手動新增到白名單，則此欄位會維持空白。

備份的反惡意程式碼掃描

使用針對備份的防惡意軟體掃描，您可以透過檢查備份是否沒有惡意軟體，來防止復原受感染的檔案。防惡意軟體掃描是由位在 Cyber Protection 資料中心的雲端代理程式執行，不會使用本機計算資源。

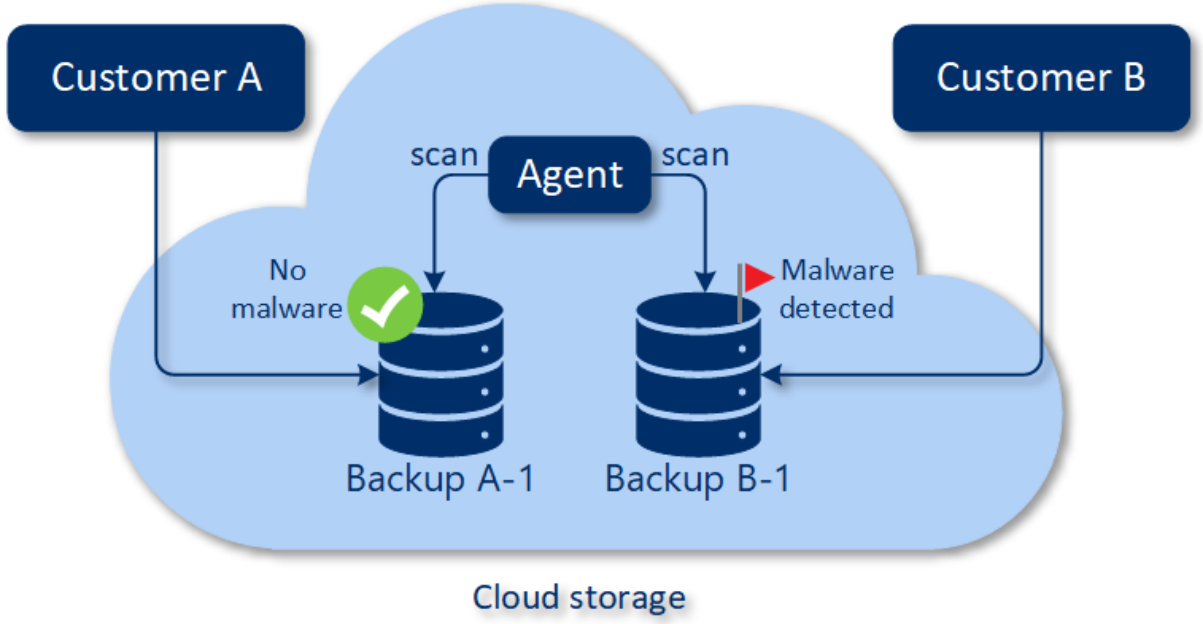
注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

若要執行防惡意軟體掃描，您必須設定備份掃描計劃.有關更多如何執行此操作的詳細資訊，請參閱 "備份掃描計劃" (第 210 頁)。

每個備份掃描計劃都會針對雲端代理程式建立一個掃描工作，並將此工作新增到佇列中，每個資料中心一個。掃描工作會根據其在佇列中的順序來處理。此外，掃描時間端視備份大小而定。這就是建立備份掃描計劃和完成掃描之間會有延遲的原因。

您選擇要掃描的備份可以為下列狀態之一：

- 未掃描
- 無惡意程式碼
- 偵測到惡意程式碼



您可以在 **[備份掃描詳細資料 (威脅)]** 桌面小工具中，檢查備份掃描的結果。您可以在 Cyber Protect 主控台的 **[監控]** > **[概觀]** 索引標籤中找到它。

限制

- 下列工作負載的 **[整部電腦]** 或 **[磁碟/磁碟區]** 備份支援防惡意軟體掃描：
  - 已安裝保護代理程式的 Windows 電腦。
  - Hyper-V 用代理程式和 VMware 用代理程式 (Windows) 在 Hypervisor 層級備份 (無代理程式備份) 的 Windows 虛擬機器。

  虛擬裝置 (例如 VMware 用代理程式 (虛擬裝置)、Virtuozzo 用代理程式、Scale Computing HC3 用代理程式、Azure 用代理程式和 oVirt 用代理程式) 建立的備份不支援防惡意軟體掃描。
- 只會掃描具有 NTFS 檔案系統，以及 GPT 或 MBR 磁碟分割的磁碟區。

- 僅支援預設雲端儲存空間作為備份位置。不支援本機儲存空間和合作夥伴擁有的雲端儲存空間。
- 在合規模式下，租用戶不支援防惡意軟體掃描。
- 當您選擇要掃描的備份時，可以選擇包含連續資料保護 (CDP) 備份的備份集。但是，系統只會掃描這些備份集中的非 CDP 備份。如需有關 CDP 備份的詳細資訊，請參閱 "連續資料保護 (CDP)" (第 363 頁)。
- 當您對整部電腦執行安全復原時，可以選擇包含 CDP 備份的備份集。但是，此復原作業將不會使用 CDP 備份中的資料。若要復原 CDP 資料，請執行額外的 **[檔案/資料夾]** 復原作業。

使用進階保護功能

根據預設，Cyber Protect 包含涵蓋大多數網路安全威脅的功能。不需要額外的費用，您就可以使用這些功能。此外，您也可以啟用進階功能增強對工作負載的保護。

- 如果啟用進階保護功能供您使用，則該功能會出現在以進階功能圖示  標示的保護計劃中。
- 如果您無法使用進階保護功能，請聯絡您的系統管理員以啟用所需的進階保護套件。
- 如果系統管理員讓您購買額外的安全性套件，您可以選擇啟用進階功能。此時會出現一則訊息提示您進入一個畫面，通知您需要支付額外費用。

注意事項

如果至少已啟用一個功能，則您必須購買對應的 [進階保護] 套件。

注意事項

如果在您的保護計劃上停用所有進階功能，則會停用對應的 [進階保護] 套件。

進階保護套件	進階保護功能
Advanced Backup	持續保護工作負載，並確保不會失去工作的最新變更。功能包括： • 單鍵復原 • 連續資料保護 • Microsoft SQL Server 叢集和 Microsoft Exchange 叢集的備份支援 – Always On 可用性群組 (AAG) 和資料庫可用性群組 (DAG) • MariaDB、MySQL、Oracle DB 和 SAP HANA 的備份支援 • 資料保護圖和合規性報告 • 脫離主機資料處理 • Microsoft 365 與 Google Workspace 工作負載的備份頻率 • 可開機媒體的相關遠端作業 • 直接備份至 Microsoft Azure、Amazon S3 和 Wasabi 公有雲端儲存空間
Advanced Security + XDR	Advanced Security + XDR 套件包括 "Extended Detection and Response (XDR)" (第 862 頁)、"Endpoint Detection and Response (EDR)" (第 793 頁) 和 [受管理的偵測與回應 (MDR)]，可持續保護您的工作負載免受所有惡意軟體威脅。功能包括： • 與協力廠商解決方案整合，包括 Perception Point、Microsoft 365 協同作業應用程式和 Microsoft Entra ID • 在集中式的 [案件] 頁面中管理案件 • 將案件的範圍和影響視覺化 • 建議和修復步驟 • 使用威脅摘要對您的工作負載檢查公開披露的攻擊 • 儲存安全性事件 180 天 • 包含本機特徵比對偵測的防毒和防惡意程式保護 (含即時保護) • 漏洞利用防禦 • URL 篩選

	• 端點防火牆管理 • 鑑識備份、惡意程式碼的掃描備份、安全復原、公司允許名單 • 智慧型保護計劃 (與 CPOC 警示整合) • 惡意程式碼的集中備份掃描 • 遠端抹除 • Microsoft Defender 防毒軟體 • Microsoft Security Essentials
Advanced Management	讓您修補受保護工作負載上的弱點。功能包括： • 修補程式管理 • 磁碟健全狀況 • 軟體清查 • 故障安全的修補程式 • 網路指令碼撰寫 • 遠端協助 • 檔案傳輸與共用 • 選擇要連線的工作階段 • 以多重檢視觀察工作負載 • 連線模式：控制、僅檢視和窗簾 • 透過快速協助應用程式的連線 • 遠端連線通訊協定：NEAR 與 Apple 畫面共用 • NEAR 連線的工作階段錄製 • 螢幕擷取畫面傳輸 • 工作階段歷程記錄報告 • 24 個監視器 • 基於閾值的監控 • 基於異常的監控
Advanced Data Loss Prevention	防止從受保護的工作負載洩漏機密資訊。功能包括： • 內容感知透過週邊裝置和網路通訊，防止工作負載導致資料遺失 • 預先組建的自動偵測個人識別資訊 (PII)、受保護的健康資訊 (PHI) 和支付卡行業資料安全標準 (PCI DSS) 資料，以及「標記為機密」類別的文件 • 透過選擇性終端使用者協助，自動建立資料外洩防護原則 • 以自動學習為基礎的原則調整功能，執行調適性資料外洩防護 • 雲端式集中稽核記錄、警示和終端使用者通知

Advanced Data Loss Prevention

Advanced Data Loss Prevention 模組會分析受保護工作負載上資料傳輸的內容和環境，並根據資料流程原則，防止透過週邊裝置或公司網路內外的網路傳輸，洩漏敏感資料。

如果為此客戶啟用保護服務和 Advanced Data Loss Prevention 套件，則可以將 Advanced Data Loss Prevention 功能包含在客戶租用戶的任何保護計劃中。

開始使用 [Advanced Data Loss Prevention] 模組之前，請確認您閱讀並瞭解基礎指南中所述之 Advanced DLP 管理的基本概念和邏輯。

您也可以檢閱技術規格文件。

建立資料流程原則和原則規則

資料洩漏防禦的主要原則要求應該允許公司 IT 系統的使用者僅在執行其工作職責所需的範圍內，處理敏感資料。其他任何敏感資料傳輸 (與業務流程不相關) 應該遭到封鎖。因此，區分與業務相關的資料傳輸和欺詐資料傳輸或流程至關重要。

資料流程原則包含指定允許哪些資料流程以及禁止哪些資料流程的規則，從而在保護計劃中啟用 [資料洩漏防禦] 模組並在 [執行] 模式下執行時，防止未經授權傳輸機密資訊。

原則中的每個敏感度類別都包含一個預設規則 (以星號 (*) 標示) 以及一個或多個明確 (非預設) 規則 (用於定義特定使用者或群組的資料流程)。在基礎指南中閱讀更多關於原則規則類型的資訊。

在觀察模式下執行 Advanced Data Loss Prevention 時，通常會自動建立資料流程原則。建立代表性資料流程原則所需的時間大約是一個月，但根據您組織的業務流程，可能有所不同。資料流程原則也可以由公司或單位系統管理員手動建立、設定或編輯。

若要開始自動建立資料流程原則

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 導覽至 **[管理]** > **[保護計劃]**。
3. 按一下 **[建立計劃]**。
4. 展開 **[資料洩漏防禦]** 區段，然後按一下 **[模式]** 列。
5. 在 [模式] 對話方塊中，選擇 **[觀察模式]**，然後選擇處理資料傳輸的方式：

選項	描述
全部允許	從使用者工作負載進行的所有敏感資料傳輸都會被視為業務流程所需，而且安全無虞。系統會針對不符合原則中已定義規則的每個偵測到的資料流程，建立一個新規則。
全部證明	從使用者工作負載進行的所有敏感資料傳輸都會被視為業務流程所需，但是有風險。因此，每次將敏感資料傳輸至不符合先前所建立資料流程的任何收件者或目的地 (組織內部和外部) 遭到攔截時，使用者都必須提供一次性的業務理由。提交理由後，就會在資料流程原則中建立一個新的資料流程規則。
混合	系統會針對所有內部敏感資料流程套用 [允許所有邏輯]，並針對所有外部資料流程套用 [證明所有邏輯]。 **注意事項** 如需有關內部和外部資料的詳細資訊，請參閱自動偵測目的地

6. 儲存保護計劃並將其套用至您要從中收集資料的工作負載以建立原則。

注意事項
在觀察模式期間無法防止資料洩漏。

若要手動設定資料流程原則

1. 在 Cyber Protect 主控台中，導覽至 **[保護]** > **[資料流程原則]**。
2. 按一下 **[新增資料流程規則]**。
   [新增資料流程規則] 窗格隨即在右側展開。
3. 選擇敏感度類別、新增寄件者和收件者，然後針對所選類別、寄件者和收件者，定義資料傳輸的權限。

選項	描述
允許	允許此寄件者將這個敏感度類別的資料傳輸給此收件者。
例外	不允許此寄件者將這個敏感度類別的資料傳輸給此收件者，但允許寄件者針對特定傳輸提交規則的例外。 當此寄件者嘗試將這個敏感度類別的資料傳輸給此收件者時，封鎖傳輸，並要求寄件者提交例外以允許此次傳輸。提交例外之後，就允許繼續進行資料傳輸。 **重要事項** 提交例外之後，將允許此寄件者與這個敏感度類別的收件者之間所有後續的資料傳輸。
拒絕	不允許此寄件者將這個敏感度類別的資料傳輸給此收件者，而且不允許寄件者要求規則的例外。

4. (選用) 選擇在觸發規則時應該執行的動作。

動作	描述
在記錄中寫入	觸發規則時，在稽核記錄中儲存事件記錄。建議針對具有 **[例外]** 權限的規則選擇此動作。
產生警示	觸發規則時，在 Cyber Protect **[警示]** 索引標籤中產生警示。如果針對系統管理員啟用通知，也將傳送電子郵件通知。
資料傳輸遭到拒絕時通知終端使用者	當使用者觸發規則時，以畫面上的警告即時通知他們。

5. 按一下 **[儲存]**。
6. 重複步驟 2 到 5 以便為不同敏感度類別和選項建立多個規則，並確認所產生的規則對應到您選擇的選項。

資料流程原則結構

在 **[資料流程原則]** 檢視中，原則規則會根據其所控制的敏感資料類別分組。敏感度類別識別碼會顯示在原則規則群組的正上方。

- 敏感
  - 受保護的健康資訊 (PHI)
  - 個人識別資訊 (PII)
  - 支付卡產業資料安全標準 (PCI DSS),
  - 已標示為機密
- 非敏感

如需有關資料流程原則概念和功能的詳細資訊，請參閱基礎指南。

規則結構

每個原則規則都包含下列元素。

- **敏感度類別**
  - **受保護的健康資訊 (PHI)**
  - **個人識別資訊 (PII)**
  - **支付卡產業資料安全標準 (PCI DSS)**
  - **已標示為機密**

    請參閱 "敏感資料定義" (第 781 頁)
- **寄件者** - 指定受此規則控制之資料傳輸的起始端。它可能是單一使用者、使用者清單或使用者群組。
  - **任何內部** - 包含組織所有內部使用者的使用者群組。
  - **聯絡人/寄件者組織** - 組織中的 Windows 帳戶，由 Advanced Data Loss Prevention 以及特定 Windows 帳戶先前使用過的其他所有帳戶 (包括第三方通訊應用程式所使用的帳戶) 識別。
  - **聯絡人/自訂身分識別** - 以下列其中一種格式指定的內部使用者識別碼：電子郵件、Skype ID、ICQ 識別碼、IRC 識別碼、Jabber 電子郵件、Mail.ru Agent 電子郵件、Viber 電話號碼、Zoom 電子郵件。

    下列萬用字元可以用於指定一組聯絡人：
    - ***** - 任意數目的符號
    - **?** - 任何單一符號
- **收件者** - 指定受此規則控制之資料傳輸的目的地。它可能是單一使用者、使用者清單或使用者群組，以及以下所指定的其他類型目的地。
  - **任何** - Advanced DLP 支援的任何收件者類型。
  - **聯絡人/任何聯絡人** - 任何內部或外部聯絡人。
  - **聯絡人/任何內部聯絡人** - 任何內部使用者的聯絡人 (請參閱 "自動偵測目的地" (第 781 頁))。
  - **聯絡人/任何外部聯絡人** - 任何外部人員或實體的聯絡人。
  - **聯絡人/寄件者組織** - 與 [寄件者] 欄位中描述的原則相同。
  - **聯絡人/自訂身分識別** - 與 [寄件者] 欄位中描述的原則相同。
  - **檔案共用服務** - 受控制的檔案共用服務識別碼。
  - **社群網路** - 受控制的社群網路識別碼。
  - **主機/任何主機** - Advanced DLP 視為內部或外部的任何電腦。
  - **主機/任何內部主機** - Advanced DLP 視為內部的任何電腦。
  - **主機/任何外部主機** - Advanced DLP 視為外部的任何電腦。

- **主機/特定主機** - 指定為主機名稱的電腦識別碼 (例如FQDN) 或 IP 位址 (IPv4 或 IPv6)。
- **裝置/任何裝置** - 連線到工作負載的任何週邊裝置。
- **裝置/外部儲存裝置** - 連線到工作負載的卸除式儲存裝置或重新導向的對應磁碟機。
- **裝置/加密的卸除式裝置** - 使用 BitLocker To Go 加密的卸除式儲存裝置。
- **裝置/重新導向的剪貼簿** - 連線到工作負載的重新導向的剪貼簿。
- **印表機** - 連線到工作負載的任何本機或網路印表機。

- **權限** - 透過此規則控制的資料傳輸執行的預防性控制。詳述於主題資料流程原則規則中的權限。
- **動作** - 觸發此規則時執行的非預防性動作。根據預設，此欄位設定為 [無動作]。這些選項包括：
  - **在記錄中寫入** - 觸發規則時，在稽核記錄中儲存事件記錄。
  - **資料傳輸遭到拒絕時通知終端使用者** - 觸發規則時，以畫面上的即時警告通知使用者。
  - **產生警示** - 觸發規則時，警示系統管理員。

警告！
選擇**無動作**且觸發該規則後：
- 不會將任何事件記錄新增至稽核記錄；
- 不會將任何警示傳送給系統管理員；
- 不會向終端使用者顯示任何螢幕上的通知。

什麼會觸發原則規則？

如果下列所有條件都成立，則表示資料傳輸符合資料流程原則規則：

- 此資料傳輸的所有寄件者都有列出或屬於規則的 **[寄件者]** 欄位中指定的使用者群組。
- 此資料傳輸的所有收件者都有列出或屬於規則的 **[收件者]** 欄位中指定的使用者群組。
- 要傳輸的資料符合規則的**敏感度類別**。

調整資料流程原則規則中的權限

Advanced Data Loss Prevention 支援資料流程原則規則中的三種權限。這些權限是在每個原則規則中個別設定的。

允許 (許可)
允許符合在規則中定義之敏感度類別、寄件者和收件者組合的資料傳輸。

例外 (禁止)
不允許符合在規則中定義之敏感度類別、寄件者和收件者組合的資料傳輸，但是寄件者可以提交規則的例外以允許特定傳輸。

重要事項
提交例外之後，將允許此寄件者與這個敏感度類別的收件者之間所有後續的資料傳輸。

拒絕 (禁止)
不允許符合在規則中定義之敏感度類別、寄件者和收件者組合的資料傳輸，而且寄件者無法選擇提交例外。

此外，還可以將優先順序旗標指派給 **[允許]** 和 **[例外]** 權限，以提高原則管理的靈活度。您可以透過這個設定，在原則的其他資料流程規則中，覆寫針對特定群組設定的權限。您可以使用該權限，將群組資料流程規則僅套用到其部分成員。為達到此目的，您必須針對您要從群組規則中排除的特定使用者，建立資料流程規則，然後將其權限的優先順序設定為高於在規則中，針對這些使用者所屬群組設定的資料流程限制。如需結合規則時權限優先順序的相關資訊，請參閱 "結合資料流程原則規則" (第 775 頁)。

重要事項

將公司或單位原則從 [觀察] 模式切換到 [執行] 模式之前，將每個敏感資料類別的預設規則從許可狀態調整為禁止狀態。在 **[資料流程原則]** 檢視中，預設規則會以星號 (*) 標示。在基礎指南中閱讀更多關於原則規則類型的資訊。

若要編輯原則規則中的權限

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 導覽至 **[保護]** > **[資料流程原則]**。
3. 選擇您想要編輯的原則規則，然後按一下規則清單上方的 **[編輯]**。
   [編輯資料流程規則] 視窗隨即開啟。
4. 在 **[權限]** 區段中，選擇 **[允許]**、**[例外]** 或 **[拒絕]**。
5. (選用) 若要將此規則的 **[允許]** 或 **[例外]** 權限優先順序設定為高於其他規則中的權限，請選擇 **[優先]** 核取方塊。
   您不需要使用此核取方塊，將資料流程規則的優先順序設定為高於預設的 [任何] > [其他規則]，因為其在原則中的優先順序預設為最低。
   如需結合規則時權限優先順序的相關資訊，請參閱 "結合資料流程原則規則" (第 775 頁)。
6. (選用) 選擇要在觸發規則時執行的動作。
7. 將變更儲存至原則規則。

結合資料流程原則規則

當資料傳輸符合多個規則時，會結合並套用針對所有規則設定的權限和動作，如下所示。

權限

如果資料傳輸符合多個規則，而且這些規則對於相同資料類別的權限不同，則根據下列權限優先順序清單 (以遞減順序排序)，覆寫規則是優先順序較高的權限：

1. 具有 **[優先]** 旗標的例外
2. 具有 **[優先]** 旗標的允許
3. 拒絕
4. 例外
5. 允許

如果資料傳輸符合多個規則，而且這些規則對於不同資料類別的權限不同，則會套用下列邏輯以進行覆寫：

1. 系統會針對資料傳輸符合的每個敏感度類別，定義最嚴格的規則權限。
2. 系統會強制執行在第 1 點定義的最嚴格規則權限。

範例

檔案傳輸符合不同敏感度類別中的三個規則，如下所示：

敏感度類別	權限
PII	允許 - 優先
PHI	例外 - 優先
PCI	拒絕

將套用的權限為 [拒絕]。

動作

如果資料傳輸符合多個規則，而且這些規則已在 **[動作]** 欄位中設定不同的選項，則會執行所有觸發的規則中所有已設定的動作。

原則檢閱與管理

在執行自動建立的基準資料流程原則之前，該原則必須經過客戶的檢閱、驗證和核准，因為客戶本身才知道其業務流程的所有特點，而且可以評估這些流程在基準原則中，是否以一致的方式解譯。此外，客戶可以識別不準確之處，然後由合作夥伴系統管理員修正。

在原則檢閱期間，合作夥伴系統管理員會將基準資料流程原則呈現給客戶，讓客戶檢閱原則中的每個資料流程，並驗證與其業務流程的一致性。驗證不需要任何技術上的技能，因為 Cyber Protect 主控台中顯示的原則規則非常直覺式：每個規則都會描述敏感資料流程的寄件者和收件者是誰。

根據客戶的指示，合作夥伴系統管理員會透過編輯、刪除和建立資料流程原則規則，手動調整基準原則。客戶核准後，就會將已套用到這些工作負載的保護計劃切換到 [執行] 模式，以便對受保護的工作負載執行經過檢閱的原則。

執行經過檢閱的原則之前，請務必在所有針對敏感資料類別自動建立的預設原則規則中，將 **[允許]** 權限變更為 **[拒絕]** 或 **[例外]**。使用者無法覆寫 **[拒絕]** 權限，而 **[例外]** 權限則會封鎖符合規則的所有傳輸，但允許使用者在緊急情況下，透過提交業務相關例外來覆寫封鎖。

資料流程原則更新

當公司或其單位的業務流程發生重大變更時，必須更新其 DLP 原則，使其與所更新業務流程敏感資料流程中的變更保持一致。如果員工的工作角色變更，也需要更新原則。在此案例中，也必須更新用於保護員工工作負載的單位原則部分。

Advanced DLP 原則管理工作流程可讓系統管理員針對整個公司、單位、使用者或單位中的部分使用者，自動更新原則。

更新公司或單位的原則

[觀察] 模式的所有選項都可以用來更新整個公司或整個單位的原則，以及單位中一或多個使用者的部分單位原則。

若要更新公司或單位的原則

更新程序包含下列步驟，公司系統管理員或管理公司工作負載的合作夥伴都必須完成這些步驟。

1. 刪除強制執行原則中的所有非預設規則。
2. 若要開始更新，請根據最適合此特定公司或單位的選項，將已將 Advanced DLP 套用到公司或單位的保護計劃切換到其中一個觀察模式選項，然後將該計劃套用到該公司或單位中的所有工作流程。
3. 當更新期間結束後，與客戶一起檢閱新的公司或單位原則、必要時進行調整，然後獲得客戶核准。
4. 將已套用到公司或單位工作負載的保護計劃切換到適當的執行模式選項，客戶會將此選項視為最適合防止資料從單位的工作負載洩漏。

更新公司或單位中一或多個使用者的原則

您可以使用 [觀察] 模式的任何選項以及調適型執行模式，更新使用者層級的原則。

使用觀察模式來更新使用者原則

使用觀察模式來更新公司 (或單位) 中某個使用者或部分使用者的原則具備下列特點：在更新期間，不會透過使用者的資料傳輸，執行對整個公司 (或單位) 執行的資料流程原則。因此，可以在更新期間為使用者建立個別的規則，這些規則可能會公司 (或單位) 執行政策中的現有群組規則互相矛盾或相符。完成更新並透過使用者的資料傳輸重新執行原則之後，這些為使用者建立的新個別規則實際上是否會套用至使用者的資料傳輸，取決於其與這些資料傳輸相符之原則中其他規則相比的優先順序。

若要透過觀察模式更新使用者的原則

更新程序包含下列步驟，公司系統管理員或管理公司工作負載的合作夥伴都必須完成這些步驟。

1. 在針對將使用者當作其單一寄件者的公司 (或單位) 執行的原則中，刪除所有非預設規則。
2. 從已執行的原則中所有非預設資料流程規則的寄件者清單移除使用者。
3. 在觀察模式下，使用 Advanced DLP 建立新的保護計劃，並將其套用至使用者的工作負載，以開始更新 (觀察) 期間。
   更新期間的持續時間取決於使用者完成全部或 90-95% 從工作負載傳輸敏感資料相關定期業務活動可能需要的時間。
4. 當更新期間結束後，檢閱與已新增至強制原則的這個使用者相關的新規則、必要時進行調整，然後獲得客戶核准。
5. 將已套用到使用者工作負載的保護計劃切換到 **[嚴格執行]** 模式或 **[調適型執行]** 模式，端視客戶將哪個選項視為最適合防止資料從使用者的工作負載洩漏而定。
   或者，您可以將已套用到公司 (或單位) 的保護計劃重新套用到使用者的工作負載。

使用調適型執行模式來更新使用者原則

在 Advanced DLP 已套用至使用者工作負載的情況下，使用保護計劃的 [調適型執行] 模式可以對公司 (或單位) 中的單一使用者或部分使用者執行原則更新。

注意事項

此原則更新方法具備下列特點：對於具有使用者成員資格 (亦即，任何內部) 的寄件者群組，已執行的公司 (單位) 原則在更新期間，也會透過從此使用者進行資料傳輸來執行。因此，更新將不會為使用者建立與這些寄件者群組現有原則互相矛盾或相符的新個別規則。在這兩個方法中，哪個方法對於特定客戶的使用者原則更新更有效率，取決於其具體的 IT 安全性需求

若要透過調適型執行模式更新使用者的原則

更新程序包含下列步驟，公司系統管理員或管理公司工作負載的合作夥伴都必須完成這些步驟。

1. 在針對將使用者當作其單一寄件者的公司 (單位) 執行的原則中，刪除所有非預設規則。
2. 從已執行的原則中所有非預設資料流程規則的寄件者清單移除使用者。
3. 針對為公司 (或單位) 執行的原則中的所有預設規則，將其權限設定為 **[例外]**，然後在 **[動作]** 欄位中，選擇 **[在記錄中寫入]** 動作。
4. 如果目前已套用到使用者工作負載的保護計劃設定為 **[嚴格執行]** 模式，請使用 Advanced DLP 建立新的保護計劃，並在 **[調適型執行]** 模式下，將其套用到使用者的工作負載，以開始更新期間。
   更新期間的持續時間取決於使用者完成全部或 90-95% 從工作負載傳輸敏感資料相關定期業務活動可能需要的時間。
5. 當更新期間結束後，檢閱與已新增至強制原則的這個使用者相關的新規則、必要時進行調整，然後獲得客戶核准。
6. 將已套用到使用者工作負載的保護計劃切換到 **[嚴格執行]** 模式或留在 **[調適型執行]** 模式，端視客戶將哪個選項視為最適合防止資料從使用者的工作負載洩漏而定。
   或者，您可以將已套用到公司 (或單位) 的保護計劃重新套用到使用者的工作負載。

在保護計劃中啟用 Advanced Data Loss Prevention

如果為此客戶啟用保護服務和 Advanced Data Loss Prevention 套件，則可以將 Advanced Data Loss Prevention 功能包含在客戶租用戶的任何保護計劃中。

Advanced DLP 是資料外洩防護功能群組的進階模組。[Advanced DLP] 功能和 [裝置控制] 可以獨立使用，也可以一起使用 (在單一保護計劃中，或在保護相同工作負載的兩個計劃中)。如果一起使用，其功能協調如下。

- [裝置控制] 會停止控制使用者對 Advanced DLP 檢查傳輸資料內容所在本機通道的存取。辦事，如果這些本機通道被設定為 [唯讀] 或 [拒絕存取]，則 [裝置控制] 仍保留對以下裝置類型的控制：
  - 抽取式
  - 加密的卸除式
  - 對應的磁碟機

例如，如果您在單一保護計劃或在保護相同工作負載的兩個計劃中同時啟用 [裝置控制] 和 [Advanced DLP]，而且您在 [裝置控制] 中為 USB 裝置設定了 [唯讀] 存取權，則無論 Advanced DLP 模組中的存取設定為何，[唯讀] 存取權將會套用到所有 USB 裝置，但允許名單中的 USB 裝置除外。如果在 [裝置控制] 中設定了預設的 [啟用存取]，則將會套用 Advanced DLP 中的存取設定。

- 裝置控制會執行使用者對允許名單中下列邏輯通道和週邊裝置的存取：
  - 光碟機
  - 軟碟機
  - 連線 MTP 的行動裝置
  - 藍牙介面卡
  - Windows 剪貼簿
  - 螢幕擷取畫面擷取
  - USB 裝置和裝置類型 (但卸除式儲存裝置和加密裝置除外)

若要使用 Advanced DLP 建立保護計劃

1. 導覽至 **[管理]** > **[保護計劃]**。
2. 按一下 **[建立計劃]**。
3. 展開 **[資料洩漏防禦]** 區段，然後按一下 **[模式]** 列。
   [模式] 對話方塊隨即開啟。
   - 若要開始建立或更新資料流程原則，請選擇 **[觀察模式]**，然後選擇處理資料傳輸的方式：

選項	描述
全部允許	從使用者工作負載進行的所有敏感資料傳輸都會被視為業務流程所需，而且安全無虞。系統會針對不符合原則中已定義規則的每個偵測到的資料流程，建立一個新規則。
全部證明	從使用者工作負載進行的所有敏感資料傳輸都會被視為業務流程所需，但是有風險。因此，每次將敏感資料傳輸至不符合先前所建立資料流程的任何收件者或目的地 (組織內部和外部) 遭到攔截時，使用者都必須提供一次性的業務理由。提交理由後，就會在資料流程原則中建立一個新的資料流程規則。
混合	系統會針對所有內部敏感資料傳輸套用 [允許所有邏輯]，並針對所有外部敏感資料傳輸套用 [證明所有邏輯]。 如需內部目的地的定義，請參閱 "自動偵測目的地" (第 781 頁)

警告！

- 只有在您之前未建立資料流程原則或您要更新原則時，才選擇 **[觀察模式]**。在您開始更新原則之前，請參閱 "資料流程原則更新" (第 776 頁)。
- 在觀察模式下無法防止資料洩漏。請參閱 《基礎指南》中的觀察模式。

   - 若要執行現有的資料流程原則，請選擇 **[執行模式]**，然後選擇執行資料流程原則規則的嚴格程度：

選項	描述
嚴格執行	資料流程原則以原樣執行，而且在偵測到之前未觀察到的敏感資料流程時，不會使用新的權限原則規則進行擴展。請參閱 《基礎指南》中的嚴格執行。
調適型執行 (透過學習來執行)	已執行的原則會繼續自動適應在觀察期間未執行的業務作業或業務流程的變化。此模式可讓已執行的資料流程原則根據在工作負載上偵測到新學到的資料流程，進行擴充。請參閱 《基礎指南》中的調適型執行。

重要事項
將公司或單位原則從 [觀察] 模式切換到 [執行] 模式之前，將每個敏感資料類別的預設規則從許可狀態調整為禁止狀態。在 **[資料流程原則]** 檢視中，預設規則會以星號 (*) 標示。在基礎指南中閱讀更多關於原則規則類型的資訊。

4. 按一下 **[完成]**，關閉 [模式] 對話方塊。
5. (選用) 若要設定光學字元辨識、允許名單以及其他保護選項，按一下 **[進階設定]**。
   如需可用選項的相關資訊，請參閱 "進階設定" (第 780 頁)。
6. 儲存保護計劃並將其套用至您要保護的工作負載。

進階設定

您可以使用保護計劃中的進階設定搭配 Advanced Data Loss Prevention，以提高 Advanced Data Loss Prevention 所控制之通道中資料內容檢查的品質，並從任何預防性控制中，排除對允許名單中的週邊裝置類型、網路通訊類別、目的地主機起始的資料傳輸，以及由允許名單中應用程式起始的資料傳輸。您可以設定下列進階設定：

- **光學字元辨識**
  此設定可開啟或關閉光學字元辨識 (OCR)，以便從文件、訊息、掃描、螢幕擷取畫面與其他物件中的圖形檔案和影像擷取 31 種語言的片段文字，以進行進一步的內容檢查。
- **傳輸受密碼保護的資料**
  無法檢查受密碼保護之存檔和文件的內容。透過此設定，Advanced DLP 可讓系統管理員選擇允許還是封鎖受密碼保護資料的傳出傳輸。
- **防止發生錯誤時傳輸資料**
  有時候正在傳送的內容分析可能會失敗，或者在 DLP 代理程式操作時可能會發生其他控制錯誤。若啟用此選項，將會封鎖傳輸。若停用此選項，即使發生錯誤，也會允許傳輸。
- **裝置類型和網路通訊的允許名單**
  無論資料的敏感度和強制執行的資料流程原則為何，都允許將資料傳輸到此清單中勾選的週邊裝置類型和網路內通訊類型。

警告！
如果發生特定裝置類型或通訊協定問題，會使用此選項。除非支援代表建議，否則請不要啟用該選項。

- **遠端主機的允許名單**
  無論資料的敏感度和強制執行的資料流程原則為何，都允許將資料傳輸到此清單中指定的目的地主機。
- **應用程式的允許名單**
  無論資料的敏感度和強制執行的資料流程原則為何，都允許此清單中指定的應用程式執行資料傳輸。

在 **[建立保護計劃]** 檢視以及保護計劃 [詳細資料] 檢視中顯示之 [進階] 設定的 **[安全性層級]** 指標具備下列層級跡象的邏輯：

- **[基本]** 表示未開啟任何進階設定。
- **[中度]** 表示已開啟一或多個設定，但未啟用 **[OCR]**、**[傳輸受密碼保護的資料]** 和 **[防止發生錯誤時傳輸資料]** 的組合。
- **[嚴格]** 表示至少已啟用 **[OCR]**、**[傳輸受密碼保護的資料]** 和 **[防止發生錯誤時傳輸資料]** 的組合。

自動偵測目的地

在 [混合觀察] 模式下，Advanced Data Loss Prevention 會根據偵測到的資料傳輸目的地 (內部或外部) 而套用不同的規則。判斷目的地為內部的邏輯如下所述。其他所有目的地都被視為外部。

針對每個攔截的資料傳輸，Advanced Data Loss Prevention 會透過執行 DNS 要求，並比較執行資料洩漏防禦代理程式所在電腦和遠端伺服器的 FQDN 名稱，以自動偵測目的地 HTTP、FTP 或 SMB 伺服器是否為內部。如果 DNS 要求失敗，其也會檢查受保護的工作負載和遠端伺服器是否在相同的網路中。網域名稱與執行資料洩漏防禦代理程式所在電腦相同 (或位於相同子網路) 的伺服器會被視為內部。

對於電子郵件通訊，如果收件者電子郵件與寄件者電子郵件位於相同的網域，且收件者郵件伺服器名稱相同，則 Advanced Data Loss Prevention 會將使用公司郵件伺服器，從公司電子郵件地址傳送的所有電子郵件視為內部傳輸。

除非已知收件者帳戶，否則非公司電子郵件會被視為外部通訊。當資料洩漏防禦監視網路上的使用者活動，並在後端將資料庫更新為與使用者相關聯之電子郵件地址的資料時，會更新已知電子郵件地址。

除非已知收件者帳戶，否則透過即時訊息進行的通訊會被視為外部通訊。當資料洩漏防禦監視網路上的使用者活動，並在後端將資料庫更新為與使用者相關聯之帳戶的資料時，會更新已知帳戶。

敏感資料定義

本主題描述在內容分析期間用於識別敏感資料的邏輯。

若要減少誤報的數目，針對所描述邏輯運算式的所有群組，相同的符合項目會計為一個符合項目。

重要事項
用於內容識別的邏輯運算式僅供參考，不會詳細描述解決方案。

受保護的健康資訊 (PHI)

支援語言

- 美國、英國、英文 (國際)
- 芬蘭文
- 義大利文
- 法文
- 波蘭文
- 俄文
- 匈牙利文
- 挪威文
- 西班牙文

被視為受保護的健康資訊的資料

下列資料被視為受保護的健康資訊。

- 名字和姓氏
- 地址 (街道、縣/市、區域、郵遞區號及其對等的地理代碼)
- 電話號碼
- 電子郵件地址
- 社會安全號碼
- 健康計劃受益人編號
- 銀行帳號
- URL
- IP 位址編號
- ICD-10-CM 代碼
- ICD-10-PCS-and-GEMs
- HIPAA
- 其他健康醫療相關
- 信用卡號碼

用於內容偵測的邏輯運算式

邏輯運算式包含以邏輯運算子 OR 加入的下列字串。如果未明確指定 AND 運算子，則 OR 運算子用於加入上方清單中的不同資料群組。括號中的數字表示偵測到且將傳回正面偵測結果的執行個體數目。

- **社會安全號碼** (5)
- (名字和姓氏 (3) OR 地址 (3) OR 電話號碼 (3) OR 電子郵件地址 (3) OR 銀行賬號 (3) OR 信用卡號碼 (3)) AND (社會安全號碼 (3) OR 健康計劃受益人號碼 (3) * OR ICD-10-CM 代碼 (3) OR ICD-10-PCS-and-GEMs (3) OR HIPAA (3) OR * 其他健康醫療相關 (3))

個人識別資訊 (PII)

支援語言

- 美國、英國、英文 (國際)
- 保加利亞文
- 繁體中文
- 捷克文
- 丹麥文
- 荷蘭文
- 芬蘭文
- 法文
- 德文
- 匈牙利文
- 印尼文
- 義大利文
- 韓文
- 馬來文
- 挪威文
- 波蘭文
- 葡萄牙文 (巴西)
- 葡萄牙文 (葡萄牙)
- 羅馬尼亞語
- 俄文
- 塞爾維亞文
- 新加坡
- 西班牙文
- 瑞典文
- 台灣
- 土耳其文
- 泰語
- 日文

被視為個人識別資訊 (PII) 的資料

- 名字和姓氏
- 地址 (街道、縣/市、郵遞區號)
- 銀行帳號
- 個人身分證號碼和財政 ID 號碼
- 護照號碼

- 社會安全號碼
- 電話號碼
- 車牌號碼
- 駕駛執照號碼
- 識別碼和序號
- IP 位址
- 電子郵件地址
- 信用卡號碼

用於內容偵測的邏輯運算式

用於日文之外所有支援的語言的邏輯運算式

邏輯運算式包含以邏輯運算子 OR 或 AND 加入的下列字串。括號中的數字表示偵測到且將傳回正面偵測結果的執行個體數目。

- 個人身分證號碼和財政 ID 號碼 (5)
- 名字和姓氏 (3) AND **(**信用卡號碼 (3) OR 社會安全號碼 (3) OR 銀行帳號 (3) OR 個人身分證號碼和財政 ID 號碼 (3) OR 駕駛執照號碼 (3) OR 護照號碼 (3) OR 社會安全號碼 (3) OR IP 位址 (3) OR 車牌號碼 (3) OR 識別碼和序號**)**
- 電話號碼 (3) AND **(**信用卡號碼 (3) OR 社會安全號碼 (3) OR 銀行帳號 (3) OR 地址 (3) OR 個人身分證號碼和財政 ID 號碼 (3) OR 駕駛執照號碼 (3) OR 護照號碼 (3) OR 社會安全號碼 (3) OR 車牌號碼 (3) OR 識別碼和序號 (3)**)**
- **(**名字和姓氏 (30) OR 地址 (30)**)** AND **(**電子郵件地址 (30) OR 電話號碼 (30) OR IP 位址 (30)**)**
- 電子郵件地址 (3) AND **(**信用卡號碼 (3) OR 社會安全號碼 (3) OR 銀行帳號 (3) OR 個人身分證號碼和財政 ID 號碼 (3) OR 駕駛執照號碼 (3) OR 護照號碼 (3) OR 社會安全號碼 (3) OR 車牌號碼 (3) OR 識別碼和序號 (3)**)**
- 電子郵件地址 (30) AND **(**地址 (30) OR 電話號碼 (30)**)**
- 名字和姓氏 (30) AND 地址 (30)
- 電話號碼 (30) AND 地址 (30)
- 名字和姓氏 (3) AND 銀行帳號 (3)
- 電話號碼 (3) AND **(**信用卡號碼 (3) OR 銀行帳號 (3) OR 社會安全號碼 (3) OR 個人身分證號碼和財政 ID 號碼 (3) OR 駕駛執照號碼 (3) OR 護照號碼 (3)**)**

用於日文的邏輯運算式

注意事項
內容偵測只會計算獨特的相符項目。

邏輯運算式包含以邏輯運算子 OR 加入的下列字串。如果未明確指定邏輯運算子 AND, 則運算子 OR 用於加入不同的群組。

- 社會安全號碼 (5)
- 名字和姓氏 (3) AND **(**信用卡號碼 (3) OR 銀行帳號 (3) OR 駕駛執照號碼 (3) OR 護照號碼 (3) OR 社會安全號碼 (3)**)**
- 名字和姓氏 (30) AND **(**電子郵件地址 (30) OR 電話號碼 (30) OR IP 位址 (30) OR 地址 (30)**)**
- 地址 (3) AND **(**信用卡號碼 (3) OR 銀行帳號 (3) OR 駕駛執照號碼 (3) OR 護照號碼 (3) OR 社會安全號碼 (3)**)**
- 電子郵件地址 (3) AND **(**信用卡號碼 (3) OR 銀行帳號 (3) OR 社會安全號碼 (3) OR 駕駛執照號碼 (3)**)**
- 地址 (5) AND **(**電子郵件地址 (5) OR 名字和姓氏 (5) OR 電話號碼 (5) OR IP 位址 (5)**)**
- 名字和姓氏 (3) AND 銀行帳號 (3)
- 電話號碼 (3) AND **(**信用卡號碼 (3) OR 銀行帳號 (3) OR 地址 (3) OR 社會安全號碼 (3) OR 駕駛執照號碼 (3)**)**

支付卡產業資料安全標準 (PCI DSS)

支援語言

此敏感度群組與語言無關。所有國家/地區的 PCI DSS 資料都採用英文。

被視為 PCI DSS 的資料

- 持卡人資料
  - 主要帳號 (PAN)
  - 持卡人姓名
  - 到期日
  - 服務代碼
- 敏感驗證資料
  - 完整追蹤資料 (磁條資料或晶片上的同等資料)
  - CAV2/CVC2/CVV2/CID
  - PIN/PIN 區塊

用於內容偵測的邏輯運算式

邏輯運算式包含以邏輯運算子 OR 加入的下列字串。括號中的數字表示偵測到且將傳回正面偵測結果的執行個體數目。

- 信用卡號碼 (5)
- 信用卡號碼 (3) AND (美國名字 (Ex) (3) OR 美國名字 (3) OR PCI DSS 關鍵字 (3) OR 日期 (月/年) (3))
- 信用卡傾印 (5)

已標示為機密

標示為機密的資料是透過關鍵字群組偵測的。

Match 條件是以權重為基礎，每個字的權重 == 1。當 Match if 權重 > 3 時，內容偵測會被視為正面的。

支援語言

- 英文
- 保加利亞文
- 簡體中文
- 繁體中文
- 捷克文
- 丹麥文
- 荷蘭文
- 芬蘭文
- 法文
- 德文
- 匈牙利文
- 印尼文
- 義大利文
- 日文
- 韓文
- 馬來文
- 挪威文
- 波蘭文
- 葡萄牙文 - 巴西
- 葡萄牙文 - 葡萄牙
- 俄文
- 塞爾維亞文
- 西班牙文
- 瑞典文
- 土耳其文

關鍵字群組

每個語言的關鍵字群組都包含以下用於英語的國家/地區專用的相等關鍵字 (不區分大小寫)。

- confidential
- internal distribution
- not for distribution
- do not distribute
- not for public
- not for external distribution
- for internal use only

- highly qualified documentation
- private
- privileged information
- for internal use only
- for official use only

資料洩漏防禦事件

Advanced Data Loss Prevention 會在 DLP 事件檢視中產生事件，如下所示。

- 在觀察模式期間，系統會針對所有已證明的資料傳輸產生事件。
- 在執行模式期間，系統會根據針對所觸發的每個原則規則設定的 **[在記錄中寫入]** 動作產生事件。

若要檢視資料流程原則中規則的事件

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 導覽至 **[保護]** > **[資料流程原則]**。
3. 找出您要檢視其事件的規則，然後按一下規則行結尾的省略符號。
4. 選擇 **[檢視事件]**。

若要在 DLP 事件檢視中檢視某個事件的詳細資料

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 導覽至 **[保護]** > **[DLP 事件]**。
3. 按一下清單中的某個事件，以檢視其詳細資料。
   [事件詳細資料] 窗格隨即在右側展開。
4. 在 [事件詳細資料] 窗格中上下捲動可檢視可用的資訊。
   顯示在窗格中的詳細資料取決於觸發事件的規則類型以及規則設定。

若要在 DLP 事件清單中篩選事件

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 導覽至 **[保護]** > **[DLP 事件]**。
3. 在左上角按一下 **[篩選]**。
4. 從下拉式功能表中選擇敏感度類別、工作負載、動作類型、使用者以及通道。
   您可以在下拉式功能表中選擇多個項目。篩選會在相同功能表中的項目之間套用邏輯運算子 OR，但在不同功能表中的項目之間使用邏輯運算子 AND。
   例如，如果您選擇 **PHI** 和 **PII** 敏感度類別，結果將傳回包含 PHI 或 PII 或兩者的所有事件。如果您選擇 **PHI** 敏感度類別以及 **[寫入存取]** 動作，則只有符合兩個類別的事件才會出現在篩選的結果中。
5. 按一下 **[套用]**。
6. 若要再次檢視所有事件，依序按一下 **[篩選]** 和 **[重設為預設值]**，最後再按一下 **[套用]**。

若要在 DLP 事件清單中搜尋事件

1. 重複以上程序中的步驟 1-2。
2. 從 [篩選] 右側的下拉式清單中，選擇您要搜尋的類別：**[寄件者]**、**[目的地]**、**[程序]**、**[訊息主旨]** 或 **[原因]**。
3. 在文字方塊中，輸入您感興趣的字詞，然後按下鍵盤上的 Enter 鍵來確認。
   只有符合您所輸入之字詞的事件才會出現在清單中。
4. 若要重設事件清單，按一下 [搜尋] 文字方塊中的 **X** 符號，然後按下 Enter 鍵。

若要檢視資料流程原則中與特定規則相關事件的清單

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 導覽至 **[保護]** > **[資料流程原則]**。
3. 選擇您感興趣的原則規則名稱前方的核取方塊。
   如果需要，您可以選擇多個原則規則。
4. 按一下 **[檢視事件]**。
   此檢視畫面會切換到 **[保護]** > **[DLP 事件]**，與您所選原則規則相關的事件就會出現在清單中。

概觀儀表板上的 Advanced Data Loss Prevention 桌面小工具

[概觀] 儀表板提供許多可自訂的桌面小工具，可概覽與 Cyber Protection 服務相關的作業，包括 Advanced Data Loss Prevention。您可以在 **[概觀]** 儀表板上的 **[監控]** 底下，找到下列 Advanced Data Loss Prevention 桌面小工具。

- **敏感資料傳輸** - 顯示傳送給內部和外部收件者的敏感資料傳輸作業總數。此圖表按權限類型劃分：已允許、已證明或已封鎖。您可以選擇所需的時間範圍 (1 天、7 天、30 天或當月) 來自訂此桌面小工具。
- **輸出敏感資料類別** - 顯示傳送給外部收件者的敏感資料傳輸總數。此圖表按敏感類別劃分：受保護的健康資訊 (PHI)、個人識別資訊 (PII)、PCI DSS 和已標示為機密 (機密)。
- **輸出敏感資料的常見寄件者** - 顯示從組織傳給外部收件者的敏感資料傳輸總數和傳輸數量最大的前五個使用者的清單 (以及這些傳輸的數量)。此統計資料包括允許的和證明的傳輸。您可以選擇所需的時間範圍 (1 天、7 天、30 天或當月) 來自訂此桌面小工具。
- **敏感資料傳輸遭封鎖的常見寄件者** - 顯示封鎖的敏感資料傳輸總數和嘗試傳輸次數最多的前五個使用者的清單 (以及這些傳輸的數量)。您可以選擇所需的時間範圍 (1 天、7 天、30 天或當月) 來自訂此桌面小工具。
- **最近的 DLP 事件** - 針對所選時間範圍顯示最近資料洩漏防禦事件的詳細資料。您可以使用下列選項自訂此桌面小工具：
  - **範圍 (張貼日期)** (1 天、7 天、30 天或當月)。
  - **工作負載**的名稱
  - **作業狀態** (已允許、已證明或已封鎖)
  - **敏感度** (PHI、PII、機密、PCI DSS)
  - **目的地類型** (外部、內部)
  - **分組** (工作負載、使用者、通道、目的地類型)

系統會每五分鐘更新一次桌面小工具。動態小工具帶有可按一下的元素，可讓您調查問題並進行疑難排解。您可以透過 .pdf 和/或 .xlsx 格式下載最新狀態的儀表板或透過電子郵件進行傳送。

自訂敏感度類別

自訂敏感資料類別可以透過擴展 Advanced DLP 內建的合規法規相關內容定義的目錄，協助組織保護專屬於該組織的智慧財產和機密資料。

若要建立自訂敏感度類別

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 導覽至 **[保護]** > **[資料洩漏防禦]** > **[資料分類器]**。
3. 選擇 **[敏感度類別]**。
4. 您將會看到敏感度清單，其中同時包含內建 (例如，受保護的健康資訊或個人識別資訊) 和自訂的類別。
5. 按一下視窗右上角的 **[建立敏感度]**。
6. 在下一個視窗中輸入其名稱。
7. 預設一律停用新的自訂敏感度。您可以在設定所有參數之後啟用這些敏感度。
8. 建立新的敏感度之後，您將需要設定其內容偵測器。按一下箭頭以展開新敏感度的內容，然後選擇 **[新增內容偵測器]**。
9. 在下一個視窗中，您可以使用任何現有的內容偵測器 (透過按一下其名稱旁的核取方塊，然後按一下右下角的 **[新增]**) 或定義新的內容偵測器。
10. 您也可以透過複製現有的內容偵測器並調整其參數以重複使用現有的內容偵測器 (內建或現有的自訂敏感度)，而不必從頭開始建立新的敏感度。
    - 若要複製現有的敏感度，按一下其名稱旁的核取方塊，然後從左上角的 [動作] 下拉式功能表 (以省略符號表示) 選擇 **[複製]**。您可以一次選擇多個項目以複製多個敏感度。
    - 在下一個視窗中，您可以按一下每個參數旁的核取方塊，來選擇您要保留之現有敏感度的參數。

    注意事項
    複製某個租用戶中的內建敏感度時，將會建立包含相同偵測器的新敏感度 (一旦複製之後，就會變成自訂敏感度)

若要建立新的內容偵測器

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 導覽至 **[保護]** > **[資料洩漏防禦]** > **[資料分類器]**。
3. 選擇 **[內容偵測器]**。
4. 您將會看到內容偵測器清單，其中同時包含內建和自訂的內容偵測器。
5. 按一下視窗右上角的 **[建立內容偵測器]**。
6. 下拉式功能表隨即開啟，您可以在其中選擇您要建立的偵測器類型，目前只提供 **[檔案類型]** 內容偵測器，之後更新將會提供更多內容偵測器。

7. 在以下視窗中，您可以設定內容偵測器。

內容偵測器類型	描述
檔案類型內容偵測器	a. 有兩個清單：**[支援的檔案類型]** 和 **[所選檔案類型]**。按一下支援的檔案類型右側的「加號」圖示，您就可以將該檔案類型移至 [所選檔案類型] 清單。您也可以透過按一下支援的檔案類型名稱旁的核取方塊，然後使用右上角的 **[新增選取的項目]** 按鈕來選擇多個支援的檔案類型。 b. 若要從 [所選檔案類型] 清單中移除某個檔案類型，請按一下其名稱右側的垃圾桶圖示。您也可以使用核取方塊和 **[移除選取的項目]** 按鈕，一次移除多個檔案類型。
關鍵字內容偵測器	a. 建立新的關鍵字內容偵測器時，您將需要從檔案匯入關鍵字。成功匯入後，您可以將合併新的關鍵字與現有關鍵字清單，或將現有的關鍵字取代為匯入的關鍵字。 b. 您也需要決定您希望內容偵測器比對清單中的所有關鍵字、清單中的任何關鍵字，還是自訂數量的關鍵字。

8. 您也可以透過複製現有的內容偵測器並調整其參數以重複使用現有的內容偵測器 (內建或現有的自訂敏感度)，而不必從頭開始建立新的內容偵測器。
   - 若要複製現有的內容偵測器，按一下其名稱旁的核取方塊，然後從左上角的 [動作] 下拉式功能表 (以省略符號表示) 選擇 **[複製]**。您可以一次選擇多個項目以複製多個內容偵測器。

注意事項
複製內建的內容偵測器會使偵測器變成自訂偵測器。

組織圖

注意事項
此功能僅可供公司系統管理員使用者存取。

組織圖是一種資料庫，其中包含遭到 Advanced DLP 攔截的使用者及其所有帳戶的資料，您可以使用這些帳戶，透過即時訊息、電子郵件或其他任何方式傳輸資料。

組織圖提供了在 Advanced DLP 中建立和管理使用者群組，以及在 Advanced DLP 中管理使用者關聯帳戶的方法。之後，使用者群組就可以用於基於群組的 DLP 原則管理。

若要尋找組織圖

- 在 Cyber Protect Cloud 主控台中，導覽至 **[保護]** > **[資料外洩防護]** > **[組織圖]**。

它如何工作？

注意事項
當 Advanced DLP 模組在 [觀察] 模式下運作時，會填入組織圖。

對於 DLP 代理程式攔截的每個資料傳輸，後端都會收集以下屬性。

屬性	描述	UI 中的標籤
組織單位	手動建立的群組。組織單元可以有一個或多個巢狀組織單元。	群組名稱，如定義
安全性 ID	唯一的安全性識別碼。	在使用者詳細資料頁面上 > **SID**
	衍生自使用者帳戶名稱的使用者易用顯示名稱。此名稱不一定可用於組織圖。	**名稱**
電腦\使用者名稱	端點 (工作負載) 的使用者名稱。 一個使用者名稱只能指派給一個組織單位。	**使用者名稱**
裝置 (工作負載)	端點 (工作負載) 的名稱。	**工作負載**
帳戶	使用者透過即時訊息和電子郵件進行通訊所使用且已遭到 DLP 代理程式攔截的帳戶。例如，如果代理程式偵測到使用者名稱 'PC\John' 使用 john@gmail.com 傳送電子郵件，則此帳戶是連結到 PC\John 使用者名稱。	**帳戶**

在組織圖中，您可以檢視和搜尋帳戶、使用者與群組，以及建立、編輯和刪除群組。

若要搜尋特定帳戶

進行事件調查時，系統管理員使用者可能需要找到與潛在資料外洩有關的特定帳戶的擁有者。

1. 在 Cyber Protect Cloud 主控台中，導覽至 **[保護]** > **[資料外洩防護]** > **[組織圖]**。
2. 在使用者清單上方的 **[搜尋]** 文字方塊中，開始輸入或貼上帳戶。
   系統會在您輸入時進行篩選。

若要搜尋特定使用者名稱

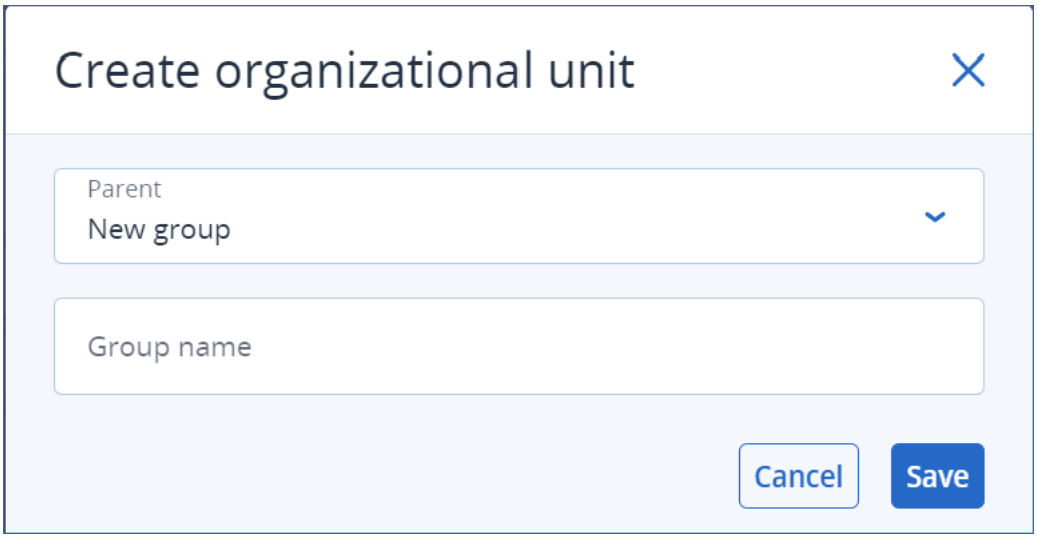
1. 在 Cyber Protect Cloud 主控台中，導覽至 **[保護]** > **[資料外洩防護]** > **[組織圖]**。
2. 若要在特定群組中搜尋，請按一下清單中的群組名稱。
3. 在使用者清單上方的 **[搜尋]** 文字方塊中，開始輸入或貼上使用者名稱。
   系統會在您輸入時進行篩選。

若要檢視特定使用者名稱使用的帳戶

1. 在使用者清單中找出使用者。
2. 按一下使用者列結尾的三個點，然後選擇 **[檢視]**。
3. 在使用者詳細資料對話方塊中，找出 **[相關聯的帳戶]** 區段。
4. 您可以在 [描述] 文字方塊中新增註解。

若要建立使用者群組

1. 在 Cyber Protect Cloud 主控台中，導覽至 **[保護]** > **[資料外洩防護]** > **[組織圖]**。
2. 在群組清單的左下方區段中，按一下 **[建立群組]**。
   [建立組織單位] 對話方塊隨即開啟。



3. 從 [父項] 下拉式功能表中，選擇新群組的內容。

注意事項
您之後無法變更父項。群組在此內容中將維持巢狀狀態。

4. 輸入群組名稱，然後按一下 **[儲存]**。

若要將使用者新增至群組

1. 在 Cyber Protect Cloud 主控台中，導覽至 **[保護]** > **[資料外洩防護]** > **[組織圖]**。
2. 在使用者清單中，找出您要新增的使用者，然後選擇使用者列開頭的核取方塊。
   [移動所選] 和 **[刪除所選]** 按鈕隨即出現在使用者清單上方。
3. 按一下 **[移動所選]**。
   [移動使用者] 對話方塊隨即開啟。
4. 為所選使用者選擇一個新的父項，然後按一下 **[儲存]**。

注意事項
一個使用者只能屬於一個群組。

若要刪除與使用者相關聯的帳戶

1. 在使用者清單中找出使用者。
2. 按一下使用者列結尾的三個點，然後選擇 **[檢視]**。
3. 在使用者詳細資料對話方塊中，找出 **[相關聯的帳戶]** 區段。
4. 找出您要刪除的帳戶，然後按一下該帳戶旁邊的三個點。
5. 從下拉式清單中選擇 **[刪除]**。

若要重新命名使用者群組

1. 在 Cyber Protect Cloud 主控台中，導覽至 **[保護]** > **[資料外洩防護]** > **[組織圖]**。
2. 按一下群組名稱旁邊的三個點，然後按一下 **[重新命名]**。

若要刪除使用者群組

1. 在 Cyber Protect Cloud 主控台中，導覽至 **[保護]** > **[資料外洩防護]** > **[組織圖]**。
2. 按一下群組名稱旁邊的三個點，然後按一下 **[刪除]**。
   群組中的所有使用者都將移動到父實體中。

已知問題和限制

- [DEVLOCK-4028] 在 Zoom 桌面代理程式中無法控制群組聊天。
- [DEVLOCK-4016] 若是建立草稿，則不會為 GMX Web 郵件和 Web.de Mail 擷取擷取易記名稱和寄件者 ID。
- [DEVLOCK-4447] 若是建立草稿，則 naver.com WebMail 不會有 [理由] 對話方塊。
- [DEVLOCK-1033] DeviceLockDriver：IRP_MN_QUERY_DEVICE_RELATIONS 處理期間的鎖死情況導致潛在錯誤檢查 DRIVER_POWER_STATE_FAILURE。

Endpoint Detection and Response (EDR)

注意事項
此功能是 Advanced Security + XDR 保護套件的一部分，而該套件又是 [資安防護] 服務的一部分。請注意，當您將 EDR 功能新增至保護計劃時，您可能需要支付額外費用。

EDR 會偵測工作負載上的可疑活動，包括未引起注意的攻擊。接著，EDR 會產生事件，這些事件會提供每次攻擊的逐步概觀，從而協助您瞭解攻擊是如何發生的以及如何防止它再次發生。由於攻擊的每個階段都有易於瞭解的解釋，因此調查攻擊所花的時間可以減少到幾分鐘。

從 C24.05 開始，您可以使用 Extended Detection and Response (XDR) 擴充 EDR 功能。使用 XDR 圖表，透過將偵測與 XDR 資料來源中的事件相關聯，即可獲得 EDR 事件的其他豐富觀點，其中包括電子郵件和身分識別管理中繼資料。如需詳細資訊，請參閱 "Extended Detection and Response (XDR)" (第 862 頁)"Extended Detection and Response (XDR)" (第 862 頁)。

為什麼您需要 Endpoint Detection and Response (EDR)

在當今網路威脅和惡意攻擊不斷擴大的世界中，預防不再保證 100% 的防護。有些攻擊總是能通過防禦層並成功滲透到網路中。傳統解決方案無法看到這種情況何時發生，因而讓攻擊者得以在您的環境中自由駐留數天、數週或數月。

現有的 EDR 解決方案確實有助於透過快速尋找並移除攻擊者來防止這些「隱藏的失效」。但是，它們通常需要高階的安全專業知識或昂貴的安全營運中心 (SOC) 分析人員，而且事件分析可能非常耗時。

Acronis Advanced Security + EDR 功能可偵測未引起注意的攻擊，並協助您瞭解攻擊是如何發生的以及如何防止它再次發生，藉此克服這些限制，從而減少調查攻擊所花的時間。

以下是您需要 EDR 的原因：

- **完整能見度**:即使是未引起注意的攻擊,也能瞭解發生什麼情況以及它是如何發生的。每個攻擊的演化過程也可以透過視覺上安排的方式逐步顯示 (從最初的進入點到檢視成為目標和/或遭到滲透的資料),讓您能夠快速瞭解事件的範圍和影響。如需詳細資訊,請參閱 "如何調查網路攻擊鏈中的事件" (第 818 頁)。
- **將調查時間減至最少**:將事件調查時間從數小時減少到只需要幾分鐘。EDR 會以清楚、易於理解的人類語言,詳細說明攻擊的每個步驟,從而有助於降低對昂貴專家或額外員工的需求。如需詳細資訊,請參閱 "調查事件" (第 817 頁)
- **檢查工作負載上的已知威脅**:您可以自動搜尋您的工作負載,以尋找來自惡意軟體、弱點和可能影響您資料保護之其他類型全球事件的威脅。這些威脅稱為入侵指標 (IOC),而且是以從資安防護營運中心 (CPOC) 收到的威脅資料為基礎。如需詳細資訊,請參閱 "在對工作負載的公開攻擊中,檢查其入侵指標 (IOC)" (第 828 頁)。
- **回應事件的速度更快**:您可以透過存取所有入侵後活動和攻擊鏈每個步驟的明細,執行多個動作來修復每個攻擊點。除此之外,您可以使用遠端控制和鑑識備份調查 (此功能不適用於優先體驗版本)、隔離工作負載,以及終止惡意軟體程序。您也可以使用 Cyber Disaster Recovery Cloud 復原業務營運。如需詳細資訊,請參閱 "修復事件" (第 831 頁)。
- **放心報告您的安全性狀態**:啟用 EDR 後,您可以消除很多對網路攻擊可能對業務造成影響的不安全感和恐懼。此外,與事件相關的資訊會保存 180 天,這可用於稽核用途。

功能

Endpoint Detection and Response (EDR) 包含以下功能:

- 發生入侵時收到警示通知
- 在 [事件] 頁面上管理您的事件
- 以易於瞭解的方式,將攻擊故事情節視覺化
- 建議和修復步驟
- 使用威脅摘要對您的工作負載檢查公開披露的攻擊
- 在儀表板中顯示快速概觀
- 儲存安全性事件 180 天

發生入侵時收到警示通知

EDR 會在每次事件發生時提供警示通知。這些警示會在 Cyber Protect 主控台的主功能表中醒目提示。之後調查警示時,可以按一下 **[調查事件]** 按鈕,就會將您重新導向至事件調查畫面 (亦稱為網路攻擊鏈)。

如需詳細資訊,請參閱 "檢閱事件" (第 798 頁)。

在 [事件] 頁面上管理您的事件

EDR 可讓您在 [事件] 頁面 (可從 Cyber Protect 主控台的 **[防護]** 功能表中存取) 上管理您所有的事件。您可以根據需求,篩選的 **[事件]** 頁面上的資訊,以快速且輕鬆地瞭解事件的目前狀態,包括其嚴重性、受影響的工作負載以及確實性層級。您也可以直接導覽至網路攻擊鏈,以便逐節點檢視攻擊故事情節。

如需有關 [事件] 頁面的詳細資訊,請參閱 "檢閱事件" (第 798 頁)。

以易於瞭解的方式，將攻擊故事情節視覺化

EDR 會以易於閱讀的格式，提供攻擊的視覺表示。如此可確保即使是非安全人員，也能理解任何攻擊的目標和嚴重性。真的不需要安全營運中心 (SOC) 服務或聘請安全專家，EDR 就可以詳細說明攻擊究竟是如何發生的，包括：

- 攻擊者如何進入
- 攻擊者如何隱藏他們的踪跡
- 造成什麼傷害
- 攻擊如何傳播

如需詳細資訊，請參閱 "如何調查網路攻擊鏈中的事件" (第 818 頁)。

建議和修復步驟

EDR 為解決對工作負載的攻擊而提供清楚且易於實作的建議。若要快速解決攻擊，請按一下 **[修復整個事件]** 按鈕以檢視並遵循建議步驟來緩解事件。這些建議步驟可讓您快速恢復受攻擊影響的作業。但是，如果您想要採取更細微的修復步驟，您可以導覽至每個節點，並使用相關動作對其進行修復。

您也可以按一下 **Copilot**，啟動 AI 輔助的 Copilot 聊天工具以輸入多個要求，並接收所選事件的建議回應動作。

如需詳細資訊，請參閱 "修復事件" (第 831 頁)。

使用威脅摘要對您的工作負載檢查公開披露的攻擊

EDR 包含針對您的工作負載，檢閱威脅摘要中已知現有攻擊的功能。這些威脅摘要是根據接收自資安防護營運中心 (CPOC) 的威脅資料自動產生的；EDR 可讓您確認威脅是否將影響您的工作負載，然後採取必要的步驟來消除威脅。

如需詳細資訊，請參閱 "在對工作負載的公開攻擊中，檢查其入侵指標 (IOC)" (第 828 頁)。

在儀表板中顯示快速概觀

EDR 在 Cyber Protect 主控台儀表板中提供各式各樣的統計資料。您可以檢視：

- 目前的威脅狀態，包括需要調查的事件數。
- 依嚴重性顯示攻擊的演變，指出可能的攻擊活動。
- 事件結案的效率。
- 用於攻擊客戶最具針對性的手法。
- 工作負載的網路狀態，表示是隔離狀態還是連線狀態。

儲存安全性事件 180 天

EDR 會收集工作負載和應用程式事件，並將其儲存 180 天。早於 180 天的事件將遭到刪除 (事件刪除是根據存留期而不是根據儲存空間)。請注意，即使關閉 EDR，之前針對工作負載收集的所有事件都會保留下來，而且可用於事件調查。

軟體需求

Endpoint Detection and Response (EDR) 支援下列作業系統：

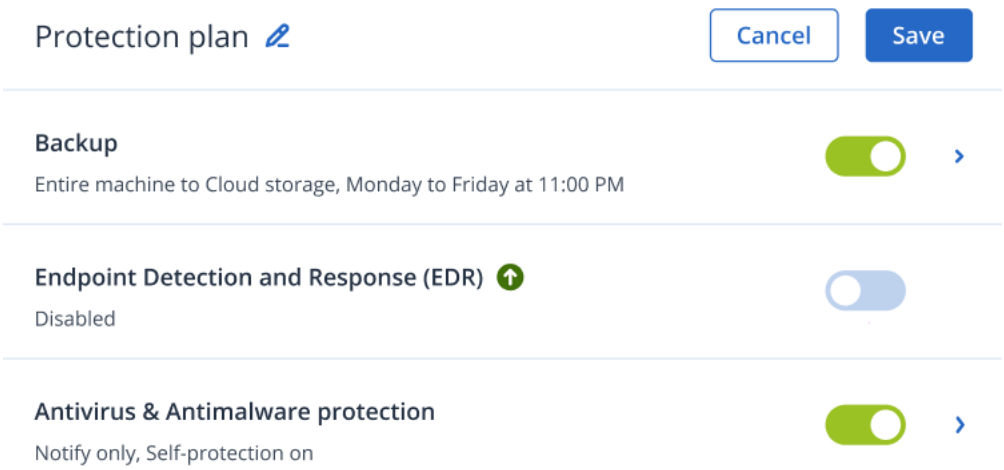
- Microsoft Windows 7 Service Pack 1 和更新版本
- Microsoft Windows Server 2008 R2 和更新版本
- macOS 13 版及更新版本

啟用 Endpoint Detection and Response (EDR) 功能

您可以在任何保護計劃中啟用 EDR。

若要啟用 EDR

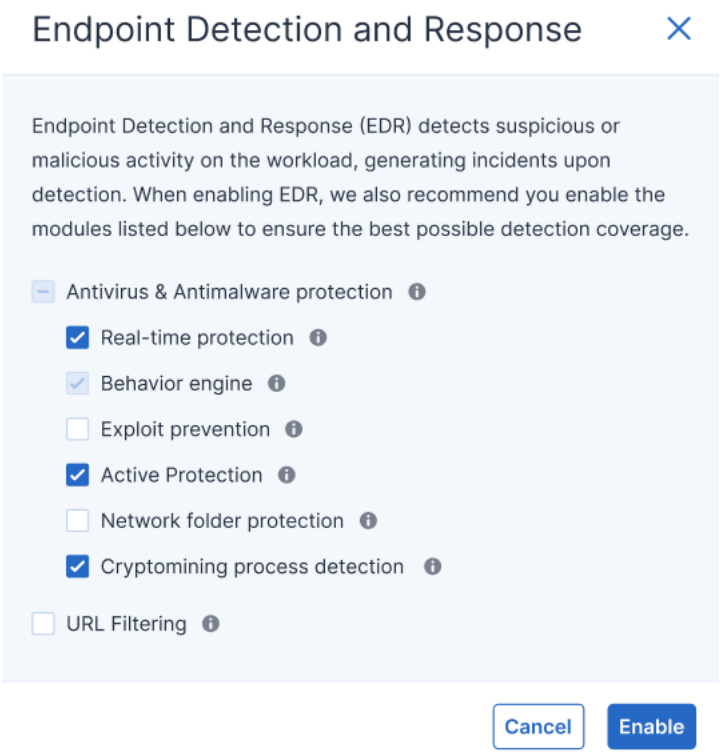
1. 在 Cyber Protect 主控台，前往 **[管理] > [保護計劃]**。
2. 從顯示的清單中選擇相關的保護計劃，然後在右側邊欄中，按一下 **[編輯]**。
   或者，您可以建立新的保護計劃，然後繼續進行下一個步驟。如需有關使用保護計劃的進一步資訊，請參閱 "保護計劃和模組" (第 191 頁)。
3. 在保護計劃側邊欄中，按一下模組名稱旁的開關，以啟用 **[Endpoint Detection and Response (EDR)]** 模組。



   根據您選擇的其他套件而定，**[Advanced Security + EDR]** 套件圖示 (如下所示) 會新增到實作保護計劃所需之保護套件的清單中。

4. 在顯示的對話方塊中，按一下 **[啟用]**。請注意，您可以在保護計劃中啟用 EDR，而且仍然可以停用 [防毒和防惡意軟體]、[Active Protection] 和 [URL 篩選] 功能。



注意事項

如果在啟用 EDR 時，於保護計劃中停用 **[行為引擎]** 或 **[防毒和防惡意軟體防護]**，則也會停用 **[Endpoint Detection and Response (EDR)]**。

如何使用 Endpoint Detection and Response (EDR)

EDR 可讓您偵測未引起注意的攻擊，同時協助您瞭解攻擊是如何發生的以及如何防止它再次發生。由於攻擊的每個階段都有易於瞭解的解釋，因此調查攻擊所花的時間可以減少到幾分鐘。

下表描述使用 EDR 時的一般工作流程。最初，您將檢閱任何新事件並排定其優先順序、在網路攻擊鏈中進行進一步調查，然後採取相關的修復動作。

步驟	如何使用 EDR
步驟 1:檢閱事件	在 EDR 事件清單中: • 瞭解組織的安全性狀態:有多少事件需要進行調查? • 瞭解哪些是最嚴重的事件，並根據其嚴重性，排定調查的優先順序。 • 瞭解哪些事件是新的或正在發生的。
步驟 2:調查事件	在 EDR 網路攻擊鏈中: • 瞭解攻擊者的目標並檢視所使用的攻擊手法。 • 確認任何事件是真正的惡意攻擊的可能性。 • 確認威脅摘要是否將影響您的工作負載。 • 查看已對事件應用了哪些回應動作。

步驟	如何使用 EDR
步驟 3:修復事件	在相關的 EDR 修復區段中： • 應用全域回應動作，快速輕鬆地修復整個事件。 • 修復事件中的個別攻擊點。 • 採取動作以防止攻擊 (或之後的攻擊) 傳播或影響尚未成為攻擊者目標的工作負載。

檢閱事件

Endpoint Detection and Response (EDR) 可提供事件清單，其中包含對工作負載的預防 (或惡意軟體) 和可疑偵測。事件清單可讓您快速概覽將影響工作負載的任何攻擊或威脅，包括尚未緩解的威脅。

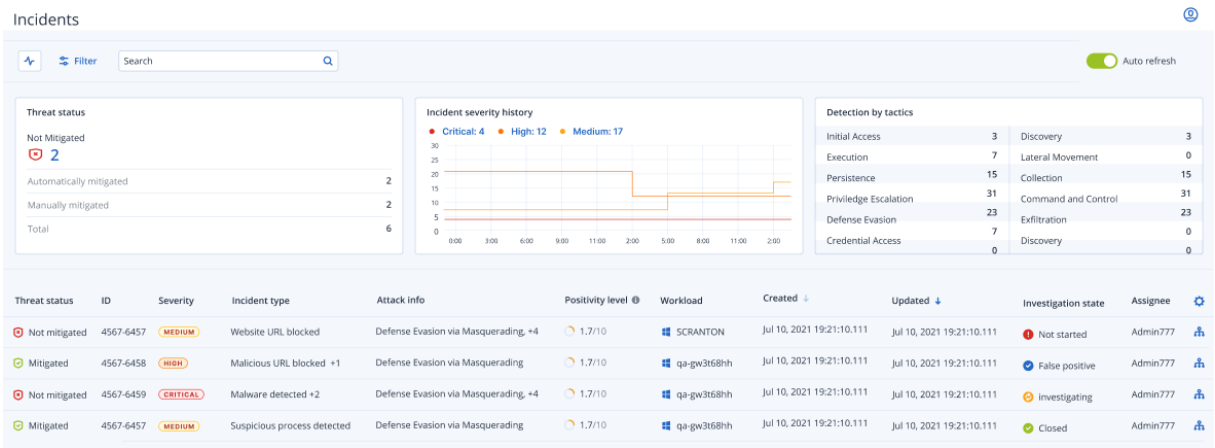
從事件清單中，您可以快速確定：

- 組織的安全性狀態：有多少事件需要進行調查？
- 哪些是最嚴重的事件，並根據其嚴重性，排定調查的優先順序。
- 哪些事件是新的或正在發生的。

注意事項
以合作夥伴系統管理員身分登入時，您可以在整合所有客戶事件的單一畫面中，檢視所有 EDR 事件，而無需存取每個客戶的個別事件檢視。系統會顯示額外的 **[客戶]** 欄，其中包含每個事件所屬的客戶名稱。此外，**[概觀]** 儀表板上顯示的小工具會顯示為所有客戶彙總的指標資料。

如下所示的事件清單是從 Cyber Protect 主控台中的 **[防護]** 功能表存取的。如需有關檢閱事件清單中事件的進一步資訊，請參閱 "檢視目前未緩解的事件" (第 801 頁)。若要深入瞭解建立事件的時機，請參閱究竟什麼是事件？ 。

注意事項
如果您的工作負載已啟用 [受管理的偵測與回應] (MDR)，則會顯示一個額外的 **[MDR 票證]** 欄。此欄會顯示 MDR 廠商提供的票證號碼。



注意事項
Cyber Protect 主控台必須開啟，您才能收到事件通知。

究竟什麼是事件?

事件 (或安全性事件) 可以被視為至少一個預防或可疑偵測點 (或混合) 的*容器*，而且包含所有相關事件和單一攻擊的偵測。這些安全性事件也可以包含其他良性事件，這些事件會為所發生的情況提供進一步的背景資訊。

這可讓您在單一事件中一起檢視攻擊事件，並瞭解攻擊者所執行的邏輯步驟。此外，其有助於加快攻擊的調查時間。

在保護計劃中啟用 EDR 時，安全性事件會在以下情況下建立：

- **預防層阻止某些情況：**系統會根據保護計劃設定，將這些事件自動結案。但是，您可以調查惡意軟體在遭到阻止之前到底做了什麼。例如，勒索軟體在開始加密檔案時遭到阻止，但在此之前可能已竊取認證或安裝服務。
- **EDR 偵測到可疑活動：**這些是應該進行調查並修復的偵測。您可以透過檢視視覺上增強的網路攻擊鏈 (如需詳細資訊，請參閱 "如何調查網路攻擊鏈中的事件" (第 818 頁))，輕鬆地應用相關的修復動作。

針對需要立即注意的事件排定優先順序

您可以隨時從 主控台的 **[防護]** 功能表中存取 Cyber Protect 主控台事件清單。事件清單可讓您快速概覽任何攻擊或威脅，如此可針對需要注意的事件，排定其優先順序。

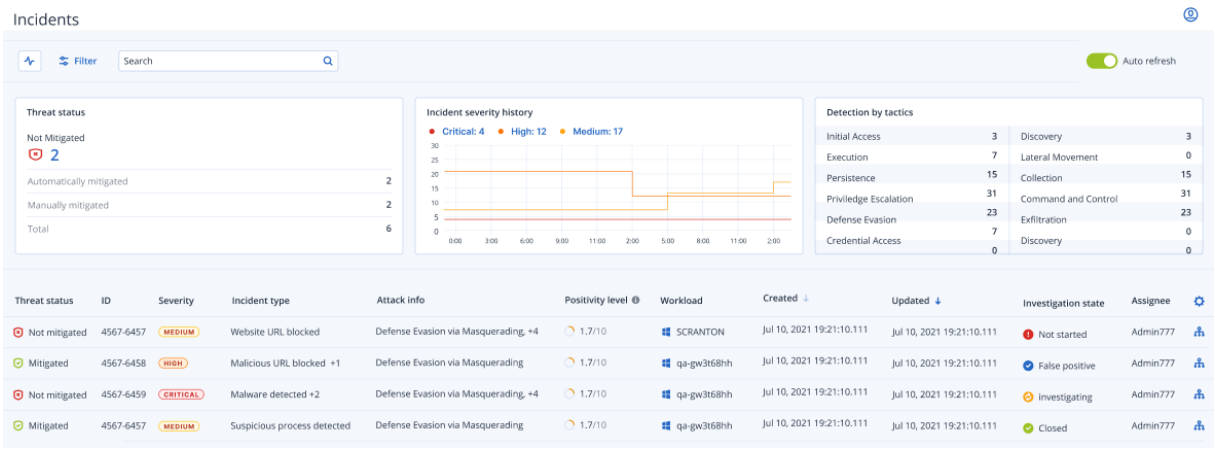
重要事項
為確保您的工作負載保持安全，請*一律*分析正在發生或未緩解的事件，並排定其優先順序。

如何針對需要立即注意的安全性事件排定優先順序

事件清單可讓您分析列出需要注意的事件，並排定其優先順序。您可以：

- 檢視目前未緩解的事件：從事件清單中快速瞭解是否有任何攻擊目前正在進行中。您應該立即查看未緩解的任何事件，如 **[威脅狀態]** 欄中所示 (事件清單預設篩選為顯示這些事件)。
- 瞭解事件的範圍和影響：根據您對新發起或正在進行的攻擊的篩選，瞭解所篩選事件的嚴重性以及對您業務的影響。

一旦您有了精緻的最重要事件清單，您就可以分析事件詳細資料以便更瞭解特定事件，以及攻擊者為實現其目標所使用的手法。如需詳細資訊，請參閱 "分析事件詳細資料" (第 802 頁)。

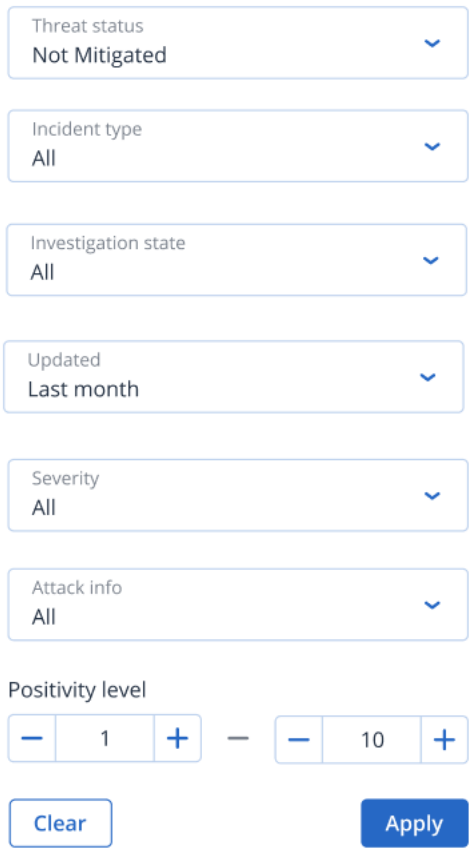


注意事項

根據預設，事件清單是根據 **[更新時間]** 欄排序的，如此可詳細說明上次使用事件內記錄的新偵測更新事件的日期和時間。請注意，即使事件之前已結案，還是可以隨時更新現有的事件。您也可以篩選清單以便根據您的需求，顯示新發起或正在進行的攻擊，如以下程序所述。

若要篩選事件清單

1. 按一下 [事件] 清單頂端的 **[篩選]** 可篩選顯示的事件清單。例如，如果您在 **[建立時間]** 欄位中選擇開始和結束日期，則事件清單和桌面小工具會顯示已定義期間所建立的相關事件。



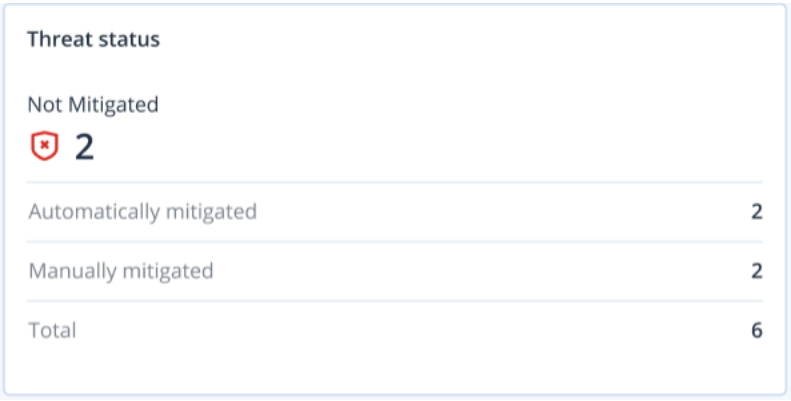
2. 完成後，按一下 **[套用]**。

檢視目前未緩解的事件

您可以在 **[威脅狀態]** 欄中檢視事件的目前威脅狀態，這會顯示事件為 **[已緩解]** 還是 **[未緩解]**。威脅狀態是由 EDR 自動定義；未緩解的任何事件都應該盡快進行調查。

接著，您可以套用篩選條件，進一步精簡所顯示的事件清單。例如，如果您想要根據威脅狀態*和*特定的嚴重性層級篩選清單，請選擇相關的篩選選項。一旦篩選出您感興趣的事件，就可以進行調查，如 "調查事件" (第 817 頁) 中所述。

您也可以使用以下所示的 **[威脅狀態]** 桌面小工具，快速概覽目前的威脅狀態。請注意，顯示在此桌面小工具中的資料會反映您所套用的篩選條件；請參閱 "若要篩選事件清單" (第 800 頁)。



瞭解事件的範圍和影響

您可以檢閱 **[嚴重性]**、**[攻擊資訊]** 和 **[確實性層級]** 欄，以快速瞭解事件的範圍和影響。如上所提及，在您確定目前進行中的事件之後，就可以篩選這些額外的欄來執行下列操作：

- 在 **[嚴重性]** 欄中檢閱哪些事件更嚴重。事件的嚴重性可能是 **[重大]**、**[高]** 或 **[中]**。
  - **重大**：存在惡意網路活動的嚴重風險，而且可能危及您環境中的重要主機。
  - **高**：惡意網路活動的風險很高，而且有可能對您的環境造成嚴重破壞。
  - **中**：惡意網路活動的風險增加。

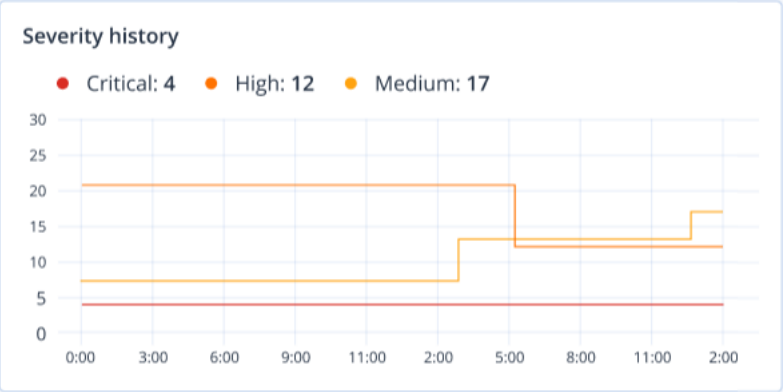
  注意事項
  在確定嚴重性時，EDR 演算法會考慮工作負載類型以及攻擊每個步驟的範圍。例如，包含與認證竊取相關步驟的事件會設定為 **[重大]**。

- 瞭解在 **[事件類型]** 欄中建立事件的原因。事件類型可以包含以下任一項或多項：
  - **偵測到勒索軟體**
  - **偵測到惡意程式碼**
  - **偵測到可疑程序**
  - **偵測到惡意程序**
  - **已封鎖可疑 URL**
  - **已封鎖惡意 URL**
- 在 **[攻擊資訊]** 欄中確定正在使用的攻擊手法，並瞭解攻擊是否存在共同的主題或模式。

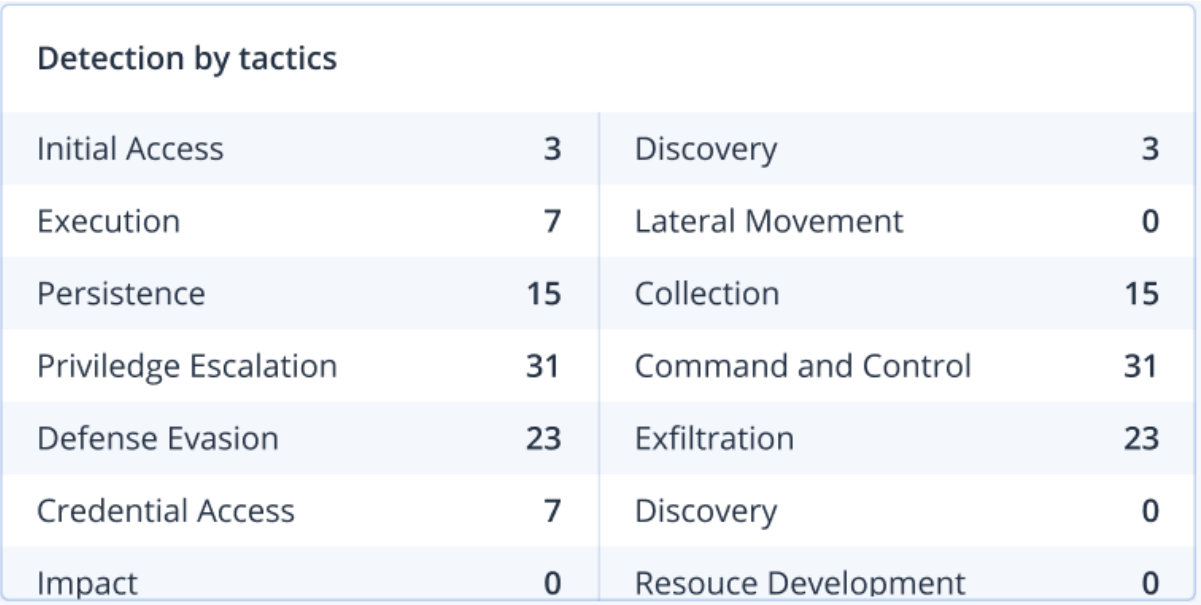
- 確認事件是真正的惡意攻擊的可能性有多大;**[確實性層級]**欄包含 1-10 的分數 (分數越高，攻擊越有可能是真正的惡意攻擊)。

在您找出需要立即注意的事件之後，可以進行調查，如 "調查事件" (第 817 頁) 中所述

您也可以使用 **[嚴重性歷程記錄]** 和 **[手法偵測]** 桌面小工具來快速概覽嚴重性和攻擊手法。



[手法偵測] 桌面小工具會顯示所使用的各種攻擊手法，值為綠色或紅色時，表示在先前指定的時間範圍內增加或減少。此桌面小工具提供已篩選事件中所有目標的彙總檢視，讓您快速瞭解對客戶的影響。



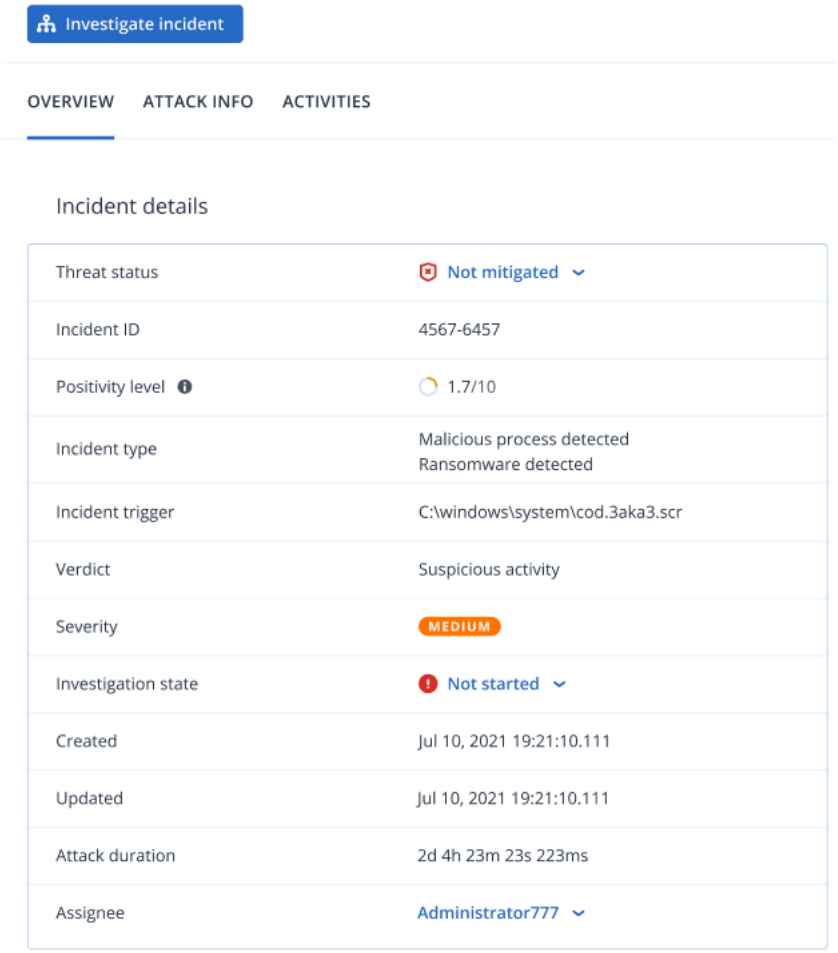
分析事件詳細資料

在事件檢閱階段，您也可以從 [Endpoint Detection and Response (EDR)] 事件清單中分析每個事件的詳細資料。這些詳細資料可讓您向下鑽研整個事件，並瞭解發生的方式和時間。此外，您可以將事件指派給特定使用者進行調查，並設定調查狀態。

若要分析事件詳細資料

1. 在 Cyber Protect 主控台中，移至 **[防護] > [事件]**。事件清單隨即顯示。
2. 按一下您要檢閱的事件。所選事件的詳細資料隨即顯示。

3. 在顯示的 **[概觀]** 索引標籤中，您可以檢閱事件和工作負載詳細資料，包括目前威脅狀態和嚴重性。您也可以定義 **[調查狀態]**（從 **[正在調查]**、**[未開始]**（預設狀態）、**[誤報]** 或 **[已結案]** 中選擇），並選擇要將事件指派給哪一個使用者（在 **[被指派者]** 下拉式清單中，選擇相關的使用者）。



4. 按一下 **[攻擊資訊]** 索引標籤可檢閱攻擊的詳細資料以及攻擊中使用的手法。按一下每個列出的攻擊手法旁的連結可在 MITRE.org 上檢閱攻擊手法的進一步資訊。
5. 按一下 **[活動]** 索引標籤可檢閱在網路攻擊鏈中採取的任何動作，以緩解事件。如需詳細資訊，請參閱 "如何調查網路攻擊鏈中的事件"（第 818 頁）。
   例如，如果對工作負載執行修補程式，您可以看到修補程式起始者、所需的時間，以及在實作修補程式期間發生的任何錯誤。
6. 按一下 **[調查事件]** 可存取網路攻擊鏈，您可以在其中逐節點調查事件。如需詳細資訊，請參閱 "如何調查網路攻擊鏈中的事件"（第 818 頁）。

搜尋入侵指標 (IoC) 和可疑活動

注意事項
此功能是優先體驗方案的一部分。部分功能和描述可能不完整。

若要在威脅升級為高度影響事件之前偵測並緩解威脅，請使用 **[事件搜尋]** 功能。此搜尋功能可讓您在使用 Endpoint Detection and Response (EDR) 啟用的所有工作負載中尋找 IoC 和可疑活動。

使用 **[事件搜尋]** 功能可以：

- 對從所有工作負載收集的事件資料執行自訂查詢以搜尋雜湊。或者，您可以取得指標來回答某些問題 (例如，顯示程序數量異常多的工作負載)。
- 使用 EDR 端點提供的屬性和其他整合的資料 (例如，作業系統活動、使用者活動和網路活動) 篩選查詢。

[事件搜尋] 功能可從 主控台中的 **[保護]** 功能表中存取。

注意事項
EDR 事件搜尋結果的預設保留期限為 7 天。

搜尋事件

注意事項
此功能是優先體驗方案的一部分。部分功能和描述可能不完整。

您可以在受 EDR 保護的所有工作負載中搜尋 Endpoint Detection and Response (EDR) 事件。

請注意，當您使用合作夥伴租用戶 **(所有客戶)** 層級上的 Cyber Protect 主控台時，可以搜尋所有受控客戶中的事件。如果您在客戶租用戶層級工作，則可以搜尋專屬於所選客戶的事件。

若要搜尋事件

1. 在 Cyber Protect 主控台中，移至 **[保護]** > **[事件搜尋]**。
2. 使用 Acronis XDR 查詢語言 (XQL) 輸入搜尋查詢，並定義日期範圍。
   請注意，XQL 會使用自動完成協助您建置查詢。如需有關可用語法和查詢選項的詳細資訊，請參閱 "語法" (第 805 頁)。
3. 按一下輸入欄位右側的箭頭圖示以執行查詢。
   請注意，也可以使用以下鍵盤按鍵操作：
   - 按下 **Enter** 可將游標移至下一行。"|" 字元也會新增在新行的開頭 (這在撰寫多階段查詢時很有幫助)。
   - 按 **Shift+Enter** 可將游標移至下一行。
   - 按 **Ctrl+Enter** 可執行查詢。
4. 根據需要，精簡您的搜尋查詢。例如，選擇顯示包含特定檔案名稱的特定欄位或事件。

Acronis XDR 查詢語言 (XQL)

注意事項
此功能是優先體驗方案的一部分。部分功能和描述可能不完整。

使用 XQL 搜尋 Endpoint Detection and Response (EDR) 事件，然後向下鑽研您要尋找的事件。此區段會列出搜尋 EDR 事件時應熟悉的 XQL 的各種元素：

- 語法 (包括範例查詢)
- 事件類型和欄位

如需有關使用 **[事件搜尋]** 功能的詳細資訊，請參閱 "搜尋入侵指標 (IoC) 和可疑活動" (第 803 頁)。

語法

作業	範例
選擇資料來源 選擇要操作的查詢的資料來源。此運算子必須是查詢中的第一個運算子。	`eventType`
篩選資料 根據條件篩選資料，開頭必須是 `where` 關鍵字。 請注意以下篩選選項： • 字串可以用單引號或雙引號括住。 • `AND` 和 `OR` 等邏輯運算子可用於結合篩選條件。 `key = value AND key < value OR key = value` • 運算子周圍可以加上括號： `(key = value) AND (key < value OR key = value)` • 將 `CONTAINS` 用於部分字串比對： `key CONTAINS 'value'` • 將 `ICONTAINS` 用於不區分大小寫的部分字串比對： `key ICONTAINS 'value'` • 將 `IN` 用於成員資格檢查： `key IN ('value1', 'value2')` • 根據 RE2 標準，使用規則運算式比對： `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*'`
選擇欄位 指定從查詢中選擇並傳回的欄位。	`eventType | columns field1, field2, field3 ...`
排序 將查詢結果排序 (遞增或遞減)。如果未指定順序，則預設順序為遞增。	`eventType | order field1, field2, field3 ...` `eventType | order field asc` `eventType | order field desc`
限制 限制查詢的結果。	`eventType | limit 10` `eventType | limit 1000 | group [field1, field2] | limit 10`
群組作業 對資料執行`group operation`。 (選擇性) 您可以指定要對彙總欄位執行的彙總函數，也可以僅指定彙總函數，而不對特定欄位執	`eventType | group [field]` `eventType | group [field1, field2, field3, ...]` `eventType | group with [max(field1), min(field2), avg(field3)]`

作業	範例
行group operation。	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]
彙總 彙總查詢結果以執行作業。 這些函數只能與group operation一起使用 (請參閱上方)。	min(field) max(field) avg(field) count() count(field) countdistinct(field)

範例查詢

本節包含許多範例查詢，以說明如何將 XQL 語法規則套用至查詢。

- 從 WinProcCreate 事件類型中選擇欄位：

```
WinProcCreate | columns host_name, parent_start, parent_gpid, parent_pid, parent_
user, proc_name
```

- 按 proc_name 對結果進行分組之前，使用條件進行篩選，並對 parent_pid 套用彙總函數 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)]
```

- 使用篩選條件選擇資料，然後計算傳回的列數並對其進行排序：

```
WinProcCreate | where host_name == 'BNi-Kub' | group with [count() as new_count] |
order new_count
```

- 使用規則運算式篩選條件選擇資料：

```
WinProcCreate | where host_name matches 'BNi.*'
```

- 使用複雜的篩選條件選擇資料，並限制結果：

```
WinProcCreate | where (host_name contains 'BNi-Kub') OR (host_name in
('Computer1', 'Computer2')) | limit 10
```

- 使用篩選條件選擇資料，然後計算傳回的相異列數：

```
WinProcCreate | where host_name == 'BNi-Kub' | group with [countdistinct(*)]
```

- 使用篩選條件選擇資料、按欄位排序，並限制傳回的列數：

```
WinProcCreate | where host_name == 'BNi-Kub' | order host_name | limit 10
```

事件類型和欄位

此區段包含：

- 事件類型
- 範例資料類型
- 事件欄位

事件類型

名稱	描述	類型
WinProcCreate 如需有關可用欄位的詳細資訊，請參閱 WinProcCreate。	Windows 處理序建立事件	事件
WinProcTerminate 如需有關可用欄位的詳細資訊，請參閱 WinProcTerminate。	Windows 處理序終止事件	事件

名稱	描述	類型
WinNetAccess 如需有關可用欄位的詳細資訊，請參閱 WinNetAccess。	Windows 網路存取事件	事件
WinRegAccess 如需有關可用欄位的詳細資訊，請參閱 WinRegAccess。	Windows 登錄存取事件	事件
WinScriptExec 如需有關可用欄位的詳細資訊，請參閱 WinScriptExec。	Windows 指令碼執行事件 (包括 PowerShell、VBS 等)	事件
WinFileAccess 如需有關可用欄位的詳細資訊，請參閱 WinFileAccess。	Windows 檔案存取事件 (讀取/寫入)	事件
WinLogin 如需有關可用欄位的詳細資訊，請參閱 WinLogin。	Windows 使用者登入事件	事件
WinLogout 如需有關可用欄位的詳細資訊，請參閱 WinLogout。	Windows 使用者登出事件	事件
WinAgentDetection 如需有關可用欄位的詳細資訊，請參閱 WinAgentDetection。	Windows 偵測事件	偵測

範例資料類型

資料類型	範例	描述
String	`WinProcCreate | where host_name == 'BNi-Kub'` `WinProcCreate | where host_name == "BNi-Kub"`	字串必須用單引號或雙引號括住。
UUID	`WinProcCreate | where agent_id == '61f0c404-5cb3-11e7-907b-a6006ad3dba0'` `WinProcCreate | where agent_id == "61f0c404-5cb3-11e7-907b-a6006ad3dba0"`	UUID 是字串值，必須用單引號或雙引號括住。 UUID 值必須採用 8-4-4-4-12 序列。
DateTime	`WinProcCreate | where event_time < '2022-11-01'` `WinProcCreate | where event_time < "2022-11-01"`	DateTime 是字串值，必須用單引號或雙引號括住。 DateTime 必須採用 YYYY-MM-DD

資料類型	範例	描述
		格式。
Bool	`WinLogin | where is_admin == 1` `WinLogin | where is_admin == 0` `WinLogin | where is_admin == true` `WinLogin | where is_admin == false`	布林值可以用 `1`、`0`、`true` 或 `false` 表示。
整數	`WinLogin | where proc_pid > 25`	整數值。

事件欄位

事件類型	欄位 (資料類型)
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)

事件類型	欄位 (資料類型)
	• proc_prod (String) • proc_prod_desc (String) • proc_sha1 (String) • proc_sha256 (String) • proc_signatures (String) • 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)

事件類型	欄位 (資料類型)
	• term_sha1 (String) • term_sha256 (String) • term_start (DateTime) • term_upn (String) • term_user (String) • 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)

事件類型	欄位 (資料類型)
	• 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)
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)

事件類型	欄位 (資料類型)
	• proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • 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)

事件類型	欄位 (資料類型)
	• 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) • 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)

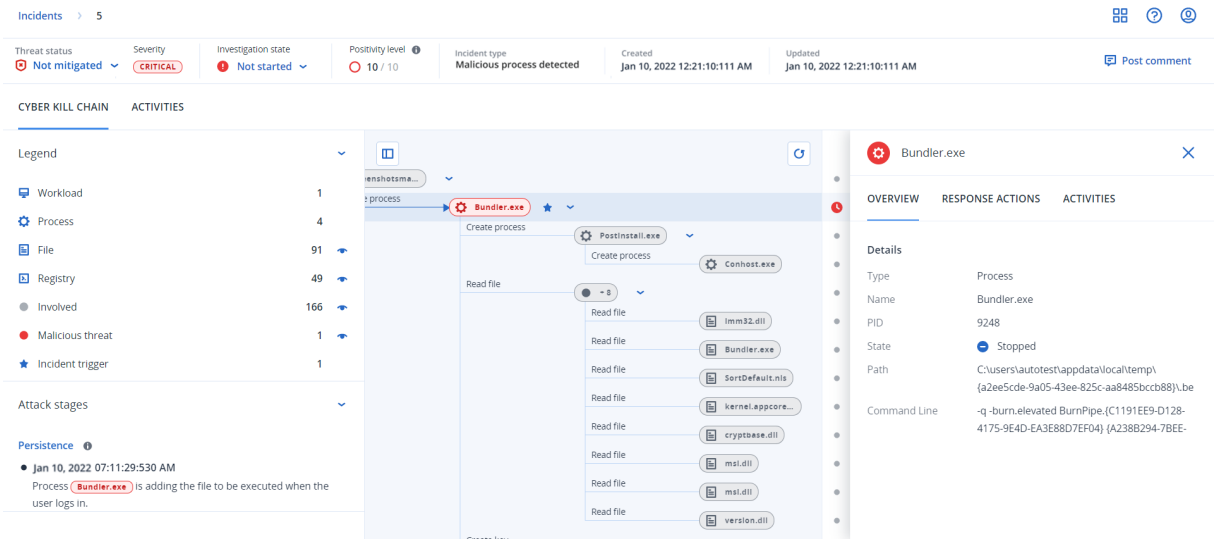
事件類型	欄位 (資料類型)
	• proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • 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)

事件類型	欄位 (資料類型)
	• customer (String) • detection_type (String) • event_time (DateTime) • file_md5 (String) • file_name (String) • 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)

事件類型	欄位 (資料類型)
	• proc_user_domain (String) • resource_id (UUID) • severity (String) • threat_name (String) • timestamp (DateTime) • url (String) • url_blocked (Bool) • url_cat (Array(String)) • url_list (String) • url_md5 (String)

調查事件

Endpoint Detection and Response (EDR) 可讓您調查整個事件，包括所有攻擊階段以及受攻擊影響的物件 (程序、登錄檔、排程工作和網域)。這些物件在易於瞭解的網路攻擊鏈中，以節點表示，如下所示。使用網路攻擊鏈可快速瞭解發生的實際情況及其發生時間。



攻擊的每個步驟都可以在網路攻擊鏈中檢視，這可為您提供事件發生方式和原因的詳細解釋。網路攻擊鏈使用易於瞭解的句子和圖表來協助解釋攻擊的每個步驟，從而有助於將調查時間減至最少。

您可以透過對應到 MITRE 架構的攻擊演變，快速瞭解事件的範圍和影響。這可讓您分析在攻擊的每個步驟中發生的情況，包括：

- 最初的進入點
- 進行攻擊的方式
- 任何權限提升
- 規避偵測手法
- 對其他工作負載的橫向移動

- 認證竊取
- 滲透嘗試

您也可以按一下 **Copilot**，啟動 Copilot 聊天工具，如此可讓您輸入多個要求，並接收所選事件的建議回應動作。如需詳細資訊，請參閱 "如何調查網路攻擊鏈中的事件"(第 818 頁)。

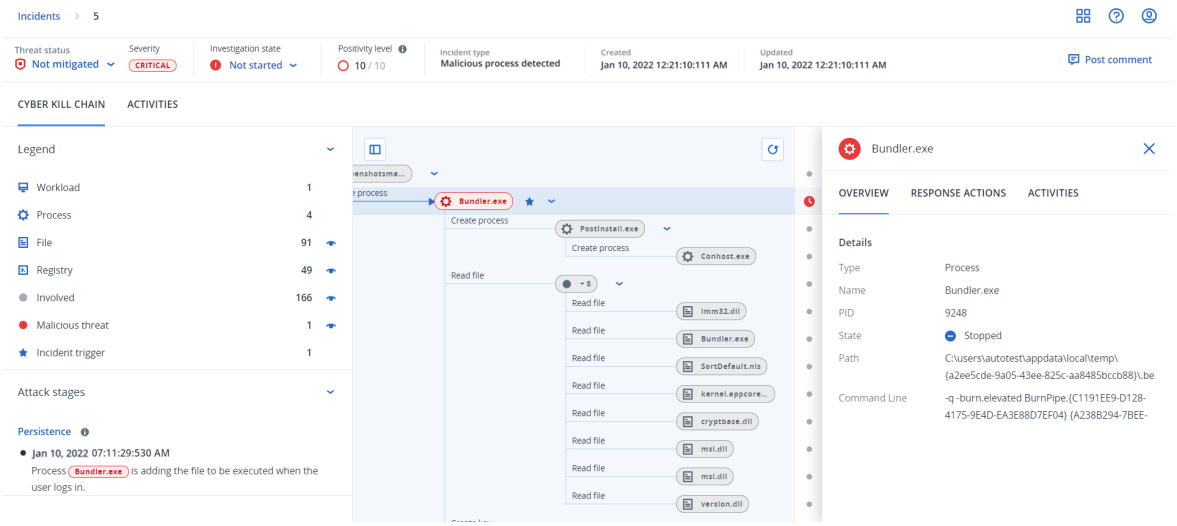
注意事項
在攻擊中受到影響的每個物件 (無論是程序、登錄檔、排程工作還是網域) 在網路攻擊鏈中都是以節點表示。

如何調查網路攻擊鏈中的事件

您可以在網路攻擊鏈中調查攻擊的每個步驟。按照網路攻擊鏈淺顯易懂的句子和圖表來瞭解攻擊的每個步驟，從而協助您將調查時間減至最少。

若要在網路攻擊鏈中開始調查

1. 在 Cyber Protect 主控台中，移至 **[防護] > [事件]**。
2. 在顯示的事件清單中，按一下您想要調查的事件最右側欄內的 。所選事件的網路攻擊鏈隨即顯示。



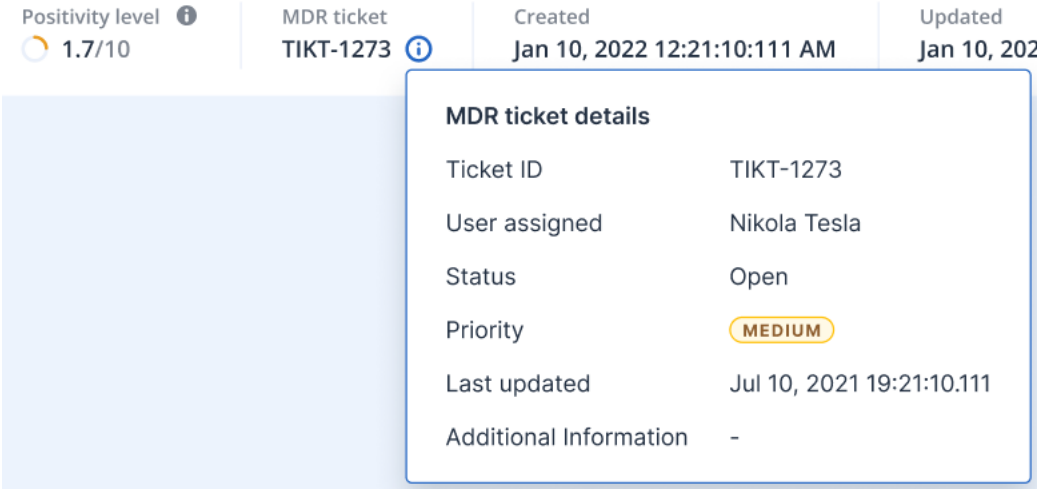
3. 在頁面頂端的威脅狀態列中，檢視事件摘要。威脅狀態列包含以下資訊：
   - 目前威脅狀態：威脅狀態是由系統自動定義。**未緩解**的任何事件都應該盡快進行調查。

     重要事項
     從備份成功完成還原時，或所有偵測皆透過停止程序、隔離或復原動作成功修復時，會將事件設定為 **[已緩解]**。

     尚未從備份成功完成還原時，或至少一個偵測尚未透過停止程序、隔離或復原動作成功修復時，會將事件設定為 **[未緩解]**。

     您也可以將威脅狀態手動設定為 **[已緩解]** 或 **[未緩解]**。無論選擇哪一種狀態，您都會收到輸入註解的提示。此註解會儲存為調查活動的一部分，而且可以在 **[活動]** 索引標籤中檢視。請注意，如果發現重新偵測到事件或已執行並成功完成回應動作，則 EDR 仍然可以將威脅狀態還原為 **[已緩解]** 或 **[未緩解]**。

   - 事件嚴重性：**[重大]**、**[高]** 或 **[中]**。如需詳細資訊，請參閱 "檢閱事件" (第 798 頁)。
   - 目前調查狀態：**[正在調查]**、**[未開始]** (預設狀態)、**[誤報]** 或 **[已結案]** 之一。您應該在開始調查事件時變更狀態，讓其他同事知道事件的任何變化。
   - 確實性層級：指出事件是真正的惡意攻擊的可能性有多大，範圍是 1-10。如需詳細資訊，請參閱 "檢閱事件" (第 798 頁)。
   - 事件類型：**[偵測到勒索軟體]**、**[偵測到惡意軟體]**、**[偵測到可疑程序]**、**[偵測到惡意程序]**、**[已封鎖可疑 URL]** 和 **[已封鎖惡意 URL]** 中的一項或多項。
   - 如果工作負載已啟用 [受管理的偵測與回應] (MDR)，則會顯示一個 **[MDR 票證]** 欄位。您可以檢視針對事件建立的 MDR 票證的詳細資料，以及指派給事件的 MDR 安全性分析師的詳細資料。

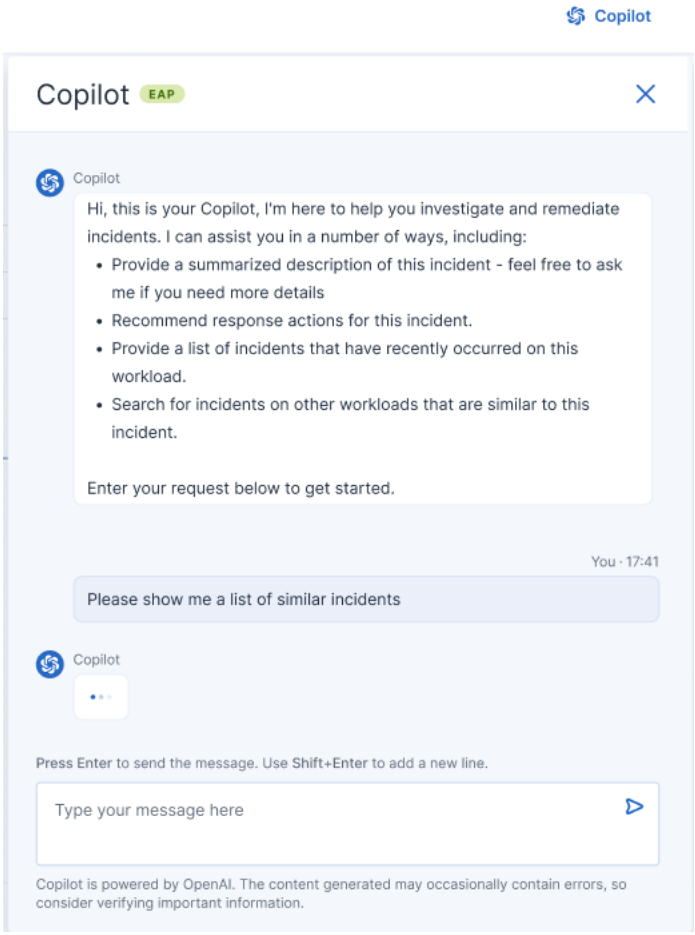


   - 事件的建立和更新時間：偵測到事件的日期和時間，或是上次使用事件內記錄的新偵測更新事件的時間。

4. 按一下 **[圖例]** 索引標籤可檢視組成攻擊鏈圖表的各種節點，並定義要檢視的節點。如需進一步資訊，請參閱 "瞭解與自訂網路攻擊鏈檢視" (第 820 頁)。

5. 請執行以下步驟以調查並修復事件。請注意，這是調查並修復事件的典型工作流程，但根據每個事件和您自己的需求，可能會有所不同。
   a. 在 **[攻擊階段]** 索引標籤中調查攻擊的每個階段。如需進一步資訊，請參閱 "如何導覽攻擊階段" (第 822 頁)。
   b. 按一下 **[修復整個事件]** 以套用修復動作。如需進一步資訊，請參閱 "修復整個事件" (第 831 頁)。您也可以修復網路攻擊鏈中的個別節點，如 "個別網路攻擊鏈節點的回應動作" (第 835 頁) 中所述。

      或者，按一下 **[Copilot]** 以啟動 AI 輔助的 Copilot 聊天工具。Copilot 會提供回應選項 (視事件而定)，以及事件的相關內容資訊，例如，有關攻擊類型的詳細資料。您可以選擇相關的回應選項，然後依照畫面上的指示進行。這些回應選項詳述於 "個別網路攻擊鏈節點的回應動作" (第 835 頁)。



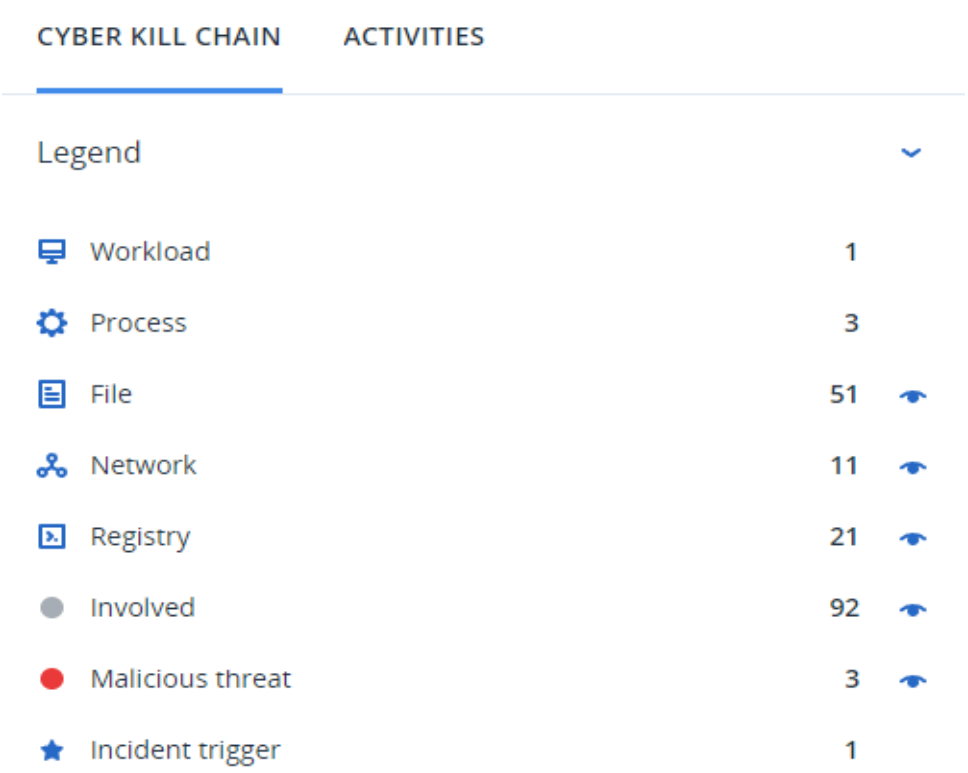
   c. 在 **[活動]** 索引標籤中檢閱為緩解事件所採取的動作。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

瞭解與自訂網路攻擊鏈檢視

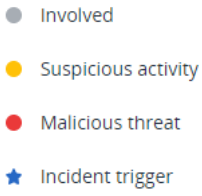
為瞭解在網路攻擊鏈中受到影響的節點，請存取圖例。此圖例會顯示事件中涉及的所有節點，從而讓您瞭解各種節點如何受到攻擊者的影響。您也可以在網路攻擊鏈中，定義您要隱藏或顯示的節點。

若要存取圖例

1. 按一下 [圖例] 區段右側的箭頭圖示。
   [圖例] 區段隨即展開，如下所示。



2. 圖例中使用四個主要色彩，這可讓您快速瞭解網路攻擊鏈中的每個節點所發生的情況，如下所示。這些以色彩編碼的節點也包含在攻擊階段中，如 "如何導覽攻擊階段" (第 822 頁) 中所述。



若要在網路攻擊鏈中隱藏或顯示節點

1. 在展開的 [圖例] 區段中，確認 顯示在您要在網路攻擊鏈中顯示的節點旁邊。如果顯示的圖示為 ，請按一下該圖示，將其變更為 。
2. 若要在網路攻擊鏈中隱藏節點，按一下 。此圖示會變更為 ，且節點不會顯示在網路攻擊鏈中。

調查事件的攻擊階段

事件的攻擊階段會針對每個事件，提供一個易於理解的解釋。

每個工作階段都會摘要說明究竟發生了什麼情況及其所針對的目標 (在網路攻擊鏈中指的是*節點*)。例如，如果下載的檔案偽裝成其他檔案，攻擊階段將指出該檔案，並包含網路攻擊鏈中，指向您可以調查之相關節點的連結，以及指向相關 MITRE ATT&CK 技術的連結。

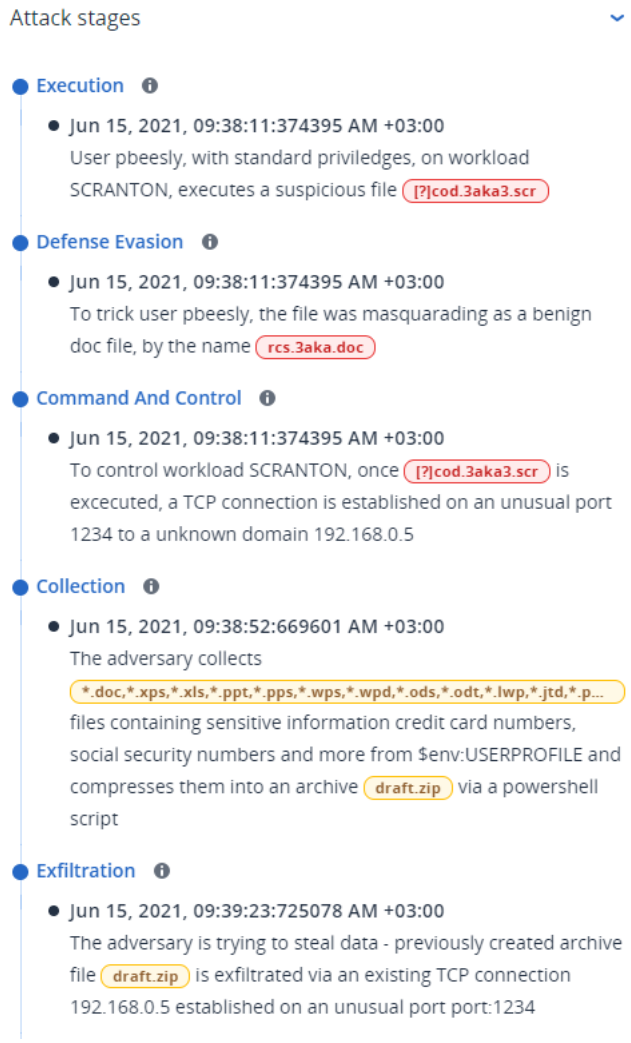
每個攻擊階段都會為您提供解決以下三個關鍵問題所需的資訊：

- 攻擊者的目標是什麼?
- 攻擊者如何實現此目標?
- 目標是哪些節點?

更重要的是,提供的解釋可確保大幅減少調查事件所花費的時間,因為您不再需要從時間軸或圖形節點中查看每個安全性事件,然後嘗試建立對攻擊的解釋。

攻擊階段所包含的資訊是有關內含機密資訊 (例如信用卡號碼和社會安全號碼) 的受感染檔案,如以下範例中的 **[收集]** 階段所示。

如需詳細資訊,請參閱 "攻擊階段中包含哪些資訊? "(第 823 頁)。



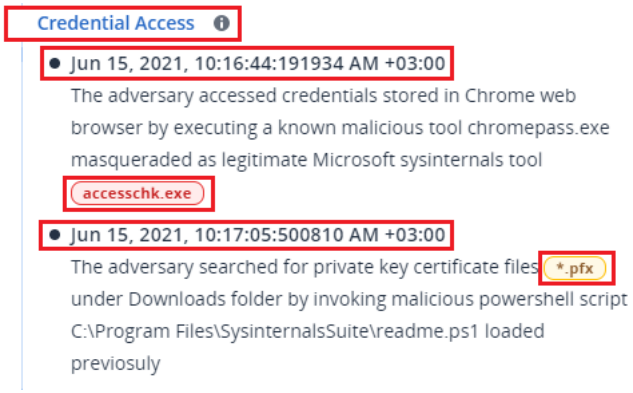
如何導覽攻擊階段

攻擊階段是按時間順序列出。向下捲動可查看事件攻擊階段的完整清單。

若要進一步調查特定的攻擊階段,請按一下該攻擊階段的任何位置,即可導覽至網路攻擊鏈圖表中的相關節點。如需有關導覽網路攻擊鏈圖表和特定節點的詳細資訊,請參閱 "調查網路攻擊鏈中的個別節點" (第 824 頁)。

攻擊階段中包含哪些資訊?

每個攻擊階段都會以易於閱讀的人類語言，提供一個易於瞭解的攻擊解釋。此解釋包含數種元素，如下所示，並詳述於下表中。



攻擊階段元素	描述
標頭	透過指向已知 MITRE ATT&CK 技術的連結，描述攻擊者嘗試做的事情及其目標 (在以上範例中為 **[認證存取]**)。按一下該連結可在 MITRE ATT&CK 網站上瞭解更多資訊。 **注意事項** 如果攻擊階段不是已知的 MITRE ATT&CK 技術，則不會連結標頭文字。這與通用技術相關，例如在隨機資料夾中偵測到的檔案。
時間戳記	攻擊階段發生的時間。
技術	攻擊者如何在技術上達到其目標，以及哪些物件 (登錄項目、檔案或排程工作) 受到影響。 攻擊技術的文字描述中包含指向網路攻擊鏈中每個受影響節點以色彩編碼的連結，如以上範例所示。這些以色彩編碼的連結可讓您快速導覽至受影響的節點，調查究竟發生了什麼情況。攻擊階段使用的色彩表示如下： ● Involved ● Suspicious activity ● Malicious threat ★ Incident trigger 從上述圖例我們可以看到「認證存取」範例的攻擊階段有一個指向惡意軟體節點

攻擊階段元素	描述
	accesschk.exe 和一個可疑檔案節點 *.pfx 的連結 (按一下連結可跳到網路攻擊鏈中的對應節點)。如需有關導覽這些節點和可用動作的詳細資訊，請參閱 "調查網路攻擊鏈中的個別節點" (第 824 頁)。 請注意，攻擊階段也包含指向檔案節點的連結，這些檔案節點中有包含機密資訊的遭入侵檔案相關資訊，例如，受保護的健康資訊 (PHI)、信用卡號碼，以及社會安全號碼。

注意事項
每個攻擊階段都是一個單一偵測事件。每個階段中列出的內容 (標頭、時間戳記、技術) 都是根據偵測事件中的特定參數產生的，而且這些內容是以 Endpoint Detection and Response (EDR) 所儲存的攻擊階段範本為基礎。

調查網路攻擊鏈中的個別節點

除了檢閱攻擊階段之後，您還可以導覽網路攻擊鏈中的每個攻擊節點。如此可讓您向下鑽研網路攻擊鏈中的特定節點，並在需要時，導覽並修復每個節點。

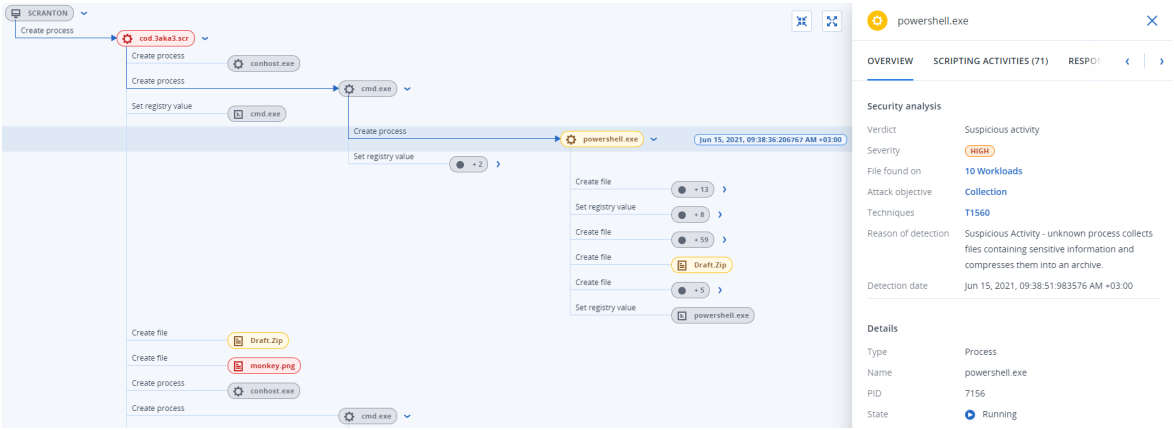
例如，您可以判斷某個事件為真正惡意攻擊的可能性。您也可以根據您的調查，將多個回應動作套用到節點，包括隔離工作負載或隔離可疑檔案。

若要調查網路攻擊鏈中的個別節點

1. 在 Cyber Protect 主控台中，移至 **[防護] > [事件]**。
2. 在顯示的事件清單中，按一下您想要調查的事件最右側欄內的 。所選事件的網路攻擊鏈隨即顯示。
3. 導覽至相關的節點，然後按一下該節點以顯示其側邊欄。

   注意事項
   按一下該節點將其展開，並顯示相關聯的節點。

   例如，按一下以下範例中的 **powershell.exe** 節點會開啟該節點的側邊欄。您也可以按一下節點旁的箭頭圖示以檢視可能受到 **powershell.exe** 節點影響的相關聯節點，包括檔案和登錄值。接著，您可以按一下這些相關聯的節點來進一步調查。



4. 調查包含在側邊欄索引標籤中的資訊：
   - **概觀**：包含兩個主要區段，可提供受攻擊節點的安全性摘要。
     - **安全性分析**：提供受攻擊節點的分析，包括威脅的 EDR 結果 (如可疑活動)、根據 MITRE 攻擊手法的攻擊目標 (按一下連結可前往 MITRE 網站)、偵測原因，以及可能受到攻擊影響的工作負載數目 (按一下 **[n 工作負載]** 連結可檢視受影響的工作負載)。

       注意事項
       [n 工作負載] 連結意指已在其他工作負載上*找到*的特定惡意或可疑目標。這不表示攻擊發生在其他這些工作負載上，而是表示其他這些工作負載上存在入侵指標。攻擊可能已經發生 (並產生其他事件)，或者攻擊者正準備使用他們的攻擊「工具組」攻擊其他這些工作負載。

     - **詳細資料**：包含節點的詳細資料，其中包括其類型、名稱和目前狀態、節點路徑，以及任何檔案雜湊及數位簽章 (例如 MD5 和憑證序號)。
   - **指令碼活動**：包含攻擊中叫用或載入的任何指令碼的詳細資料。按一下 可將指令碼複製到剪貼簿進行進一步調查。

     注意事項
     系統只會針對執行命令或指令碼 (例如 cmd 或 PowerShell 命令) 的程序節點，顯示 **[指令碼活動]** 索引標籤。

   - **回應動作**：包含多個區段，可根據節點類型，提供其他調查、修復和預防動作。
     例如，針對工作負載節點，您可以定義多個回應，其中包括鑑識備份和從備份還原。或者，您可以針對惡意或可疑節點，停止或隔離該節點、復原攻擊所做的變更，並將其新增到保護計劃允許名單或封鎖名單。
     如需有關將回應動作套到到特定節點的詳細資訊，請參閱 "個別網路攻擊鏈節點的回應動作" (第 835 頁)。
   - **活動**：以時間順序顯示套用到事件的動作。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

瞭解為緩解事件所採取的動作

檢閱事件並調查攻擊發生的方式之後，您通常要套用回應動作。一旦您套用回應動作之後，就可以在多個位置檢視這些動作，讓您更瞭解為緩解事件已經採取哪些步驟。

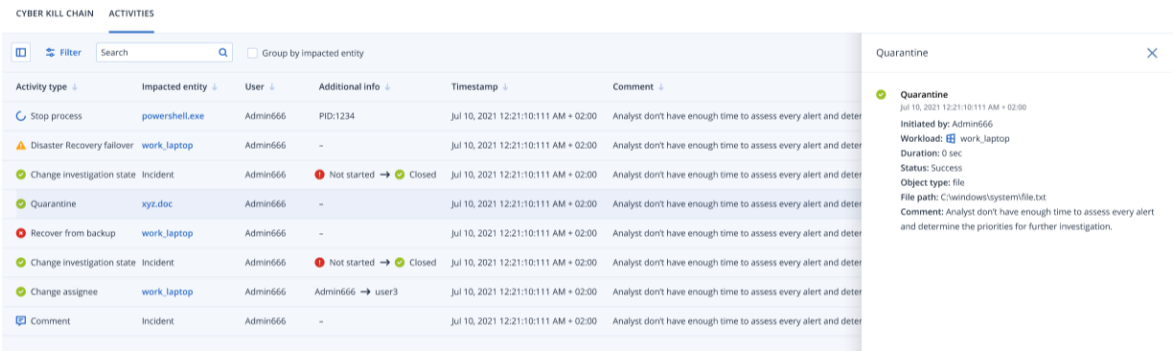
注意事項

預防層所建立的事件會自動套用在保護計劃中設定的動作。若是偵測點，您需要定義相關的回應動作，才能緩解每個攻擊案例。

為瞭解所採取的回應動作，您可以檢視套用到整個事件的所有回應動作，或檢視套用到事件網路攻擊鏈中特定節點的動作。

若要檢視套用到事件的所有回應動作

1. 在 Cyber Protect 主控台中，移至 **[防護] > [事件]**。
2. 在顯示的事件清單中，按一下您想要調查的事件最右側欄內的 。所選事件的網路攻擊鏈隨即顯示。
3. 按一下**[活動]**索引標籤。
   已套用到事件的回應動作清單隨即顯示。



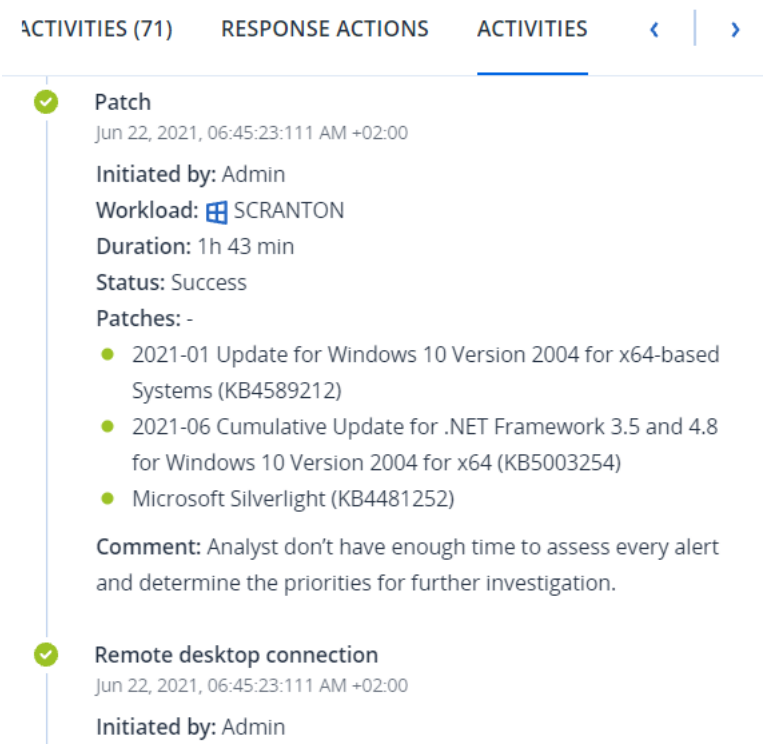
注意事項

如果回應動作是當作自動化工作流程一部分來起始，**[起始者]**欄位將顯示 **[自動化工作流程]**。如需詳細資訊，請參閱 "使用自動化工作流程" (第 852 頁)。

4. 您可以在顯示的清單上執行多個動作：
   - 按一下活動類型列可顯示所選活動的詳細資訊。資訊隨即顯示在側邊欄 (如步驟 3 中所示) 中，並包含動作起始者、其狀態、檔案路徑，以及起始者所新增之任何註解的詳細資料。
   - 使用 **[搜尋]**方塊可搜尋特定動作。
   - 按一下 **[篩選]**可將篩選條件套用至清單。
   - 選擇 **[依受影響的實體分組]**核取方塊，根據實體將相關動作分組。
   - 按一下 可顯示/隱藏已完成動作的清單。
     請確認 顯示在您要顯示的動作旁邊。如果您要從顯示的清單中隱藏某個動作，再按一下即可將其變更為 。

若要檢視套用到特定節點的回應動作

1. 在網路攻擊鏈中，按一下某個節點可檢視該節點的側邊欄。
2. 按一下**[活動]**索引標籤。



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).

注意事項
如果回應動作是當作自動化工作流程一部分來起始，**[起始者]**欄位將顯示**[自動化工作流程]**。如需詳細資訊，請參閱 "使用自動化工作流程"(第 852 頁)。

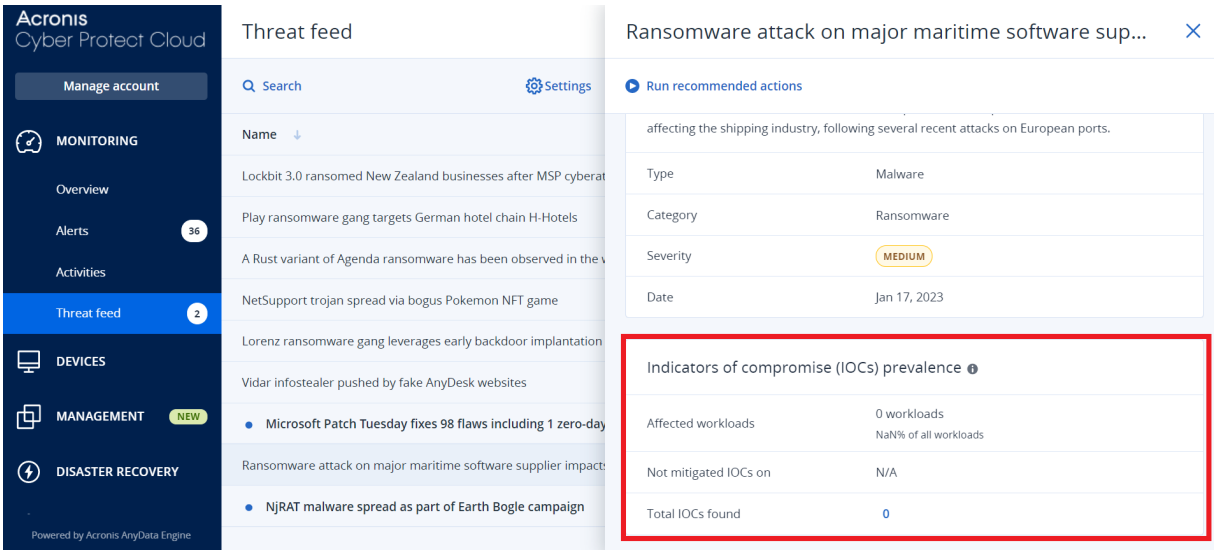
在對工作負載的公開攻擊中，檢查其入侵指標 (IOC)

Endpoint Detection and Response (EDR) 包含針對您的工作負載，檢閱威脅摘要中已知現有攻擊的功能。這些威脅摘要是根據接收自資安防護營運中心 (CPOC) 的威脅資料自動產生的；EDR 可讓您確認威脅是否將影響您的工作負載，然後採取必要的步驟來消除威脅。

您可以從 Cyber Protect 主控台中的**[監控]**功能表存取威脅摘要。如需詳細資訊，請參閱 "威脅摘要"(第 251 頁)。

若要檢視特定威脅的詳細資料並確認其是否影響您的工作負載，請按一下某個威脅摘要。您可以檢視偵測到的 IOC 數目和受影響的工作負載，並向下鑽研包含未緩解之 IOC 的工作負載。

注意事項
如果保護計劃未啟用 EDR，則不會顯示這個額外的威脅摘要功能，如下所示。



定義威脅摘要設定

您可以定義多個威脅摘要設定，以自動找出並緩解任何已知的威脅。

若要定義威脅摘要設定

1. 在 Cyber Protect 主控台中，移至 **[監控] > [威脅摘要]**。
2. 在顯示的 [威脅摘要] 頁面中，按一下 **[設定]**。
3. 在顯示的對話方塊中，執行下列任何一個選項：

選項	描述
搜尋入侵指標 (IOC)	按一下開關可對您的工作負載啟用自動搜尋 IOC。 啟用此選項時，也會顯示 **[與偵測相關的動作]** 和 **[產生警示]** 選項。
與偵測相關的動作	從下拉式清單中，選擇在工作負載上發現威脅時，要對相關檔案採取的動作： • **無動作** • **隔離** • **刪除** • **隔離工作負載**
產生警示	選擇在工作負載上找到 IOC 時產生警示的核取方塊。警示將會顯示在 [警示] 頁面中。

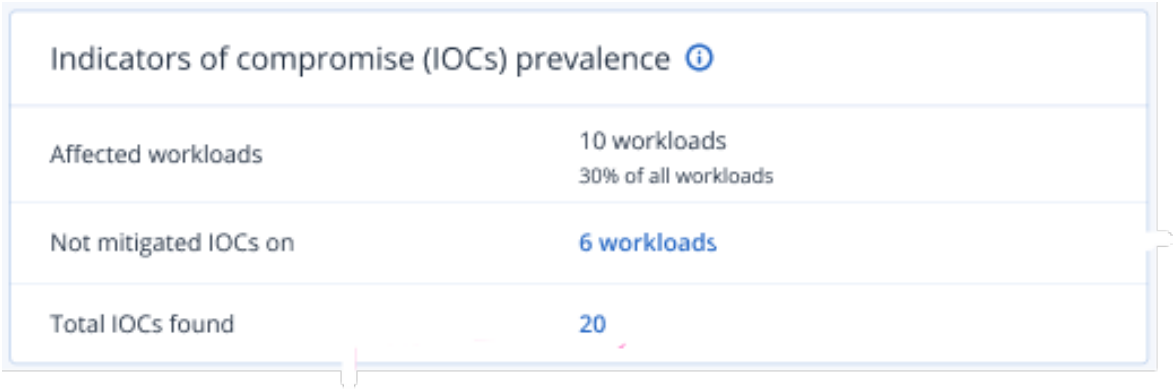
4. 按一下**[套用]**。

檢閱並緩解受影響工作負載上的 IOC

在保護計劃中啟用 [Endpoint Detection and Response (EDR)] 時，您可以在保護計劃中檢視影響工作負載的任何已知威脅。您也可以緩解未自動緩解的任何剩餘入侵指標 (IOC)。如需如何自動緩解 IDC 的相關資訊，請參閱 "定義威脅摘要設定" (第 829 頁)。

若要檢閱並緩解受影響的工作負載

1. 在 Cyber Protect 主控台中，移至 **[監控] > [威脅摘要]**。
2. 按一下某個威脅可顯示該威脅的詳細資料。
3. 在 **[入侵指標 (IOC) 流行程度]** 區段中，按一下 ***[n 工作負載]*** 連結可檢視具有未緩解 IOC 的工作負載。



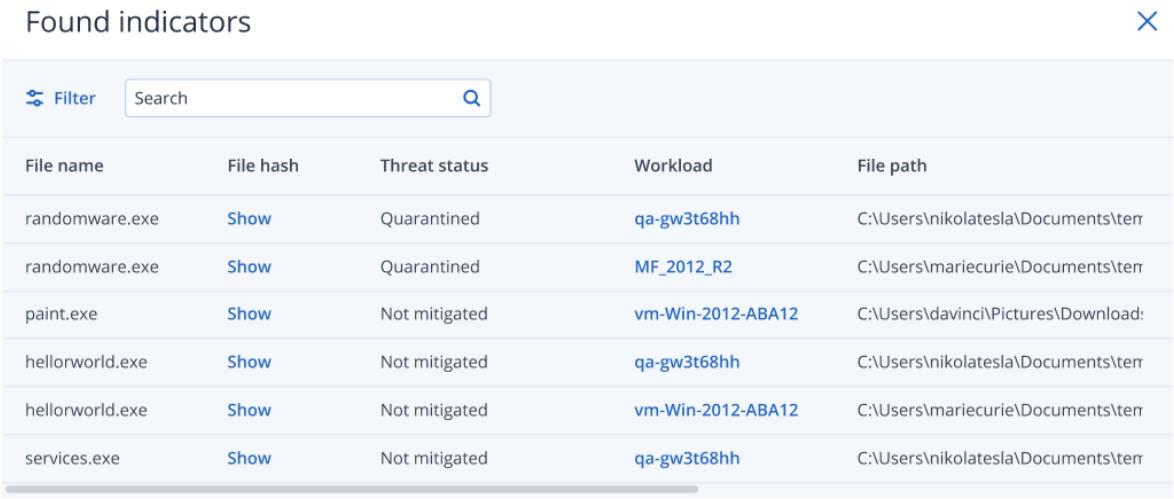
4. 在顯示的 [工作負載] 頁面中，按一下相關的工作負載並檢閱其詳細資料。您可以對工作負載執行特定的功能，包括定義要篩選的其他 URL (請參閱 "URL 篩選" (第 753 頁))，以及封鎖惡意程序 (請參閱 "防毒和防惡意程式保護設定" (第 733 頁) 中的「排除項目」一節)。
例如，如果威脅摘要指出某個工作負載受到 IOC 影響，請先找出並分析該 IOC，如 "檢閱並分析已發現的 IOC" (第 830 頁) 中所述。接著，移至工作負載的保護計劃，然後定義其他防護，例如，封鎖惡意檔案雜湊或程序。

檢閱並分析已發現的 IOC

除了檢閱受已知威脅影響的任何工作負載之外，您還可以檢閱並分析特定的入侵指標 (IOC)。這可讓您檢視受 IOC 影響的個別工作負載，並緩解 IOC。

若要檢閱並分析 IOC

1. 在 Cyber Protect 主控台中，移至 **[監控] > [威脅摘要]**。
2. 按一下某個威脅可顯示該威脅的詳細資料。
3. 在 **[入侵指標 (IOC) 流行程度]** 區段中，按一下 **[找到的 IOC 總計]** 連結。
[找到的指標] 頁面隨即顯示。



4. (選用) 使用 **[篩選]** 選項，根據 IOC 狀態篩選其清單。您也可以使用 **[搜尋]** 選項搜尋特定的 IOC。
5. 若要檢視受 IOC 影響的工作負載，請按一下 **[工作負載]** 欄中的連結。接著，您可以對工作負載執行各種動作，例如，執行修補程式管理或修改保護計劃。
6. (選用) 在 **[檔案雜湊]** 欄中，按一下 **[顯示]** 可顯示針對特定 IOC 找到的檔案雜湊。在顯示的對話方塊中，按一下 可將 IOC 的檔案雜湊複製到文字編輯器。

修復事件

Endpoint Detection and Response (EDR) 可讓您修復整個事件或事件的個別攻擊點。

您可以透過修復整個事件來選擇您要對事件全域執行的修復。如果您需要更精細地管理事件，可以根據需要，修復個別的攻擊點。例如，您可以隔離工作負載網路以阻止橫向移動或命令和控制 (C&C) 活動；這可確保即使工作負載遭到隔離，所有 Acronis Cyber Protect 技術仍可運作，而且可以發動調查。

EDR 可透過以下方式確保有效修復：

- 緩解 - 確保阻止威脅。
- 復原 - 確保服務立即恢復連線。
- 預防 - 確保在之後的攻擊中防止攻擊所使用的手法。

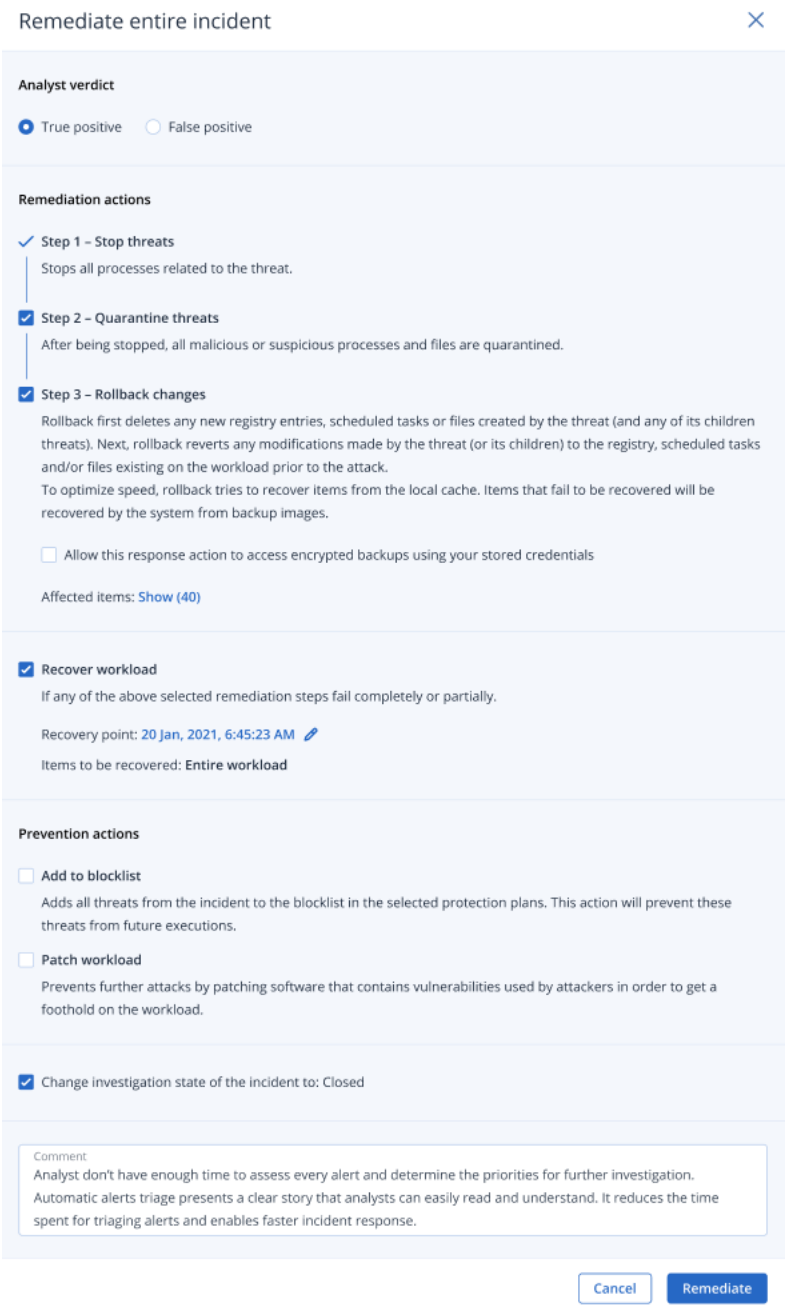
修復整個事件

您可以透過修復整個事件，快速且輕鬆地選擇您要對事件全域執行的修復。Endpoint Detection and Response (EDR) 會引導您逐步完成修復程序。

如果您需要更精細地管理網路和事件，請參閱 "個別網路攻擊鏈節點的回應動作" (第 835 頁)。

若要修復整個事件

1. 在 Cyber Protect 主控台中，移至 **[防護] > [事件]**。
2. 在顯示的事件清單中，按一下您想要調查的事件最右側欄內的 。所選事件的網路攻擊鏈隨即顯示。
3. 按一下 **[修復整個事件]**。[修復整個事件] 對話方塊隨即顯示。



4. 在 **[分析人員結果]** 區段中，根據您的事件調查，選擇以下其中一項：
   - **確判為真**：選擇您是否確定攻擊是真正的攻擊。一旦選擇之後，您要新增修復和預防動作，如以下步驟中所述。
   - **誤報**：選擇您是否確定攻擊不是真正的攻擊。在此模式下，您可以定義如何防止再次發生此攻擊，例如，透過將事件新增至保護計劃允許名單。

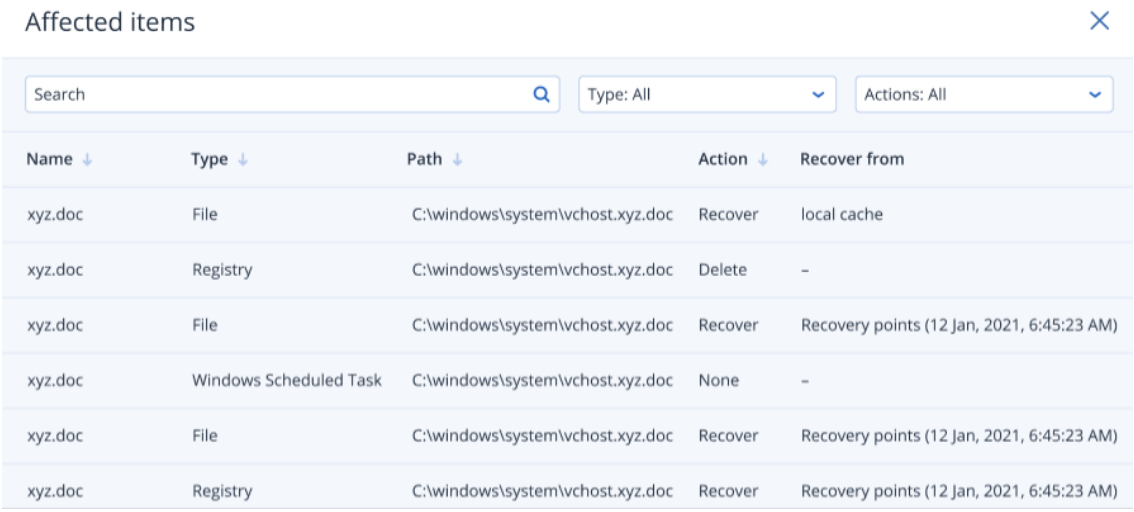
     注意事項
     選擇 **[誤報]** 之後，您僅能定義預防動作。如需詳細資訊，請參閱 "修復誤報事件" (第 834 頁)。

5. 在 **[修復動作]** 區段中，執行下列修復步驟。請注意，這些步驟必須循序執行，例如，不得先完成步驟 2 再完成步驟 1。

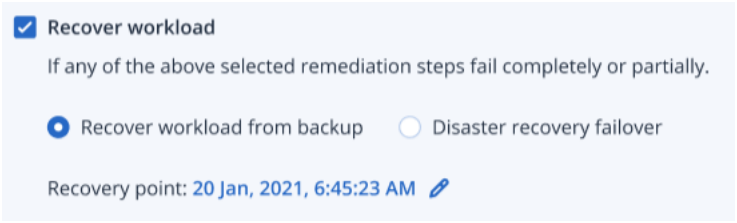
a. **步驟 1 - 阻止威脅**：選擇停止與威脅相關所有程序的核取方塊。
b. **步驟 2 - 隔離威脅**：一旦威脅遭到阻止之後，選擇隔離所有惡意和可疑程序與檔案的核取方塊。
c. **步驟 3 - 復原變更**：威脅遭到隔離之後，選擇刪除威脅 (及其任何子威脅) 所建立之任何新登錄項目、排程工作或檔案的核取方塊。接下來，復原程序會在威脅之前，將威脅 (或其子項) 所進行的任何修改還原至工作負載上現有的登錄檔、排程工作和/或檔案。為將速度最佳化，復原程序會嘗試從本機快取復原項目。無法復原的項目將會由系統從備份映像復原。

注意事項
復原程序僅能從本機快取中的項目復原。從備份存檔復原將在未來版本中提供。

如果對相關備份的存取經過加密，請選擇 **[允許此回應動作使用已儲存的認證存取加密備份]** 核取方塊。EDR 會存取已儲存的使用者認證，為加密存檔解密，並搜尋相關的檔案。
您也可以按一下 **[受影響的項目]** 來檢視受復原影響的所有項目 (檔案、登錄檔或排程工作)、所套用的動作 (**[刪除]**、**[復原]** 或 **[無]**)，以及這些項目是從本機快取還是備份映像還原。



d. **復原工作負載**：選擇如果以上任何修復步驟失敗 (無論是完全失敗還是部分失敗) 則復原工作負載的核取方塊。



選擇下列其中一個復原選項：

- **從備份復原工作負載**：可讓您從特定復原點復原工作負載。按一下復原點編輯圖示可從復原備份清單中選擇。
- **災難復原容錯移轉**：可讓您執行災難復原 (如果已在您的保護計劃中啟用此功能)。對於 AD 伺服器或資料庫伺服器等重要工作負載，建議您使用此選項。如需詳細資訊，請參閱 "實作災難復原" (第 655 頁)。

6. 在 **[預防動作]** 區段中，選擇相關的修復步驟：
   - **新增至封鎖名單**：選擇此核取方塊，並從顯示的保護計劃清單中，選擇相關的保護計劃。此預防動作可確保阻止對所選保護計劃執行所有事件偵測。
   - **修補工作負載**：選擇修補任何易受攻擊的軟體並防止攻擊者存取工作負載的核取方塊。接著，您可以在修補完成後，根據使用者是否已登入而定，選擇要執行的相關動作 (**[不要重新啟動]**、**[重新啟動]** 或 **[僅在必要時重新啟動]**)。
     您也可以選擇 **[請勿在備份正在進行時重新啟動]** 核取方塊來確保在備份期間不會重新啟動工作負載。

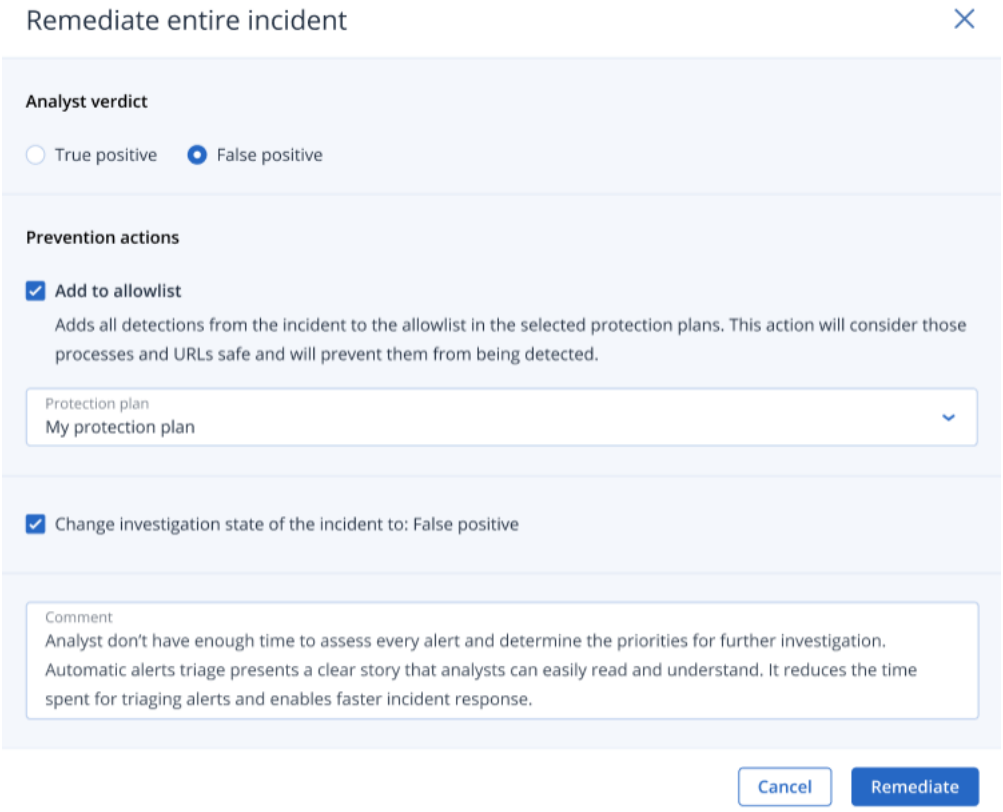
7. 選擇 **[將事件的調查狀態變更為：已結案]** 核取方塊。如果未選擇，調查狀態將維持其先前狀態。
8. 按一下**[修復]**。您選擇的修復動作將逐步執行，而且每個修復步驟的進度會顯示在 [修復整個事件] 對話方塊中。
   按一下之後，該按鈕會顯示 **[前往活動]**。按一下 **[前往活動]** 可檢閱已套用到事件的所有回應動作。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

修復誤報事件

如果您確定攻擊不是真正的攻擊 (即誤報)，則您可以定義如何防止事件再次發生。例如，您可以將事件新增至保護計劃允許名單。

若要修復誤報事件

1. 在所選事件的網路攻擊鏈中，按一下 **[修復整個事件]**。[修復整個事件] 對話方塊隨即顯示。
2. 在 **[分析人員結果]** 區段中，選擇 **[誤報]**。



3. 在 **[預防動作]** 區段中，選擇 **[新增至允許名單]** 核取方塊。從顯示的保護計劃清單中，選擇相關的保護計劃。
   此預防動作可確保不會針對所選保護計劃偵測所有事件偵測。
4. 選擇 **[將事件的調查狀態變更為：誤報]** 核取方塊。
5. 按一下 **[修復]**。
   按一下之後，該按鈕會顯示 **[前往活動]**。按一下 **[前往活動]** 可檢閱已套用到事件的回應動作。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

個別網路攻擊鏈節點的回應動作

如果您需要更精細地管理事件，可以將各種回應動作套用到個別的網路攻擊鏈節點。這些回應動作可讓您快速且輕鬆地修復任何節點。

注意事項
若要將全域回應動作套用到整個事件，請參閱 "修復整個事件" (第 831 頁)。

回應動作分成以下四個類別，但並非所有節點都包含以下所有類別：

- **修復**：此類別中的動作可讓您將立即回應套用到攻擊，包括管理工作負載的網路隔離，以及刪除和隔離檔案、程序和登錄值。
- **調查**：此類別中的動作 (僅適用於工作負載) 可讓您執行鑑識備份或遠端桌面連線，以便進行更深入的調查。

- **調查**:此類別中的動作 (僅適用於工作負載) 可讓您執行遠端桌面連線,以進行更深入的調查。
- **復原**:此類別中的動作 (僅適用於工作負載) 可讓您透過從備份執行復原或災難復原容錯移轉來回應密集的攻擊。
- **預防**:此類別中的動作可讓您將威脅和誤報新增至保護計劃允許名單或封鎖名單,以防止之後發生。

注意事項

如果事件已結案,您就無法將回應動作套用至節點。不過,您可以將事件的調查狀態變更為 **[調查中]**,以重新開啟已結案的事件。重新開啟後,您就可以套用回應動作。

下表描述網路攻擊鏈中的每個節點類型、適用於每個節點的類別,以及可用的回應動作。

節點	類別	回應動作
工作負載	修復	• 管理網路隔離 • 重新啟動工作負載
	調查	• 鑑識備份 • 遠端桌面連線
	調查	• 遠端桌面連線
	復原	• 從備份復原 • 災難復原容錯移轉
	預防	• 修補程式
程序	修復	• 停止程序 • 隔離
	預防	• 新增至允許名單 • 新增至封鎖名單
檔案	修復	• 刪除 • 隔離
	預防	• 新增至允許名單 • 新增至封鎖名單

節點	類別	回應動作
登錄	修復	• 刪除
網路	預防	• 新增至允許名單 • 新增至封鎖名單

定義受影響工作負載的回應動作

您可以將下列動作套用到受影響的工作負載，作為您對攻擊的回應：

- **管理網路隔離**：可讓您管理工作負載的網路隔離以阻止橫向移動或命令和控制 (C&C) 活動。如需詳細資訊，請參閱 "管理工作負載的網路隔離" (第 837 頁)。
- **修補**：可讓您修補工作負載，以防止將來在之後的潛在攻擊中利用弱點。如需詳細資訊，請參閱 "修補工作負載" (第 840 頁)。
- **重新啟動工作負載**：可讓您立即重新啟動工作負載，或根據預先定義的逾時期間，重新啟動工作負載。如需詳細資訊，請參閱 "重新啟動工作負載" (第 841 頁)。
- **鑑識備份**：可讓您執行按需鑑識備份以供稽核或進一步調查之用。如需詳細資訊，請參閱 "在工作負載上執行按需鑑識備份" (第 842 頁)
- **遠端桌面連線**：可讓您從遠端存取調查中的工作負載。如需詳細資訊，請參閱 "工作負載的遠端連線" (第 843 頁)。
- **從備份復原**：可讓您從備份復原整部電腦，或復原特定的檔案或資料夾。如需詳細資訊，請參閱 "從備份復原" (第 844 頁)。
- **災難復原容錯移轉**：可讓您執行 "實作災難復原" (第 655 頁)。請注意，您的工作負載中必須包含 Advanced Disaster Recovery 的訂購授權。如需詳細資訊，請參閱 "災難復原容錯移轉" (第 845 頁)。

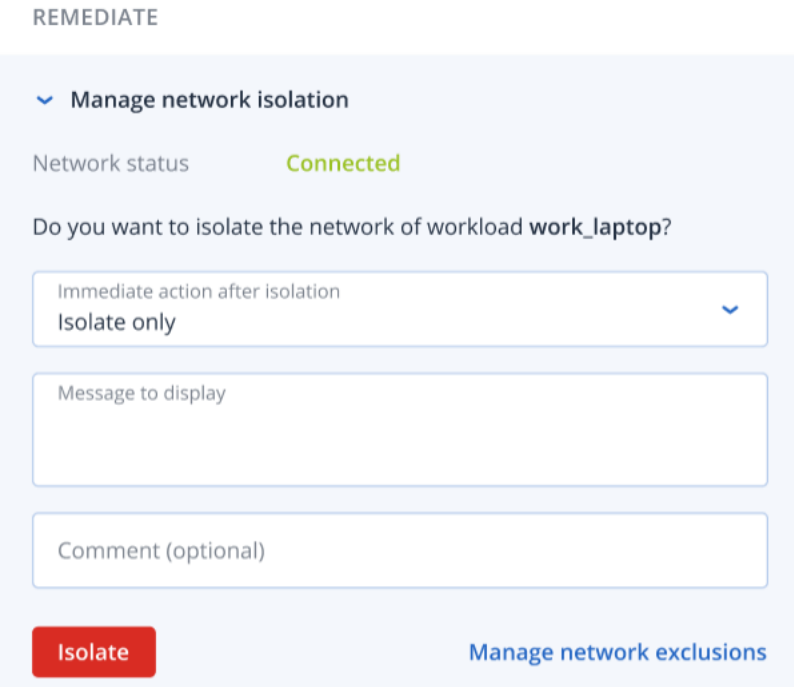
管理工作負載的網路隔離

EDR 可讓您管理工作負載的網路隔離以阻止橫向移動或命令和控制 (C&C) 活動。根據您的需求，有一些隔離選項可供選擇。請注意，即使工作負載遭到隔離，所有 Acronis Cyber Protect 技術都還是可以運作，如此可確保能夠全面展開調查。

若要從網路隔離工作負載

1. 在網路攻擊鏈中，按一下您要修復的工作負載節點。
2. 在顯示的側邊欄中，按一下 **[回應動作]** 索引標籤。

3. 在 **[修復]** 區段中，按一下 **[管理網路隔離]**。



注意事項
[網路狀態] 值可指出工作負載目前是否已連線。如果此值顯示 **[已隔離]**，則您可以將已隔離的工作負載重新連線至網路，如以下程序中所述。如果工作負載離線，您仍然可以隔離工作負載，但是當工作負載恢復連線時，會自動將該工作負載置於 **[已隔離]** 狀態。

4. 在 **[隔離後的立即動作]** 下拉式清單中，選擇以下其中一項：
   - **僅隔離**
   - **隔離與備份工作負載**
   - **隔離與備份具有鑑識資料的工作負載**
   - **隔離並關閉工作負載**

   如需有關定義備份位置和加密選項的詳細資訊，請參閱 "管理工作負載和檔案的備份與復原" (第 353 頁)。
5. [選用] 在 **[要顯示的訊息]** 欄位中，新增存取已隔離的工作負載時，要向終端使用者顯示的訊息。例如，您可以通知使用者工作負載現在遭到隔離，而且目前無法使用網路存取工作負載。請注意，此訊息也會顯示為系統匣監視器通知，而且在使用者關閉訊息前會持續顯示。
6. [選用] 在 **[註解]** 欄位中，新增註解。此註解可在 **[活動]** 索引標籤中看到 (針對單一節點或整個事件)，而且可以協助您 (或您的同事) 在重新造訪該事件時回想起您採取該動作的原因。
7. 按一下 **[管理網路排除項目]** 可新增能夠在隔離期間存取工作負載的連接埠、URL、主機名稱和 IP 位址。如需詳細資訊，請參閱如何管理網路排除項目。
8. 按一下 **[隔離]**。
   工作負載隨即遭到隔離。您也可以在個別節點或整個事件的 **[活動]** 索引標籤中檢視此動作。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

注意事項

工作負載在 Cyber Protect 主控台的 **[工作負載]** 功能表下，也會顯示為 **[已隔離]**。您也可以從 **[工作負載] > [含代理程式的工作負載]** 功能表隔離單一或多個工作負載；選擇相關的工作負載，然後在右側邊欄中，選擇 **[管理網路隔離]**。在顯示的對話方塊中，您可以管理網路排除項目，然後按一下 **[隔離]** 或 **[全部隔離]**，即可隔離所選工作負載。

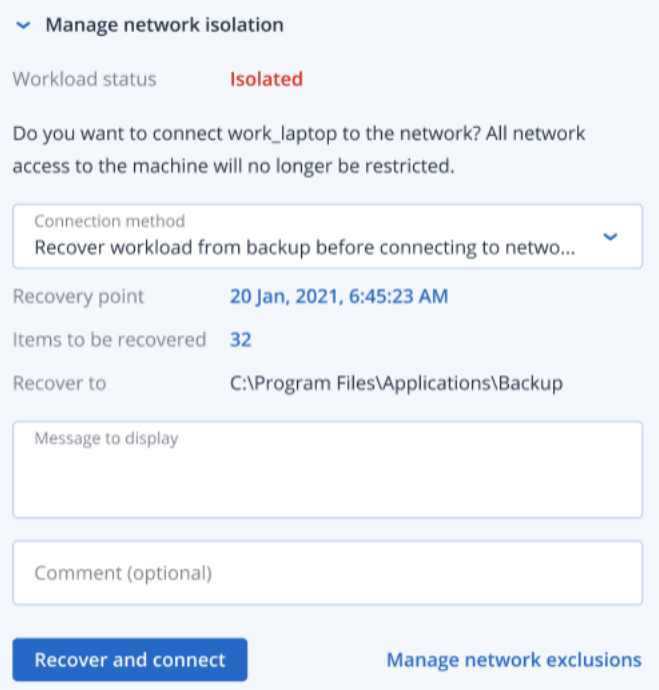
若要將已隔離的工作負載連線回網路

1. 在網路攻擊鏈中，按一下您要重新連線的工作負載節點。

注意事項

如果已隔離的工作負載目前離線，您仍然可以將其重新連線回網路，但是當工作負載恢復連線時，會自動將該工作負載置於 **[已連線]** 狀態。

2. 在顯示的側邊欄中，按一下 **[回應動作]** 索引標籤。
3. 在 **[修復]** 區段中，按一下 **[管理網路隔離]**。
4. 選擇以下其中一項：
   - **立即連線到網路**：工作負載會重新連線至網路。
   - **從備份復原工作負載，然後再連線至網路**：選擇要從中復原工作負載的復原點。
     a. 在 **[復原點]** 欄位中，按一下 **[選擇]**。
     b. 在顯示的側邊欄中，選擇相關的復原點。
     c. 按一下 **[復原] > [整個工作負載]** 可復原工作負載上的所有檔案和資料夾。
     或者
     按一下 **[復原] > [檔案/資料夾]** 可復原工作負載上的特定檔案和資料夾。接著，系統會提示您選擇相關的檔案或資料夾。一旦選擇之後，您可以按一下 **[要復原的項目]** 欄位中的相關值，即可檢視項目清單。



注意事項
如果您選擇的復原點經過加密，則系統會提示您輸入密碼。

5. [選用] 選擇 **[需要時，自動重新啟動工作負載]** 核取方塊。只有當您在步驟 4 中選擇 **[復原] > [整個工作負載]** 時，此選項才相關。
6. [選用] 在 **[要顯示的訊息]** 欄位中，新增存取已連線的工作負載時，要向終端使用者顯示的訊息。例如，您可以通知使用者備份已還原到工作負載，而且已恢復使用網路存取工作負載。
7. [選用] 在 **[註解]** 欄位中，新增註解。此註解可在 **[活動]** 索引標籤中看到 (針對單一節點或整個事件)，而且可以協助您 (或您的同事) 在重新造訪該事件時回想起您採取該動作的原因。
8. 如果您在步驟 4 中選擇 **[立即連線到網路]**，則按一下 **[連線]**。
   或者
   如果您在步驟 4 中選擇 **[從備份復原工作負載，然後再連線至網路]**，則按一下 **[復原並連]**。
   工作負載會重新連線至網路，而且對於工作負載的所有網路存取將不再受到限制。

注意事項
您也可以從 Cyber Protect 主控台中的 **[工作負載] > [含代理程式的工作負載]** 功能表連線單一或多個已隔離的工作負載；選擇相關的工作負載，然後在右側邊欄中，選擇 **[管理網路隔離]**。在顯示的對話方塊中，按一下 **[連線]** 或 **[全部連線]**，以便將所選工作負載連線至網路。

若要管理網路排除項目

注意事項
即使在工作負載處於隔離狀態時所有 Acronis Cyber Protect 技術都還可以運作，還是有一些情況您需要額外建立網路連線 (例如，您可能需要將檔案從工作負載上傳至共用目錄)。在這些情況下，您可以新增網路排除項目，但要在您新增排除項目之前，確保已移除所有威脅。

1. 在 **[回應動作]** 索引標籤的 **[修復]** 區段中，按一下 **[管理網路排除項目]**。
2. 在 [網路排除項目] 側邊欄中，新增相關的排除項目。針對每個可用的選項 (連接埠、URL 位址，以及主機名稱/IP 位址)，執行以下操作：
   a. 按一下 **[新增]**，然後輸入相關的連接埠、URL 位址，或主機名稱/IP 位址。
   b. 在 **[流量方向]** 下拉式清單中，選擇 **[傳入和傳出連線]**、**[僅傳入連線]** 或 **[僅傳出連線]**。
   c. 按一下 **[新增]**。
3. 按一下 **[儲存]**。

修補工作負載

EDR 會自動檢查工作負載是否需要修補程式，並可讓您修補工作負載以防止將來在之後的潛在攻擊中利用弱點。請注意，只有在合作夥伴的工作負載有 Advanced Management 的訂購授權時，才可以使用此功能。

若要修補工作負載

1. 在網路攻擊鏈中，按一下您要修補的工作負載節點。
2. 在顯示的側邊欄中，按一下 **[回應動作]** 索引標籤。

3. 在 **[修復]** 區段中，按一下 **[修補]**。
4. 在 **[要安裝的修補程式]** 欄位中，按一下 **[選擇]**。在顯示的對話方塊中，選擇相關的修補程式，然後按一下 **[選擇]**。
5. 在 **[安裝後選項]** 欄位中，按一下顯示的連結。[安裝後選項] 對話方塊隨即顯示。
6. 選擇您是否要在安裝修補程式後將電腦重新開機：

選項	描述
否	安裝修補程式後，電腦將不會自動重新開機。
可以	安裝修補程式後，電腦將會自動重新開機。您也可以排程重新開機時間。
如有需要	只有在需要套用修補程式時，才會將電腦重新開機。

7. [選用] 選擇 **[在備份完成之前，請不要重新開機]** 核取方塊可確保正在進行備份時不會重新啟動工作負載。
8. 按一下 **[儲存]**。
9. 在 **[回應動作]** 索引標籤中，按一下 **[修補]**。
   所選修補程式隨即執行。您也可以在個別節點或整個事件的 **[活動]** 索引標籤中檢視此動作。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

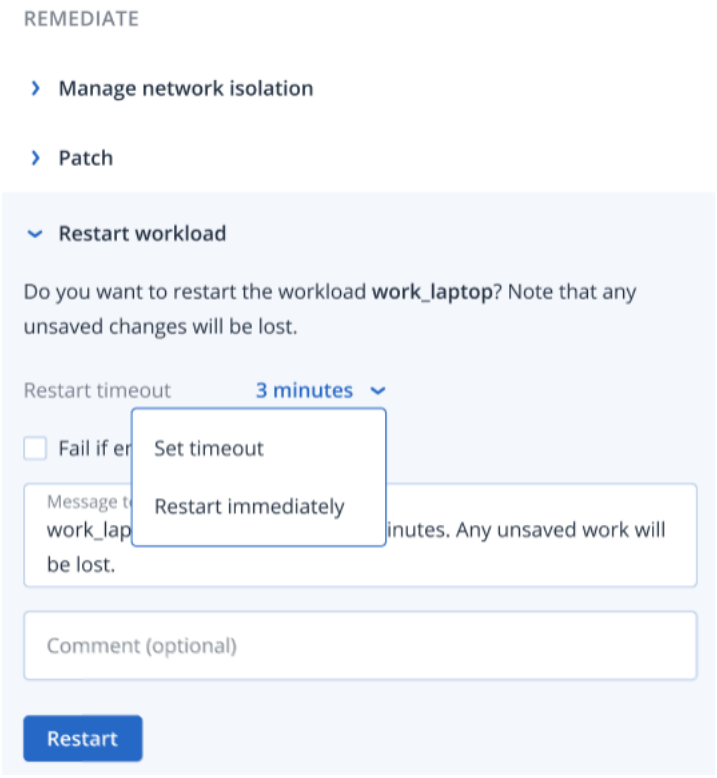
重新啟動工作負載

EDR 可讓您立即重新啟動工作負載，或根據預先定義的逾時期間，重新啟動工作負載，作為您對攻擊的修復回應。

若要重新啟動工作負載

1. 在網路攻擊鏈中，按一下您要為其重新啟動排程的工作負載節點。
2. 在顯示的側邊欄中，按一下 **[回應動作]** 索引標籤。

3. 在 **[修復]** 區段中，按一下 **[重新啟動工作負載]**。



4. 在 **[重新啟動逾時]** 欄位中，按一下顯示的連結，然後選擇下列其中一項：
   - **設定逾時**：在 [重新啟動逾時] 對話方塊中，設定工作負載的重新啟動期間，然後按一下 **[儲存]**。
   - **立即重新啟動**：選擇立即重新啟動工作負載。
5. [選用] 選擇 **[如果使用者已登入，則失敗]** 核取方塊可確保使用者登入時不會重新啟動工作負載。
6. 在 **[要顯示的訊息]** 欄位中，新增存取已隔離的工作負載時，要向使用者顯示的訊息。
7. [選用] 在 **[註解]** 欄位中，新增註解。此註解可在 **[活動]** 索引標籤中看到 (針對單一節點或整個事件)，而且可以協助您 (或您的同事) 在重新造訪該事件時回想起您採取該動作的原因。
8. 按一下 **[重新啟動]**。
   工作負載設定為根據定義的排程重新啟動。您也可以在個別節點或整個事件的 **[活動]** 索引標籤中檢視此動作。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

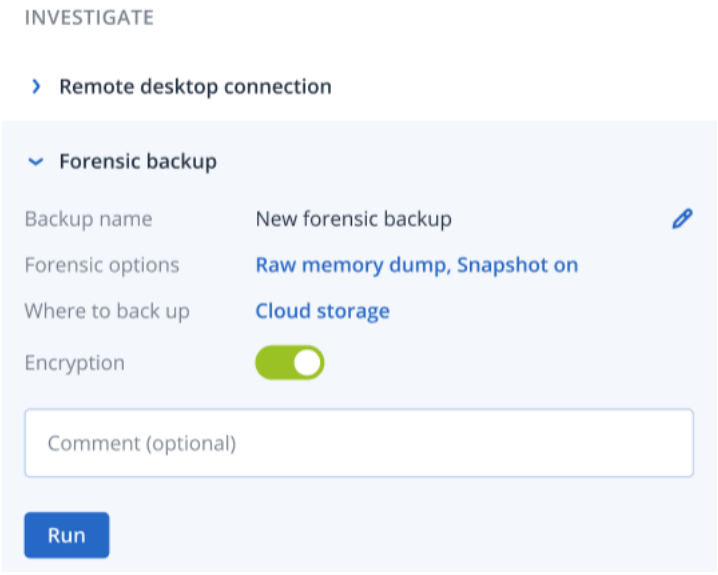
在工作負載上執行按需鑑識備份

調查攻擊時，EDR 可讓您執行按需鑑識備份以供稽核或進一步調查之用。請注意，只有在合作夥伴的工作負載有 Advanced Backup 的訂購授權時，才可以使用此功能。

若要執行鑑識備份

1. 在網路攻擊鏈中，按一下您要對其執行鑑識備份的工作負載節點。
2. 在顯示的側邊欄中，按一下 **[回應動作]** 索引標籤。

3. 在 **[調查]** 區段中，按一下 **[鑑識備份]**。



4. [選擇性] 在 **[備份名稱]** 欄位中，按一下編輯圖示以編輯備份名稱。
5. 在 **[鑑識選項]** 欄位中，按一下顯示的連結。在顯示的 [鑑識選項] 對話方塊中，選擇下列其中一項：
   - **收集原始記憶體傾印**
   - **收集核心記憶體傾印**

   您也可以選擇 **[執行中程序的快照]** 核取方塊，以新增備份開始時執行之程序的相關資訊。此資訊儲存在備份映像中。

   按一下 **[儲存]** 以關閉 [鑑識選項] 對話方塊。
6. 在 **[備份位置]** 欄位中，按一下所顯示的連結，以定義備份位置。
7. [選擇性] 按一下 **[加密]** 選項以啟用加密。在顯示的對話方塊中，輸入加密備份的密碼，然後選擇相關的加密演算法。
8. [選用] 在 **[註解]** 欄位中，新增註解。此註解可在 **[活動]** 索引標籤中看到 (針對單一節點或整個事件)，而且可以協助您 (或您的同事) 在重新造訪該事件時回想起您採取該動作的原因。
9. 按一下 **[執行]**。

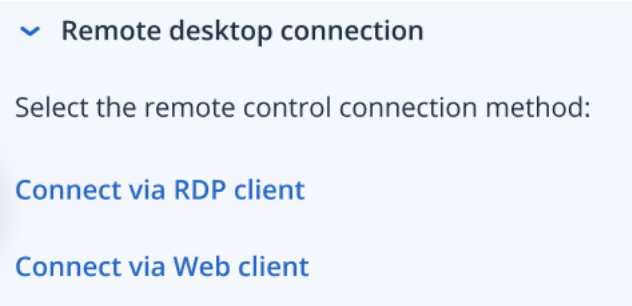
   鑑識備份隨即開始。您也可以在個別節點或整個事件的 **[活動]** 索引標籤中檢視此動作。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

工作負載的遠端連線

調查攻擊時，EDR 可讓從遠端存取調查中的工作負載。

若要從遠端連線到工作負載

1. 在網路攻擊鏈中，按一下您要從遠端連線的工作負載節點。
2. 在顯示的側邊欄中，按一下 **[回應動作]** 索引標籤。
3. 在 **[調查]** 區段中，按一下 **[遠端桌面連線]**。



4. 選擇下列其中一個遠端連線方法：
   - **透過 RDP 用戶端連線**：此方法將會提示您下載並安裝 Remote Desktop Connection Client。接著，您可以從 主控台遠端連線到工作負載。
   - **透過 Web 用戶端連線**：此方法不需要在工作負載上安裝 RDP 用戶端。系統會將您重新導向至必須輸入遠端電腦的認證所在的登入畫面。

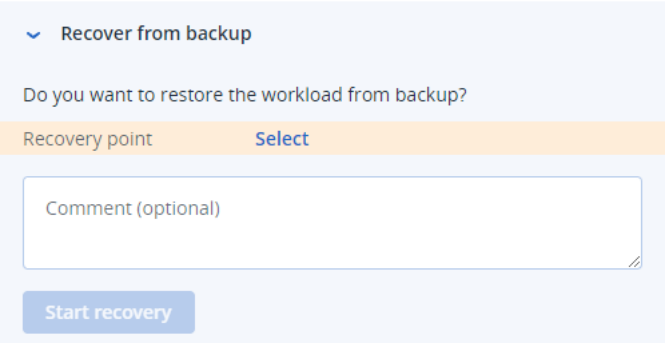
   啟動遠端連線時，您可以在個別節點和整個事件的 **[活動]** 索引標籤中檢視此動作。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

從備份復原

EDR 可讓您從備份復原整部電腦，或復原特定的檔案或資料夾，作為您對攻擊的復原回應。

若要從備份復原工作負載

1. 在網路攻擊鏈中，按一下您要復原的工作負載節點。
2. 在顯示的側邊欄中，按一下 **[回應動作]** 索引標籤。
3. 在 **[復原]** 區段中，按一下 **[從備份復原]**。



4. 在 **[復原點]** 欄位中，按一下 **[選擇]**，然後執行下列步驟：
   a. 在顯示的側邊欄中，選擇相關的復原點。
   b. 按一下 **[復原] > [整個工作負載]** 可復原工作負載上的所有檔案和資料夾。

      或者

      按一下 **[復原] > [檔案/資料夾]** 可復原工作負載上的特定檔案和資料夾。接著，系統會提示您選擇相關的檔案或資料夾。一旦選擇之後，您可以按一下 **[要復原的項目]** 欄位中的相關值，即可檢視針對復原所選擇的項目。

      注意事項
      如果您選擇的復原點經過加密，則系統會提示您輸入密碼。

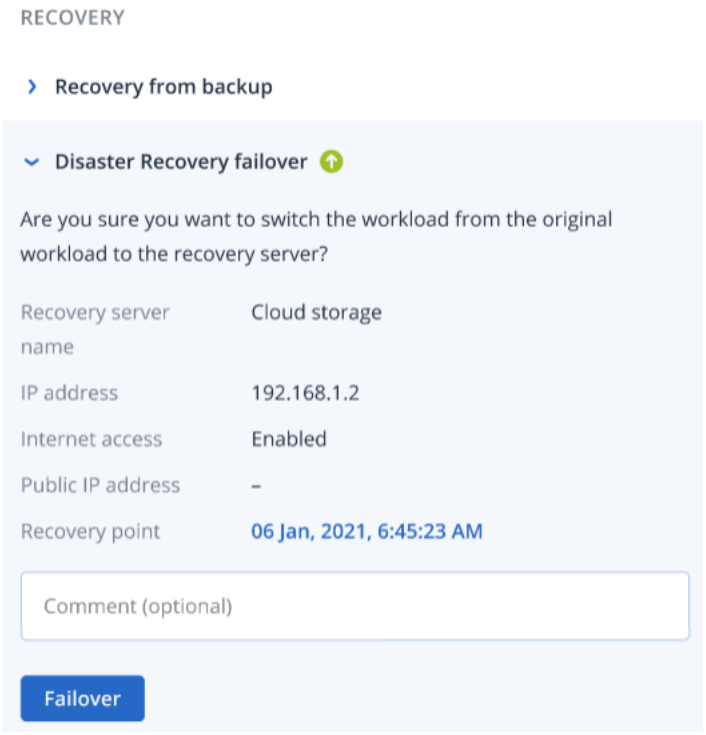
5. [選用] 選擇 **[自動重新啟動工作負載]** 核取方塊。只有當您在步驟 4 中選擇 **[復原] > [整個工作負載]** 時，此選項才相關。
6. [選用] 在 **[註解]** 欄位中，新增註解。此註解可在 **[活動]** 索引標籤中看到 (針對單一節點或整個事件)，而且可以協助您 (或您的同事) 在重新造訪該事件時回想起您採取該動作的原因。
7. 按一下 **[開始復原]**。
   復原工作負載的程序隨即開始。您可以在個別節點或整個事件的 **[活動]** 索引標籤中檢視此動作的程序。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

災難復原容錯移轉

EDR 可讓您執行 "實作災難復原" (第 655 頁)，作為您對攻擊的復原回應，這允許您將工作負載切換到復原伺服器。請注意，您的工作負載中必須包含 Advanced Disaster Recovery 的訂購授權。

若要執行災難復原容錯移轉

1. 在網路攻擊鏈中，按一下您要復原的工作負載節點。
2. 在顯示的側邊欄中，按一下 **[回應動作]** 索引標籤。
3. 在 **[復原]** 區段中，按一下 **[災難復原容錯移轉]**。



4. 在 **[復原點]** 欄位中，執行下列步驟：
   a. 按一下目前的復原點日期以選擇復原點。
   b. 在顯示的側邊欄中，選擇相關的復原點。

注意事項
如果您有 Advanced Disaster Recovery 訂購授權，可以選擇在 [災難復原] 中建立的相關復原伺服器 (離線 VM)。如果您沒有訂購授權，系統將會提示您設定災難復原。

5. [選用] 在 **[註解]** 欄位中，新增註解。此註解可在 **[活動]** 索引標籤中看到 (針對單一節點或整個事件)，而且可以協助您 (或您的同事) 在重新造訪該事件時回想起您採取該動作的原因。
6. 按一下 **[容錯移轉]**。
   工作負載隨即切換到復原伺服器。您可以在個別節點或整個事件的 **[活動]** 索引標籤中檢視此動作。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

定義可疑程序的回應動作

您可以將下列動作套用到可疑程序，作為您對攻擊的修復回應：

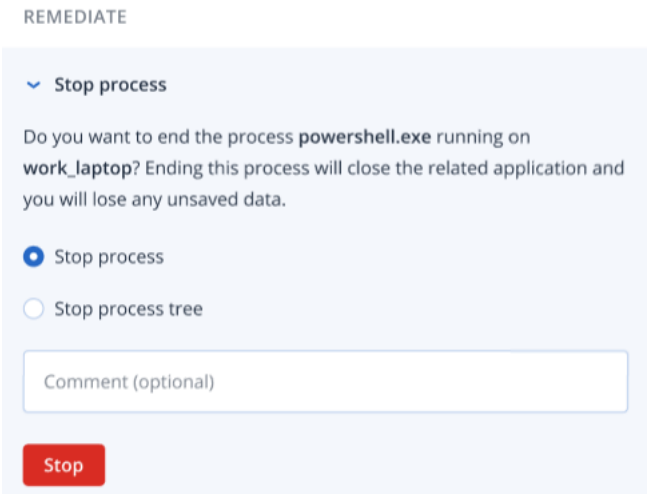
- 停止程序 (請參閱以下內容)
- 隔離程序 (請參閱以下內容)
- 復原程序所做的變更 (請參閱以下內容)
- 將程序新增至保護計劃允許名單或封鎖名單 (請參閱 "在保護計劃封鎖名單或允許名單中新增或移除程序、檔案或網路" (第 850 頁))

若要停止可疑程序

1. 在網路攻擊鏈中，按一下您要修復的程序節點。

   注意事項
   您無法停止 Windows 重要程序或非執行中程序，要在網路攻擊鏈中停用。

2. 在顯示的側邊欄中，按一下 **[回應動作]** 索引標籤。
3. 在 **[修復]** 區段中，按一下 **[停止程序]**。



4. 選擇下列一項：
   - **停止程序** (停止特定程序)
   - **停止程序樹狀結構** (停止特定程序和所有子程序)
5. [選用] 新增註解。此註解可在 **[活動]** 索引標籤中看到 (針對單一節點或整個事件)，而且可以協助您 (或您的同事) 在重新造訪該事件時回想起您採取該動作的原因。

6. 按一下 **[停止]**。程序隨即停止。

注意事項
相關的應用程式會關閉，而且將會失去所有未儲存的資料。

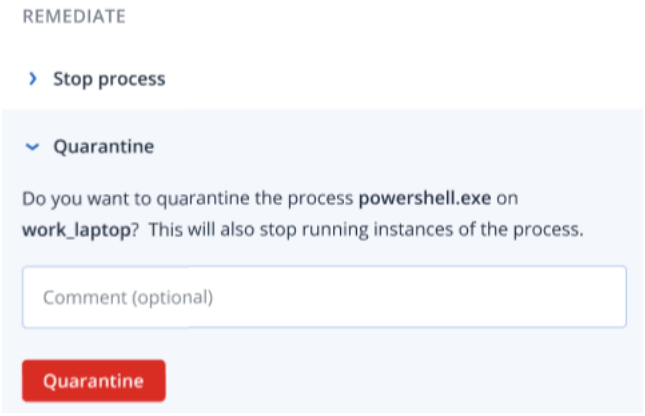
您也可以在個別節點或整個事件的 **[活動]** 索引標籤中檢視此動作。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

若要隔離可疑程序

1. 在網路攻擊鏈中，按一下您要隔離的程序節點。

注意事項
您無法隔離 Windows 重要程序，要在網路攻擊鏈中停用。

2. 在顯示的側邊欄中，按一下 **[回應動作]** 索引標籤。
3. 在 **[修復]** 區段中，按一下 **[隔離]**。



4. [選用] 新增註解。此註解可在 **[活動]** 索引標籤中看到 (針對單一節點或整個事件)，而且可以協助您 (或您的同事) 在重新造訪該事件時回想起您採取該動作的原因。
5. 按一下 **[隔離]**。程序隨即停止，然後隔離。

注意事項
系統會該程序新增到 [防惡意軟體防護] 下的隔離區段並進行管理。

您也可以在個別節點或整個事件的 **[活動]** 索引標籤中檢視此動作。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

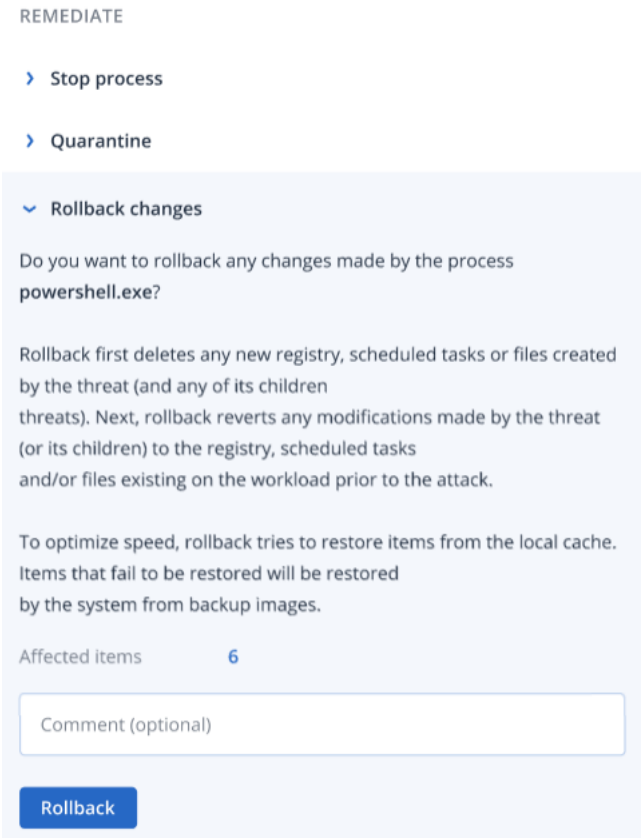
若要復原變更

1. 在網路攻擊鏈中，按一下您要復原其變更的程序節點。

注意事項
此動作僅適用於偵測節點 (顯示為紅色或黃色節點)。

2. 在顯示的側邊欄中，按一下 **[回應動作]** 索引標籤。

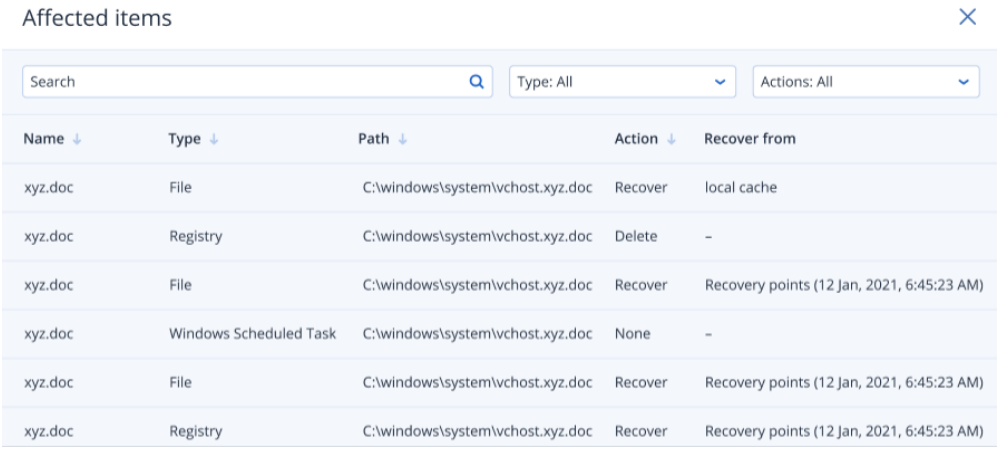
3. 在 **[修復]** 區段中，按一下 **[復原變更]**。



注意事項

復原程序僅能從本機快取中的項目復原。從備份存檔復原將在未來版本中提供。

4. 若要檢視受復原變更影響的項目，請按一下 **[受影響的項目]** 連結。所顯示的對話方塊會顯示復原將還原的所有項目 (檔案、登錄檔、排程工作)，及其所使用的動作 (**[刪除]**、**[復原]** 或 **[無]**)。此外，您可以查看還原的項目將從本機快取還是備份復原點復原。



5. [選用] 新增註解。此註解可在 **[活動]** 索引標籤中看到 (針對單一節點或整個事件)，而且可以協助您 (或您的同事) 在重新造訪該事件時回想起您採取該動作的原因。
6. 按一下 **[復原]**。復原功能會使用以下步驟，還原程序對任何登錄檔、檔案或排程工作所做的變更：

a. 威脅 (及其子威脅) 所建立的任何新項目 (登錄檔、排程工作、檔案) 都會遭到刪除。
b. 威脅 (及其子威脅) 對攻擊前存在於工作負載上的登錄檔、排程工作和/或檔案所做的任何修改都會還原。
c. 復原會嘗試從本機快取復原項目。對於無法復原的項目，EDR 將會自動從清理備份映像中復原這些項目。

您也可以在個別節點或整個事件的 **[活動]** 索引標籤中檢視復原動作。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

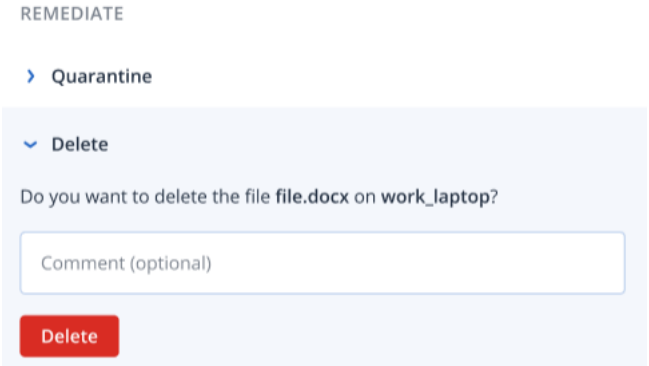
定義可疑檔案的回應動作

您可以將下列動作套用到可疑檔案，作為您對攻擊的修復回應：

- 刪除檔案 (請參閱以下內容)
- 隔離檔案 (請參閱以下內容)
- 將檔案新增至保護計劃允許名單或封鎖名單 (請參閱 "在保護計劃封鎖名單或允許名單中新增或移除程序、檔案或網路" (第 850 頁))

若要刪除可疑檔案

1. 在網路攻擊鏈中，按一下您要修復的檔案節點。
2. 在顯示的側邊欄中，按一下 **[回應動作]** 索引標籤。
3. 在 **[修復]** 區段中，按一下 **[刪除]**。

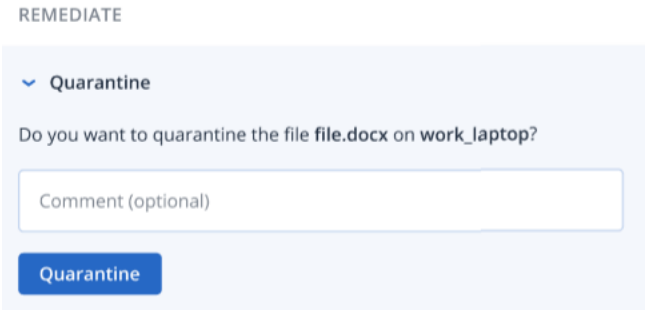


4. [選用] 新增註解。此註解可在 **[活動]** 索引標籤中看到 (針對單一節點或整個事件)，而且可以協助您 (或您的同事) 在重新造訪該事件時回想起您採取該動作的原因。
5. 請按一下 **[刪除]**。
檔案隨即遭到刪除。您也可以在個別節點或整個事件的 **[活動]** 索引標籤中檢視此動作。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

若要隔離可疑檔案

1. 在網路攻擊鏈中，按一下您要修復的檔案節點。
2. 在顯示的側邊欄中，移至 **[回應動作]**。

3. 在 **[修復]** 區段中，按一下 **[隔離]**。



4. [選用] 新增註解。此註解可在 **[活動]** 索引標籤中看到 (針對單一節點或整個事件)，而且可以協助您 (或您的同事) 在重新造訪該事件時回想起您採取該動作的原因。
5. 按一下 **[隔離]**。
   檔案隨即遭到隔離。您也可以在個別節點或整個事件的 **[活動]** 索引標籤中檢視此動作。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

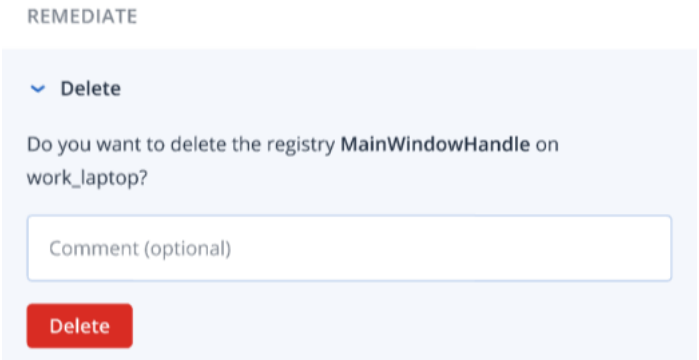
定義可疑登錄項目的回應動作

您可以刪除可疑登錄項目，作為您對攻擊的修復回應。

此選項適用於登錄網路攻擊鏈節點。

若要刪除可疑登錄項目

1. 在網路攻擊鏈中，按一下您要修復的節點。
2. 在顯示的側邊欄中，按一下 **[回應動作]** 索引標籤。
3. 在 **[修復]** 區段中，按一下 **[刪除]**。



4. [選用] 新增註解。此註解可在 **[活動]** 索引標籤中看到 (針對單一節點或整個事件)，而且可以協助您 (或您的同事) 在重新造訪該事件時回想起您採取該動作的原因。
5. 請按一下 **[刪除]**。
   登錄項目隨即遭到刪除。您也可以在個別節點或整個事件的 **[活動]** 索引標籤中檢視此動作。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

在保護計劃封鎖名單或允許名單中新增或移除程序、檔案或網路

您可以將某個節點新增到您的保護計劃允許名單或封鎖名單中，作為對攻擊的預防性回應的一部分。

如果您認為某個節點安全無虞，而且希望防止之後對其進行任何偵測，可以將該節點新增至允許名單中。將某個節點新增到封鎖名單可阻止之後執行該節點將。

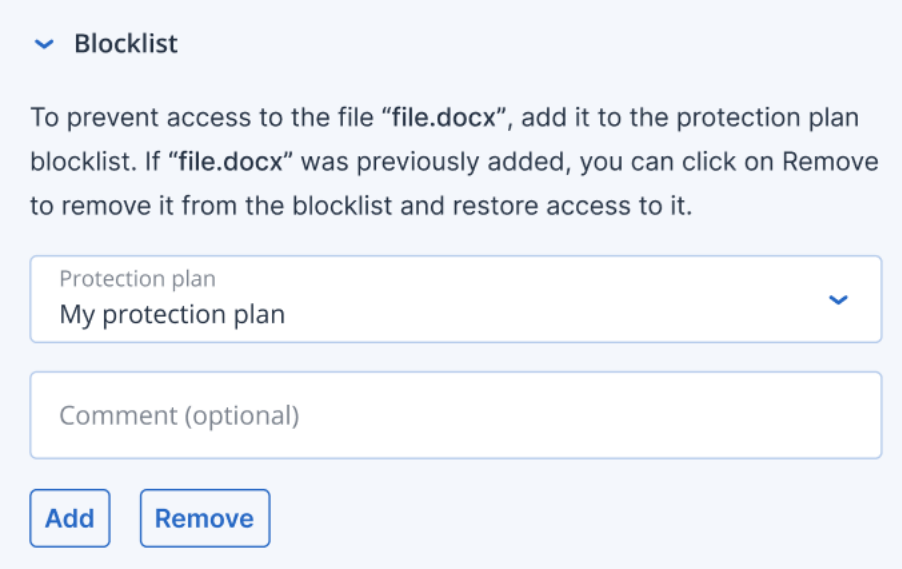
您也可以從允許名單或封鎖名單中移除節點，以允許或防止之後對該節點的任何存取。

此選項適用於下列網路攻擊鏈節點：

- 程序
- 檔案
- 網路

若要在保護計劃封鎖名單中新增或移除程序、檔案或網路

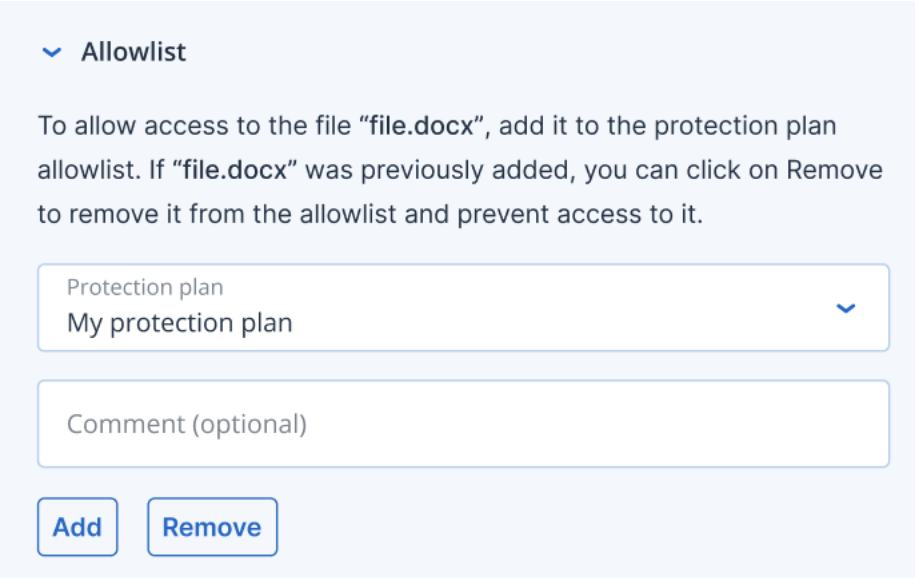
1. 在網路攻擊鏈中，按一下您要修復的程序、檔案或網路節點。
2. 在顯示的側邊欄中，按一下 **[回應動作]** 索引標籤。
3. 在 **[預防]** 區段中，按一下 **[封鎖名單]** 旁的箭頭圖示。



4. 選擇您想要在其中套用此動作的相關保護計劃。
5. [選用] 新增註解。此註解可在 **[活動]** 索引標籤中看到 (針對單一節點或整個事件)，而且可以協助您 (或您的同事) 在重新造訪該事件時回想起您採取該動作的原因。
6. 按一下 **[新增]**。
   系統會實作此動作，並防止之後啟動該程序、檔案或網路。
   或者，如果程序、檔案或網路之前已新增至封鎖名單，而您現在想要將其從封鎖名稱中移除，請按一下 **[移除]**。這將允許之後對該節點的存取。
   您也可以在個別節點或整個事件的 **[活動]** 索引標籤中檢視新增或移除動作。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

若要在保護計劃允許名單中新增或移除程序、檔案或網路

1. 在網路攻擊鏈中，按一下您要修復的程序、檔案或網路節點。
2. 在顯示的側邊欄中，按一下 **[回應動作]** 索引標籤。
3. 在 **[預防]** 區段中，按一下 **[允許名單]** 旁的箭頭圖示。



4. 選擇您想要在其中套用此動作的相關保護計劃。
5. [選用] 新增註解。此註解可在 **[活動]** 索引標籤中看到 (針對單一節點或整個事件), 而且可以協助您 (或您的同事) 在重新造訪該事件時回想起您採取該動作的原因。
6. 按一下 **[新增]**。
   系統會實作此動作, 並防止之後刪除該程序、檔案或網路。
   或者, 如果程序、檔案或網路之前已新增至允許名單, 而您現在想要將其從允許名稱中移除, 請按一下 **[移除]**。這將防止之後對該節點的存取。
   您也可以在個別節點或整個事件的 **[活動]** 索引標籤中檢視新增或移除動作。如需詳細資訊, 請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

使用自動化工作流程

您可以使用 Acronis 自動化工作流程套用一組預先定義的動作, 這些動作可以自動修復 Endpoint Detection and Response (EDR) 和 Extended Detection and Response (XDR) 中的事件。這些工作流程或手冊可讓您簡化安全營運以縮短回應時間, 同時減輕管理和回應安全性事件的操作負擔。

預先定義的 EDR 工作流程有六個, 每個工作流程都可以按需要進行設定。如需詳細資訊, 請參閱 "Endpoint Detection and Response (EDR) 工作流程" (第 852 頁)。

若要存取自動化工作流程, 請前往 **[管理] > [工作流程]**。顯示的工作流程清單會顯示目前已啟用或已停用的工作流程、上次執行時間和狀態。

Endpoint Detection and Response (EDR) 工作流程

根據您的需求, 有六個您可以設定的預設 EDR 工作流程:

- 隔離威脅 (建立 EDR 事件時)
- 隔離威脅 (更新 EDR 事件時)
- 隔離工作負載 (建立 EDR 事件時)
- 隔離工作負載 (更新 EDR 事件時)

- 需要注意的惡意軟體事件
- 需要注意的事件

下表說明每個工作流程適用的預設觸發程序、條件和動作。如需有關修改這些條件和動作的詳細資訊，請參閱 "設定自動化的 Endpoint Detection and Response (EDR) 工作流程" (第 855 頁)。

工作流程	觸發	條件	動作
隔離威脅	已建立 EDR 事件	威脅狀態 =「未緩解」 和 事件狀態 =「未開始」 和 嚴重性 =「高」 和 事件類型 =「偵測到處理程序」或「偵測到惡意軟體」	1. 停止處理程序。 2. 隔離處理程序。 3. 新增註解。預設註解文字為「<工作流程名稱> - 已隔離高嚴重性威脅」。 4. 事件結案。
隔離威脅	已更新 EDR 事件		

工作流程	觸發	條件	動作
隔離工作負載	已建立 EDR 事件	威脅狀態 =「未緩解」 和 事件狀態 =「未開始」 和 嚴重性 =「嚴重」 和 結果 =「惡意」 和 確實性層級 > 9 和 事件類型 =「偵測到處理程序」或「偵測到惡意軟體」	1. 停止處理程序。 2. 隔離處理程序。 3. 隔離工作負載。 4. 新增註解。預設註解文字為「<工作流程名稱> - 工作負載 <工作負載名稱> 在偵測到嚴重惡意軟體後已遭到隔離」。 5. 將電子郵件傳送給所選 Cyber Protect 主控台使用者。
隔離工作負載	已更新 EDR 事件		
需要注意的惡意軟體事件	已建立 EDR 事件	威脅狀態 =「未緩解」 和 事件狀態 =「未開始」 和 事件存留期 > 8 小時 和 嚴重性 =「高」或「嚴重」 和 結果 =「惡意」 和 事件類型 =「惡意軟體偵測」	1. 停止處理程序。 2. 隔離處理程序。 3. 新增註解。預設註解文字為「<工作流程名稱} - 8 小時未進行調查，隔離嚴重性為高/嚴重的威

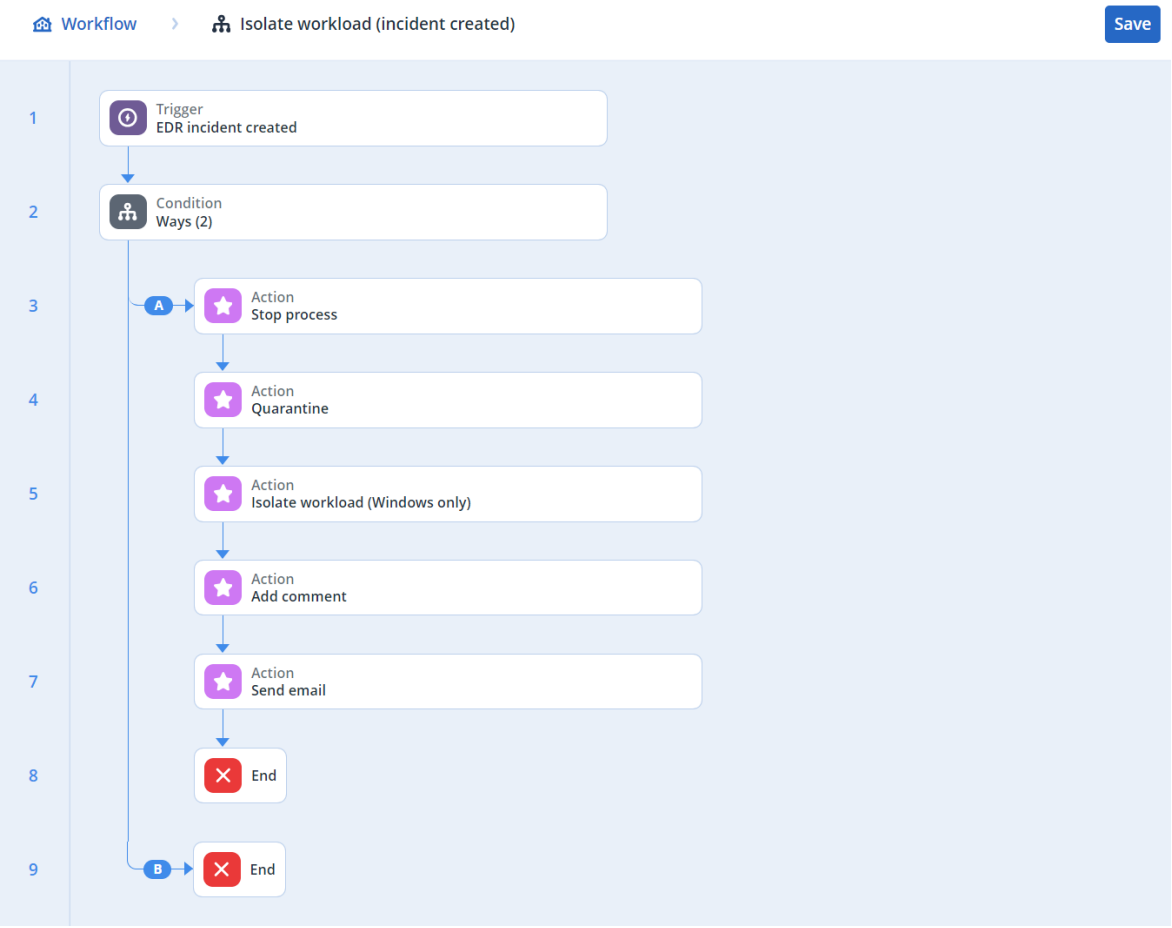
工作流程	觸發	條件	動作
			脅」。 4. 將電子郵件傳送給所選 Cyber Protect 主控台使用者。
需要注意的事件	已建立 EDR 事件	威脅狀態 =「未緩解」 和 事件狀態 =「未開始」 和 事件存留期 > 24 小時 和 嚴重性 =「高」或「嚴重」 和 結果 =「惡意」	1. 停止處理程序。 2. 隔離處理程序。 3. 新增註解。預設註解文字為「<工作流程名稱> - 24 小時未進行調查，隔離嚴重性為高/嚴重的威脅」。 4. 將電子郵件傳送給所選 Cyber Protect 主控台使用者。

設定自動化的 Endpoint Detection and Response (EDR) 工作流程

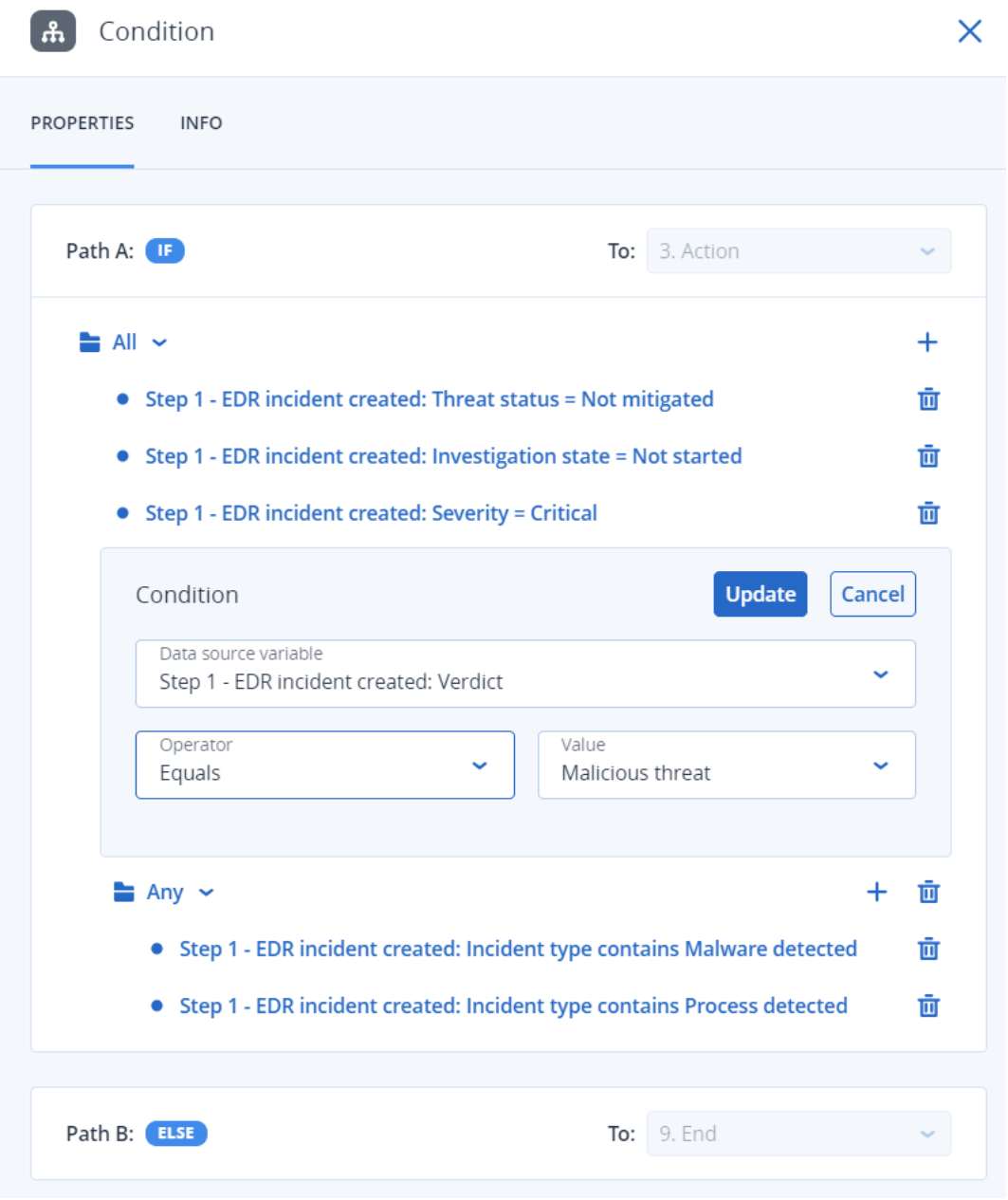
您可以根據需求，設定任何預先定義的 EDR 工作流程。

若要設定 EDR 工作流程

1. 在 Cyber Protect 主控台中，前往 **[管理] > [工作流程]**。
2. 在最右邊的欄中，按一下您要設定的工作流程的列中的省略符號圖示 (...)，然後選擇 **[開啟]**。
   或者，按一下相關的工作流程，並在顯示的窗格中，按一下 **[開啟]**。
   工作流程的條件和動作隨即顯示。



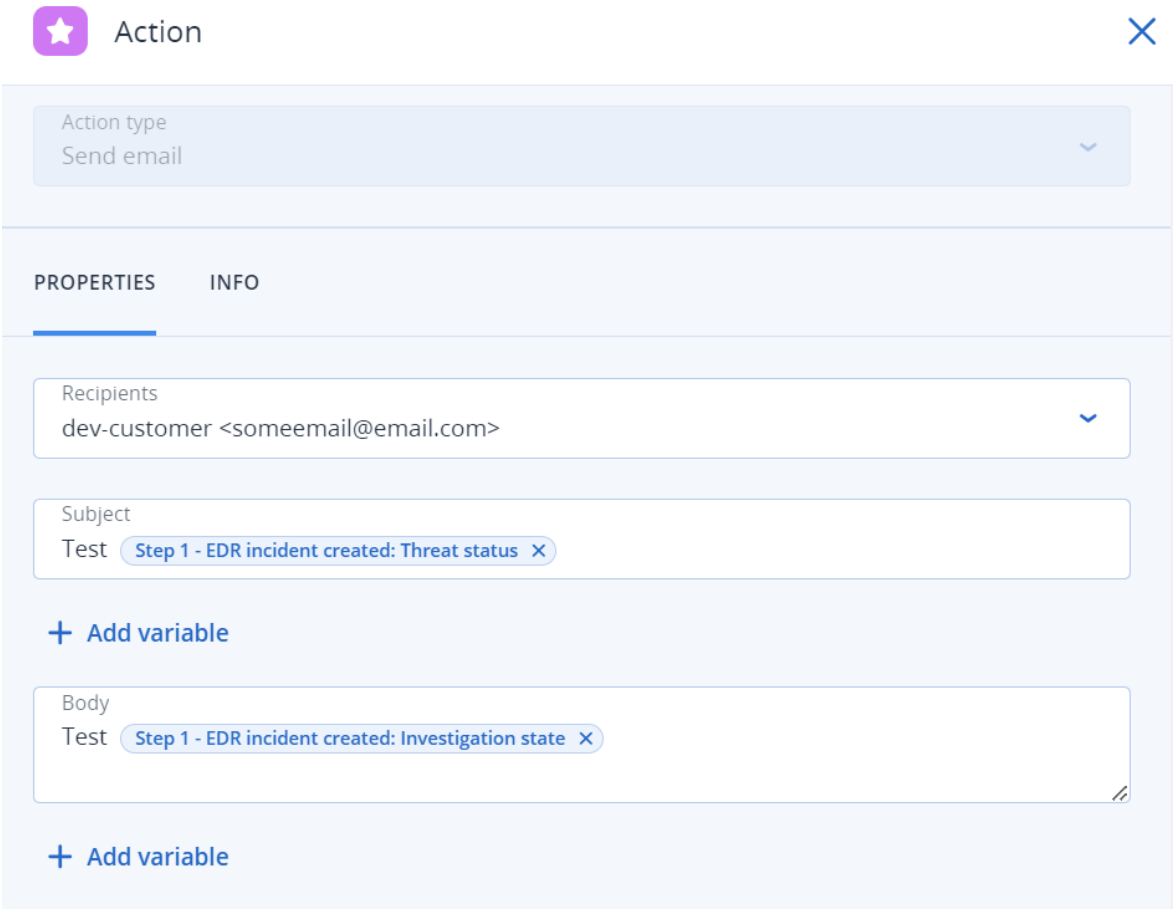
3. 若要檢視並修改任何工作流程條件，按一下 **[條件]** 區塊。



條件區塊可定義一組必須當作工作流程一部分執行的條件，而且由兩種區塊類型組成：

- **全部**：應該符合此區塊中的所有條件，才能繼續工作流程的下一個步驟。
- **任何**：必須符合此區塊中的至少一個條件，才能繼續工作流程的下一個步驟。

4. 若要修改條件，請按一下條件，然後修改相關值。完成後，按一下 **[更新]**。
   請注意，您也可以按一下條件旁邊的垃圾桶圖示，刪除該條件。
5. 若要修改動作，請按一下要修改的動作。
6. 在顯示的窗格中，進行相關變更。
   例如，按一下 **[傳送電子郵件]** 動作，然後修改當作此工作流程一部分傳送的電子郵件的所選收件者、本文和主旨。



7. [選用] 修改其他動作。
8. 按一下 **[儲存]**。

   如果先前未啟用工作流程且處於 **[草稿]** 狀態，按一下 **[儲存並啟用]** 即可啟用。或者，按一下 **[儲存]**，將工作流程保留在 **[停用]** 狀態。

   請注意，您可以按一下相關的工作流程，並選擇 **[啟用]** 或 **[停用]**，從主要工作流程畫面啟用或停用工作流程。

為 Endpoint Detection and Response (EDR) 啟用監控模式

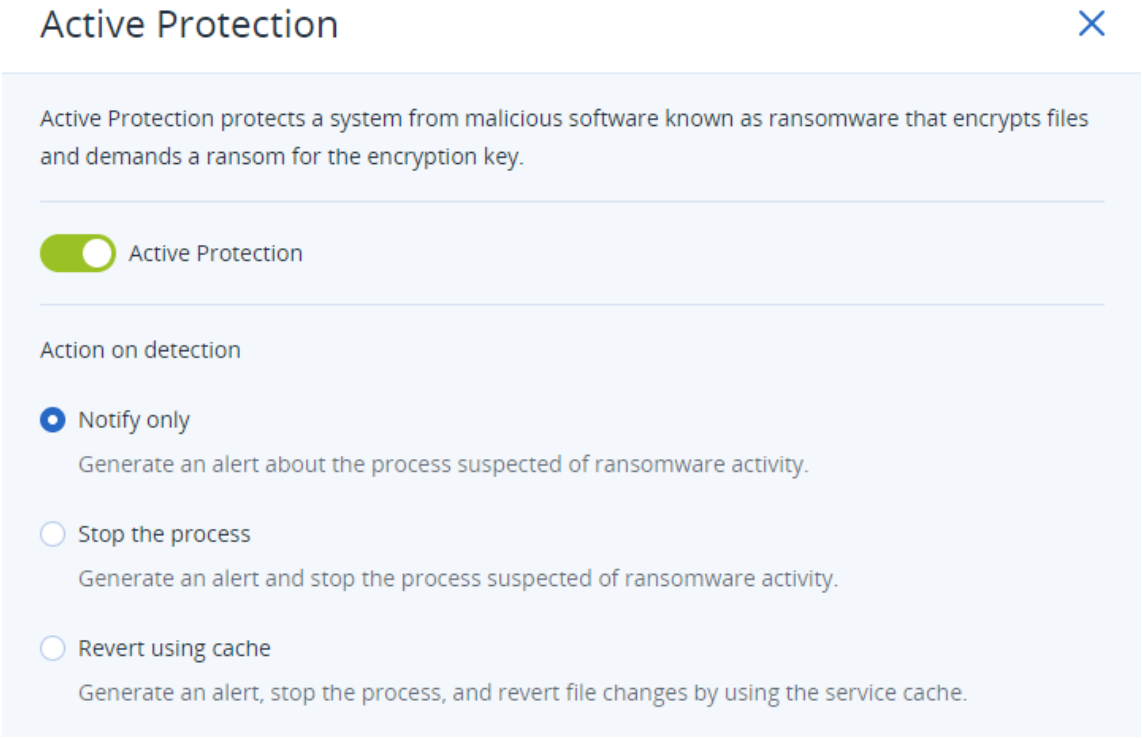
Cyber Protection 中的監控模式可讓您在實際運作環境中使用 EDR。接著，這可讓您檢查任何誤判，並在完整部署 EDR 之前，進行所需的排除。

在監控模式下，不會封鎖或停止任何操作，而且會建立事件，但不會起始任何回應。

若要為 EDR 啟用監控模式

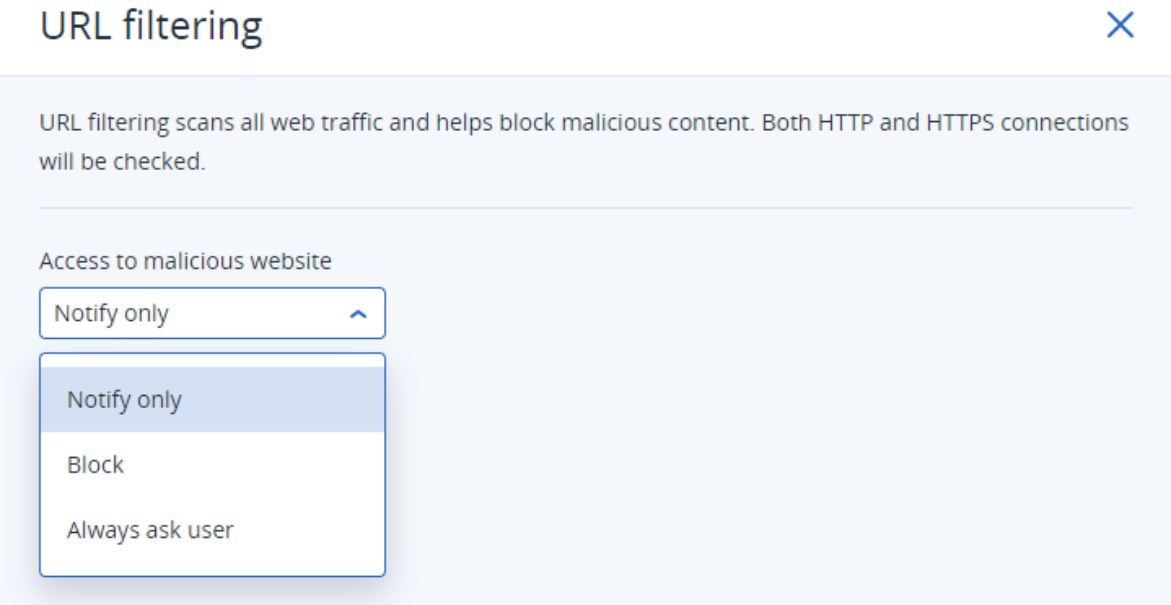
1. 在相關的保護計劃中，請確保已啟用 EDR。如需詳細資訊，請參閱 "啟用 Endpoint Detection and Response (EDR) 功能" (第 796 頁)。
2. 展開 **[防毒和防惡意軟體防護]** 模組，然後定義以下內容：
   - 按一下 **[主動式防護]**，並在 **[與偵測相關的動作]** 區段中，選擇 **[僅通知]**。然後按一下 **[完成]**。

     如需詳細資訊，請參閱 "Active Protection" (第 734 頁)。



- 按一下 **[行為引擎]**，並在 **[與偵測相關的動作]** 區段中，選擇 **[僅通知]**。然後按一下 **[完成]**。如需詳細資訊，請參閱 "行為引擎"(第 738 頁)。
- 按一下 **[漏洞利用防禦]**，並在 **[與偵測相關的動作]** 區段中，選擇 **[僅通知]**。然後按一下 **[完成]**。如需詳細資訊，請參閱 "漏洞利用防禦"(第 738 頁)。
- 按一下 **[即時保護]**，並在 **[與偵測相關的動作]** 區段中，選擇 **[僅通知]**。然後按一下 **[完成]**。如需詳細資訊，請參閱 "即時保護"(第 740 頁)。
- 按一下 **[排程掃描]**，並在 **[與偵測相關的動作]** 區段中，選擇 **[僅通知]**。然後按一下 **[完成]**。如需詳細資訊，請參閱 "排程掃描"(第 741 頁)。

3. 展開 **[URL 篩選]** 模組，並在 **[存取惡意網站]** 下拉式清單中，選擇 **[僅通知]**。然後按一下 **[完成]**。如需詳細資訊，請參閱 "URL 篩選"(第 753 頁)。



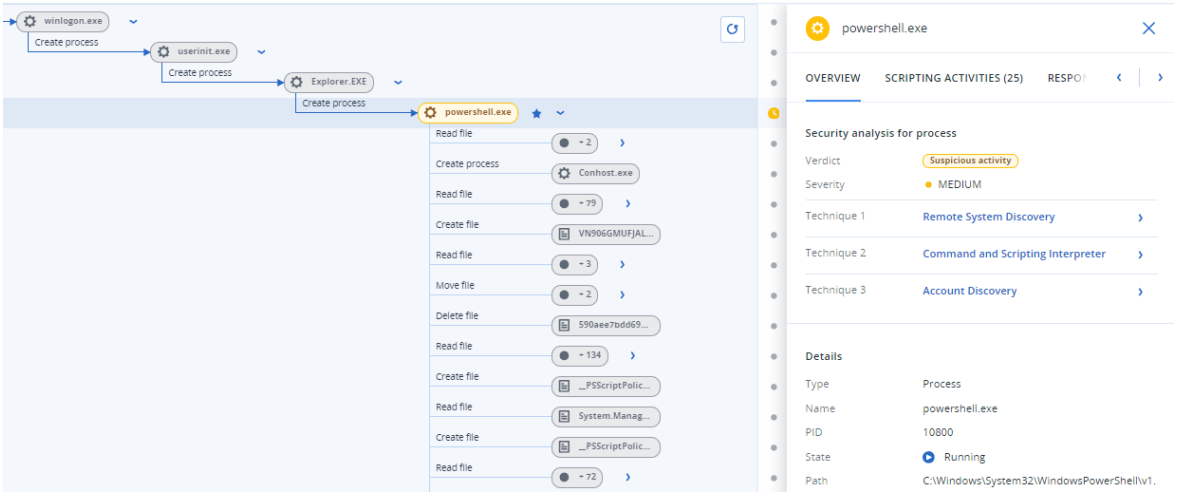
如何測試 Endpoint Detection and Response (EDR) 是否正確運作

為確保已部署 EDR 且正在運作，您可以執行多個觸發 EDR 偵測的命令。

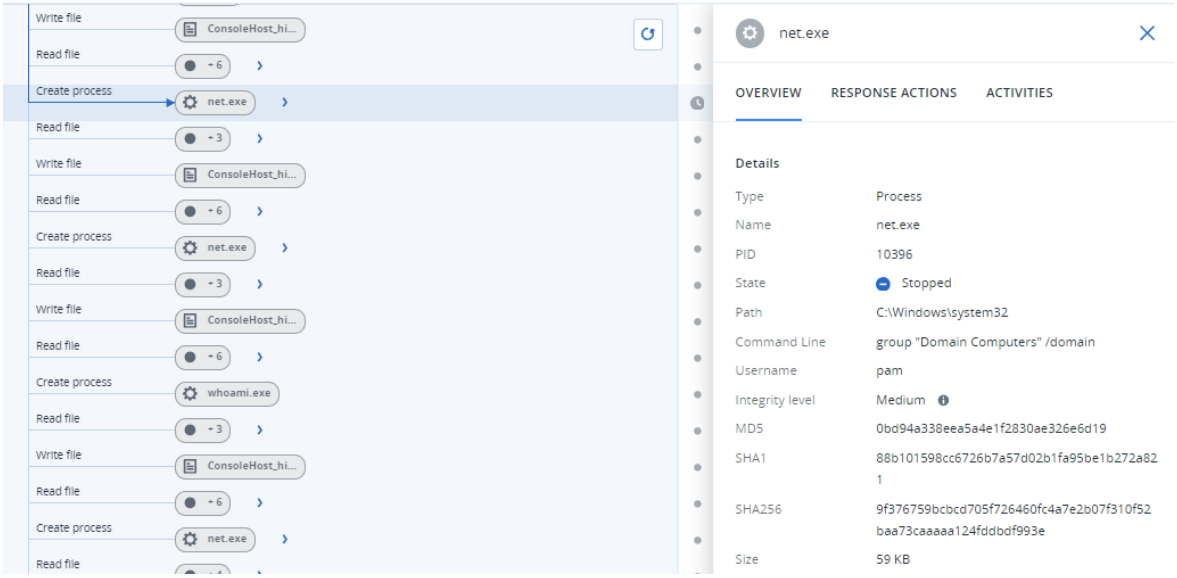
注意事項
若已部署 EDR，發生任何可疑活動時，您應該會立即看到事件。以下步驟可讓您在數天未觸發任何新事件時檢查 EDR 是否正在運作。

若要測試是否已部署 EDR 且正確運作

1. 登入已加入相關網域的 Active Directory 使用者帳戶。
2. 在 Windows PowerShell 中，執行以下兩個命令：
   - `net group "Domain Computers" /domain`
   - `net user administrator /domain`
3. 在 Cyber Protect 主控台中，移至 **[防護] > [事件]** 以檢視產生的事件。
   您也可以按一下已觸發的 **[中]** 嚴重性類型事件，以便將其顯示在 EDR 網路攻擊鏈中，並確認您在上一個步驟中執行的 PowerShell 命令，如以下範例所示。



4. 在 Windows PowerShell 中，執行以下命令：
   - `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 網路攻擊鏈中，按一下可執行檔節點 (例如，**net.exe** 或 **whoami.exe**)，以顯示在命令列上執行的確切 PowerShell 命令。在以下的範例中，這些命令會顯示在 **[概觀]** 索引標籤的 **[詳細資料]** 區段內。



6. 在您確認已產生 EDR 事件之後，請將事件的 **[威脅狀態]** 手動設定為 **[已緩解]**，並將 **[調查狀態]** 設定為 **[已結案]**。如需詳細資訊，請參閱 "如何調查網路攻擊鏈中的事件" (第 818 頁)。您也可以為事件輸入註解，表示這是測試事件。

Extended Detection and Response (XDR)

注意事項
此功能是 Advanced Security + XDR 保護套件的一部分，而此套件又是資安防護服務的一部分。請注意，您必須在保護計畫中啟用 [Endpoint Detection and Response (EDR)]功能，XDR 才能運作。

XDR 使用 EDR 進行事件關聯並識別端點上的進階攻擊，然後透過跨端點、電子郵件、身分識別等識別進階威脅來擴展該功能。

您也可以透過跨多個 XDR 整合 (包括 Perception Point 和 Microsoft Entra ID) 使用 XDR 圖表，以每種整合類型可用的特定動作來回應事件，例如封鎖電子郵件寄件者或暫停使用者。

XDR 與工作站、伺服器、虛擬機器和 Web 託管伺服器相容。

為什麼您需要 Extended Detection and Response (XDR)

先前提供安全性服務的 MSP 需要在防護不足和防護不完整，或昂貴和複雜的解決方案之間做出選擇。XDR 透過擴展和豐富 "Endpoint Detection and Response (EDR)" (第 793 頁) 提供的功能，並在端點、電子郵件、身分識別等範疇中識別進階威脅，從而克服這些限制。

由於*不斷擴大的攻擊面* (遠端位置有多個客戶、內部部署和雲端型工作負載混合，以及私有和公有雲端)，*安全基礎架構差距* (由於為不同客戶部署了大量安全工具，警示使技術人員不堪重負，且缺乏安全性人才)，以及不斷*演變的網路威脅* (例如，以 AI 為基礎的工具可讓攻擊者找到並利用零時差弱點，以及勒索軟體產生器)，因此，明顯需要一個解決方案，以簡化的修復步驟來阻止新型的網路威脅。

以下是您需要 XDR 的原因：

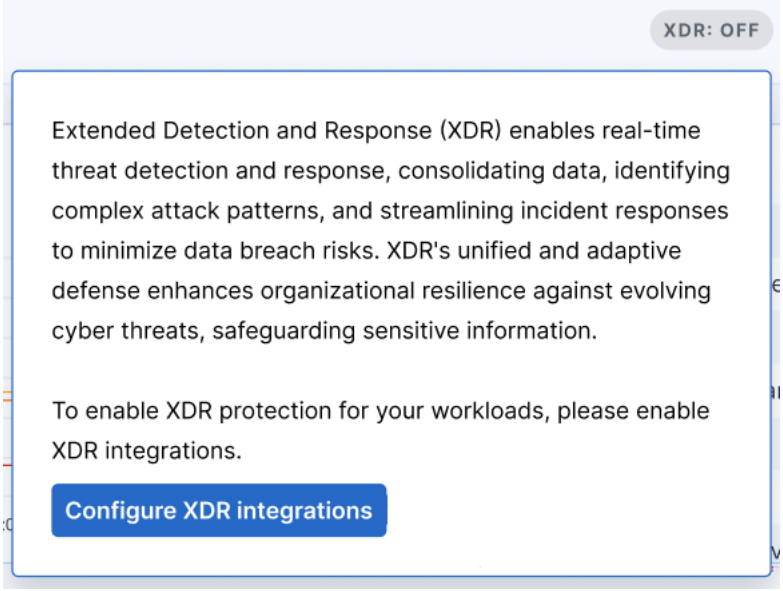
- **擴展防護**：透過掌握涵蓋端點、電子郵件、Microsoft Entra ID 和 Microsoft 365 應用程式 (例如 SharePoint、OneDrive 和 Teams) 的各種情況，防範易受攻擊的用戶端環境中的複雜威脅。增強的可見性意味著比 EDR 可以提供的偵測速度更快。
- **原生整合**：跨網路安全、資料保護和端點管理平台輕鬆整合。XDR 旨在保護易受攻擊的攻擊面，以實現無與倫比的業務持續性。
- **效率高，並具備增強的修復功能**：可輕鬆啟動、管理、擴充和提供安全性服務。此外，XDR 還包含 AI 支援的事件分析和一鍵回應功能 (可輕鬆進行調查並修復)，以及 AI 輔助和自動修復動作 (可防範多階段和進階網路威脅)。主動式安全性也可讓技術人員在攻擊者利用問題之前識別並修復潛在問題。

啟用 Extended Detection and Response (XDR)

重要事項
若要讓 XDR 運作，則必須先在相關的保護計劃中啟用 [Endpoint Detection and Response (EDR)] 選項。如此可確保在客戶租用戶中顯示 **[XDR: 開/關]** 選項開關。若未顯示此選項開關，請聯絡合作夥伴系統管理員。

若要啟用 XDR

1. 請確認 EDR 已在您的保護計劃中啟用。如需詳細資訊，請參閱 "啟用 Endpoint Detection and Response (EDR) 功能" (第 796 頁)。
2. 移至 **[防護]** > **[事件]**。
3. 在畫面右上方，按一下 XDR: OFF 。
4. 系統會提示您設定 XDR 整合，這是 XDR 保護您的工作負載所需。按一下 **[設定 XDR 整合]**。



如果您已設定現有的 XDR 整合，而且想要新增其他整合，請按一下 **[新增 XDR 整合]**。

系統會將您自動重新導向至管理入口網站，您可以在此選擇並設定相關的 XDR 整合。如需詳細資訊，請參閱與第三方系統的整合。

如需有關與 Microsoft Entra ID 整合的詳細資訊，請參閱這些整合步驟。

如需有關與 Perception Point 整合的詳細資訊，請參閱這些整合步驟。

當已設定至少一個 XDR 組態時，會啟用 XDR 選項開關 XDR: ON ，因此您可以開始使用 XDR。

使用 XDR 圖表

XDR 圖表透過建立偵測與 XDR 資料來源 (包括電子郵件和身分識別管理中繼資料) 中的事件關聯，為檢視 EDR (Endpoint Detection and Response) 事件新增另一個豐富的觀點。

顯示在圖表中的節點類型取決於 XDR 整合。例如，當與電子郵件和身分識別管理整合時，圖表將顯示電子郵件節點、電子郵件檔案附件節點和使用者身分識別節點。如需有關 XDR 圖表中顯示的各種節點圖示的詳細資訊，請參閱 "XDR 圖表圖示" (第 867 頁)。

使用 XDR 圖表可：

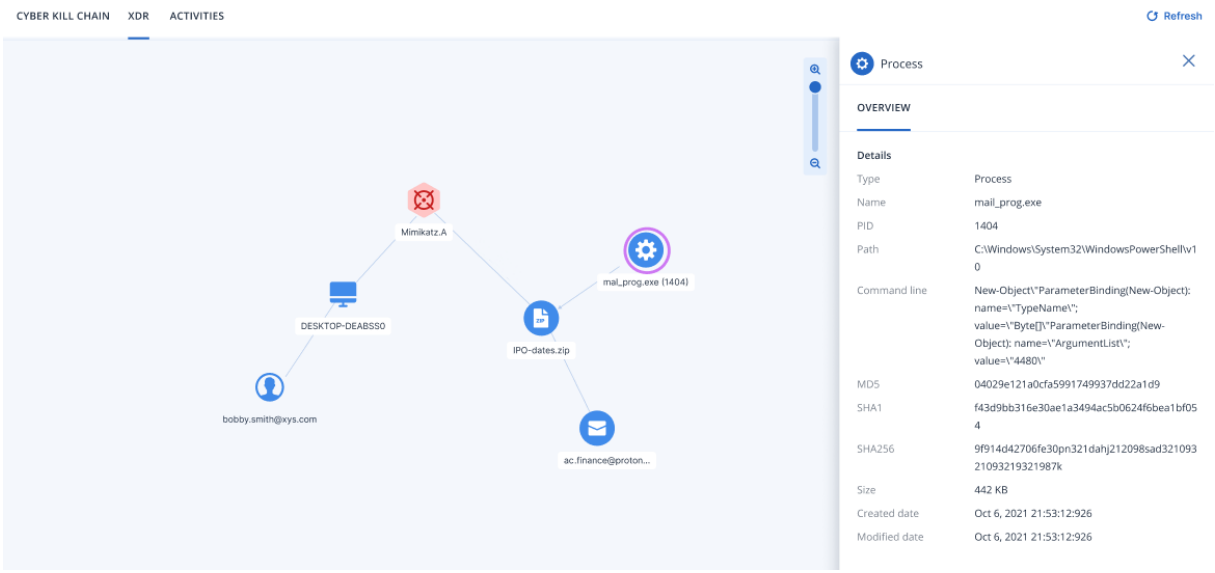
- 調查個別節點
- 將回應動作套用至節點
- 檢視整合錯誤

若要存取 XDR 圖表，請移至 **[防護]** > **[事件]**，按一下相關的事件，然後按一下 **[XDR]** 索引標籤。

若要重新整理 XDR 圖表的內容，請按一下 Refresh 。

注意事項

只有在啟用 XDR 時才會顯示 **[XDR]** 索引標籤。如需詳細資訊，請參閱 "啟用 Extended Detection and Response (XDR)" (第 862 頁)。

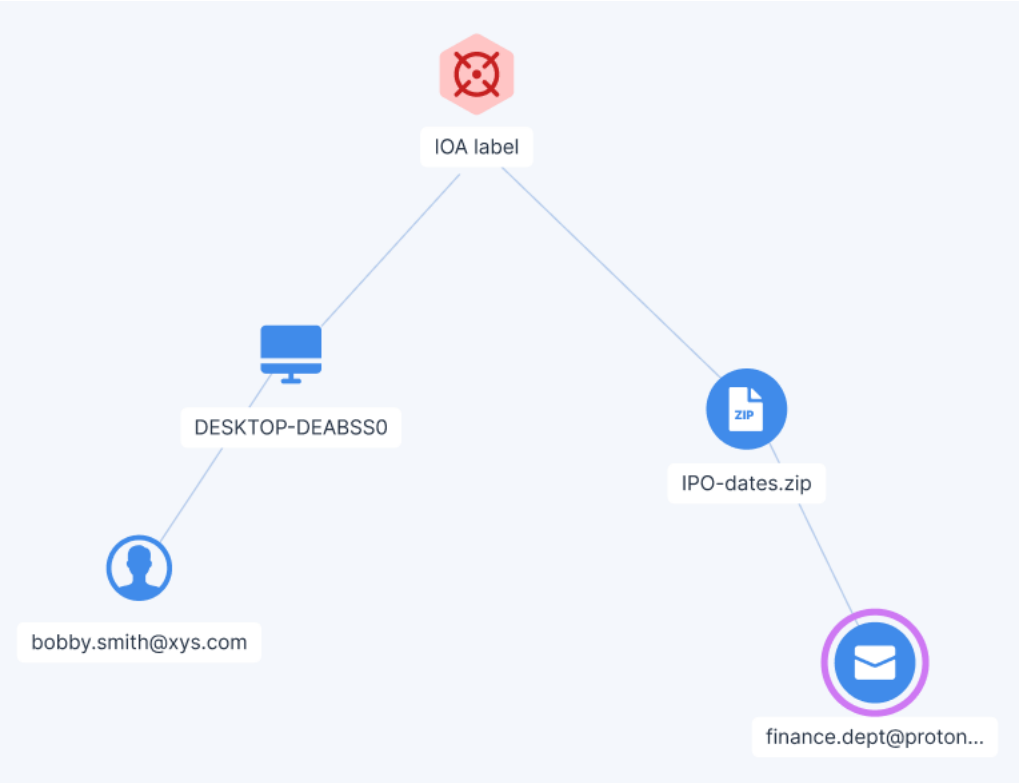


如何分析 XDR 圖表

XDR (Extended Detection and Response) 會將其他詳細資料新增至 EDR (Endpoint Detection and Response) 事件，例如，驗證威脅是來自電子郵件附件還是電子郵件中的連結，登入並負責開啟惡意附件的使用者。透過分析 XDR 圖表，您將獲得事件發生情況的其他內容，以及是否需要採取 EDR 功能以外的動作，例如封鎖使用者的帳戶，和/或封鎖電子郵件寄件者。

查看以下所示的 XDR 圖表中顯示的節點，您可以看到從下載至 **DESKTOP-DEABSS0** 的電子郵件所附的 zip 檔案中擷取了惡意威脅。寄件者的電子郵件地址為 **finance.dept@proton.me**，登入並開啟 zip 檔案的使用者為 **bobby.smith@xys.com**。

透過按一下桌面圖示，您可以在 **[概觀]** 索引標籤中查看該工作負載是否為已登入使用者常用的工作負載。如果使用者使用以前從未使用過的作業系統或 IP 位址登入，則該事件很可能是惡意的。接著，您可以對受感染裝置上的使用者套用所需的回應動作，以確保他們無法存取敏感資料和 IT 資源。



還有其他的 XDR 圖表元素可協助您瞭解確切的情況。

例如，XDR 與 Perception Point 的整合包括下列元素：

- 當惡意檔案是電子郵件的直接附件時，會顯示一條線，將惡意檔案節點連接到電子郵件節點。
- 當惡意節點為 URL 節點時，會顯示一條線，將惡意 URL 節點連接到電子郵件節點。
- 從 zip 存檔附件 (或其他類型的壓縮存檔) 中擷取惡意檔案時，會為 zip 存檔建立一個檔案節點，並顯示一條線，將惡意檔案節點連接到附件節點。

調查個別節點

您可以檢視任何 XDR 圖表節點的詳細資料。這可讓您向下鑽研至圖表中的特定節點，並根據需要，調查回應動作並將其套用至每個節點。

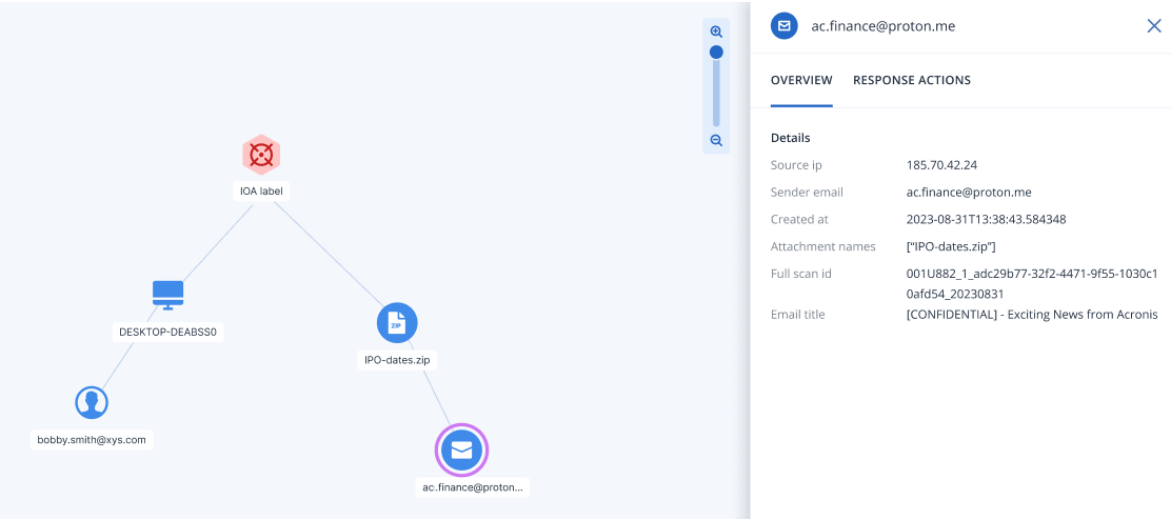
顯示的節點將根據實作的 XDR 整合而有所不同。節點詳細資料會顯示在 **[概觀]** 索引標籤中，而該節點可用的回應動作則會顯示在 **[回應動作]** 索引標籤中。

注意事項
指標威脅 (IoC) 和攻擊指標 (IoA) 節點沒有可用的回應動作。

若要調查個別節點

1. 在 Cyber Protect 主控台中，移至 **[防護] > [事件]**。
2. 在顯示的事件清單中，按一下您想要調查的事件最右側欄內的 。
3. 按一下 **[XDR]** 索引標籤。
4. 導覽至相關的節點，然後按一下該節點以顯示其側邊欄。

例如，按一下以下範例中的電子郵件節點會開啟該節點的側邊欄。



5. 調查包含在側邊欄索引標籤中的資訊：
   - **概觀**：此索引標籤包含有關所選節點的詳細資料，視節點類型而定。
     - 攻擊指標 (IoA) 節點：包括偵測時間戳記、偵測嚴重性、偵測描述、MITRE 手法和技術，以及威脅名稱。
     - 入侵指標 (IoC) 節點：每個 IoC 節點類型 (程序、檔案或 URL) 都有其自己的一組欄位，這些欄位也用於 Endpoint Detection and Response (EDR)。如需詳細資訊，請參閱 "調查網路攻擊鏈中的個別節點" (第 824 頁)。
     - 整合節點：包含所選節點的詳細資料，視整合而定。例如，電子郵件節點包含寄件者 IP 位址、名稱和使用的用戶端，以及每個附件的名稱、格式和大小等詳細資料。
   - **回應動作**：此索引標籤會列出可用的各種回應動作，視整合而定。例如，電子郵件節點將會顯示可將寄件者的電子郵件當作惡意內容封鎖，並刪除附件的選項。如需詳細資訊，請參閱 "套用回應動作" (第 866 頁)。

套用回應動作

您可以將各種回應動作套用到個別的 XDR 圖表節點。這些回應動作可讓您快速且輕鬆地修復任何節點。

若要套用回應動作

1. 在 Cyber Protect 主控台中，移至 **[防護] > [事件]**。
2. 在顯示的事件清單中，按一下您想要調查的事件最右側欄內的 。
3. 按一下 **[XDR]** 索引標籤。
4. 導覽至相關的節點，然後按一下該節點以顯示其側邊欄。

   請注意，如果節點是分組的身分識別、電子郵件或協同作業節點類型 (以節點上的標籤號碼表示)，則套用到此節點的回應動作會套用到群組節點中的所有子節點。
5. 按一下 **[回應動作]** 索引標籤。
6. 針對所需的回應動作，按一下 **[執行]**。

   例如，Perception Point 整合支援黑名單寄件者回應動作。

若是 Microsoft Entra ID 整合，可用的動作包括終止使用者工作階段、強制重設密碼和暫停使用者回應。

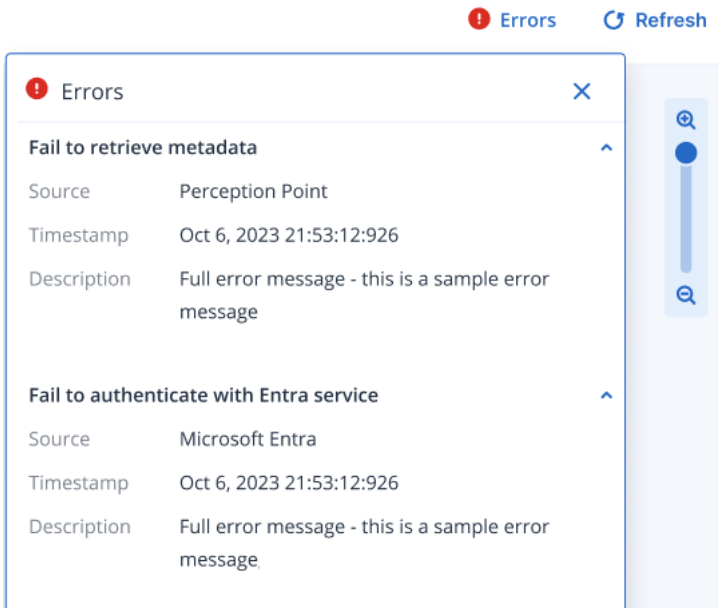
注意事項
按一下 **[執行]** 時，會暫時停用其他回應動作。當動作完成後，則會啟用其他回應動作。

7. (選擇性) 按一下 **[活動]** 索引標籤，以檢閱套用至節點的所有回應動作。請注意，針對 XDR 事件執行的回應動作會與 Endpoint Detection and Response (EDR) 事件一起顯示。如需詳細資訊，請參閱 "瞭解為緩解事件所採取的動作" (第 825 頁)。

檢視 XDR 整合錯誤

如果在與協力廠商 XDR 解決方案整合期間發生錯誤，則會顯示 [錯誤] 對話方塊。此對話方塊會顯示整合錯誤，包括連線至整合來源失敗或整合設定不正確。

存取 XDR 圖表時，若有錯誤，則會自動顯示 [錯誤] 對話方塊。若要在其他任何時間存取此對話方塊，請按一下 XDR 圖表右上角的 **[錯誤]**。請注意，如果目前沒有 XDR 圖表錯誤，則不會顯示 **[錯誤]** 按鈕。



XDR 圖表圖示

下表列出 XDR 圖表目前可用的各種圖示。

請注意，節點可以進行「分組」，以包含相同類型的多個個別節點。代表節點的圖示會顯示一個數字，表示群組節點中的節點數目。

例如， 

表示事件中有超過 100 個程序。如果分組的節點數量少於 100，則會顯示實際數量。

圖示	描述
	表示一般或所插入程序的威脅指標 (IoC)。 此圖示上會標示程序名稱，例如 **processname.exe**。
	表示一般、文件、可執行檔或指令碼檔案的威脅指標 (IoC)。 此圖示上會標示檔案名稱，例如 **filename.dll**。
	表示 URL 的威脅指標 (IoC)。 此圖示上會標示 URL，例如 **abc.com**。
	攻擊指標 (IoA)。 此圖示上會標示 IoA 名稱，例如 **Minikatz**。
	工作負載 此圖示上會標示工作負載名稱，例如 **DESKTOP-D123**。
	身分識別 (使用者) 此圖示上會標示使用者的帳戶 ID，例如 **david.smith@b.com**。
	表示一般電子郵件、附件或 URL的 電子郵件圖示。 此圖示上會標示寄件者的電子郵件地址，例如 **david.smith@b.com**。

評估漏洞和管理修補程式

弱點評估 (VA) 是識別、量化系統中找到的弱點，並確定其優先順序的一種程序。在 [弱點評估] 模組中，您可以掃描電腦中的弱點，並檢查作業系統和已安裝的應用程式皆處於最新狀態且運作正常。

具有下列作業系統的電腦支援弱點評估掃描：

- Windows。如需詳細資訊，請參閱 "支援的 Microsoft 和第三方產品" (第 869 頁)。
- macOS。如需詳細資訊，請參閱 "支援的 Apple 和協力廠商產品" (第 871 頁)。
- Linux (CentOS 7/Virtuozzo/Acronis Cyber Infrastructure) 電腦。如需詳細資訊，請參閱 "支援的 Linux 產品" (第 871 頁)。

使用 **[修補程式管理]** (PM) 功能，為電腦上所安裝的應用程式和作業系統，管理修補程式 (更新)，並將您的系統維持在最新狀態。在 [修補程式管理] 模組中，您可以自動或手動核准電腦上的更新安裝。

具有 Windows 作業系統的電腦支援修補程式管理。如需詳細資訊，請參閱 "支援的 Microsoft 和第三方產品" (第 869 頁)。

弱點評估

弱點評估程序包含下列步驟：

1. 您在已啟用 [弱點評估] 模組的情況下，建立保護計劃、指定弱點評估設定，然後將計劃指派給電腦。
2. 系統會依排程或視需要，將執行弱點評估掃描的命令傳送到電腦上安裝的保護代理程式。
3. 代理程式會取得命令、開始掃描電腦中的弱點，然後產生掃描活動。
4. 弱點評估掃描完成之後，代理程式會產生結果，並將其傳送到監控服務。
5. 監控服務會處理來自代理程式的資料，並將結果顯示在弱點評估桌面小工具和已找到弱點的清單中。
6. 當您取得已找到弱點的清單時，可以處理該清單並決定必須修正哪些找到的弱點。

您可以在 **[監控]** > **[概觀]** > **[弱點/現有的弱點]** 桌面小工具中，監視弱點評估掃描的結果。

支援的 Microsoft 和第三方產品

下列 Microsoft 產品和適用於 Windows 作業系統的協力廠商產品支援弱點評估和修補程式管理。

支援的 Microsoft 產品

桌面作業系統

- Windows 11
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 (Enterprise, Professional, Ultimate)

伺服器作業系統

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Microsoft Office 和相關元件

- Microsoft Office 2019 (x64, x86)
- Microsoft Office 2016 (x64, x86)
- Microsoft Office 2013 (x64, x86)
- Microsoft Office 2010 (x64, x86)

Windows 相關元件

- Internet Explorer
- Microsoft Edge
- Windows Media Player
- .NET Framework
- Visual Studio 和應用程式
- 作業系統元件

伺服器應用程式

- 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 支援的協力廠商產品

Cyber Protect 支援各種協力廠商應用程式的弱點評估和修補程式管理，包括對於遠端工作案例至關重要協同作業工具和 VPN 用戶端，例如：

- Microsoft Teams
- Zoom

- Skype
- Slack
- Webex
- NordVPN
- TeamViewer

如需 Windows 支援的協力廠商產品完整清單，請參閱修補程式管理支援的協力廠商產品清單 (62853)。

支援的 Apple 和協力廠商產品

下列 Apple 產品和適用於 macOS 的協力廠商產品支援弱點評估：

支援的 Apple 產品

macOS

- macOS 10.13.x 及更新版本

macOS 內建應用程式

- Safari、iTunes 等等。

支援的適用於 macOS 的協力廠商產品

- Microsoft Office (Word、Excel、PowerPoint、Outlook、OneNote)
- Adobe Acrobat Reader
- Google Chrome
- Firefox
- Opera
- Zoom
- Skype
- Thunderbird
- VLC 媒體播放程式

支援的 Linux 產品

支援適用於 VA 的下列 Linux 發行版和版本：

- Virtuozzo 7.x
- CentOS 7.x
- CentOS 8.x

弱點評估設定

若要瞭解如何使用 [弱點評估] 模組建立保護計劃，請參閱「建立保護計劃」。您可以依排程或視需要執行 VA 掃描 (透過使用保護計劃中的 **[立即執行]** 動作)。

您可以在 [弱點評估] 模組中指定下列設定。

掃描內容

定義您要掃描弱點的軟體產品：

- Windows 電腦：
  - **Microsoft 產品**
  - **Windows 協力廠商產品** (如需有關 Windows OS 支援的第三方產品的詳細資訊，請參閱修補程式管理支援的第三方產品清單 (62853))
- macOS 電腦：
  - **Apple 產品**
  - **macOS 協力廠商產品**
- Linux 電腦：
  - **掃描 Linux 套件**

排程

根據將在所選電腦上執行的弱點評估掃描，定義排程：

欄位	描述
使用下列事件，排程工作執行	此設定會定義執行工作的時間。 您可以選取下列值： • **依時間排程** – 這是預設設定。工作將會根據指定的時間執行。 • **當使用者登入系統時** – 根據預設，任何使用者的登入都將觸發工作。您可以修改此設定，因此只有特定使用者帳戶能夠觸發工作。 • **當使用者登出系統時** – 根據預設，任何使用者的登出都將觸發工作。您可以修改此設定，因此只有特定使用者帳戶能夠觸發工作。 **注意事項** 工作將不會在系統關機時執行。關機和登出在排程設定上是不同的動作。 • **在系統啟動時** – 工作將會在作業系統啟動時執行。 • **在系統關機時** – 工作將會在作業系統關機時執行。
排程類型	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[依時間排程]**，此欄位將會出現。 您可以選取下列值： • **每月** – 選擇執行工作的月份以及該月的週數或日期。 • **每天** – 這是預設設定。選擇工作將在一週的哪幾天執行。 • **每小時** – 選擇工作將在一週的哪幾天執行、重複次數以及時間間隔。
開始時間	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[依時間排程]**，此欄位將會

欄位	描述
	出現 選擇執行工作的明確時間。
在日期範圍內執行	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[依時間排程]**，此欄位將會出現。 設定一個範圍，已設定的排程將在該範圍內生效。
指定使用者帳戶，該帳戶登入作業系統時將啟動工作	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[當使用者登入系統時]**，此欄位將會出現。 您可以選取下列值： • **任何使用者** - 如果您希望任何使用者登入時都能觸發工作，請使用此選項。 • **下列使用者** - 如果您僅希望在特定使用者帳戶登入時觸發工作，請使用此選項。
指定使用者帳戶，該帳戶登出作業系統時將啟動工作	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[當使用者登出系統時]**，此欄位將會出現。 您可以選取下列值： • **任何使用者** - 如果您希望任何使用者登出時都能觸發工作，請使用此選項。 • **下列使用者** - 如果您僅希望在特定使用者帳戶登出時觸發工作，請使用此選項。
開始條件	定義必須同時符合，工作才能執行的所有條件。 防惡意軟體掃描的開始條件與 **[備份]** 模組的開始條件類似，其詳述於「開始條件」中。 您可以定義下列額外的開始條件： • **在時間視窗中分配工作開始時間** – 此選項可讓您設定工作的時間範圍，以避免網路瓶頸。您可以以小時或分鐘，指定延遲時間。例如，如果預設開始時間為上午 10:00，且延遲為 60 分鐘，則工作將會在上午 10:00 到上午 11:00 之間開始。 • **如果電腦關閉，則在電腦啟動時執行遺漏的工作** • **防止在工作執行期間進入睡眠或休眠模式** – 此選項僅適用於執行 Windows 的電腦。 • **如果未符合開始條件，請無論如何在此時間後執行工作** – 指定無論開始條件為何，將會在其後執行工作的時段。 **注意事項** Linux 不支援開始條件。

適用於 Windows 電腦的弱點評估

您可以掃描 Windows 電腦和適用於 Windows 的協力廠商產品的弱點。

若要設定適用於 Windows 電腦的弱點評估

1. 在 Cyber Protect 主控台中，建立保護計劃，然後啟用 **[弱點評估]** 模組。
2. 指定弱點評估設定：
   - **掃描內容** – 選擇 **[Microsoft 產品]**、**[Windows 協力廠商產品]**，或兩者。
   - **排程** – 定義執行弱點評估的排程。

   如需有關 **[排程]** 選項的詳細資訊，請參閱 "弱點評估設定"(第 871 頁)。
3. 將計劃指派給 Windows 電腦。

弱點評估掃描之後，您可以查看已找到弱點的清單。您可以處理這項資訊並決定必須修正哪些找到的弱點。

若要監視弱點評估的結果，請查看 **[監視]** > **[概觀]** > **[弱點/現有的弱點]** 桌面小工具。

Linux 電腦的弱點評估

您可以掃描 Linux 電腦中是否有應用程式層級和核心層級的弱點。

設定 Linux 電腦的弱點評估

1. 在 Cyber Protect 主控台中，建立保護計劃，然後啟用 **[弱點評估]** 模組。
2. 指定弱點評估設定：
   - **掃描內容** – 選擇 **[掃描 Linux 套件]**。
   - **排程** – 定義執行弱點評估的排程。

   如需有關 **[排程]** 選項的詳細資訊，請參閱 "弱點評估設定"(第 871 頁)。
3. 將計劃指派給 Linux 電腦。

弱點評估掃描之後，您可以查看已找到弱點的清單。您可以處理這項資訊並決定必須修正哪些找到的弱點。

若要監視弱點評估的結果，請查看 **[監視]** > **[概觀]** > **[弱點/現有的弱點]** 桌面小工具。

適用於 macOS 裝置的弱點評估

您可以掃描 macOS 裝置中的作業系統層級和應用程式層級弱點。

若要設定適用於 macOS 裝置的弱點評估

1. 在 Cyber Protect 主控台中，建立保護計劃，然後啟用 **[弱點評估]** 模組。
2. 指定弱點評估設定：
   - **掃描內容** – 選擇 **[Apple 產品]**、**[macOS 協力廠商產品]**，或兩者。
   - **排程** – 定義執行弱點評估的排程。

   如需有關 **[排程]** 選項的詳細資訊，請參閱 "弱點評估設定"(第 871 頁)。
3. 將計劃指派給 macOS 裝置。

弱點評估掃描之後，您可以查看已找到弱點的清單。您可以處理這項資訊並決定必須修正哪些找到的弱點。

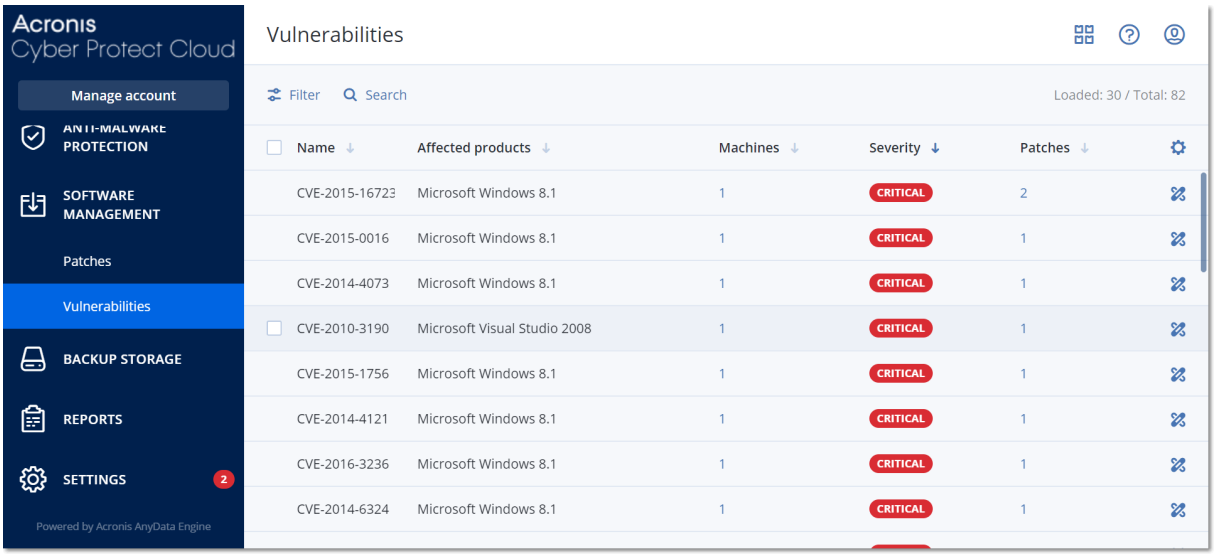
若要監視弱點評估的結果，請查看 **[監視]** > **[概觀]** > **[弱點/現有的弱點]** 桌面小工具。

管理找到的弱點

如果至少執行過弱點評估一次，且找到一些弱點，您可以在 **[軟體管理]** > **[弱點]** 中看到這些弱點。弱點清單會同時顯示具有要安裝之修補程式的弱點，以及沒有建議之修補程式的弱點。您可以使用篩選功能，僅顯示具有修補程式的弱點。

名稱	描述
名稱	弱點的名稱。
受影響的產品	找到其中有弱點的軟體產品。
電腦	受影響電腦的數量。
嚴重性	找到之弱點的嚴重性。根據通用弱點評分系統 (CVSS)，可以指派下列層級： • **重大**：9 - 10 CVSS • **高**：7 - 9 CVSS • **中**：3 - 7 CVSS • **低**：0 - 3 CVSS • **無**
修補程式	適用修補程式的數量。
已發佈	在 Common Vulnerabilities and Exposures (CVE) 中發佈弱點的日期和時間。
已偵測到	在電腦上偵測到現有弱點的第一個日期。

在清單中按一下找到之弱點的名稱，就可以找到其描述。



開始弱點修復程序

1. 在 Cyber Protect 主控台中，移至 **[軟體管理]** > **[弱點]**。
2. 在清單中選擇弱點，然後按一下 **[安裝修補程式]**。弱點修復精靈將會開啟。

3. 選擇要安裝在所選電腦上的修補程式，然後按一下 **[下一步]**。
4. 選擇您要安裝修補程式所在的電腦。
5. 選擇重新開機選項。
   a. 選擇您是否要在安裝修補程式後將電腦重新開機。

選項	描述
否	安裝修補程式後，電腦將不會自動重新開機。
如有需要	只有在需要套用修補程式時，才會將電腦重新開機。
可以	安裝修補程式後，電腦將會自動重新開機。您也可以指定重新開機延遲。

   b. [選用] 如果您要在電腦備份進行中時延遲電腦重新開機，請選擇 **[在備份完成之前，請不要重新開機]**。
6. 按一下 **[安裝修補程式]**。

因此，所選修補程式會安裝在所選電腦上。

修補程式管理

注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

如需有關 Windows OS 支援的第三方產品的詳細資訊，請參閱修補程式管理支援的第三方產品清單 (62853)。

使用修補程式管理功能可：

- 安裝 OS 層級與應用程式層級的更新
- 手動或自動核准修補程式
- 視需要或根據排程，安裝修補程式
- 依下列不同的條件，精確地定義要安裝的修補程式：嚴重性、類別和核准狀態
- 執行更新前備份以防止可能不成功的更新
- 定義修補程式安裝後的重新開機動作

注意事項
若要使用 Windows 更新，修補程式管理功能會要求您在工作負載上啟用 Windows 更新。

Cyber Protection 推出對等技術，可將網路頻寬流量減至最少。您可以選擇一或多個專用代理程式，這些代理程式將從網際網路下載更新，並在網路中的其他代理程式之間散佈。所有代理程式也會當作對等代理程式，彼此共用更新。

修補程式管理工作流程

修補程式管理工作流程包含以下步驟：設定並套用保護計劃、執行弱點評估掃描、設定修補程式設定、核准修補程式，最後再安裝核准的修補程式。工作負載的確切步驟如下。

1. 設定已啟用 **[弱點評估]** 和 **[修補程式管理]** 模組的保護計劃。
2. 設定弱點評估設定。如需有關這些設定的詳細資訊，請參閱 "弱點評估設定" (第 871 頁)。
3. 設定修補程式管理設定。如需有關這些設定的詳細資訊，請參閱 "保護計劃中的修補程式管理設定" (第 877 頁)
4. 將保護計劃套用至一或多部電腦。
5. 等待弱點評估掃描完成。此掃描將會根據保護計劃中設定的排程，自動開始。或者，您可以視需要在保護計劃的 **[弱點評估]** 模組中按一下 **[立即執行]** 圖示，手動開始掃描。
6. 核准修補程式。您可以定義自動核准修補程式的設定，其中包括在測試電腦上自動安裝修補程式。如需詳細資訊，請參閱 "自動核准修補程式" (第 883 頁)。或者，您可以將修補程式的核准狀態設定為 **[已核准]** 以手動核准修補程式。如需詳細資訊，請參閱 "手動核准修補程式" (第 886 頁)。
7. 安裝修補程式。系統可以根據保護計劃中設定的排程，自動安裝核准的修補程式。或者，您可以視需要手動安裝修補程式。如需詳細資訊，請參閱 "視需要安裝修補程式" (第 887 頁)。

您可以在 **[監控]** > **[概觀]** > **[修補程式安裝歷史記錄]** 桌面小工具中，監控修補程式安裝的結果。

保護計劃中的修補程式管理設定

在保護計劃的 **[修補程式管理]** 模組中，您可以設定下列修補程式管理設定：

- 要針對 Microsoft 和 Windows 作業系統用第三方產品安裝哪些更新。
- 什麼時候執行自動安裝修補程式。
- 是否要執行更新前備份。

如需有關建立保護計劃與啟用 **[修補程式管理]** 模組的詳細資訊，請參閱 "建立保護計劃" (第 192 頁)。

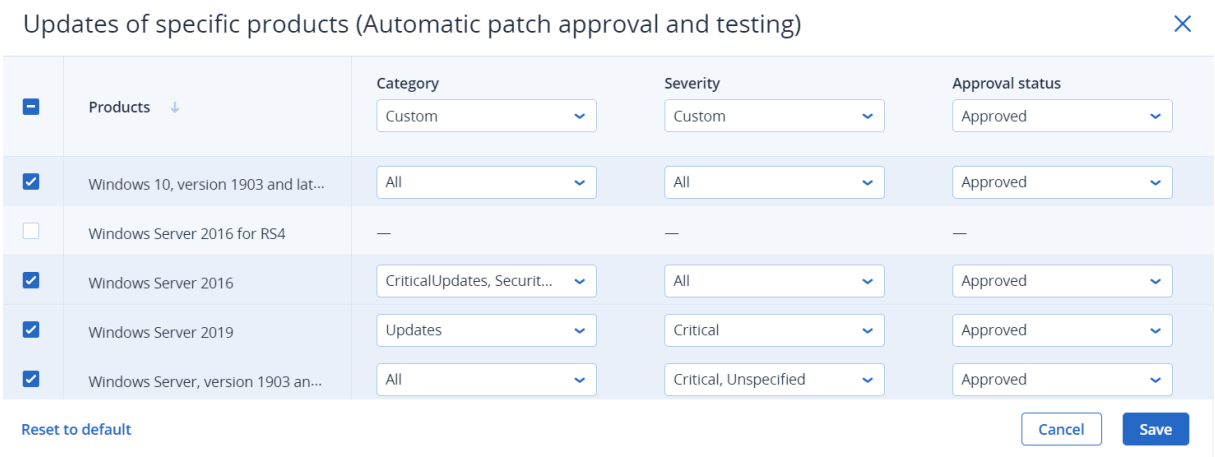
注意事項
是否能夠使用此功能視您帳戶啟用的服務配額而定。

Microsoft 產品

若要在所選電腦上安裝 Microsoft 更新，請啟用 **[更新 Microsoft 產品]** 選項。

選擇安裝選項：

選項	描述
所有更新	如果您要安裝所有經過核准的更新，請使用此選項。
僅限安全性更新和重大更新	如果您要安裝所有經過核准的安全性更新和重大更新，請使用此選項。
特定產品的更新 (自動核准並測試修補程式)	如果您要定義不同產品的自訂設定，請使用此選項。 如果您要更新特定產品，可以依類別、嚴重性或核准狀態，為每個產品定義要安裝的更新。 如果您要設定自動核准測試並測試修補程式，請選擇此選項。



對於 Microsoft 產品，修補程式分配會使用 Windows API 服務。內部或分配代理程式中並未下載或儲存修補程式和更新。反之，這些內容是從 Microsoft CDN 中下載的。因此，就算已獲指派 [更新者] 角色，代理程式仍無法下載更新並分配修補程式。

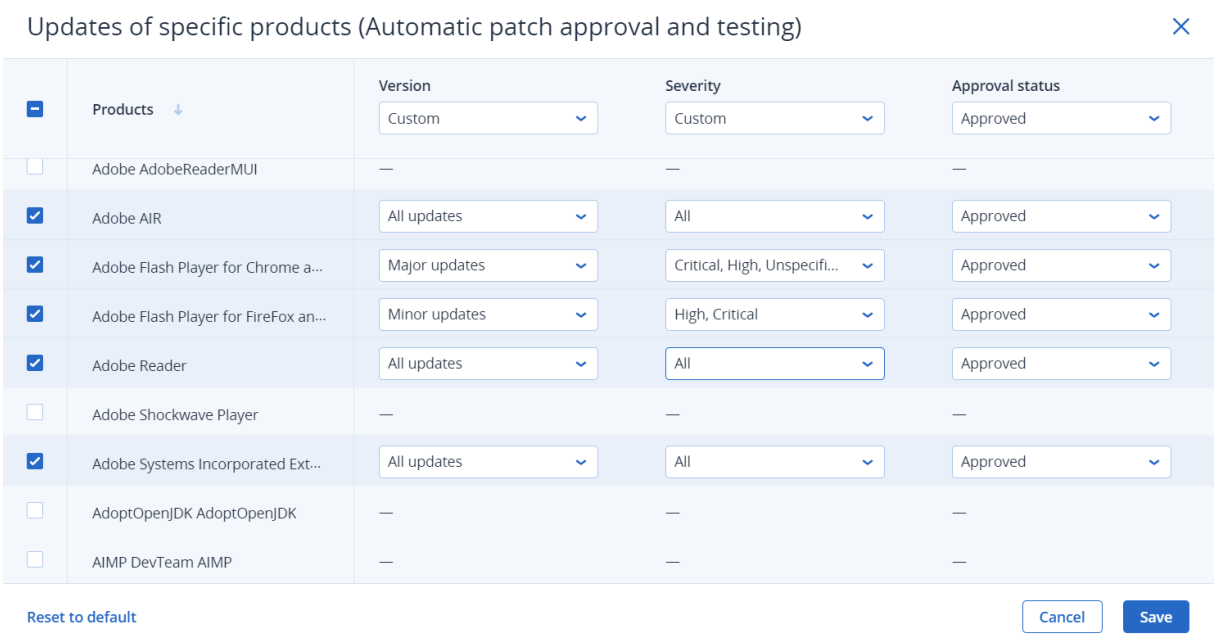
Windows 協力廠商產品

若要在所選電腦上安裝適用於 Windows OS 的第三方更新，請啟用 **[Windows 協力廠商產品]** 選項。

選擇安裝選項：

選項	描述
所有更新	如果您要安裝所有經過核准的更新，請使用此選項。*
僅限主要更新	如果您要安裝所有經過核准的主要更新，請使用此選項。
僅限小幅度更新	如果您要安裝經過核准的小幅度更新，請使用此選項。
特定產品的更新 (自動核准並測試修補程式)	如果您要定義不同產品的自訂設定，請使用此選項。 如果您之後要更新特定產品，可以依類別、嚴重性或核准狀態，為每個產品定義要安裝的更新。 如果您要設定自動核准測試並測試修補程式，請選擇此選項。
僅針對偵測到弱點的應用程式安裝最新的版本	如果您僅要針對偵測到弱點的應用程式安裝最新的更新，請選擇此核取方塊。*

* 此選項需要 Cyber Protect 代理程式 23.11.36772 版或更新版本。



對於 Windows 協力廠商產品，修補程式會直接從內部 Acronis 資料庫分配至受管理的工作負載。當代理程式獲指派 [更新者] 角色時，將使用此代理程式下載並分配修補程式。

排程

根據將在所選電腦上安裝的更新，定義排程和條件。

欄位	描述
使用下列事件，排程工作執行	此設定會定義執行工作的時間。 您可以選取下列值： • **依時間排程** – 這是預設設定。工作將會根據指定的時間執行。 • **當使用者登入系統時** – 根據預設，任何使用者的登入都會啟動工作。您可以修改此設定，因此只有特定使用者帳戶能夠觸發工作。 • **當使用者登出系統時** – 根據預設，任何使用者的登出都會啟動工作。您可以修改此設定，因此只有特定使用者帳戶能夠觸發工作。 **注意事項** 工作將不會在系統關機時執行。關機和登出在排程設定上是不同的動作。 • **在系統啟動時** – 工作將會在作業系統啟動時執行。 • **在系統關機時** – 工作將會在作業系統關機時執行。
排程類型	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[依時間排程]**，此欄位將會出現。 您可以選取下列值： • **每月** – 選擇執行工作的月份以及該月的週數或日期。

欄位	描述
	• **每天** – 這是預設設定。選擇工作將在一週的哪幾天執行。 • **每小時** – 選擇工作將在一週的哪幾天執行、重複次數以及時間間隔。
開始時間	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[依時間排程]**，此欄位將會出現 選擇執行工作的明確時間。
為修補程式設定維護時段	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[依時間排程]**，此欄位將會出現。 如果您希望修補程式安裝僅在您指定的時間間隔執行，請選擇此設定。如果修補程式安裝程序在針對修補程式的維護時段定義的結束時間前還未完成，將會自動停止。
在日期範圍內執行	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[依時間排程]**，此欄位將會出現。 設定一個範圍，已設定的排程將在該範圍內生效。
指定使用者帳戶，該帳戶登入作業系統時將啟動工作	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[當使用者登入系統時]**，此欄位將會出現。 您可以選取下列值： • **任何使用者** - 如果您希望任何使用者登入時都能觸發工作，請使用此選項。 • **下列使用者** - 如果您僅希望在特定使用者帳戶登入時觸發工作，請使用此選項。
指定使用者帳戶，該帳戶登出作業系統時將啟動工作	如果您在 **[使用下列事件，排程工作執行]** 中選擇 **[當使用者登出系統時]**，此欄位將會出現。 您可以選取下列值： • **任何使用者** - 如果您希望任何使用者登出時都能觸發工作，請使用此選項。 • **下列使用者** - 如果您僅希望在特定使用者帳戶登出時觸發工作，請使用此選項。
開始條件	定義必須同時符合，工作才能執行的所有條件。 防惡意軟體掃描的開始條件與 **[備份]** 模組的開始條件類似，其詳述於「開始條件」中。 您可以定義下列額外的開始條件： • **在時間視窗中分配工作開始時間** – 此選項可讓您設定工作的時間範圍，以避免網路瓶頸。您可以以小時或分鐘，指定延遲時間。例如，如果預設開始時間為上午 10:00，且延遲為 60 分鐘，則工作將會在上午 10:00 到上午 11:00 之間開始。 • **如果電腦關閉，則在電腦啟動時執行遺漏的工作**

欄位	描述
	• **防止在工作執行期間進入睡眠或休眠模式** – 此選項僅適用於執行 Windows 的電腦。 • **如果未符合開始條件，請無論如何在此時間後執行工作** – 指定無論開始條件為何，將會在其後執行工作的時段。 **注意事項** Linux 不支援開始條件。
更新之後重新開機	定義在更新安裝完成後是否要自動為電腦重新開機。 您可以選取下列值： • **永不** – 更新後絕不會起始重新開機。 • **如有需要** – 只有在需要套用更新時，才會起始重新開機。 • **一律** – 更新後將一律起始重新開機。您可以指定重新開機延遲。
在備份完成之前，請不要重新開機	如果您選擇此選項，當備份程序正在執行時，電腦重新開機將會延遲，直到備份完成為止。

預先更新備份

安裝軟體更新前執行備份 – 系統將會在電腦上安裝任何更新之前，先建立電腦的增量備份。如果沒有稍早建立的備份，將會建立電腦的完整備份。它可以防止更新安裝失敗而且需要恢復到之前狀態的情況。若要讓 **[預先更新備份]** 選項運作，對應的電腦必須在保護計劃和要備份的項目 (整部電腦或開機+系統磁碟區) 中同時啟用修補程式管理和備份模組。如果您選擇不適當的項目進行備份，則系統將不會允許您啟用 **[預先更新備份]** 選項。

檢視可用修補程式的清單

弱點評估掃描完成之後，您可以在 **[軟體管理]** > **[修補程式]** 中檢視可用修補程式的相關資訊。

若要檢視特定修補程式的詳細資料，請在修補程式清單中，按一下對應的修補程式。

下表描述您可以在畫面上檢視的修補程式的相關資訊。

欄位	描述
核准狀態	核准狀態主要是自動核准案例所需。 您可以為修補程式定義下列其中一個狀態： • **已核准** – 修補程式已安裝在至少一部電腦上且驗證為正常 • **已拒絕** – 修補程式不安全，而且可能會損毀電腦系統 • **待核准** – 修補程式狀態不清楚，應該進行驗證
授權合約	• 同意 • 不同意。如果您不同意授權合約，則修補程式狀態會變成 **[已拒絕]**，因此將不會安裝

嚴重性	修補程式的嚴重性： • **重大** • **高** • **中** • **低** • **無**
廠商	修補程式的廠商
受影響的產品	修補程式適用的產品
已安裝的版本	已經安裝的產品版本
版本	修補程式的版本
類別	修補程式所屬的類別： • **重大更新** – 針對特定問題廣泛發佈的修正，用於解決與安全性無關的重大錯誤。 • **安全性更新** – 針對特定產品廣泛發佈的修正，用於解決安全性問題。 • **定義更新** – 病毒或其他定義檔的更新。 • **更新彙總套件** – 累積 Hotfix、安全性更新、重大更新以及封裝在一起以方便部署的更新的集合。彙總套件通常是針對特定領域 (例如安全性) 或特定元件 (例如 Internet Information Services (IIS))。 • **Service Pack** – 累積所有 Hotfix、安全性更新、重大更新，以及自發佈產品以來建立的更新的集合。Service Pack 也可能包含有限數量的客戶要求設計變更或功能。 • **工具** – 有助於完成一項或多項工作的公用程式或功能。 • **Feature Pack** – 新功能版本，通常會在下一個版本發佈到產品中。 • **更新** – 針對特定問題廣泛發佈的修正，用於解決與安全性無關的非重大錯誤。 • **應用程式** – 應用程式的修補程式。
發佈日期	發佈修補程式的日期
上次報告時間	上次報告修補程式的日期
首次安裝時間	首次在電腦上成功安裝修補程式的日期
Microsoft KB	如果是適用於 Microsoft 產品的修補程式，則此欄位會顯示 KB 文章 ID
電腦	受影響電腦的數量
弱點	弱點的數量。如果您按一下弱點，系統會將您重新導向至弱點的清單。
大小	修補程式的平均大小
語言	修補程式支援的語言

廠商網站	廠商的官方網站

在清單中設定修補程式存留時間

您可以透過在 **[修補程式]** 畫面上的清單中設定修補程式存留時間，將修補程式清單維持在最新狀態。此設定會定義偵測到的可用修補程式會顯示在修補程式清單中的時間長度。在修補程式成功安裝在被指出缺少的電腦上後，或在經過清單中的存留時間後，該修補程式將會從清單中移除。

若要在清單中設定修補程式存留時間

1. 在 Cyber Protect 主控台中，移至 **[軟體管理]** > **[修補程式]**。
2. 按一下 **[設定]**。
3. 在 **[清單中的存留時間]** 中，選擇適當的選項。

選項	描述
永遠	修補程式將會永遠保留在清單中。
7 天	首次安裝經過 7 天之後，修補程式將會從清單中移除。 例如，假設您有兩部必須安裝修補程式的電腦。一部電腦處於連線狀態，另一部電腦則離線。修補程式安裝在第一部電腦上。7 天後，即使修補程式未安裝在第二部電腦上 (因為離線)，該修補程式也將從修補程式清單中移除。
30 天	首次安裝經過 30 天之後，修補程式將會從清單中移除。

自動核准修補程式

自動核准修補程式可讓您更輕鬆地在電腦上安裝更新。使用自動核准修補程式，修補程式的安裝就不會遭到手動核准修補程式程序延遲。重要更新和修正的安裝速度更快，從而提高您系統的可靠度。

您可以在測試案例中使用自動核准修補程式，以便自動安裝修補程式。如果在測試電腦上成功安裝修補程式，則也會將這些修補程式自動安裝在實際運作電腦上。如需有關此案例的詳細資訊，請參閱 "自動核准並測試修補程式的使用案例" (第 884 頁)。

您也可以在案例中使用自動核准修補程式，以便略過測試階段，在實際運作環境中自動安裝修補程式。如需有關此案例的詳細資訊，請參閱 "自動核准但不測試修補程式的使用案例" (第 886 頁)。

設定自動核准修補程式

您可以設定自動核准修補程式，並確保修補程式的安裝就不會遭到手動核准修補程式程序延遲。

設定自動核准修補程式

1. 在 Cyber Protect 主控台中，移至 **[軟體管理]** > **[修補程式]**。
2. 按一下 **[設定]**。
3. 啟用 **[自動核准修補程式]**。
4. 設定自動核准修補程式的設定。

a. 選擇自動核准修補程式選項。

選項	描述
自動核准並測試修補程式	在成功安裝修補程式後經過所選天數時，修補程式的核准狀態將變更為 **[已核准]**。如果您要先在測試電腦上安裝修補程式來進行測試，確保一切如預期般運作，然後再將修補程式安裝到實際運作環境中，建議您使用此設定。
自動核准但不測試修補程式	在找到修補程式後經過所指天數時，修補程式的核准狀態將變更為 **[已核准]**。

b. 選擇符合自動核准修補程式選項的條件後必須經過的天數。在此期間之後，修補程式的核准狀態將會自動從 **[待核准]** 變更為 **[已核准]**。

5. 選擇 **[自動接受授權合約]**。
6. 按一下**[套用]**。

自動核准並測試修補程式的使用案例

如果您想要先在測試電腦上測試新的修補程式，然後再將其安裝在實際運作電腦上，則您可以設定兩個保護計劃：一個計劃用於安裝測試用途的修補程式，另一個計劃則用於在實際運作電腦上安裝經過測試的修補程式。因此，您將確保安裝在實際運作環境中的修補程式安全無虞，而且在安裝修補程式後，您的實際運作電腦正確運作。

此使用案例包含下列階段：

1. 設定自動核准修補程式的設定。選擇 **[自動核准並測試修補程式]** 選項。如需詳細資訊，請參閱 "設定自動核准修補程式" (第 883 頁)。
2. 利用已啟用的 **[修補程式管理]** 模組，設定測試用途的保護計劃 (例如，「測試修補」)，並將其套用至測試環境中的電腦。指定修補程式安裝的下列條件：修補程式核准狀態必須是 **[待核准]**。您需要此步驟才能驗證修補程式，並在修補程式安裝之後確認電腦是否正常運作。如需詳細資訊，請參閱 "設定測試修補保護計劃" (第 884 頁)。
3. 利用已啟用的 **[修補程式管理]** 模組，設定實際運作環境的保護計劃 (例如，「實際運作修補」)，並將其套用至實際運作環境中的電腦。指定修補程式安裝的下列條件：修補程式狀態必須是 **[已核准]**。如需詳細資訊，請參閱 "設定實際運作修補保護計劃" (第 885 頁)。
4. 執行「測試修補」計劃並檢查結果。將沒有問題的電腦的核准狀態保留為 **[待核准]**，但將運作不正確的電腦的核准狀態變更為 **[已拒絕]**。根據在 **[自動核准修補程式]** 設定中設定的天數，修補程式的狀態將會自動從 **[待核准]** 變更為 **[已核准]**。當您執行實際運作修補計劃時，只會將 **[已核准]** 修補程式安裝在實際運作電腦上。如需詳細資訊，請參閱 "執行測試修補保護計劃並拒絕不安全的修補程式" (第 886 頁)。
5. 執行實際運作修補計劃。

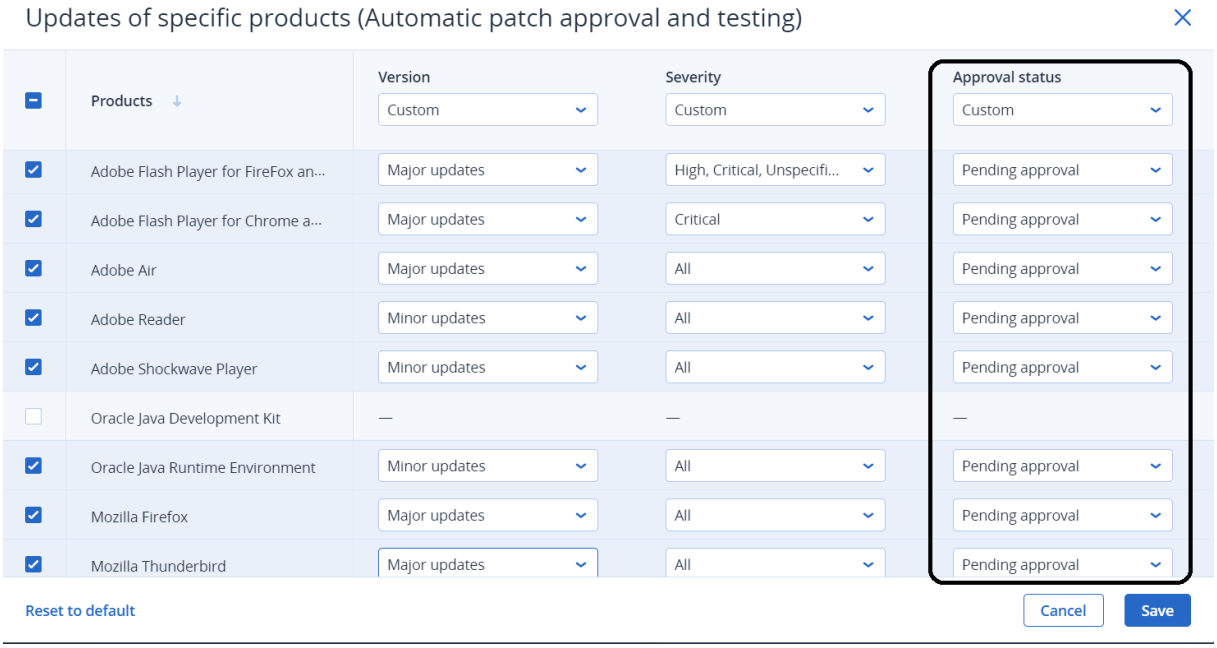
設定測試修補保護計劃

您可以針對測試環境中的電腦，設定具有修補程式安裝設定的保護計劃。

若要設定測試修補保護計劃

1. 在 Cyber Protect 主控台，前往 **[管理]** > **[保護計劃]**。
2. 按一下 **[建立計劃]**。
3. 啟用 **[修補程式管理]** 模組。
4. 定義要為 Microsoft 和第三方產品安裝的更新、排程，以及更新前備份。如需有關這些設定的詳細資訊，請參閱 "保護計劃中的修補程式管理設定"(第 877 頁)。

重要事項
針對要更新的所有產品，選擇 **[待核准]** 核准狀態。因此，代理程式僅會將 **[待核准]** 的修補程式安裝在測試環境中的所選電腦上。



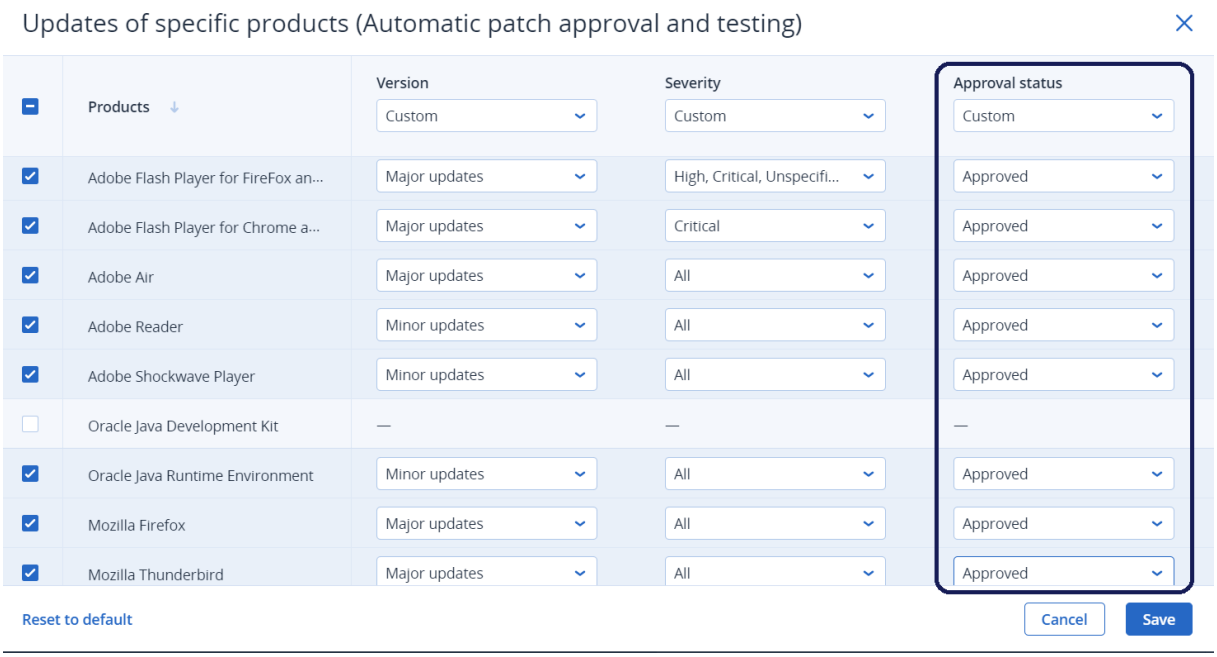
設定實際運作修補保護計劃

您可以針對實際運作環境中的電腦，設定具有修補程式安裝設定的保護計劃。

若要設定實際運作修補保護計劃

1. 在 Cyber Protect 主控台，前往 **[管理]** > **[保護計劃]**。
2. 按一下 **[建立計劃]**。
3. 啟用 **[修補程式管理]** 模組。
4. 定義要為 Microsoft 和第三方產品安裝的更新、排程，以及更新前備份。如需有關這些設定的詳細資訊，請參閱 "保護計劃中的修補程式管理設定"(第 877 頁)。

重要事項
針對要更新的所有產品，將 **[核准狀態]** 設定為 **[已核准]**。因此，代理程式僅會將 **[已核准]** 的修補程式安裝在實際運作環境中的所選電腦上。



執行測試修補保護計劃並拒絕不安全的修補程式

在修補程式安裝在測試環境下的電腦上之後，您可以檢查一切是否如預期般運作。您可以將沒有問題的電腦的核准狀態保留為 **[待核准]**，但將運作不正確的電腦的核准狀態變更為 **[已拒絕]**。

若要執行測試修補保護計劃並拒絕不安全的修補程式

1. 執行測試修補保護計劃 (依排程或手動)。
2. 根據結果，查看哪些已安裝的修補程式安全。
3. 移至 **[軟體管理]** > **[修補程式]**，然後針對不安全的修補程式，將 **[核准狀態]** 設定為 **[已拒絕]**。

自動核准但不測試修補程式的使用案例

如果您想要盡快在實際運作電腦上自動安裝新的修補程式，而不想要將其先安裝在測試電腦上，您可以僅設定一個保護計劃。

此使用案例包含下列階段：

1. 設定自動核准修補程式的設定。選擇 **[自動核准但不測試修補程式]** 選項。如需詳細資訊，請參閱 "設定自動核准修補程式" (第 883 頁)。
2. 利用已啟用的 **[修補程式管理]** 模組，設定實際運作環境的保護計劃 (例如，「實際運作修補」)，並將其套用至實際運作環境中的電腦。指定修補程式安裝的下列條件：修補程式狀態必須是 **[已核准]**。如需詳細資訊，請參閱 "設定實際運作修補保護計劃" (第 885 頁)。
3. 執行實際運作修補計劃。

手動核准修補程式

您可以手動核准修補程式，並透過略過測試階段加速其安裝速度。

必要條件

- 已啟用 **[修補程式管理]** 模組的保護計劃會套用到至少一部 Windows 電腦。
- 套用保護計劃的一或多部電腦上仍有未安裝的修補程式。

若要手動核准修補程式

1. 在 Cyber Protect 主控台中，移至 **[軟體管理]** > **[修補程式]**。
2. 選擇您要安裝的修補程式，然後接受授權合約。
3. 將修補程式的 **[核准狀態]** 設定為 **[已核准]**。

   修補程式的核准狀態隨即設定為 **[已核准]**。修補程式將會根據保護計劃中定義的排程，自動安裝在電腦上。如果您要立即安裝修補程式，請依照 "視需要安裝修補程式" (第 887 頁) 中所述的程序操作。

視需要安裝修補程式

當您不想等待排程的安裝時間時，可以視需要手動安裝修補程式。

您可以從三個畫面開始手動安裝修補程式：**[修補程式]**、**[弱點]** 和 **[所有裝置]**。

若要手動安裝修補程式

從修補程式

1. 在 Cyber Protect 主控台中，移至 **[軟體管理]** > **[修補程式]**。
2. 針對您要安裝的修補程式，接受授權合約。
3. 在 **[安裝修補程式]** 精靈中，選擇您要安裝的修補程式，然後按一下 **[安裝]**。
4. 選擇您要安裝修補程式所在的電腦。
5. 選擇重新開機選項。
   a. 選擇您是否要在安裝修補程式後將電腦重新開機。

選項	描述
否	安裝修補程式後，電腦將不會自動重新開機。
如有需要	只有在需要套用修補程式時，才會將電腦重新開機。
可以	安裝修補程式後，電腦將會自動重新開機。您也可以指定重新開機延遲。

   b. [選用] 如果您要在電腦備份進行中時延遲電腦重新開機，請選擇 **[在備份完成之前，請不要重新開機]**。
6. 按一下 **[安裝修補程式]**。

從弱點

1. 在 Cyber Protect 主控台中，移至 **[軟體管理]** > **[弱點]**。
2. 執行修復程序，如 "管理找到的弱點" (第 875 頁) 中所述。

從所有裝置

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 選擇您要安裝修補程式所在的電腦。
3. 按一下 **[修補程式]**。
4. 選擇您要安裝的修補程式，然後按一下 **[下一步]**。
5. 選擇重新開機選項。
   a. 選擇您是否要在安裝修補程式後將電腦重新開機。

選項	描述
否	安裝修補程式後，電腦將不會自動重新開機。
如有需要	只有在需要套用修補程式時，才會將電腦重新開機。
可以	安裝修補程式後，電腦將會自動重新開機。您也可以指定重新開機延遲。

   b. [選用] 如果您要在電腦備份進行中時延遲電腦重新開機，請選擇 **[在備份完成之前，請不要重新開機]**。
6. 按一下 **[安裝修補程式]**。

管理軟體與硬體清查

軟體清查

軟體清查功能適用於已啟用進階套件或具備 (舊版) Cyber Protect 授權的裝置。此功能可讓您檢視安裝在所有 Windows 和 macOS 裝置上的所有軟體應用程式。

若要取得軟體清查資料，您可以在裝置上執行自動或手動掃描。

您可以使用軟體清查資料來：

- 瀏覽並比較安裝載公司裝置上的所有應用程式的相關資訊
- 判斷應用程式是否需要更新
- 判斷未使用的應用程式是否需要移除
- 確定多個公司裝置上的軟體版本相同
- 監視連續掃描之間軟體狀態的變更。

啟用軟體清查掃描

在裝置上啟用軟體清查掃描時，系統會每 12 小時自動收集軟體資料一次。

預設會針對具備所需授權的所有裝置，啟用軟體清查掃描功能，但必要時，您可以變更設定。

注意事項
客戶租用戶可以啟用或停用軟體清查掃描。單位租用戶僅能檢視軟體清查掃描設定，但無法變更設定。

若要啟用軟體清查掃描

1. 在 Cyber Protect 主控台中，移至 **[設定]**。
2. 按一下 **[保護]**。
3. 按一下 **[清查掃描]**。
4. 按一下模組名稱旁邊的開關，以啟用 **[軟體清查掃描]** 模組。

若要停用軟體清查掃描

1. 在 Cyber Protect 主控台中，移至 **[設定]**。
2. 按一下 **[保護]**。
3. 按一下 **[清查掃描]**。
4. 按一下模組名稱旁邊的開關，以停用 **[軟體清查掃描]** 模組。

手動執行軟體清查掃描

您可以從 **[軟體清查]** 畫面，或從 **[清查]** 畫面中的 **[軟體]** 索引標籤，手動執行軟體清查掃描。

必要條件

- 此裝置可使用 Windows 或 macOS 作業系統。
- 裝置具備所需的 (舊版) Cyber Protect 授權，或已啟用 Advanced Management 套件。

若要從 [軟體清查] 畫面執行軟體清查掃描

1. 在 Cyber Protect 主控台中，移至 **[軟體管理]**。
2. 按一下 **[軟體清查]**。
3. 在 **[分組依據：]** 下拉式欄位中，選擇 **[裝置]**。
4. 尋找您要掃描的裝置，然後按一下 **[立即掃描]**。

若要從 [清查] 畫面中的 [軟體] 索引標籤執行軟體清查掃描

1. 在 Cyber Protect 主控台中，移至 **[裝置]**。
2. 按一下您要掃描的裝置，然後按一下 **[清查]**。
3. 在 **[軟體]** 索引標籤中，按一下 **[立即掃描]**。

瀏覽軟體清查

您可以檢視並瀏覽資料中可用於所有公司裝置的所有軟體應用程式。

必要條件

- 這些裝置可使用 Windows 或 macOS 作業系統。
- 裝置具備所需的 (舊版) Cyber Protect 授權，或已啟用 Advanced Management 套件。
- 裝置上的軟體清查掃描已成功完成。

若要檢視適用於所有 Windows 和 macOS 公司裝置的所有軟體應用程式

1. 在 Cyber Protect 主控台中，移至 **[軟體管理]**。
2. 按一下 **[軟體清查]**。

   根據預設，資料會依裝置分組。下表描述 **[軟體清查]** 畫面中顯示的資料。

欄	描述
名稱	應用程式的名稱。
版本	應用程式的版本。
狀態	應用程式的狀態。 • **新增**。 • **已更新**。 • **已移除**。 • **無變更**。
廠商	應用程式的廠商。

欄	描述
安裝日期	安裝應用程式的日期及時間。
上次執行時間	僅限 macOS 裝置。應用程式上次作用中的日期及時間。
位置	安裝應用程式所在的目錄。
使用者	安裝應用程式的使用者。
系統類型	僅限 Windows 裝置。應用程式的位元類型。 • **X86** (適用於 32 位元應用程式)。 • **X64** (適用於 64 位元應用程式)。

3. 若要將資料依應用程式分組，請在 **[分組依據:]** 下拉式欄位中，選擇 **[應用程式]**。
4. 若要縮小畫面上顯示的資訊範圍，請使用一個篩選條件或多個篩選條件的組合。
   a. 按一下 **[篩選]**。
   b. 選擇一個篩選條件或數個篩選條件的組合。

      下表描述 **[軟體清查]** 畫面中的篩選條件。

篩選器	描述
裝置名稱	裝置名稱。可以複選。如果您要比較特定裝置上的軟體，請使用此篩選條件。
應用程式	應用程式名稱。可以複選。如果您要比較特定裝置或所有裝置上特定應用程式的資料，請使用此篩選條件。
廠商	應用程式的廠商。可以複選。如果您要在特定裝置或所有裝置上，檢視特定廠商的所有應用程式，請使用此篩選條件。
狀態	應用程式狀態。可以複選。如果您要在特定裝置或所有裝置上，檢視所選狀態的所有應用程式，請使用此篩選條件。
安裝日期	安裝應用程式的日期。如果您要在特定裝置或所有裝置上，檢視特定日期安裝的所有應用程式，請使用此篩選條件。
掃描日期	軟體清查掃描的日期。如果您要在該日期掃描的特定裝置或所有裝置上，檢視軟體的相關資訊，請使用此篩選條件。

   c. 按一下**[套用]**。
5. 若要瀏覽整個軟體清查清單，請使用畫面下半部的分頁。

- 按一下您要開啟的頁面的號碼。
- 在下拉式欄位中，選擇您要開啟的頁面的頁碼。

檢視單一裝置的軟體清查

您可以檢視安裝在單一裝置上的所有軟體應用程式的清單，以及應用程式的相關詳細資訊，例如，狀態、版本、廠商、安裝日期、上次執行時間和位置。

必要條件

- 此裝置可使用 Windows 或 macOS 作業系統。
- 裝置具備所需的 (舊版) Cyber Protect 授權，或已啟用 Advanced Management 套件。
- 裝置上的軟體清查掃描已成功完成。

若要從 [軟體清查] 畫面檢視單一裝置的軟體清查

1. 在 Cyber Protect 主控台中，移至 **[軟體管理]**。
2. 按一下 **[軟體清查]**。
3. 在 **[分組依據：]** 下拉式欄位中，選擇 **[裝置]**。
4. 使用下列其中一個選項，尋找您要檢查的裝置。
   - 使用 **[篩選]** 尋找裝置：
     a. 按一下 **[篩選]**。
     b. 在 **[裝置名稱]** 欄位上，選擇您要檢視的裝置的名稱。
     c. 按一下**[套用]**。
   - 使用動態 **[搜尋]** 尋找裝置：
     a. 按一下 **[搜尋]**。
     b. 輸入裝置的完整或部分名稱。

若要從 [裝置] 畫面檢視單一裝置的軟體清查

1. 在 Cyber Protect 主控台中，移至 **[裝置]**。
2. 按一下您要檢視的裝置，然後按一下 **[清查]**。
3. 按一下 **[軟體]** 索引標籤。

硬體清查

硬體清查功能可讓您檢視適用於下列裝置的所有硬體元件：

- 實體 Windows 和 macOS 裝置，其中包含支援硬體清查功能的授權。
- 在下列虛擬化平台上執行的須你 Windows 和 macOS 電腦：VMware、Hyper-V、Citrix、Parallels、Oracle、Nutanix、Virtuozzo 和 Virtuozzo Hybrid Infrastructure。如需有關支援的虛擬化平台版本的詳細資訊，請參閱 "支援的虛擬化平台" (第 30 頁)。

注意事項
Cyber Protect 舊版不支援虛擬機器的硬體清查功能。

只有已安裝保護代理程式的裝置支援硬體清查功能。

若要取得硬體清查資料，您可以在裝置上執行自動或手動掃描。

您可以使用硬體清查資料來：

- 探索組織的所有硬體資產
- 瀏覽組織中所有裝置的硬體清查
- 比較多個公司裝置上的硬體元件
- 檢視硬體元件的詳細資訊。

啟用硬體清查掃描

在實體裝置和虛擬機器上啟用硬體清查掃描時，系統會每 12 小時自動收集硬體資料一次。

預設會啟用硬體清查掃描功能，但必要時，您可以變更設定。

注意事項
客戶租用戶可以啟用或停用硬體清查掃描。單位租用戶僅能檢視硬體清查掃描設定，但無法變更設定。

若要啟用硬體清查掃描

1. 在 Cyber Protect 主控台中，移至 **[設定]**。
2. 按一下 **[保護]**。
3. 按一下 **[清查掃描]**。
4. 按一下模組名稱旁邊的開關，以啟用 **[硬體清查掃描]** 模組。

若要停用硬體清查掃描

1. 在 Cyber Protect 主控台中，移至 **[設定]**。
2. 按一下 **[保護]**。
3. 按一下 **[清查掃描]**。
4. 按一下模組名稱旁邊的開關，以停用 **[硬體清查掃描]** 模組。

手動執行硬體清查掃描

您可以對單一裝置手動執行硬體清查掃描，並檢視裝置硬體元件的目前資料。

注意事項
只有在虛擬機器的目前日期和時間對應到 UTC 的目前日期和時間時，才支援虛擬機器的硬體清查掃描。為確保虛擬機器使用正確的時間設定，請停用虛擬機器的 **[時間同步]** 選項，設定目前的日期、時間和時區，然後重新啟動 **Acronis Agent Core Service** 和 **Acronis Managed Machine Service**。

必要條件

- (適用於所有裝置) 這些裝置可使用 Windows 或 macOS 作業系統。
- (對於所有裝置) 裝置具備支援硬體清查功能的授權。請注意，(舊版) Cyber Protect 不支援虛擬機器的硬體清查功能。
- (適用於所有裝置) 裝置上已安裝保護代理程式。

- (適用於虛擬機器) 電腦可在其中一個支援的虛擬化平台上運作。如需詳細資訊，請參閱 "硬體清查" (第 892 頁)。

若要在單一裝置上執行硬體清查掃描

1. 在 Cyber Protect 主控台中，移至 **[裝置]**。
2. 按一下您要掃描的裝置，然後按一下 **[清查]**。
3. 在 **[硬體]** 索引標籤中，按一下 **[立即掃描]**。

瀏覽硬體清查

您可以檢視並瀏覽資料中可用於所有公司裝置的所有硬體元件。

必要條件

- (適用於所有裝置) 這些裝置可使用 Windows 或 macOS 作業系統。
- (適用於所有裝置) 這些裝置的授權支援硬體清查功能。請注意，Cyber Protect 舊版不支援虛擬機器的硬體清查功能。
- (適用於所有裝置) 裝置上已安裝保護代理程式。
- (適用於所有裝置) 裝置上的硬體清查掃描已成功完成。
- (適用於虛擬機器) 電腦可在其中一個支援的虛擬化平台上運作。如需詳細資訊，請參閱 "硬體清查" (第 892 頁)。

若要檢視適用於 Windows 和 macOS 公司裝置的所有硬體元件

1. 在 Cyber Protect 主控台中，移至 **[裝置]**。
2. 在 **[檢視：]** 下拉式欄位中，選擇 **[硬體]**。

注意事項
此檢視是一組欄位，可決定在畫面中顯示的資料。預先定義的檢視為 **[標準]** 和 **[硬體]**。您可以建立並儲存包含不同組欄位，且更方便滿足您需求的自訂檢視。

下表描述 **[硬體]** 檢視中顯示的資料。

欄	描述
名稱	裝置名稱。
硬體掃描狀態	硬體掃描的狀態。 • **[已完成]**。 • **[未開始]**。 • 系統會針對不支援硬體清查功能的工作負載，顯示 **[不支援]** 狀態，亦即，虛擬機器、行動裝置、Linux 裝置。 • 如果在裝置上安裝過期版本的代理程式，則會顯示 **[更新代理程式]**。按一下此動作將會重新導向至 [設定] > [代理程式] 頁面，系統管理員

欄	描述
	可以在該頁面上執行代理程式更新。 • **升級配額**。按一下此選項將開啟一個對話方塊，系統管理員可以在該對話方塊中，將目前的授權切換到其他可用於租用戶授權的其中一個授權
處理器	裝置所有處理器的型號。
處理器核心	裝置所有處理器的型號。
磁碟儲存空間	以使用的儲存空間，以及裝置所有磁碟的總儲存空間。
記憶體	裝置的 RAM 容量總計。
掃描日期	上次硬體清查掃描的日期和時間。
主機板	裝置的主機板。
主機板序號	主機板的序號。
BIOS 版本	系統 BIOS 的版本。
組織	裝置所屬的組織。
擁有者	裝置的擁有者。
網域	裝置的網域。
作業系統	裝置的作業系統。
作業系統組建	裝置作業系統的組建。

3. 若要在表格中新增欄，按一下欄選項圖示，然後選擇您要在表格中顯示的欄。
4. 若要縮小畫面上顯示的資訊範圍，請使用一或多個篩選條件。
   a. 按一下 **[搜尋]**。
   b. 按一下箭頭，然後按一下 **[硬體]**。
   c. 選擇一個篩選條件或數個篩選條件的組合。

      下表描述 **[硬體]** 篩選條件。

篩選器	描述
處理器型號	可以複選。如果您要檢視具備指定處理器型號之裝置的硬體資料，請使用此篩選條件。
處理器核心	如果您要檢視具備指定處理器核心數目之裝置的硬體資料，請使用此篩選條件。
磁碟大小總計	如果您要檢視具備指定儲存空間大小總計之裝置的硬體資料，請使用此篩選條件。

篩選器	描述
記憶體容量	如果您要檢視具備指定 RAM 容量之裝置的硬體資料，請使用此篩選條件。

d. 按一下**[套用]**。

5. 若要以遞增順序排序資料，按一下欄名稱。

檢視單一裝置的硬體

您可以檢視特定裝置的主機板、處理器、記憶體、圖形卡、儲存磁碟機、網路和系統的詳細資訊。

必要條件

- (適用於所有裝置) 這些裝置可使用 Windows 或 macOS 作業系統。
- (適用於所有裝置) 這些裝置的授權支援硬體清查功能。請注意，Cyber Protect 舊版不支援虛擬機器的硬體清查功能。
- (適用於所有裝置) 裝置上已安裝保護代理程式。
- (適用於所有裝置) 裝置上的硬體清查掃描已成功完成。
- (適用於虛擬機器) 電腦可在其中一個支援的虛擬化平台上運作。如需詳細資訊，請參閱 "硬體清查" (第 892 頁)。

若要檢視特定裝置硬體的詳細資訊

1. 在 Cyber Protect 主控台中，移至 **[裝置]** -> **[所有裝置]**。
2. 在 **[檢視：]** 下拉式欄位中，選擇 **[硬體]**。
3. 使用以下所述的其中一個方法，尋找您要檢查的裝置。
   - 使用 **[篩選]** 尋找裝置：
     a. 按一下 **[篩選]**。
     b. 選擇一個篩選參數或數個篩選參數的組合以尋找裝置。
     c. 按一下**[套用]**。
   - 使用 **[搜尋]** 尋找裝置：
     a. 按一下 **[搜尋]**。
     b. 輸入裝置的完整或部分名稱，然後按一下 **Enter**。
4. 按一下列出裝置的那一列，然後按一下 **[清查]**。
5. 按一下 **[硬體]** 索引標籤。

   隨即提供下列硬體資料。

硬體元件	顯示的資訊
主機板	裝置主機板的名稱、製造商、型號和序號。
處理器	裝置各個處理器的製造商、型號、最大時脈速度和核心數目。

硬體元件	顯示的資訊
記憶體	裝置記憶體的容量、製造商和序號。
圖形卡	裝置 GPU 的製造商和型號。
儲存磁碟機	裝置儲存磁碟機的型號、媒體類型、可用空間和大小。
網路	裝置網路介面卡的 Mac 位址、IP 位址和類型。
系統	系統的產品識別碼、原始安裝日期、系統開機時間、系統製造商、系統型號、BIOS 版本、開機裝置、系統地區設定和時區。

連線至遠端桌面或遠端協助的工作負載

遠端桌面和協助功能是一種便利的方式，可連線到您組織中的工作負載以進行遠端控制或遠端協助。從 2022 年 12 月開始，此功能支援 NEAR、RDP 和 [Apple 畫面共用] 通訊協定。如需詳細資訊，請參閱 "遠端連線通訊協定" (第 902 頁)。

您可以使用遠端桌面功能執行下列工作。

- 在僅檢視模式下，使用 NEAR 連線到遠端 Windows、macOS 和 Linux 工作負載。
- 使用 RDP 連線到遠端 Windows 工作負載。
- 在僅檢視或窗簾模式下，使用 [Apple 畫面共用] 連線到遠端 macOS 工作負載。
- 使用雲端遠端連線，連線到受管理的工作負載並從遠端進行控制。
- 使用直接遠端連線，連線到未受管理的工作負載並從遠端進行控制。
- 使用 Acronis 快速協助 連線到未受管理的遠端工作負載。
- 使用不同的驗證方法連線至遠端工作負載：使用遠端工作負載認證 (透過要求觀察或控制的權限)，或是使用存取代碼 (適用於 快速協助)。
- 在多重檢視中同時觀察多個監視器。
- 錄製遠端工作階段 (透過 NEAR 連線時)。
- 檢視工作階段歷程記錄報告。

如需有關標準和 Advanced Management 套件隨附功能的詳細資訊，請參閱 "支援的遠端桌面與協助功能" (第 899 頁)。

您可以使用遠端協助功能執行下列工作。

- 在控制模式下，使用 NEAR 連線到遠端 Windows、macOS 和 Linux 工作負載。
- 在控制模式下，使用 [Apple 畫面共用] 連線到遠端 macOS 工作負載。
- 使用雲端遠端連線，為工作負載提供遠端協助。
- 在本機和遠端工作負載之間傳輸檔案。
- 在遠端工作負載上執行基本管理動作：重新啟動、關閉、睡眠、清空資源回收桶，以及登出遠端使用者。
- 透過定期擷取其桌面的螢幕擷取畫面來監控遠端工作負載。

如需有關標準保護和 Advanced Management 隨附功能的詳細資訊，請參閱 "支援的遠端桌面與協助功能" (第 899 頁)。

重要事項

若要啟用受管理工作負載的完整遠端桌面和協助功能，您必須設定遠端管理計劃，並將其套用到工作負載。雖然您只能在工作負載上套用一個遠端管理計劃，但可以根據您的需求設定不同的遠端管理計劃，並將其套用到不同的工作負載。

例如，您可以建立僅啟用 RDP 通訊協定的遠端管理計劃，並將其套用到部分工作負載。如此一來，您將能夠從遠端連線到這些工作負載，而不必根據工作負載啟用 Advanced Management 授權，也不必支付任何額外費用。

在另一方面，您可以建立另一個啟用 NEAR 和 [Apple 畫面共用] 通訊協定的遠端管理計劃。在此情況下，將根據工作負載啟用 Advanced Management 授權，而且您將對套用此遠端管理計劃的每個工作負載付費。

如需有關遠端管理計劃和如何使用這些計劃的詳細資訊，請參閱 "遠端管理計劃" (第 905 頁)。

注意事項

遠端桌面與協助功能要求：

- 在管理 (主機) 工作負載上安裝 Connect 用戶端 一次。當您首次嘗試對目標工作負載執行遠端動作 (遠端控制或遠端協助) 時，系統會建議您下載用戶端。或者，也可以從 保護 主控台的 **[下載]** 視窗下載 Connect 用戶端。如需有關您可以進行之設定的詳細資訊，請參閱 "設定 Connect 用戶端 設定" (第 932 頁)。
- 在受管理工作負載上安裝 Connect 代理程式。Connect 代理程式 是屬於 保護 代理程式一部分的模組 (自 15.0.31266 版起)。
- 針對 macOS 遠端工作負載，應將所需的系統權限授予 Connect 代理程式。如需詳細資訊，請參閱 "在 macOS 中安裝保護代理程式" (第 76 頁)。
- 在未受管理的工作負載上執行 Acronis 快速協助 應用程式。您可以從網站下載 Acronis 快速協助。

如需有關每個遠端桌面和協助元件支援之平台的詳細資訊，請參閱 "支援的平台" (第 901 頁)。

支援的遠端桌面與協助功能

下表針對 2022 年 12 月推出的遠端桌面和協助功能支援的功能變更，提供詳細資訊。

功能	標準保護 在 2022 年 12 月之前	Advanced Management 在 2022 年 12 月之前	標準保護 在 2022 年 12 月之後	Advanced Management 在 2022 年 12 月之後
透過 Windows 版 RDP 的遠端協助連線	是	否	否	否
與使用者共用遠端連線	否	是	否	否
遠端連線				

功能	標準保護 在 2022 年 12 月之前	Advanced Management 在 2022 年 12 月之前	標準保護 在 2022 年 12 月之後	Advanced Management 在 2022 年 12 月之後
遠端動作	否	否	是	是
針對 Windows/macOS/Linux 選擇要連線的工作階段	否	否	否	是
透過 RDP 和 [Apple 畫面共用] 直接連線	否	否	否	是
多視窗控制	否	否	否	是
連線模式：控制/僅檢視/窗簾	否	否	否	是
遠端連線的常見認證支援	否	否	是	是
每個技術人員的並行連線				
透過 RDP	是	是	是	是
透過 NEAR	否	否	否	是
檔案傳輸與共用				
從 Windows 到 Windows/macOS/Linux	否	否	否	是
從 macOS 到 Windows/macOS/Linux	否	否	否	是
從 Linux 到 Windows/macOS/Linux	否	否	否	是
透過快速協助應用程式連線				
從 Windows 到 Windows/macOS/Linux	否	否	否	是
從 macOS 到 Windows/macOS/Linux	否	否	否	是
從 Linux 到 Windows/macOS/Linux	否	否	否	是
透過通訊協定遠端連線				
透過 NEAR 遠端連線				
從 Windows 到 Windows/macOS/Linux	否	否	否	是

功能	標準保護 在 2022 年 12 月之前	Advanced Management 在 2022 年 12 月之前	標準保護 在 2022 年 12 月之後	Advanced Management 在 2022 年 12 月之後
從 macOS 到 Windows/macOS/Linux	否	否	否	是
從 Linux 到 Windows/macOS/Linux	否	否	否	是
透過 RDP 遠端連線 (桌面用戶端)				
從 Windows 到 Windows	是	是	是	是
從 macOS 到 Windows	是	是	是	是
從 Linux 到 Windows	否	否	是	是
透過 RDP 遠端連線 (Web 用戶端)				
從 Windows 到 Windows	是	是	是	是
從 macOS 到 Windows	是	是	是	是
從 Linux 到 Windows	否	否	是	是
透過 [Apple 畫面共用] 遠端連線				
從 Windows/macOS/Linux 到 macOS	否	否	否	是
工作階段管理				
工作階段錄製	否	否	否	是
報告與監控				
工作階段歷程記錄和搜尋	否	否	否	是
螢幕擷取畫面傳輸	否	否	否	是
透過剪貼簿交換檔案	否	否	否	是

支援的平台

下表列出遠端桌面和協助功能的每個元件所支援的作業系統。

遠端桌面元件	支援的平台
Connect 用戶端	• Windows 7 或更新版本 • macOS 10.13 或更新版本 • Linux：

遠端桌面元件	支援的平台
	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 代理程式	• Windows 7 或更新版本 • Windows Server 2008 R2 或更新版本 • macOS 10.13 或更新版本 • 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
Acronis 快速協助	• Windows 7 或更新版本 • Windows Server 2008 R2 或更新版本 • macOS 10.13 或更新版本 • 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

遠端連線通訊協定

遠端桌面功能會針對遠端連線使用下列通訊協定。

NEAR

NEAR 是由 Acronis 開發，且高度安全的通訊協定，具有以下特性。

- ### H.264

  NEAR 實作三個品質模式：**[順暢]**、**[平衡]** 和 **[銳利]**。在 **[順暢]** 模式中，NEAR 在 macOS 和 Windows 上使用硬體 H.264 編碼來為桌面圖片編碼，如果硬體編碼器不可用，則回復為軟體編碼器。圖片大小目前限制為 Full HD 解析度 (1920x1080)。

- ### 自適應轉碼器

  在 **[平衡]** 和 **[銳利]** 品質模式中，NEAR 使用自適應轉碼器，相較於 H.264 使用的「視訊」模式，它提供 32 位元的完整圖片品質。

  在 **[平衡]** 模式中，圖片品質會根據您目前的網路條件自動調整並保留目前的幀率。

  在 **[銳利]** 模式中，圖片是完整品質，但如果您的網路、處理器或視訊卡超載，它可能會降低幀率。

  在 Windows 和 macOS 的圖形驅動程序中可用時，自適應轉碼器會使用 OpenCL。

- ### 聲音傳輸

  NEAR 能夠擷取遠端電腦聲音並傳輸到主機。如需有關在 Windows、macOS 和 Linux 上啟用遠端聲音重新導向的詳細資訊，請參閱 "遠端聲音重新導向" (第 903 頁)。

- ### 不同的登入選項

  您可以使用下列方法登入遠端主控台。

  存取代碼：登入遠端工作負載的使用者會執行 快速協助 並告知您存取代碼。使用此方式，一律會連線到目前已登入之使用者的工作階段。

  工作負載認證：使用工作負載中註冊的系統管理員認證來登入遠端工作負載。

  要求觀察或控制權限：已登入遠端工作負載的使用者將被要求允許或拒絕連線。

- ### 安全性

  您的資料一律使用 NEAR 中的 AES 加密來進行雙向加密。

RDP

遠端桌面通訊協定(RDP) 是由 Microsoft 開發的專屬通訊協定，可透過網路連線連接到遠端 Windows 電腦。

Apple 畫面共用

[Apple 畫面共用] 是 Apple 的 VNC 用戶端，包含在 macOS 10.5 和更新版本中。

遠端聲音重新導向

Connect 用戶端 支援透過 NEAR 連線通訊協定的音訊串流。如需有關 NEAR 的詳細資訊，請參閱 "遠端連線通訊協定" (第 902 頁)。

從遠端 Windows 工作負載重新導向聲音

針對 Windows 工作負載，應該會自動傳輸遠端聲音。請確認聲音輸出裝置 (喇叭或耳機) 已連線至該遠端工作負載。

從遠端 macOS 工作負載重新導向聲音

若要啟用從 macOS 工作負載的聲音重新導向，請確認下列各點：

- 此工作負載已安裝 保護 代理程式。
- 該工作負載已安裝聲音擷取驅動程式。
- 該工作負載使用 NEAR 通訊協定進行遠端連線。

注意事項
若是 macOS 10.15 Catalina，則必須將麥克風權限授予 Connect 代理程式。如需有關如何將麥克風權限授予 Connect 代理程式 的詳細資訊，請參閱 "將所需的系統權限授予 Connect 代理程式" (第 71 頁)。

該代理程式使用下列聲音擷取驅動程式：Soundflower 或 Blackhole。

Blackhole wiki 頁面描述了最新版本的安裝程序：https://github.com/ExistentialAudio/BlackHole/wiki/Installation。

注意事項
Connect 用戶端 目前僅支援雙聲道版本的 Blackhole。

或者，如果該工作負載上已安裝 Homebrew，則可透過執行下列命令來安裝 Blackhole：

```
brew install --cask blackhole-2ch
```

注意事項
當遠端 macOS 工作負載的聲音被重新導向時，已登入該遠端工作負載的使用者將不會聽到聲音。

從遠端 Linux 工作負載重新導向聲音

遠端聲音重新導向應該自動適用於大多數的 Linux 發行版。如果預設情況下，遠端聲音重新導向未運作，請執行下列命令來安裝 PulseAudio 驅動程式：

```
sudo apt-get install pulseaudio
```

連線至遠端桌面或遠端協助的遠端工作負載

遠端桌面和協助功能提供多種方式來建立與工作負載的遠端直接連線或雲端連線。

系統會在 Connect 用戶端 和未安裝代理程式的遠端工作負載之間，透過區域網路 (LAN) 中的 TCP/IP 建立直接連線。此種連線不需要網際網路存取。

系統會在 Connect 用戶端 和工作負載上的代理程式或 快速協助 之間，透過 Acronis Cloud 端建立雲端連線。

下表提供有關雲端連線選項的詳細資訊。

雲端連線	雲端連線選項	檢視模式	支援的遠端動作	可用於
透過 NEAR	從 Connect 用戶端 到 Connect 代理程式 從 Connect 用戶端 到 快速協助	控制 僅檢視	遠端桌面 遠端協助	受管理的工作負載
透過 RDP	從 Connect 用戶端 到 Connect 代理程式 從 Web 用戶端到 Connect 代理程式	控制	遠端桌面	受管理的工作負載
透過 Apple 畫面共用	從 Connect 用戶端 到 Connect 代理程式	控制 僅檢視 窗簾	遠端桌面 遠端協助	受管理的工作負載

下表提供有關直接連線選項的詳細資訊。

直接連線	直接連線選項	支援的遠端動作	可用於
透過 RDP	從 Connect 用戶端 到 RDP 伺服器	遠端桌面	未受管理的工作負載
透過 Apple 畫面共用	從 Connect 用戶端 到 Apple 畫面共用伺服器	遠端桌面 遠端協助	未受管理的工作負載

遠端管理計劃

遠端管理計劃是在 保護 代理程式上套用的計劃，用於在受管理工作負載上啟用和設定遠端桌面與協助功能。

如果工作負載上未套用任何遠端管理計劃，遠端桌面與協助功能將限制為遠端動作 (重新啟動、關閉、睡眠、清空資源回收桶，以及登出遠端使用者)。

注意事項

您在遠端管理計劃中可以設定之設定的可用性，端視租用戶上套用的 Service Pack 而定。若要存取所有設定，請啟用 Advanced Management 套件。如需有關標準和 Advanced Management 套件隨附功能的詳細資訊，請參閱 "支援的遠端桌面與協助功能" (第 899 頁)。

建立遠端管理計劃

您可以建立遠端管理計劃，然後將其指派給工作負載，以便在受管理的工作負載上設定遠端桌面和協助功能。

注意事項
遠端管理計劃的設定之可用性，端視指派給租用戶的服務配額而定。如果使用標準功能，則只能透過 RDP 設定連線。

必要條件

已為您的使用者帳戶啟用 2FA。

若要建立遠端管理計劃

來自遠端管理計劃

1. 在 Cyber Protect 主控台中，移至 **[管理]** > **[遠端管理計劃]**。
2. 使用兩個選項其中之一，建立遠端管理計劃。
   - 如果清單中沒有遠端管理計劃，請按一下 **[建立]**。
   - 如果清單中有遠端管理計劃，請按一下 **[建立計劃]**。
3. [選用] 若要變更計劃的預設名稱，請按一下鉛筆圖示，輸入計劃的名稱，然後按一下 **[繼續]**。
4. 按一下 **[連線通訊協定]**，並啟用您要在此遠端管理計劃中用於遠端連線的通訊協定 - NEAR、RDP 或 [Apple 畫面共用]。
5. [選用] 針對 NEAR 通訊協定，在 **[安全性設定]** 區段中，選擇或清除核取方塊以啟用或停用相對應的設定，然後按一下 **[完成]**。

設定	描述	可用於
當使用者中斷與主控台工作階段的連線時鎖定工作負載	如果選擇此設定，則當您中斷與主控台工作階段的連線時，將會鎖定遠端工作負載。	Windows、macOS
一次僅允許一個使用者使用 NEAR 連線或傳輸檔案	如果選擇此設定，當與工作負載有作用中的遠端連線時，就不可能使用 NEAR 連線和檔案傳輸。	Windows、macOS、Linux
允許工作負載系統管理員連線到任何非系統管理員使用者工作階段	如果選擇此設定，系統管理員將被允許連線到工作負載上的任何標準使用者工作階段。 如果 **[允許工作負載系統管理員連線到任何非系統管理員使用者工作階段]** 和 **[允許建立系統工作階段]** 皆清除，則您將只能連線至遠端	Windows、macOS

設定	描述	可用於
	macOS 工作負載上的作用中系統管理員工作階段。	
允許建立系統工作階段	如果選擇此設定，當建立遠端連線時，系統管理員將會在新的工作階段中連線，而不會在現有作用中的工作階段其中之一連線。	macOS
允許剪貼簿同步	如果選擇此設定，將可在您的剪貼簿與遠端工作負載的剪貼簿之間傳輸資料。例如，您可以從遠端工作負載的某個檔案複製部分文字，並貼到您的工作負載上的檔案中，反之亦可。	Windows、macOS、Linux

6. 按一下 **[安全性設定]** 區段中，選擇或清除核取方塊以啟用或停用相對應的設定，然後按一下 **[完成]**。

設定	描述
顯示工作負載是否從遠端控制	如果選擇此設定，當工作負載有作用中的遠端桌面連線時，將會在遠端工作負載的桌面上顯示一個通知。
要求使用者擷取工作負載螢幕擷取畫面的權限	如果選擇此設定，則遠端工作負載的使用者將會在系統管理員要求從工作負載傳輸螢幕擷取畫面時收到通知。

7. 按一下 **[工作負載管理]**，選擇您希望在遠端工作負載上可使用的功能，然後按一下 **[完成]**。

設定	描述	可用於
檔案傳輸	啟用本機與遠端工作負載之間的檔案傳輸。	Windows、macOS、Linux
螢幕擷取畫面傳輸	可將遠端工作負載的桌面螢幕擷取畫面傳輸到 Cyber Protect 主控台。	Windows、macOS、Linux

8. 按一下 **[顯示設定]**，選擇或清除核取方塊以啟用或停用對應的設定，然後按一下 **[完成]**。

注意事項
[顯示設定] 僅適用於透過 NEAR 連線。

設定	描述	可用於
使用桌面重複資料刪除擷取桌面	桌面複製是 Windows 上的其中一個螢幕擷取方法。在某些環境中，此方法可能不穩定。如果您未使用桌面重複資料刪除，將會改用基本方法 (BitBit) - 此方法的速度慢很多，但是較穩定。	Windows
使用 OpenCL 加速	OpenCL 加速可以透過在圖形處理器 (GPU) 上執行某些計算，來加速自適應轉碼器；該轉碼器負責 **[平衡]** 品質模式。這需要在遠端 Linux 上安裝 OpenCL 驅動程式。 在 macOS 和 Windows 上，如果在您的圖形驅動程式中可用，則自適應轉碼器會使用 OpenCL。	Linux
使用硬體 H.264 編碼	NEAR 支援三個品質模式：**[順暢]**、**[平衡]** 和 **[銳利]**。 **[順暢]** 模式會使用硬體 H.264 編碼，為桌面圖片編碼。 **[平衡]** 模式使用自適應轉碼器，相較於 H.264 使用的「視訊」模式，它提供 32 位元的完整圖片品質。圖片品質會根據您目前的網路條件自動調整並保留目前的畫面播放速率。 **[銳利]** 模式使用自適應轉碼器，相較於 H.264 使用的「視訊」模式，它提供 32 位元的完整圖片品質。您一律會獲得完整圖片品質，但如果您的網路或處理器/視訊卡超載，它可能會降低每秒畫面格數。	Windows、macOS

9. 如果您希望上次登入工作負載的使用者相關資訊顯示在工作負載的詳細資料中，按一下 **[工具箱]**，選擇 **[顯示上次登入的使用者]**，然後按一下 **[完成]**。
   如需有關上次登入的使用者的詳細資訊，請參閱 "找出最後登入的使用者" (第 326 頁)。
10. [選用] 若要將工作負載新增到計劃：

a. 按一下 **[新增工作負載]**。
b. 選擇工作負載，然後按一下 **[新增]**。
c. 如果有要解決的相容性問題，請遵照 "解決遠端管理計劃的相容性問題" (第 915 頁) 中所述的程序進行。

11. 按一下 **[建立]**。

從所有裝置

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 按一下您要套用至遠端管理計劃的工作負載。
3. 按一下 **[保護]**，然後按一下 **[新增計劃]**。
4. 按一下 **[建立計劃]**，然後選擇 **[遠端管理]**。
5. [選用] 若要變更計劃的預設名稱，請按一下鉛筆圖示，輸入計劃的名稱，然後按一下 **[繼續]**。
6. 按一下 **[連線通訊協定]**，並啟用您要在此遠端管理計劃中用於遠端連線的通訊協定 - NEAR、RDP 或 [Apple 畫面共用]。
7. [選用] 針對 NEAR 通訊協定，在 **[安全性設定]** 區段中，選擇或清除核取方塊以啟用或停用相對應的設定，然後按一下 **[完成]**。

設定	描述	可用於
當使用者中斷與主控台工作階段的連線時鎖定工作負載	如果選擇此設定，則當您中斷與主控台工作階段的連線時，將會鎖定遠端工作負載。	Windows、macOS
一次僅允許一個使用者使用 NEAR 連線或傳輸檔案	如果選擇此設定，當與工作負載有作用中的遠端連線時，就不可能使用 NEAR 連線和檔案傳輸。	Windows、macOS、Linux
允許工作負載系統管理員連線到任何非系統管理員使用者工作階段	如果選擇此設定，系統管理員將被允許連線到工作負載上的任何標準使用者工作階段。 如果 **[允許工作負載系統管理員連線到任何非系統管理員使用者工作階段]** 和 **[允許建立系統工作階段]** 皆清除，則您將只能連線至遠端 macOS 工作負載上的作用中系統管理員工作階段。	Windows、macOS
允許建立系統工作階段	如果選擇此設定，當建立遠端連線時，系統管理員將會在新的工作階段中連線，而不會在現有作用中的工作階段其中之一連線。	macOS

設定	描述	可用於
允許剪貼簿同步	如果選擇此設定，將可在您的剪貼簿與遠端工作負載的剪貼簿之間傳輸資料。例如，您可以從遠端工作負載的某個檔案複製部分文字，並貼到您的工作負載上的檔案中，反之亦可。	Windows、macOS、Linux

8. 按一下 **[安全性設定]** 區段中，選擇或清除核取方塊以啟用或停用相對應的設定，然後按一下 **[完成]**。

設定	描述
顯示工作負載是否從遠端控制	如果選擇此設定，當工作負載有作用中的遠端桌面連線時，將會在遠端工作負載的桌面上顯示一個通知。
要求使用者擷取工作負載螢幕擷取畫面的權限	如果選擇此設定，則遠端工作負載的使用者將會在系統管理員要求從工作負載傳輸螢幕擷取畫面時收到通知。

9. 按一下 **[工作負載管理]**，選擇您希望在遠端工作負載上可使用的功能，然後按一下 **[完成]**。

設定	描述	可用於
檔案傳輸	啟用本機與遠端工作負載之間的檔案傳輸。	Windows、macOS、Linux
螢幕擷取畫面傳輸	可將遠端工作負載的桌面螢幕擷取畫面傳輸到 Cyber Protect 主控台。	Windows、macOS、Linux

10. 按一下 **[顯示設定]**，選擇或清除核取方塊以啟用或停用對應的設定，然後按一下 **[完成]**。

注意事項
[顯示設定] 僅適用於透過 NEAR 連線。

設定	描述	可用於
使用桌面重複資料刪除擷取桌面	桌面複製是 Windows 上的其中一個螢幕擷取方法。在某些環境中，此方法可能不穩定。如果您未使用桌面重複資料刪除，將會改用基本方法 (BitBit) - 此方法的速度慢很多，但是較穩定。	Windows

設定	描述	可用於
使用 OpenCL 加速	OpenCL 加速可以透過在圖形處理器 (GPU) 上執行某些計算，來加速自適應轉碼器；該轉碼器負責 **[平衡]** 品質模式。這需要在遠端 Linux 上安裝 OpenCL 驅動程式。 在 macOS 和 Windows 上，如果在您的圖形驅動程式中可用，則自適應轉碼器會使用 OpenCL。	Linux
使用硬體 H.264 編碼	NEAR 支援三種品質模式：**[順暢]**、**[平衡]** 和 **[銳利]**。 **[順暢]** 模式會使用硬體 H.264 編碼，為桌面圖片編碼。 **[平衡]** 模式使用自適應轉碼器，相較於 H.264 使用的「視訊」模式，它提供 32 位元的完整圖片品質。圖片品質會根據您目前的網路條件自動調整並保留目前的畫面播放速率。 **[銳利]** 模式使用自適應轉碼器，相較於 H.264 使用的「視訊」模式，它提供 32 位元的完整圖片品質。您一律會獲得完整圖片品質，但如果您的網路或處理器/視訊卡超載，它可能會降低每秒畫面格數。	Windows、macOS

11. 如果您希望上次登入工作負載的使用者相關資訊顯示在工作負載的詳細資料中，按一下 **[工具箱]**，選擇 **[顯示上次登入的使用者]**，然後按一下 **[完成]**。
    如需有關上次登入的使用者的詳細資訊，請參閱 "找出最後登入的使用者" (第 326 頁)。
12. 按一下 **[建立]**。

將工作負載新增至遠端管理計劃

視您的需要而定，可以在建立遠端管理計劃之後，將工作負載新增至該計劃。

必要條件

已為您的使用者帳戶啟用 2FA。

若要將工作負載新增至遠端管理計劃

來自遠端管理計劃

1. 在 Cyber Protect 主控台中，移至 **[管理]** > **[遠端管理計劃]**。
2. 按一下遠端管理計劃。
3. 根據該計劃是否已套用至任何工作負載而定，執行以下作業：
   - 如果該計劃尚未套用至任何工作負載，請按一下 **[新增工作負載]**。
   - 如果該計劃已套用至任何工作負載，請按一下 **[管理工作負載]**。
4. 從清單中選擇工作負載，然後按一下 **[新增]**。
5. 按一下 **[儲存]**。
6. 按一下 **[確認]** 將所需的服務配額套用至工作負載。

從所有裝置

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 按一下您要套用至遠端管理計劃的工作負載。
3. 按一下 **[保護]**，然後按一下 **[新增計劃]**。
4. 在 **[從底下的清單中選擇一個計劃]** 中，選擇 **[遠端管理]** 以僅檢視遠端管理計劃。
5. 按一下**[套用]**。
6. 按一下 **[確認]** 將所需的服務配額套用至工作負載。

從遠端管理計劃中移除工作負載

視您的需要而定，可以從遠端管理計劃移除工作負載。

必要條件

已為您的使用者帳戶啟用 2FA。

若要從遠端管理計劃中移除工作負載

1. 在 Cyber Protect 主控台中，移至 **[管理]** > **[遠端管理計劃]**。
2. 按一下遠端管理計劃。
3. 按一下 **[管理工作負載]**。
4. 選擇您要從遠端管理計劃移除的一或多個工作負載，然後按一下 **[移除]**。
5. 按一下**[完成]**。
6. 按一下 **[儲存]**。

現有遠端管理計劃的其他動作

在 **[遠端管理計劃]** 畫面上，您可以對遠端管理計劃執行以下其他動作：檢視詳細資料、編輯、檢視活動、檢視警示、重新命名、啟用、停用、複製、匯出、設為我的最愛、設為預設和刪除。

檢視詳細資料

必要條件

已為您的使用者帳戶啟用 2FA。

若要檢視遠端管理計劃的詳細資料

1. 在 **[遠端管理計劃]** 畫面中，按一下遠端管理計劃的 **[更多動作]** 圖示。
2. 按一下 **[檢視詳細資料]**。

編輯

必要條件

已為您的使用者帳戶啟用 2FA。

若要編輯計劃

1. 在 **[遠端管理計劃]** 畫面中，按一下遠端管理計劃的 **[更多動作]** 圖示。
2. 按一下 **[編輯]**。

活動

若要檢視與遠端管理計劃相關的活動

1. 在 **[遠端管理計劃]** 畫面中，按一下遠端管理計劃的 **[更多動作]** 圖示。
2. 按一下 **[活動]**。
3. 按一下活動，以檢視有關它的更多詳細資料。

警示

若要檢視警示

1. 在 **[遠端管理計劃]** 畫面中，按一下遠端管理計劃的 **[更多動作]** 圖示。
2. 按一下 **[警示]**。

重新命名

必要條件

已為您的使用者帳戶啟用 2FA。

若要重新命名遠端管理計劃

1. 在 **[遠端管理計劃]** 畫面中，按一下遠端管理計劃的 **[更多動作]** 圖示。
2. 按一下 **[重新命名]**。
3. 輸入該計劃的新名稱，然後按一下 **[繼續]**。

啟用

必要條件

已為您的使用者帳戶啟用 2FA。

若要啟用遠端管理計劃

1. 在 **[遠端管理計劃]** 畫面中，按一下遠端管理計劃的 **[更多動作]** 圖示。
2. 按一下 **[啟用]**。

停用

必要條件

已為您的使用者帳戶啟用 2FA。

若要停用遠端管理計劃

1. 在 **[遠端管理計劃]** 畫面中，按一下遠端管理計劃的 **[更多動作]** 圖示。
2. 按一下 **[停用]**。

複製

必要條件

已為您的使用者帳戶啟用 2FA。

若要複製遠端管理計劃

1. 在 **[遠端管理計劃]** 畫面中，按一下遠端管理計劃的 **[更多動作]** 圖示。
2. 按一下 **[複製]**。
3. 按一下 **[建立]**。

匯出

必要條件

已為您的使用者帳戶啟用 2FA。

若要匯出遠端管理計劃

1. 在 **[遠端管理計劃]** 畫面中，按一下遠端管理計劃的 **[更多動作]** 圖示。
2. 按一下 **[匯出]**。
   計劃設定將以 JSON 格式匯出到本機電腦。

設為預設

必要條件

已為您的使用者帳戶啟用 2FA。

若要將遠端管理計劃設為預設

1. 在 **[遠端管理計劃]** 畫面中，按一下遠端管理計劃的 **[更多動作]** 圖示。
2. 按一下 **[設為預設]**。
3. 在確認視窗中，按一下 **[設定]**。
   在 **[遠端管理計劃]** 畫面上，**[預設]** 標籤會出現在計劃名稱旁。

設為我的最愛

必要條件

已為您的使用者帳戶啟用 2FA。

若要將遠端管理計劃設為我的最愛

1. 在 **[遠端管理計劃]** 畫面中，按一下遠端管理計劃的 **[更多動作]** 圖示。
2. 按一下 **[新增至我的最愛]**。
   在 **[遠端管理計劃]** 畫面上，星形圖示會出現在計劃名稱旁。

刪除

必要條件

已為您的使用者帳戶啟用 2FA。

若要刪除遠端管理計劃

1. 在 **[遠端管理計劃]** 畫面中，按一下遠端管理計劃的 **[更多動作]** 圖示。
2. 請按一下 **[刪除]**。
3. 選擇 **[我確認]**，然後按一下 **[刪除]**。

遠端管理計劃的相容性問題

在某些情況下，對工作負載套用遠端管理計劃可能會導致相容性問題。您可能會觀察到下列相容性問題：

- 衝突的計劃 - 當另一個遠端管理計劃已套用於工作負載時，會出現此問題，因為只能將一個遠端管理計劃套用於工作負載。
- 不相容的作業系統 - 當工作負載的作業系統不受支援時，會出現此問題。
- 不支援的代理程式 - 當工作負載上的保護代理程式版本已過期，而且不支援遠端桌面功能時，會出現此問題。
- 配額不足 - 當租用戶中沒有足夠的服務配額可指派給所選的工作負載時，會出現此問題。

如果將遠端管理計劃套用至多達 150 項個別選取的工作負載，系統會提示您先解決現有衝突，然後才能儲存計劃。若要解決衝突，請移除其根本原因或從計劃移除受影響的工作負載。如需詳細資訊，請參閱 "解決遠端管理計劃的相容性問題" (第 915 頁)。如果在未解決衝突的情況下儲存計劃，對於不相容的工作負載，該計劃將自動停用，並且會顯示警示。

如果將遠端管理計劃套用至超過 150 項工作負載或裝置群組，則會先儲存計劃，然後再檢查相容性。系統會自動針對不相容的工作負載停用該計劃，並顯示警示。

解決遠端管理計劃的相容性問題

根據相容性問題的原因，您可以執行不同的動作來解決相容性問題，作為建立新遠端管理計劃程序的一部分。

注意事項
透過移除計劃中的工作負載來解決相容性問題時，您無法移除屬於裝置群組一部分的工作負載。

若要解決相容性問題

1. 按一下 **[檢閱問題]**。
2. [透過從新計劃中移除工作負載以解決現有遠端管理計劃的相容性問題]

a. 在 **[衝突的計劃]** 索引標籤上，選擇您要移除的工作負載。
b. 按一下 **[從計劃中移除工作負載]**。
c. 按一下 **[移除]**，然後按一下 **[關閉]**。

3. [透過停用已套用於工作負載的計劃來解決與遠端管理計劃的相容性問題]
   a. 按一下 **[停用已套用的計劃]**。
   b. 按一下 **[停用]**，然後按一下 **[關閉]**。
4. [解決與不相容作業系統的相容性問題]
   a. 在 **[不相容的作業系統]** 索引標籤上，選擇您要移除的工作負載。
   b. 按一下 **[從計劃中移除工作負載]**。
   c. 按一下 **[移除]**，然後按一下 **[關閉]**。
5. [透過從計劃中移除工作負載來解決與不支援的代理程式的相容性問題]
   a. 在 **[不支援的代理程式]** 索引標籤上，選擇您要移除的工作負載。
   b. 按一下 **[從計劃中移除工作負載]**。
   c. 按一下 **[移除]**，然後按一下 **[關閉]**。
6. [透過更新代理程式版本來解決與不支援的代理程式的相容性問題] 按一下 **[移至代理程式清單]**。

   注意事項
   此選項僅適用於客戶系統管理員。

7. [透過從計劃中移除工作負載來解決配額不足的相容性問題]
   a. 在 **[配額不足]** 索引標籤上，選擇您要移除的工作負載。
   b. 按一下 **[從計劃中移除工作負載]**。
   c. 按一下 **[移除]**，然後按一下 **[關閉]**。
8. [透過增加租用戶配額來解決配額不足的相容性問題]

   注意事項
   此選項僅適用於合作夥伴系統管理員。

   a. 在 **[配額不足]** 索引標籤上，按一下 **[前往管理入口網站]**。
   b. 增加客戶的服務配額。

工作負載認證

您可以新增遠端工作負載的系統管理員或非系統管理員認證 (使用者名稱與密碼，或是 VNC 密碼)，將它們儲存在雲端認證存放區，然後在連線到您所管理的工作負載時，使用它們進行自動驗證。如此一來，就不用每次在連線的驗證步驟過程中手動輸入這些認證，您可以將這些認證儲存在認證存放區一次，將其指派給多個工作負載，然後每次您要從遠端連線到工作負載時，Connect 用戶端 就會使用這些認證。

注意事項
儲存在認證存放區中的認證不會在不同租用戶層級之間共用。它們僅在同一個客戶租用戶或合作夥伴租用戶的同一個租用戶層級上共用。

這表示，如果一個客戶租用戶有多個系統管理員，他們將會看到並共用認證存放區中的認證，而任何其他合作夥伴系統管理員或其他租用戶的客戶系統管理員將無法檢視或使用這些認證。

新增認證

您可以新增認證，然後使用它們遠端連線到多個工作負載。

若要新增認證至工作負載並將認證儲存在認證存放區中

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 按一下您要新增其認證的工作負載。
3. 透過下列其中一種方式，存取 **[設定]** 功能表：
   - 按一下 **[遠端桌面]**，然後按一下 **[設定]**。
   - 按一下 **[管理]**，然後按一下 **[設定]**。
4. 按一下 **[新增認證]**。
5. 在 **[認證存放區]** 中，按一下 **[新增認證]**。
6. 輸入認證。

欄位	描述
認證名稱	認證存放區中看得到的認證識別碼。
使用者名稱	將用於遠端連線至目標工作負載的使用者名稱。
密碼	將用於遠端連線至目標工作負載的密碼。
VNC 密碼	此欄位僅適用於 [Apple 畫面共用]。

7. 按一下 **[儲存]**。

將認證指派給工作負載

新增認證之後，當您連線到您管理的工作負載時，可以使用它們自動驗證。

將已儲存用於自動驗證的認證指派給工作負載

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 透過下列其中一種方式，存取 **[設定]** 功能表：
   - 按一下 **[遠端桌面]**，然後按一下 **[設定]**。
   - 按一下 **[管理]**，然後按一下 **[設定]**。
3. 在支援的通訊協定 (NEAR、RDP 或 Apple 畫面共用) 的索引標籤上，按一下 **[新增認證]**。
4. 在 **[認證存放區]** 中，從清單中選擇認證，然後按一下 **[選擇認證]**。

刪除認證

您可以刪除再也不需要的認證。

若要從認證存放區刪除認證

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 透過下列其中一種方式，存取 **[設定]** 功能表：
   - 按一下 **[遠端桌面]**，然後按一下 **[設定]**。
   - 按一下 **[管理]**，然後按一下 **[設定]**。
3. 在支援的通訊協定 (NEAR、RDP 或 Apple 畫面共用) 的索引標籤上，按一下 **[刪除]**。
4. 在確認視窗中，按一下 **[刪除]**。

從工作負載取消指派認證

您可以從工作負載取消指派認證，但仍保留在認證存放區中。

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 透過下列其中一種方式，存取 **[設定]** 功能表：
   - 按一下 **[遠端桌面]**，然後按一下 **[設定]**。
   - 按一下 **[管理]**，然後按一下 **[設定]**。
3. 在支援的通訊協定 (NEAR、RDP 或 Apple 畫面共用) 的索引標籤上，按一下 **[取消指派]**。
4. 在確認視窗中，按一下 **[取消指派]**。

使用管理的工作負載

受管理的工作負載指的是已安裝 保護 代理程式的工作負載。

在遠端受管理的工作負載上，您可以執行下列動作：

- 在控制或僅檢視模式下使用 NEAR 的遠端協助或遠端桌面連線
- 在控制模式下使用 RDP 的遠端桌面連線
- 在控制、僅檢視或窗簾模式下使用 [Apple 畫面共用] 的遠端協助或遠端桌面連線
- 透過 Web 用戶端的遠端桌面連線
- 重新啟動、關閉、睡眠、清空資源回收桶、從遠端工作負載登出遠端使用者
- 在您的工作負載與遠端工作負載之間傳輸檔案
- 透過擷取螢幕擷取畫面加以監控

注意事項
與受管理工作負載的遠端桌面連線，必須在該工作負載上安裝 保護 代理程式並套用遠端管理計劃。

設定 RDP 設定

您可以設定將針對受管理工作負載的遠端控制 RDP 連線自動套用的設定。

若要設定工作負載的 RDP 設定

1. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[具有代理程式的電腦]**。
2. 透過下列其中一種方式，存取 **[設定]** 功能表：
   - 按一下 **[遠端桌面]**，然後按一下 **[設定]**。
   - 按一下 **[管理]**，然後按一下 **[設定]**。
3. 在 **[RDP]** 索引標籤上進行設定。

設定	描述
音訊播放	此設定可啟用或停用您本機工作負載上之遠端工作負載聲音的重新導向。
音訊錄製	此設定可決定是否將音訊錄製 (對著麥克風講話) 傳輸到遠端工作負載。
重新導向印表機	如果選擇此設定，您工作負載的印表機將可供遠端工作負載使用。
重新導向檔案	此設定會定義您本機工作負載的檔案將共用到遠端工作負載。
色彩深度	此設定可決定 RDP 將傳輸之圖片的色彩數。值越高，所需的頻寬越高。 **高彩**：16 位元 **全彩**： • 24 位元，用於透過 Web 用戶端的 RDP 連線 • 32 位元，用於透過 Connect 用戶端 連線 RDP

4. 按一下關閉按鈕。

連線至遠端桌面或遠端協助的受管理工作負載

注意事項
可用於遠端連線的連線通訊協定可用性，端視遠端管理計劃設定和遠端工作負載的作業系統而定。

必要條件

- 已啟用相對應連線通訊協定的遠端管理計劃會套用至受管理的工作負載。
- 所需的服務配額會指派給工作負載。(當您將遠端管理計劃套用至工作負載時，會自動取得服務配額)。
- [針對 [Apple 畫面共用] 連線] 在 macOS 工作負載上啟用 [Apple 畫面共用]。
- 2FA 已在 Acronis Cyber Protect Cloud 中為您的使用者帳戶啟用。

若要從遠端連線至遠端桌面或遠端協助的受管理工作負載

1. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[具有代理程式的電腦]**。
2. 按一下您要連線的工作負載。
3. 按一下 **[遠端桌面]**。
   預設情況下，選擇 NEAR 作為連線通訊協定。

4. [選用] 在 **[連線通訊協定]** 下拉式清單中，選擇您要使用的連線通訊協定。
5. 按一下您要使用的檢視模式。

通訊協定	遠端連線至	檢視模式	支援的遠端動作
NEAR	Windows Linux macOS	**控制** - 在此模式下，您可以觀察及執行遠端工作負載上的作業。 **僅檢視** - 在此模式下，您只能觀察遠端工作負載。	遠端桌面 遠端協助
RDP	Windows	**控制** - 在此模式下，您可以檢視及執行遠端工作負載上的作業。 **注意事項** 如果在工作負載的作業系統設定中停用 RDP，將會出現快顯視窗。使用此視窗為目前工作階段的工作負載或一般工作負載啟用 RDP： • 如果您僅要針對目前工作階段的這個工作負載啟用 RDP，請選擇 **[工作階段結束後停用它]**，然後按一下 **[允許]**。 • 如果您僅要針對這個工作負載啟用 RDP，按一下 **[允許]**。	遠端桌面
Apple 畫面共用	macOS	**控制** - 在此模式下，您可以觀察及執行遠端工作負載上的作業。 **僅檢視** - 在此模式下，您只能觀察遠端工作負載。 **窗簾** - 僅供 rmacOS 工作負載使用。如果您以窗簾模式連線至遠端工作負載，遠端工作負載的顯示將會變暗，而且遠端使用者將無法看到您對工作負載所做的動作。	遠端桌面 遠端協助

6. 根據您的工作負載上是否已安裝 Connect 用戶端 而定，執行下列其中一項操作：
   - 如果未安裝 Connect 用戶端，請先下載、安裝，然後在出現的確認快顯視窗中，選擇 **[允許]**。
   - 如果已安裝 Connect 用戶端，請在出現的確認快顯視窗中，選擇 **[開啟 Connect 用戶端]**。
7. 在 **[驗證]** 視窗中，選擇驗證選項，然後提供所需的認證。

注意事項
如果您已經將認證指派給工作負載，將會自動執行驗證並略過此步驟。如需詳細資訊，請參閱 "將認證指派給工作負載" (第 917 頁)。

驗證選項	描述
使用遠端工作負載認證	提供遠端工作負載系統管理員使用者的使用者名稱和密碼後，您就獲准建立遠端連線。 此選項適用於 NEAR、RDP 和 [Apple 畫面共用]。

驗證選項	描述
	您可以使用此選項，針對遠端桌面和遠端協助進行驗證。
要求觀察權限	在登入遠端工作負載的使用者允許後，您將獲准以觀察模式建立遠端連線。 此選項適用於 NEAR 和 [Apple 畫面共用]。 您可以使用此選項，針對遠端協助進行驗證。
要求控制權限	在登入遠端工作負載的使用者允許後，您將獲准以控制模式建立遠端連線。 此選項適用於 NEAR 和 [Apple 畫面共用]。 您可以使用此選項，針對遠端協助進行驗證。

8. 按一下 **[連線]**，然後按一下要顯示的工作階段 (如果工作負載上可用的使用者工作階段超過一個)。

   Connect 用戶端 將會開啟一個新的檢視器視窗，您將可在其中看到遠端工作負載的桌面。檢視器有一個工具列，其中包含您可在建立遠端連線後對遠端工作負載執行的額外動作。如需詳細資訊，請參閱 "使用檢視器視窗中的工具列" (第 929 頁)。

透過 Web 用戶端連線至受管理的工作負載

您可以透過 Web 用戶端，建立受管理工作負載的遠端桌面連線。

必要條件

- 標準服務配額會指派給工作負載。
- 啟用 RDP 的遠端管理計劃會套用至受管理的工作負載。
- RDP 已在受管理的工作負載上啟用。
- 您的瀏覽器支援 HTML5。
- 2FA 已在 Acronis Cyber Protect Cloud 中為您的使用者帳戶啟用。

若要透過 Web 用戶端從遠端連線至工作負載

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 按一下您要從遠端連線的工作負載，然後按一下 **[遠端桌面]** > **[透過 Web 用戶端連線]**。
3. 輸入用來存取工作負載的登入和密碼，然後按一下 **[連線]**。

注意事項
如果您已經將認證指派給工作負載，將會自動執行驗證並略過此步驟。如需詳細資訊，請參閱 "將認證指派給工作負載" (第 917 頁)。

正在傳輸檔案

您可以在本機工作負載和受管理的工作負載之間輕鬆地傳輸檔案。

必要條件

- 已啟用 NEAR 通訊協定和檔案傳輸的遠端管理計劃會套用至工作負載。
- Advanced Management 配額會套用至工作負載。
- 2FA 已在 Acronis Cyber Protect Cloud 中為您的使用者帳戶啟用。

若要在您的工作負載和受管理的工作負載之間遠端傳輸檔案

1. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[具有代理程式的電腦]**。
2. 按一下您要用來傳輸檔案的工作負載。
3. 按一下 **[管理]**，然後按一下 **[傳輸檔案]**。
4. 根據您的工作負載上是否已安裝 Connect 用戶端 而定，執行下列其中一項操作：
   - 如果未安裝 Connect 用戶端，請先下載、安裝，然後在出現的確認快顯視窗中，按一下 **[允許]**。
   - 如果已安裝 Connect 用戶端，請在出現的確認快顯視窗中，選擇 **[開啟 Connect 用戶端]**。
5. 在 **[驗證]** 視窗中，選擇驗證選項，然後提供所需的認證。

驗證選項	描述
使用遠端工作負載認證	提供遠端工作負載系統管理員使用者的使用者名稱和密碼後，您就獲准建立遠端連線。
要求傳輸檔案權限	在登入遠端工作負載的使用者允許後，您將獲准傳輸檔案。

6. 在 **[檔案傳輸]** 視窗中，瀏覽檔案，並將它們拖放到所需的目的地。

注意事項
本機工作負載的檔案會列在左窗格中，而遠端工作負載的檔案則列在右窗格中。
當檔案傳輸開始時，會列在 **[工作]** 窗格中。

7. [選用] 如果要從 **[工作]** 窗格中移除已完成的工作，請按一下 **[清除已完成]**。
8. 當所有傳輸完成時，關閉視窗。

在工作負載之間共用剪貼簿內容

您可以透過 NEAR，將工作負載的剪貼簿內容傳送至遠端工作負載，或從遠端工作負載取得剪貼簿內容。例如，您可以從遠端工作負載上的檔案複製部分文字，然後將其貼至工作負載上的文件中，反之亦然。

傳送剪貼簿

必要條件

已為您的使用者帳戶啟用 2FA。

將您工作負載的剪貼簿內容傳送至遠端工作負載

1. 透過 NEAR, 對受控工作負載開始遠端控制工作階段。
   如需詳細資訊, 請參閱 "連線至遠端桌面或遠端協助的受管理工作負載" (第 919 頁)。
2. [選用] 若要讓剪貼簿的內容和遠端工作負載的剪貼簿自動同步, 請在 **[檢視器]** 工具列中按一下 **[其他]** 圖示, 然後選擇 **[剪貼簿自動同步]**。
3. 若要將剪貼簿上的內容與遠端工作負載的剪貼簿共用, 請執行下列動作。
   - 如果已停用 **[剪貼簿自動同步]**, 請執行對應的步驟:
     a. 在您的本機工作負載上, 複製您想要傳送的文字或影像。
     b. 在遠端工作負載的 **[檢視器]** 工具列中, 按一下 **[其他]** 圖示。
     c. 按一下 **[傳送剪貼簿]**。
     d. 開啟要貼上內容的檔案, 然後將其貼上。
   - 如果已啟用 **[剪貼簿自動同步]**, 請依據您想要共用的內容, 執行對應的步驟。

選項	動作
如果您想要在本機剪貼簿中共用一或多個檔案	a. 在您的本機工作負載上, 複製您想要傳送的一或多個檔案。 b. 開啟遠端工作負載的 **[檢視器]** 視窗。 c. 在出現的警示快顯視窗中, 按一下 **[傳送至遠端電腦]**。 d. 將內容貼至遠端工作負載。
如果您想要從本機剪貼簿中的檔案共用文字	a. 在您的本機工作負載上, 複製您想要傳送的文字。 b. 開啟遠端工作負載的 **[檢視器]** 視窗。 c. 開啟要貼上內容的檔案。 d. 將內容貼至檔案。

取得剪貼簿

必要條件

已為您的使用者帳戶啟用 2FA。

若要在您的工作負載取得遠端工作負載中的剪貼簿內容

1. 透過 NEAR, 對受控工作負載開始遠端控制工作階段。
   如需詳細資訊, 請參閱 "連線至遠端桌面或遠端協助的受管理工作負載" (第 919 頁)。
2. 若要讓剪貼簿的內容和遠端工作負載的剪貼簿自動同步, 請在 **[檢視器]** 工具列中按一下 **[其他]** 圖示, 然後選擇 **[剪貼簿自動同步]**。
3. 若要在您的工作負載取得遠端工作負載剪貼簿的內容, 請執行下列動作。
   - 如果已停用 **[剪貼簿自動同步]**, 請執行對應的步驟。
     a. 在遠端工作負載上, 複製您想要共用的文字或影像。
     b. 在遠端工作負載的 **[檢視器]** 工具列中, 按一下 **[其他]** 圖示。
     c. 按一下 **[取得剪貼簿]**。
     d. 在本機工作負載上, 開啟要貼上內容的檔案。

e. 將內容貼至檔案。

- 如果已啟用 **[剪貼簿自動同步]**，請依據您想要取得的內容，執行對應的步驟。

選項	動作
如果您想要在您的本機剪貼簿取得遠端工作負載的一或多個檔案	a. 在遠端工作負載上，複製您想要取得的一或多個檔案。 b. 在出現的警示快顯視窗中，按一下 **[接收剪貼簿]**。 c. 在您的本機工作負載上，貼上內容。
如果您想要在您的本機剪貼簿取得遠端工作負載剪貼簿中的文字	a. 在遠端工作負載上，複製您想要取得的文字。 b. 在您的本機工作負載上，將內容貼至檔案。

在受管理的工作負載上執行控制動作

您可以透過對遠端工作負載執行下列基本控制動作，來加以管理：清空資源回收桶、睡眠、重新啟動、關機以及登出遠端使用者。

必要條件

- 標準服務配額會套用至工作負載。
- 2FA 已在 Acronis Cyber Protect Cloud 中為您的使用者帳戶啟用。

清空資源回收桶

若要在遠端工作負載上清空資源回收筒

1. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[具有代理程式的電腦]**。
2. 按一下您要對其執行此動作的工作負載。
3. 按一下 **[管理]**，然後按一下 **[清空資源回收桶]**。
4. 選擇您要對其執行此動作的使用者工作階段，然後按一下 **[清空資源回收桶]**。

睡眠

若要讓遠端工作負載進入睡眠狀態

1. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[具有代理程式的電腦]**。
2. 按一下您要對其執行此動作的工作負載。
3. 按一下 **[管理]**，然後按一下 **[睡眠]**。

重新啟動

若要重新啟動遠端工作負載

1. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[具有代理程式的電腦]**。
2. 按一下您要對其執行此動作的工作負載。

3. 按一下 **[管理]**，然後按一下 **[重新啟動]**。
   - 若是 Windows 工作負載，請選擇您是否要允許目前在本機登入工作負載的使用者先儲存變更再重新啟動工作負載、選擇使用者，然後再按一次 **[重新啟動]**。
   - 若是 macOS 工作負載，請選擇您是否要允許目前在本機登入工作負載的使用者先儲存變更再重新啟動工作負載，然後再按一次 **[重新啟動]**。
   - 對於 Linux 工作負載，按一下 **[重新啟動]**。

關機

若要關機遠端工作負載

1. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[具有代理程式的電腦]**。
2. 按一下您要對其執行此動作的工作負載。
3. 按一下 **[管理]**，然後按一下 **[關機]**。
   - 若是 Windows 工作負載，請選擇您是否要允許目前在本機登入工作負載的使用者先儲存變更再關閉工作負載、選擇使用者，然後再按一次 **[關機]**。
   - 若是 macOS 工作負載，請選擇您是否要允許目前在本機登入工作負載的使用者先儲存變更再關閉工作負載，然後再按一次 **[關機]**。
   - 對於 Linux 工作負載，再按一次 **[關機]**。

登出遠端使用者

若要登出遠端工作負載的使用者

1. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[具有代理程式的電腦]**。
2. 按一下您要對其執行此動作的工作負載。
3. 按一下 **[管理]**，然後按一下 **[登出遠端使用者]**。
4. 選擇您要登出的使用者，然後按一下 **[登出]**。

透過傳輸螢幕擷取畫面監控工作負載

您可以透過使用螢幕擷取畫面傳輸功能，來監控工作負載的狀態。

必要條件

- 已啟用螢幕擷取畫面傳輸功能的遠端管理計劃會套用至工作負載。
- 保護代理程式版本是最新的，並支援螢幕擷取畫面傳輸功能。
- Advanced Management 服務配額會套用至工作負載。
- 工作負載在線上。
- 2FA 已在 Acronis Cyber Protect Cloud 中為您的使用者帳戶啟用。

透過傳輸螢幕擷取畫面監控工作負載

若要透過傳輸螢幕擷取畫面監控工作負載

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[螢幕擷取畫面傳輸]**。
2. 按一下您要監控的工作負載。
3. 選擇使用者工作階段。

4. 選擇顯示。
5. 選擇擷取新的桌面螢幕擷取畫面之更新率。
6. 選擇影像品質。
7. 若要下載螢幕擷取畫面，請按一下下載圖示。

擷取工作負載的螢幕擷取畫面

若要擷取工作負載的螢幕擷取畫面

1. 在 Cyber Protect 主控台中，前往 **[裝置]** > **[具有代理程式的電腦]**。
2. 按一下您要擷取其螢幕擷取畫面的工作負載。
3. 按一下 **[管理]**，然後按一下 **[擷取桌面螢幕擷取畫面]**。
   接著會開啟 **[螢幕擷取畫面傳輸]** 畫面，而且已預先選擇工作負載。根據套用於工作負載的遠端管理計劃設定，您將會看到螢幕擷取畫面，或者將在遠端工作負載的使用者核准要求後看到螢幕擷取畫面。

同時觀察多個受管理工作負載

您可以在單一視窗中同時觀察多個遠端工作負載的桌面。

注意事項
您可在視窗中同時看到的桌面數量，取決於您的螢幕大小。

必要條件

- 在已套用到工作負載的遠端管理計劃中，已啟用 NEAR/Apple 畫面共用。
- Advanced Management 服務配額會套用至工作負載。
- 2FA 已在 Acronis Cyber Protect Cloud 中為您的使用者帳戶啟用。

若要同時觀察多個工作負載

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 選擇您要觀察的工作負載。
3. 按一下 [**多重檢視**]。
4. 根據您的工作負載上是否已安裝 Connect 用戶端 而定，執行下列其中一項操作：
   - 如果未安裝 Connect 用戶端，請先下載、安裝，然後在出現的確認快顯視窗中，選擇 **[允許]**。
   - 如果已安裝 Connect 用戶端，請在出現的確認快顯視窗中，選擇 **[開啟 Connect 用戶端]**。
5. 在 **[驗證]** 視窗中，選擇驗證選項，然後提供所需的認證。

驗證選項	描述
使用遠端工作負載認證	在遠端工作負載上提供系統管理員使用者的使用者名稱和密碼後，您就獲准建立遠端連線。
要求觀察權限	在登入遠端工作負載的使用者允許後，您將獲准以觀察模式建立遠端連線。

6. 如果要使用與連線到步驟 2 中選擇之所有遠端工作負載時的相同驗證方法和認證，請選擇 **[在其他電腦上使用]**。
7. 按一下 **[連線]**。

   在多重檢視視窗的工具列中，可以選擇連線到工作負載的檢視模式。此動作將為該工作負載開啟一個單獨的 [檢視器] 視窗。

注意事項

如果任何所選的工作負載處於離線狀態，或者安裝了過時版本的代理程式，它將不會顯示在多重檢視視窗中。

與遠端工作負載的所有多重檢視連線都在 **[僅檢視]** 模式中。

使用未受管理的工作負載

未受管理的工作負載指的是未安裝 保護 代理程式的工作負載。

在未受管理的遠端工作負載上，您可以執行下列動作：

- 使用 Acronis 快速協助 的遠端協助連線
- 使用 IP 位址的遠端桌面或遠端協助連線
- 透過使用 快速協助 在您的工作負載與遠端工作負載之間傳輸檔案

注意事項

使用 快速協助 從遠端連線到未受管理的工作負載時，請確認：

- 已為您的客戶租用戶啟用 Advanced Management 套件。
- 快速協助 應用程式正在您要連線的遠端工作負載上執行。

透過 Acronis 快速協助 連線至未受管理的工作負載

您可以使用 [快速協助] 功能，依需要遠端連線至未受管理的工作負載及提供一次性協助。

必要條件

- Advanced Management 套件已指派到您的客戶租用戶。
- 2FA 已在 Acronis Cyber Protect Cloud 中為您的使用者帳戶啟用。
- 遠端使用者已從 快速協助 提供工作負載 ID 和存取代碼。
- 遠端使用者已下載並執行 Acronis 快速協助。

若要使用 快速協助 連線至遠端協助的工作負載

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 按一下 **[快速協助]**。
3. 在 **[快速協助]** 視窗中，輸入終端使用者提供給您的工作負載 ID，然後選擇 **[連線]**。
4. 按一下 **[連線]**。

5. 根據您的工作負載上是否已安裝 Connect 用戶端 而定，執行下列其中一項操作：
   - 如果未安裝 Connect 用戶端，請先下載、安裝，然後在出現的確認快顯視窗中，選擇 **[允許]**。
   - 如果已安裝 Connect 用戶端，請在出現的確認快顯視窗中，選擇 **[開啟 Connect 用戶端]**。
6. 在 **[驗證]** 視窗中，輸入存取代碼。
7. Connect 用戶端 將會開啟一個新的檢視器視窗，您將可在其中看到遠端工作負載的桌面。檢視器有一個工具列，其中包含您可在建立遠端連線後對遠端工作負載執行的額外動作。如需詳細資訊，請參閱 "使用檢視器視窗中的工具列" (第 929 頁)。

透過 IP 位址連線至未受管理的工作負載

如果您的 LAN 中有未受管理的工作負載，可以使用其 IP 位址，針對遠端控制或遠端協助，連線至該工作負載。此連線不需要網際網路存取。

必要條件

- Advanced Management 套件已指派到您的客戶租用戶。
- 2FA 已在 Acronis Cyber Protect Cloud 中為您的使用者帳戶啟用。

若要使用其 IP 位址連線至遠端桌面或遠端協助的工作負載

1. 在 Cyber Protect 主控台，前往 **[所有裝置]**。
2. 按一下 **[快速協助]**。
3. 按一下 **[透過 IP 位址]** 索引標籤。
4. 輸入工作負載的 IP 位址和連接埠。
5. 選擇連線通訊協定 - RDP (Windows 工作負載) 或 [Apple 畫面共用] (macOS 工作負載)，端視遠端工作負載的作業系統而定。

   注意事項
   透過 RDP 連線支援遠端桌面動作，而透過 [Apple 畫面共用] 連線則同時支援遠端桌面和遠端協助動作。

6. 按一下 **[連線]**。
7. 在 **[驗證]** 視窗中，提供所需的認證。

若是 [Apple 畫面共用] 連線，Connect 用戶端 將會開啟一個新的檢視器視窗，您將可以在其中看到遠端工作負載的桌面。檢視器有一個工具列，其中包含您可在建立遠端連線後對遠端工作負載執行的額外動作。如需詳細資訊，請參閱 "使用檢視器視窗中的工具列" (第 929 頁)。

透過 Acronis 快速協助 傳輸檔案

您可以使用 [快速協助] 功能，在您的工作負載與未受管理的工作負載之間傳輸檔案。

必要條件

- Advanced Management 套件已指派到您的客戶租用戶。
- 2FA 已在 Acronis Cyber Protect Cloud 中為您的使用者帳戶啟用。

- 遠端使用者已下載並執行 Acronis 快速協助。
- 遠端使用者已從 快速協助 提供電腦 ID 和存取代碼。

若要使用 快速協助 將檔案傳輸到工作負載

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 按一下 **[快速協助]**。
3. 在 **[快速協助]** 視窗中，輸入終端使用者提供給您的工作負載 ID，然後選擇 **[檔案傳輸]**。
4. 按一下 **[連線]**。
5. 根據您的工作負載上是否已安裝 Connect 用戶端 而定，執行下列其中一項操作：
   - 如果未安裝 Connect 用戶端，請先下載、安裝，然後在出現的確認快顯視窗中，選擇 **[允許]**。
   - 如果已安裝 Connect 用戶端，請在出現的確認快顯視窗中，選擇 **[開啟 Connect 用戶端]**。
6. 在 **[驗證]** 視窗中，輸入存取代碼。
7. 在 **[檔案傳輸]** 視窗中，瀏覽檔案，並將它們拖放到所需的目的地。

   注意事項
   本機工作負載的檔案會列在左窗格中，而遠端工作負載的檔案則列在右窗格中。
   當檔案傳輸開始時，會列在 **[工作]** 窗格中。

8. [選用] 如果要從 **[工作]** 窗格中移除已完成的工作，請按一下 **[清除已完成]**。
9. 當所有傳輸完成時，關閉視窗。

使用檢視器視窗中的工具列

連線到遠端工作負載之後，您可以使用檢視器視窗中的工具列快速執行不同動作。

圖示	描述
	**實際大小** 縮放遠端工作負載的桌面，使遠端桌面的一個像素對應於檢視器視窗上的一個像素。
	**縮放至適當比例** 縮放遠端工作負載桌面，以符合檢視器視窗。
	**鎖定**和**解除鎖定螢幕** 在遠端工作負載顯示器上顯示預留位置，如此一來，遠端使用者將不會看到您的動作。
	**擷取螢幕擷取畫面** 將遠端伺服器的桌面影像儲存到本機檔案。
	**選擇顯示器** 選擇您要檢是的遠端工作負載顯示器和所需的解析度。

圖示	描述
	適用於與 macOS 的 [Apple 畫面共用] 連線，以及與任何作業系統的 NEAR 連線。 如果遠端電腦有多台顯示器，您可以為多台顯示器選擇下列顯示模式： • **合併** - 所有遠端顯示器都會顯示在單一視窗中。 • **分割** - 每台遠端顯示器都會顯示在不同的視窗中。 如果您有多台顯示器連線至本機工作負載，則此模式非常方便。例如，在此情況下，您可以安排在每台本機顯示器上查看一台遠端顯示器。 如果您關閉任何遠端工作負載顯示器，則遠端連線將結束。若要檢視遠端工作負載顯示器，則必須再次重新連線。 僅適用於 NEAR 連線
	**影像品質** 在 [Apple 畫面共用] 連線上，將遠端畫面影像品質從黑白調整至最高。
	**NEAR 影像品質** 調整 NEAR 連線上的品質/效能比。滑桿的左側 (平滑) 表示效能優先於影像品質，右側 (銳利) 表示遠端桌面螢幕的最佳品質，但效能可能更差。
	**傳送 Ctrl+Alt+Del** 傳送 Ctrl + Alt + Delete 序列到遠端工作負載。 適用於 Windows 和 Linux 工作負載。
	**檔案傳輸** 開啟 [檔案管理員] 視窗，以在遠端和本機工作負載之間交換檔案。適用於 NEAR 連線。
	**釘選工具列** 關閉檢視器工具列的自動隱藏。 適用於 Windows 工作負載。
	**全螢幕** 切換到全螢幕模式，並縮放遠端工作負載以完全充滿本機螢幕。 適用於 Windows 工作負載。
	**關閉** 關閉 [檢視器] 視窗並結束遠端控制工作階段。 適用於 Windows 工作負載。

根據連線類型，當您按一下 **[其他]** 圖示時，可能會有其他可用選項。

選項	描述
開始錄製/停止錄製	錄製目前的遠端桌面工作階段。 工作階段錄製內容在本機工作負載上儲存為 .crec 檔案。您可以使用 Acronis Connect 用戶端 開啟 .crec 檔案。 適用於 NEAR 連線
剪貼簿自動同步	當您啟用此選項時，用戶端將會自動同步您的本機剪貼簿和遠端電腦的剪貼簿。 適用於 NEAR 連線
傳送剪貼簿	**[傳送剪貼簿]** 會將遠端工作負載的剪貼簿內容取代為本機剪貼簿的內容。 如果啟用 **[剪貼簿自動同步]**，則會停用此選項。 如需詳細資訊，請參閱 "在工作負載之間共用剪貼簿內容" (第 922 頁)。 適用於 NEAR 連線
取得剪貼簿	**[取得剪貼簿]** 會將遠端工作負載的剪貼簿內容傳送至本機工作負載的剪貼簿。 如果啟用 **[剪貼簿自動同步]**，則會停用此選項。 如需詳細資訊，請參閱 "在工作負載之間共用剪貼簿內容" (第 922 頁)。 適用於 NEAR 連線
智慧型鍵盤/原始按鍵/具備所有快速鍵的原始按鍵	變更目前連線的鍵盤輸入模式。 **智慧型鍵盤**- 用戶端可將本機輸入符號的 Unicode 代碼傳輸到遠端電腦 **原始按鍵**- 用戶端可使用您所按下之鍵盤按鈕的原始代碼。 **包含所有快速鍵的原始按鍵**- 用戶端可停用本機系統快速鍵，如此一來，這些快速鍵也會傳輸到遠端作業系統。
滑鼠暫留時的鍵盤焦點	啟用時，當您的本機滑鼠游標放在 [檢視器] 視窗上時，用戶端只擷取鍵盤輸入。 停用時，用戶端會在其視窗為作用中時擷取您的鍵盤。
顯示連線資訊/隱藏連線資訊	當選擇 **[顯示連線資訊]** 時，會有一個小型資訊面板出現在遠端桌面畫面上，顯示有關目前連線的最基本資訊。
遠端聲音	讓用戶端將聲音從遠端電腦重新導向到本機電腦。 適用於 NEAR 連線

選項	描述
喜好設定	設定 Connect 用戶端 的設定。如需詳細資訊，請參閱 "設定 Connect 用戶端 設定" (第 932 頁)。

錄製和播放遠端工作階段

您可以在 Acronis Connect 用戶端 中，透過 NEAR 錄製遠端工作階段。

若要錄製遠端工作階段

1. 在 Connect 用戶端 中的 [檢視器] 工具列上，按一下 **[其他]**，然後選擇 **[開始錄製]**。
2. 選擇記錄的名稱和位置。

   預設情況下，此檔案將以目前日期和時間命名，並位於目前使用者主目錄的 **Documents** 資料夾中。當錄製處於啟用狀態時，在 **[檢視器]** 工具列中，您將會在遠端畫面和錄製計時器的右上角看到一個閃爍的紅色圓圈。
3. 若要停止錄製，請按一下 **[其他]**，然後按一下 **[停止錄製]**。在 Mac 上，您也可以按一下工具列上的 **[停止]**。

   使用 Acronis Connect 用戶端 建立的所有 .crec 檔案預設將使用 Acronis Connect 用戶端 開啟。

若要播放錄製內容

1. 找出錄製檔案。
2. 開啟該檔案。

   Acronis Connect 用戶端 的錄製播放程式隨即開啟。請注意，您無法導覽錄製內容。若要尋找錄製內容中的某個時刻，請等到播放程式到達該時刻。
3. [選用] 若要調整播放速度，請使用播放控制區段中的 **<<** 和 **>>** 圖示。

   錄製內容會儲存為在連線期間往返遠端伺服器傳輸的一系列事件。這可確保以最小的檔案大小，獲得最佳的錄製品質。然而，這也意味著您無法導覽錄製內容。目前還無法將錄製內容轉換為影片格式。

設定 Connect 用戶端 設定

在您的工作負載上安裝 Connect 用戶端 之後，可以根據您的喜好來設定其設定。

若要設定 Connect 用戶端 的設定

1. 在 [開始] 功能表中，找到 **Connect 用戶端**，然後加以啟動。
2. 在 **[一般]** 索引標籤上進行設定。

選項	描述
寫入詳細記錄	選擇此選項可允許 Connect 用戶端 寫入詳細記錄。如果停用，用戶端將只能寫入一般資訊到記錄檔。
Proxy 設定	選擇是否使用預設的系統 Proxy，或者設定自訂 SOCKSS Proxy。

3. 在 **[檢視器]** 索引標籤上進行設定。

選項	描述
關閉檢視器時要求確認	如果希望 Connect 用戶端 在您嘗試關閉 [檢視器] 視窗時顯示確認訊息，以防止意外關閉，請選擇此選項。
最小化時	選擇當最小化時是否暫停 [檢視器] 活動，以便減少 CPU 負載。
最大化時	選擇當最大化時是否啟用全螢幕模式。
剪貼簿傳輸	啟用每當複製或貼上文字和影像時，在 [檢視器] 視窗中顯示剪貼簿傳輸指標。
鍵盤模式	啟用每當滑鼠和鍵盤事件傳送到遠端電腦時，在 [檢視器] 視窗標題中顯示輸入模式指標。
剪貼簿	選擇 **[自動同步剪貼簿]** 可啟用自動剪貼簿同步 (如果可用)。
傳送鍵盤事件	選擇是在 Connect 用戶端 視窗處於作用中狀態時擷取本機鍵盤輸入，還是僅在本機滑鼠指標停在其上時擷取本機鍵盤輸入。
檢視器背景顏色	變更 [檢視器] 視窗背景顏色。
自動重新連線	如果您希望 在中斷時自動重新建立連線，請選擇 **[啟用以自動重新連線]**。
H.264	您可以停用硬體解碼器。
閒置時關閉	選擇關閉 [檢視器] 視窗之前的閒置時間間隔。

4. 在 **[鍵盤]** 索引標籤上進行設定。

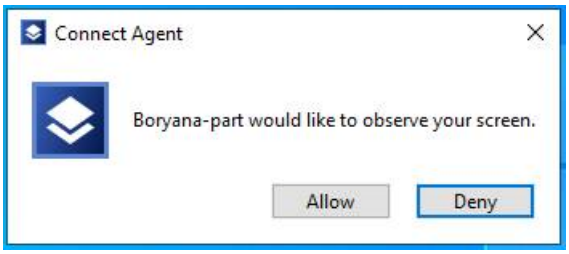
選項	描述
輔助按鍵對應	使用快顯功能表變更輔助按鍵的行為。這些設定會針對 NEAR、Apple 畫面共用和 RDP 連線分別儲存。
輸入模式	針對每種類型的連線 (在窗格標頭中選擇)，選擇預設的鍵盤輸入模式。

5. 按一下 **[確定]**。

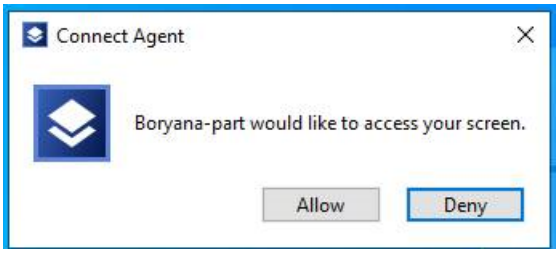
遠端桌面通知程式

下列情況下，Connect 代理程式 會在遠端工作負載的桌面上顯示動作對話方塊 (通知程式)：

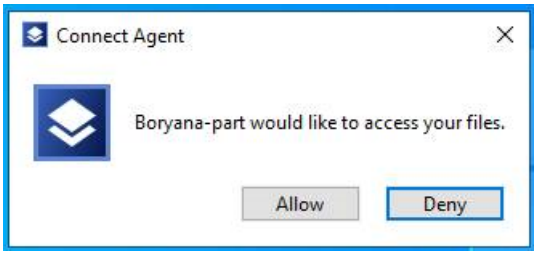
- 當您嘗試透過要求觀察權限，以遠端方式連線到工作負載時。以本機方式登入遠端工作負載的使用者可允許或拒絕要求。



- 當您嘗試透過要求控制權限，以遠端方式連線到工作負載時。以本機方式登入遠端工作負載的使用者可允許或拒絕要求。



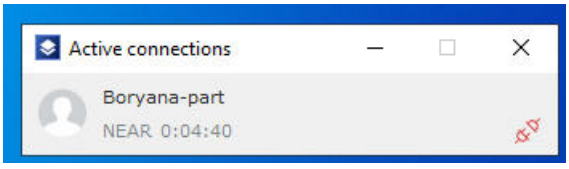
- 當您嘗試透過要求傳輸檔案權限，在您的工作負載與遠端工作負載之間交換檔案時。以本機方式登入遠端工作負載的使用者可允許或拒絕要求。



當您建立與工作負載的遠端桌面連線時，已登入該工作負載的使用者將會看到一個不同的連線通知程式，其中包含下列資訊：

- 遠端連線的使用者名稱
- 用於建立遠端連線的連線通訊協定
- 遠端連線的持續時間

以本機方式登入遠端工作負載的使用者，隨時可透過按下 **[中斷連線]** 圖示或 **[關閉]** 圖示來結束連線。



監控工作負載的健全狀況和效能

您可以監控系統參數以及組織中工作負載的健全狀況。如果參數不正常，您將立即收到通知並能夠快速解決問題。您也可以設定自訂警示和自動回應動作。這些動作將會自動執行，以解決工作負載行為中的異常。

注意事項
若要使用監控功能，需要在工作負載上安裝 保護 代理程式 15.0.35324 版或更新版本。

監控計劃

為開始監控受管理工作負載的效能、硬體、軟體、系統和安全性參數，請在其中套用監控計劃。監控計劃是由您可以啟用並設定的不同監視器所組成。部分監視器支援基於異常的監控類型。如需有關監控計劃的詳細資訊，請參閱 "監控計劃" (第 961 頁)。如需有關您可以在監控計劃中設定之可用監視器的詳細資訊，請參閱 "可設定的監視器" (第 936 頁)。

如果代理程式基於某種原因而無法從工作負載收集資料，系統將會產生警示。

監控類型

您必須為您在計劃中啟用的每個監視器設定監控類型。監控類型可決定監視器評估工作負載之正常行為和偏差所使用的演算法。有兩種監控類型：基於閥值和基於異常。部分監視器僅支援基於閥值的監控類型。

基於閥值的監控類型會追蹤參數的值高於還是低於您所設定的閥值。使用此監控類型時，您負責為工作負載定義正確的閥值。系統會根據這些靜態閥值確定正常行為，而不需考慮可能導致該行為的其他特定條件。因此，相較於基於異常的監控，基於閥值的監控可能比較不準確。

基於異常的監控使用機器學習來建立工作負載的正常行為模式，並偵測異常行為。如需詳細資訊，請參閱 "基於異常的監控" (第 935 頁)。

基於異常的監控

基於異常的監控使用機器學習模型來建立工作負載的正常行為模式，並偵測工作負載行為中的異常行為 (時間序列資料非預期地激增)。當您啟用此監控類型時，系統會建立一個模型並開始自我訓練，進而根據收集自工作負載的資料，調整特定工作負載的模型。也就是說，在訓練期開始時，資料可能不完全準確。建立可靠的模型需要至少三週的模型訓練。隨著系統收集更多資料並分析歷史資料集，它會使模型逐漸完善，並為每個工作負載指標建立動態的閾值上限和下限。相較於基於閾值的監控，此監控類型更彈性，因為系統會監控參數及其內容的值。例如，對於特定的工作負載來說，一天中的某些時間負載較大可能是正常的。基於閾值的監控類型會將此錯誤地解釋為異常行為並觸發警示。

您可以重設工作負載的機器學習模型。在此情況下，系統將會針對套用到工作負載的監視器，刪除其所有資料和模型。如需詳細資訊，請參閱 "重設機器學習模型" (第 970 頁)。

支援監控的平台

下列作業系統支援監控功能。

支援的 Windows 版本	支援的 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)

可設定的監視器

監控功能支援下列監視器，其分成六個類別：硬體、效能、軟體、系統、安全性和自訂。

監視器	描述	支援的作業系統	資料收集頻率	支援基於異常的監控	可用於標準保護或 Advanced Management
硬體					
磁碟空間	監控工作負載的特定磁碟機上的可用空間。	Windows macOS	1 分鐘	是	標準保護
CPU 溫度	監控 CPU 溫度。	Windows macOS	30 秒	是	Advanced Management
GPU 溫度	監控 GPU 溫度。	Windows macOS	30 秒	是	Advanced Management
硬體變更	監控硬體變更，例如在工作負載上新增、移除或更換硬體	Windows macOS	24 小時	否	標準保護
效能					
CPU 使用量	監控整體 CPU 使用量 (依工作負載上的所有 CPU)。	Windows macOS	30 秒	是	Advanced Management
記憶體使用	監控整體記憶體使用量 (依工	Windows	30	是	Advanced

監視器	描述	支援的作業系統	資料收集頻率	支援基於異常的監控	可用於標準保護或 Advanced Management
量	作負載上的所有記憶體插槽)。	macOS	秒		Management
磁碟傳輸速率	監控工作負載上每個實體磁碟的讀寫速度。	Windows macOS	30 秒	是	Advanced Management
網路使用量	針對工作負載的每個網路介面卡，監控傳入與傳出流量。	Windows macOS	30 秒	是	Advanced Management
CPU 使用量 (依程序)	依特定程序監控 CPU 使用量。	Windows macOS	30 秒	否	Advanced Management
記憶體使用量 (依程序)	依所選程序監控記憶體使用量。	Windows macOS	30 秒	否	Advanced Management
磁碟傳輸速率 (依程序)	監控所選程序的讀寫速度。	Windows macOS	30 秒	否	Advanced Management
網路使用量 (依程序)	監控所選程序的傳入與傳出流量。	Windows macOS	30 秒	否	Advanced Management
軟體					
Windows 服務狀態	監控所選 Windows 服務的狀態 (執行中或已停止)。	Windows	30 秒	否	Advanced Management
程序狀態	監控所選程序的狀態 (執行中或已停止)。	Windows macOS	30 秒	否	Advanced Management
已安裝的軟體	監控軟體應用程式的安裝、更新或刪除。	Windows macOS	24 小時	否	Advanced Management
系統					
上次系統重新啟動	監控工作負載何時重新啟動。	Windows macOS	1 小時	否	標準保護
Windows 事件日誌	監控 Windows 事件記錄中的特定重要業務事件。	Windows	10 分鐘	否	Advanced Management
檔案和資料夾大小	監控所選檔案或資料夾的大小總計。	Windows macOS	10 分鐘	否	標準保護

監視器	描述	支援的作業系統	資料收集頻率	支援基於異常的監控	可用於標準保護或 Advanced Management
安全性					
Windows Update 狀態	監控工作負載的 Windows Update 狀態，以及是否已安裝最新更新。	Windows	15 分鐘	否	Advanced Management
防火牆狀態	監控工作負載上已安裝的內建或第三方防火牆狀態。	Windows macOS	5 分鐘	否	Advanced Management
防惡意軟體狀態	監控工作負載上已安裝的內建或第三方防惡意軟體狀態。	Windows macOS	5 分鐘	否	Advanced Management
失敗的登入	監控工作負載上未成功的登入嘗試。	Windows	1 小時	否	Advanced Management
自動執行狀態	監控卸除式儲存媒體的自動執行功能是否已啟用。	Windows	1 小時	否	Advanced Management
自訂					
自訂	透過執行中的指令碼監控自訂物件。	Windows macOS	自訂	否	Advanced Management

磁碟空間監視器的設定

磁碟空間會監控工作負載的特定磁碟機上的可用空間。

注意事項

計算空間時，監視器會針對 Windows 和 macOS 工作負載，使用二進位位元組 (1024 位元組/KB、1024 KB/MB 和 1024 MB/GB)。

您可以設定下列監視器設定。

設定	描述
基於閾值的監控	
磁碟機	您要監控的磁碟機。 下列值可供使用。 • **系統磁碟機** —這是預設值。 • **任何磁碟機**
運算子	運算子是一種條件式函式，可定義如何衡量指標的效能。

設定	描述
	下列值可供使用。 • **小於** —這是預設值。 • **小於或等於**
磁碟可用空間閾值	閾值和**運算子**值可決定所監控指標的正常效能。當所監控指標的值超出正常範圍時，系統會產生警示。 輸入 1-100 (%) 範圍內的整數值。預設值為 20。
包含卸除式磁碟機	如果 **[磁碟機]** 值為 **[任何磁碟機]**，則可以使用此設定。 如果您要新增卸除式磁碟機 (如 USB 快閃磁碟機) 進行監控，請選擇此設定。此設定預設為停用狀態。
時間期限	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 30。
基於異常的監控	
磁碟機	您要監控的磁碟機。 下列值可供使用。 • **系統磁碟機** —這是預設值。 • **任何磁碟機**
模型訓練期間	系統將根據從代理程式收集的資料，訓練機器學習模型，然後建立工作負載正常行為模式的期間。模型訓練期間越長，系統將建立的長期行為模式越精確。建議模型訓練期間下限為 21 天。 輸入一個整數值 (天數)。預設值為 21。
訓練期間接收異常警示	如果您選擇此設定，您將會在模型訓練期間，收到關於異常的警示。這些警示可能是錯誤的，因為模型仍在訓練中，因此可能不夠準確。 此設定預設為選取狀態。
敏感度層級	如果異常的值在特定範圍內，則敏感度層級會充當異常的初步篩選條件。此篩選條件會與異常偵測演算法分開運作。其目的在於阻止異常偵測演算法處理指定範圍內的異常。 在訓練期間： 1. 使用在訓練期間收集到的資料，訓練演算法。 2. 演算法對訓練資料執行異常偵測。 3. 根據平均值和標準差，套用篩選程序。 4. 篩選指定期間內的任何異常。 5. 從剩餘的異常資料點中，選擇異常層級最低的異常。在模型中記錄這個層級 (介於 0 到 1 之間的浮點數)。

設定	描述
	在期間預測： 1. 演算法預測推斷資料的異常。 2. 根據敏感度層級，依平均值和標準差篩選預測的異常。 3. 其餘的異常則根據以下原則進一步篩選：高於閾值層級的值會被視為異常，而低於閾值層級的值則會被視為正常行為。 下列值可供使用。 • **低** — 低層級要等於平均值和標準差值。 • **正常** — 這是預設值。正常層級要等於平均值以及兩倍的標準差值。 • **高** — 高層級要等於平均值以及三倍的標準差值。
異常持續時間	只有在指定的期間內持續存在異常行為時，系統才會針對偵測到的異常產生警示。 預設值為 30 分鐘。

CPU 溫度監視器的設定

CPU 溫度會監控工作負載的 CPU 溫度。

您可以設定下列監視器設定。

設定	描述
基於閾值的監控	
CPU 溫度已超過 (C°)	所監控指標的最大值。如果超出此值，則系統會產生警示。 輸入一個整數值 (C°)。預設值為 80。
時間期限	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 5。
基於異常的監控	
模型訓練期間	系統將根據從代理程式收集的資料，訓練機器學習模型，然後建立工作負載正常行為模式的期間。模型訓練期間越長，系統將建立的長期行為模式越精確。建議模型訓練期間下限為 21 天。 輸入一個整數值 (天數)。預設值為 21。
敏感度層級	如果異常的值在特定範圍內，則敏感度層級會充當異常的初步篩選條件。此篩選條件會與異常偵測演算法分開運作。其目的在於阻止異常偵測演算法處理指定範圍內的異常。 在訓練期間： 1. 使用在訓練期間收集到的資料，訓練演算法。 2. 演算法對訓練資料執行異常偵測。

設定	描述
	3. 根據平均值和標準差，套用篩選程序。 4. 篩選指定期間內的任何異常。 5. 從剩餘的異常資料點中，選擇異常層級最低的異常。在模型中記錄這個層級 (介於 0 到 1 之間的浮點數)。 在期間預測： 1. 演算法預測推斷資料的異常。 2. 根據敏感度層級，依平均值和標準差篩選預測的異常。 3. 其餘的異常則根據以下原則進一步篩選：高於閾值層級的值會被視為異常，而低於閾值層級的值則會被視為正常行為。 下列值可供使用。 • **低** — 低層級要等於平均值和標準差值。 • **正常** — 這是預設值。正常層級要等於平均值以及兩倍的標準差值。 • **高** — 高層級要等於平均值以及三倍的標準差值。
異常持續時間	只有在指定的期間內持續存在異常行為時，系統才會針對偵測到的異常產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 15。

GPU 溫度監視器的設定

GPU 溫度會監控工作負載的 GPU 溫度。

您可以設定下列監視器設定。

設定	描述
基於閾值的監控	
GPU 溫度已超過	所監控指標的最大值。如果超出此值，則系統會偵測到異常。 輸入一個整數值 (C°)。預設值為 80。
時間期限	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 5。
基於異常的監控	
模型訓練期間	系統將根據從代理程式收集的資料，訓練機器學習模型，然後建立工作負載正常行為模式的期間。模型訓練期間越長，系統將建立的長期行為模式越精確。建議模型訓練期間下限為 21 天。 輸入一個整數值 (天數)。預設值為 21。

設定	描述
敏感度層級	如果異常的值在特定範圍內，則敏感度層級會充當異常的初步篩選條件。此篩選條件會與異常偵測演算法分開運作。其目的在於阻止異常偵測演算法處理指定範圍內的異常。 在訓練期間： 1. 使用在訓練期間收集到的資料，訓練演算法。 2. 演算法對訓練資料執行異常偵測。 3. 根據平均值和標準差，套用篩選程序。 4. 篩選指定期間內的任何異常。 5. 從剩餘的異常資料點中，選擇異常層級最低的異常。在模型中記錄這個層級 (介於 0 到 1 之間的浮點數)。 在期間預測： 1. 演算法預測推斷資料的異常。 2. 根據敏感度層級，依平均值和標準差篩選預測的異常。 3. 其餘的異常則根據以下原則進一步篩選：高於閾值層級的值會被視為異常，而低於閾值層級的值則會被視為正常行為。 下列值可供使用。 • **低** — 低層級要等於平均值和標準差值。 • **正常** — 這是預設值。正常層級要等於平均值以及兩倍的標準差值。 • **高** — 高層級要等於平均值以及三倍的標準差值。
異常持續時間	只有在指定的期間內持續存在異常行為時，系統才會針對偵測到的異常產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 15。

硬體變更監視器的設定

硬體變更會監控硬體變更，例如在工作負載上新增、移除或更換硬體。

您可以設定下列監視器設定。

設定	描述
硬體元件	請選擇您要監控是否變更的一或多個硬體元件。 下列值可供使用。 • **全部** — 這是預設值。 • **主機板** • **CPU** • **RAM** • **磁碟** • **GPU** • **網路介面卡**

設定	描述
要監控的內容	指定您要監控所選硬體元件的變更。您可以從清單中選擇多個項目。 下列值可供使用。 • **任何變更** —這是預設值。 • **已新增的元件** • **已更換的元件** • **已移除的元件**

CPU 使用量監視器的設定

CPU 使用量會監控工作負載的 CPU 總使用量 (處理器使用量)。如果工作負載有多個 CPU, CPU 總使用量將是每個 CPU 的 CPU 使用量加總。

您可以設定下列監視器設定。

設定	描述
基於閾值的監控	
運算子	運算子是一種條件式函式, 可定義如何衡量指標的效能。 下列值可供使用。 • **大於** —這是預設值。 • **大於或等於** • **小於** • **小於或等於**
CPU 使用量閾值	閾值和**運算子**值可決定所監控指標的正常效能。當所監控指標的值超出正常範圍時, 系統會產生警示。 輸入 1-100 (%) 範圍內的整數值。預設值為 90。
時間期限	只有在指定的期間內指標值超出正常範圍時, 系統才會針對偵測到的問題產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 5。
基於異常的監控	
模型訓練期間	系統將根據從代理程式收集的資料, 訓練機器學習模型, 然後建立工作負載正常行為模式的期間。模型訓練期間越長, 系統將建立的長期行為模式越精確。建議模型訓練期間下限為 21 天。 輸入一個整數值 (天數)。預設值為 21。
訓練期間接收異常警示	如果您選擇此設定, 您將會在模型訓練期間, 收到關於異常的警示。這些警示可能是錯誤的, 因為模型仍在訓練中, 因此可能不夠準確。 此設定預設為選取狀態。

設定	描述
敏感度層級	如果異常的值在特定範圍內，則敏感度層級會充當異常的初步篩選條件。此篩選條件會與異常偵測演算法分開運作。其目的在於阻止異常偵測演算法處理指定範圍內的異常。 在訓練期間： 1. 使用在訓練期間收集到的資料，訓練演算法。 2. 演算法對訓練資料執行異常偵測。 3. 根據平均值和標準差，套用篩選程序。 4. 篩選指定期間內的任何異常。 5. 從剩餘的異常資料點中，選擇異常層級最低的異常。在模型中記錄這個層級 (介於 0 到 1 之間的浮點數)。 在期間預測： 1. 演算法預測推斷資料的異常。 2. 根據敏感度層級，依平均值和標準差篩選預測的異常。 3. 其餘的異常則根據以下原則進一步篩選：高於閾值層級的值會被視為異常，而低於閾值層級的值則會被視為正常行為。 下列值可供使用。 • **低** — 低層級要等於平均值和標準差值。 • **正常** — 這是預設值。正常層級要等於平均值以及兩倍的標準差值。 • **高** — 高層級要等於平均值以及三倍的標準差值。
異常持續時間	只有在指定的期間內持續存在異常行為時，系統才會針對偵測到的異常產生警示。輸入 1-60 (分鐘) 範圍內的整數值。預設值為 15。

記憶體使用量監視器的設定

記憶體使用量會監控整體記憶體使用量 (依工作負載的所有記憶體模組)

您可以設定下列監視器設定。

設定	描述
基於閾值的監控	
運算子	運算子是一種條件式函式，可定義如何衡量指標的效能。 下列值可供使用。 • **大於** —這是預設值。 • **大於或等於** • **小於** • **小於或等於**
記憶體使用量	閾值和**運算子**值可決定所監控指標的正常效能。當所監控指標的值超出正常範圍時，系統會產生警示。

設定	描述
閾值	輸入 1-100 (%) 範圍內的整數值。預設值為 90。
時間期限	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 5。
基於異常的監控	
模型訓練期間	系統將根據從代理程式收集的資料，訓練機器學習模型，然後建立工作負載正常行為模式的期間。模型訓練期間越長，系統將建立的長期行為模式越精確。建議模型訓練期間下限為 21 天。 輸入一個整數值 (天數)。預設值為 21。
訓練期間接收異常警示	如果您選擇此設定，您將會在模型訓練期間，收到關於異常的警示。這些警示可能是錯誤的，因為模型仍在訓練中，因此可能不夠準確。 此設定預設為選取狀態。
敏感度層級	如果異常的值在特定範圍內，則敏感度層級會充當異常的初步篩選條件。此篩選條件會與異常偵測演算法分開運作。其目的在於阻止異常偵測演算法處理指定範圍內的異常。 在訓練期間： 1. 使用在訓練期間收集到的資料，訓練演算法。 2. 演算法對訓練資料執行異常偵測。 3. 根據平均值和標準差，套用篩選程序。 4. 篩選指定期間內的任何異常。 5. 從剩餘的異常資料點中，選擇異常層級最低的異常。在模型中記錄這個層級 (介於 0 到 1 之間的浮點數)。 在期間預測： 1. 演算法預測推斷資料的異常。 2. 根據敏感度層級，依平均值和標準差篩選預測的異常。 3. 其餘的異常則根據以下原則進一步篩選：高於閾值層級的值會被視為異常，而低於閾值層級的值則會被視為正常行為。 下列值可供使用。 • **低** — 低層級要等於平均值和標準差值。 • **正常** — 這是預設值。正常層級要等於平均值以及兩倍的標準差值。 • **高** — 高層級要等於平均值以及三倍的標準差值。
異常持續時間	只有在指定的期間內持續存在異常行為時，系統才會針對偵測到的異常產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 30 分鐘。

磁碟傳輸速率監視器的設定

磁碟傳輸速率會監控工作負載上每個實體磁碟的讀寫速度。

您可以設定下列監視器設定。

設定	描述
基於閾值的監控	
要監控的內容	選擇您要監控的速度。 下列值可供使用。 • **讀取速度和寫入速度**。這是預設值。 • **讀取速度** • **寫入速度**
讀取速度運算子	運算子是一種條件式函式，可定義如何衡量指標的效能。 下列值可供使用。 • **大於**。這是預設值。 • **大於或等於** • **小於** • **小於或等於**
讀取速度閾值	閾值和**運算子**值可決定所監控指標的正常效能。當所監控指標的值超出正常範圍時，系統會產生警示。 輸入一個整數值 (kb/秒)。預設值為 0 kb/秒。
讀取速度時間期限	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 5。
寫入速度運算子	運算子是一種條件式函式，可定義如何衡量指標的效能。 下列值可供使用。 • **大於** —這是預設值。 • **大於或等於** • **小於** • **小於或等於**
寫入速度閾值	閾值和**運算子**值可決定所監控指標的正常效能。當所監控指標的值超出正常範圍時，系統會產生警示。 輸入一個整數值 (kb/秒)。預設值為 0 kb/秒。
寫入速度時間期限	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。

設定	描述
	輸入 1-60 (分鐘) 範圍內的整數值。預設值為 5。
基於異常的監控	
模型訓練期間	系統將根據從代理程式收集的資料，訓練機器學習模型，然後建立工作負載正常行為模式的期間。模型訓練期間越長，系統將建立的長期行為模式越精確。建議模型訓練期間下限為 21 天。 輸入一個整數值 (天數)。預設值為 21。
訓練期間接收異常警示	如果您選擇此設定，您將會在模型訓練期間，收到關於異常的警示。這些警示可能是錯誤的，因為模型仍在訓練中，因此可能不夠準確。 此設定預設為選取狀態。
要監控的內容	選擇您要監控的速度。 下列值可供使用。 • **讀取速度和寫入速度**。這是預設值。 • **讀取速度** • **寫入速度**
敏感度層級	如果異常的值在特定範圍內，則敏感度層級會充當異常的初步篩選條件。此篩選條件會與異常偵測演算法分開運作。其目的在於阻止異常偵測演算法處理指定範圍內的異常。 在訓練期間： 1. 使用在訓練期間收集到的資料，訓練演算法。 2. 演算法對訓練資料執行異常偵測。 3. 根據平均值和標準差，套用篩選程序。 4. 篩選指定期間內的任何異常。 5. 從剩餘的異常資料點中，選擇異常層級最低的異常。在模型中記錄這個層級 (介於 0 到 1 之間的浮點數)。 在期間預測： 1. 演算法預測推斷資料的異常。 2. 根據敏感度層級，依平均值和標準差篩選預測的異常。 3. 其餘的異常則根據以下原則進一步篩選：高於閾值層級的值會被視為異常，而低於閾值層級的值則會被視為正常行為。 下列值可供使用。 • **低** — 低層級要等於平均值和標準差值。 • **正常** — 這是預設值。正常層級要等於平均值以及兩倍的標準差值。 • **高** — 高層級要等於平均值以及三倍的標準差值。
異常持續時間 (讀取速度)	只有在指定的期間內持續存在異常行為時，系統才會針對偵測到的異常產生警示。

設定	描述
	輸入 1-60 (分鐘) 範圍內的整數值。 預設值為 25。
異常持續時間 (寫入速度)	只有在指定的期間內持續存在異常行為時，系統才會針對偵測到的異常產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。 預設值為 25。

網路使用量監視器的設定

網路使用量會針對工作負載的每個網路介面卡，監控傳入與傳出流量。

您可以設定下列監視器設定。

設定	描述
基於閾值的監控	
流量方向	您要監控的流量方向。 下列值可供使用。 • **傳入流量和傳出流量**。這是預設值。 • **傳入流量** • **傳出流量**
傳入流量運算子	運算子是一種條件式函式，可定義如何衡量指標的效能。 下列值可供使用。 • **大於** —這是預設值。 • **大於或等於** • **小於** • **小於或等於**
傳入流量閾值	閾值和**運算子**值可決定所監控指標的正常效能。當所監控指標的值超出正常範圍時，系統會產生警示。 輸入一個整數值 (kb/秒)。預設值為 0 kb/秒。
傳入流量時間期限	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 5。
傳出流量運算子	運算子是一種條件式函式，可定義如何衡量指標的效能。 下列值可供使用。 • **大於** —這是預設值。

設定	描述
	• **大於或等於** • **小於** • **小於或等於**
傳出流量閥值	閾值和**運算子**值可決定所監控指標的正常效能。當所監控指標的值超出正常範圍時，系統會產生警示。 輸入一個整數值 (kb/秒)。預設值為 0 kb/秒。
傳出流量時間期限	閾值和**運算子**值可決定所監控指標的正常效能。當所監控指標的值超出正常範圍時，系統會產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 5。
基於異常的監控	
模型訓練期間	系統將根據從代理程式收集的資料，訓練機器學習模型，然後建立工作負載正常行為模式的期間。模型訓練期間越長，系統將建立的長期行為模式越精確。建議模型訓練期間下限為 21 天。 輸入一個整數值 (天數)。預設值為 21。
訓練期間接收異常警示	如果您選擇此設定，您將會在模型訓練期間，收到關於異常的警示。這些警示可能是錯誤的，因為模型仍在訓練中，因此可能不夠準確。 此設定預設為選取狀態。
流量方向	• **傳入流量和傳出流量**。這是預設值。 • **傳入流量** • **傳出流量**
敏感度層級	如果異常的值在特定範圍內，則敏感度層級會充當異常的初步篩選條件。此篩選條件會與異常偵測演算法分開運作。其目的在於阻止異常偵測演算法處理指定範圍內的異常。 在訓練期間： 1. 使用在訓練期間收集到的資料，訓練演算法。 2. 演算法對訓練資料執行異常偵測。 3. 根據平均值和標準差，套用篩選程序。 4. 篩選指定期間內的任何異常。 5. 從剩餘的異常資料點中，選擇異常層級最低的異常。在模型中記錄這個層級 (介於 0 到 1 之間的浮點數)。 在期間預測： 1. 演算法預測推斷資料的異常。 2. 根據敏感度層級，依平均值和標準差篩選預測的異常。 3. 其餘的異常則根據以下原則進一步篩選：高於閾值層級的值會被視為異常，而低於閾值層級的值則會被視為正常行為。

設定	描述
	下列值可供使用。 • **低** — 低層級要等於平均值和標準差值。 • **正常** — 這是預設值。正常層級要等於平均值以及兩倍的標準差值。 • **高** — 高層級要等於平均值以及三倍的標準差值。
異常持續時間 (傳入)	只有在指定的期間內持續存在異常行為時，系統才會針對偵測到的異常產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。 預設值為 25。
異常持續時間 (傳出)	只有在指定的期間內持續存在異常行為時，系統才會針對偵測到的異常產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。 預設值為 25。

CPU 使用量 (依程序) 監視器的設定

CPU 使用量 (依程序) 會監控所選程序的 CPU 使用量。如果相同的程序有多個執行個體，系統將會監控所有程序執行個體的總使用量，而且會在符合條件時產生警示。

您可以設定下列監視器設定。

設定	描述
程序名稱	您要監控之程序的名稱。輸入程序名稱 (不含副檔名)。
運算子	運算子是一種條件式函式，可定義如何衡量指標的效能。 下列值可供使用。 • **大於** —這是預設值。 • **大於或等於** • **小於** • **小於或等於**
閾值	閾值和**運算子**值可決定所監控指標的正常效能。當所監控指標的值超出正常範圍時，系統會產生警示。 輸入 1-100 (%) 範圍內的整數值。預設值為 90。
時間期限	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 5。

記憶體使用量 (依程序) 監視器的設定

記憶體使用量 (依程序) 會監控所選程序的記憶體使用量。如果相同的程序有多個執行個體，系統將會監控所有程序執行個體的總使用量，而且會在符合條件時產生警示。

注意事項
代理程式會使用整個程序工作集 (私人和共用)，依程序評估記憶體使用量的大小。這就是為什麼桌面小工具顯示的大小可能與 Windows 工作管理員 (私人工作集) 中顯示的記憶體使用量大小不同的原因。

您可以設定下列監視器設定。

設定	描述
程序名稱	您要監控之程序的名稱。輸入程序名稱 (不含副檔名)。
運算子	運算子是一種條件式函式，可定義如何衡量指標的效能。 下列值可供使用。 • **大於** —這是預設值。 • **大於或等於** • **小於** • **小於或等於**
閾值	閾值和**運算子**值可決定所監控指標的正常效能。當所監控指標的值超出正常範圍時，系統會產生警示。 輸入一個整數值 (kb)。預設值為 1。
時間期限	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 5。

磁碟傳輸速率 (依程序) 監視器的設定

磁碟傳輸速率 (依程序) 會監控所選程序的讀寫速度。如果相同的程序有多個執行個體，系統將會監控所有程序執行個體的總使用量，而且會在符合條件時產生警示。

您可以設定下列監視器設定。

設定	描述
程序名稱	您要監控之程序的名稱。輸入程序名稱 (不含副檔名)。
要監控的內容	您要監控的速度。 下列值可供使用。

設定	描述
	• **讀取速度和寫入速度**。這是預設值。 • **讀取速度** • **寫入速度**
讀取速度運算子	運算子是一種條件式函式，可定義如何衡量指標的效能。 下列值可供使用。 • **大於** —這是預設值。 • **大於或等於** • **小於** • **小於或等於**
讀取速度閥值	閾值和**運算子**值可決定所監控指標的正常效能。當所監控指標的值超出正常範圍時，系統會產生警示。 輸入一個整數值 (kb/秒)。預設值為 0 kb/秒。
讀取速度時間期限	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 5。
寫入速度運算子	運算子是一種條件式函式，可定義如何衡量指標的效能。 下列值可供使用。 • **大於** —這是預設值。 • **大於或等於** • **小於** • **小於或等於**
寫入速度閥值	閾值和**運算子**值可決定所監控指標的正常效能。當所監控指標的值超出正常範圍時，系統會產生警示。 輸入一個整數值 (kb/秒)。預設值為 0 kb/秒。
寫入速度時間期限	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 5。

網路使用量 (依程序) 監視器的設定

網路使用量 (依程序) 會監控所選程序的傳入與傳出流量。如果相同的程序有多個執行個體，系統將會監控所有程序執行個體的總使用量，而且會在符合所有執行個體的條件時產生警示。

您可以設定下列監視器設定。

設定	描述
程序名稱	您要監控之程序的名稱。輸入程序名稱 (不含副檔名)。
流量方向	您要監控的流量方向。 下列值可供使用。 • **傳入流量和傳出流量**。這是預設值。 • **傳入流量** • **傳出流量**
傳入流量運算子	運算子是一種條件式函式，可定義如何衡量指標的效能。 下列值可供使用。 • **大於** —這是預設值。 • **大於或等於** • **小於** • **小於或等於**
傳入流量閾值	閾值和**運算子**值可決定所監控指標的正常效能。當所監控指標的值超出正常範圍時，系統會產生警示。 輸入一個整數值 (kb/秒)。預設值為 0 kb/秒。
傳入流量時間期限	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 5。
傳出流量運算子	運算子是一種條件式函式，可定義如何衡量指標的效能。 下列值可供使用。 • **大於** —這是預設值。 • **大於或等於** • **小於** • **小於或等於**
傳出流量閾值	閾值和**運算子**值可決定所監控指標的正常效能。當所監控指標的值超出正常範圍時，系統會產生警示。 輸入一個整數值 (kb/秒)。預設值為 0 kb/秒。
傳出流量時間期限	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 5。

Windows 服務狀態監視器的設定

Windows 服務狀態會監控所選 Windows 服務執行中還是已停止。

您可以設定下列監視器設定。

設定	描述
服務名稱	您要監控之 Windows 服務的名稱。 您可以從 Windows 服務清單中選擇一個服務名稱。在工作負載上成功完成軟體清查掃描之後，租用戶的所有代理程式都會填入此清單。您也可以新增不在清單中的服務名稱。如果未在工作負載上執行軟體清查掃描，則這是唯一可用的選項。
服務狀態	如果服務處於所選狀態，系統將會產生事件。 下列值可供使用。 • **執行中** • **已停止**—這是預設值。
時間期限	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 1。

程序狀態監視器的設定

程序狀態會監控所選程序執行中還是已停止。如果相同的程序有多個執行個體，系統將會監控程序的每個執行個體，而且會在符合程序所有執行個體的條件時產生警示。

您可以設定下列監視器設定。

設定	描述
程序名稱	您要監控之程序的名稱。輸入可執行檔的名稱 (不含副檔名)。
程序狀態	如果程序處於所選狀態，系統將會產生事件。 下列值可供使用。 • **執行中** • **已停止**—這是預設值。
時間期限	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。 輸入 1-60 (分鐘) 範圍內的整數值。預設值為 1。

已安裝的軟體監視器的設定

已安裝的軟體會監控工作負載上軟體應用程式的安裝、更新或刪除。

您可以設定下列監視器設定。

設定	描述
要監控的軟體	指定您要監控的軟體。 下列值可供使用。 • **任何軟體** —這是預設值。 • **特定軟體**
軟體名稱	如果您針對 **[要監控的軟體]** 選擇 **[特定軟體]** 值，則此設定會變成可用。 請輸入一或多個軟體應用程式的名稱。 您可以從 Windows 服務清單中選擇一個軟體應用程式名稱。在工作負載上成功完成軟體清查掃描之後，租用戶的所有代理程式都會填入此清單。您也可以新增不在清單中的軟體應用程式名稱。如果未在工作負載上執行軟體清查掃描，則這是唯一可用的選項。
安裝狀態	指定您是要監控已安裝、未安裝還是已更新的軟體。 下列值可供使用。 • **已安裝** - 這是預設值。如果您選擇此值，監視器將會在工作負載上安裝新軟體應用程式時產生警示。 • **已更新** - 如果您選擇此值，監視器將會在更新軟體應用程式時產生警示。 • **未安裝** - 如果選擇此值，當軟體應用程式遭到解除安裝或無法在工作負載上使用時，監視器將會產生警示。

上次系統重新啟動監視器的設定

上次系統重新啟動會監控工作負載上次重新啟動的時間。

您可以設定下列監視器設定。

設定	描述
工作負載尚未重新啟動	自上次重新啟動工作負載以來的期間 (天數)。如果工作負載未重新啟動的期間比您指定的期間還長，系統將會產生警示。 輸入 1-180 (天) 範圍內的整數值。預設值為 30。

Windows 事件記錄監視器的設定

Windows 事件記錄會監控 Windows 事件記錄中的特定重要業務事件。

您可以設定下列監視器設定。

設定	描述
事件記錄名稱	從 Windows 事件檢視器中的 Windows 事件記錄清單中，選擇某個事件記錄。 下列值可供使用。

設定	描述
	• **任何** —這是預設值。 • **應用程式** • **安全性** • **系統**
事件來源	事件來源名稱 您可以從收集自租用戶所有代理程式的事件來源清單中選擇該值，或者手動輸入來源名稱。 如果租用戶的軟體清查掃描遭到停用，事件來源清單將是空的。
比對模式	在此欄位中，您可以指定要使用 **[任何]** 還是 **[全部]** 運算子來連接 **[事件 ID]**、**[事件類型]** 和 **[事件描述]** 設定。 下列值可供使用。 • **任何** —這是預設值。只有在符合任何所選準則時產生警示。 • **全部** — 只有在符合所有所選準則時產生警示。
事件 ID	請輸入一或多個事件 ID，並以逗號分隔。如果系統在事件記錄中找到您在此欄位中輸入的任何事件代碼，則會產生警示。
事件類型	請選擇您要監控的一或多個事件類型。 下列值可供使用。 • **任何** —這是預設值。 • **錯誤** • **警告** • **資訊** • **成功稽核** • **失敗稽核**
事件描述	事件描述中，您要搜尋的特定關鍵字或字詞。您輸入的每個關鍵字或字詞都必須使用引號括住，而且必須以逗號分隔。如果系統找到您輸入的任何關鍵字或字詞，則會產生警示。
發生次數	事件在該段時間內必須在記錄中存在，才能讓系統產生警示的發生次數下限。 輸入 1-1000 範圍內的整數值。
時間期限	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。 輸入一個整數值，然後選擇單位：分鐘或小時。預設值為 60 分鐘。

檔案和資料夾大小監視器的設定

檔案和資料夾大小會監控所選檔案或資料夾的大小總計。

您可以設定下列監視器設定。

設定	描述
要監控的檔案或資料夾	您想要監控之檔案或資料夾的路徑。您也可以指定您想要從監控排除的檔案或資料夾。 您可以使用以下萬用字元。 • * — 用於檔案或資料夾名稱中的零個或更多個字元 • ? — 用於檔案或資料夾名稱中的一個字元 對於 Windows 工作負載： • 完整路徑開頭應該是磁碟機代號，後面緊接著 :\ 分隔字元。 • 您可以使用正斜線或反斜線作為路徑分隔字元。 • 檔案或資料夾名稱結尾不得為空格或句號。 對於 macOS 工作負載： • 完整路徑開頭應該是根目錄。 • 您可以使用正斜線作為路徑分隔字元。 • 檔案或資料夾名稱結尾不得為空格或句號。 對於排除篩選器，指定特定位置並非強制的。所輸入的檔案如果沒有特定位置，將從受監控資料夾中排除。
運算子	運算子是一種條件式函式，可定義如何衡量指標的效能。 下列值可供使用。 • **大於** —這是預設值。 • **小於**
閾值	閾值和**運算子**值可決定所監控指標的正常效能。當所監控指標的值超出正常範圍時，系統會產生警示。 輸入一個整數值 (MB)。
時間期限	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。 輸入 10-60 (分鐘) 範圍內的整數值。預設值為 10。

Windows Update 狀態監視器的設定

Windows Update 狀態會監控工作負載的 Windows Update 狀態，以及是否已安裝最新更新。

如果您啟用此監視器，系統將會在下列情況下產生警示。

- 工作負載上已停用 Windows Update。
- 工作負載上已啟用 Windows Update，但是未安裝最新更新。

防火牆狀態監視器的設定

防火牆狀態會監控工作負載上已安裝的內建或第三方防火牆。

如果您啟用此監視器，系統將會在下列情況下產生警示。

- 內建的作業系統防火牆 (Windows Defender 防火牆或 macOS 防火牆) 遭到停用，沒有任何第三方防火牆正在執行。
- 公用網路的 Windows Defender 防火牆遭到停用。
- 私人網路的 Windows Defender 防火牆遭到停用。
- 網域網路的 Windows Defender 防火牆遭到停用。

失敗的登入監視器的設定

失敗的登入會監控工作負載上未成功的登入嘗試。

您可以設定下列監視器設定。

設定	描述
失敗的登入嘗試閾值	閾值可決定所監控指標正常效能的界限。超出閾值時，該值就會超出常態。 輸入一個整數值。預設值為 60。
時間期限	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。 輸入 1-24 範圍內的整數值，然後選擇單位：小時或天數。預設值為 12。

防惡意軟體狀態監視器的設定

防惡意軟體狀態會監控工作負載上已安裝的內建或第三方防惡意軟體狀態。

如果您啟用此監視器，系統將會在識別下列其中一種情況時產生警示。

- 工作負載上未安裝防惡意軟體。
- 已安裝防惡意軟體，但未執行。
- 已安裝防惡意軟體並在執行中，但是惡意軟體定義不是最新的。

注意事項
系統已針對 Windows 和 Windows Server 作業系統檢查此條件。

作業系統	支援的防惡意軟體
Windows	• Acronis Cyber Protect • Windows Defender • Symantec Endpoint Security • Norton 360 • Norton Antivirus • SentinelOne • Trend Micro Endpoint Security with Apex One • Trend Micro Worry-Free Business

作業系統	支援的防惡意軟體
	• 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 • 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	• Acronis Cyber Protect • Windows Defender • ESET Endpoint Security **注意事項** 監視器可能可以搭配其他防惡意軟體應用程式使用，但不保證。
macOS	• Acronis 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

作業系統	支援的防惡意軟體
	• K7 Antivirus for Mac • Vipre Advanced Security • Total AV for Mac **注意事項** 監視器可能可以搭配其他防惡意軟體應用程式使用，但不保證。

自動執行功能狀態監視器的設定

自動執行功能狀態會監控是否已啟用卸除式媒體的自動執行功能。

基於安全性考量，建議在工作負載上停用卸除式媒體的自動執行功能。如果啟用此功能，系統將會產生警示。

自訂監視器的設定

自訂會透過執行指令碼監控自訂物件。

您可以設定下列監視器設定。

設定	描述
要執行的指令碼	來自指令碼存放庫的預先定義的指令碼清單。
排程	執行指令碼的時間和執行指令碼應該符合的其他條件 (選擇性)。 下列值可供使用。 • **依時間排程** — 指令碼將在您指定的確切時間、天、週或月內執行。這是預設值。 **排程類型** — **[每小時]**、**[每天]** 或 **[每月]** **在日期範圍內執行** — 執行指令碼的時間範圍。 • **當使用者登入系統時** — 指令碼將在使用者登入工作負載時執行。 • **當使用者登出系統時** — 指令碼將在使用者登出工作負載時執行。 • **在系統啟動時** - 指令碼將在工作負載的作業系統啟動時執行。 • **當系統關閉時** — 指令碼將在工作負載關閉時執行。 • **當系統上線時** — 指令碼將在工作負載在線上變成可用時執行。 **啟動條件** — 只有在符合條件時，才會在指定的時間或事件執行工作。選擇多個條件時，必須同時符合所有條件，才能開始工作。 預設會選擇 **[防止睡眠或休眠模式啟動排程工作]** 條件。 **如果未符合啟動條件，請無論如何在此時間後執行工作** — 此條件預設為啟用狀態。預設值為 1 小時。
執行指令碼的帳戶	將對其執行指令碼的帳戶。

設定	描述
	下列值可供使用。 • **系統帳戶** — 這是預設值。 • **目前已登入的帳戶**
持續時間上限	指令碼可在工作負載上執行的時間長度上限。 如果指令碼未在此期間內完成，作業將會失敗。 輸入 1-1440 (分鐘) 範圍內的整數值。預設值為 3 分鐘。
PowerShell 執行原則	PowerShell 執行原則。 下列值可供使用。 • **Undefined** • **AllSigned** • **Bypass** — 這是預設值。 • **RemoteSigned** • **Restricted** • **Unrestricted** 如需有關這些值的詳細資訊，請參閱 Microsoft 文件。

監控計劃

監控計劃是您在受管理工作負載上套用的計劃，用於啟用和設定監控功能。

如果沒有對工作負載套用任何監控計劃，則監控功能將無法用於工作負載。

注意事項
您在監控計劃中可以設定之設定的可用性，端視租用戶上套用的 Service Pack 而定。若要存取所有設定，請啟用 Advanced Management 套件。

建立監控計劃

您可以建立監控計劃，然後將工作負載新增到其中，以便在受管理的工作負載上設定監控功能。

必要條件

工作負載上安裝的代理程式版本支援監控功能。

若要建立監控計劃

從 [監控計劃]

1. 在 保護 主控台中，移至 **[管理]** > **[監控計劃]**。
2. 使用兩個選項其中之一，建立監控計劃。

- 如果清單中沒有監控計劃，請按一下 **[建立]**。
- 如果清單中有監控計劃，請按一下 **[建立計劃]**。

3. 在 **[建立監控計劃]** 視窗中，根據是否針對您的租用戶啟用 Advanced Management 套件而定，執行下列操作：
   - 如果您的租用戶使用的是標準保護，系統會將以下四個監視器自動新增到監控計劃：磁碟空間、硬體變更、上次系統重新啟動，以及檔案和資料夾大小。
   - 如果要為您的租用戶啟用 Advanced Management 套件，請選擇其中一個範本選項，然後按一下 **[下一步]**。

選項	描述
建議	選擇此選項可使用預設的監控設定建立監控計劃。
自訂	使用此選項可從頭開始建立監控計劃。

4. [選用] 若要變更計劃的預設名稱，請按一下鉛筆圖示，輸入計劃的名稱，然後按一下 **[確定]**。
5. [選用] 若要將監視器新增至計劃，按一下 **[新增監視器]**，按一下清單中的監視器，然後按一下 **[新增]**。

   注意事項
   監視器的設定將會自動填入預設值。
   您最多可以將 3 個相同類型的監視器新增至監控計劃，總共可以新增 30 個監視器。

6. [選用] 在監視器參數畫面中，變更監視器和警示的預設設定，然後按一下 **[完成]**。

   注意事項
   您可以為不同的監視器設定不同的設定。如需詳細資訊，請參閱 "可設定的監視器" (第 936 頁) 和 "設定監控警示" (第 970 頁)。

7. [選用] 若要刪除監視器，按一下垃圾桶圖示，然後按一下 **[刪除]**。
8. [選用] 若要將工作負載新增到計劃：
   a. 按一下 **[新增工作負載]**。
   b. 選擇工作負載，然後按一下 **[新增]**。
   c. 如果有要解決的相容性問題，請遵照 "解決監控計劃的相容性問題" (第 969 頁) 中所述的程序進行。
9. 按一下 **[建立]**。

從所有裝置

1. 在 保護 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 按一下您要套用至監控計劃的工作負載。
3. 按一下 **[保護]**。
4. 根據監控計劃是否套用到工作負載而定，執行下列操作：

- 如果已在工作負載上套用監控計劃，按一下 **[建立計劃]**，然後選擇 **[監控]**。
- 如果在工作負載上未套用任何監控計劃，按一下 **[新增計劃]**，然後按一下 **[建立計劃]**，並選擇 **[監控]**。

5. 在 **[建立監控計劃]** 視窗中，選擇其中一個範本選項，然後按一下 **[下一步]**。

選項	描述
建議	選擇此選項可使用預設的監控設定建立監控計劃。
自訂	使用此選項可從頭開始建立監控計劃。

6. [選用] 若要變更計劃的預設名稱，請按一下鉛筆圖示，輸入計劃的名稱，然後按一下 **[確定]**。
7. [選用] 如果您要變更監視器和警示的預設設定，請設定新值，然後按一下 **[完成]**。

注意事項
您最多可以將 3 個相同類型的監視器新增至監控計劃，總共可以新增 30 個監視器。

8. [選用] 在監視器參數畫面中，變更監視器和警示的預設設定，然後按一下 **[完成]**。

注意事項
您可以為不同的監視器設定不同的設定。如需詳細資訊，請參閱 "可設定的監視器"(第 936 頁) 和 "設定監控警示"(第 970 頁)。

9. [選用] 若要刪除監視器，按一下垃圾桶圖示，然後按一下 **[刪除]**。
10. 按一下 **[建立]**。

將工作負載新增至監控計劃

視您的需要而定，可以在建立監控計劃之後，將工作負載新增至該計劃。

必要條件

- 已為您的使用者帳戶啟用 2FA。
- 工作負載上安裝的代理程式版本支援監控功能。
- 至少可以使用一個監控計劃。

若要將工作負載新增至監控計劃

從 [監控計劃]

1. 在 保護 主控台中，移至 **[管理]** > **[監控計劃]**。
2. 按一下監控計劃。
3. 根據該計劃是否已套用至任何工作負載而定，執行以下作業：
   - 如果該計劃尚未套用至任何工作負載，請按一下 **[新增工作負載]**。
   - 如果該計劃已套用至任何工作負載，請按一下 **[管理工作負載]**。
4. 從清單中選擇工作負載，然後按一下 **[新增]**。

5. 按一下 **[儲存]**。
6. 必要時，按一下 **[確認]**，將所需的服務配額套用至工作負載。

從 [所有裝置]

1. 在 保護 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 按一下您要套用至監控計劃的工作負載。
3. 按一下 **[保護]**。
4. 尋找您要在其中新增工作負載的監控計劃，然後按一下 **[套用]**。
5. 必要時，按一下 **[確認]**，將所需的服務配額套用至工作負載。

撤銷監控計劃

您可以從套用計劃的工作負載中撤銷監控計劃。

必要條件

至少一個監控計劃會套用到工作負載中。

若要撤銷監控計劃

1. 在 保護 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 按一下工作負載，然後按一下 **[保護]**。
3. 按一下您要撤銷之監控計劃的 **[更多動作]** 圖示，然後按一下 **[撤銷]**。

設定自動回應動作

發出警示的事件中的自動回應動作為預先定義的動作，或為回應偵測到的事件或案件而自動觸發的措施。這些動作旨在緩解潛在威脅並使損失降到最低。

您可以在發出警示的事件中設定一個或多個自動回應動作。每個監視器的自動回應動作最大數量為 20。

若要設定自動回應動作

1. 在 保護 主控台中，移至 **[管理]** > **[監控計劃]**。
2. 選擇要設定自動回應動作的監控計劃。
3. 選擇要設定自動回應動作的監視器，或者如果您尚未新增監視器，按一下 **[新增監視器]**，按一下清單中的監視器，按一下 **[新增]**，然後選擇監視器。
4. 按一下 **[自動回應動作]** 旁的連結。
5. 在 **[自動回應動作]** 視窗中，新增當觸發警示時自動執行的一或多個回應動作。
6. 設定每個回應動作。例如，如果您已新增回應動作 **[啟動 Windows 服務]**，則進行以下操作：
   a. 按一下 **[Windows 服務]** 旁邊的 **[指定]**。
   b. 在 **[服務]** 欄位中，選擇要作為回應動作啟動的服務。
   c. 按一下**[完成]**。
7. 在所有已新增回應動作的清單中，使用向上和向下箭頭或拖曳設定回應動作的順序。

8. 設定前一個回應動作失敗時，如何處理後續回應動作。選擇下列一項：
   a. **繼續下一個回應動作**。
   b. **不要繼續下一個回應動作**。
9. 按一下**[完成]**。
   您將在監控計劃設定的 **[自動回應動作]** 旁邊見到已設定動作的數量。您可以編輯或刪除動作，並在之後任何時候增加新動作。

下表列出並描述所有監視器設定中可使用的自動回應動作。

自動回應動作	描述	支援的 OS
執行指令碼	若您新增此動作，則可以： 1. 選擇要在工作負載上執行的特定指令碼。 2. 指定您執行指令碼所要使用的帳戶。 3. 指定操作的持續時間上限。 4. 指定 PowerShell 執行原則。 5. 執行指令碼。 若要執行此動作，您需要有工作負載的 Advanced Management 套件授權 (如果還未獲指派)。 滿足條件時，系統將執行所選遠端指令碼。	Windows、macOS
重新啟動工作負載	若您新增此動作，系統將在滿足條件時遠端重新啟動工作負載。	Windows、macOS
停止程序	若您新增此動作，則可以透過手動輸入程序名稱指定要停止的程序。 滿足條件時，系統將停止程序。	Windows、macOS
啟動 Windows 服務	若您新增此動作，則可以從自代理程式填入的動態服務清單中選擇要啟動的 Windows 服務。 滿足條件時，系統將啟動服務。	Windows
停止 Windows 服務	若您新增此動作，則可以從自代理程式填入的動態服務清單中選擇要停止的 Windows 服務。 滿足條件時，系統將停止服務。	Windows
啟用 Windows Update	若您新增此動作，系統將在滿足條件時啟用 Windows Update。 此動作僅適用於 Windows Update 狀態監視器。	Windows
停用卸除式磁碟機上的自動執行	若您新增此動作，系統將在滿足條件時停用工作負載的卸除式儲存媒體之自動執行功能。 此動作僅適用於自動執行功能狀態監視器。	Windows

監控計劃的其他動作

在 **[監控計劃]** 畫面上，您可以對監控計劃執行以下其他動作：檢視詳細資料、編輯、檢視活動、檢視警示、重新命名、啟用、停用、複製、匯出、設為我的最愛、設為預設和刪除。

檢視詳細資料

若要檢視監控計劃的詳細資料

1. 在 **[監控計劃]** 畫面中，按一下監控計劃的 **[更多動作]** 圖示。
2. 按一下 **[檢視詳細資料]**。
3. [選用] 如果您要檢視在計劃中啟用之監視器的詳細資料，請按一下監視器名稱。

編輯

必要條件

已為您的使用者帳戶啟用 2FA。

若要編輯計劃

1. 在 **[監控計劃]** 畫面中，按一下監控計劃的 **[更多動作]** 圖示。
2. 按一下 **[編輯]**。
3. [選用] 若要從計劃中刪除某個監視器，按一下監視器名稱右側的資源回收筒圖示。
4. [選用] 若要啟用或停用計劃中的監視器，請使用監視器名稱旁邊的切換開關。
5. [選用] 若要編輯監視器參數，請執行以下操作。
   a. 按一下監視器名稱。
   b. 按一下監視器參數的概觀。
   c. 在 **[監視器參數]** 畫面中設定參數，然後按一下 **[完成]**。

   注意事項
   您可以為不同的監視器設定不同的設定。如需詳細資訊，請參閱 "可設定的監視器" (第 936 頁) 和 "設定監控警示" (第 970 頁)。

   d. 關閉畫面並確認變更。
6. [選用] 若要新增監視器，按一下 **[新增監視器]**，然後編輯參數 (如有需要)，如上一個步驟中所述。
7. 按一下 **[儲存]**。

活動

若要檢視與監控計劃相關的活動

1. 在 **[監控計劃]** 畫面中，按一下監控計劃的 **[更多動作]** 圖示。
2. 按一下 **[活動]**。
3. 按一下活動，以檢視有關它的更多詳細資料。

警示

若要檢視警示

1. 在 **[監控計劃]** 畫面中，按一下監控計劃的 **[更多動作]** 圖示。
2. 按一下 **[警示]**。

重新命名

必要條件

已為您的使用者帳戶啟用 2FA。

若要重新命名監控計劃

1. 在 **[監控計劃]** 畫面中，按一下監控計劃的 **[更多動作]** 圖示。
2. 按一下 **[重新命名]**。
3. 輸入計劃的名稱，然後按一下 **[確定]**。

啟用

必要條件

- 已為您的使用者帳戶啟用 2FA。
- 監控計劃隨即套用到至少一個工作負載。

若要啟用監控計劃

1. 在 **[監控計劃]** 畫面中，按一下監控計劃的 **[更多動作]** 圖示。
2. 按一下 **[啟用]**。

停用

必要條件

已為您的使用者帳戶啟用 2FA。

若要停用監控計劃

1. 在 **[監控計劃]** 畫面中，按一下監控計劃的 **[更多動作]** 圖示。
2. 按一下 **[停用]**。

複製

必要條件

已為您的使用者帳戶啟用 2FA。

若要複製監控計劃

1. 在 **[監控計劃]** 畫面中，按一下監控計劃的 **[更多動作]** 圖示。
2. 按一下 **[複製]**。
3. 按一下 **[建立]**。

匯出

必要條件

已為您的使用者帳戶啟用 2FA。

若要匯出監控計劃

1. 在 **[監控計劃]** 畫面中，按一下監控計劃的 **[更多動作]** 圖示。
2. 按一下 **[匯出]**。
   計劃設定將以 JSON 格式匯出到本機電腦。

刪除

必要條件

已為您的使用者帳戶啟用 2FA。

若要刪除監控計劃

1. 在 **[監控計劃]** 畫面中，按一下監控計劃的 **[更多動作]** 圖示。
2. 請按一下 **[刪除]**。
3. 選擇 **[我確認]**，然後按一下 **[刪除]**。

設為預設

必要條件

已為您的使用者帳戶啟用 2FA。

若要將監控計劃設為預設

1. 在 **[監控計劃]** 畫面中，按一下監控計劃的 **[更多動作]** 圖示。
2. 按一下 **[設為預設]**。
3. 在確認視窗中，按一下 **[設定]**。
   在 **[監控計劃]** 畫面上，**[預設]** 標籤會出現在計劃名稱旁。

新增至我的最愛

必要條件

已為您的使用者帳戶啟用 2FA。

若要將監控計劃設為我的最愛

1. 在 **[監控計劃]** 畫面中，按一下監控計劃的 **[更多動作]** 圖示。
2. 按一下 **[新增至我的最愛]**。
   在 **[監控計劃]** 畫面上，星形圖示會出現在計劃名稱旁。

監控計劃的相容性問題

在某些情況下，對工作負載套用監控計劃可能會導致相容性問題。您可能會觀察到下列相容性問題：

- 不相容的作業系統 - 當工作負載的作業系統不受支援時，會出現此問題。
- 不支援的代理程式 – 當工作負載上的保護代理程式版本已過期，而且不支援監控功能時，會出現此問題。
- 配額不足 - 當租用戶中沒有足夠的服務配額可指派給所選的工作負載時，會出現此問題。

如果監控計劃套用至多達 150 項個別選取的工作負載，系統會提示您先解決現有衝突，然後才能儲存計劃。若要解決衝突，請移除其根本原因或從計劃移除受影響的工作負載。如需詳細資訊，請參閱 "解決監控計劃的相容性問題" (第 969 頁)。如果在未解決衝突的情況下儲存計劃，對於不相容的工作負載，該計劃將自動停用，並且會顯示警示。

如果將監控計劃套用至超過 150 項工作負載或裝置群組，則會先儲存計劃，然後再檢查相容性。系統會自動針對不相容的工作負載停用該計劃，並顯示警示。

解決監控計劃的相容性問題

根據相容性問題的原因，您可以執行不同的動作來解決相容性問題，作為建立新監控計劃程序的一部分。

若要解決相容性問題

1. 按一下 **[檢閱問題]**。
2. [選用] 若要透過從計劃中移除工作負載來解決不相容作業系統的相容性問題：
   a. 在 **[不相容的作業系統]** 索引標籤上，選擇您要移除的工作負載。
   b. 按一下 **[從計劃中移除工作負載]**。
   c. 按一下 **[移除]**，然後按一下 **[關閉]**。
3. [選用] 若要透過停用計劃中的監視器來解決不相容作業系統的相容性問題：
   a. 在 **[不相容的作業系統]** 索引標籤上，選擇您要移除的監視器。
   b. 按一下 **[停用監視器]**。
   c. 按一下 **[停用]**，然後按一下 **[關閉]**。
4. [選用] 若要透過從計劃中移除工作負載來解決與不支援的代理程式的相容性問題：
   a. 在 **[不支援的代理程式]** 索引標籤上，選擇您要移除的工作負載。
   b. 按一下 **[從計劃中移除工作負載]**。
   c. 按一下 **[移除]**，然後按一下 **[關閉]**。
5. [選用] 若要透過更新代理程式版本來解決與不支援的代理程式的相容性問題，請按一下 **[移至代理程式清單]**。

   注意事項
   此選項僅適用於客戶系統管理員。

6. [選用] 若要透過從計劃中移除工作負載來解決配額不足的相容性問題：
   a. 在 **[配額不足]** 索引標籤上，選擇您要移除的工作負載。
   b. 按一下 **[從計劃中移除工作負載]**。
   c. 按一下 **[移除]**，然後按一下 **[關閉]**。
7. [選用] 若要透過增加租用戶配額來解決配額不足的相容性問題：

a. 在 **[配額不足]** 索引標籤上，按一下 **[前往管理入口網站]**。
b. 增加客戶的服務配額。

注意事項
此選項僅適用於合作夥伴系統管理員。

重設機器學習模型

當工作負載模型過期或因為特定原因而無效時，您可以進行重設。此動作將會刪除所建立的模型以及具有基於異常之監控類型的監視器針對工作負載收集的資料，然後將從頭開始為工作負載訓練機器學習模型。

若要重設工作負載的機器學習模型

1. 在 保護 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 按一下清單中的工作負載，然後按一下 **[詳細資料]** 索引標籤。
3. 在 **[重設機器學習模型]** 區段中，按一下 **[重設]**。
4. 在確認視窗中，再按一下 **[重設]**。

監控警示

監控警示會顯示在 保護 主控台中，並在受監控的工作負載行為異常時，透過電子郵件傳送。這些警示可確保在組織的 IT 環境出現任何問題時，利害關係人能夠盡快收到通知。

注意事項
若要透過電子郵件啟用監控警示，您必須為對應的警示類型設定至少一個電子郵件通知原則。如需詳細資訊，請參閱 "設定電子郵件通知原則" (第 976 頁)。

設定監控警示

您可以在將監視器新增到監控計劃時，或在編輯已在監控計劃中提供的監視器時，設定監視器的警示設定。

若要設定監控警示

1. 在 **[監視器參數]** 視窗中，前往 **[產生警示]** 區段。
2. 在 **[警示嚴重性]** 中，選擇對應警示優先順序的嚴重性。

選項	描述
重大	這些警示的優先順序最高，而且與對工作負載操作至關重要的問題相關。請盡快解決這些問題。
錯誤	錯誤警示比較不嚴重，表示發生錯誤或行為不正常。及時解決問題可防止造成更嚴重的問題。
警	警告警示表示存在您應該注意的特定情況，但它可能尚未造成問題。請在修正導致

選項	描述
告	重大和錯誤警示的問題後解決這些問題。 這是預設值。
資訊	這些警示的優先順序最低。告知性嚴重性並不表示存在問題。這類警示所提供的資訊是與所監控物件相關的動作。

3. 在 **[警示頻率]** 中，選擇在符合條件時，系統應該多久產生一次警示。

選項	描述
一次，直到檢查通過	系統將會產生警示一次，執行檢查成功完成為止。 這是預設值。
在連續失敗 X 次之後	系統將會在檢查連續失敗 X 次之後產生警示，其中 X 是整數值。

4. 在 **[警示訊息]** 中，按一下鉛筆圖示可編輯系統產生警示時將使用的預設警示訊息。您可以指定包含變數的自訂警示訊息。如需有關您可以使用之變數的詳細資訊，請參閱 "監控警示變數" (第 971 頁)。

   注意事項
   您可以為部分監視器設定多個警示訊息。

5. 如果您希望系統在所監控指標回復到正常狀態且行為再次正常時自動解決警示，請啟用 **[自動解決警示]**。此設定預設為啟用狀態。

監控警示變數

您可以針對不同的監視器設定不同的警示變數。若要使用變數，其必須以 {{}} 括住。

下表提供有關可用變數的詳細資訊。

變數	描述	可用於監視器
plan_name	原則名稱	所有監視器
monitor_name	監控計劃中，子原則的名稱	所有監視器
workload_name	工作負載的名稱	所有監視器
threshold_value	用於產生警示的特定監控條件或閾值	支援基於閾值的監控的所有監視器。
threshold_unit	與閾值相關聯的單位。例如，%、MB 或 mb/秒。	支援基於閾值的監控的所有監視器。
time_period	只有在指定的期間內指標值超出正常範圍時，系統才會針對偵測到的問題產生警示。	支援基於閾值的監控的所有監視器。
time_unit	與時間期限相關聯的單位 (秒/分/小時/天)。	支援基於閾值的監控

變數	描述	可用於監視器
		的所有監視器。
anomaly_value	異常值	支援基於異常的監控的所有監視器。
anomaly_unit	與異常值相關聯的單位	支援基於異常的監控的所有監視器。
deviation_value	偏差值	支援基於異常的監控的所有監視器。
deviation_unit	與偏差值相關聯的單位	支援基於異常的監控的所有監視器。
drive_name	Windows 的磁碟機或 macOS 的磁碟分割	磁碟空間,
CPU_model	受監控 CPU 的型號	CPU 溫度
GPU_model	受監控 GPU 的型號	GPU 溫度
hardware_model	受監控元件的型號	硬體變更
hardware_component	受監控硬體的類型	硬體變更
hardware_model_old	已更換的受監控元件的型號	硬體變更
hardware_model_new	已新增的新受監控元件的型號	硬體變更
disk_model	磁碟的型號	磁碟傳輸速率
network_adapter_model	網路介面卡的型號	網路使用
process_name	程序的名稱	CPU 使用量 (依程序) 記憶體使用量 (依程序) 磁碟傳輸速率 (依程序) 網路使用量 (依程序) 程序狀態
service_name	服務的名稱	Windows 服務狀態

變數	描述	可用於監視器
software_name	軟體應用程式的名稱	已安裝的軟體
software_version	軟體應用程式的版本	已安裝的軟體
software_version_old	軟體應用程式更新前的版本	已安裝的軟體
software_version_new	新的或更新的軟體應用程式版本	已安裝的軟體
number_of_occurrences	事件出現在記錄中的次數	Windows 事件日誌
event_types	事件的類型	Windows 事件日誌
event_source	事件的來源	Windows 事件日誌
event_log_name	事件的名稱	Windows 事件日誌
firewall_software_name	防火牆軟體的名稱	防火牆狀態
antimalware_software_name	防惡意軟體的名稱	反惡意程式碼軟體狀態
user_name	使用者的名稱	自動執行功能狀態
script_name	指令碼的名稱	自訂

手動回應動作

當您看到警示時，可以選擇您要對發出警示的事件執行的回應動作。

若要執行手動回應動作

1. 在 保護 主控台中，移至 **[警示]**。
2. 開啟您要檢視的警示。
3. 按一下 **[回應動作]**，然後從下拉式清單中選擇一個回應動作。

可用於特定警示之回應動作的清單取決於警示類型、特定租用戶的功能可用性，以及工作負載作業系統。

下表列出並描述所有手動回應動作，以供您參考。

手動回應動作	描述	支援的 OS
瀏覽磁碟空間使用狀況趨勢	開啟具有**磁碟空間使用狀況**圖表的視窗，其中您可以： • 瀏覽磁碟空間使用狀況如何隨著時間變化	Windows、macOS

手動回應動作	描述	支援的 OS
	(過去 1 天/7 天/1 個月)。 • 瀏覽所選期間磁碟空間使用狀況相對值 (%) 的增量。	
瀏覽檔案大小成長趨勢	開啟具有**檔案大小成長**圖表的視窗，其中您可以： • 瀏覽所監控檔案和資料夾的總大小如何隨著時間變化 (過去 1 天/7 天/1 個月)。 • 瀏覽所選期間檔案總大小相對值 (%) 的增量。	Windows、macOS
執行指令碼	開啟視窗，其中您可以： 1. 選擇要在工作負載上執行的特定指令碼。 2. 指定您執行指令碼所要使用的帳戶。 3. 指定操作的持續時間上限。 4. 指定 PowerShell 執行原則。 5. 執行指令碼。 若要執行此動作，您需要有工作負載的 Advanced Management 套件授權 (如果還未獲指派)。	Windows、macOS
透過 NEAR 連線	Acronis Connect 用戶端 會建立遠端連線。	Windows、macOS
透過 RDP 連線	Acronis Connect 用戶端 會建立遠端連線。	Windows
開啟硬體清查	系統會將您重新導向到目前工作負載的 **[硬體清查]** 索引標籤。	Windows、macOS
瀏覽已載入 CPU 的前 10 個程序	開啟一個視窗，其中包含已載入 CPU 且可能已導致其過熱的前 10 個程序 (產生警示時的系統快照)。	Windows、macOS
瀏覽已載入 GPU 的前 10 個程序	開啟一個視窗，其中包含已載入 GPU 且可能已導致其過熱的前 10 個程序 (產生警示時的系統快照)。	Windows、macOS
瀏覽已載入記憶體的前 10 個程序	開啟一個視窗，其中包含已載入記憶體的前 10 個程序 (產生警示時的系統快照)。	Windows、macOS
瀏覽已載入磁碟的前 10 個程序	開啟一個視窗，其中包含已載入磁碟的前 10 個程序 (產生警示時的系統快照)。	Windows、macOS
瀏覽已載入網路的前 10 個程序	開啟一個視窗，其中包含已載入網路介面卡的前 10 個程序 (產生警示時的系統快照)。	Windows、macOS
瀏覽資源使用量 (依程序)	開啟一個視窗，其中包含硬體資源使用量 (依	Windows、

手動回應動作	描述	支援的 OS
	相關程序) 的詳細資訊：CPU 使用量、記憶體使用量、磁碟 I/O、網路使用量。	macOS
重新啟動工作負載	開啟一個確認視窗。確認後重新啟動工作負載。	Windows、macOS
啟動 Windows 服務	開啟一個確認視窗。確認後啟動 Windows 服務。	Windows
停止 Windows 服務	開啟一個確認視窗。確認後停止 Windows 服務。	Windows
停止程序	開啟一個確認視窗。確認後停止警示所指的程序。	Windows、macOS
啟用 Windows Update	開啟一個確認視窗。確認後啟用 Windows Update。	Windows
停用卸除式磁碟機上的自動執行功能	開啟一個確認視窗。確認後，在工作負載的系統層級上停用自動執行功能。	Windows

重要事項

基於安全，需要使用雙重驗證機制才能執行下列手動回應動作：

- 執行指令碼
- 透過 NEAR 連線
- 透過 RDP 連線
- 重新啟動工作負載
- 啟動 Windows 服務
- 停止 Windows 服務
- 停止程序
- 啟用 Windows Update
- 停用卸除式磁碟機上的自動執行功能

檢視工作負載的監控警示

在 **[警示]** 索引標籤中，您可以檢視特定工作負載的監控警示，並執行不同的警示動作。

若要檢視工作負載的監控警示

1. 在 保護 主控台，前往 **[所有裝置]**。
2. 按一下工作負載，然後選擇 **[警示]** 索引標籤。
3. [選用] 在監控警示窗格中，執行以下其中一個動作：

- 若要清除警示，按一下 **[清除]**。
- 若要採取回應動作，按一下 **[回應動作]**，然後按一下該動作。
- 若要聯絡支援團隊，按一下 **[取得支援]**。

4. [選用] 若要清除工作負載的所有監控警示，按一下 **[全部清除]**。

檢視監控警示的警示記錄

您可以按時間順序查看與監控警示相關的所有事件：已執行的回應動作 (自動或手動) 以及已傳送的電子郵件通知。

若要檢視監控警示的稽核記錄

1. 在 保護 主控台中，移至 **[警示]**。
2. 開啟 **[表格檢視]**。
3. 在警示清單中，按一下您要檢視的監控警示。
4. 按一下 **[詳細資料]**，然後按一下 **[警示記錄]**。

設定電子郵件通知原則

電子郵件通知原則可指定哪些使用者將從不同的監視器收到電子郵件通知。

從 **[電子郵件通知]** 畫面中，您可以對電子郵件通知原則執行以下動作：新增、編輯、啟用、停用和刪除。

新增

若要新增電子郵件通知原則

1. 在 保護 主控台中，移至 **[設定]** > **[電子郵件通知]**。
2. 按一下 **[新增原則]**。
3. 按一下 **[選擇收件者]**。
4. 在 **[選擇收件者]** 畫面中，選擇您希望收到電子郵件警示的使用者，然後按一下 **[選擇]**。
5. 在 **[警示類型]** 中，選擇您希望系統為其傳送電子郵件警示的監視器。
6. 按一下 **[新增]**。

編輯

若要編輯電子郵件通知原則

1. 在 保護 主控台中，移至 **[設定]** > **[電子郵件通知]**。
2. 按一下通知原則的省略符號圖示，然後按一下 **[編輯]**。
3. [選用] 若要變更收件者，按一下 **[編輯收件找]**，從清單中新增或移除使用者，然後按一下 **[選擇]**。
4. [選用] 在 **[警示類型]** 中，選擇您希望傳送給所選收件者的監控警示類型。
5. 按一下 **[儲存]**。

啟用

若要啟用電子郵件通知原則

1. 在 保護 主控台中，移至 **[設定]** > **[電子郵件通知]**。
2. 在 **[電子郵件通知]** 畫面中，按一下電子郵件通知原則的 **...** 圖示。
3. 按一下 **[啟用]**。

停用

若要停用電子郵件通知原則

1. 在 保護 主控台中，移至 **[設定]** > **[電子郵件通知]**。
2. 在 **[電子郵件通知]** 畫面中，按一下電子郵件通知原則的 **...** 圖示。
3. 按一下 **[停用]**。

刪除

若要刪除電子郵件通知原則

1. 在 保護 主控台中，移至 **[設定]** > **[電子郵件通知]**。
2. 在 **[電子郵件通知]** 畫面中，按一下電子郵件通知原則的 **...** 圖示。
3. 按一下 **[刪除]**，然後按一下 **[確認]**。

檢視監視器資料

對於每個工作負載，您可以檢視所套用監視器的清單、監視器的目前狀態，以及圖形檢視中的歷史效能詳細資料。您可以使用此資訊分析工作負載的狀態以及狀態隨時間的變化。

必要條件

- 監控計劃是在工作負載上套用的。
- 此工作負載在線上而且有對應監視器的資料。
- 工作負載上安裝的代理程式版本支援監控計劃。

若要檢視套用到工作負載的監視器及監視器資料

1. 在 保護 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 按一下工作負載，然後按一下 **[監控]** 索引標籤。

   [監控] 索引標籤會針對為工作負載啟用的每個監視器，顯示其桌面小工具。每個桌面小工具都會顯示以下資訊。

顯示的資訊	描述
監視器名稱	監視器名稱
上次結果	所監控指標的最新值或事件的最新狀態

顯示的資訊	描述
上次檢查	監視器收集上次資料的日期與時間
警示	由監視器產生且仍未解決的警示數量。 如果此監視器產生至少一個未解決的警示，按一下該數字將會開啟 **[警示]** 索引標籤。系統將會篩選警示，而且只會列出此監視器的警示。

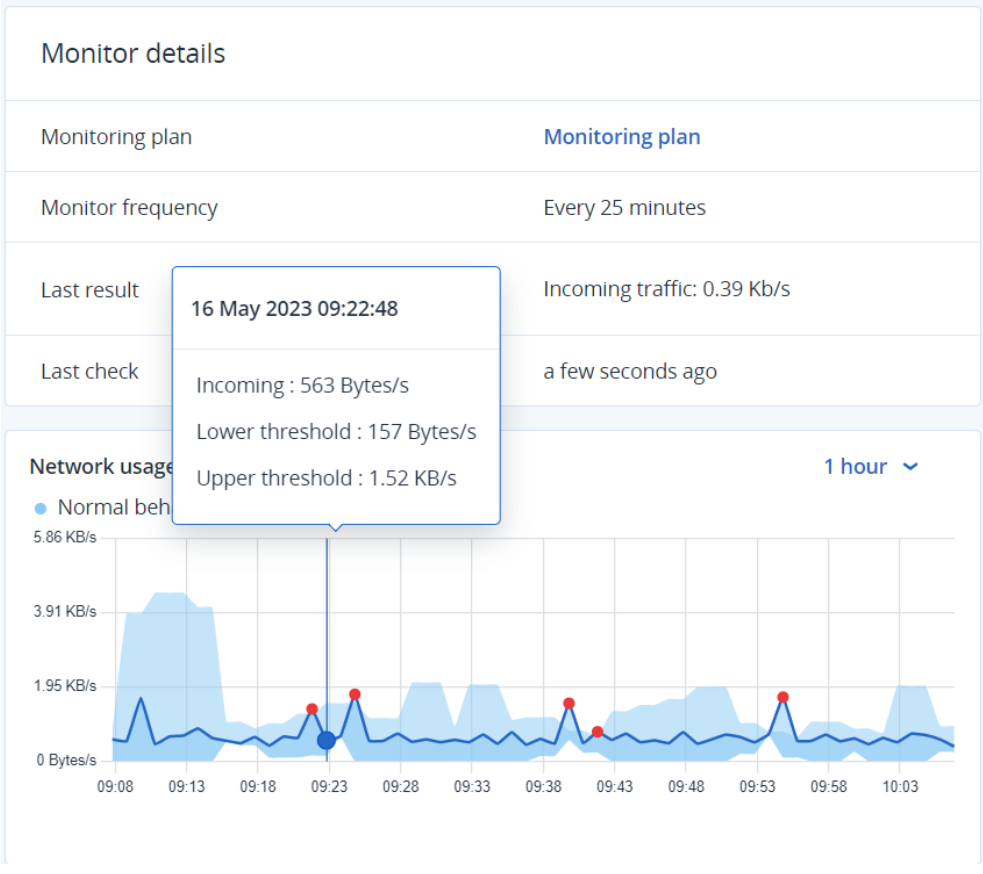
注意事項
將監控計劃套用至工作負載之後，桌面小工具將會在索引標籤上顯示 15 分鐘 (或是針對監視器設定的監視器頻率下限)。

3. [選用] 若要檢視更多有關監視器的詳細資料以及針對所監控指標收集的歷史資料 (若適用)，請在監視器的桌面小工具中，按一下省略符號圖示，然後按一下 **[詳細資料]**。
   如需有關您可以在桌面小工具查看之監視器詳細資料的詳細資訊，請參閱 "監視器桌面小工具" (第 978 頁)。

監視器桌面小工具

在監視器桌面小工具中，您可以查看關於監視器的下列詳細資料。

詳細資料	描述
監控計劃	包含監視器之監控計劃的名稱。監控計劃的名稱是一個連結，可在檢視模式下開啟監控計畫。
監控頻率	監視器從工作負載收集資料的時間間隔
上次結果	所監控指標的最新值或事件的最新狀態
上次檢查	監視器收集上次資料的日期與時間

詳細資料	描述
上次警示	產生上次警示的日期與時間。只有在針對監視器至少產生一個警示時，才會顯示此欄位。
歷史圖表	針對收集時間序列資料的監視器，動態小工具會在圖形檢視中顯示所選期間 (1 小時、6 小時、12 小時、1 天、1 週或 1 個月) 的歷史資料。 此圖表會顯示所選期間內，指標的實際值。如果基於某種原因，代理程式未將收集的資料傳送到雲端，則缺少的值將顯示為虛線，將資料點與缺少的值前後的實際值連接起來。 對於使用**基於異常**的監控的監視器，此圖表會顯示基準線區域、可顯示指標實際值的線條，以及異常。異常是超出基準線的峰值或值，在圖表上會顯示為紅點。 如果您將滑鼠暫留在圖表上，可以看到特定時間的實際值和閥值。  **注意事項** 圖表上的資料會以本機系統的時區顯示。亦即，您存取 保護 主控台所在工作負載的瀏覽器時區。

其他 Cyber Protection 工具

合規模式

合規模式是針對具有更高安全性需求的用戶端而設計。此模式要求強制加密所有備份，而且僅允許在本機設定加密密碼。

使用合規模式時，在客戶租用戶及其單位中建立的所有備份都會自動使用 AES 演算法和 256 位元金鑰加密。使用者僅能在受保護的裝置上設定加密密碼，而且無法在保護計劃中設定加密密碼。

重要事項
無法停用合規模式。

限制

- 合規模式僅與版本為 15.0.26390 或更新版本的代理程式相容。
- 合規模式不適用於執行 Red Hat Enterprise Linux 4.x 或 5.x 及其衍生產品的裝置。
- 雲端服務無法存取加密密碼。基於此限制，部分功能在合規模式下無法用於租用戶。

不支援的功能

下列功能在合規模式下無法用於租用戶：

- 透過 Cyber Protect 主控台復原
- 透過 Cyber Protect 主控台瀏覽檔案層級的備份
- 雲端對雲端備份
- 網站備份
- 應用程式備份
- 備份行動裝置
- 備份的反惡意程式碼掃描
- 安全復原
- 自動建立公司白名單
- 資料保護圖
- 災難復原
- 與無法使用之功能相關的報告和儀表板

設定加密密碼

您必須在受保護的裝置本機上設定加密密碼。您無法在保護計劃中設定加密密碼。如果沒有密碼，建立備份將會失敗。

警告！
若是遺失或忘記密碼，則無法復原加密的備份。

您可以利用下列方式，設定加密密碼：

1. 在安裝保護計劃期間 (適用於 Windows、macOS 和 Linux)。
2. 使用命令列 (適用於 Windows 和 Linux)。
   這是在虛擬裝置上設定加密密碼的唯一方式。
   如需有關如何使用 **Acropsh** 工具設定加密密碼的詳細資訊，請參閱 "加密" (第 390 頁)。
3. 在 Cyber Protect Monitor 中 (適用於 Windows 和 macOS)。

在 Cyber Protect Monitor 中設定加密密碼

1. 在受保護的裝置上，以系統管理員身分登入。
2. 按一下通知區域 (Windows) 或功能表列 (macOS) 中的 [Cyber Protect Monitor] 圖示。
3. 按一下齒輪圖示。
4. 按一下**加密**。
5. 設定加密密碼。
6. 按一下 **[確定]**。

變更加密密碼

您可以在保護計劃建立任何備份之前，變更加密密碼。

建議您不要在建立備份之後變更加密密碼，因為後續的備份將會失敗。若要繼續保護相同的電腦，您必須為其建立新的保護計劃。同時變更加密密碼和保護計劃將會導致建立使用變更後的密碼加密的新備份。在這些變更之前建立的備份將不會受到影響。

或者，您可以保留已套用的保護計劃，僅變更其中的備份檔案名稱。這也將導致建立使用變更後的密碼加密的新備份。若要深入瞭解備份檔案名稱，請參閱 "備份檔案名稱" (第 399 頁)。

您可以利用下列方式，變更加密密碼：

1. 在 Cyber Protect Monitor 中 (適用於 Windows 和 macOS)。
2. 使用命令列 (適用於 Windows 和 Linux)。
   如需有關如何使用 **Acropsh** 工具設定加密密碼的詳細資訊，請參閱 "加密" (第 390 頁)。

在合規模式下復原租用戶的備份

您無法使用合規模式，在 Cyber Protect 主控台中復原備份。

您可以選取下列選項：

- 使用可開機媒體復原整部電腦、其磁碟或檔案。
- 使用 [Windows 檔案總管]，透過已安裝的代理程式，從 Windows 電腦本機備份解擷取檔案。

不可變動儲存空間

固定儲存空間可讓您在指定的保留期間內存取已刪除的備份。您可從這些備份中復原內容，但無法變更、移動或刪除。當保留期限結束後，將永久刪除已刪除的備份。

不可變動儲存空間包含下列備份：

- 手動刪除的備份。
- 根據保護計劃的 **[保留時間]** 區段中的設定，或清理計劃的 **[保留規則]** 區段中的設定，自動刪除的備份。

固定儲存空間中已刪除的備份仍然會使用儲存空間，並據以收費。

已刪除的租用戶無需支付任何儲存空間費用，包括固定儲存空間。

固定儲存空間模式

針對客戶租用戶，固定儲存空間可在下列模式中使用：

固定儲存空間可在下列模式中使用：

- **治理模式**
  您可以停用後再重新啟用固定儲存空間。您可以變更保留期間或切換到 [合規] 模式。
- **合規模式**

  警告！
  選擇 [合規] 模式是不可逆的。

  您無法停用固定儲存空間。您無法變更保留期間，也無法切換回 [治理] 模式。

支援的儲存空間和代理程式

- 僅雲端儲存空間支援固定儲存空間。
  固定儲存空間適用於使用 Acronis Cyber Infrastructure 4.7.1 版或更新版本的 Acronis 託管和合作夥伴託管的雲端儲存空間。
  支援可以搭配 Acronis Cyber Infrastructure Backup Gateway 使用的所有儲存空間。例如，Acronis Cyber Infrastructure 儲存體、Amazon S3 和 EC2 儲存體以及 Microsoft Azure 儲存體。
  固定儲存空間要求為 Acronis Cyber Infrastructure 中的 Backup Gateway 服務開放 TCP 連接埠 40440。在 4.7.1 版和更新版本中，會自動透過 **[Backup (ABGW) 公用]** 流量類型開放 TCP 連接埠 40440。如需有關流量類型的詳細資訊，請參閱 Acronis Cyber Infrastructure 文件。
- 固定儲存空間需要保護代理程式版本 21.12 (組建 15.0.28532) 或更高版本。
- 僅支援 TIBX(版本 12) 備份。

啟用固定儲存空間

您可以在 Cyber Protect 主控台或管理入口網站中設定固定儲存空間設定。兩者都可以存取相同的設定。以下程序使用 Cyber Protect 主控台。若要瞭解如何在管理入口網站中設定固定儲存空間設定，請參閱系統管理員指南中的設定固定儲存空間。

設定固定儲存空間設定必須在系統管理員帳戶所屬的租用戶中，使用雙重驗證機制。

啟用固定儲存空間

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 移至 **[設定]** > **[系統設定]**。

3. 捲動預設備份選項清單，然後按一下 **[固定儲存空間]**。
4. 啟用 **[固定儲存空間]** 開關。
5. 指定一個介於 14 到 3650 天之間的保留期間。
   預設保留期間為 14 天。保留期間較長時，將會導致儲存空間使用量增加。
6. 選擇固定儲存空間模式，然後在出現提示時確認您的選擇。
   在 [治理] 模式下，您可以啟用或停用固定儲存空間，並變更保留期間。您可以從 [治理] 模式切換到 [合規] 模式。

   警告！
   切換至 [合規模式] 是不可逆的。選擇 [合規] 模式之後，您就無法停用固定儲存空間，也無法變更其模式或保留期間。

7. 按一下 **[儲存]**。
8. 若要讓現有的存檔支援固定儲存空間，請在該存檔中建立新備份。
   若要建立新備份，請手動或依排程執行保護計劃。

   警告！
   如果您在讓存檔支援固定儲存空間之前刪除備份，則該備份會遭到永久刪除。

停用固定儲存空間

注意事項
您只能在 [治理] 模式下停用固定儲存空間。

停用固定儲存空間

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 在導覽功能表中，按一下 **[設定]** > **[系統設定]**。
3. 捲動預設備份選項清單，然後按一下 **[固定儲存空間]**。
4. 停用 **[固定儲存空間]** 開關。
5. 按一下 **[停用]**，確認您的選擇。

警告！
停用固定儲存空間不會立即生效。在 14 天的寬限期內，固定儲存空間仍處於作用中狀態，而且您可以根據其原始的保留期限，存取已刪除的備份。當寬限期結束後，將永久刪除固定儲存空間內的所有備份。

存取固定儲存空間中已刪除的備份

在整個保留期間，您可以存取已刪除的備份並從中復原資料。

注意事項
為允許存取已刪除的備份，應該在備份儲存上，針對傳入連線啟用連接埠 40440。

若要存取已刪除的備份

1. 在 **[備份儲存空間]**索引標籤上，選擇包含已刪除備份的雲端儲存空間。
2. [僅適用於已刪除的存檔] 若要查看已刪除的存檔，請按一下 **[顯示已刪除]**。
3. 選擇包含您要復原之備份的存檔。
4. 按一下 **[顯示備份]**，然後按一下 **[顯示已刪除]** 的備份組。
5. 選擇您要復原的備份。
6. 繼續執行復原作業，如 "復原" (第 442 頁) 中所述。

異地備援儲存空間

異地備援儲存會將資料以非同步方式複製到在地理上遠離主要位置的次要位置，藉此確保資料的持久性。透過異地備援，即使主要位置無法使用，您的資料也可供存取。

重要事項
複寫的資料會佔用與原始資料相同的儲存空間。

啟用和停用異地備援儲存空間

必要條件

- 只有在合作夥伴系統管理員在管理入口網站中或透過 API 啟用之後，異地備援儲存空間才能在 Cyber Protect 主控台中使用。
- 只有系統管理員可以在 Cyber Protect 主控台中啟用或停用異地備援儲存空間。請確認您擁有系統管理員權限。

若要啟用異地備援儲存空間

1. [只有在透過 API 啟用異地備援儲存空間時] 在最上方的「異地備援適用於雲端中的所有資料」警示中，按一下 **[啟用異地備援雲端儲存]**。
2. 在 Cyber Protect 主控台中，移至 **[設定]** > **[系統設定]**。
3. 捲動預設備份選項清單，然後按一下 **[異地備援雲端儲存]**。
4. 啟用 **[異地備援雲端儲存]** 開關。
5. 按一下 **[儲存]**。
   現在，您的資料將會複寫到次要位置，而且即使主要位置發生故障，也將保持可用。

若要停用異地備援儲存空間

警告！
停用異地備援之後，複寫的資料將會在一天內遭到刪除。

1. 在 Cyber Protect 主控台中，移至 **[設定]** > **[系統設定]**。
2. 捲動備份選項清單，然後按一下 **[異地備援雲端儲存]**。
3. 停用 **[異地備援雲端儲存]** 開關。
4. 輸入 **[停用]** 以確認您的選擇，然後按一下 **[停用]**。

異地複寫狀態

異地備援意味著資料會複寫到次要位置。異地複寫狀態會顯示此程序的階段。可能的狀態如下：

- **同步** — 資料已複寫到次要位置。
- **同步中** — 資料正在複寫到次要位置。此作業的持續時間取決於資料的大小。
- **暫停** — 資料複寫暫時遭到暫停。
- **已停用** — 資料複寫遭到停用。

若要在 Cyber Protect 主控台中檢查複寫狀態

1. 在 Cyber Protect 主控台中，移至 **[備份儲存]**。
2. 選擇位置和備份集。
3. 按一下 **[詳細資料]**，然後檢查**異地複寫狀態**中的狀態。

限制

- 目前複寫資料的次要位置僅適用於美國、德國和加拿大。
- 如需使用異地備援時災難復原服務限制的相關資訊，請參閱「災難復原」文件。

站台對站台 OpenVPN - 其他資訊

當您建立復原伺服器時，您要設定其**實際執行網路中的 IP 位址**及其**測試 IP 位址**。

執行容錯移轉 (在雲端執行虛擬機器)，並登入虛擬機器檢查伺服器的 IP 位址之後，您會看到**實際執行網路中的 IP 位址**。

當您執行測試容錯移轉時，只有使用僅能在復原伺服器設定中看到的**測試 IP 位址**，才能連線測試伺服器。

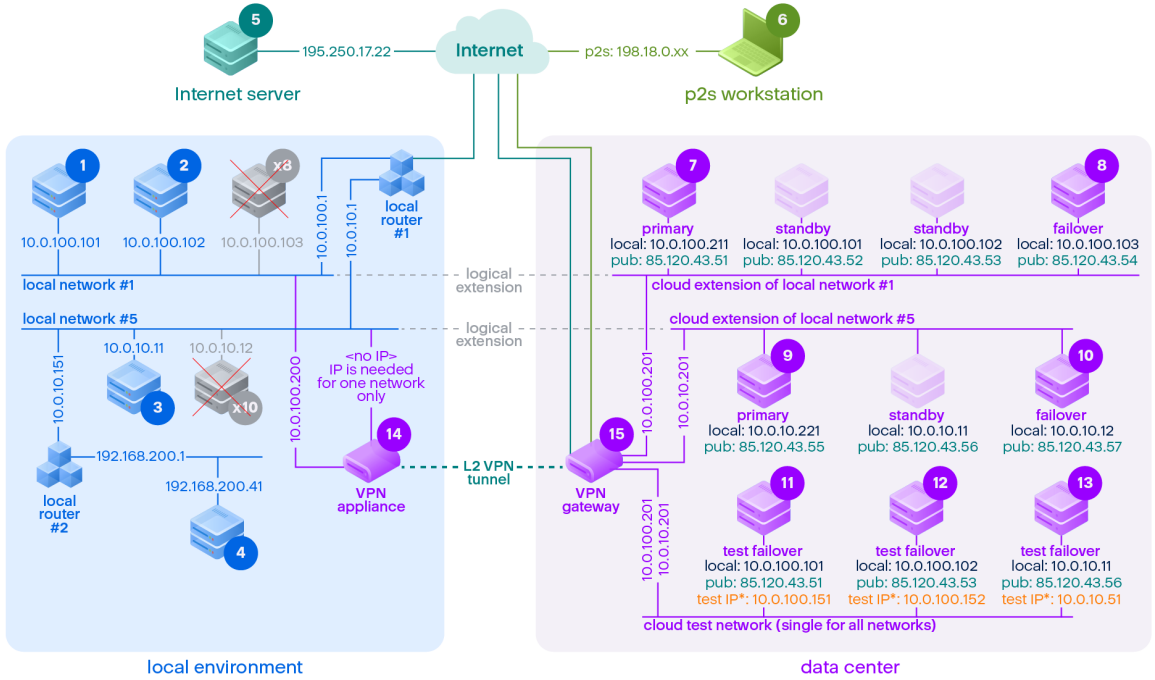
若要從本機站台連線測試伺服器，您必須使用**測試 IP 位址**。

注意事項

伺服器的網路設定一律會顯示**實際執行網路中的 IP 位址** (因為測試伺服器會鏡像實際執行伺服器的外觀)。發生這種情況是因為測試 IP 位址不屬於測試服務器，而是屬於 VPN 閘道，而且會使用 NAT 轉換為實際執行 IP 位址。

下圖顯示站台對站台 OpenVPN 設定的範例。本機環境中的部分伺服器會使用容錯移轉復原到雲端 (當網路基礎架構正常時)。

1. 客戶透過下列方式啟用 Disaster Recovery：
   a. 設定 VPN 設備 (14)，然後將其連線至雲端 VPN 伺服器 (15)
   b. 使用 Disaster Recovery (1、2、3、x8 和 x10) 保護部分本機伺服器
      本機站台上的部分伺服器 (如 4) 連線至未連線到 VPN 設備的網路。這類伺服器沒有受到 Disaster Recovery 保護。
2. 部分伺服器 (已連線到不同的網路) 在本機站台運作：(1、2、3 和 4)
3. 受保護的伺服器 (1、2 和 3) 正在使用測試容錯移轉 (11、12 和 13) 進行測試
4. 本機站台中的部分伺服器無法使用 (x8、x10)。執行容錯移轉之後，這些伺服器變得可在雲端使用 (8 和 10)
5. 連線至不同網路的部分主要伺服器 (7 和 9) 可在雲端環境中使用
6. (5) 是網際網路中擁有公用 IP 位址的伺服器
7. (6) 是使用站台對站台 VPN 連線 (p2s) 連線至雲端的工作站



在此範例中，下列連線設定可用於 (例如，"ping") **[來源：]** 列中的伺服器到 **[目的地：]** 欄中的伺服器。

	至:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
從:		本機	本機	本機	本機	網際網路	p2s	主要	容錯移轉	主要	容錯移轉	測試容錯移轉	測試容錯移轉	測試容錯移轉	VPN 設備	VPN 伺服器
1	本機		直接	透過本	透過本機路由	透過本機路由器 1 和	否	透過通道：本機	透過通道：本機	透過通道：本機	透過通道：本機	透過通道：NAT (VPN 伺	透過通道：NAT (VPN 伺	透過本機路由器 1 和通	直接	否

	至:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
				機路由器 1	器 2	網際網路		透過本機路由器 1 和網際網路：pub	透過本機路由器 1 和網際網路：pub	透過本機路由器 1 和網際網路：pub	透過本機路由器 1 和網際網路：pub	服器) 透過本機路由器 1 和網際網路：pub	服器) 透過本機路由器 1 和網際網路：pub	道：NAT (VPN 伺服器) 透過本機路由器 1 和網際網路：pub		
2	本機	直接		透過本機路由器 1	透過本機路由器 2	透過本機路由器 1 和網際網路	否	透過通道：本機 透過本機路由器 1 和網際網路：pub	透過通道：本機 透過本機路由器 1 和網際網路：pub	透過通道：本機 透過本機路由器 1 和網際網路：pub	透過通道：本機 透過本機路由器 1 和網際網路：pub	透過通道：NAT (VPN 伺服器) 透過本機路由器 1 和網際網路：pub	透過通道：NAT (VPN 伺服器) 透過本機路由器 1 和網際網路：pub	透過本機路由器 1 和通道：NAT (VPN 伺服器) 透過本機路由器 1 和網際網路：pub	直接	否
3	本機	透過本機路由器 1	透過本機路由器 1		透過本機路由器 2	透過本機路由器 1 和網際網路	否	透過通道：本機 透過本機路由器 1 和網際網路：pub	透過通道：本機 透過本機路由器 1 和網際網路：pub	透過通道：本機 透過本機路由器 1 和網際網路：pub	透過通道：本機 透過本機路由器 1 和網際網路：pub	透過通道：NAT (VPN 伺服器) 透過本機路由器 1 和網際網路：pub	透過通道：NAT (VPN 伺服器) 透過本機路由器 1 和網際網路：pub	透過本機路由器 1 和通道：NAT (VPN 伺服器) 透過本機路由器 1	透過本機路由器	否

	至:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
														和網際網路：pub		
4	本機	透過本機路由器 2 和路由器 1	透過本機路由器 2 和路由器 1	透過本機路由器 2		透過本機路由器 2 和路由器 1 和網際網路	否	透過本機路由器 2 和通道：本機 透過本機路由器 2 和本機路由器 1 和網際網路：pub	透過本機路由器 2 和通道：本機 透過本機路由器 2 和本機路由器 1 和網際網路：pub	透過本機路由器 2 和通道：本機 透過本機路由器 2 和本機路由器 1 和網際網路：pub	透過本機路由器 2 和通道：本機 透過本機路由器 2 和本機路由器 1 和網際網路：pub	透過通道：NAT (VPN 伺服器) 透過本機路由器 2 和路由器 1 和網際網路：pub	透過通道：NAT (VPN 伺服器) 透過本機路由器 2 和路由器 1 和網際網路：pub	透過通道：NAT (VPN 伺服器) 透過本機路由器 2 和路由器 1 和網際網路：pub	透過本機路由器 2	否
5	網際網路	否	否	否	否		不適用	透過網際網路：pub	透過網際網路：pub	透過網際網路：pub	透過網際網路：pub	透過網際網路：pub	透過網際網路：pub	透過網際網路：pub	否	否
6	p2s	否	否	否	否	透過網際網路		透過 p2s VPN (VPN 伺服器)：本機 透過網際網路：pub	透過 p2s VPN (VPN 伺服器)：本機 透過網際網路：pub	透過 p2s VPN (VPN 伺服器)：本機 透過網際網路：pub	透過 p2s VPN (VPN 伺服器)：本機 透過網際網路：pub	透過 p2s VPN - NAT (VPN 伺服器) 透過網際網路：pub	透過 p2s VPN - NAT (VPN 伺服器) 透過網際網路：pub	透過 p2s VPN - NAT (VPN 伺服器) 透過網際網路：pub	否	否
7	主要	透過通道	透過通道	透過通道	透過通道和本機路	透過網際網路 (透過 VPN 伺	否		在雲端直接：本機	透過通道和本機路由器 1：本機	透過通道和本機路由器 1：本機	透過 VPN 伺服器：NAT	透過 VPN 伺服器：NAT	透過通道和本機路由器 1：NAT	否	僅限 DHCP 和 DNS 通訊協

	至:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
				和本機路由器 1	由器 1 和 2	服器)										定
8	容錯移轉	透過通道	透過通道	透過通道和本機路由器 1	透過通道和本機路由器 1 和 2	透過網際網路 (透過 VPN 伺服器)	否	在雲端直接：本機		透過通道和本機路由器 1：本機	透過通道和本機路由器 1：本機	透過 VPN 伺服器：NAT	透過 VPN 伺服器：NAT	透過通道和本機路由器 1：NAT	否	僅限 DHCP 和 DNS 通訊協定
9	主要	透過通道和本機路由器 1	透過通道和本機路由器 1	透過通道	透過通道	透過網際網路 (透過 VPN 伺服器)	否	透過通道和本機路由器 1：本機	透過通道和本機路由器 1：本機		在雲端直接：本機	透過通道和本機路由器 1：NAT	透過通道和本機路由器 1：NAT	透過 VPN 伺服器：NAT	否	僅限 DHCP 和 DNS 通訊協定
10	容錯移轉	透過通道和本機路	透過通道和本機路	透過通道	透過通道	透過網際網路 (透過 VPN 伺	否	透過通道和本機路由器 1：本機	透過通道和本機路由器 1：本機	在雲端直接：本機		透過通道和本機路由器 1：NAT	透過通道和本機路由器 1：NAT	透過 VPN 伺服器：NAT	否	僅限 DHCP 和 DNS 通訊協

	至:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		由器 1	由器 1			服器)										定
11	測試容錯移轉	否	否	否	否	透過網際網路 (透過 VPN 伺服器)	否	否	否	否	否		在雲端直接:本機	透過 VPN 伺服器:本機 (路由)	否	僅限 DHCP 和 DNS 通訊協定
12	測試容錯移轉	否	否	否	否	透過網際網路 (透過 VPN 伺服器)	否	否	否	否	否	在雲端直接:本機		透過 VPN 伺服器:本機 (路由)	否	僅限 DHCP 和 DNS 通訊協定
13	測試容錯移轉	否	否	否	否	透過網際網路 (透過 VPN 伺服器)	否	否	否	否	否	透過 VPN 伺服器:本機 (路由)	透過 VPN 伺服器:本機 (路由)		否	僅限 DHCP 和 DNS 通訊協定
14	VPN 設備	直接	直接	透過本機路由器 1	透過本機路由器 2	透過網際網路 (本機路由器 1)	否	否	否	否	否	否	否	否		否
15	VPN	否	否	否	否	否	否	否	否	否	否	否	否	否	否	

	至:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	伺服器															

辭彙表

R

Runbook

[災難復原] 計劃的案例，其中包含可自動執行災難復原動作的可設定步驟。

U

USB 裝置資料庫

[裝置控制] 裝置控制模組會維護 USB 裝置的資料庫，您可以從該資料庫中，將 USB 裝置新增到裝置存取控制的排除清單。此資料庫會依裝置 ID 註冊 USB 裝置，您可以手動輸入或從 Cyber Protect 主控台中的已知裝置選擇。

V

VPN 設備

[災難復原] 特殊的虛擬機器，可透過安全的 VPN 通道，在區域網路和雲端站台之間連線。VPN 設備是在本機站台上部署的。

VPN 閘道 (前身為 VPN 伺服器或連線閘道)

[災難復原] 特殊的虛擬機器，可透過安全的 VPN 通道，提供本機站台和雲端站台網路間的連線。VPN 閘道是在雲端站台上部署的。

公

公共 IP 位址

[災難復原] 讓雲端伺服器可以從網際網路使用所需的 IP 位址。

主

主要伺服器

[災難復原] 在本機站台 (例如，復原伺服器) 上沒有連結電腦的虛擬機器。主要伺服器用於保護應用程式或執行各種輔助服務 (例如，網頁伺服器)。

本

本機站台

[災難復原] 在公司內部部署上部署的本機基礎架構。

完

完整備份

包含已選要備份的所有資料的獨立備份。您無需存取任何其他備份來從完整備份復原資料。

孤

孤立備份

孤立備份是與保護計劃不再有關聯的備份。

保

保護代理程式

保護代理程式是要安裝在電腦上以保護資料的代理程式。

保護計劃

保護計劃是一種結合資料保護模組的計劃，包括備份、防毒和防惡意程式保護、URL 篩選、Windows Defender 防毒軟體、Microsoft Security Essentials、弱點評估、修補程式管理、資料保護圖、裝置控制。

容

容錯回復

將工作負載從備用伺服器 (例如，虛擬機器複本或在雲端執行的復原伺服器) 切換回實際執行

伺服器。

容錯移轉

將工作負載從實際執行伺服器切換到備用伺服器 (例如，虛擬機器複本或在雲端執行的復原伺服器)。

差

差異備份

差異備份能對照最新的完整備份，儲存資料的變更。您需要存取相對應的完整備份，以從差異備份復原資料。

站

站台對站台 (S2S) 連線

[災難復原] 將區域網路透過安全的 VPN 通道延伸至雲端的連線。

備

備份集

可套用個別保留規則的一組備份。如果是 [自訂] 備份配置，備份集會對應備份方法 ([完整]、[差異] 與 [增量])。在其他所有案例中，備份集為 [每月]、[每天]、[每週] 與 [每小時]。每月備份指的是當月一開始所建立的第一個備份。每週備份指的是在 [每週備份] 選項中 (按一下齒輪圖示，然後再按一下 [備份選項] > [每週備份]) 選擇的那一天所建立的第一個備份。如果每週備份指的是每月一開始所建立的第一個備份，則此備份會被視為每月備份。在此情況下，每週備份將會在下一週選擇的那天建立。除非此備份落在每月或每週備份的定義範圍內，否則每日備份指的是每日一開始所建立的第一個備份。除非此備份落在每月、每週或每日備份的定義範圍內，否則每小時備份指的是每小時一開始所建立的第一個備份。

單

單一檔案備份格式

備份格式，會將初始完整備份及後續增量備份儲存為單一的 .tibx 檔案。此格式可以善用了增量備份方法的速度，同時避免其主要的缺點 - 不容易刪除過期備份。軟體會將過期備份所使用的區塊標示為「可用」，並在區塊中寫入新備份。結果會以耗費最少資源的方式，產生極快速的清理。備份至不支援隨機存取讀寫的位置時，無法使用單一檔案備份格式。

復

復原伺服器

[災難復原] 原始電腦的 VM 複本，以儲存在雲端的受保護伺服器備份為基礎。復原伺服器在發生災難時，用於從原始伺服器切換工作負載。

復原點目標 (RPO)

[災難復原] 因電力中斷而遺失的資料量，以計劃的電力中斷或災難事件發生的時間量計算。RPO 閥值會定義上次適合容錯移轉的復原點和目前時間之間允許的最大時間間隔。

最

最終化

將從備份執行的臨時虛擬機器變成永久虛擬機器的作業。實際上，這表示將所有虛擬機器磁碟，以及在電腦執行時發生的變更，復原至儲存這些變更的資料存放區。

測

測試 IP 位址

[災難復原] 測試容錯移轉時所需的 IP 位址，可防止實際執行 IP 位址重複。

測試網路

[災難復原] 隔離的虛擬網路，用於測試容錯移轉程序。

虛

虛擬機器

外部代理程式 (例如 VMware 用代理程式或 Hyper-V 用代理程式) 在 Hypervisor 層級備份的虛擬機器。從備份觀點來看，內部具有代理程式的虛擬機器會被視為實體機器。

雲

雲端伺服器

[災難復原] 復原或主要伺服器的一般參考。

雲端站台 (或 DR 網站)

[災難復原] 在雲端託管並用於執行復原基礎架構的遠端站台 (萬一發生災難)。

裝

裝置控制模組

裝置控制模組運用每個受保護電腦上的資料洩漏防禦代理程式功能子集，偵測並防止本機電腦通道上未經授權的資料存取和傳輸，作為保護計劃的一部分。這些包括使用者對週邊裝置和連接埠的存取、文件列印、剪貼簿複製/貼上作業、媒體格式化和退出作業，以及與本機連線行動裝置的同步。裝置控制模組對允許使用者在受保護的電腦上存取的裝置和連接埠的類型，以及使用者可以在這些裝置上執行的動作，提供精細的情境控制。

資

資料洩漏防禦 (先前稱為資料外洩防禦)

一種整合式技術和組織措施的系統，旨在偵測和防止組織內外部未經授權的實體有意和無意地洩露/存取機密、受保護或敏感的資料，或將此類資料傳輸到不受信任的環境。

資料洩漏防禦代理程式

資料洩漏防禦系統的用戶端元件，可透過套用環境和內容分析技術的組合，並強制執行集中管理的資料洩漏防禦政策，保護其主機電腦，免於未經授權者使用、傳輸和儲存機密、受保護或敏感的資料。網路保護提供一個功能全面的資料洩漏防禦代理程式。但是，代理程式在受保護電腦上的功能受限於網路保護授權使用的一組資料洩漏防禦功能，並取決於套用至該電腦的保護計劃。

實

實際執行網路

[災難復原] 透過 VPN 通道延伸，並涵蓋本機和雲端站台的內部網路。本機伺服器和雲端伺服器可以在實際執行網路中彼此通訊。

實體電腦

作業系統中所安裝之代理程式備份的電腦。

增

增量備份

這種備份能對照最新的備份，儲存資料的變更。您需要存取其他備份，以便從增量備份中復原資料。

模

模組

模組是保護計劃的一部分，可提供特定的資料保護功能，例如，備份模組、防毒和防惡意程式保護模組等等。

點

點對站台 (P2S) 連線

[災難復原] 使用端點裝置 (例如電腦或筆記型電腦), 從外部到雲端和本機站台進行的安全 VPN 連線。

驗

驗證

此作業會檢查從備份復原資料的可能性。驗證檔案備份會模擬將所有檔案從備份復原到虛擬目的地。磁碟備份的驗證作業會計算備份中所儲存之各資料區塊的檢查碼。這兩個程序都屬於資源密集型。儘管成功驗證代表成功復原的可能性很高, 但無法檢查影響復原過程的所有因素。

索引

S

U

V

W

X

比

主

代

以

功

加

可

失

它

必

多

如

究

系

防

事

使

依

其

具

初

協

取

受

固

定

客

建

後

指

按

活

為

執

基

密

將

從

移

符

組

脫

處

被

規

設

軟

透

逐

連

部

備

單

報

復

惡

描

智

最

測

無

登

發

硬

程

新

概

準

節

萬

裝

解

資

磁

管

網

與

語

遠

需

範

編

複

調

適

篩

選

瞭

聲

還

隱

點

叢

擷

瀏

舊

轉

雙

關

警

續

驅

權

鑑

變

驗