Acronis

acronis.com

Acronis Cyber Protect 15

Update 6

使用指南

版本：2023/6/15

目錄

版權聲明

Acronis 專利技術

本產品使用之技術受以下一項或多項美國專利號碼保障及保護：7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; 與申請中的專利。

Acronis Cyber Protect 15 版本

Acronis Cyber Protect 15 可在下列版本中使用：

- Cyber Protect Essentials
- Cyber Protect Standard
- Cyber Protect Advanced
- Cyber Backup Standard
- Cyber Backup Advanced

如需有關各版本隨附功能的詳細資訊，請參閱「包括雲端部署在內的Acronis Cyber Protect 15 版本比較」。

Acronis Cyber Protect 15 的所有版本都是依照受保護的工作負載數目及其類型 (工作站、伺服器和虛擬主機) 授權。Cyber Protect 版本僅提供訂購授權。Cyber Backup 版本則同時提供訂購授權和永久授權。如需有關可用選項的詳細資訊，請參閱 "授權" (第 21 頁)。

第 15 版的永久授權金鑰無法搭配 Acronis Cyber Backup 12.5 的備份代理程式使用。但是，即使其管理伺服器升級到第 15 版，這些代理程式還是將繼續使用舊的授權金鑰。

即使代理程式升級到第 15 版，備份訂購授權還是可以搭配第 12.5 版代理程式使用。Cyber Protect 訂購授權僅能由第 15 版代理程式使用。

在 15 版管理伺服器上註冊的 12.5 版備份代理程式無法執行脫離主機資料處理作業，例如備份複寫、備份驗證、清理，或是轉換至虛擬機器。

注意事項
不同版本的功能會有所不同。您的授權可能無法使用本文件中所述的部分功能。如需有關各版本隨附功能的詳細資訊，請參閱「包括雲端部署在內的Acronis Cyber Protect 15 版本比較」。

作業系統支援的 Cyber Protect 功能。

下列作業系統支援 Cyber Protect 功能：

- Windows：Windows 7 和更新版本、Windows Server 2008 R2 和更新版本。
  Windows 8.1 和更新版本支援 Windows Defender 防毒軟體管理。
- Linux：CentOS 7.x、CentOS 8.0、Virtuozzo 7.x、Acronis Cyber Infrastructure 3.x。
  其他 Linux 發行版和版本可能也支援 Cyber Protect 功能，但尚未經過測試。
- macOS：10.13.x 和更新版本 (僅防毒和反惡意程式碼保護受到支援)。

重要事項
只有已安裝保護代理程式的電腦支援 Cyber Protect 功能。對於在無代理程式模式下受到 (例如，Hyper-V 用代理程式、VMware 用代理程式或 Scale Computing 用代理程式) 保護的虛擬機器，只有備份受到支援。

Cyber Protect 功能	Windows	Linux	macOS

鑑識備份	是	否	否
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
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
手動新增裝置	是	否	否
Acronis 反惡意程式碼保護			
根據程序行為 (基於 AI) 進行勒索軟體偵測	是	否	否
加密採礦程序偵測	是	否	否
即時反惡意軟體防護	是	否	是
從本機快取自動復原受影響的檔案	是	否	否
Acronis 備份檔案的自我保護	是	否	否
Acronis 軟體的自我保護	是	否	否
針對可攜式可執行檔進行靜態分析	是	否	是*
外接磁碟機保護 (HDD、快閃磁碟機、SD 卡)	是	否	否
網路資料夾保護	是	否	否
伺服器端保護	是	否	否
保護 Zoom、WebEx、Microsoft Teams 以及其他遠端工作保護	是	否	否
按需反惡意程式碼掃描	是	否	是
掃描存檔檔案	是	否	是
檔案/資料夾排除	是	否	是**
程序排除	是	否	否

全公司的白名單	是	否	是
行為偵測	是	否	否
隔離	是	否	是
URL 篩選 (http/https)	是	否	否
Windows Defender 防毒管理	是	否	否
Microsoft Security Essentials 管理	是	否	否
弱點評估			
作業系統及其原生應用程式的弱點評估	是	是***	否
適用於協力廠商應用程式的弱點評估	是	否	否
修補程式管理			
修補程式自動核准	是	否	否
修補程式手動安裝	是	否	否
自動排程修補程式安裝	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,則取消電腦重新啟動	是	否	否
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
資料保護圖中的保護動作	是	否	否
磁碟健全狀況			
基於 AI 的 HDD 和 SSD 健全狀況控制	是	否	否
以 Acronis 網路保護營運中心 (CPOC) 警示為基礎的智慧型保護計劃			
威脅饋送	是	否	否
修復精靈	是	否	否
備份掃描			

掃描加密備份	是	否	否
掃描本機儲存空間、網路共用以及 Acronis Cloud Storage 中的磁碟備份	是	否	否
安全復原			
在復原過程中，使用 Acronis 防毒和反惡意程式碼保護進行反惡意程式碼掃描	是	否	否
遠端桌面			
透過 HTML5 型用戶端連線	是	否	否
透過原生 Windows RDP 用戶端連線	是	否	否
遠端抹除	是****	否	否
Cyber Protect 監視器	是	否	是

* 在 macOS 上，只有排程掃描才支援針對可攜式可執行檔進行靜態分析。

** 在 macOS 上，您僅能使用排除來指定即時保護或排程掃描將不會掃描的檔案和資料夾。

*** 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。

**** 遠端抹除僅適用於執行 Windows 10 或更新版本的電腦。

授權

若要透過使用 Acronis Cyber Protect 來保護工作負載，則需要授權。安裝 Acronis Cyber Protect 無需授權。

授權類型

Acronis Cyber Protect 適用於訂購授權。自購買日起的有效期限內，提供無限更新和免費技術支援。有效期限結束後，現有的保護計劃會停止運作，也無法建立新的保護計劃。

我們提供舊版永久授權續訂。部分功能 (例如雲端部署或雲端對雲端備份) 不適用於永久授權。

我們也提供試用版授權。此授權為您提供自授權啟用起 30 天存取所有產品功能。

如需有關不同授權選項的更多詳細資料，請參閱知識庫的 Acronis Cyber Protect 15: 授權與升級/降級常見問答。Acronis 授權政策位於以下網址：https://www.acronis.com/company/licensing.html

重要事項
Acronis Cyber Protect 15 Update 3 引入了新的授權模型。它需要授權註冊和內部部署管理伺服器的啟用。

Acronis Cyber Protect 15 Update 3 或更新版本中的授權

在 Acronis Cyber Protect 15 Update 3 或更新版本中，管理伺服器 (`https://<您管理伺服器的 IP 位址>:<連接埠>`) 的本機主控台中不會新增任何授權金鑰。

反之，要將授權新增至您在 Acronis 客戶入口網站 (`https://account.acronis.com`) 中的帳戶，然後在 Acronis Cyber Protect 雲端主控台 (`https://cloud.acronis.com`) 中管理您的授權。

離線管理伺服器的授權管理需要在本機和雲端主控台操作。

若要深入瞭解本機和雲端主控台，請參閱 "Acronis 帳戶，本機和雲端主控台" (第 23 頁)。

若要開始使˙用具備 Acronis Cyber Protect 15 Update 3 或更新版本的管理伺服器

1. 在 Acronis 客戶入口網站 (`https://account.acronis.com`) 中，將一或多個授權新增至您的帳戶。您在線上購買的授權會自動新增到此帳戶中。
2. [針對內部部署部署模式] 啟用管理伺服器。
3. 將授權配置到管理伺服器。

管理伺服器類型

視您的部署方法而定，您可以使用以下類型的管理伺服器：

- 雲端管理伺服器
- 內部部署管理伺服器
  - 線上管理伺服器
  - 離線管理伺服器

在您的 Acronis 帳戶中，可以擁有多個管理伺服器。您也可以使用具備雲端管理伺服器與內部部署管理伺服器的混合部署模型。

如果使用多個管理伺服器，您可以在它們之間分割授權配額。如需有關操作方式的詳細資訊，請參閱 "將授權配額傳輸至另一台管理伺服器" (第 31 頁)。

雲端管理伺服器

使用雲端部署，您無需在您的網路內安裝及維護管理伺服器。您使用的是已部署在 Acronis 資料中心內的管理伺服器，您只需為您的工作負載安裝保護代理程式即可。

雲端管理伺服器不需要啟用。它始終在線上，而且授權資訊會在伺服器與您的 Acronis 帳戶之間自動同步。

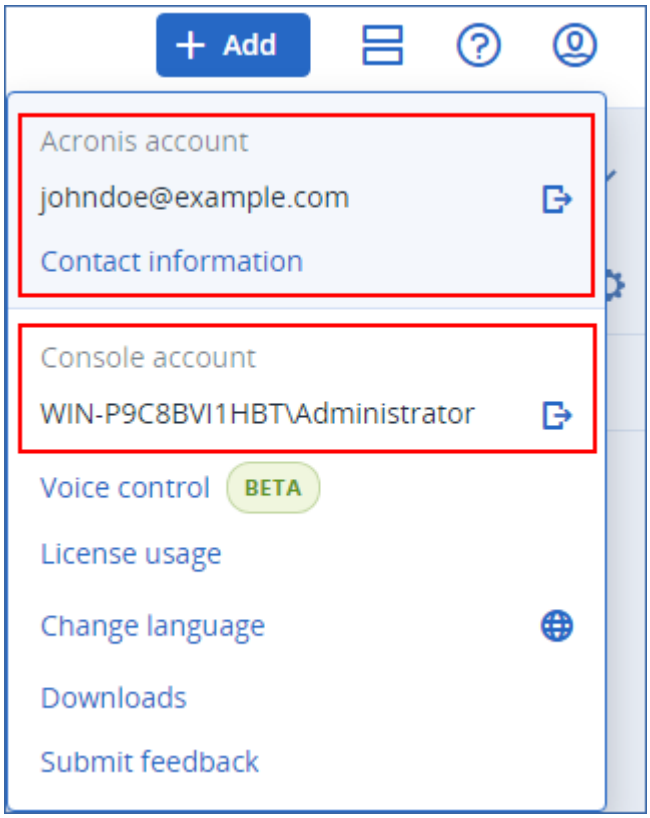
內部部署管理伺服器

使用內部部署，您要在您的網路中安裝管理伺服器和保護代理程式。您可以擁有不連線至網際網路的離線管理伺服器，也可以擁有可存取網際網路的線上管理伺服器。

內部部署管理伺服器需要啟用。如需有關啟用的詳細資訊，請參閱 "啟用管理伺服器" (第 25 頁)。

注意事項

在已啟用的內部部署管理器的本機主控台中，會顯示兩個不同帳戶：Acronis帳戶，用於同步授權資訊；以及主控台帳戶，用於存取本機主控台本身。



線上內部部署管理伺服器

當您首次存取本機主控台時，藉著登入您的 Acronis 帳戶，可透過網際網路啟用線上管理伺服器。

離線內部部署管理伺服器

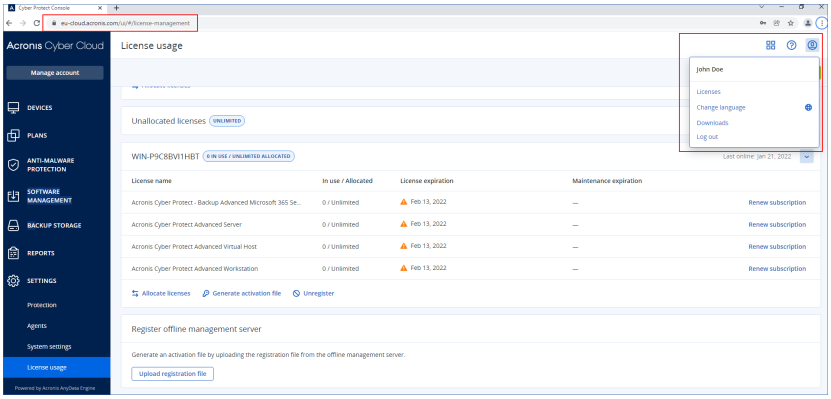
透過檔案，手動啟用離線管理伺服器並將其授權資訊與您的 Acronis 帳戶同步。

Acronis 帳戶，本機和雲端主控台

若要使用 Acronis Cyber Protect 及管理授權和其使用狀況，則需要 Acronis 帳戶。您的所有授權和管理伺服器都會註冊到該帳戶。

使用此帳戶，您可存取下列主控台：

- 雲端主控台 (https://cloud.acronis.com)

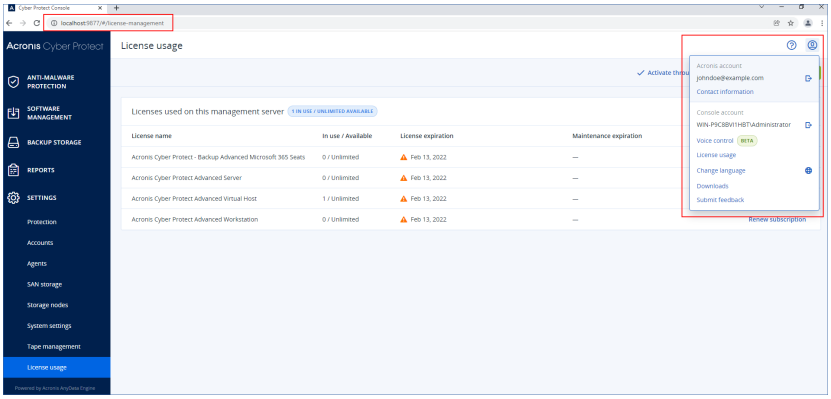


注意事項

在您登入雲端主控台之後，其 URL 會變更並顯示您帳戶所屬的確切資料中心。例如，https://eu-cloud.acronis.com 或 https://jp-cloud.acronis.com。

雲端主控台是您管理授權的主要位置。此處，在 **[設定]** > **[授權使用狀況]** 索引標籤上，您可以將可用授權和授權配額配置給特定管理伺服器、將授權配額重新配置給另一個管理伺服器，或是完成離線管理伺服器的註冊。

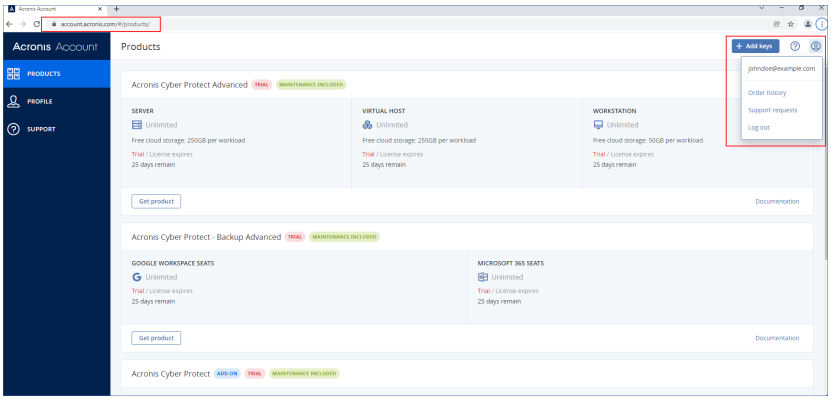
- 內部部署管理伺服器的本機主控台 (https://<您管理伺服器的 IP 位址>:<連接埠>)



此處可以檢查已配置的授權、其配額和使用狀況，以及其到期日。

當您啟用離線管理伺服器或將授權配置給它時，可使用本機主控台搭配雲端主控台。

- Acronis 客戶入口網站 (https://account.acronis.com)



在 Acronis 客戶入口網站中，您可以管理所購買的產品，例如，檢查您的訂購授權到期日、新增新的授權金鑰、註冊授權續訂，或要求升級。您也可以聯絡支援小組、下載產品安裝檔案，以及存取產品文件。

管理授權

下表摘要了可用操作，並顯示從何處執行它們。

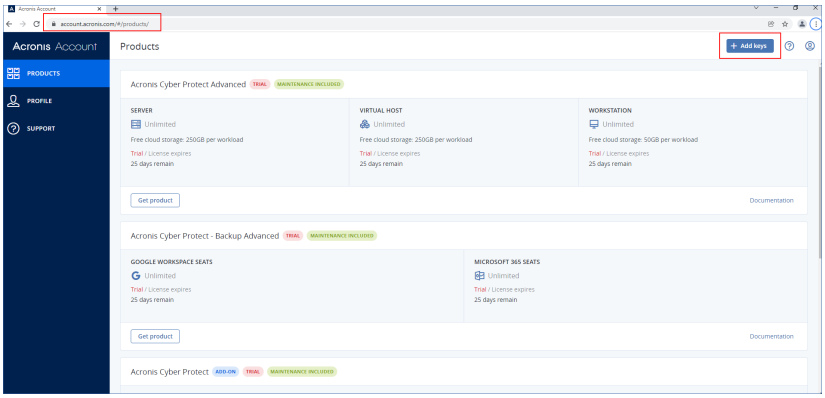
作業	位置
新增授權至您的帳戶	您要在 Acronis 客戶入口網站 (https://account.acronis.com) 中新增授權。該處會自動新增您在線上購買的授權。
啟用管理伺服器	您可透過在您的帳戶中註冊管理伺服器來啟用它。 透過登入您的 帳戶，您可在線上管理伺服器的本機主控台 (https://<您管理伺服器的 IP 位址>:<連接埠>) 中啟用線上管理伺服器。 離線管理伺服器的啟動需要在本機和雲端主控台操作。
將授權配置給管理伺服器 修改現有授權配置	在線上管理伺服器上，可使用雲端主控台 (https://cloud.acronis.com) 來配置授權。所配置的授權會自動同步至管理伺服器。 在離線管理伺服器上，要透過啟用檔案來配置授權。此程序需要使用管理伺服器 (https://<您管理伺服器的 IP 位址>:<連接埠>) 的本機主控台，以及雲端主控台 (https://cloud.acronis.com)。
將授權指派給工作負載	此作業為自動。
從您的帳戶取消註冊管理伺服器	透過使用雲端主控台 (https://cloud.acronis.com)，您可取消註冊線上管理伺服器。 取消註冊離線管理伺服器則要透過停用檔案。此程序需要使用離線管理伺服器 (https://<您管理伺服器的 IP 位址>:<連接埠>) 的本機主控台，以及雲端主控台 (https://cloud.acronis.com)。 若要取消註冊您沒有存取權的離線管理伺服器，則只能使用雲端主控台。

新增授權至您的 Acronis 帳戶

若要使用授權，您必須將它新增至您的 Acronis 帳戶中。您在線上購買的授權會自動新增到您的帳戶中。您必須手動新增離線購買的授權。

若要新增授權至您的 Acronis 帳戶中

1. 使用您的帳戶認證登入 Acronis 客戶入口網站 (https://account.acronis.com)。
2. 在導覽功能表中，按一下 **[產品]**。
3. 按一下 **[新增金鑰]**。



4. 輸入一或多個授權金鑰，每行一個，然後按一下 **[新增]**。

> **注意事項**
> 您最多可以同時輸入 100 個授權金鑰。

授權現已新增至您的帳戶，您可以在雲端主控台 (https://cloud.acronis.com) 中管理其使用狀況。

重要事項

在升級至 Acronis Cyber Protect 15 Update 3 之前，將儲存在本機的永久授權匯出至檔案，然後將它們新增至您的 Acronis 帳戶。

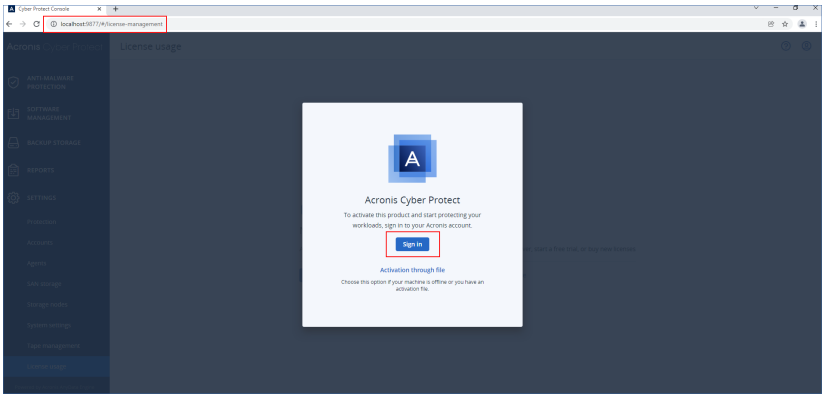
若要檢查您在管理伺服器上以本機方式輸入的授權金鑰，請前往 `https://<您管理伺服器的 IP 位址>:<連接埠>/api/account_server/v2/licensing/legacy/license_keys`。

啟用管理伺服器

您可透過在 Acronis 帳戶中註冊管理伺服器來啟用它。

若要啟用註冊線上管理伺服器

1. 在安裝 Acronis Cyber Protect 管理伺服器之後，開啟其本機主控台 (`https://<IP address of your management server>:<port>`)。
2. 在開啟的對話方塊中，按一下 **[登入]**。



3. 登入您的 Acronis 帳戶。

結果，會自動註冊及啟用管理伺服器。

若要開始保護您的工作負載，請將至少一個授權配置給此伺服器。如需有關配置授權的詳細資訊，請參閱 "將授權配置給管理伺服器" (第 29 頁)。

注意事項

線上管理伺服器需要網際網路存取，以將授權資訊同步到您的 Acronis 帳戶。如果這類伺服器離線超過 30 天，其保護計劃將會停止運作，而您的工作負載將變成不受保護。

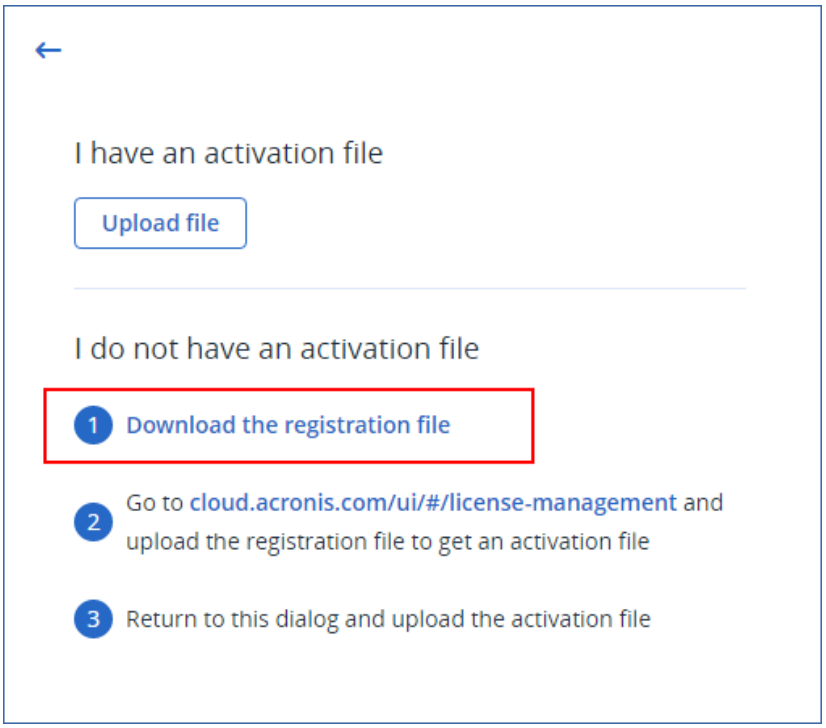
如果您從本機主控台登出您的 Acronis 帳戶，則無法同步授權資訊。如果您在 30 天內未再次登入，則保護計劃將會停止運作，而您的工作負載將變成不受保護。

若要啟用離線管理伺服器

離線管理伺服器的啟動需要在本機和雲端主控台操作。

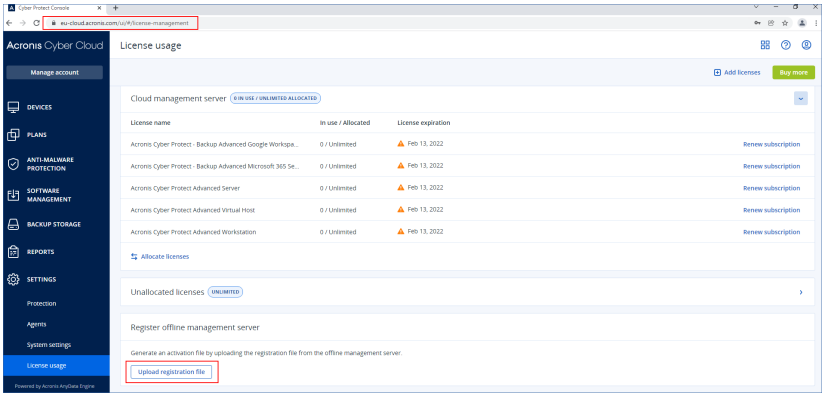
若要存取雲端主控台，您需要第二部已連線至網際網路的電腦。

1. 在安裝 Acronis Cyber Protect 管理伺服器之後，開啟其本機主控台 (`https://`<您管理伺服器的 IP 位址>:<連接埠>)。
2. 在開啟的對話方塊中，按一下 **[透過檔案啟用]**。
3. 在 **[我沒有啟用檔案]** 底下，按一下 **[下載註冊檔案]**。



註冊檔案會下載到您的電腦中。

4. 在可存取網際網路的電腦上，登入雲端主控台 (https://cloud.acronis.com)，然後前往 **[設定]** > **[授權使用狀況]**。
5. 在 **[註冊離線管理伺服器]** 區段中，按一下 **[上傳註冊檔案]**。



6. 在開啟的對話方塊中，按一下 **[瀏覽]**，然後選擇您從離線管理伺服器中下載的註冊檔案。
7. 在開啟的對話方塊中，按一下 **[下載檔案]**。

啟用檔案會下載到您的電腦中。

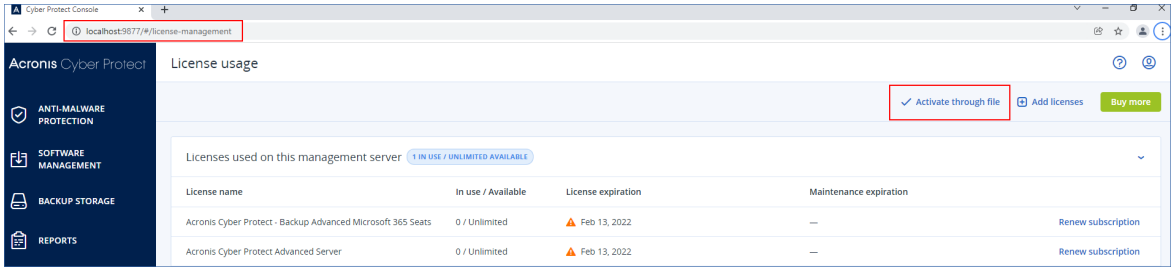
重要事項

如果此離線管理伺服器是您環境中唯一的管理伺服器，那麼您的 Acronis 帳戶中的授權將會自動配置給它。啟用檔案將會包含此資訊，因此不需要額外配置。

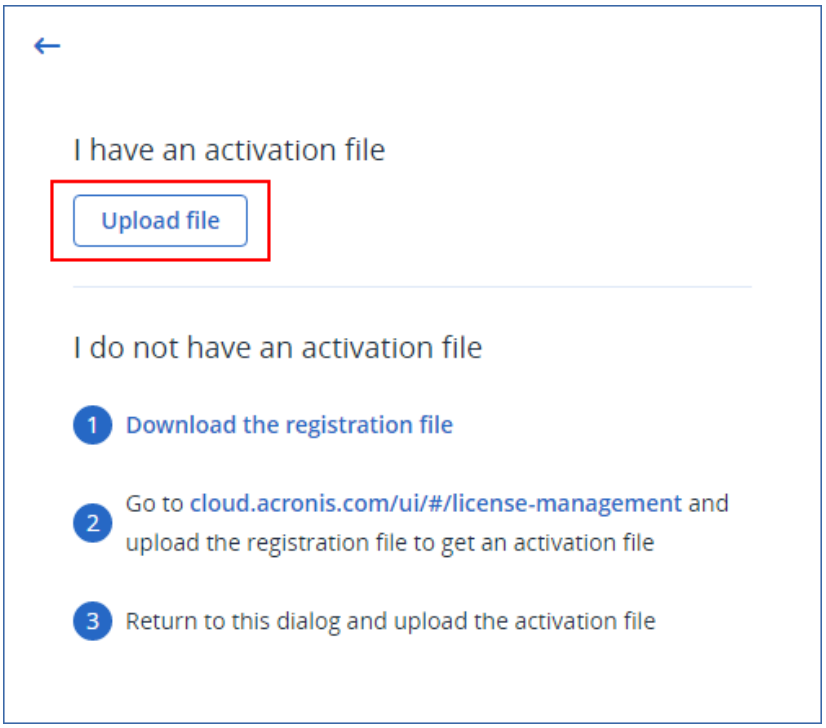
如果這不是您環境中唯一的管理伺服器，則在啟用之後，必須遵照 "將授權配置給管理伺服器" (第 29 頁) 中的程序配置授權。

8. 在離線管理伺服器 (https://<您管理伺服器的 IP 位址>:<連接埠>) 的本機主控台中，前往 **[透過檔案啟用]** 對話方塊。

注意事項
如果 **[透過檔案啟用]** 對話方塊未開啟，請瀏覽至 **[設定]** > **[授權使用狀況]**，然後按一下 **[透過檔案啟用]**。



9. 在 **[我有啟用檔案]** 底下，按一下 **[上傳檔案]**，然後選擇要從雲端主控台下載的啟用檔案。



完成後，離線管理伺服器就會註冊到您的 Acronis 帳戶中並啟用。

注意事項
您可能無法啟用在 UUID 非唯一的虛擬機器上執行的管理伺服器。當您複製虛擬機器的 UUID 或使用 VMware vCenter Converter 等加以轉換時，該 UUID 可能會重複。如果碰到類似問題，請聯絡我們的支援小組。

如需有關如何在 VMware 虛擬機器上防止 UUID 重複的詳細資訊，請參閱編輯具有重複 UUID.bios 的虛擬機器 (1002403)。

將授權配置給管理伺服器

若要使用授權，您必須將其配額或其配額的一部分配置給管理伺服器。您可以將一個以上的授權配置給管理伺服器。此外，也可以分割授權配額，並將配額的不同部分配置給不同的管理伺服器。

注意事項

如果您的 Acronis 帳戶中只有一個管理伺服器，您所有授權都會自動配置給該伺服器。若要瞭解如何將授權重新配置給另一台管理伺服器，請參閱 "將授權配額傳輸至另一台管理伺服器" (第 31 頁)。

如果您的 Acronis 帳戶中有一個以上的管理伺服器，則新授權會顯示在雲端伺服器 (https://cloud.acronis.com) 的 **[未配置的授權]** 底下。您必須手動配置這些授權。

授權的所有作業都會自動同步至線上管理伺服器。若要將配置變更同步至離線管理伺服器，請建立新的啟用檔案，然後重複配置程序。若要瞭解不同的管理伺服器的更多資訊，請參閱 "管理伺服器類型" (第 21 頁)。

若要將授權配置給線上管理伺服器

1. 在雲端主控台 (https://cloud.acronis.com) 中，按一下 **[設定]** > **[授權使用狀況]**。
2. 瀏覽至您要配置授權的管理伺服器。
3. 按一下 **[配置授權]**。
4. 在開啟的對話方塊中，指定您要配置給此伺服器的授權和授權配額。
5. 按一下 **[儲存]**。

完成後，授權資訊會自動同步至管理伺服器，而且您可以使用所配置的授權來保護您的工作負載。

若要修改配置，請重複上述程序。

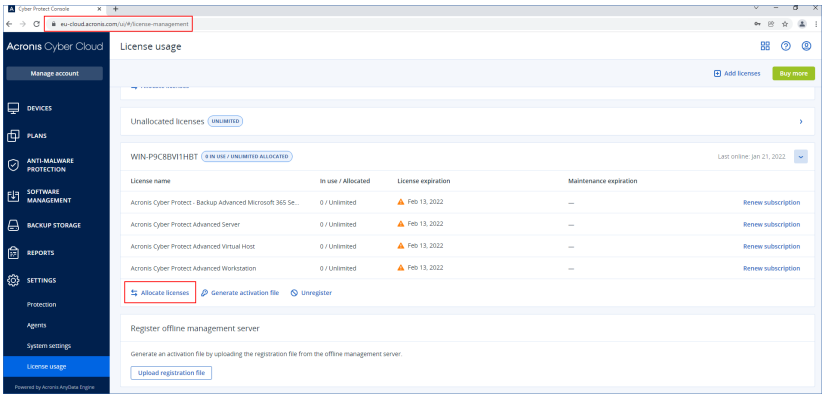
重要事項

如果修改過的授權配額小於保護代理程式數量，則負載最少的代理程式將會停止運作。此選擇為自動。如果不符合您的需求，請手動重新指派可用的授權。

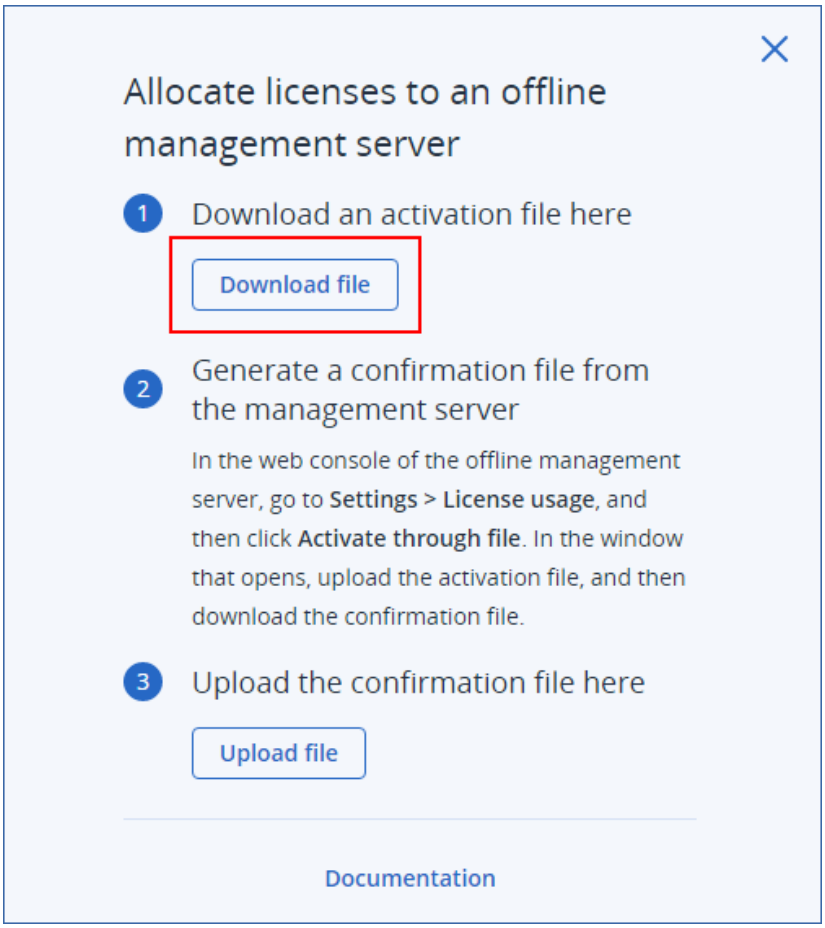
若要將授權配置給離線管理伺服器

若要將授權配置給離線管理伺服器，您必須使用雲端和本機主控台。若要存取雲端主控台，您需要第二部已連線至網際網路的電腦。

1. 在具備網際網路存取的電腦上，登入雲端主控台 (https://cloud.acronis.com)，然後按一下 **[設定]** > **[授權使用狀況]**。
2. 瀏覽至您要配置授權的管理伺服器。
3. 按一下 **[配置授權]**。

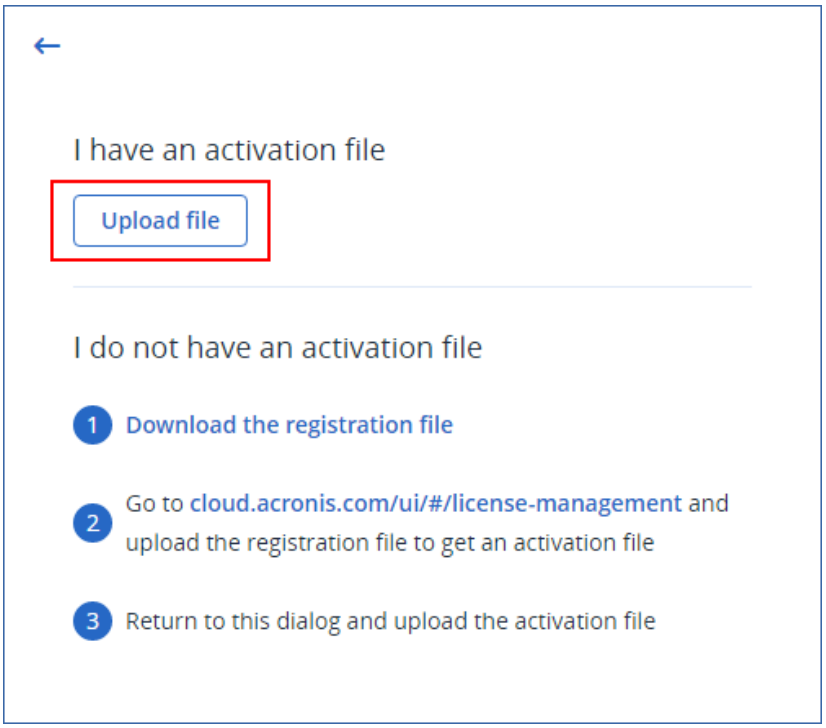


4. 在開啟的對話方塊中，指定您要配置給此伺服器的授權和授權配額。
5. 按一下 **[儲存]**。
6. 在 **[將授權配置給離線管理伺服器]** 對話方塊中，按一下 **[下載檔案]**。



啟用檔案會下載到您的電腦中。

7. 在離線管理伺服器 (`https://`<您管理伺服器的 IP 位址>:<連接埠>) 的本機主控台中，瀏覽至 **[設定]** > **[授權使用狀況]**，然後按一下 **[透過檔案啟用]**。
8. 在開啟的對話方塊中的 **[我有啟用檔案]** 底下，按一下 **[上傳檔案]**，然後選擇要從雲端主控台下載的啟用檔案。



完成後，授權資訊會在您的 Acronis 帳戶與離線管理伺服器之間同步。

若要增加所配置的授權配額，請重複上述程序。

若要減少所配置的授權配額，請參閱 "減少配置給離線管理伺服器的授權配額" (第 31 頁)。

將授權配額傳輸至另一台管理伺服器

您可以將授權配額從一台管理伺服器傳輸到另一台。當授權配置給沒有任何工作負載使用的管理伺服器，而且另一台管理伺服器需要更多授權時，此選項可能很實用。

注意事項

如果您的 Acronis 帳戶中只有一個管理伺服器，您所有授權都會自動配置給該伺服器。

如果您的 Acronis 帳戶中有一個以上的管理伺服器，則新授權會顯示在雲端伺服器 (https://cloud.acronis.com) 的 **[未配置的授權]** 底下。您必須手動配置這些授權。

若要將授權配額傳輸至另一台管理伺服器

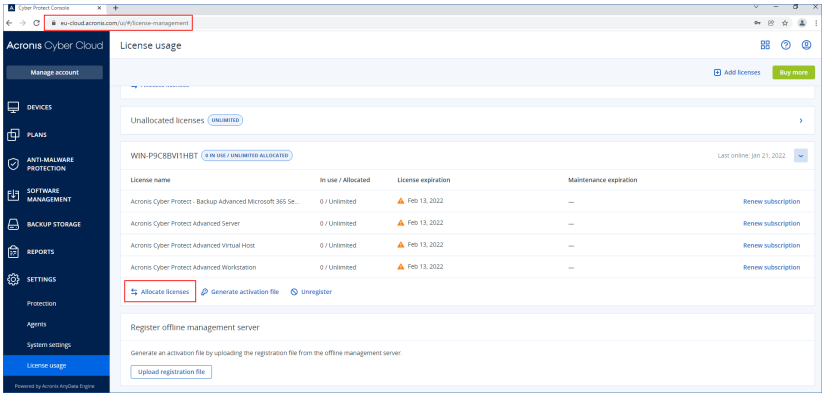
1. 透過依照 "將授權配置給管理伺服器" (第 29 頁) 中的程序，減少配置給原始管理伺服器的授權配額。

   釋放的授權配額會出現在雲端主控台中的 **[未配置的授權]** 區段中。
2. 透過依照 "將授權配置給管理伺服器" (第 29 頁) 中的程序，將授權配額配置給第二台管理伺服器。

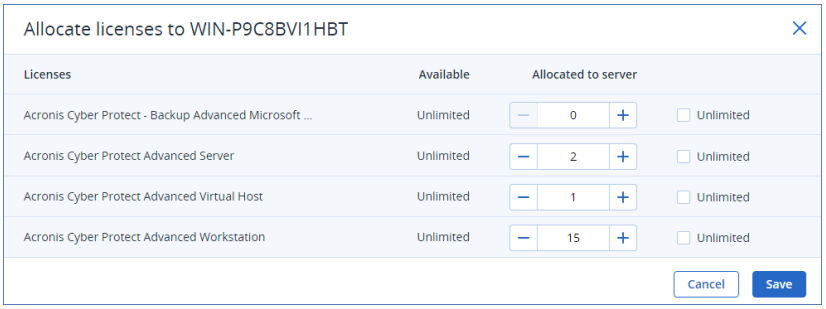
減少配置給離線管理伺服器的授權配額

若要減少已配置給離線管理伺服器的授權配額，您必須使用雲端和本機主控台。若要存取雲端主控台，您需要第二部已連線至網際網路的電腦。

1. 在可存取網際網路的電腦上，登入雲端主控台 (https://cloud.acronis.com)，然後按一下 **[設定]** > **[授權使用狀況]**。
2. 瀏覽至您要配置授權的管理伺服器，然後按一下 **[配置授權]**。

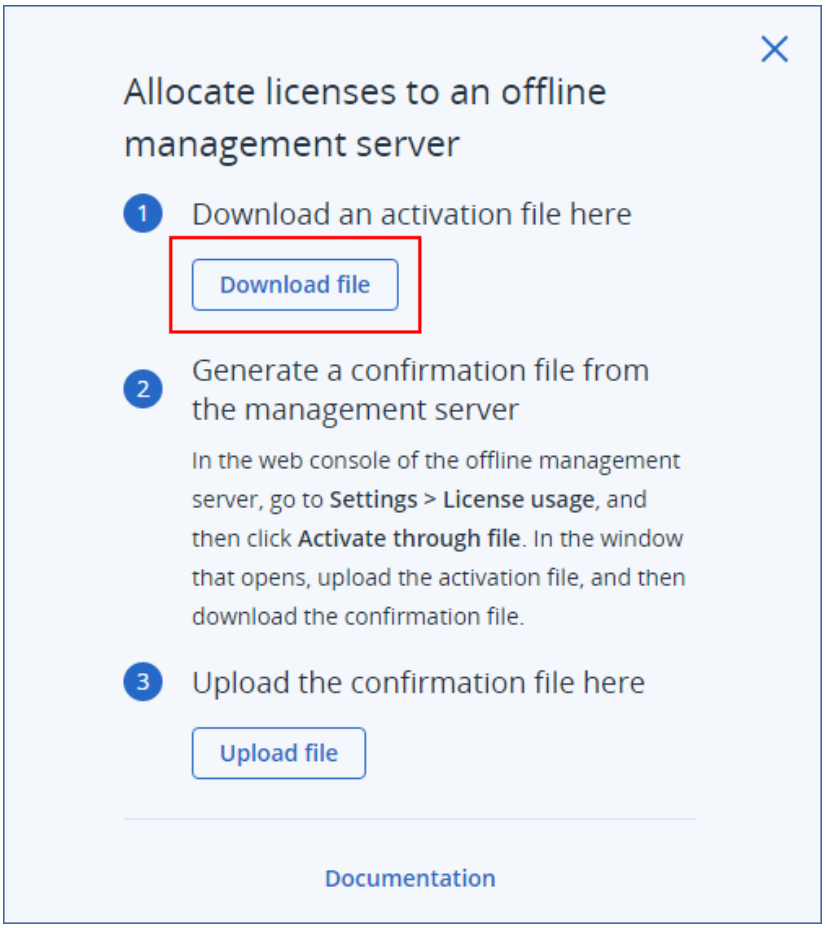


3. 在開啟的對話方塊中，修改授權和配置給此伺服器的授權配額，然後按一下 **[儲存]**。



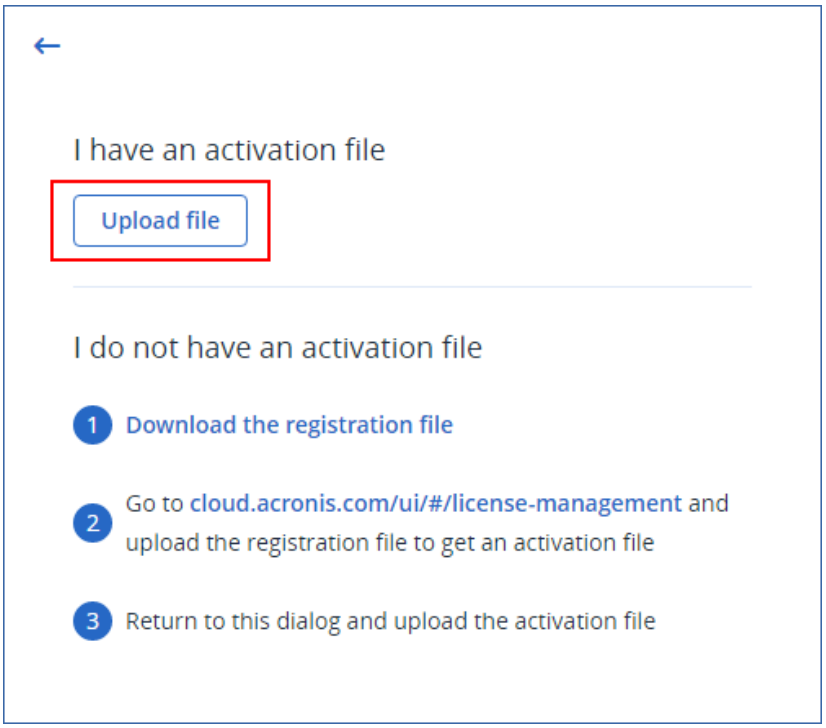
新配置現在正在等候中。若要加以取消，請按一下 **[移除此配置]**。

4. 在 **[將授權配置給離線管理伺服器]** 對話方塊中，按一下 **[下載檔案]**。

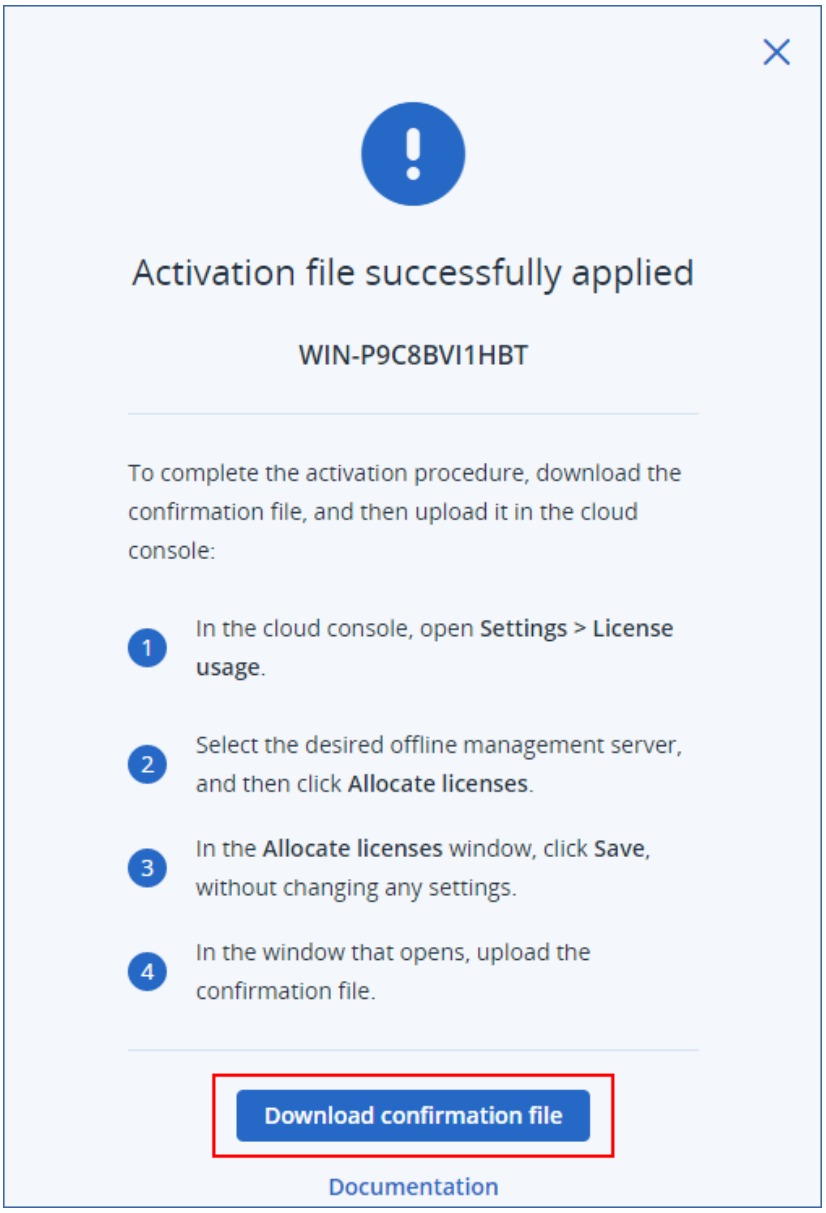


啟用檔案會下載到您的電腦中。

5. 在離線管理伺服器 (`https://`<您管理伺服器的 `IP` 位址>`:`<連接埠>) 的本機主控台中，瀏覽至 **[設定]** > **[授權使用狀況]**，然後按一下 **[透過檔案啟用]**。
6. 在開啟的對話方塊中的 **[我有啟用檔案]** 底下，按一下 **[上傳檔案]**，然後選擇要從雲端主控台下載的啟用檔案。

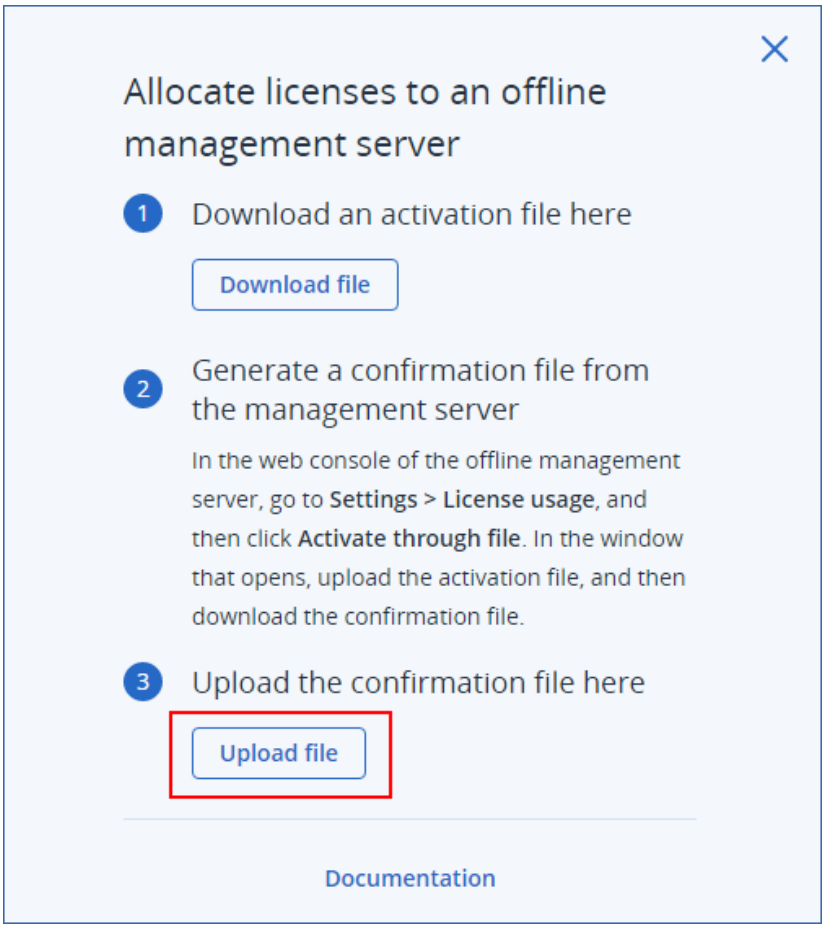


7. 在開啟的對話方塊中，按一下 **[下載確認檔案]**。



確認檔案會下載到您的電腦中。

8. 在雲端主控台 (https://cloud.acronis.com) 中，按一下 **[設定]** > **[授權使用狀況]**。
9. 瀏覽至您要配置授權的管理伺服器，然後按一下 **[配置授權]**。
10. 在開啟的對話方塊中，按一下 **[儲存]**，無需變更任何設定。
11. 在 **[將授權配置給離線管理伺服器]** 對話方塊中，按一下 **[上傳檔案]**，然後選擇您從離線管理伺服器下載的確認檔案。。



完成後，授權資訊會在您的 Acronis 帳戶與離線管理伺服器之間同步。

重要事項
如果修改過的授權配額小於保護代理程式數量，則負載最少的代理程式將會停止運作。此選擇為自動。如果不符合您的需求，請手動重新指派可用的授權。

將授權指派給工作負載

管理伺服器會將所配置的授權分配給此伺服器上已註冊的工作負載。

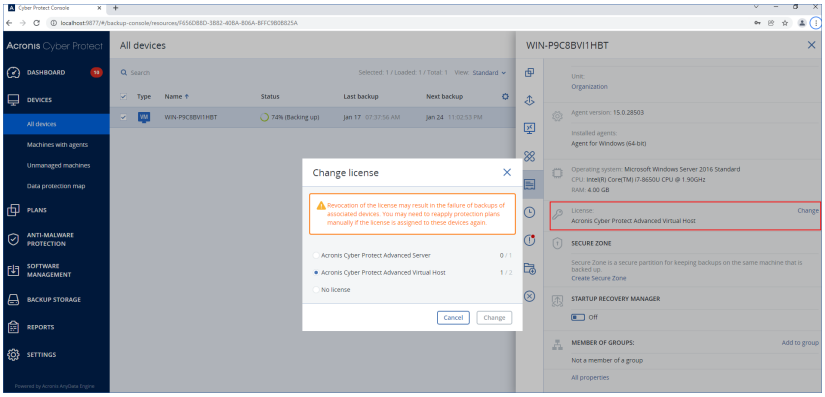
管理伺服器會在您首次套用保護計劃到某個工作負載時，將授權指派給該工作負載。如果有一個以上的授權配置給管理伺服器，則會根據工作負載類型、作業系統和所需的保護層級，為工作負載指派最適合的授權。

若要檢查所指派的授權，請在管理伺服器的 Web 主控台中，選擇所需的工作負載，然後按一下 **[詳細資料]**。

若要將手動重新指派授權給工作負載

1. 在管理伺服器的 Web 主控台中，按一下 **[裝置]**，然後選擇所需的工作負載。
2. 按一下**[詳細資料]**。
3. [針對內部部署管理伺服器] 瀏覽至 **[授權]** 區段，然後按一下 **[變更]**。
4. [針對雲端管理伺服器] 瀏覽至 **[服務配額]** 區段，然後按一下 **[變更]**。

5. 選擇所需的授權 (服務配額), 然後按一下 **[變更]**。



限制

針對離線管理伺服器, 授權配額的目前使用狀況只會顯示在本機主控台中。離線管理伺服器不會將此資料同步至您的 Acronis 帳戶, 而且在雲端主控台中無法使用。

已知問題

在雲端主控台, 可能無法正確顯示**虛擬主機**授權的授權使用狀況或指派。如需詳細資訊, 請參閱這篇知識庫文章。

取消註冊管理伺服器

若要取消註冊線上管理伺服器

1. 在雲端主控台 (https://cloud.acronis.com) 中, 按一下 **[設定]** > **[授權使用狀況]**。
2. 瀏覽至所需的管理伺服器, 然後按一下 **[取消註冊]**。
3. 即會顯示 **[取消註冊管理伺服器]** 視窗。
4. 輸入與帳戶相關聯的電子郵件地址以確認取消註冊。
5. 按一下 **[取消註冊]**。

完成後, 配置給未註冊伺服器的所有授權都會釋放, 並可配置給您帳戶中的另一台管理伺服器。在未註冊管理伺服器的本機主控台中, 授權會重設為零。

若要取消註冊離線管理伺服器

有兩種不同的進入點可取消註冊離線管理伺服器:

在本機主控台中:

1. 在本機主控台中, 按一下顯示帳戶那一行上的 **[取消註冊]**。即會顯示 **[取消註冊管理伺服器]** 視窗。
2. 在 **[登入]** 欄位中, 輸入與本機系統管理員相關聯的電子郵件地址。
3. 按一下 **[取消註冊]**。
4. 即會顯示 **[取消註冊成功]** 快顯視窗。
5. 按一下 **[下載取消註冊檔案]**。
6. 在雲端主控台中, 按一下 **[取消註冊]**。即會顯示 **[取消註冊管理伺服器]** 視窗。

7. 按一下 **[取消註冊離線管理伺服器]**。即會顯示 **[取消註冊離線管理伺服器]** 視窗。
8. 按一下 **[瀏覽]**，然後選擇您從本機主控台中下載的取消註冊檔案。
9. 按一下 **[取消註冊]**。

在雲端主控台中：

1. 在具備網際網路存取的電腦上，登入雲端主控台 (https://cloud.acronis.com)，然後按一下 **[設定]** > **[授權使用狀況]**。
2. 瀏覽至所需的管理伺服器，然後按一下 **[取消註冊]**。即會顯示 **[取消註冊管理伺服器]** 視窗。
3. 按一下 **[取消註冊離線管理伺服器]**。即會顯示 **[取消註冊離線管理伺服器]** 視窗。
4. 在您要取消註冊的管理伺服器 (https://<您管理伺服器的 IP 位址>:<連接埠>) 的本機主控台中，前往 **[設定]** > **[授權使用狀況]**，然後按一下 **[取消註冊]**。取消註冊檔案會下載到您的電腦中。
5. 在雲端主控台中，返回 **[取消註冊離線管理伺服器]** 視窗。
6. 按一下 **[瀏覽]**，然後選擇您從本機主控台中下載的取消註冊檔案。
7. 按一下 **[取消註冊]**。
8. 或者，如果您無法存取安裝管理伺服器所在的電腦，請按一下 **[我無法存取具有管理伺服器的電腦]**。

警告！
此電腦將遭到永久封鎖並從您的帳戶移除。您再也無法在此電腦上註冊管理伺服器。

完成後，配置給未註冊伺服器的所有授權都會釋放，並可配置給您帳戶中的另一台管理伺服器。在未註冊管理伺服器的本機主控台中，授權會重設為零。

Acronis Cyber Protect 15 Update 2 或更舊版本中的授權

若要開始使用 Acronis Cyber Protect 15 Update 2 版或更舊版本，您需要將至少一個授權金鑰新增至管理伺服器。保護計劃套用後，授權便會自動指派給電腦。

還可以手動指派或撤銷授權。只有組織管理員可以進行授權的手動作業。如需有關系統管理員的詳細資訊，請參閱 "單位與系統管理帳戶" (第 545 頁)。

將授權金鑰新增至管理伺服器

在 Acronis Cyber Protect 15 Update 2 或更舊版本中，您要將授權金鑰新增至管理伺服器。

若將授權金鑰新增至管理伺服器

1. 在 Cyber Protect Web 主控台中，移至 **[設定]** > **[授權]**。
2. 按一下 **[新增金鑰]**。
3. 輸入一或多個授權金鑰，每行一個金鑰。
4. 按一下 **[新增]**。
5. [當新增訂閱授權金鑰時] 若要啟用訂閱授權，請登入您的 Acronis 帳戶。
   a. 在登入表格中，輸入您用於 Acronis 客戶入口網站 (https://account.acronis.com) 的認證，然後按一下 **[登入]**。

b. 確認您的帳戶，然後按一下 **[同步]**。

c. 作業成功完成之後，按一下 **[完成]**。

6. 在 **[新增授權金鑰]** 面板中，按一下 **[完成]**。

注意事項

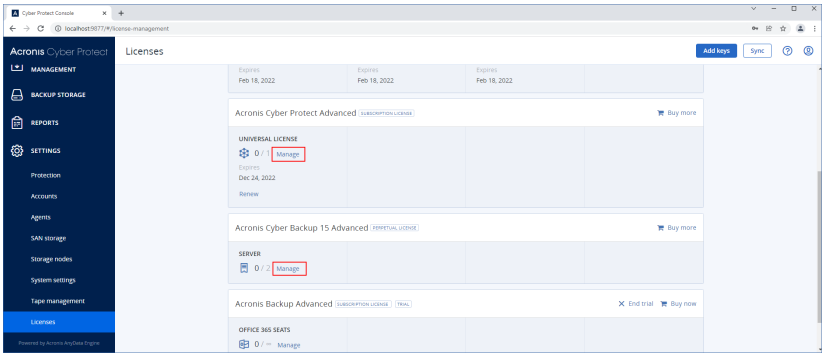
您可以自動匯入已在您的 Acronis 帳戶中註冊的訂閱授權金鑰，而不用再次將它們新增至管理伺服器。若要匯入授權金鑰，請在 **[新增授權金鑰]** 面板中按一下 **[與 Acronis 帳戶同步]**，然後登入您的 Acronis 帳戶。

管理訂購授權

在將授權指派給工作負載之前，必須將授權金鑰新增至管理伺服器。如需有關操作方式的詳細資訊，請參閱 "將授權金鑰新增至管理伺服器" (第 38 頁)。

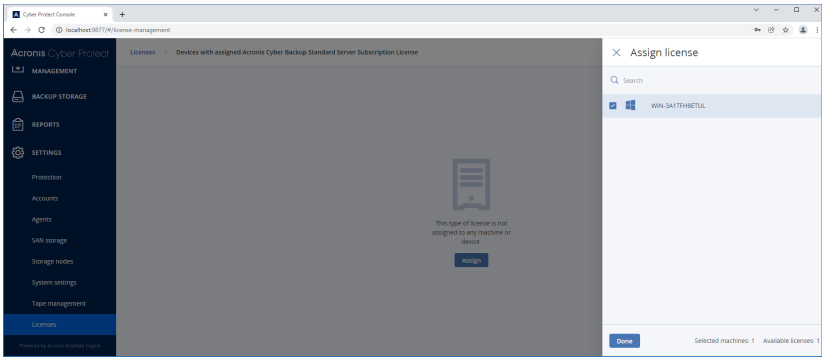
若要將訂購授權指派給工作負載

1. 在 Cyber Protect Web 主控台中，移至 **[設定]** > **[授權]**。
2. 瀏覽至所需的授權，然後按一下 **[管理]**。



3. 按一下 **[指派]**。

接著會顯示可指派此授權的工作負載。



4. 選擇工作負載，然後按一下 **[完成]**。

若要撤銷工作負載的訂閱授權

1. 在 Cyber Protect Web 主控台中，移至 **[設定]** > **[授權]**。
2. 瀏覽至所需的授權，然後按一下 **[管理]**。

接著會顯示已指派此授權的所有工作負載。

3. 選擇要撤銷授權的工作負載。
4. 按一下 **[撤銷]**。
5. 確認選項無誤。

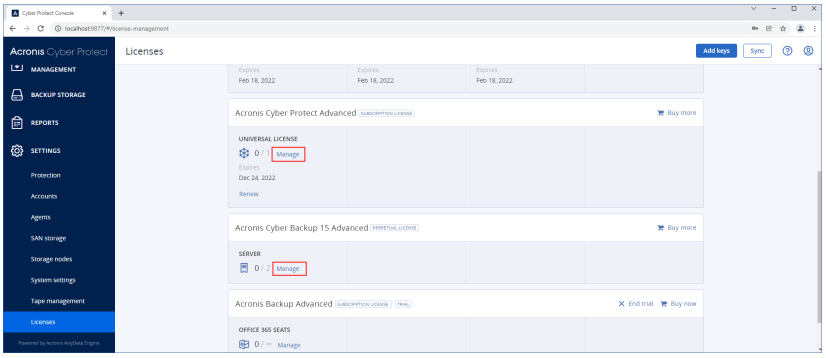
   已撤銷的授權會釋放，您可將其指派給另一個工作負載。

管理永久授權

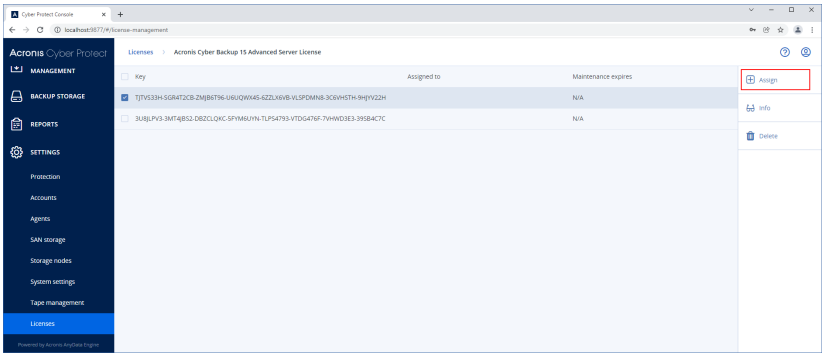
在將授權指派給工作負載之前，必須將授權金鑰新增至管理伺服器。如需有關操作方式的詳細資訊，請參閱 "將授權金鑰新增至管理伺服器"(第 38 頁)。

若要將永久授權指派給工作負載

1. 在 Cyber Protect Web 主控台中，移至 **[設定]** > **[授權]**。
2. 瀏覽至所需的授權，然後按一下 **[管理]**。



   接著會顯示與已選定授權相對應的授權金鑰。
3. 選擇要指派給工作負載的授權金鑰。
4. 按一下 **[指派]**。



   接著會顯示可指派此授權金鑰的工作負載。
5. 選擇工作負載，然後按一下 **[完成]**。

若要撤銷工作負載的永久授權

1. 在 Cyber Protect Web 主控台中，移至 **[設定]** > **[授權]**。
2. 選擇所需的授權，然後按一下 **[管理]**。

   接著會顯示與已選定授權相對應的授權金鑰。在 **[已派定]** 欄中，檢查指派此授權金鑰的工作負載。
3. 選擇要撤銷的授權金鑰。

4. 按一下 **[撤銷]**。
5. 確認選項無誤。

   已撤銷的授權金鑰會留在授權清單中，您可將其指派給另一個工作負載。

安裝

安裝概觀

Acronis Cyber Protect 支援兩種部署方法：內部部署和雲端部署。這兩者最大的差別在於 Acronis Cyber Protect 管理伺服器的位置。

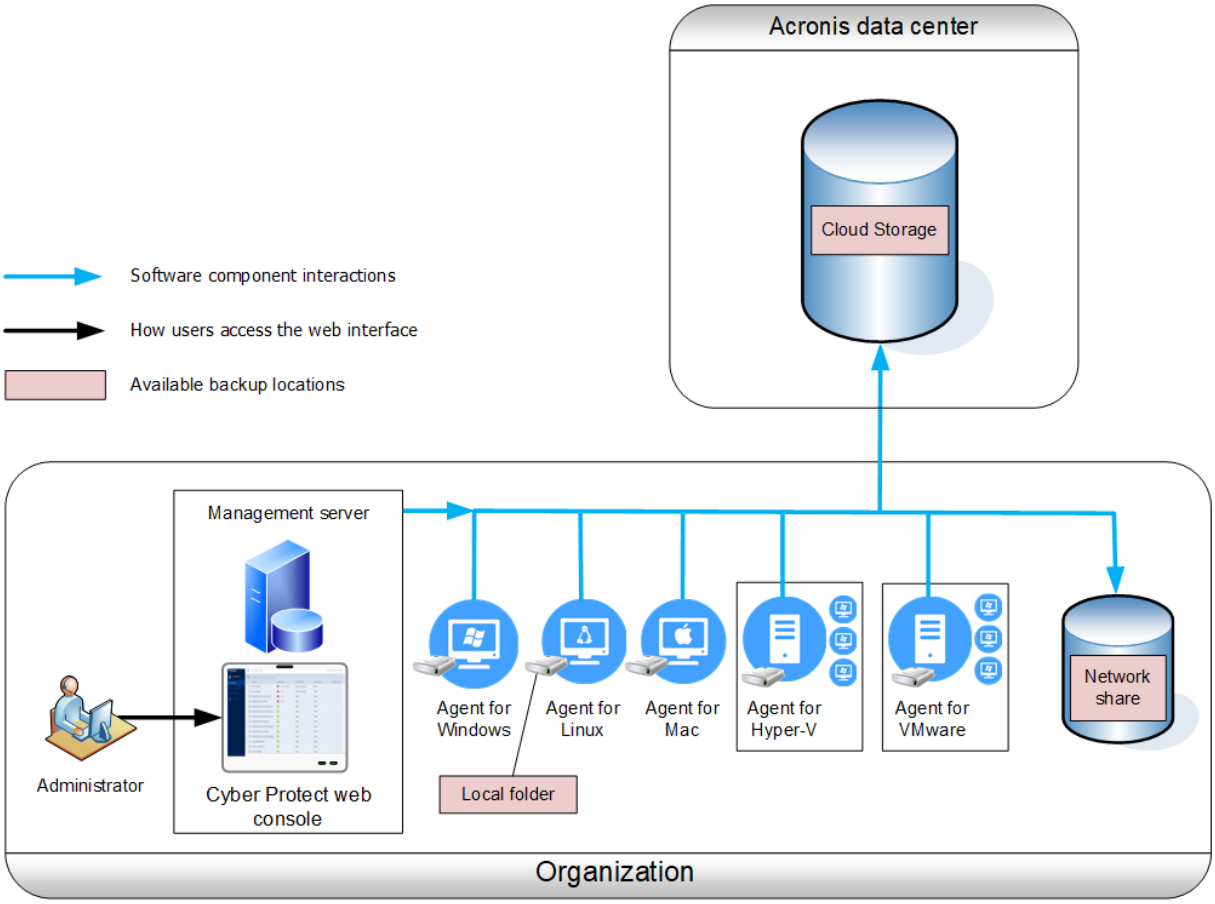
管理伺服器是管理您所有備份的核心。就內部部署而言，它就安裝在您的區域網路中；就雲端部署而言，它則位於其中一個 Acronis 資料中心。此伺服器的 Web 介面名稱為 Cyber Protect Web 主控台。

管理伺服器負責與保護代理程式通訊，並執行一般計劃管理功能。在每次保護活動之前，代理程式都會參考管理伺服器以確認先決條件。有時候可能會失去與管理伺服器的連線，如此將無法部署新的保護計劃。不過，如果保護計劃已經部署到電腦，代理程式會在失去與管理伺服器的通訊之後，繼續保護作業 30 天。

這兩種部署均需要將保護代理程式安裝在您想要備份的每部電腦上。支援的儲存類型也一樣：雲端儲存空間與 Acronis Cyber Protect 授權分開銷售。

內部部署

內部部署表示所有的產品元件均安裝在您的區域網路中。這是永久授權唯一可用的部署方法。此外，如果您的電腦並未連線至網際網路，就必須使用這個方法。



管理伺服器位置

您可以將管理伺服器安裝在執行 Windows 或 Linux 的電腦上。

建議您安裝在 Windows 上，因為這樣您便可以從管理伺服器，將代理程式部署在其他電腦上。使用「進階」授權，您可以建立組織單位並在其中加入管理員。如此一來，您就可以委派保護管理給其存取權限被嚴格限制為相對應單位的其他人員。

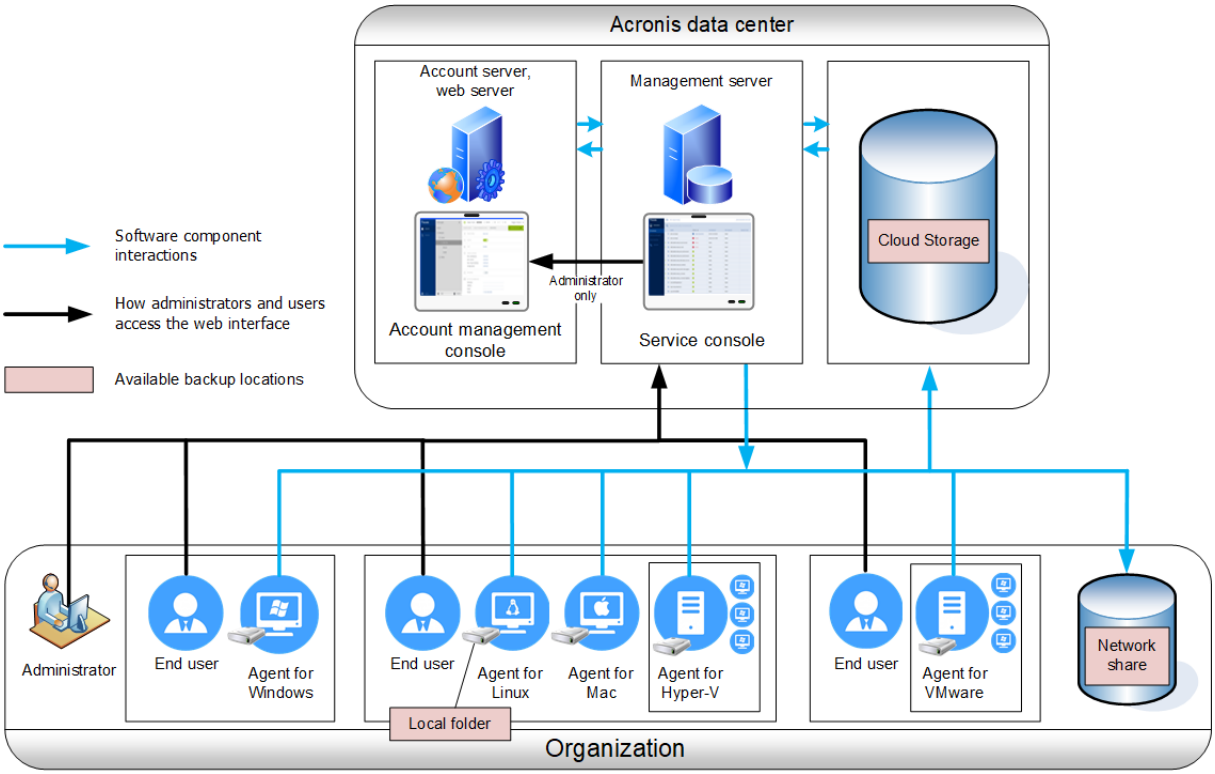
若要安裝在 Linux 上，則限僅有 Linux 的環境中。您有需要將代理程式安裝在您想要備份的本機上。

雲端部署

雲端部署即是，管理伺服器位於某個 Acronis 資料中心。此方法的好處是，您毋需在本機網路中維持管理伺服器。您可以將 Acronis Cyber Protect 視為 Acronis 提供給您的網路保護服務。

存取帳戶伺服器，可讓您建立使用者帳戶，為其設定服務使用量配額，以及建立使用者群組 (單位) 以反映您組織的結構。每個使用者均能存取 Cyber Protect Web 主控台、下載所需的代理程式，且能在短短幾分鐘內將其安裝在他們的電腦上。

管理員帳戶可以建立在單位或組織層級。每個帳戶的控制區域都有檢視範圍。使用者僅能存取他們自己的備份。



下表摘要說明內部部署和雲端部署的差異。每欄都會列出僅適用於對應部署類型的功能。

內部部署	雲端部署

• 可以使用永久授權 • 可用於氣隙環境的內部部署管理伺服器* • SFTP 伺服器作為備份位置 • Acronis Cyber Infrastructure 作為備份位置 • 磁帶裝置和 Acronis Storage Node 作為備份位置** • 從 Acronis Cyber Protect 的先前版本升級，包括 VMware 的 Acronis Backup	• Microsoft 365 資料的雲端對雲端備份，包括保護群組、公用資料夾、OneDrive*** 和 SharePoint Online 資料 • Google Workspace 資料的雲端對雲端備份 • Mac 用代理程式支援 x64 和 ARM 型處理器 (例如 Apple Silicon M1 和 M2) • Virtuozzo 用代理程式 (在 Hypervisor 層級備份 Virtuozzo 虛擬機器) • oVirt 用代理程式 (在 Hypervisor 層級備份 oVirt KVM 虛擬機器) • Virtuozzo Hybrid Infrastructure 用代理程式 (在 Hypervisor 層級備份 Virtuozzo Hybrid Infrastructure 虛擬機器) • 災難復原即雲端服務****

* 如需有關在氣隙環境中啟用管理伺服器的詳細資訊，請參閱 "若要啟用離線管理伺服器" (第 26 頁)。

** 此功能不適用於 Standard Edition。

***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存檔中有無效內容。

**** 該功能僅能搭配 Disaster Recovery 附加元件使用。

元件

代理程式

代理程式是在 Acronis Cyber Protect 所管理之電腦上，執行資料備份、復原和其他作業的應用程式。

Windows 用代理程式已隨 Exchange 用代理程式、SQL 用代理程式、Active Directory 用代理程式以及 Oracle 用代理程式一同安裝。例如，如果您安裝 SQL 用代理程式，您也將可備份已安裝代理程式的整部電腦。

部分代理程式僅能安裝在具有特定角色或應用程式的電腦上，例如，Hyper-V 用代理程式安裝在執行 Hyper-V 角色的電腦上、SQL 用代理程式安裝在執行 SQL 資料庫的電腦上、Exchange 用代理程式安裝在執行 Microsoft Exchange Server 信箱角色的電腦上，而 Active Directory 用代理程式則安裝在網域控制站上。

選擇代理程式，視您要備份的內容而定。下表摘述可協助您做出決定的資訊。

您要備份什麼內容?	要安裝哪一個代理程式?	要安裝在哪裡?	代理程式可用性	
			內部部署	雲端

實體機器				
執行 Windows 之虛擬機器上的磁碟、磁碟區及檔案	Windows 用代理程式	在將進行備份的實體機器上。	+	+
執行 Linux 之虛擬機器上的磁碟、磁碟區及檔案	Linux 用代理程式		+	+
執行 Mac OS 之實體機器上的磁碟、磁碟區及檔案	Mac 用代理程式		+	+
應用程式				
SQL 資料庫	SQL 用代理程式	在執行 Microsoft SQL Server 的電腦上。	+	+
Exchange 資料庫和信箱	Exchange 用代理程式	在執行 Microsoft Exchange Server 信箱角色的電腦上。* 如果只需要備份信箱，則可將代理程式安裝到任何執行 Microsoft Exchange Server 的用戶端存取角色，且連接到網路的電腦上。	+ 無信箱備份	
Microsoft 365 信箱	Office 365 用代理程式	在已連線至網際網路的 Windows 電腦上。	+	+
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。	+	+
執行 Oracle 資料庫的電腦	適用於 Oracle 的代理程式	在執行 Oracle 資料庫的電腦上。	+	-
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	在 Scale Computing HC3 主機上。	+	+
裝載於 Windows Azure 主機上的虛擬機器	與實體電腦相同***	在將進行備份的實體機器上。	+	+
裝載於 Amazon EC2 主機上的虛擬機器			+	+
Citrix XenServer 虛擬機器			+****	+
Red Hat Virtualization (RHV/RHEV) 虛擬機器				
核心虛擬機器 (KVM)				
Oracle 虛擬機器				
Nutanix AHV 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「不透過 LAN 備份」。

***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。不過，您在雲端部署中設定機器的數量配額時，系統會將該電腦視為虛擬機器。

****使用 Acronis Cyber Protect Advanced 虛擬主機授權時，這些虛擬機器會被視為虛擬的 (使用每個主機授權)。***使用 Acronis Cyber Protect 虛擬主機授權，這些虛擬機器將被視為是實體的(使用每個機器授權時) 。

其他元件

元件	功能	要安裝在哪裡?	可用性	
			內部部署	雲端
管理伺服器	Management Server 是管理您所有備份的核心。就內部部署而言，它就安裝在您的區域網路中。 它會管理代理程式並提供 Web 介面給使用者。	在執行 Windows 或 Linux 的電腦上。	+	-
Components for Remote Installation	將代理程式安裝套件儲存到本機資料夾。	執行管理伺服器的 Windows 電腦上。	+	-
掃描服務	可在雲端儲存空間、本機資料夾或網路資料夾中，對備份執行反惡意程式碼掃描的選用元件。 掃描服務需要使用 Microsoft SQL Server 或 PostgreSQL 資料庫。它與管理伺服器使用的預設 SQLite 資料庫不相容。	在執行管理伺服器的 Windows 或 Linux 電腦上。	+	-
可開機媒體組建	建立可開機媒體。	在執行 Windows 或 Linux 的電腦上。	+	-
命令列工具	支援具有 **acrocmd** 公用程式的命令列介面。**acrocmd** 不包含實際執行命令的任何工具。而是僅向 Cyber Protect 元件 (代理程式與管理伺服器) 提供命令列介面。	在執行 Windows、Linux 或 macOS 的電腦上。	+	+
Acronis Cyber Protect 15 監視器	提供 Windows 用代理程式和 Mac 用代理程式的圖形化使用者介面。其會顯示安裝代理程式所	在執行 Windows 或 Mac OS 的電腦上。	+	+

	在電腦保護狀態的相關資訊，並可讓其使用者設定備份加密和 Proxy 伺服器設定。 在 Windows 中，Acronis Cyber Protect 15 監視器要求 Windows 用代理程式安裝在相同的電腦上。			
儲存節點	儲存備份。用於編目與重複資料刪除。 儲存節點要求 Windows 用代理程式安裝在相同的電腦上。	在執行 Windows 的電腦上。	+	-
目錄服務	在儲存節點上執行備份的編目。	在執行 Windows 的電腦上。	+	-
PXE 伺服器	透過網路，將開機電腦啟用為可開機媒體。	在執行 Windows 的電腦上。	+	-

在您的環境中使用 Acronis Cyber Protect 搭配其他安全解決方案

您可以在您的環境中使用 Acronis Cyber Protect 搭配其他安全解決方案，例如獨立的防毒軟體，或者不搭配也行。

如果不搭配其他安全解決方案，您可以使用 Acronis Cyber Protect 做到完整的網路保護或傳統的備份與復原，端視您的授權與需求而定。如需有關各授權可使用功能的詳細資訊，請參閱「包括雲端部署在內的 Acronis Cyber Protect 15 版本比較」。您可以透過僅啟用需要的模組，來調整保護計劃的範圍。

您可以選擇 Acronis Cyber Protect 進行完整的網路保護，包括防禦病毒與其他惡意程式碼，即使您的環境中已經有其他安全解決方案也行。在此情況下，您必須停用或移除其他安全解決方案，以避免衝突。

或者，您可能希望在不停用或移除目前安全解決方案的情況下，加強您的網路保護。這也是可能的，只要確認在您的保護計劃中不使用防毒與反惡意程式碼模組就可以。所有其他模組皆可自由使用。

限制

- 備份的反惡意程式碼掃描需要您在安裝 Cyber Protect Management Server 時安裝掃描服務。
- 只有在執行 Linux 的電腦上安裝 Management Server 的情況下，才能使用透過 HTML5 用戶端遠端存取。

軟體需求

支援的網頁瀏覽器

Web 介面支援下列網頁瀏覽器：

- Google Chrome 29 或更新版本
- Mozilla Firefox 23 或更新版本
- Opera 16 或更新版本
- Windows Internet Explorer 10 或更新版本

注意事項
在雲端部署中，不支援 Internet Explorer。

- 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

代理程式

Windows 用代理程式

- Windows XP Professional SP1 (x64)、SP2 (x64)、SP3 (x86)
- Windows XP Professional SP2 (x86) – 支援特殊版本的 Windows 用代理程式。如需此項支援的詳細資料與限制，請參閱「Windows XP SP2 用代理程式」。
- Windows XP Embedded SP3
- Windows Server 2003 SP1/2003 R2 以及更新版本 - Standard 與 Enterprise 版 (x86、x64)

注意事項
Acronis Cyber Protect 需要使用 Microsoft 的 KB940349 更新無法再單獨下載。為確保您的電腦上可以使用 KB940349 原始提供的功能，請安裝目前適用於 Windows Server 2003 的所有可用更新。
如需有關 KB940349 的詳細資訊，請參閱這篇知識庫文章。

- Windows Small Business Server 2003/2003 R2
- Windows Server 2008 - Standard、Enterprise、Datacenter、Foundation 和 Web 版本 (x86、x64)
- Windows Small Business Server 2008
- Windows 7 – 所有版本 (x86、x64)

注意事項

若要在 Windows 7 使用 Acronis Cyber Protect，您必須安裝以下 Microsoft 更新：

- 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

SQL 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)，以及 Active Directory 用代理程式

每一個代理程式都可以安裝在執行任何上述所列之作業系統的電腦上，以及個別應用程式的支援版本，但例外如下：

- 在 Windows 7 Starter 和 Home 版本 (x86、x64) 上，SQL 用代理程式不支援內部部署

Exchange 用代理程式 (適用於信箱備份)

無論電腦是否有 Microsoft Exchange 伺服器，此代理程式均可在其上安裝。

- 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

Office 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)

Linux 用代理程式

注意事項
下列 Linux 發行版和核心版本已經過專門測試。不過，即使您的 Linux 發行版或核心版本未列在下方，由於 Linux 作業系統的特殊性，仍可能在所有必要情境中正常運作。

如果您在使用 Acronis Cyber Protect 搭配 Linux 發行版與核心版本組合時發生問題，請聯絡支援小組以便進一部調查。

含核心 2.6.9 至 5.19 及 glibc 2.3.4 或更新版本的 Linux，包括下列 x86 和 x86_64 發行版本：

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04

- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- SUSE Linux Enterprise Server 10, 11, 12, 15

重要事項
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
- CentOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*– Unbreakable Enterprise Kernel 與 Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*、8.5*
- Rocky Linux 8.4*
- ALT Linux 7.0

在不使用 RPM 套件管理員的系統 (如 Ubuntu 系統) 上安裝產品前，必須先手動安裝此管理員，例如執行以下命令 (以 root 使用者身分)：`apt-get install rpm`

如果您的 Linux 發行版不支援 D-Bus 機制 (例如，Red Hat Enterprise Linux 6.x 或 CentOS 6.x)，Acronis Cyber Protect 將使用預設位置來儲存安全金鑰，因為作業系統不提供 D-Bus 相容位置。

* 僅支援 4.18 到 5.19 之間的核心

Mac 用代理程式

注意事項
不支援 ARM 型處理器 (例如 Apple Silicon M1 和 M2)。

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

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
- 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 with Hyper-V – 所有安裝選項，Nano Server 除外

Scale Computing HC3 用代理程式 (虛擬裝置)

此代理程式會當作在 Scale Computing HC3 叢集中透過 Cyber Protect Web 主控台部署的虛擬裝置交付。此代理程式沒有獨立的安裝程式。

Scale Computing Hypercore 8.8、8.9、9.0

Management Server (僅適用於內部部署)

在 Windows 中

- Windows 7 – 所有版本 (x86、x64)

注意事項

若要在 Windows 7 使用 Acronis Cyber Protect，您必須安裝以下 Microsoft 更新：

- 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 和 Foundation 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 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

在 Linux 中

注意事項
下列 Linux 發行版和核心版本已經過專門測試。不過，即使您的 Linux 發行版或核心版本未列在下方，由於 Linux 作業系統的特殊性，仍可能在所有必要情境中正常運作。

如果您在使用 Acronis Cyber Protect 搭配 Linux 發行版與核心版本組合時發生問題，請聯絡支援小組以便進一部調查。

含核心 2.6.9 至 5.19 及 glibc 2.3.4 或更新版本的 Linux，包括下列 x86_64 發行版。

不支援 x86 發行版。

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

  重要事項
  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
- CentOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*– Unbreakable Enterprise Kernel 與 Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*、8.5*

- Rocky Linux 8.4*
- ALT Linux 7.0

在不使用 RPM 套件管理員的系統 (如 Ubuntu 系統) 上安裝產品前，必須先手動安裝此管理員，例如執行以下命令 (以 root 使用者身分)：`apt-get install rpm`

如果您的 Linux 發行版不支援 D-Bus 機制 (例如，Red Hat Enterprise Linux 6.x 或 CentOS 6.x)，Acronis Cyber Protect 將使用預設位置來儲存安全金鑰，因為作業系統不提供 D-Bus 相容位置。

* 僅支援 4.18 到 5.19 之間的核心

儲存節點 (僅限內部部署)

- Windows Server 2008 - Standard、Enterprise、Datacenter 和 Foundation 版本 (僅限 x64)
- Windows Small Business Server 2008
- Windows 7 – 所有版本 (僅限 x64)
- Windows Server 2008 R2 - Standard、Enterprise、Datacenter 和 Foundation 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(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
- Windows 10 – Home、Pro、Education、Enterprise 以及 IoT Enterprise 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 Server 2022 – 所有安裝選項，Nano Server 除外

Windows XP SP2 用代理程式

Windows XP SP2 用代理程式僅支援 32 位元版 Windows XP SP2。

若要保護執行 Windows XP SP1 (x64)、Windows XP SP2 (x64) 或 Windows XP SP3 (x86) 的電腦，請使用一般 Windows 用代理程式。

Windows XP SP2 用代理程式需要使用 Acronis Cyber Backup 12.5 授權。不支援 Acronis Cyber Protect 15 授權金鑰。

安裝

Windows XP SP2 用代理程式需要至少 550 MB 的磁碟空間以及 150 MB 的 RAM。備份時，代理程式通常耗用約 350 MB 的記憶體。最高耗用量可能會達到 2 GB，視處理的資料量而定。

Windows XP SP2 用代理程式僅能安裝在所要備份的電腦本機上。若要下載代理程式安裝程式，按一下右上角的帳戶圖示，然後按一下 **[下載]** > **[Windows XP SP2 用代理程式]**。

無法安裝 Cyber Protect 監視器和 Bootable Media Builder。若要下載可開機媒體的 ISO 檔案，請按一下右上角的帳戶圖示 > **[下載]** > **[可開機媒體]**。

更新

Windows XP SP2 用代理程式不支援遠端更新功能。若要更新代理程式，請下載新版本的安裝程式，然後重複安裝程序。

如果您已從 Windows XP SP2 更新為 SP3，請解除安裝 Windows XP SP2 用代理程式，然後安裝一般 Windows 用代理程式。

限制

- 只有磁碟層級備份可以使用。個別檔案可以從磁碟或磁碟區備份復原。
- 不支援按事件排程。
- 不支援保護計劃執行的條件。
- 僅支援下列備份目的地：
  - 雲端儲存
  - 本機資料夾
  - 網路資料夾
  - Secure Zone
- 不支援 **12 版**備份格式以及需要 **12 版**備份格式的功能。特別是，無法使用實體資料運送。**[效能和備份視窗]** 選項 (如有啟用) 僅適用於綠色層級設定。
- 在復原期間，不支援在 Web 介面中選取個別磁碟/磁碟區進行復原和手動磁碟對應。此功能僅能在可開機媒體下使用。
- 不支援脫離主機資料處理。
- Windows XP SP2 用代理程式無法使用備份執行下列作業：
  - 將備份轉換至虛擬機器
  - 從備份掛載磁碟區
  - 從備份解壓縮檔案
  - 匯出與手動驗證備份。

  您可以使用其他代理程式執行這些作業。
- Windows XP SP2 用代理程式建立的備份無法當做虛擬機器執行。

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

上述 SQL Server 版本的 SQL Server Express 版本也受到支援。

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

Acronis Cyber Protect 15 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 資料庫 11g 版，所有版本
- Oracle 資料庫 12c 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。

支援的虛擬化平台

下表概述各種虛擬化平台的支援情況。

注意事項

透過**從客體作業系統內進行備份**方法支援的下列 Hypervisor 廠商與版本已經過專門測試。不過，即使您執行 Hypervisor 的廠商或 Hypervisor 版本未列在下方，**從客體作業系統內進行備份**方法仍可能在所有必要情經中正確運作。

如果您在搭配 Hypervisor 供應商和版本使用 Acronis Cyber Protect 時遇到問題，請與支援團隊聯絡以進一步調查。

平台	Hypervisor 層級備份 (無代理程式備份)	從客體作業系統內進行備份
VMware		
VMware vSphere 版本：4.1、5.0、5.1、5.5、6.0、6.5、6.7、7.0、8.0 **VMware vSphere 版本：** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	+	+
VMware vSphere Hypervisor (Free ESXi)**		+
VMware Server (VMware Virtual server) VMware 工作站 VMware ACE VMware 播放機		+
Microsoft* **		
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	+	+

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		
Microsoft Virtual PC 2004 和 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Scale Computing		
Scale Computing Hypercore 8.8、8.9、9.0	+	+
Citrix		
Citrix XenServer 4.1.5、5.5、5.6、6.0、6.1、6.2、6.5、7.0、7.1、7.2、7.3、7.4、7.5、7.6		僅限完全虛擬化 (亦即 HVM) 的客體。不支援半虛擬化 (亦即 PV) 的客體。
Red Hat 和 Linux		
Red Hat Enterprise Virtualization (RHEV) 2.2、3.0、3.1、3.2、3.3、3.4、3.5、3.6 Red Hat Virtualization (RHV) 4.0、4.1		+
Red Hat Virtualization (受 oVirt 管理) 4.2、4.3、4.4 (僅適用於雲端部署)	+	+
核心虛擬機器 (KVM)		+
受 Red Hat Enterprise Linux 7.6、7.7 或 CentOS 7.6、7.7 上執行的 oVirt 4.3 管理的核心虛擬機器 (KVM) (僅適用於雲端部署和 Advanced 授權)	+	+
受 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) (僅適用於雲端部署和 Advanced 授權)	+	+
受 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)	+	+

(僅適用於雲端部署和 Advanced 授權)		
Parallels		
Parallels 工作站		+
Parallels Server 4 裸機		+
Oracle		
Oracle VM Server 3.0、3.3、3.4		僅限完全虛擬化 (亦即 HVM) 的客體。不支援半虛擬化 (亦即 PV) 的客體。
Oracle VM VirtualBox 4.x		+
Nutanix		
Nutanix Acropolis Hypervisor (AHV) 20160925.x 到 20180425.x		+
Virtuozzo (僅適用於雲端部署)		
Virtuozzo 6.0.10、6.0.11、6.0.12	+	僅限虛擬機器。不支援容器。
Virtuozzo 7.0.13、7.0.14	僅限 Ploop 容器。不支援虛擬機器。	僅限虛擬機器。不支援容器。
Virtuozzo Hybrid Server 7.5	+	僅限虛擬機器。不支援容器。
Virtuozzo Hybrid Infrastructure (僅適用於雲端部署)		
Virtuozzo Hybrid Infrastructure 3.5、4.0、4.5	+	+
Amazon		
Amazon EC2 執行個體		+
Microsoft Azure		
Azure 虛擬機器		+

***** 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。

*** 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

- **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。
- **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**

  VMware 用代理程式和 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。ESXi 和 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。
- **含有邏輯磁碟區 (LVM) 的 Linux 電腦**

  VMware 用代理程式與 Hyper-V 用代理程式不支援對含有 LVM 的 Linux 電腦進行下列作業：
  - P2V 與 V2P 移轉。使用 Linux 用代理程式或可開機媒體建立要復原的備份和可開機媒體。
  - 從 Linux 用代理程式或可開機媒體建立的備份執行虛擬機器。
  - 將 Linux 用代理程式或可開機媒體建立的備份轉換至虛擬機器。
- **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 vSphere 6.5 提供)
  虛擬機器復原為新的虛擬機器後，**安全開機**會停用。完成復原後，可手動啟用此選項。
- VMware vSphere 7.0 不支援 **ESXi 設定備份**。

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**	sudo zypper install kernel-source sudo zypper install gcc

	make **perl**	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。

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 Drive Encryption
- CheckPoint Harmony Endpoint
- McAfee 端點加密
- PGP 全磁碟加密

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。
2. 安裝保護代理程式。
3. 建立 Secure Zone。
4. 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。請勿嘗試使用可開機媒體進行備份。

軟體特定的復原程序

Microsoft BitLocker 磁碟機加密和 CheckPoint Harmony Endpoint

您可以透過重新啟動進行復原或使用可開機媒體來復原系統。

使用重新啟動復原

若要復原加密系統，請遵循 "復原實體機器" (第 270 頁) 中的步驟。

請確認符合 "使用重新啟動復原" (第 276 頁) 中的需求。

注意事項
對於 BitLocker 加密磁碟區，透過重新啟動進行復原僅適用於執行 Windows 7 與更新版本或 Windows Server 2008 R2 與更新版本上的 UEFI 型電腦。對於 CheckPoint 加密磁碟區，透過重新啟動進行復原僅適用於執行 Windows 10 和 Windows 11 的 UEFI 型電腦。

透過重新啟動進行復原不適用於執行 Linux 或 macOS 的 BIOS 型電腦。

使用可開機媒體復原

1. 從可開機媒體開機。
2. 復原系統。

   重要事項
   已備份的資料會被當作未加密復原。

3. 將已復原的系統重新開機。
4. 開啟加密軟體。

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，請在作業系統中執行復原。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

透過 Acronis Cyber Protect，您可以使用 Dell EMC Data Domain 裝置作為備份儲存空間。支援保留鎖定 (治理模式)。

如果啟用保留鎖定，您需要將 `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。

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。

若要在 Windows 中新增變數

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。

若要在 Linux 中新增變數

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。

若要在虛擬裝置中新增變數

1. 以系統管理員身分，登入虛擬裝置電腦。
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. 重新啟動虛擬裝置電腦。

系統需求

下表摘述一般安裝的磁碟空間和記憶體需求。依照預設設定執行安裝。

將要安裝的元件	安裝所需的磁碟空間	記憶體最低耗用量
Windows 用代理程式	850 MB	150 MB
Windows 用代理程式，以及下列其中一個代理程式： • SQL 用代理程式 • Exchange 用代理程式	950 MB	170 MB
Windows 用代理程式，以及下列其中一個代理程式： • VMware 用代理程式 (Windows) • Hyper-V 用代理程式	1170 MB	180 MB

Office 365 用代理程式	500 MB	170 MB
Linux 用代理程式	2.0 GB	130 MB
Mac 用代理程式	500 MB	150 MB
僅限內部部署		
Windows 的管理伺服器	1.7 GB	200 MB
Linux 的管理伺服器	1.5 GB	200 MB
管理伺服器和 Windows 用代理程式	2.4 GB	360 MB
執行 Windows、Microsoft SQL Server、Microsoft Exchange Server，和 Active Directory 網域服務電腦上的管理伺服器和代理程式	3.35 GB	400 MB
管理伺服器和 Linux 用代理程式	4.0 GB	340 MB
儲存節點與 Windows 用代理程式 • 僅限 64 位元平台 • 若要使用重複資料刪除功能，需要至少 8GB 的 RAM。如需詳細資訊，請參閱 "重複資料刪除最佳作法" (第 530 頁)。	1.1 GB	330 MB

備份時通常耗用約 350 MB 的記憶體 (以 500-GB 磁碟區備份做測量)。最高耗用量可能會達到 2 GB，視處理的資料量和資料類型而定。

備份至大型備份集 (600 GB 或更多) 時，每 1 TB 的備份集需要約 1 GB 的 RAM。

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。

擁有一個已註冊工作負載的管理伺服器，會耗用 200 MB 的記憶體。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。每個額外的工作負載會新增約 2MB。因此，已註冊 100 個工作負載的伺服器大約耗用 400 MB，不含作業系統和執行應用程式。

已註冊工作負載的數目上限為 900-1000。此項限制源自管理伺服器的內嵌 SQLite 資料庫。

若要克服此限制，可在管理伺服器安裝期間，指定一個外部 Microsoft SQL Server 執行個體。使用外部 SQL 資料庫時，最多可註冊 8000 個工作負載至管理伺服器，且不會造成明顯的效能下降。在有 8000 個已註冊工作負載的情況下，SQL Server 將耗用 8 GB 左右的 RAM。

為獲得更佳的備份效能，請依群組管理工作負載，且每個群組最多含 500 個工作負載。

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。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	WinPE 可開機媒體	Linux 可開機媒體	Mac 可開機媒體	
FAT16/32	所有代理程式	+	+	+	無限制
NTFS		+	+	+	
ext2/ext3/ext4		+	+	-	
HFS+	Mac 用代理程式	-	-	+	
APFS		-	-	+	• 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	-	+	-	• 無法從磁碟備份中排除檔案 • 無法啟用快速增量/差異備份
ReiserFS3		-	+	-	
ReiserFS4		-	+	-	• 無法從磁碟備份中排除檔案 • 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	+	+	+	
XFS		+	+	+	• 無法從磁碟備份中排除檔案 • 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 • 不支援從儲存在磁帶上的備份復原檔案
Linux swap	Linux 用代	-	+	-	無限制

	理程式				
exFAT	所有代理程式	+	+ 如果備份*是儲存在* exFAT 上，則可開機媒體無法用於復原。	+	• 僅支援磁碟/磁碟區備份 • 檔案無法從備份中排除 • 個別檔案無法從備份中復原

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。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。

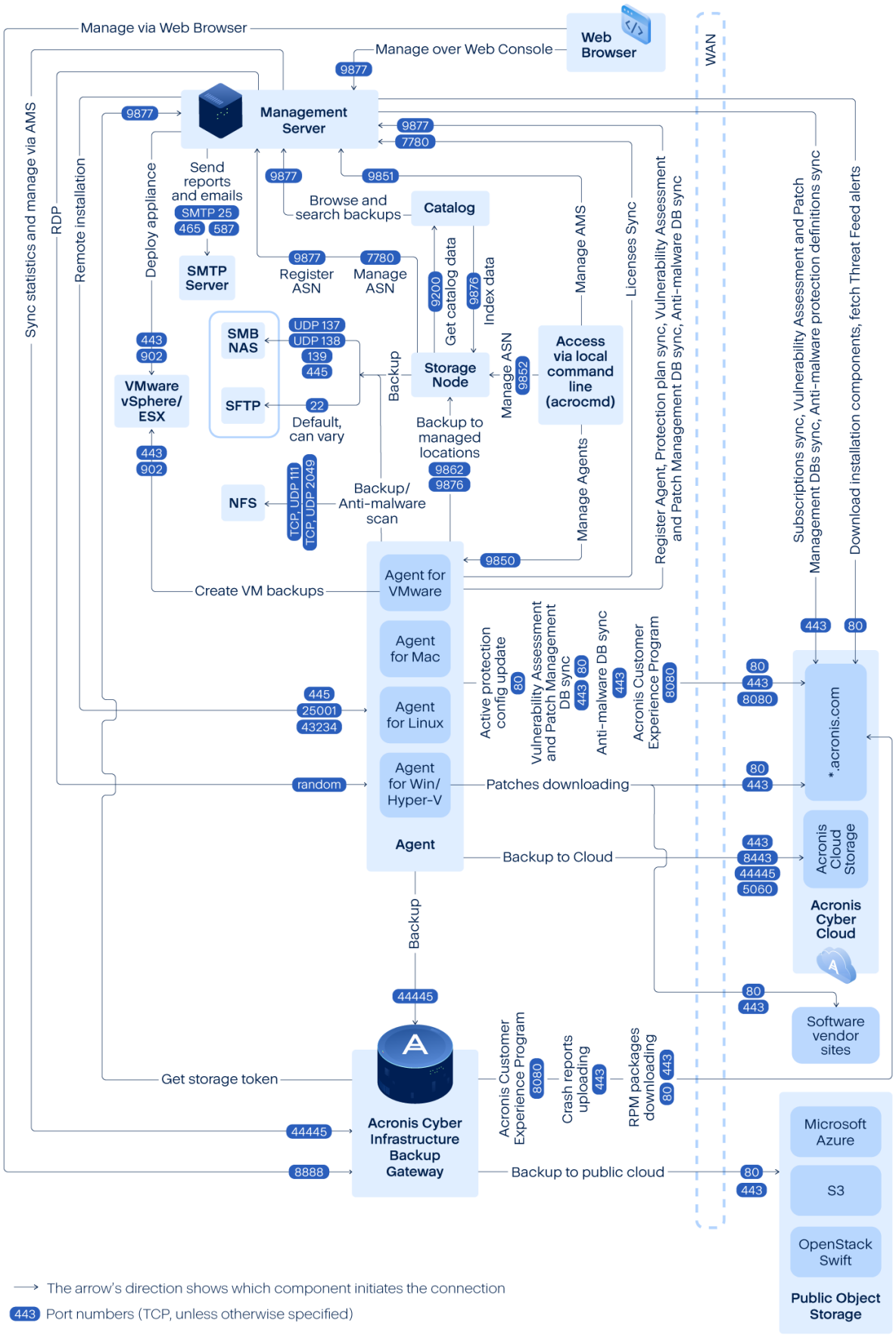
Acronis Cyber Protect 的網路連線圖

本主題包含 Acronis Cyber Protect 的連線圖表。

如需 Acronis Cyber Protect 所使用之連接埠、服務和處理程序的清單，請瀏覽知識庫：

- 針對 Windows，請參閱 Windows 服務和處理程序 (65663)。
- 針對 Linux，請參閱 Linux 元件、服務和處理程序 (67276)。

網路連線圖 - Cyber Protect 處理程序



重要事項
網路圖表中的傳出連接埠為動態內容。有些服務也可以為傳入連線使用動態連接埠。當您對網路問題進行疑難排解時，請確認允許通過動態連接埠的流量。

動態連接埠由作業系統管理並隨機指派。Windows 中的預設動態連接埠範圍是 49152 至 65535。此範圍可能視作業系統而有所不同，而且可以手動進行變更。

管理伺服器是 Acronis Cyber Protect 的中心元件。它公開兩個 TCP 連接埠：7780 和 9877。連接埠 9877 受 TLS 保護，用來提供 REST API 和網頁型使用者介面。REST API 端點使用表視為單獨 HTTP 標頭或編碼為 HTTP Cookie 的 JWT 權杖，來驗證要求。連接埠 7780 使用 ZMTP CURVE 驗證與加密，來實作 ZeroMQ 通訊協定。代理程式和儲存節點使用連接埠 7780 來與管理伺服器非同步交換管理訊息。管理伺服器也與雲端服務通訊，透過標準 HTTP 和 HTTPS 連接埠來下載更新。

儲存節點是 Acronis Cyber Protect 的儲存元件。它公開 TCP 連接埠 9876。此連接埠是用來傳送及接收備份資料。傳輸是受 TLS 保護，而驗證則是使用相互 TLS 來完成。應用程式層級通訊協定為 Acronis 專屬。儲存節點使用適當的通訊協定與驗證機制，與後端儲存系統通訊。

目錄 是 Acronis Cyber Protect 的支援元件。它會在儲存節點上建立索引，在連接埠 9876 上存取它並在連接埠 9200 上公開索引。

備份閘道實作新一代的 Acronis 專屬資料存取通訊協定。如果客戶選擇使用雲端備份，則 Acronis Cyber Cloud 中會使用相同元件。閘道使用的是註冊於 IANA 的 TCP 連接埠 44445。資料保護是透過 TLS 完成，而驗證則是使用相互 TLS 來完成。備份閘道也可能將連接埠 8888 用於 HTTPS 型的管理服務。

如上所述，**代理程式**會透過連接埠與管理伺服器、儲存節點和備份閘道通訊。當標準型檔案服務 (SMB、NFS) 用來作為備份目的地時，代理程式也會與它們通訊。在此情況下，會使用標準連接埠和適當的驗證通訊協定。設定此類功能時，VMware 用代理程式會透過 VMware vSphere 定義的連接埠來使用 VMware vSphere API。

Linux 的弱點評估是透過 Acronis Cyber Cloud 中部署的 CVSS 服務實作的。保護代理程式會透過 ping，從清單 https://cloud.acronis.com/services.json 中動態選擇最近的資料中心。

內部部署

內部部署包含許多軟體元件，這些元件如 "元件" (第 44 頁) 一節中所述。如需有關這些元件及所需連接埠之間互動的詳細資料，請參閱 "Acronis Cyber Protect 的網路連線圖" (第 71 頁)。

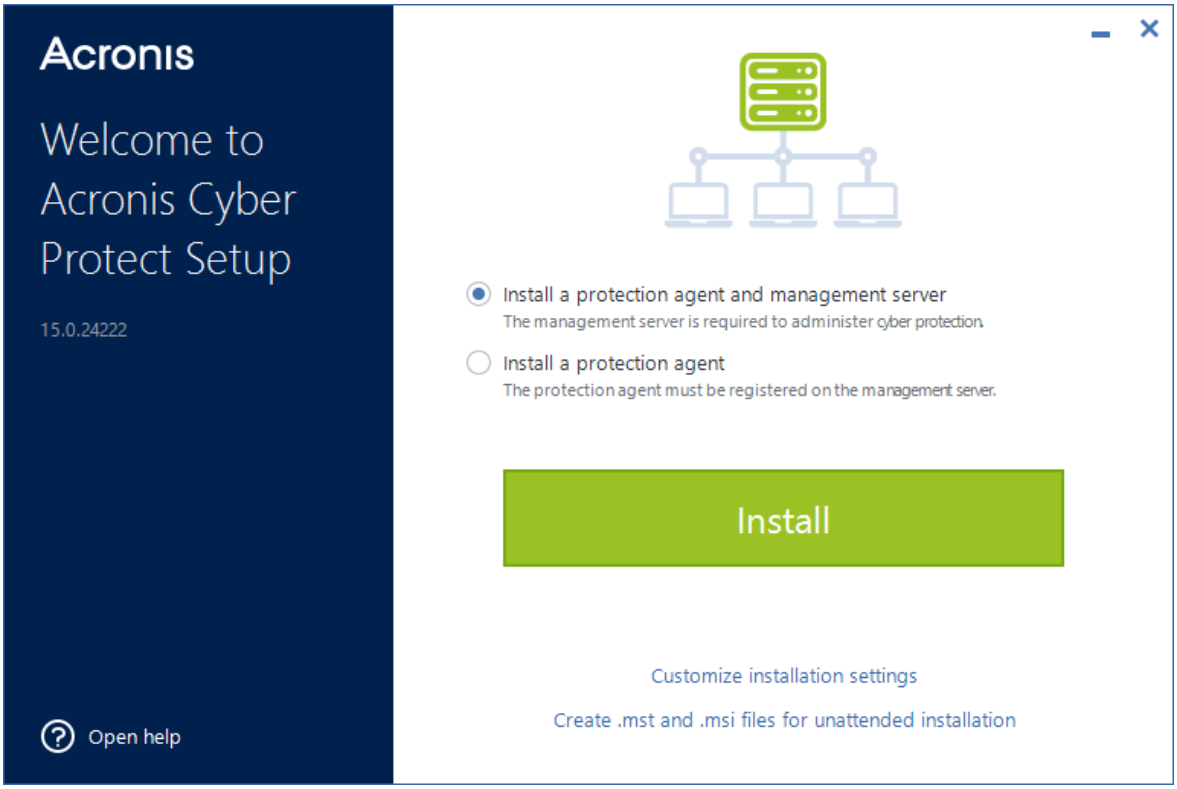
安裝管理伺服器

在 Windows 中安裝

若要安裝管理伺服器

1. 以系統管理員身分登入，並啟動 Acronis Cyber Protect 安裝程式。
2. [選擇性步驟]：若要變更安裝程式的語言，請按一下 **[設定語言]**。
3. 接受授權合約和隱私權聲明的條款，然後按一下 **[下一步]**。

4. 保留預設設定 **[安裝保護代理程式和管理伺服器]**。



5. 執行下列任何一項作業：
   - 按一下 **[安裝]**。
     這是安裝產品的最簡單方法。大部分安裝參數將設為預設值。
     將安裝以下元件：
     - 管理伺服器
     - Components for Remote Installation
     - Windows 用代理程式
     - 其他代理程式 (Hyper-V 用代理程式、Exchange 用代理程式、SQL 用代理程式，以及 Active Directory 用代理程式)，如果電腦上偵測到個別的 Hypervisor 或應用程式
     - 可開機媒體組建
     - 命令列工具
     - Cyber Protect 監視器
   - 按一下 **[自訂安裝設定]** 來設定安裝。
     您可以選擇想要安裝的元件，並指定額外的參數。如需詳細資訊，請參閱 "自訂安裝設定" (第 76 頁)。
   - 按一下 **[為自動安裝建立 .mst 和 .msi 檔案]** 以解壓縮安裝套件。檢閱或修改將新增到 .mst 檔案中的安裝設定，然後按一下 **[產生]**。此程序無需執行更多步驟。
     若要透過「群組原則」部署代理程式，請參閱 "透過群組原則部署代理程式" (第 156 頁)。
6. 繼續安裝。
7. 安裝完成後，請按一下**[關閉]**。

若要開始使用您的管理伺服器，請登入您的 Acronis 帳戶或透過啟用檔案來啟用它。

自訂安裝設定

本節描述可以在安裝期間變更的設定。

要安裝的元件

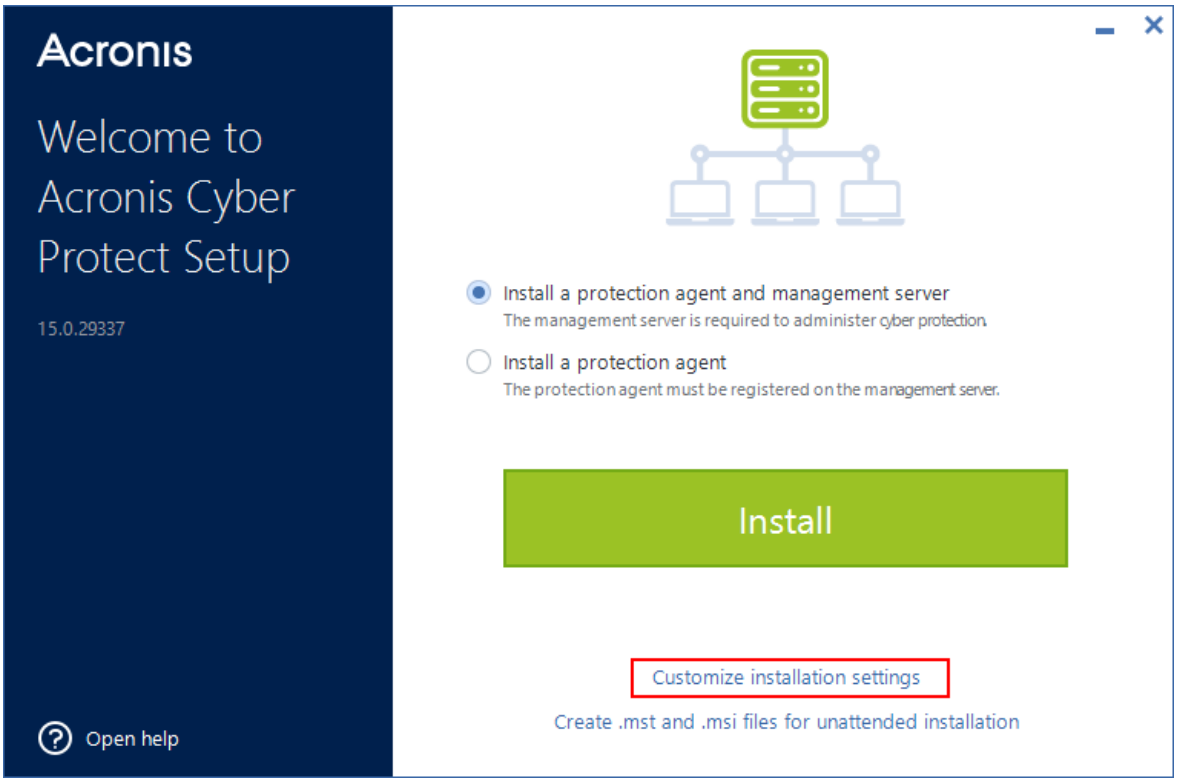
根據您是安裝管理伺服器和保護代理程式，還是僅安裝保護代理程式而定，預設會選取下列元件：

管理伺服器與保護代理程式	僅保護代理程式
管理伺服器	Windows 用代理程式
Components for Remote Installation	可開機媒體組建
Windows 用代理程式	命令列工具
可開機媒體組建	Cyber Protect 監視器
命令列工具	
Cyber Protect 監視器	

如需可用元件的完整清單，請參閱 "元件" (第 44 頁)。

若要安裝選用元件

1. 在安裝精靈中，按一下 **[自訂安裝設定]**。



2. 在 **[要安裝的項目]** 中，按一下 **[變更]**。
3. 選擇所需的元件，然後按一下 **[完成]**。

4. 如果出現提示，請設定所選元件的設定。
5. 按一下 **[安裝]**。

服務登入帳戶

您可以分別使用 **[代理程式服務的登入帳戶]** 和 **[管理伺服器服務的登入帳戶]** 選項來變更執行代理程式或管理伺服器所使用的帳戶。

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。此選項的優點在於，網域安全性原則不會影響這些帳戶的使用者權限。依預設，此代理程式在**本機系統**帳戶下執行。
- **建立新的帳戶**（預設適用於管理伺服器服務以及儲存節點服務）
  代理程式服務、管理伺服器服務，以及儲存節點服務的帳戶名稱分別為 **Acronis Agent User**、**AMS User** 及 **ASN User**。
- **使用下列帳戶**
  若您將產品安裝在網域控制站上，則安裝程式會提示您為每個服務指定現有帳戶（或相同帳戶）。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。
  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。
  此外，如果您使用 SQL 資料庫設定管理伺服器，選擇 **[使用下列帳戶]** 可讓您將 Windows 驗證用於 Microsoft SQL Server。

如果您選擇 **[建立新的帳戶]** 或 **[使用以下帳戶]** 選項，請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獲指派的使用者權限，則相關元件可能會運作不正確或無法運作。

服務登入帳戶所需的使用者權限

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下列權限，代理程式才能正確運作：

1. MMS 使用者必須包含在 **[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. MMS 使用者必須獲授予資料夾 `%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. MMS 使用者必須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. MMS 使用者必須在 Windows 中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**
   - **取代處理程序層級權杖**
   - **修改韌體環境值**

ASN 使用者必須具備安裝 Acronis Storage Node 所在電腦的本機系統管理員權限。

若要在 Windows 中指派使用者權限

注意事項
此程序會使用 **[以服務方式登入]** 使用者權限作為範例。其他使用者權限的設定方式相同。

1. 以系統管理員身分登入電腦。
2. 在 **[控制台]** 中，開啟 **[系統管理工具]**。或者，按下鍵盤上的 Win+R、輸入 **control admintools**，然後按下 Enter。
3. 開啟 **[本機安全性原則]**。
4. 展開 **[本機原則]**，然後按一下 **[使用者權限指派]**。
5. 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]**。
6. 按一下 **[新增使用者或群組...]**，加入新的使用者。
7. 在 **[選擇使用者或群組]** 視窗中，尋找您要新增的使用者，然後按一下 **[確定]**。
8. 在 **[以服務方式登入內容]** 視窗中，按一下 **[確定]** 以儲存變更。

注意事項
您新增至 **[以服務方式登入]** 使用者權限的使用者不得列在 **[本機安全性原則]** 的 **[拒絕以服務方式登入]** 原則中。

重要事項
不建議在安裝完成之後，手動變更登入帳戶。

管理伺服器的資料庫

您可以使用下列資料庫設定管理伺服器：

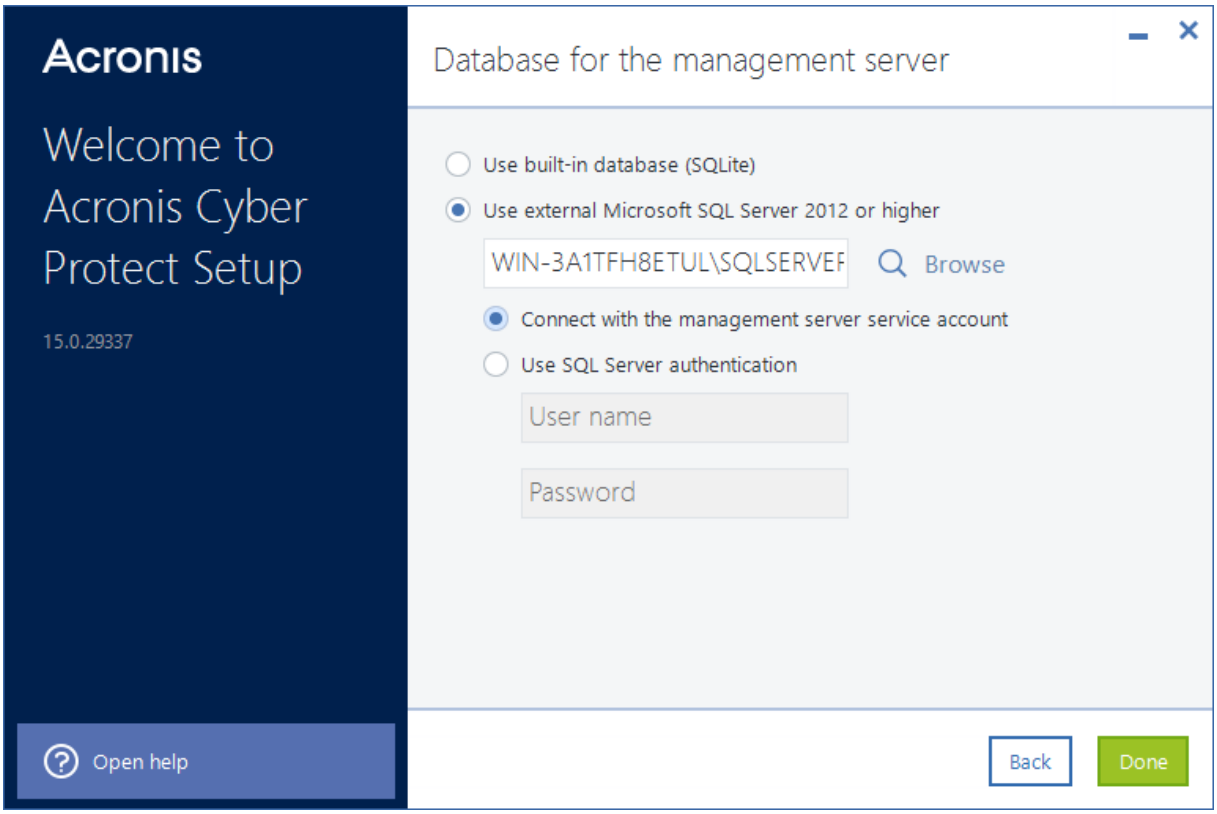
- SQLite

  依照預設，管理伺服器會使用內建的 SQLite 資料庫。其允許在管理伺服器上註冊大約 900-1000 個工作負載。SQLite 與掃描服務不相容，
- Microsoft SQL

  Microsoft SQL 允許在管理伺服器上註冊最多 8000 個工作負載，且不會造成明顯的效能下降。相同的 Microsoft SQL 執行個體可由管理伺服器、掃描服務和其他程式使用。

  支援下列 MS SQL Server 版本：
  - Microsoft SQL Server 2019 (在 Windows 中執行)
  - Microsoft SQL Server 2017 (在 Windows 中執行)
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2014
  - Microsoft SQL Server 2012

如果 Microsoft SQL 執行個體是預設的 **MSSQLSERVER**，您僅能指定執行此執行個體所在電腦的名稱。如果執行個體有自訂名稱，您必須使用下列格式加以指定：電腦名稱\執行個體名稱。



注意事項

請確認在執行 Microsoft SQL 執行個體的電腦上已啟用 SQL Server Browser 服務和 TCP/IP 用戶端通訊協定。如需有關如何啟動 SQL Server Browser 服務的詳細資訊，請參閱 http://msdn.microsoft.com/en-us/library/ms189093.aspx。您可以使用類似的程序啟用 TCP/IP 通訊協定。

若要連線至指定的 Microsoft SQL 執行個體，您可以使用下列驗證方法：

- Windows 驗證 (**使用管理伺服器服務帳戶連線**)

  如果您已使用 **[使用下列帳戶]** 選項設定管理伺服器服務的登入帳戶，例如，透過指定 <電腦名稱>\Administrator，您可以使用此方法。指定的帳戶在 Microsoft SQL Server 中必須具備 **dbcreator** 或 **sysadmin** 角色。

  如需有關登入帳戶的詳細資訊，請參閱 "服務登入帳戶所需的使用者權限" (第 77 頁)。
- SQL Server 驗證

  您一律可以使用此方法。指定的帳戶在 Microsoft SQL Server 中必須具備 **dbcreator** 或 **sysadmin** 角色。

掃描服務

掃描服務是一種選用元件，可在雲端儲存空間、本機資料夾或網路資料夾中，對備份執行反惡意程式碼掃描。掃描服務要求在相同的電腦上安裝管理伺服器。

安裝掃描服務可存取下列功能：

- 備份掃描計劃
- 備份掃描詳細資料桌面小工具
- 公司白名單
- 安全復原
- 備份清單中的 **[狀態]** 欄

您可以在安裝管理伺服器期間安裝掃描服務，或者您稍後可以修改現有的安裝，以新增掃描服務。如需有關如何安裝選用元件作為掃描服務的詳細資訊，請參閱 "若要安裝選用元件" (第 76 頁)。

重要事項

掃描服務與管理伺服器使用的預設 SQLite 資料庫不相容。

您可以使用 Microsoft SQL 或 PostgreSQL 資料庫設定掃描服務。如需有關如何選擇的詳細資訊，請參閱 "用於掃描服務的資料庫" (第 81 頁)。

用於掃描服務的資料庫

掃描服務與管理伺服器的預設資料庫 SQLite 不相容。

如果您的管理伺服器使用 SQLite，則僅能使用 PostgreSQL 資料庫設定掃描服務。支援 PostgreSQL 9.6 和更新版本。

如果您的管理伺服器使用 Microsoft SQL Server，則可以使用相同的資料庫設定掃描服務，而不需要額外的設定。您也可以使用 PostgreSQL 資料庫設定掃描服務。

若要使用 PostgreSQL 資料庫設定掃描服務

1. 在安裝精靈中的 **[用於掃描服務的資料庫]** 底下，按一下 **[變更]**。
2. 選取 **[PostgreSQL Server 資料庫]**。
3. 指定 PostgreSQL 執行個體主機名稱或 IP 位址和連接埠。
4. 針對擁有 **CREATEDB** 權限或本身為 superuser 的使用者，指定其認證。

   注意事項
   不支援 PostgreSQL 10 和更新版本中的 SCRAM-SHA-256 驗證方法。

5. 按一下**[完成]**。

連接埠

您可以自訂網頁瀏覽器將用來存取管理伺服器的連接埠 (預設為 9877)，以及將用於產品元件間通訊的連接埠 (預設為 7780)。安裝完成之後變更後一個連接埠，將需要重新登錄所有元件。

會在安裝期間自動設定 Windows 防火牆。如果使用不同的防火牆，請確保開啟該連接埠並且內送和外送請求可穿過該防火牆。

Proxy 伺服器

您可以在雲端儲存空間中進行備份和復原作業時，選擇保護代理程式是否使用 HTTP Proxy 伺服器。

此外，您要將相同的 Proxy 伺服器用於不同 Acronis Cyber Protect 元件之間的通訊。

若要使用 Proxy 伺服器，請指定其主機名稱或 IP 位址以及連接埠號碼。如果 Proxy 伺服器要求驗證，請指定存取認證。

注意事項
使用 Proxy 伺服器時，無法更新保護定義 (防毒和反惡意程式碼定義、進階偵測定義、弱點評估和修補程式管理定義)。

在 Linux 中安裝

準備

1. 如果要與管理伺服器一併安裝 Linux 用代理程式，請確保必要的 Linux 套件已安裝在電腦上。
2. 選擇由管理伺服器使用的資料庫。

限制

在 Linux 電腦上執行的管理伺服器不支援保護代理程式的遠端安裝，而這是在自動探索等中所使用的。如需有關可能的工作負載的詳細資訊，請參閱我們的知識庫：https://kb.acronis.com/content/69553。

安裝

若要安裝管理伺服器，您需要至少 4 GB 的可用磁碟空間。

若要安裝管理伺服器

1. 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>
   ```

2. 接受授權合約條款。
3. 選擇性步驟：選擇您要安裝的元件。
   依預設，系統會安裝下列元件。
   - 管理伺服器
   - Linux 用代理程式
   - 可開機媒體組建
4. 指定 Web 瀏覽器用來存取管理伺服器的連接埠。預設值為 9877。
5. 指定連接埠用於產品元件間的通訊。預設值為 7780。
6. 按一下**[下一步]**開始安裝。
7. 安裝完成後，選擇 **[開啟 Web 主控台]**，然後按一下 **[結束]**。Cyber Protect Web 主控台將會在預設的網頁瀏覽器中開啟。

若要開始使用您的管理伺服器，請登入您的 Acronis 帳戶或透過啟用檔案來啟用它。

Acronis Cyber Protect 裝置

藉助 Acronis Cyber Protect 裝置，您可使用下列軟體輕鬆取得虛擬機器：

- CentOS
- Acronis Cyber Protect 元件：

- 管理伺服器
- Linux 用代理程式
- VMware 用代理程式 (Linux)

以 .zip 存檔提供裝置。存檔包含 .ovf 和 .iso 檔。您可以部署 .ovf 檔至 ESXi 主機，或使用 .iso 檔啟動現有的虛擬機器。存檔還包含應與 .ovf 位於同一目錄的 .vmdk 檔。

注意事項
VMware Host Client (一種用於管理獨立 ESXi 6.0+ 的 Web 用戶端) 不容許部署內含 ISO 影像的 OVF 範本。若您的情況如此，則建立一個符合以下需求的虛擬機器，並使用 .iso 檔來安裝軟體。

虛擬裝置的需求如下所示：

- 最低系統需求：
  - 2 顆 CPU
  - 6 GB RAM
  - 一個 10 GB 虛擬磁碟 (建議 40 GB)
- 在 VMware 虛擬機器設定中，按一下 **[選項]** 索引標籤 > **[一般]** > **[設定參數]**，然後確認 `disk.EnableUUID` 參數值為 `true`。

限制

在 Linux 電腦上執行的管理伺服器 (包括 Acronis Cyber Protect 裝置) 不支援保護代理程式的遠端安裝，而這是在自動探索等中所使用的。如需有關可能的工作負載的詳細資訊，請參閱我們的知識庫：https://kb.acronis.com/content/69553。

安裝軟體

1. 執行下列其中一項操作：
   - 從 .ovf 部署應用程式。部署完成之後，開啟所產生的電腦電源。
   - 從 .iso 啟動現有的虛擬機器。
2. 選擇 **[安裝或更新 Acronis Cyber Protect]**，然後按 **Enter** 鍵。等待起始安裝視窗顯示。
3. [選擇性步驟] 若要變更安裝設定，選擇 **[變更設定]**，然後按 **Enter** 鍵。您可以指定下列設定：
   - 裝置的主機名稱 (依預設，`AcronisAppliance-<隨機部分>`)。
   - 將用於登入 Cyber Protect Web 主控台之 "root" 帳戶的密碼 (依預設，**未指定**)。
     若保留預設值，則在安裝 Acronis Cyber Protect 之後，系統會提示您指定密碼。若無此密碼，您將無法登入 Cyber Protect Web 主控台以及 Cockpit Web 主控台。
   - 網路介面卡的網路設定：
     - **使用 DHCP** (依預設)
     - **設定靜態 IP 位址**

     若電腦具有數個網路介面卡，則軟體會隨機選擇一個，並對其套用這些設定。
4. 選擇 **[使用現行設定進行安裝]**。

由此，將會在電腦上安裝 CentOS 和 Acronis Cyber Protect。

其他動作

安裝完成之後，軟體會顯示 Cyber Protect Web 主控台以及 Cockpit Web 主控台的連結。連線至 Cyber Protect Web 主控台，即可開始使用 Acronis Cyber Protect：新增更多裝置、建立備份計劃等等。

若要新增 ESXi 虛擬機器，請按一下 **[新增]** > **[VMware ESXi]**，然後指定 vCenter Server 或獨立 ESXi 主機的位址和認證。

沒有任何在 Cockpit Web 主控台中進行設定的 Acronis Cyber Protect 設定。為方便使用而提供用於疑難排解的主控台。

更新軟體

1. 使用新裝置版本下載和解壓縮 .zip 存檔。
2. 從前一個步驟中解壓縮的 .iso 啟動電腦。
   a. 將 .iso 儲存到 vSphere 資料存放區。
   b. 將 .iso 連線至電腦的 CD/DVD 光碟機。
   c. 重新啟動電腦。
   d. [僅在第一次更新期間] 按下 **F2**，然後變更開機順序，讓 CD/DVD 光碟機出現在第一個。
3. 選擇 **[安裝或更新 Acronis Cyber Protect]**，然後按 **Enter** 鍵。
4. 選擇 **[更新]**，然後按 **Enter** 鍵。
5. 更新完成後，請中斷 .iso 與電腦 CD/DVD 光碟機的連線。

由此，將會更新 Acronis Cyber Protect。如果 .iso 檔案中的 CentOS 版本也比磁碟上的版本新，則在更新 Acronis Cyber Protect 之前會先更新作業系統。

從 Cyber Protect Web 主控台新增電腦

您可以透過下列其中一種方式新增電腦：

- 下載安裝程式，然後在本機目標電腦上執行。
- 在目標電腦上遠端安裝保護代理程式。

限制

- 遠端安裝僅適用於在 Windows 電腦上執行的管理伺服器。目標電腦也必須執行 Windows。
- 不支援在執行 Windows XP 的電腦上進行遠端安裝。
- 不支援在網域控制器上進行遠端安裝。若要瞭解如何在網域控制站上安裝保護代理程式，請參閱 "在 Windows 中安裝" (第 92 頁)。請確認您透過選擇 **[代理程式服務的登入帳戶]** 下的 **[使用下列帳戶]** 來自訂安裝設定。若要深入瞭解此選項，請參閱 "服務登入帳戶所需的使用者權限" (第 77 頁)。

新增執行 Windows 的電腦

您可以在 Cyber Protect Web 主控台中遠端安裝保護代理程式，或是在本機下載並執行安裝程式，來新增 Windows 電腦。

若要遠端安裝代理程式

重要事項

開始安裝前，請確認符合遠端安裝的必要條件，而且您的環境中至少有一個可當作部署代理程式使用的代理程式。如需詳細資訊，請參閱 "遠端安裝的必要條件" (第 86 頁) 和 "部署代理程式" (第 87 頁)。

1. 在 Cyber Protect Web 主控台中，移至 **[裝置]** > **[所有裝置]**。
2. 按一下 **[新增]**。
3. [若要安裝 Windows 用代理程式] 按一下 **[Windows]**。
4. [若要安裝另一個支援的代理程式] 按一下對應至您要保護之應用程式的按鈕。

   您可以選取下列代理程式：
   - Hyper-V 用代理程式
   - SQL 用代理程式 + Windows 用代理程式
   - Exchange 用代理程式 + Windows 用代理程式

     如果您按一下 **[Microsoft Exchange Server]** > **[Exchange 信箱]**，且至少已註冊一個 Exchange 用代理程式，則移至步驟 9。
   - Active Directory 用代理程式 + Windows 用代理程式
   - Office 365 用代理程式
5. 在開啟的窗格中，選擇部署代理程式。
6. 指定目標電腦的主機名稱或 IP 位址，以及具有該電腦系統管理權限之帳戶的認證。

   建議您使用內建的系統管理員帳戶。若要使用另一個帳戶，請將該帳戶新增至系統管理員群組，然後修改目標電腦的登錄檔，如下列文章中所述：https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows。
7. 選擇代理程式將用來存取管理伺服器的名稱或 IP 位址。

   依預設，會選擇伺服器名稱。如果您的管理伺服器有超過一個網路介面，或是您遇到造成代理程式註冊失敗的 DNS 問題，您可能需要改為選擇 IP 位址。
8. 按一下 [**安裝**]。
9. [若在步驟 4 中已選擇 **Microsoft Exchange Server** > **Exchange 信箱**] 指定啟用 Microsoft Exchange Server 的 **[用戶端存取]** 伺服器角色 (CAS) 所在的電腦。如需詳細資訊，請參閱 "信箱備份" (第 388 頁)。

若要在本機下載並安裝代理程式

1. 在 Cyber Protect Web 主控台中，按一下右上角的帳戶圖示，然後按一下 **[下載]**。
2. 按一下您需要之 Windows 安裝程式的名稱。

安裝程式會下載到您的電腦中。

3. 在您要保護的電腦上執行安裝程式。如需詳細資訊，請參閱 "在 Windows 中安裝" (第 92 頁)。

遠端安裝的必要條件

- 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]** 選項。
- 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 "若要停用 UAC" (第 86 頁)。
- 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 "若要停用 UAC 遠端限制" (第 87 頁)。
- 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 或更高版本的電腦上] 移至 **[控制台]** > **[Windows 防火牆]** > **[網路和共用中心]** > **[變更進階共用設定]**。
- Acronis Cyber Protect 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。如果您想要在之後從遠端更新代理程式，則必須將連接埠 **445** 和 **43234** 保持為開放狀態。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。

注意事項
不支援在執行 Windows XP 的電腦上進行遠端安裝。

注意事項
不支援在網域控制器上進行遠端安裝。若要瞭解如何在網域控制站上安裝保護代理程式，請參閱 "在 Windows 中安裝" (第 92 頁)。請確認您透過選擇 **[代理程式服務的登入帳戶]** 下的 **[使用下列帳戶]** 來自訂安裝設定。若要深入瞭解此選項，請參閱 "服務登入帳戶所需的使用者權限" (第 77 頁)。

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 **[控制台] > [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**。

部署代理程式

若要從 Cyber Protect Web 主控台在遠端電腦上安裝保護代理程式，您的環境必須至少已經安裝一個代理程式。此代理程式會當作遠端安裝的部署代理程式，而且會連線至管理伺服器和目標遠端電腦。

環境中的第一個保護代理程式通常是您與管理伺服器一起安裝的代理程式。但是，您可以在環境中選擇要當作部署代理程式的 Windows 用代理程式。

注意事項
當您在多部電腦上使用自動探索安裝保護代理程式時，部署代理程式稱為探索代理程式。

部署代理程式的運作方式

1. 部署代理程式會連線至管理伺服器並下載 `web_installer.exe` 檔案。
2. 部署代理程式會使用遠端電腦的主機名稱或 IP 位址，以及您指定的系統管理員認證來連線至該部電腦，然後將 `web_installer.exe` 檔案上傳。
3. `web_installer.exe` 檔案會以自動模式在遠端電腦上執行。
4. 根據所需安裝的範圍，Web 安裝程式會從管理伺服器上的 `installation_files` 資料夾擷取其他安裝套件，然後使用 `msiexec` 命令將它們安裝到目標電腦上。

   `installation_files` 資料夾位於：

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

5. 安裝完成後，會在管理伺服器上註冊代理程式。

要遠端安裝的元件

遠端安裝的元件依預設會在您安裝管理伺服器的時候加以安裝。

根據執行管理伺服器之電腦的作業系統，您可以在下列位置中找到這些元件：

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

如果您已從舊版的 Acronis Cyber Protect 升級或在安裝管理伺服器的時候明確排除**遠端安裝的元件**，這些位置可能不可用。在此情況下，您需要更新並修改 Acronis Cyber Protect 現有的安裝，來手動新增遠端安裝的元件。

若要將遠端安裝的元件新增至現有的安裝

1. 從 Acronis 網站 下載 Acronis Cyber Protect 最新的安裝檔案。
   選擇對應至您作業系統之位元的安裝檔案。在大多數情況下，您會需要 **Windows 64 位元**的安裝檔案。如果您需要在 32 位元電腦遠端安裝保護代理程式，則下載 **Windows 32/64 位元**的安裝檔案。
2. 在執行管理伺服器的電腦上，啟動安裝檔案，然後選擇 **[更新]**。
3. 更新完成後，再次啟動安裝檔案，然後選擇 **[修改目前安裝]**。
4. 選擇 **[遠端安裝的元件]**，然後按一下 **[完成]**。

安裝完成後，您就能夠從 Cyber Protect Web 主控台在遠端電腦上安裝保護代理程式。

新增執行 Linux 的電腦

您只能在本機安裝保護代理程式來新增 Linux 電腦。不支援遠端安裝。

若要新增執行 Linux 的電腦

1. 在 Cyber Protect Web 主控台中，按一下 **[所有裝置]** > **[新增]**。
2. 按一下 **[Linux]**。
   安裝程式會下載到您的電腦中。
3. 在您要保護的電腦上執行安裝程式。如需詳細資訊，請參閱 "在 Linux 中安裝" (第 93 頁)。

新增執行 macOS 的電腦

您只能在本機安裝保護代理程式來新增 macOS 電腦。不支援遠端安裝。

若要新增執行 macOS 的電腦

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

安裝程式會下載到您的電腦中。

3. 在您要保護的電腦上執行安裝程式。如需詳細資訊，請參閱 "在 Mac OS 中安裝" (第 95 頁)。

新增 vCenter 或 ESXi 主機

將 vCenter 或獨立 ESXi 主機新增至管理伺服器有四種方法：

- 部署 VMware 用代理程式 (虛擬裝置)

  在大多數情況下，建議使用此方法。虛擬裝置將會根據您指定的 vCenter，自動部署至每台主機。您可以選擇主機，並自訂虛擬裝置設定。
- 安裝 VMware 用代理程式 (Windows)

  為了進行卸載式備份或不透過 LAN 的備份，您可能想要在執行 Windows 的實體機器上安裝 VMware 用代理程式。
  - **卸載式備份**

    如果您的生產 ESXi 主機負載繁重，而不適合執行虛擬裝置，不妨使用此方法。
  - **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。如需詳細說明，請參閱「不透過 LAN 備份」。

  如果 Windows 中正在執行管理伺服器，代理程式將會自動部署至您指定的電腦。否則，您必須手動安裝代理程式。
- 登錄已安裝的 VMware 用代理程式

  這是在重新安裝管理伺服器之後的必要步驟。此外，您可以註冊及設定從 OVF 範本部署的 VMware 用代理程式 (虛擬裝置)。
- 設定已註冊的 VMware 用代理程式

  這是在手動安裝 VMware 用代理程式 (Windows) 或部署 Acronis Cyber Protect 設備之後的必要步驟。此外，您可以將已設定的 VMware 用代理程式與其他 vCenter Server 或獨立 ESXi 主機相關聯。

從 Web 介面部署 VMware 用代理程式 (虛擬裝置)

1. 按一下**[所有裝置]** > **[新增]**。
2. 按一下 **[VMware ESXi]**。
3. 選擇 **[以虛擬裝置的形式部署至每個 vCenter 的主機]**。
4. 指定 vCenter Server 或獨立 ESXi 主機的位址與存取認證。我們建議使用已指派**系統管理員**角色的帳戶。否則，在 vCenter Server 或 ESXi 中提供具備必要權限的帳戶。
5. 選擇代理程式將用來存取管理伺服器的名稱或 IP 位址。

   依預設，會選擇伺服器名稱。如果您的管理伺服器有超過一個網路介面，或是您遇到造成代理程式註冊失敗的 DNS 問題，您可能需要改為選擇 IP 位址。
6. [選擇性步驟] 按一下 **[設定]** 以自訂部署設定：
   - 您要部署代理程式的 ESXi 主機 (必須在上一步驟中指定 vCenter Server)。
   - 虛擬裝置名稱。

- 裝置所在的資料存放區。
- 將包含裝置的資源集區或 vApp。
- 虛擬裝置的網路介面卡將連線的網路。
- 虛擬裝置的網路設定。您可以選擇 DHCP 自動設定或手動指定值，包括靜態 IP 位址。

7. 按一下 **[部署]**。

安裝 VMware 用代理程式 (Windows)

準備

遵照「新增執行 Windows 的電腦」一節所述的預備步驟。

安裝

1. 按一下**[所有裝置]** > **[新增]**。
2. 按一下 **[VMware ESXi]**。
3. 選擇 **[在執行 Windows 的電腦上遠端安裝]**。
4. 選擇部署代理程式。
5. 指定目標電腦的名稱或 IP 位址，以及在該電腦上具有系統管理權限之帳戶的認證。
6. 選擇代理程式將用來存取管理伺服器的名稱或 IP 位址。
   依預設，會選擇伺服器名稱。如果您的管理伺服器有超過一個網路介面，或是您遇到造成代理程式註冊失敗的 DNS 問題，您可能需要改為選擇 IP 位址。
7. 按一下 **[連線]**。
8. 指定 vCenter Server 或獨立 ESXi 主機的位址和認證，然後按一下 **[連線]**。我們建議使用已指派 **系統管理員** 角色的帳戶。否則，在 vCenter Server 或 ESXi 中提供具備必要權限的帳戶。
9. 按一下 **[安裝]** 以安裝代理程式。

登錄已安裝的 VMware 用代理程式

本節說明經由 Web 介面登錄 VMware 用代理程式。

替代登錄方法：

- 您可以指定在虛擬裝置 UI 中的管理伺服器，登錄 VMware 用代理程式 (虛擬裝置)。請參閱「從 OVF 範本部署 VMware 用代理程式 (虛擬裝置)」一節中「設定虛擬裝置」底下的步驟 3。
- VMware 用代理程式 (Windows) 在進行本機安裝時已註冊。

欲登錄 VMware 用代理程式

1. 按一下**[所有裝置]** > **[新增]**。
2. 按一下 **[VMware ESXi]**。
3. 請選擇 **[登錄已安裝的代理程式]**。
4. 選擇部署代理程式。
5. 如果您註冊 *[VMware 用代理程式 (Windows)]*，請指定安裝代理程式所在電腦的主機名稱或 IP 位址，以及在該電腦上具有系統管理權限之帳戶的認證。

若要登錄 *[VMware 用代理程式 (虛擬裝置)]*，請指定虛擬裝置的主機名稱或 IP 位址，以及 vCenter Server 或執行裝置的獨立 ESXi 主機認證。

6. 選擇代理程式將用來存取管理伺服器的名稱或 IP 位址。
   依預設，會選擇伺服器名稱。如果您的管理伺服器有超過一個網路介面，或是您遇到造成代理程式註冊失敗的 DNS 問題，您可能需要改為選擇 IP 位址。
7. 按一下 **[連線]**。
8. 請指定 vCenter Server 或 ESXi 主機的主機名稱或 IP 位址，以及用於對其進行存取的認證，然後按一下 **[連線]**。我們建議使用已指派**系統管理員**角色的帳戶。否則，在 vCenter Server 或 ESXi 中提供具備必要權限的帳戶。
9. 按一下 **[註冊]** 以註冊代理程式。

設定已註冊的 VMware 用代理程式

本節說明如何在 Web 介面中，將 VMware 用代理程式與 vCenter Server 或 ESXi 相關聯。還有另一個方法，您可以在 VMware 用代理程式 (虛擬裝置) 主控台中執行此項作業。

藉著使用此程序，您還可變更代理程式與 vCenter Server 或 ESXi 的現有關聯。或者，您可在 VMware 用代理程式 (虛擬裝置) 主控台中執行此項作業，或透過按一下 **[設定]** > **[代理程式]** > 該代理程式 > **[詳細資料]** > **vCenter/ESXi**。

若要設定 VMware 用代理程式

1. 按一下**[所有裝置]** > **[新增]**。
2. 按一下 **[VMware ESXi]**。
3. 軟體會顯示依字母順序排列的第一個未設定的 VMware 用代理程式。
   如果管理伺服器上登錄的代理程式皆已設定，請按一下 **[設定已登錄的代理程式]**，然後軟體會顯示依字母順序排列的第一個代理程式。
4. 若有必要，按一下 **[裝有代理程式的電腦]**，然後選擇要設定的代理程式。
5. 指定或變更 vCenter Server 或 ESXi 主機的主機名稱或 IP 位址及用於對其進行存取的認證。我們建議使用已指派**系統管理員**角色的帳戶。否則，在 vCenter Server 或 ESXi 中提供具備必要權限的帳戶。
6. 按一下 **[設定]** 儲存變更。

新增 Scale Computing HC3 叢集

若要將 Scale Computing HC3 叢集新增到 Cyber Protect 管理伺服器

1. 在叢集中部署 Scale Computing HC3 用代理程式 (虛擬裝置)。
2. 設定其與此叢集和 Cyber Protect 管理伺服器的連線。

安裝本機代理程式

在 Windows 中安裝

安裝 Windows 用代理程式、Hyper-V 用代理程式、Exchange 用代理程式、SQL 用代理程式或 Active Directory 用代理程式

1. 以系統管理員身分登入，並啟動 Acronis Cyber Protect 安裝程式。
2. [選擇性步驟]：若要變更安裝程式的語言，請按一下 **[設定語言]**。
3. 接受授權合約和隱私權聲明的條款，然後按一下 **[下一步]**。
4. 選擇 **[安裝保護代理程式]**。
5. 執行下列任何一項作業：
   - 按一下 **[安裝]**。
     這是安裝產品的最簡單方法。大部分安裝參數將設為預設值。
     將安裝以下元件：
     - Windows 用代理程式
     - 其他代理程式 (Hyper-V 用代理程式、Exchange 用代理程式、SQL 用代理程式，以及 Active Directory 用代理程式)，如果電腦上偵測到個別的 Hypervisor 或應用程式
     - 可開機媒體組建
     - 命令列工具
     - Cyber Protect 監視器
   - 按一下 **[自訂安裝設定]** 來設定安裝。
     您可以選擇想要安裝的元件，並指定額外的參數。如需詳細資訊，請參閱 "自訂安裝設定" (第 76 頁)。
   - 按一下 **[為自動安裝建立 .mst 和 .msi 檔案]** 以解壓縮安裝套件。檢閱或修改將新增到 .mst 檔案中的安裝設定，然後按一下 **[產生]**。此程序無需執行更多步驟。
     若要透過「群組原則」部署代理程式，請依 "透過群組原則部署代理程式" (第 156 頁) 中所述繼續。
6. 指定將註冊具有代理程式之電腦的管理伺服器：
   a. 指定已安裝管理伺服器的電腦的名稱或 IP 位址。
   b. 指定管理伺服器系統管理員的認證或註冊權杖。
      如需有關如何產生註冊權杖的詳細資訊，請參閱 "步驟 1：產生註冊權杖" (第 157 頁)。
   c. 按一下 **[完成]**。
7. 若出現提示，則選擇具有代理程式的電腦是新增至組織，還是其中一個單位。
   如果您管理多個單位或具有至少一個單位的組織，則會出現此提示。否則，電腦將以無訊息方式新增至您管理的單位或組織中。如需詳細資訊，請參閱 "單位與系統管理帳戶" (第 545 頁)。
8. 繼續安裝。
9. 安裝完成後，請按一下 **[關閉]**。

10. 若已安裝 Exchange 用代理程式，您將能備份 Exchange 資料庫。如果您想要備份 Exchange 信箱，請開啟 Cyber Protect Web 主控台 、按一下 **[新增]** > **[Microsoft Exchange Server]** > **[Exchange 信箱]**，然後指定啟用 Microsoft Exchange Server 的 **[用戶端存取]** 伺服器角色 (CAS) 所在的電腦。如需詳細資訊，請參閱 "信箱備份" (第 388 頁)。

若要在沒有 Microsoft Exchange Server 的電腦上安裝 VMware 用代理程式 (Windows)、Office 365 用代理程式、Oracle 用代理程式或 Exchange 用代理程式

1. 以系統管理員身分登入，並啟動 Acronis Cyber Protect 安裝程式。
2. [選擇性步驟]：若要變更安裝程式的語言，請按一下 **[設定語言]**。
3. 接受授權合約和隱私權聲明的條款，然後按一下 **[下一步]**。
4. 選擇 **[安裝保護代理程式]**，然後按一下 **[自訂安裝設定]**。
5. 在**[要安裝的項目]** 旁，按一下**[變更]**。
6. 選擇對應於要安裝之代理程式的核取方塊。清除不想要安裝之元件的核取方塊。按一下**[完成]** 以繼續。
7. 指定將註冊具有代理程式之電腦的管理伺服器：
   a. 在 **Acronis Cyber Protect Management Server** 旁邊，按一下 **[指定]**。
   b. 指定已安裝管理伺服器的電腦的名稱或 IP 位址。
   c. 指定管理伺服器系統管理員的認證或註冊權杖。
      如需有關如何產生註冊權杖的詳細資訊，請參閱 "步驟 1：產生註冊權杖" (第 157 頁)。
   d. 按一下**[完成]**。
8. 若出現提示，則選擇具有代理程式的電腦是新增至組織，還是其中一個單位。
   如果您管理多個單位或具有至少一個單位的組織，則會出現此提示。否則，電腦將以無訊息方式新增至您管理的單位或組織中。如需詳細資訊，請參閱 "單位與系統管理帳戶" (第 545 頁)。
9. [選擇性] 變更其他安裝設定，如 "自訂安裝設定" (第 76 頁) 中所述。
10. 按一下**[安裝]** 以開始安裝。
11. 安裝完成後，請按一下**[關閉]**。
12. [僅限安裝 VMware (Windows) 用代理程式時] 執行 "設定已註冊的 VMware 用代理程式" (第 91 頁) 中所述的程序。
13. [僅在安裝 Exchange 用代理程式時] 開啟 Cyber Protect Web 主控台、按一下 **[新增]** > **[Microsoft Exchange Server]** > **[Exchange 信箱]**，然後指定啟用 Microsoft Exchange Server 的 **[用戶端存取]** 伺服器角色 (CAS) 所在的電腦。如需詳細資訊，請參閱 "信箱備份" (第 388 頁)。

在 Linux 中安裝

準備

1. 確保必要的 Linux 套件 已安裝在電腦上。
2. 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 Web 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. 以 root 使用者身分，瀏覽到有安裝檔案 (.i686 或 .x86_64 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>
   ```

2. 接受授權合約條款。
3. 指定要安裝的元件：
   a. 清除 **[AcronisCyber Protect 管理伺服器]** 核取方塊。
   b. 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**
      - **適用於 Oracle 的代理程式**

      Oracle 用代理程式需要也安裝 Linux 用代理程式。
   c. 按 **[下一步]**。
4. 指定將註冊具有代理程式之電腦的管理伺服器：
   a. 指定已安裝管理伺服器的電腦的名稱或 IP 位址。
   b. 指定管理伺服器系統管理員的使用者名稱與密碼。
   c. 按 **[下一步]**。
5. 若出現提示，則選擇具有代理程式的電腦是新增至組織，還是其中一個單位，然後按 **Enter** 鍵。
   如果在之前步驟中指定的帳戶管理多個單位或具有至少一個單位的組織，則會出現此提示。
6. 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。

7. 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 Mac OS 中安裝

安裝 Mac 用代理程式

1. 按兩下安裝檔案 (.dmg)。
2. 請等候作業系統掛載安裝磁碟影像。
3. 按兩下 **[安裝]**，然後按一下 **[繼續]**。
4. [選擇性步驟] 按一下 **[變更安裝位置]** 以變更軟體安裝所在的磁碟。依預設，會選擇系統啟動磁碟。
5. 按一下 **[安裝]**。若出現提示，請輸入系統管理員的使用者名稱和密碼。
6. 指定將註冊具有代理程式之電腦的管理伺服器：
   a. 指定已安裝管理伺服器的電腦的名稱或 IP 位址。
   b. 指定管理伺服器系統管理員的使用者名稱與密碼。
   c. 按一下 **[註冊]**。
7. 若出現提示，則選擇具有代理程式的電腦是新增至組織，還是其中一個單位，然後按一下 **[完成]**。
   如果在之前步驟中指定的帳戶管理多個單位或具有至少一個單位的組織，則會出現此提示。
8. 安裝完成後，請按一下**[關閉]**。

自動安裝或解除安裝

Windows 中的自動安裝或解除安裝

本節描述如何使用 Windows Installer (`msiexec` 程式)，在執行 Windows 的電腦上，以自動模式安裝或解除安裝 Acronis Cyber Protect。在 Active Directory 網域中，執行自動安裝的另外一種方法是透過「群組原則」。請參閱 "透過群組原則部署代理程式" (第 156 頁)。

安裝期間，您可以使用一個稱之為**轉換**的檔案 (即 .mst 檔)。轉換是指帶有安裝參數的檔案。作為替代方案，您還可以直接在命令列中指定安裝參數。

建立 .mst 轉換和解壓縮安裝套件

1. 以系統管理員身分登入並啟動安裝程式。
2. 按一下 **[為自動安裝建立 .mst 和 .msi 檔案]**。
3. [不適用於所有安裝程式] 在 **[元件位元]** 中，選擇 **[32 位元]** 或 **[64 位元]**。
4. 在 **[要安裝的項目]** 中，選擇您要安裝的元件，然後按一下 **[完成]**。
   這些元件的安裝套件會從安裝程式中解壓縮。
5. 在 **Acronis Cyber Protect Management Server** 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 "步驟 1：產生註冊權杖" (第 157 頁)。
6. [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。

7. 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]**。
8. 選擇將產生 .mst 轉換並解壓縮 .msi 和 .cab 安裝套件所在的資料夾，然後按一下 **[產生]**。

因此，將會產生 .mst 轉換，而 .msi 和 .cab 安裝套件將會解壓縮到您指定的資料夾。

使用 .mst 轉換來安裝產品

在命令列上，執行下列命令：

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

其中：

- <封裝名稱> 是 .msi 檔案的名稱。視作業系統的位元而定，此名稱為 **AB.msi** 或 **AB64.msi**。
- <轉換名稱> 是轉換的名稱。視作業系統的位元而定，此名稱為 **AB.msi.mst** 或 **AB64.msi.mst**。

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

透過手動指定參數來安裝或解除安裝產品

在命令列上，執行下列命令：

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

其中，<封裝名稱> 是 .msi 檔案的名稱。視作業系統的位元而定，此名稱為 **AB.msi** 或 **AB64.msi**。

可用的參數及其值詳述於 "一般參數" (第 97 頁) 中。

範例

- 安裝管理伺服器和用於遠端安裝的元件。

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

- 安裝 Windows 用代理程式、命令列工具和 Cyber Protect Monitor。在之前已安裝的管理伺服器上向代理程式登錄電腦。

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

- 更新管理伺服器、儲存節點、目錄服務和保護代理程式。

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

自動安裝或解除安裝參數

此區段說明了在 Windows 中自動安裝或解除安裝期間所使用的參數。

除了這些參數之外，您還可以使用 `msiexec` 的其他參數，如 https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx 中所述。

安裝參數

一般參數

`ADDLOCAL=<list of components>`

要安裝的元件，以逗點區隔，且沒有空格字元。所有指定的元件都必須在安裝之前從安裝程式解壓縮。

完整的元件清單如下。

元件	務必一起安裝	位元	元件名稱 / 說明
AcronisCentralizedManagementServer	WebConsole	32 位元 /64 位元	管理伺服器
WebConsole	AcronisCentralizedManagementServer	32 位元 /64 位元	Web 主控台
ComponentRegisterFeature	AcronisCentralizedManagementServer	32 位元 /64 位元	Components for Remote Installation
AtpScanService	AcronisCentralizedManagementServer	32 位元 /64 位元	掃描服務
AgentsCoreComponents		32 位元	適用於代理程式的核心

		/64 位元	元件
BackupAndRecoveryAgent	AgentsCoreComponents	32 位元 /64 位元	Windows 用代理程式
ArxAgentFeature	BackupAndRecoveryAgent	32 位元 /64 位元	Exchange 用代理程式
ArsAgentFeature	BackupAndRecoveryAgent	32 位元 /64 位元	SQL 用代理程式
ARADAgentFeature	BackupAndRecoveryAgent	32 位元 /64 位元	Active Directory 用代理程式
OracleAgentFeature	BackupAndRecoveryAgent	32 位元 /64 位元	適用於 Oracle 的代理程式
ArxOnlineAgentFeature	AgentsCoreComponents	32 位元 /64 位元	Office 365 用代理程式
AcronisESXSupport	AgentsCoreComponents	32 位元 /64 位元	VMware 用代理程式 (Windows)
HyperVAgent	AgentsCoreComponents	32 位元 /64 位元	Hyper-V 用代理程式
ESXVirtualAppliance		32 位元 /64 位元	VMware 用代理程式 (虛擬裝置)

ScaleVirtualAppliance		32 位元 /64 位元	Scale Computing HC3 用代理程式 (虛擬裝置)
CommandLineTool		32 位元 /64 位元	命令列工具
TrayMonitor	BackupAndRecoveryAgent	32 位元 /64 位元	Cyber Protect 監視器
BackupAndRecoveryBootableComponents		32 位元 /64 位元	可開機媒體組建
PXEServer		32 位元 /64 位元	PXE 伺服器
StorageServer	BackupAndRecoveryAgent	64 位元	儲存節點
CatalogBrowser	JRE 8 Update 111 或更新版本	64 位元	目錄服務

`TARGETDIR=<path>`

產品的安裝資料夾。

`REBOOT=ReallySuppress`

若指定該參數，則會禁止重新啟動電腦。

`CURRENT_LANGUAGE=<language ID>`

產品語言。可用的值如下：`en`、`en_GB`、`cs`、`da`、`de`、`es_ES`、`fr`、`ko`、`it`、`hu`、`nl`、`ja`、`pl`、`pt`、`pt_BR`、`ru`、`tr`、`zh`、`zh_TW`。

`ACEP_AGREEMENT={0,1}`

若值為 1，則該電腦將參與 Acronis 客戶體驗計劃 (ACEP)。

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

已安裝管理伺服器的電腦的主機名稱或 IP 位址。ADDLOCAL 參數中指定的代理程式、儲存節點和目錄服務將會在此管理伺服器上註冊。如果連接埠號碼與預設值 (9877) 不同，則必須填入。

您必須使用此參數指定 REGISTRATION_TOKEN 參數，或 REGISTRATION_LOGIN 和 REGISTRATION_PASSWORD 參數。

REGISTRATION_TOKEN=<token>

在 Cyber Protect Web 主控台中產生的註冊權杖，如透過群組原則部署代理程式中所述。

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

管理伺服器系統管理員的使用者名稱與密碼。

REGISTRATION_TENANT=<unit ID>

組織內的單位。ADDLOCAL 參數中指定的代理程式、儲存節點和目錄服務將會新增至此單位。

若要瞭解單位 ID，請在 Cyber Protect Web 主控台中，按一下 **[設定]** > **[帳戶]**、選擇單位，然後按一下 **[詳細資料]**。

如果沒有 REGISTRATION_TOKEN 或 REGISTRATION_LOGIN 和 REGISTRATION_PASSWORD，此參數沒有作用。在此情況下，元件將新增至組織中。

若無此參數，元件將新增至組織中。

REGISTRATION_REQUIRED={0,1}

註冊失敗時的安裝結果。如果值為 1，表示安裝失敗。如果值為 0，表示即使未註冊元件，安裝還是成功完成。

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

這些彼此互斥的參數定義註冊期間管理伺服器憑證檢查的方法。如果您希望驗證管理伺服器的真實性以防止 MITM 攻擊，請檢查憑證。

如果值為 1，驗證會相應使用系統 CA，或與產品一起提供的 CA 套件。如果指定固定的公開金鑰，驗證會使用此金鑰。如果值為 0 或未指定參數，則不會執行憑證驗證，但是註冊流量仍維持加密狀態。

/l*v <log file>

如果指定該參數，則詳細模式下的安裝記錄將會儲存至指定的檔案中。記錄檔可用於分析安裝問題。

管理伺服器安裝參數

WEB_SERVER_PORT=<port number>

Web 瀏覽器用來存取管理伺服器的連接埠。預設連接埠為 9877。

AMS_ZMQ_PORT=<port number>

將用於產品元件間通訊的連接埠。預設連接埠為 7780。

`SQL_INSTANCE=<instance>`

將由管理伺服器使用的資料庫。您可以選擇 Microsoft SQL Server 2012、Microsoft SQL Server 2014 或 Microsoft SQL Server 2016 的任何一種版本。其他的程式也能使用您選擇的執行個體。

若無此參數，將會使用內建的 SQLite 資料庫。

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

Microsoft SQL Server 登入帳戶的認證。管理伺服器將使用這些認證連線至所選的 SQL Server 執行個體。如果沒有這些參數，管理伺服器將使用管理伺服器服務帳戶的認證 (**AMS User**)。

將執行管理伺服器服務所用的帳戶

指定下列其中一個參數：

- `AMS_USE_SYSTEM_ACCOUNT={0,1}`
  如果值為 1，將會使用系統帳戶。
- `AMS_CREATE_NEW_ACCOUNT={0,1}`
  如果值為 1，將會建立新帳戶。
- `AMS_SERVICE_USERNAME=<user name>` 和 `AMS_SERVICE_PASSWORD=<password>`
  將使用指定的帳戶。

代理程式安裝參數

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

代理程式所使用的 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。

`HTTP_PROXY_ONLINE_BACKUP={0,1}`

如果值為 0 或未指定參數，代理程式僅會將 Proxy 伺服器用於從雲端備份和復原。如果值為 1，代理程式也會透過 Proxy 伺服器連線至管理伺服器。

`SET_ESX_SERVER={0,1}`

如果值為 0，則要安裝的 VMware 用代理程式將不會連線至 vCenter Server 或 ESXi 主機。安裝之後，依照 < 設定已註冊的 VMware 用代理程式 > 中的描述繼續執行。

如果值為 1，請指定以下參數：

`ESX_HOST=<host name or IP address>`

vCenter Server 或 ESXi 主機的主機名稱或 IP 位址。

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

用於存取 vCenter Server 或 ESXi 主機的認證。

將執行代理程式服務所用的帳戶

指定下列其中一個參數：

- MMS_USE_SYSTEM_ACCOUNT={0,1}
  如果值為 1，將會使用系統帳戶。
- MMS_CREATE_NEW_ACCOUNT={0,1}
  如果值為 1，將會建立新帳戶。
- MMS_SERVICE_USERNAME=<user name> 和 MMS_SERVICE_PASSWORD=<password>
  將使用指定的帳戶。

儲存節點安裝參數

將執行儲存節點服務所用的帳戶

指定下列其中一個參數：

- ASN_USE_SYSTEM_ACCOUNT={0,1}
  如果值為 1，將會使用系統帳戶。
- ASN_CREATE_NEW_ACCOUNT={0,1}
  如果值為 1，將會建立新帳戶。
- ASN_SERVICE_USERNAME=<user name> 和 ASN_SERVICE_PASSWORD=<password>
  將使用指定的帳戶。

目錄服務安裝參數

CATALOG_DATA_MIGRATION_PATH=<path>

使用此參數，將目錄資料移轉至 Acronis Cyber Protect 15 Update 4 中的新版本目錄服務。指定將要匯出目錄資料的暫存資料夾路徑。

SKIP_CATALOG_DATA_MIGRATION=1

使用此參數可略過移轉目錄資料。

SKIP_CATALOG_DATA_MIGRATION 和 CATALOG_DATA_MIGRATION_PATH 參數是彼此互斥的。

解除安裝參數

REMOVE={<list of components>|ALL}

要移除的元件，以逗點區隔，且沒有空格字元。

在本區段的前面部分說明了可用的元件。

如果值為 ALL，將會解除安裝所有產品元件。此外，您還可以指定下列參數：

DELETE_ALL_SETTINGS={0, 1}

如果值為 1，則會移除產品的記錄、工作與組態設定。

Linux 中的自動安裝或解除安裝

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 Acronis Cyber Protect。

若要安裝或解除安裝產品

1. 開啟終端機。
2. 執行下列命令：

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

   其中，<封裝名稱> 是安裝套件 (.i686 或 .x86_64 檔案) 的名稱。
3. [只有在安裝 Linux 用代理程式時] 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。

安裝參數

一般參數

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

要安裝的元件，以逗點區隔，且沒有空格字元。

下列元件可用於安裝：

元件	元件說明
AcronisCentralizedManagementServer	管理伺服器
BackupAndRecoveryAgent	Linux 用代理程式
BackupAndRecoveryBootableComponents	可開機媒體組建

若無此參數，則將安裝以上所有元件。

`--language=<language ID>`

產品語言。可用的值如下：en、en_GB、cs、da、de、es_ES、fr、ko、it、hu、nl、ja、pl、pt、pt_BR、ru、tr、zh、zh_TW。

`{-d|--debug}`

若指定此參數，則會在詳細模式下寫入安裝記錄。記錄位於 **/var/log/trueimage-setup.log** 檔案中。

{-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}

若指定此參數，則在安裝期間可不需要使用 Linux 套件。

管理伺服器安裝參數

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

Web 瀏覽器用來存取管理伺服器的連接埠。預設連接埠為 9877。

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

將用於產品元件間通訊的連接埠。預設連接埠為 7780。

代理程式安裝參數

指定下列其中一個參數：

- --skip-registration
  - 請勿在管理伺服器上註冊代理程式。
- {-C |--ams=}<host name or IP address>
  - 已安裝管理伺服器的電腦的主機名稱或 IP 位址。代理程式將在此管理伺服器上註冊。

如果您在單一命令中安裝代理程式和管理伺服器，則不論 -C 參數為何，代理程式都會在此管理伺服器上註冊。

您必須使用此參數指定 token 參數，或 login 和 password 參數。

--token=<token>

在 Cyber Protect Web 主控台中產生的註冊權杖，如透過群組原則部署代理程式中所述。

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

管理伺服器系統管理員的認證。

--unit=<unit ID>

組織內的單位。代理程式將會新增至此單位中。

若要瞭解單位 ID，請在 Cyber Protect Web 主控台中，按一下 **[設定]** > **[帳戶]**、選擇單位，然後按一下 **[詳細資料]**。

若無此參數，代理程式將新增至組織中。

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

註冊期間管理伺服器憑證檢查的方法。如果您希望驗證管理伺服器的真實性以防止 MITM 攻擊，請檢查憑證。

如果值為 `https` 或未指定參數，則不會執行憑證驗證，但是註冊流量仍維持加密狀態。如果值*不是* `https`，檢查會相應使用系統 CA，或與產品一起提供的 CA 套件或固定的公開金鑰。

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

固定的公開金鑰值。只應單獨指定此參數，或與 `--reg-transport=https-pinned-public-key` 參數一起指定。

- `--http-proxy-host=<IP address>` 和 `--http-proxy-port=<port>`
  - 代理程式將用於從雲端備份和環境，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。
- `--no-proxy-to-ams`
  - 保護代理程式將會連接到管理伺服器，而且不使用 `--http-proxy-host` 和 `--http-proxy-port` 參數所指定的 Proxy 伺服器。

解除安裝參數

`{-u|--uninstall}`

解除安裝產品。

`--purge`

移除產品記錄、工作和組態設定。

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。

範例

- 安裝管理伺服器。

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

- 安裝 Management Server、指定自訂連接埠。

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

- 安裝 Linux 用代理程式，並在指定的 Management Server 上註冊。

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

- 安裝 Linux 用代理程式，並在指定單位的指定管理伺服器上註冊。

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

macOS 中的自動安裝或解除安裝

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、註冊以及解除安裝保護代理程式。如需有關如何下載安裝檔案 (.dmg) 的資訊，請參閱「新增執行 macOS 的電腦」。

安裝 Mac 用代理程式

1. 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。
2. 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，**AcronisCyberProtect_15_MAC.dmg**。
3. 執行安裝程式。

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

4. 卸離安裝檔案 (.dmg)。

   ```
   hdiutil detach <dmg_root>
   ```

範例

- ```
  mkdir mydirectory
  ```

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

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

  ```
  hdiutil detach mydirectory
  ```

若要註冊 Mac 用代理程式

執行下列其中一項操作：

- 以特定系統管理員帳戶的身分註冊代理程式。

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

  <管理伺服器位址:連接埠> 是安裝 Acronis Cyber Protect Management Server 所在電腦的主機名稱或 IP 位址。如果連接埠號碼與預設值 (9877) 不同，則必須填入。

  <使用者名稱> 和 <密碼> 是註冊代理程式所使用之系統管理員帳戶的認證。
- 註冊特定單位中的代理程式。

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

  若要瞭解單位 ID，請在 Cyber Protect Web 主控台中，按一下 **[設定]** > **[帳戶]**、選擇所需的單位，然後按一下 **[詳細資料]**。

  重要事項

  系統管理員只能透過在其組織階層的層級指定單位 ID 來註冊代理程式。單位系統管理員可以註冊其自己單位及其子單位中的電腦。組織系統管理員可以註冊所有單位中的電腦。如需有關不同系統管理員帳戶的詳細資訊，請參閱「管理使用者帳戶與組織單位」。
- 使用註冊權杖註冊代理程式。

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

  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。您可以在 Cyber Protect Web 主控台中產生一個註冊權杖，如「透過群組原則部署代理程式」中所述。
  ```

重要事項
在 macOS 10.14 或更新版本中，您需要授予保護代理程式完整磁碟存取權。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。

範例

使用使用者名稱與密碼註冊。

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

使用單位 ID 和系統管理員認證註冊。

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

使用權杖註冊。

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

若要解除安裝 Mac 用代理程式

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 Mac 用代理程式，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
  ```

手動註冊電腦

除了在代理程式安裝期間，於 Cyber Protect 管理伺服器上註冊電腦之外，您還可以使用命令列介面進行註冊。如果您已經安裝代理程式但自動註冊失敗，或者如果您想要使用新的帳戶註冊現有的電腦，您可能需要執行此動作。

註冊電腦

在安裝代理程式所在電腦的命令提示字元下，執行下列其中一個命令：
  ```

- 若要以特定系統管理員帳戶的身分註冊電腦：

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

  <註冊工具的路徑> 是：
  - 在 Windows 中：`%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe`
  - 在 Linux 中：`/usr/lib/Acronis/RegisterAgentTool/RegisterAgent`
  - 在 macOS 中：`/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent`

  <管理伺服器位址:連接埠> 是安裝 Acronis Cyber Protect Management Server 所在電腦的主機名稱或 IP 位址。如果您使用預設連接埠 9877，則不需要明確地指定連接埠。

  <使用者名稱> 和 <密碼> 是註冊代理程式所使用之系統管理員帳戶的認證。
- 若要註冊特定單位中的電腦，請指定單位 ID：

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

  若要瞭解單位 ID，請在 Cyber Protect Web 主控台中，按一下 **[設定]** > **[帳戶]**、選擇所需的單位，然後按一下 **[詳細資料]**。

  重要事項
  系統管理員只能在其組織階層的層級註冊代理程式。單位系統管理員可以註冊其自己單位及其子單位中的代理程式。組織系統管理員可以註冊所有單位中的代理程式。如需有關不同系統管理員帳戶的詳細資訊，請參閱「管理使用者帳戶與組織單位」。
- 若要使用註冊權杖註冊電腦：

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

  - 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「透過群組原則部署代理程式」。

取消註冊電腦

在安裝代理程式所在電腦的命令提示字元下，執行下列命令：

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

範例

Windows

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

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

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

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

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

Linux

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

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

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

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

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

macOS

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

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

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

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

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

包含特殊字元或空格的密碼

如果您的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：

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

範例 (Windows)：

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

如果您仍然收到錯誤：

1. 在 https://www.base64encode.org/，將密碼編碼為 base64 格式。
2. 在命令列上，使用 -b 或 --base64 參數指定編碼的密碼。

範例 (Windows)：

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

檢查軟體更新

此功能僅限組織管理員使用。

每次登入 Cyber Protect Web 主控台時，Acronis Cyber Protect 都會檢查 Acronis 網站上是否有新版本可用。若有新版本可用，則 Cyber Protect Web 主控台會在 **[裝置]**、**[計劃]** 和 **[備份儲存]** 索引標籤下的每頁底端，顯示新版本的下載連結。此連結也可以在 **[設定]** > **[代理程式]** 頁面上找到。

若要啟用或停用自動檢查更新，請變更 **[更新]** 系統設定。

若要手動檢查更新，則按一下右上角的問號圖示 > **[關於]** > **[檢查更新]**，或問號圖示 > **[檢查更新]**。

移轉管理伺服器

您可以將在 Windows 電腦上執行的管理伺服器，移轉至相同環境中的另一部 Windows 電腦。

移轉程序包含下列階段：

1. "來源電腦的相關作業" (第 112 頁)
   在此階段中，您會在原始的管理伺服器上準備資料來進行移轉。

2. "目標電腦的相關作業" (第 113 頁)

   在此階段中，您會安裝並設定新的管理伺服器，然後將原始伺服器的資料複製到新的位置。

必要條件

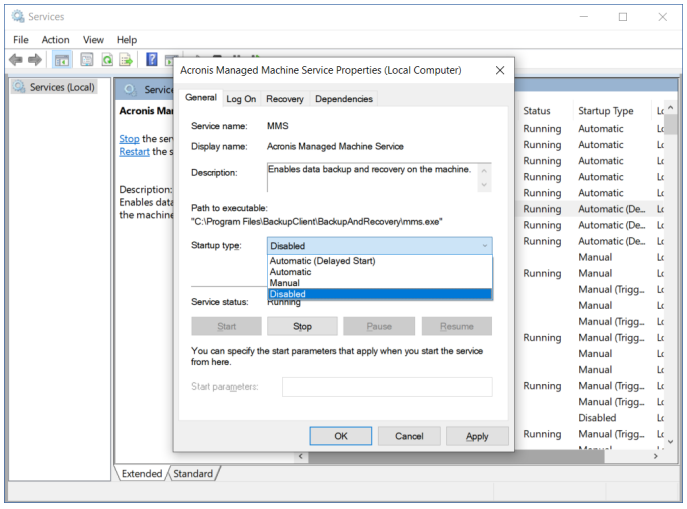
- 管理伺服器會使用外部的 Microsoft SQL Server 資料庫。Microsoft SQL Server 執行個體會在專用電腦上執行。
- 保護代理程式在管理伺服器上註冊時，使用的是其主機名稱，而非 IP 位址。
- 管理伺服器的版本是 Acronis Cyber Protect Update 4 (組建 29486) 或更新版本。
- 相同版本的管理伺服器會安裝在來源和目標電腦上。

來源電腦的相關作業

在此階段中，您會從原始的管理伺服器準備資料來進行移轉。

若要準備資料來進行移轉

1. 在原始管理伺服器的電腦上，停止所有 Acronis 服務。
   a. 開啟 **[服務]**，然後停用 Acronis 服務的啟動，但 **Acronis Active Protection Service** 和 **Acronis Cyber Protection Service** 除外。



   b. 開啟 **[Regedit]**，然後透過編輯金鑰來停用 **Acronis Active Protection Service** 和 **Acronis Cyber Protection Service**：
      - 在金鑰 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisCyberProtectionService` 中，開啟 **[開始]** 值，然後將值資料設為 4。
      - 在金鑰 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisActiveProtectionService` 中，開啟 **[開始]** 值，然後將值資料設為 4。
2. 重新啟動管理伺服器的電腦，然後確認已停用的 Acronis 服務未在執行中。

注意事項
Acronis Scheduler Service Helper 和 **Acronis TIB Mounter Monitor** 這兩項服務可能仍在執行中。您可以安全地忽略它們。

3. [如果 Cyber Protect 監視器元件安裝在管理伺服器的電腦上] 離開 Acronis Cyber Protect 監視器。
4. 在 Windows 命令提示字元中，透過執行下列命令來變更 `%ProgramData%\Acronis` 和 `%ProgramFiles%\Acronis` 資料夾的擁有者：

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

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

5. 透過執行下列命令，來編輯這些資料夾及其子資料夾的存取權限：

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

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

6. 將 `%ProgramData%\Acronis` 和 `%ProgramFiles%\Acronis` 資料夾複製到新管理伺服器電腦可以存取的網路共用。
7. 關閉原始的管理伺服器電腦。

接下來，請遵循 "目標電腦的相關作業" (第 113 頁) 中的程序。

目標電腦的相關作業

在此階段中，您會安裝並設定新的管理伺服器，然後將資料移轉過去。

在目標電腦上執行作業前，請確認您已完成 "來源電腦的相關作業" (第 112 頁) 中的程序。

若要將資料移轉至新的管理伺服器

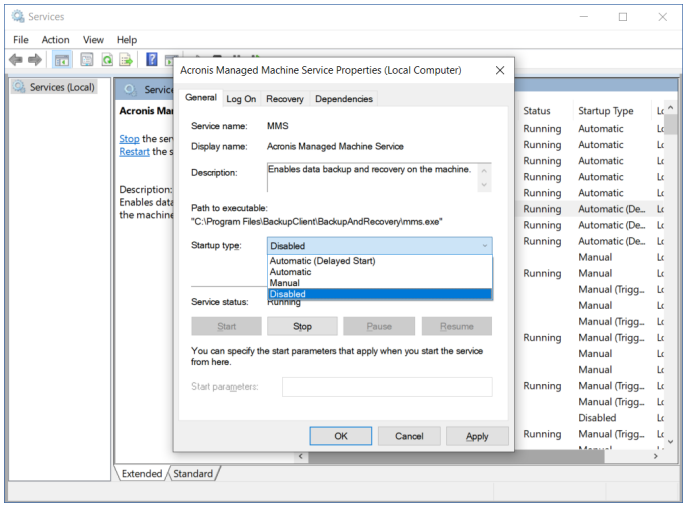
1. 設定您會安裝新管理伺服器之電腦的主機名稱。此名稱必須與原始管理伺服器的電腦名稱相同。
2. 建立防火牆規則來封鎖 TCP 連接埠 9877 上的所有流量。
3. 執行 Acronis Cyber Protect 安裝程式。
   a. 接受授權合約和隱私權聲明的條款，然後按一下 **[下一步]**。
   b. 按一下**[自訂安裝設定]**。
   c. 在 **[要安裝的項目]** 中，僅選擇下列元件，然後按一下 **[完成]**。
      - 管理伺服器
      - Components for Remote Installation
      - 可開機媒體組建
      - 命令列工具

d. 在 **[管理伺服器的資料庫]** 中，保留預設選項 **[使用內建的 SQLite]**。

e. 在 **[管理伺服器服務的登入帳戶]** 中，使用與原始管理伺服器相同的選項。

4. 停止所有的 Acronis 服務。

   a. 開啟 **[服務]**，然後停用所有 Acronis 服務的啟動。

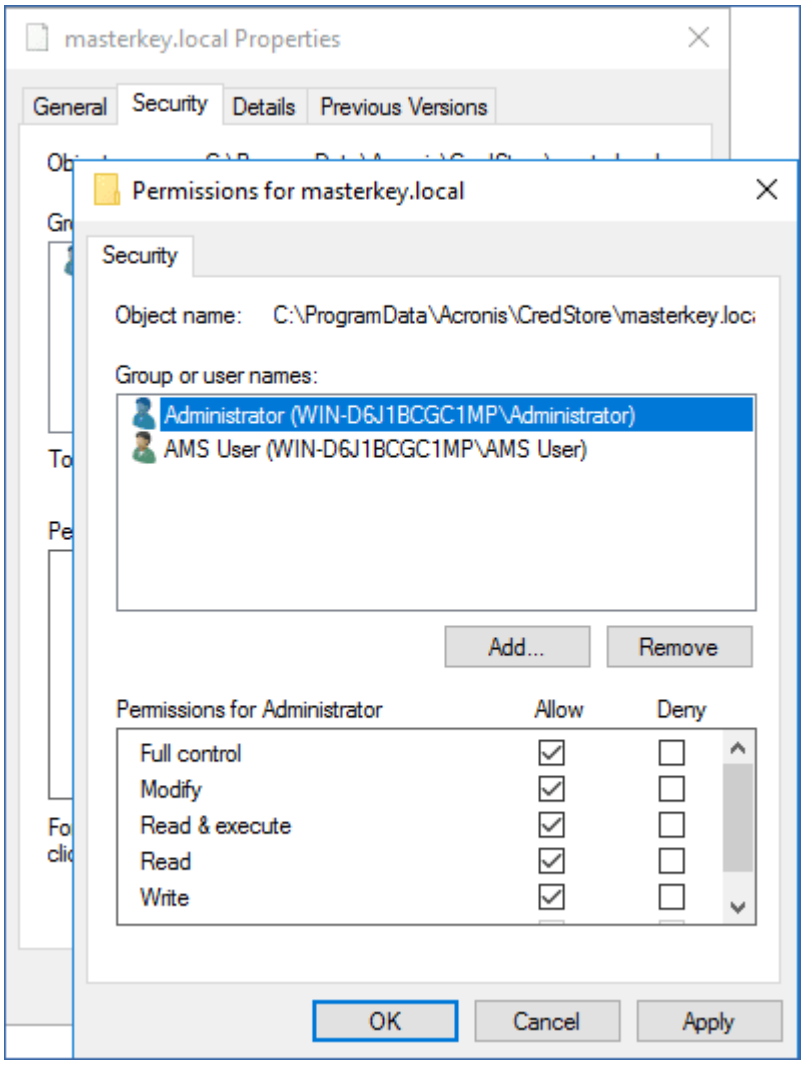


   b. 重新啟動電腦，然後確認已停用的 Acronis 服務未在執行中。

5. 瀏覽至 `%ProgramData%\Acronis\CredStore`，然後調整 `masterkey.local` 檔案的權限，如下所示：

   a. 為 **[系統管理員]** 使用者帳戶授予檔案所有權。

   b. 為 **[系統管理員]** 使用者帳戶授予 **[完整控制]** 權限。



6. 瀏覽至 `%ProgramData%\Acronis\AMS\AccessVault\config`，然後為 **[系統管理員]** 使用者帳戶授予下列檔案的 **[完整控制]** 權限：
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred`
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred.json`
7. 用您從原始管理伺服器電腦複製到網路共用的資料夾取代下列資料夾：
   - `%ProgramData%\Acronis`
   - `%ProgramFiles%\Acronis`

   重要事項
   覆寫現有資料夾前先不要刪除。

   注意事項
   如果您看到無法取代 `%ProgramFiles%\Acronis\ShellExtentions` 資料夾的訊息，您可以安全地略過此資料夾。

8. 還原下列檔案的權限：

- `%ProgramData%\Acronis\CredStore\masterkey.local` – 從具有權限的使用者清單中移除 **[系統管理員]** 使用者帳戶。
- `%ProgramData%\Acronis\AMS\AccessVault\config\preferred` – 僅為 **[系統管理員]** 使用者帳戶授予 **[讀取]** 權限。
- `%ProgramData%\Acronis\AMS\AccessVault\config\preferred.json` – 僅為 **[系統管理員]** 使用者帳戶授予 **[讀取]** 權限。

9. 為 `NGMP\latest` 資料夾建立目錄連接。
   - 在 Windows 命令提示字元中，瀏覽至 `%ProgramData%\Acronis\NGMP`，然後刪除 [最新項目] 資料夾。

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

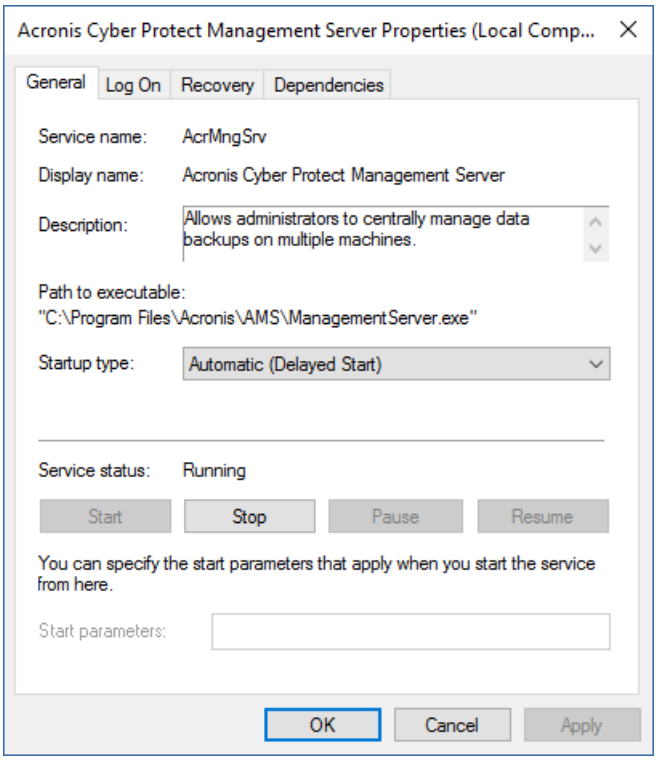
     ```
     rmdir latest
     ```

   - 建立目錄連接 [最新項目]，然後將其指向至以目前 NGMP 版本命名的資料夾，例如：

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

10. 將新的管理伺服器指向至原始管理伺服器使用的 Microsoft SQL Server 資料庫。
    a. 開啟 **[Regedit]**。
    b. 在金鑰 `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\AMS\Settings` 中，透過將資料變更為 `config://C:\ProgramData\Acronis\AMS\mssql\dml_mssql.config` 來修改 `AmsDmlDbProtocol` 值。
11. 開啟 **[服務]**，然後啟用所有已停用的 Acronis 服務。

    將 **Acronis Cyber Protect Management Server** 的啟動類型設為 **[自動 (延遲啟動)]**，並將所有其他 Acronis 服務的啟動類型設為 **[自動]**。



12. 在防火牆中，允許 TCP 連接埠 9877 上的所有流量。
13. 重新啟動電腦，然後確認所有的 Acronis 服務正在執行中。
14. 執行 Acronis Cyber Protect 安裝程式，然後安裝下列項目：
    - Windows 用代理程式
    - [選用] Cyber Protect 監視器
15. 重新啟動電腦。

雲端部署

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：

- **帳戶啟用連結。**按一下連結，然後設定帳戶的密碼。記住顯示在帳戶啟用頁面上的登入。
- **Cyber Protect Web 主控台登入頁面的連結。**日後可使用此連結來存取主控台。登入與密碼和上個步驟使用的相同。

準備

步驟 1

選擇代理程式，視您要備份的內容而定。如需有關代理程式的資訊，請參閱 "元件" (第 44 頁)。

步驟 2

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 "透過群組原則部署代理程式" (第 156 頁) 中。

若要下載 Office 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]** > **[Office 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，才能在網路保護服務中註冊電腦。如果沒有網際網路連線，安裝將無法成功執行。

步驟 3

在進行安裝前，請確保您的防火牆及網路安全系統的其他元件 (例如 Proxy 伺服器) 可同時允許透過下列 TCP 連接埠的輸入和輸出連線。

- 連接埠 **443** 和 **8443**

  這些連接埠用於存取 Cyber Protect Web 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 "Proxy 伺服器設定" (第 119 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 **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。

步驟 4

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。

Active Protection 服務正在監聽 TCP 連接埠 **6109**。請確認無其他程序正在使用該連接埠。

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`

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，代理程式會在雲端登錄本身，因此必須在安裝期間或事先提供 Proxy 伺服器設定。

在 Windows 中

如果已在 Windows (**[控制台]** > **[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。此外，您也可以在安裝期間輸入 Proxy 設定，或使用以下所述的程序，事先加以指定。若要在安裝後變更 Proxy 設定，請使用相同的程序。

若要在 Windows 中指定 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. 複製以下各行並貼到檔案中：

```
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. 如果尚未安裝保護代理程式，您可以現在安裝。或者，進行下列動作來重新啟動代理程式：
   a. 在 **[開始]** 功能表中，按一下 **[執行]**，然後輸入：**cmd**
   b. 按一下 **[確定]**。
   c. 執行以下命令：

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

在 Linux 中

利用參數 `--http-proxy-host=位址` `--http-proxy-port=連接埠` `--http-proxy-login=登入` `--http-proxy-password=密碼` 執行安裝檔案。若要在安裝後變更 Proxy 設定，請使用以下所述的程序。

若要在 Linux 中變更 Proxy 設定

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

   - 否則，複製以上幾行，並將其貼入檔案的 `<registry name="Global">...</registry>` 標籤之間。
3. 將 位址 取代為新的 Proxy 伺服器主機名稱/IP 位址，並將 連接埠 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 登入 和 密碼 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
```

在 macOS 中

您可以在安裝期間輸入 Proxy 設定，或使用以下所述的程序，事先加以指定。若要在安裝後變更 Proxy 設定，請使用相同的程序。

若要在 macOS 中指定 Proxy 設定

1. 建立 **/Library/Application Support/Acronis/Registry/Global.config** 檔案，然後在文字編輯器中開啟此檔案，例如「文字編輯」。
2. 將以下幾行複製並貼到檔案中
   <?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. 如果尚未安裝保護代理程式，您可以現在安裝。或者，進行下列動作來重新啟動代理程式：
   a. 前往 **[應用程式]** > **[公用程式]** > **[終端機]**
   b. 執行以下命令：

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

在可開機媒體中

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。若要指定 Proxy 伺服器設定，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。

安裝代理程式

在 Windows 中

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)：
   - 變更要安裝的元件 (特別是，停用 Cyber Protect 監視器和命令列工具的安裝)。
   - 變更在網路保護服務中註冊電腦的方法。您可以從 **[使用 Cyber Protect 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。
   - 變更代理程式服務的帳戶。
   - 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] 針對要讓代理程式備份其虛擬機器的 vCenter Server 或獨立 ESXi 主機，指定位址和存取認證，然後按一下 **[完成]**。我們建議使用已指派**系統管理員**角色的帳戶。否則，在 vCenter Server 或 ESXi 中提供具備必要權限的帳戶。
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 Cyber Protect 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. 執行下列其中一項操作：
   - 按一下 **[登錄電腦]**。在開啟的瀏覽器視窗中，登入 Cyber Protect Web 主控台、檢閱註冊詳細資料，然後按一下 **[確認註冊]**。
   - 按一下 **[顯示註冊資訊]**。安裝程式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。在這個案例中，您需要在註冊表單中輸入註冊碼。註冊碼的有效期限為一小時。

     或者，您可以按一下 **[所有裝置]** > **[新增]**、向下捲動至 **[透過代碼註冊]**，然後按一下 **[註冊]** 來存取註冊表單。
9. **注意事項**
   請勿結束安裝程式，直到您確認註冊為止。若要再次起始登錄，您必須重新啟動安裝程式，然後按一下 **[登錄電腦]**。

   因此，電腦將會指派給用於登入 Cyber Protect Web 主控台的帳戶。

在 Linux 中

1. 確定電腦已連線到網際網路。
2. 以 root 使用者身分執行安裝檔案。

   如果您的網路中已啟用 Proxy 伺服器，執行檔案時，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=位址 --http-proxy-port=連接埠 --http-proxy-login=登入--http-proxy-password=密碼`。

   如果您要變更在網路保護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**

沒有 Linux 用代理程式便無法安裝 Virtuozzo 用代理程式。

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，請輸入網路保護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. 執行下列其中一項操作：
   - 按一下 **[登錄電腦]**。在開啟的瀏覽器視窗中，登入 Cyber Protect Web 主控台、檢閱註冊詳細資料，然後按一下 **[確認註冊]**。
   - 按一下 **[顯示註冊資訊]**。安裝程式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。在這個案例中，您需要在註冊表單中輸入註冊碼。註冊碼的有效期限為一小時。

     或者，您可以按一下 **[所有裝置]** > **[新增]**、向下捲動至 **[透過代碼註冊]**，然後按一下 **[註冊]** 來存取註冊表單。

6. **注意事項**

   請勿結束安裝程式，直到您確認註冊為止。若要再次啟動註冊，您必須重新啟動安裝程式，然後重複安裝程序。

   因此，電腦將會指派給用於登入 Cyber Protect Web 主控台的帳戶。
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

   在安裝期間會產生一個新的金鑰，用來簽署 snapapi 模組，並註冊為電腦擁有者金鑰 (MOK)。您必須重新啟動，才能註冊此金鑰。如果沒有註冊金鑰，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，請重複安裝步驟，包括註冊 6。

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

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. 執行下列其中一項操作：
   - 按一下 **[登錄電腦]**。在開啟的瀏覽器視窗中，登入 Cyber Protect Web 主控台、檢閱註冊詳細資料，然後按一下 **[確認註冊]**。
   - 按一下 **[顯示註冊資訊]**。安裝程式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。在這個案例中，您需要在註冊表單中輸入註冊碼。註冊碼的有效期限為一小時。

     或者，您可以按一下 **[所有裝置]** > **[新增]**、向下捲動至 **[透過代碼註冊]**，然後按一下 **[註冊]** 來存取註冊表單。
10. **提示**請勿結束安裝程式，直到您確認註冊為止。若要再次啟動註冊，您必須重新啟動安裝程式，然後重複安裝程序。

因此，電腦將會指派給用於登入 Cyber Protect Web 主控台的帳戶。

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**建立新的帳戶**或**使用以下帳戶**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]** 開啟 **[系統管理工具]** (或按一下 Win+R、輸入 **control admintools**，然後按 Enter)，並開啟 **[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。

自動安裝或解除安裝

Windows 中的自動安裝或解除安裝

本節描述如何使用 Windows Installer (msiexec 程式)，在執行 Windows 的電腦上，以自動模式安裝或解除安裝保護代理程式。在 Active Directory 網域中，執行自動安裝的另外一種方法是透過「群組原則」。請參閱 "透過群組原則部署代理程式" (第 156 頁)。

安裝期間，您可以使用一個稱之為**轉換**的檔案 (即 .mst 檔)。轉換是指帶有安裝參數的檔案。或者，您可以直接在命令列上指定安裝參數。

建立 .mst 轉換和解壓縮安裝套件

1. 以系統管理員身分登入並啟動安裝程式。
2. 按一下 **[為自動安裝建立 .mst 和 .msi 檔案]**。
3. 在 **[要安裝的項目]** 中，選擇您要安裝的元件，然後按一下 **[完成]**。

這些元件的安裝套件會從安裝程式中解壓縮。

4. 在 **[註冊設定]** 中，選擇 **[使用認證]** 或 **[使用註冊權杖]**。如需有關如何產生註冊權杖的詳細資訊，請參閱 "步驟 1：產生註冊權杖" (第 157 頁)。
5. [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。
6. 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]**。
7. 選擇將產生 .mst 轉換並解壓縮 .msi 和 .cab 安裝套件所在的資料夾，然後按一下 **[產生]**。

使用 .mst 轉換來安裝產品

在命令列上，執行下列命令。

命令範本：

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

其中：

- <封裝名稱> 是 .msi 檔案的名稱。
- <轉換名稱> 是轉換的名稱。

命令範例：

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

透過手動指定參數來安裝或解除安裝產品

在命令列上，執行下列命令。

命令範本 (安裝)：

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

其中，<封裝名稱> 是 .msi 檔案的名稱。所有可用的參數及其值詳述於 "基本參數" (第 127 頁) 中。

命令範本 (解除安裝)：

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

.msi 套件必須與您要解除安裝的產品屬於相同版本。

自動安裝或解除安裝參數

此區段說明了在 Windows 中自動安裝或解除安裝期間所使用的參數。除了這些參數之外，您還可以使用 `msiexec` 的其他參數，如 https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx 中所述。

安裝參數

基本參數

`ADDLOCAL=<list of components>`

要安裝的元件，以逗點區隔，且沒有空格字元。所有指定的元件都必須在安裝之前從安裝程式解壓縮。

完整的元件清單如下：

元件	務必一起安裝	位元	元件名稱 / 說明
MmsMspComponents		32 位元/64 位元	適用於代理程式的核心元件
BackupAndRecoveryAgent	MmsMspComponents	32 位元/64 位元	Windows 用代理程式
ArxAgentFeature	BackupAndRecoveryAgent	32 位元/64 位元	Exchange 用代理程式
ArsAgentFeature	BackupAndRecoveryAgent	32 位元/64 位元	SQL 用代理程式
ARADAgentFeature	BackupAndRecoveryAgent	32 位元/64 位元	Active Directory 用代理程式
ArxOnlineAgentFeature	MmsMspComponents	32 位元/64 位元	Office 365 用代理程式
OracleAgentFeature	BackupAndRecoveryAgent	32 位元/64 位元	適用於 Oracle 的代理程式
AcronisESXSupport	MmsMspComponents	64 位元	VMware ESX(i) 用代理程式 (Windows)
HyperVAgent	MmsMspComponents	32 位元/64 位元	Hyper-V 用代理程式

CommandLineTool		32 位元/64 位元	命令列工具
TrayMonitor	BackupAndRecoveryAgent	32 位元/64 位元	Cyber Protect 監視器

TARGETDIR= <path>

產品的安裝資料夾。根據預設，此資料夾是：C:\Program Files\BackupClient。

REBOOT=ReallySuppress

若指定該參數，則會禁止重新啟動電腦。

/l*v <log file>

如果指定該參數，則詳細模式下的安裝記錄將會儲存至指定的檔案中。記錄檔可用於分析安裝問題。

CURRENT_LANGUAGE= <language ID>

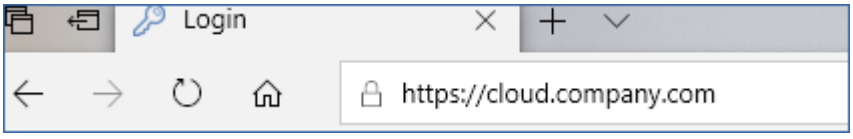
產品語言。可用的值如下：en、bg、cs、da、de、es、fr、hu、id、it、ja、ko、ms、nb、nl、pl、pt、pt_BR、ru、fi、sr、sv、tr、zh、zh_TW。
如果未指定此參數，則產品語言將由您的系統語言定義，但前提是該語言在上述清單中。否則，產品語言將設定為 [英文] (en)。

註冊參數

REGISTRATION_ADDRESS

這是 Cyber Protect 服務的 URL。您可以使用此參數搭配 REGISTRATION_LOGIN 和 REGISTRATION_PASSWORD 參數，或搭配 REGISTRATION_TOKEN 參數。

- 當您使用 REGISTRATION_ADDRESS 搭配 REGISTRATION_LOGIN 和 REGISTRATION_PASSWORD 參數時，請指定您用來**登入** Cyber Protect 服務的位址。例如，https://cloud.company.com：



- 當您使用 REGISTRATION_ADDRESS 搭配 REGISTRATION_TOKEN 參數時，請指定確實的資料中心位址。這是您**登入** Cyber Protect 服務後看到的 URL。例如，https://eu2-cloud.company.com。

請不要在這裡使用 https://cloud.company.com。

REGISTRATION_LOGIN 和 REGISTRATION_PASSWORD

在 Cyber Protect 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。

REGISTRATION_PASSWORD_ENCODED

在 Cyber Protect 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「手動註冊電腦」。

`REGISTRATION_TOKEN`

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。您可以在 Web 主控台中產生一個註冊權杖，如「透過群組原則部署代理程式」中所述。

`REGISTRATION_REQUIRED={0,1}`

定義註冊失敗時完成安裝的方式。如果值為 `1`，安裝也會失敗。預設值為 `0`，因此，如果您未指定此參數，即使未註冊代理程式，安裝也會成功完成。

其他參數

若要在 Windows 中定義代理程式服務的登入帳戶，請使用下列其中一個參數：

- `MMS_USE_SYSTEM_ACCOUNT={0,1}`
  如果值為 `1`，代理程式將會使用**本機系統**帳戶執行。
- `MMS_CREATE_NEW_ACCOUNT={0,1}`
  如果值為 `1`，代理程式將會使用新建立的帳戶 (名為 **Acronis Agent User**) 執行。
- `MMS_SERVICE_USERNAME=<user name>` 和 `MMS_SERVICE_PASSWORD=<password>`
  使用這些參數指定執行代理程式將使用的現有帳戶。

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」。

`SET_ESX_SERVER={0,1}`

- 如果值為 `0`，則要安裝的 VMware 用代理程式將不會連線至 vCenter Server 或 ESXi 主機。如果值為 `1`，請指定以下參數：
  - `ESX_HOST=<host name>`
    vCenter Server 或 ESXi 主機的主機名稱或 IP 位址。
  - `ESX_USER=<user name>` 和 `ESX_PASSWORD=<password>`
    用於存取 vCenter Server 或 ESXi 主機的認證。

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

代理程式所使用的 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。

`HTTP_PROXY_ONLINE_BACKUP={0,1}`

如果值為 `0` 或未指定參數，代理程式僅會將 Proxy 伺服器用於從雲端備份和復原。如果值為 `1`，代理程式也會透過 Proxy 伺服器連線至管理伺服器。

解除安裝參數

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

要移除的元件，以逗點區隔，且沒有空格字元。如果值為 ALL，將會解除安裝所有產品元件。

此外，您還可以指定下列參數：

DELETE_ALL_SETTINGS={0, 1}

如果值為 1，則會移除產品的記錄、工作與組態設定。

範例

- 安裝 Windows 用代理程式、命令列工具和網路保護監視器。使用使用者名稱和密碼，在 Cyber Protect 服務中登錄電腦。

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

- 安裝 Windows 用代理程式、命令列工具和網路保護監視器。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 Protect 服務中登錄電腦。

```
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 用代理程式和網路保護監視器。使用使用者名稱和以 base64 編碼的密碼，在 Cyber Protect 服務中登錄電腦。

```
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、命令列工具和網路保護監視器。使用權杖，在 Cyber Protect 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
```

- 解除安裝所有代理程式並刪除其記錄、工作和組態設定。

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

Linux 中的自動安裝或解除安裝

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。

安裝或解除安裝保護代理程式

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，<封裝名稱> 是安裝套件 (.i686 或 .x86_64 檔案) 的名稱。所有可用的參數及其值在「自動安裝或解除安裝參數」中有所說明。
- 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，後面緊接著所需的值，例如：

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

  或

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

  如果在命令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。

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

若無此參數，則將安裝以上所有元件。

Virtuozzo 用代理程式和 Oracle 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 Protect 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= <location>

安裝參數將會從文字檔案而非命令列讀取。

--language= <language 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、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=} <user name> 和 {-w|--password=}<password>

  在 Cyber Protect 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= <token>

  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。您可以在 Web 主控台中產生一個註冊權杖，如「透過群組原則部署代理程式」中所述。

  您無法使用 --token 參數搭配 --login、 --password 和 --register-with-credentials 參數。

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

    Cyber Protect 服務的 URL。

    當您使用 --login 和 --password 參數進行註冊時，您不需要明確地納入此參數，因為安裝程式預設會使用正確的位址，也就是您用來**登入** Cyber Protect 服務的位址。例如：

    不過，當您使用 {-C|--rain=} 搭配 --token 參數時，您必須指定確實的資料中心位址。這是您**登入** Cyber Protect 服務後看到的 URL。例如：

- --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 Protect 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

  如果您需要安裝代理程式，但是您打算稍後在 Cyber Protect 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「手動註冊電腦」。

其他參數

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

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=<location>`

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=}<path>`

指定用於 SSL 通訊之自訂憑證檔案的路徑。

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

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 中自動安裝和解除安裝

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、註冊以及解除安裝保護代理程式。如需有關如何下載安裝檔案 (.dmg) 的資訊，請參閱「新增執行 macOS 的電腦」。

安裝 Mac 用代理程式

1. 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。
2. 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，**AcronisAgentMspMacOSX64.dmg**。
3. 執行安裝程式。

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

4. 卸離安裝檔案 (.dmg)。

   ```
   hdiutil detach <dmg_root>
   ```

範例

- ```
  mkdir mydirectory
  ```

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

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

  ```
  hdiutil detach mydirectory
  ```

若要註冊 Mac 用代理程式

執行下列其中一項操作：

- 使用使用者名稱和密碼，以特定帳戶的身分註冊代理程式。

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

  其中：

  <Cyber Protect 服務位址> 是您用來**登入** Cyber Protect 服務的位址。例如：

  <使用者名稱> 和 <密碼> 是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。
- 使用註冊權杖註冊代理程式。
  ```

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

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。您可以在 Cyber Protect Web 主控台中產生一個註冊權杖，如「透過群組原則部署代理程式」中所述。

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**登入** Cyber Protect 服務後看到的 URL。例如：

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。

範例

使用使用者名稱與密碼註冊。

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

使用權杖註冊。

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

若要解除安裝 Mac 用代理程式

執行下列命令：

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

若要在解除安裝期間移除所有記錄、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
  ```

手動註冊電腦

除了在代理程式安裝期間，於 Cyber Protect 服務中註冊電腦之外，您還可以使用命令列介面進行註冊。如果您已經安裝代理程式但自動註冊失敗，或者如果您想要使用新的帳戶註冊現有的電腦，您可能需要執行此動作。

註冊電腦

在安裝代理程式所在電腦的命令提示字元下，執行下列其中一個命令：

- 若要以目前帳戶的身分註冊電腦：

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

  - 在這裡，<註冊工具的路徑> 是：
    - 在 Windows 中：`%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe`
    - 在 Linux 中：`/usr/lib/Acronis/RegisterAgentTool/RegisterAgent`
    - 在 macOS 中：`/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent`
- 若要以另一個帳戶的身分註冊電腦：

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

  - 在這裡，<使用者名稱> 和 <密碼> 是註冊代理程式所使用之特定帳戶的認證。這不得是合作夥伴系統管理員帳戶。

    <服務位址> 是您用來**登入** Cyber Protect 服務的 URL。例如，`https://cloud.company.com`。

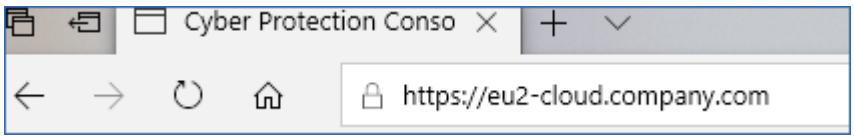
    

- 若要使用註冊權杖註冊電腦：

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

  - 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「透過群組原則部署代理程式」。

    當您使用註冊權杖時，必須指定確實的資料中心位址作為 <服務位址>。這是您**登入** Cyber Protect 服務後看到的 URL。例如，`https://eu2-cloud.company.com`。

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

取消註冊電腦

在安裝代理程式所在電腦的命令提示字元下，執行下列命令：

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

範例

Windows

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

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

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

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

Linux

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

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

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

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

macOS

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

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

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

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

包含特殊字元或空格的密碼

如果您的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：

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

範例 (Windows)：

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

如果您仍然收到錯誤：

- 在 https://www.base64encode.org/，將密碼編碼為 base64 格式。
- 在命令列上，使用 -b 或 --base64 參數指定編碼的密碼。

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

範例 (Windows)：

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

正在部署 oVirt 用代理程式 (虛擬裝置)

如需有關如何部署和設定 oVirt (虛擬裝置) 用代理程式的資訊，請參閱 Cyber Protection Cloud 文件。

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

如需有關如何部署和設定 Virtuozzo Hybrid Infrastructure (虛擬裝置) 用代理程式的資訊，請參閱 Cyber Protection Cloud 文件。

自動探索電腦

透過自動探索，您可以：

- 透過偵測 Active Directory 網域或區域網路中的電腦，自動安裝保護代理程式及將電腦註冊到管理伺服器。
- 在多部電腦上安裝及更新保護代理程式。

- 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。

必要條件

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。

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 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，該電腦上必須已安裝 Windows 更新 KB2999226。

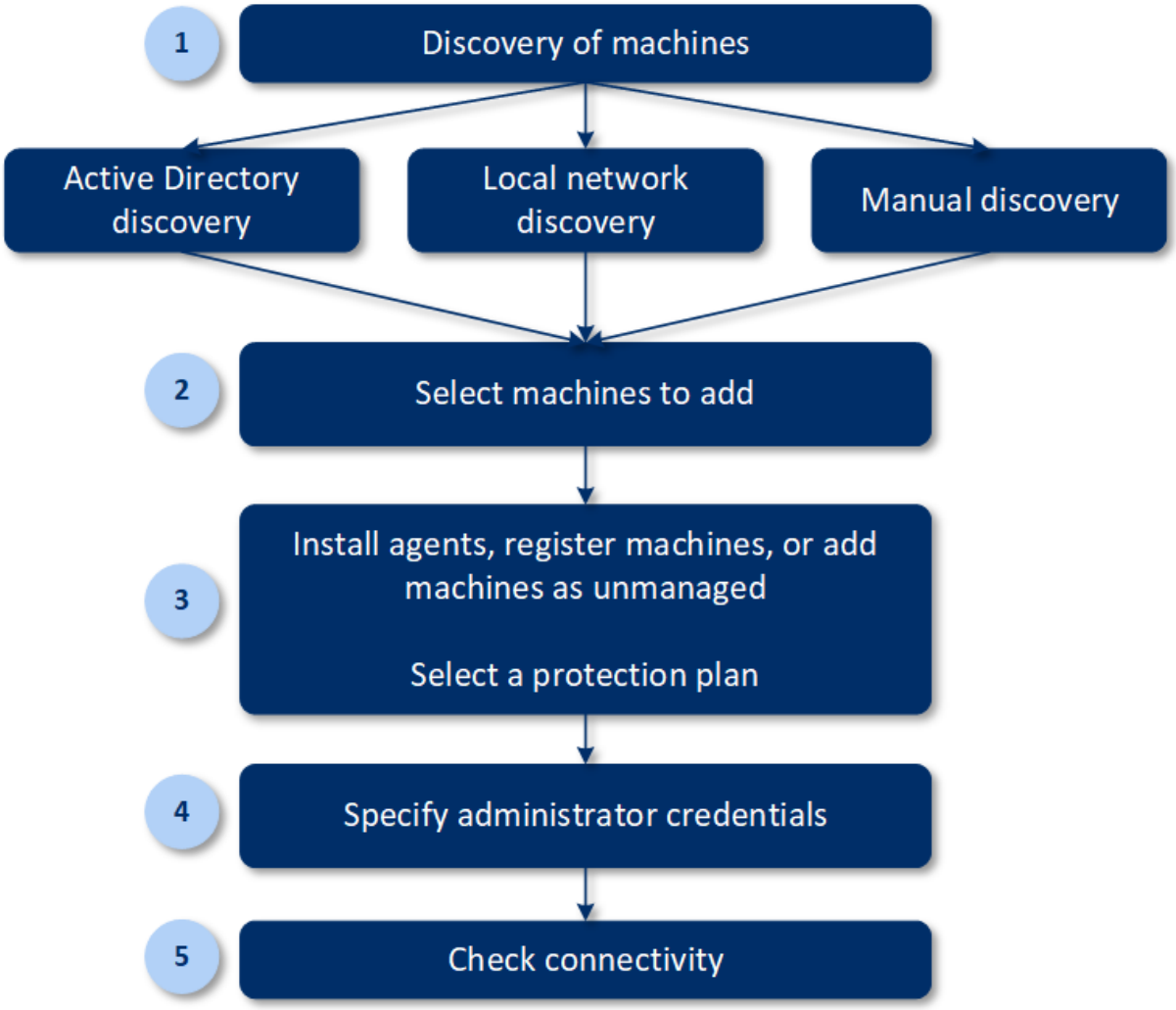
自動探索運作方式

在區域網路探索期間，探索代理程式透過 NetBIOS 探索、Web 服務探索 (WSD) 和位址解析通訊協定 (ARP) 表為網路中的每台機器收集以下資訊：

- 名稱 (短/NetBIOS 主機名稱)
- 完整網域名稱 (FQDN)
- 網域/工作群組
- IPv4/IPv6 位址
- MAC 位址
- 作業系統 (名稱/版本/系列)
- 電腦類別 (工作站/伺服器/網域控制站)

在 Active Directory 探索期間，除上述清單外，探索代理程式還會收集有關機器的組織單位 (OU) 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。

下列圖表摘要說明自動探索程序。



1. 選擇探索方法：
   - Active Directory 探索
   - 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

   Active Directory 探索或區域網路探索的結果將排除安裝保護代理程式的機器。

   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自動探索，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自動探索，則代理程式會更新到最新版本，並重新註冊到帳戶所屬的租用戶下。
2. 選擇您要新增至租用戶的電腦。
3. 選擇新增電腦的方式：
   - 在電腦上安裝保護代理程式和其他元件，並在 Web 主控台中註冊。
   - 在 Web 主控台中註冊電腦(如果已安裝保護代理程式)。
   - 將電腦新增至 Web 主控台當作**未受管理電腦**，而無需安裝保護代理程式。

   您還可以將現有保護計劃套用於安裝保護代理程式的機器或在 Web 主控台註冊的機器。
4. 提供所選電腦的系統管理員認證。

5. 選擇代理程式將用來存取管理伺服器的名稱或 IP 位址。

   依預設，會選擇伺服器名稱。如果您的管理伺服器有超過一個網路介面，或是您遇到造成代理程式註冊失敗的 DNS 問題，您可能需要改為選擇 IP 位址。

6. 請確認您可以使用提供的認證來連線到電腦。

Cyber Protect Web 主控台中顯示的電腦分為以下幾類：

- **已探索** – 已探索但尚未安裝保護代理程式的電腦。
- **受管理** – 已安裝保護代理程式的電腦。
- **未受保護** – 未套用保護計劃的電腦。未受保護的電腦包括已發現和受管理，但未套用保護計劃的電腦。
- **受保護** – 已套用保護計劃的電腦。

自動探索和手動探索

開始探索之前，請確保符合必要條件。

探索電腦

1. 在 Web 主控台中，移至 **[裝置]** > **[所有裝置]**。
2. 按一下 **[新增]**。
3. 在 **[多個裝置]** 中，按一下 **[僅限 Windows]**。探索精靈便會開啟。
4. [如果貴組織中有多個單位] 選擇一個單位。接著，在 **[探索代理程式]** 中，您將能夠選擇與所選單位及其子單位相關的代理程式。
5. 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**。請確認具有探索代理程式的電腦是 Active Directory 網域成員。
   - **掃描區域網路**。如果所選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. [如果選擇 [Active Directory 或區域網路] 探索方法] 使用清單選擇您要新增的電腦。

   [如果選擇 [手動] 探索方法] 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. 選擇探索的後續作業：

- **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」。您可以同時安裝最多 100 個代理程式。

  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。

  若您已選擇**建立新的帳戶**或**使用以下帳戶**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。
- **使用已安裝的代理程式登錄電腦**。如果電腦上已安裝代理程式，而且您只需要在 Cyber Protect 中登錄電腦，則使用此選項。如果電腦內找不到代理程式，則會將其新增為**未受管理的**電腦。
- **新增為未受管理的電腦**。電腦將不會安裝代理程式。您將可以在 Web 主控台中檢視代理程式，之後再安裝或註冊代理程式。

[如果選擇 **[安裝代理程式並登錄電腦]** 探索後動作] **需要時，重新啟動電腦** – 如果啟用此選項，將會視需要，重新啟動電腦多次，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，因為某些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。

[如果選擇 **[需要時，重新啟動電腦]**] **如果有使用者已登入，請不要重新啟動** – 如果啟用此選項，當有使用者已登入系統時，將不會自動重新啟動電腦。例如，如果當安裝需要重新啟動時使用者正在工作，將不會重新啟動系統。

如果已安裝必要條件，接著因為有使用者登入而未重新開機，則您需要為電腦重新開機，然後再次啟動安裝程式，才能完成代理程式安裝。

如果已安裝代理程式，但是之後沒有重新開機，則您需要為電腦重新開機。

[如果貴組織中有多個單位] **註冊電腦的單位** – 選擇要註冊電腦的單位。

如果您已經選擇前兩個探索後動作之一，則也有一個將保護計劃套用到電腦的選項。如果您有數個保護計劃，可以選擇要使用哪一個。

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

請注意，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。如果您要定義任何自訂系統管理員認證，則您必須手動做一些額外的準備，如「新增執行 Windows 的電腦」>「準備」中所述。

11. 選擇代理程式將用來存取管理伺服器的名稱或 IP 位址。

    依預設，會選擇伺服器名稱。如果您的管理伺服器有超過一個網路介面，或是您遇到造成代理程式註冊失敗的 DNS 問題，您可能需要改為選擇 IP 位址。

12. 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。

起始電腦探索時，您將會在 **[儀表板]** > **[活動]** > **[探索電腦]** 活動中找到對應的工作。

選擇要安裝的元件

您可以在下表中找到必要元件和其他元件的描述：

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	
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 用代理程式 (Windows)	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 Server 的 Windows 電腦上。如果選擇，則要安裝。
Office 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 Protect 監視器	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。
命令列工具	Cyber Protect 支援 acrocmd 公用程式的命令列介面。acrocmd 不包含實際執行命令的任何工具。而是僅向 Cyber Protect 元件 (代理程式與管理伺服器) 提供命令列介面。如果選擇，則要安裝。

可開機媒體組建	此元件可讓使用者建立可開機媒體，而且將會安裝在 Windows 電腦上 (如果有選擇的話)。

管理探索到的電腦

執行探索程序之後，您可以在 **[裝置]** > **[未受管理的電腦]** 中找到所有探索到的電腦。

此區段依照所使用的探索方法，分成不同的子區段。電腦參數的完整清單顯示在下方 (視探索方法而有所不同)：

名稱	描述
名稱	電腦的名稱。如果找不到電腦的名稱，將會顯示 IP 位址。
IP 位址	電腦的 IP 位址。
探索類型	偵測電腦所使用的探索方法。
組織單位	Active Directory 中電腦所屬的組織單位。如果您在 **[未受管理的電腦]** > **[Active Directory]** 中檢視電腦清單，則會顯示此欄。
作業系統	電腦上安裝的作業系統。

有一個 **[例外]** 區段，您可以在其中新增探索程序期間必須略過的電腦。例如，如果您不需要探索到確切的電腦，可以將其新增到此清單中。

若要將電腦新增到 **[例外]**，請在清單中選擇該電腦，然後按一下 **[新增至例外]**。若要從 **[例外]** 移除電腦，移至 **[未受管理的電腦]** > **[例外]**、選擇電腦，然後按一下 **[從例外移除]**。

您可以在清單中選擇一批探索到的電腦，然後按一下 **[安裝並登錄]**，以安裝保護代理程式，並在 Cyber Protect 中登錄這些電腦。開啟的精靈也可讓您將保護計劃指派給一批電腦。

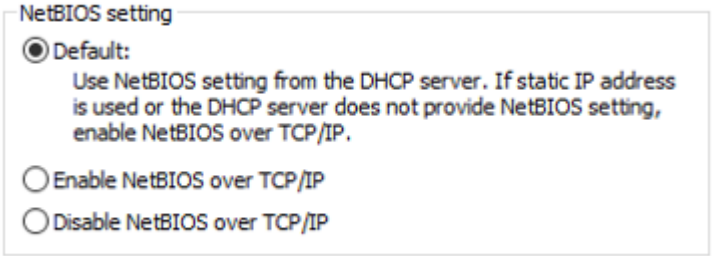
在電腦上安裝保護代理程式之後，那些電腦將會顯示在 **[裝置]** > **[具有代理程式的電腦]** 區段中。

若要檢查您的保護狀態，移至 **[儀表板]** > **[概觀]**，然後新增 **[保護狀態]** 桌面小工具或 **[探索到的電腦]** 桌面小工具。

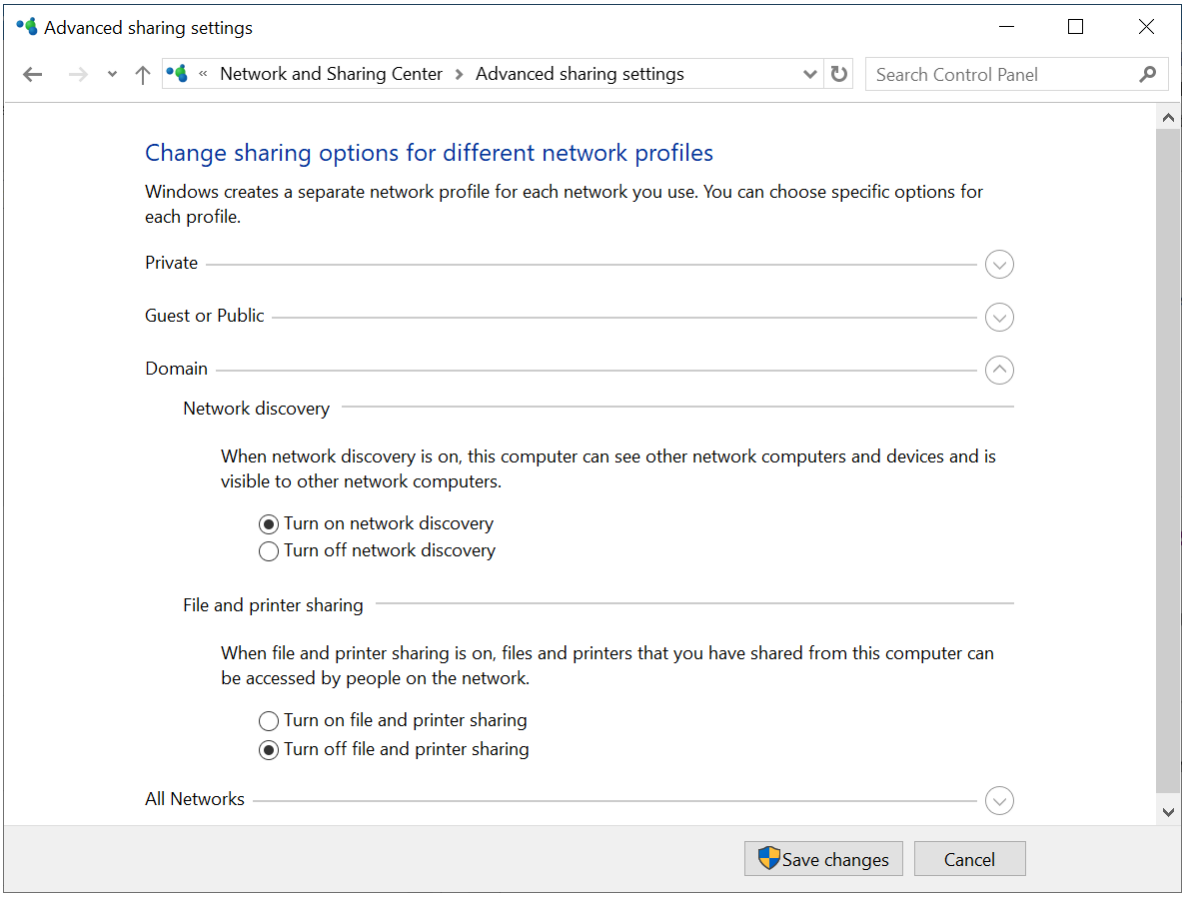
疑難排解

如果您對自動探索功能有任何問題，請嘗試下列項目：

- 確認是透過 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。



- 確認**功能探索提供者裝載**服務正在進行探索的電腦以及要探索的電腦上執行。
- 確認**功能探索資源發佈**服務正在要探索的電腦上執行。

從 OVF 範本部署 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。如果備份流量頻寬預期超過每秒 100 MB (例如，在 10-GBit 網路中)，則建議將這些資源增加到 8 GB 的 RAM 和 4 個 vCPU，才能提升備份效能。

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。

注意事項
ESXi 主機上必須安裝 vStorage API，才能啟用虛擬機器備份。請參閱 https://kb.acronis.com/content/14931。

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存放區 (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「使用本機連接的存放區」。

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

OVF 範本的位置

OVF 範本包含一個 .ovf 檔案和兩個 .vmdk 檔案。

在內部部署中

管理伺服器安裝完成後，虛擬裝置的 OVF 套件位於下列資料夾：**%ProgramFiles%\Acronis\ESXAppliance** (Windows 系統) 或 **/usr/lib/Acronis/ESXAppliance** (Linux 系統)。

在雲端部署中

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。

部署 OVF 範本

1. 請確認 OVF 範本檔案可以從執行 vSphere Client 的電腦存取。
2. 啟動 vSphere 用戶端並登入 vCenter 伺服器。
3. 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。
   - 在雲端部署中設定網路連線時，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。在內部部署中設定網路連線時，請選取含有管理伺服器的網路。

設定虛擬裝置

1. **啟動該虛擬設備**

   在 vSphere Client 中，顯示**[清查]**，用滑鼠右鍵按一下虛擬裝置的名稱，然後選擇**[電源]** > **[開機]**。選擇**[主控台]**標籤。

2. **Proxy 伺服器**

   如果您的網路中已啟用 Proxy 伺服器：

   a. 若要啟動命令殼層，在虛擬裝置 UI 中時，按下 CTRL+SHIFT+F2。

   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 *位址* 取代為新的 Proxy 伺服器主機名稱/IP 位址，並將 *連接埠* 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 *登入* 和 *密碼* 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。

   否則，請跳過此步驟。

3. **網路設定**

   透過使用動態主機設定協定 (DHCP) 自動設定該代理程式的網路連線。若要變更該預設組態，在**[代理程式選項]**之下，在**[eth0]**中，按一下**[變更]**，並指定所期望的網路設定。

4. **vCenter/ESX(i)**

在**[代理程式選項]**下的**[vCenter/ESX(i)]**中，按一下**[變更]**並指定 vCenter Server 名稱或 IP 位址。代理程式將能夠備份與復原由 vCenter Server 管理的任何虛擬機器。

如果您並未使用 vCenter Server，請指定要進行虛擬機器備份與復原之 ESXi 主機的名稱或 IP 位址。一般而言，當代理程式備份承載於其本身主機的虛擬機器時，備份速度較快。

指定代理程式將用於連線到 vCenter Server 或 ESXi 的認證。我們建議使用已指派**系統管理員**角色的帳戶。否則，在 vCenter Server 或 ESXi 中提供具備必要權限的帳戶。

您可以按一下**[檢查連線]**以確保存取認證正確。

5. **管理伺服器**
   a. 在 **[代理程式選項]** 的 **[管理伺服器]** 中，按一下 **[變更]**。
   b. 在 **[伺服器名稱/IP]** 中，執行下列其中一項操作：
      - 若是內部部署，選取 **[本機]**。指定已安裝管理伺服器的電腦的名稱或 IP 位址。
      - 若是雲端部署，選取 **[雲端]**。軟體會顯示網路保護服務位址。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]** 中，執行下列其中一項操作：
      - 若是內部部署，請指定管理伺服器系統管理員的使用者名稱與密碼。
      - 若是雲端部署，則指定網路保護服務的使用者名稱與密碼。代理程式及其所管理的虛擬機器將會以此帳戶註冊。
6. **時區**

   在**[虛擬機器]**下，在**[時區]**中，按一下**[變更]**。選擇您所在位置的時區，以確保排程作業在適當時間執行。
7. **[選擇性] 本機存放區**

   您可以將額外的磁碟附加到虛擬裝置，讓 VMware 用代理程式可以備份到這個本機附加的存放區。

   編輯虛擬機器的設定，然後按一下**[重新整理]**，以新增磁碟。**[建立存放區]**連結會變為可用狀態。按一下此連結，選擇磁碟，然後為其指定標籤。

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

部署虛擬裝置時，您可以在不同的 vCPU 和 RAM 組合中選擇。2 個 vCPU 搭配 4 GiB 的 RAM 非常適合而且足以適用於大多數作業。如果備份流量頻寬預期超過每秒 100 MB (例如，在 10-GBit 網路中)，則建議將這些資源增加到 4 個 vCPU 和 8 GiB 的 RAM，才能提升備份效能。

裝置自己的虛擬磁碟不會佔用超過 6 GB 空間。

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同數量的機器。

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。新增或移除虛擬機器或代理程式時，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，指派給代理程式的虛擬機器會分配給剩餘的代理程式。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。只有在當您從 Cyber Protect Web 介面移除這種代理程式後，才會開始重新分配。

您可檢視自動分配的結果：

- 在 **[所有裝置]** 區段中，每部虛擬機器的 **[代理程式]** 欄上
- 在 **[設定]** > **[代理程式]** 中選擇代理程式後，在 **[詳細資料]** 面板的 **[已指派的虛擬機器]** 區段中

部署虛擬裝置

1. 請登入您的 Cyber Protect 帳戶。
2. 按一下 **[裝置]** > **[所有裝置]** > **[新增]** > **[Scale Computing HC3]**。
3. 選擇您要部署的虛擬裝置數量。
4. 指定 Scale Computing HC3 叢集的 IP 位址或主機名稱。
5. 指定此叢集中已獲指派 **[VM 建立/編輯]** 角色之帳戶的認證。
6. 指定將用於暫時儲存虛擬裝置映像檔的網路共用。至少需要 2GB 的可用空間。
7. 指定可讀取和寫入此網路共用之帳戶的認證。
8. 按一下 **[部署]**。

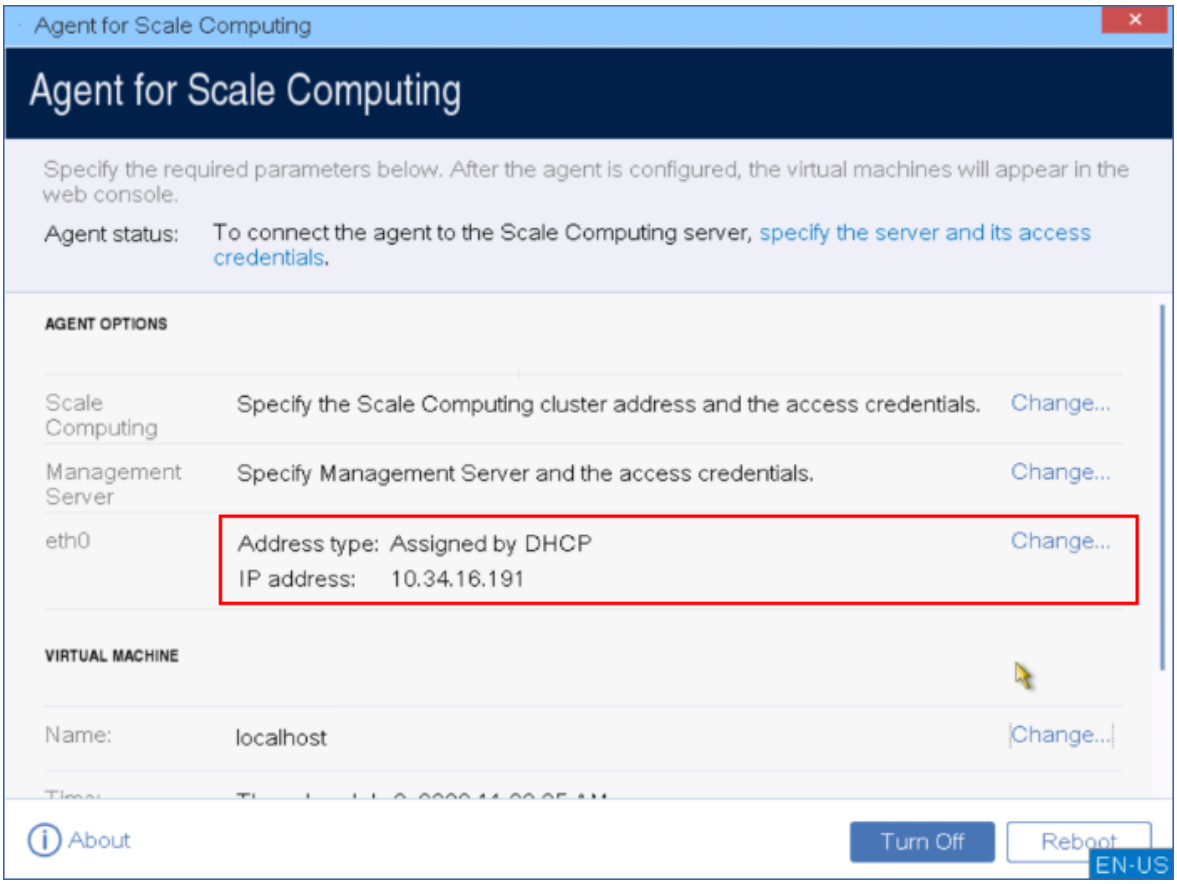
部署完成後，請設定虛擬裝置。

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 Protect 管理伺服器。

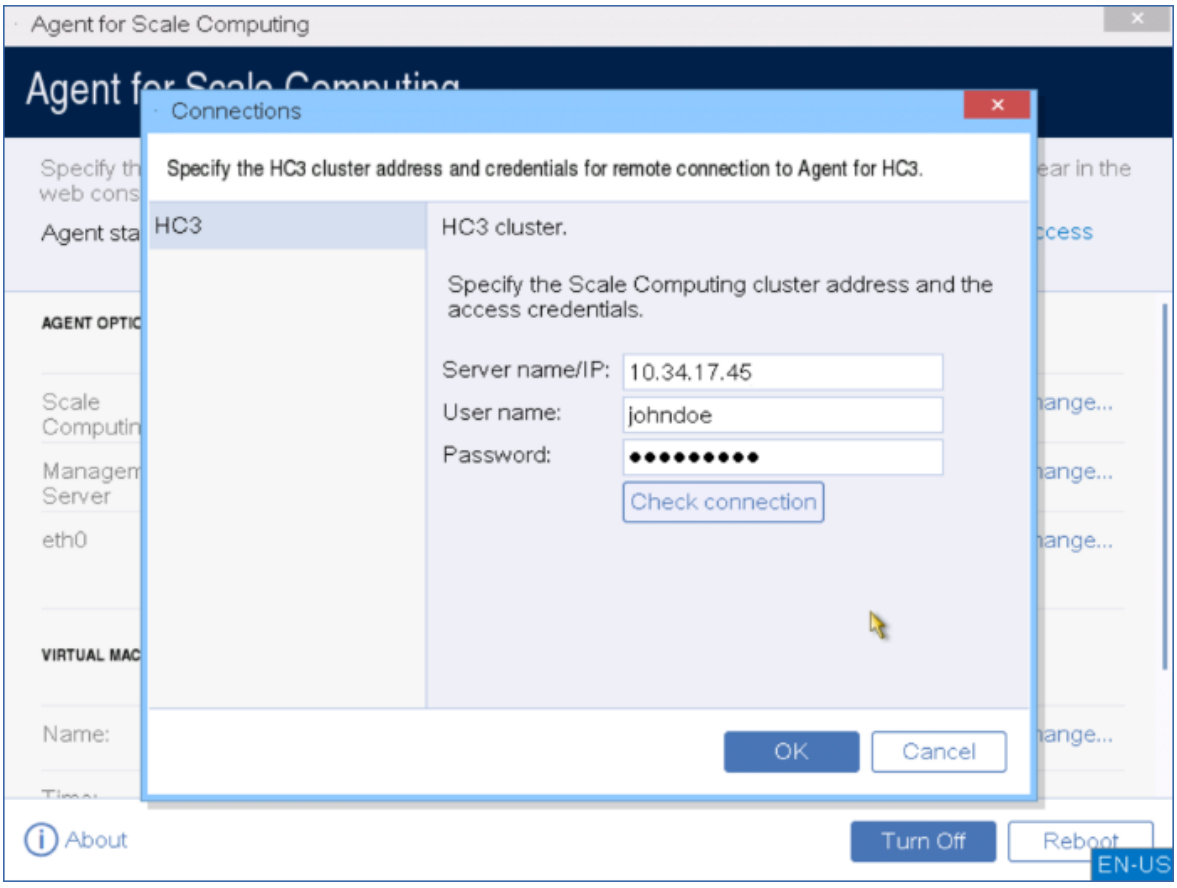
若要設定虛擬設備

1. 登入您的 Scale Computing HC3 帳戶。
2. 選擇具有您需要設定之代理程式的虛擬機器，然後按一下 **[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。

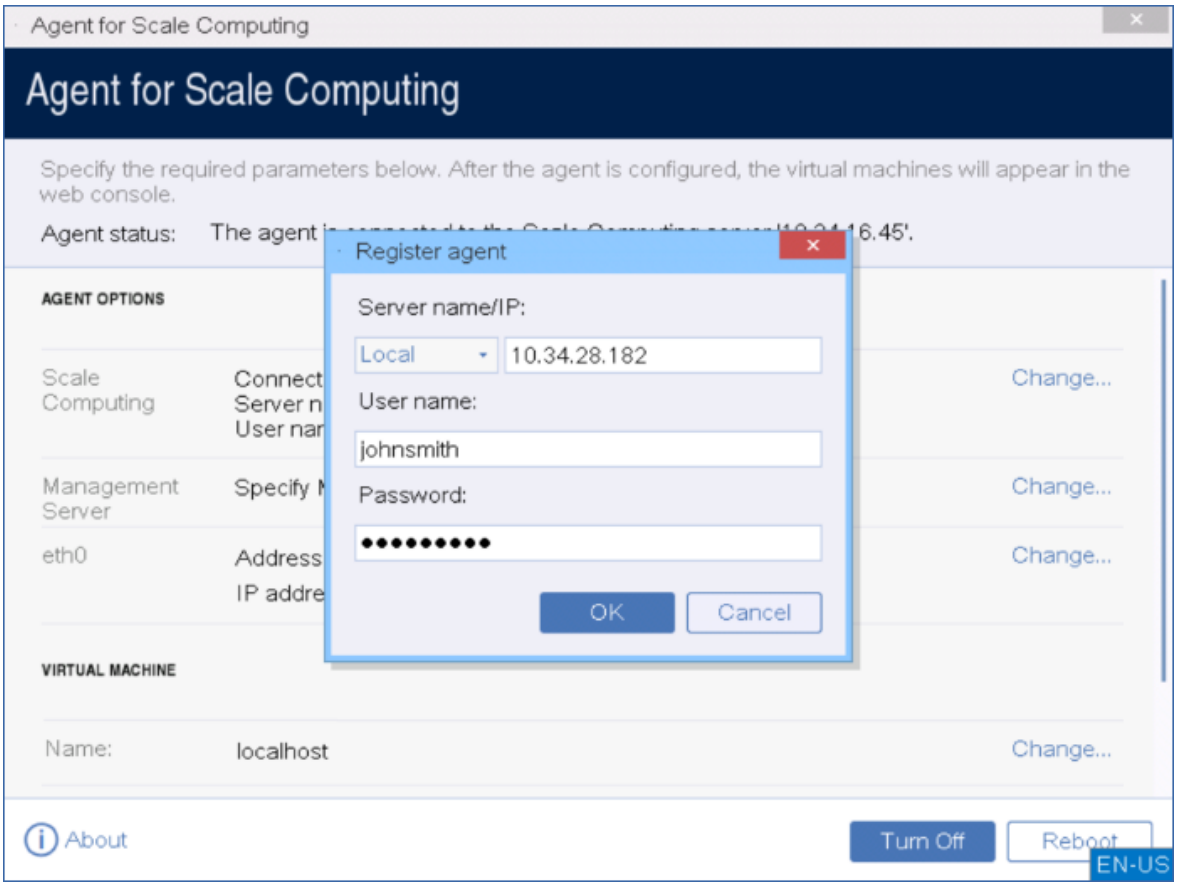


4. 指定 Scale Computing HC3 叢集位址和認證：
   - 叢集的 DNS 名稱或 IP 位址。
   - 在 **[使用者名稱]** 和 **[密碼]** 欄位中，輸入已獲指派適當角色之 Scale Computing HC3 帳戶的認證。

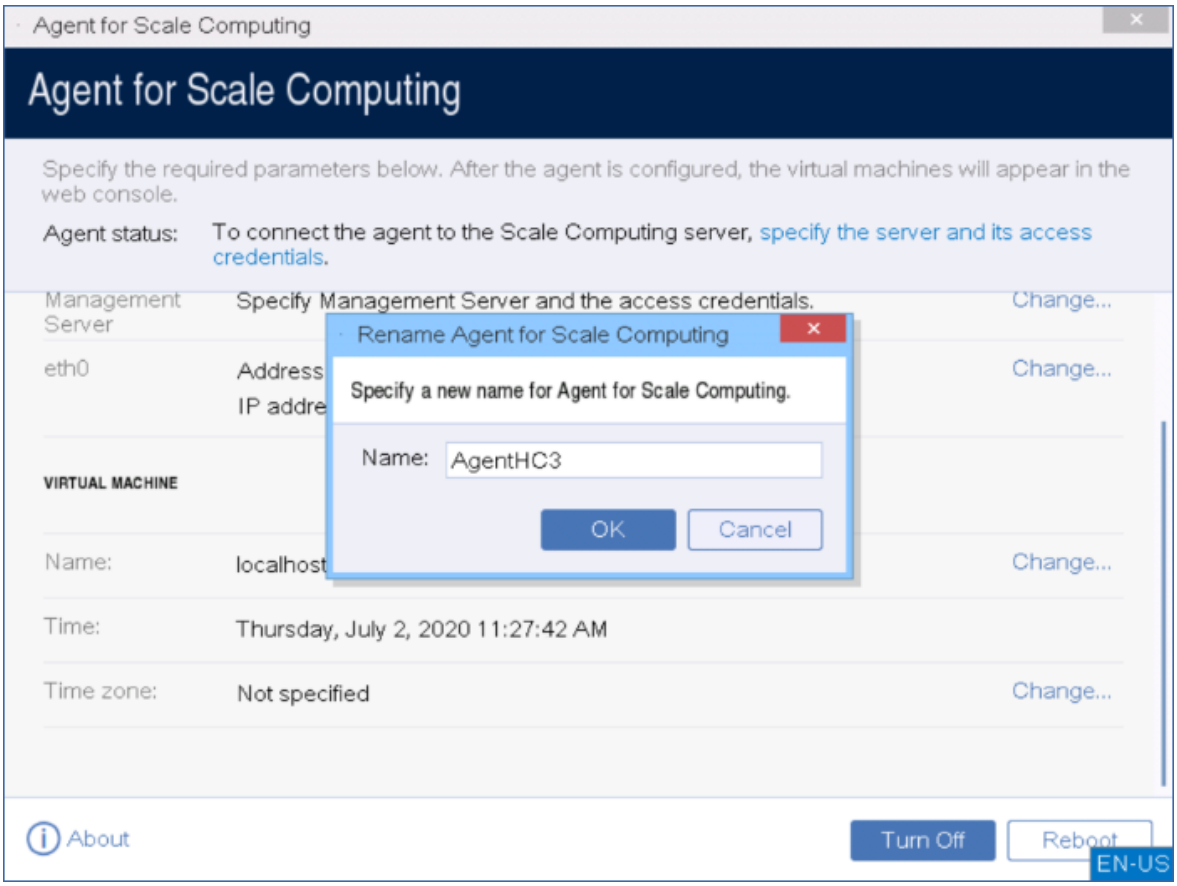
   您可以按一下**[檢查連線]**以確保存取認證正確。



5. 指定 Cyber Protect 管理伺服器位址和認證以存取它。



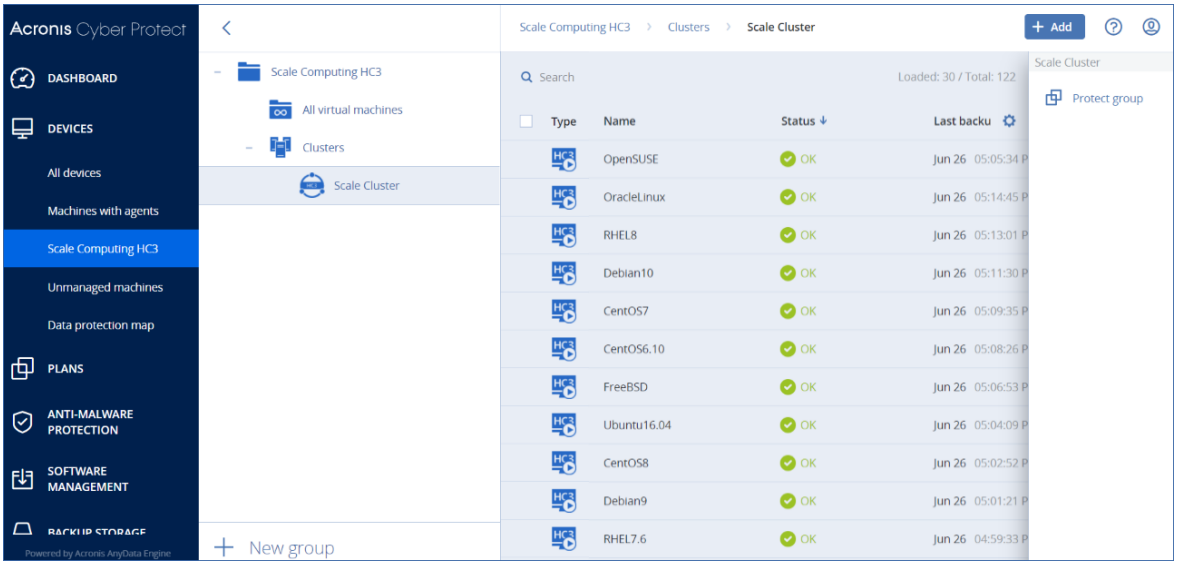
6. [選擇性] 指定代理程式的名稱。此名稱將會顯示在 Cyber Protect Web 主控台中。



7. [選擇性] 選擇您所在位置的時區，以確保排程作業在適當時間執行。

若要保護 Scale Computing HC3 叢集中的虛擬機器

1. 請登入您的 Cyber Protect 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. 選擇所需的電腦，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，以及虛擬裝置部署所需的角色。

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
虛擬裝置部署	VM 建立/編輯

透過群組原則部署代理程式

您可以透過群組原則將 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

部署代理程式之前，請確保：

- 您有 Active Directory 網域，其網域控制站執行 Microsoft Windows Server 2003 或更新版。
- 您是該網域中 **[Domain Admins]** 群組的成員。
- 您已下載 **[在 Windows 中安裝的所有代理程式]** 安裝程式。您可以在 Web 主控台中的 **[新增裝置]** 頁面取得下載連結。

步驟 1:產生註冊權杖

註冊權杖會將您的身份識別傳遞至安裝程式,但不會儲存您用於 Cyber Protect Web 主控台的登入和密碼。這可讓您以自己的帳戶註冊任意數目的電腦。為增加安全性,權杖的存留期有限。

若要產生註冊權杖

1. 使用電腦應獲指派之帳戶的認證,登入 Cyber Protect Web 主控台。
2. 按一下**[所有裝置]** > **[新增]**。
3. 向下捲動至 **[註冊權杖]**,然後按一下 **[產生]**。
4. 指定權杖存留期,然後按一下 **[產生權杖]**。
5. 複製權杖或寫下來。如果您之後需要使用權杖,請務必將其儲存起來。

   您可以按一下 **[管理使用中的權杖]** 來檢視與管理已經產生的權杖。請注意,基於安全理由,此表格不會顯示完整的權杖值。

步驟 2:建立 .mst 轉換和解壓縮安裝套件

1. 在網域中的任何一部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. 啟動安裝程式。
4. 按一下 **[為自動安裝建立 .mst 和 .msi 檔案]**。
5. 檢閱或修改將新增到 .mst 檔案中的安裝設定。指定連線至管理伺服器的方法時,選取 **[使用註冊權杖]**,然後輸入您所產生的權杖。
6. 按一下**繼續**。
7. 在 **[將檔案儲存至]** 中,指定您建立的資料夾的路徑。
8. 按一下 **[產生]**。

因此,將會產生 .mst 轉換,而 .msi 和 .cab 安裝套件將會解壓縮到您建立的資料夾。

步驟 3:設定群組原則物件

1. 請以網域系統管理員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網域控制站。
2. 如果您計劃在組織單位中部署代理程式,確保組織單位在該網域中存在。否則,請跳過此步驟。
3. 在 **[開始]** 功能表中,指向 **[系統管理工具]**,然後按一下 **[Active Directory 使用者和電腦]** (在 Windows Server 2003 中) 或 **[群組原則管理]** (在 Windows Server 2008 或更新版本中)。
4. 在 Windows Server 2003 中:
   - 用滑鼠右鍵按一下網域名稱或組織單位名稱,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]**。

   在 Windows Server 2008 或更新版本中:
   - 用滑鼠右鍵按一下網域或組織單位名稱,然後按一下 **[在此網域中建立 GPO,並將其連結至此]**。

5. 將新的群組原則物件命名為 **[Windows 用代理程式]**。
6. 開啟 **[Windows 用代理程式]** 群組原則物件進行編輯，如下所示：
   - 在 Windows Server 2003 中，按一下群組原則物件，然後按一下 **[編輯]**。
   - 在 Windows Server 2008 或更新版本中的 **[群組原則物件]** 下，用滑鼠右鍵按一下該群組原則物件，然後按一下 **[編輯]**。
7. 在群組原則物件編輯器嵌入式管理單元中，展開 **[電腦設定]**。
8. 在 Windows Server 2003 和 Windows Server 2008 中：
   - 展開 **[軟體設定]**。

   在 Windows Server 2012 或更新版本中：
   - 展開 **[原則]** > **[軟體設定]**。
9. 用滑鼠右鍵按一下 **[軟體安裝]**，然後指向 **[新增]**，並按一下 **[套件]**。
10. 選擇您先前建立的共用資料夾中之代理程式的 .msi 安裝套件，然後按一下 **[開啟]**。
11. 在 **[部署軟體]** 對話方塊中，按一下 **[進階]**，然後按一下 **[確定]**。
12. 在 **[修改]** 索引標籤上，按一下 **[新增]**，然後選擇您先前建立的 .mst 轉換。
13. 按一下 **[確定]** 關閉 **[部署軟體]** 對話方塊。

更新虛擬裝置

內部部署

若要更新其版本低於 15.24426 (2020 年 9 月發行) 的虛擬裝置 (VMware 用代理程式或 Scale Computing HC3 用代理程式)，請依照 "更新代理程式" (第 159 頁) 中的程序進行。

若要更新虛擬裝置 15.24426 版或更新版本

1. 下載更新的套件，如 http://kb.acronis.com/latest 中所述。
2. 將 `tar.bz` 檔案儲存在管理伺服器電腦的下列目錄中：
   - Windows：`C:\Program Files\Acronis\VirtualAppliances\va-updates`
   - Linux：`/usr/lib/Acronis/VirtualAppliances/va-updates`
3. 在 Cyber Protect Web 主控台中，按一下 **[設定]** > **[代理程式]**。

   軟體會顯示電腦清單。虛擬裝置已過期的電腦會以橙色驚嘆號標示。
4. 選擇您要更新虛擬裝置所在的電腦。這些電腦必須在線上。
5. 請按一下 [**更新代理程式**]。
6. 選擇部署代理程式。
7. 指定具有目標電腦系統管理權限之帳戶的認證。
8. 選擇代理程式將用來存取管理伺服器的名稱或 IP 位址。

   依預設，會選擇伺服器名稱。如果 DNS 伺服器無法將名稱解析為 IP 位址，而導致在虛擬裝置註冊期間發生錯誤，則需變更此設定。

更新進度會顯示在 [**活動**] 標籤上。

注意事項
在更新期間，進行中的所有備份都將失敗。

雲端部署

如需有關如何在雲端部署中更新虛擬裝置的資訊，請參閱雲端文件中的更新代理程式。

更新代理程式

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。Microsoft Visual C++ 可轉散發套件可以在以下網址找到：https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows。

若要尋找代理程式版本，請選擇電腦，然後按一下**詳細資料**。

您可以使用 Cyber Protect Web 主控台，或以任何可用的方式對其進行重複安裝，藉此更新代理程式。若要同時更新多個代理程式，則使用以下程序。

若要使用 Cyber Protect Web 主控台更新代理程式

1. [僅在內部部署中] 更新管理伺服器。
2. [僅在內部部署中] 確保安裝套件顯示在裝有管理伺服器的電腦上。如需準確步驟，請參閱「新增執行 Windows 的電腦」>「安裝套件」。
3. 在 Cyber Protect Web 主控台中，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。
4. 選擇您要更新代理程式的電腦。電腦必須在線上。
5. 請按一下 **[更新代理程式]**。
6. 選擇部署代理程式。
7. 指定具有目標電腦系統管理權限之帳戶的認證。
8. 選擇代理程式將用來存取管理伺服器的名稱或 IP 位址。
   依預設，會選擇伺服器名稱。如果您的管理伺服器有超過一個網路介面，或是您遇到造成代理程式註冊失敗的 DNS 問題，您可能需要改為選擇 IP 位址。
9. [僅在內部部署中] 更新進度會顯示在 **[活動]** 索引標籤上。

注意事項
在更新期間，進行中的所有備份都將失敗。

若要在電腦上更新 Cyber Protect 定義

1. 請按一下 **[設定]** > **[代理程式]**。
2. 選擇您要更新 Cyber Protect 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. 選擇要獲指派 [更新者角色] 的電腦，按一下 **[詳細資料]**，然後在 **[Cyber Protect 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]**。

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]**。

升級至 Acronis Cyber Protect 15

您可以用下列方式，將舊版產品升級至 Acronis Cyber Protect 15。

- 直接升級，無需解除安裝舊版產品。
  此選項僅適用於 Acronis Backup 12.5 Update 5 (組建 16180) 或更新版本。
- 透過解除安裝舊版產品並安裝 Acronis Cyber Protect 15 的新副本。
  此選項適用於所有符合資格的產品。如需有關這些產品的詳細資訊，請參閱這篇知識庫文章。

注意事項
建議您先備份您的系統，然後再升級。如果升級失敗，如此將可讓您回復到原始設定。

若要開始升級，請執行安裝程式並依照畫面上的指示進行。

Acronis Cyber Protect 15 中的管理伺服器具有回溯相容性，而且支援 12.5 版代理程式。但是，這些代理程式不支援 Cyber Protect 功能。

升級代理程式不會干擾現有的備份集及其設定。

解除安裝產品

若您想要移除電腦上的個別產品元件，請執行安裝程式，選擇修改產品，並清除您想要移除的選項。安裝程式連結就在 **[下載]** 頁面上 (按一下右上角的帳戶圖示 > **[下載]**)。

若想移除電腦上的所有產品元件，請依照下列所述步驟進行。

警告！
在內部部署中選擇要解除安裝的元件時要非常小心。

如果您不小心解除安裝管理伺服器，Cyber Protect Web 主控台將變成無法使用，而且您將無法再備份和復原在解除安裝的管理伺服器上登錄的電腦。

在 Windows 中

1. 以管理員身份登入。
2. 請移至 **[控制台]**，然後選擇 **[程式和功能]** (在 Windows XP 中為 **[新增或移除程式]**) > **[Acronis Cyber Protect]** > **[解除安裝]**。

3. [選擇性] 選擇 **[移除記錄和組態設定]** 核取方塊。
   若您正在解除安裝代理程式，且計劃再次安裝，請維持此核取方塊為未選擇的狀態。若您選取了核取方塊，將會在 Cyber Protect Web 主控台中複製電腦，且舊機器的備份可能無法與新機器相關聯。
4. 確認選項無誤。

在 Linux 中

1. 以 root 使用者身分執行 **/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall**。
2. [選擇性] 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。
   若您正在解除安裝代理程式，且計劃再次安裝，請維持此核取方塊為未選擇的狀態。若您選取了核取方塊，將會在 Cyber Protect Web 主控台中複製電腦，且舊機器的備份可能無法與新機器相關聯。
3. 確認選項無誤。

在 macOS 中

1. 按兩下安裝檔案 (.dmg)。
2. 請等候作業系統掛載安裝磁碟影像。
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。

移除 VMware 用代理程式 (虛擬裝置)

1. 啟動 vSphere 用戶端並登入 vCenter 伺服器。
2. 如果虛擬裝置已開啟，請用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附加的存放區，且您想要保留該磁碟上的資料，請執行下列作業：
   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]**。在 **[移除選項]** 下，按一下 **[從虛擬機器中移除]**。
   c. 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。

從 Cyber Protect Web 主控台移除電腦

解除安裝代理程式之後，將會從管理伺服器取消註冊該代理程式，而且安裝該代理程式所在的電腦將會自動從 Cyber Protect Web 主控台移除。

但是，如果在此作業期間失去與管理伺服器的連線 (例如，因為網路問題)，可能會解除安裝代理程式，但是其電腦可能仍會顯示在 Web 主控台中。在此情況下，您需要從 Web 主控台手動移除該電腦。

若要從 Web 主控台手動移除電腦

1. 在 Cyber Protect Web 主控台中，移至 **[設定]** > **[代理程式]**。
2. 選擇安裝代理程式所在的電腦。
3. 請按一下 **[刪除]**。

存取 Cyber Protect Web 主控台

若要存取 Cyber Protect Web 主控台，請在網頁瀏覽器的網址列中輸入登入頁面網址，然後依以下所述方式登入。

內部部署

登入頁面網址是管理伺服器安裝所在電腦的 IP 位址或名稱。

HTTP 和 HTTPS 通訊協定均在同一 TCP 連接埠上受支援，而連接埠可在管理伺服器安裝期間進行設定。預設連接埠為 9877。

您可以設定管理伺服器禁止透過 HTTP 存取 Cyber Protect Web 主控台，以及設定其使用第三方 SSL 憑證。

在 Windows 中

如果管理伺服器是安裝在 Windows 上，則有兩種方式可以登入 Cyber Protect Web 主控台：

- 按一下 **[登入]**，以目前 Windows 使用者的身份登入。
  這是從有安裝管理伺服器的相同電腦登入的最簡單方法。
  如果管理伺服器是安裝在不同的電腦上，則這種方法可以在以下條件時始用：
  - 您所登入的電腦與管理伺服器的 Active Directory 網域是相同的。
  - 您是以網域使用者的身份登入。

  我們建議您針對[整合 Windows 驗證]設定您的網頁瀏覽器。否則，瀏覽器將要求輸入使用者名稱和密碼。但是，您可以停用此選項。
- 按一下 **[輸入使用者名稱及密碼]**，然後指定使用者名稱與密碼。

無論在任何情況下，您的帳戶都必須位於管理伺服器系統管理員的清單內。依預設，此清單包含執行管理伺服器的電腦的**[管理員]**群組。如需更多資訊，請參閱「管理員與單位」。

若要停用 [以目前 Windows 使用者的身分登入] 選項

1. 在安裝管理伺服器所在的電腦上，移至 `C:\Program Files\Acronis\AccountServer`。
2. 開啟檔案 **account_server.json** 進行編輯。
3. 瀏覽至 [connectors] 區段，然後刪除下列幾行：

   ```
   {
   "type":"sspi",
   "name": "1 Windows Integrated Logon",
   "id": "sspi",
   "config": {}
   },
   ```

4. 瀏覽至 [checksum] 區段，然後變更 [sum] 值，如下所示：

```
"sum":"FWY/8e8C6c0AgNl0BfCrjgT4v2uj7RQNmaIYbwbjpzU="
```

5. 重新啟動 Acronis Service Manager 服務，如「使用受信任憑證授權單位發出的憑證」所述。

在 Linux 中

如果管理伺服器安裝在 Linux 中，請指定位於管理伺服器系統管理員清單中的帳戶的使用者名稱和密碼。依預設，此清單僅包含執行管理伺服器的電腦的 **root** 使用者。如需更多資訊，請參閱「管理員與單位」。

雲端部署

登入頁面網址為 https://backup.acronis.com/。使用者名稱與密碼是您 Acronis 帳戶的使用者名稱與密碼。

如果備份管理員已建立您的帳戶，您需要按一下啟動電子郵件中的連結，以啟用帳戶並設定密碼。

變更語言

登入時，您可以按一下右上角的帳戶圖示，以變更 Web 介面的語言。

為整合式 Windows 驗證設定網頁瀏覽器

如果您從執行 Windows 及任何受支援瀏覽器的電腦中存取 Cyber Protect Web 主控台，則整合式 Windows 驗證可行。

我們建議您針對[整合 Windows 驗證]設定您的網頁瀏覽器。否則，瀏覽器將要求輸入使用者名稱和密碼。

設定 Internet Explorer、Microsoft Edge、Opera 和 Google Chrome

如果執行瀏覽器的電腦與執行管理伺服器的電腦位於同一 Active Directory 網域中，請將主控台的登入頁面新增至 **[近端內部網路]** 網站清單中。

否則，將主控台的登入頁面新增至 **[信任的網站]** 清單，並啟用 **[使用現行使用者名稱及密碼自動登入]** 設定。

本節中稍後提供逐步指示。由於這些瀏覽器使用 Windows 設定，因此也可以使用 Active Directory 網域中的 [群組原則] 設定它們。

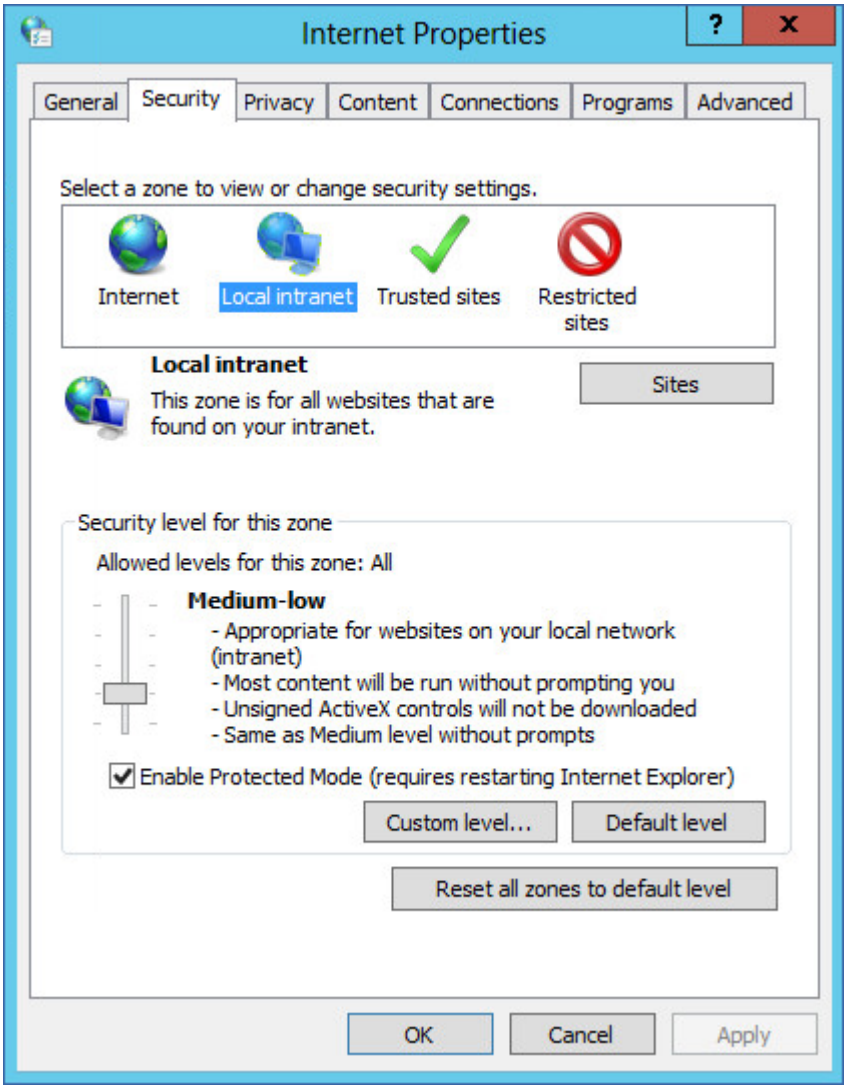
設定 Mozilla Firefox

1. 在 Firefox 中，導覽至 URL `about:config`，然後按一下 **[我接受風險]** 按鈕。
2. 在 **[搜尋]** 欄位中，搜尋 `network.negotiate-auth.trusted-uris` 喜好設定。
3. 按兩下喜好設定，然後輸入 Cyber Protect Web 主控台登入頁面的網址。

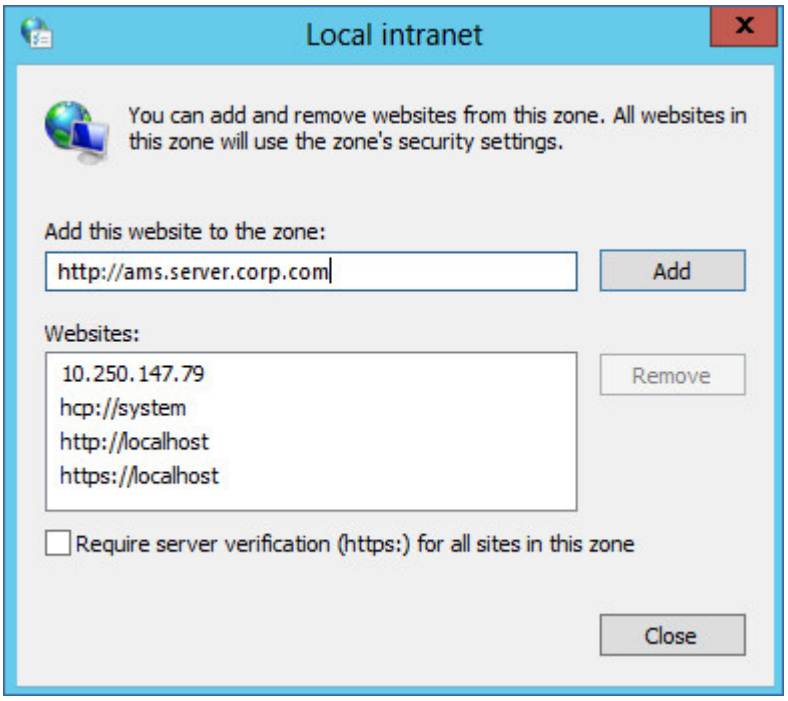
4. 針對 network.automatic-ntlm-auth.trusted-uris 喜好設定重複步驟 2-3。
5. 選擇 about:config 視窗。

新增主控台到本機內部網路網址的清單

1. 進入**[控制台]** > **[網際網路選項]**。
2. 在**[安全性]**標籤，選擇**[本機內部網路]**。



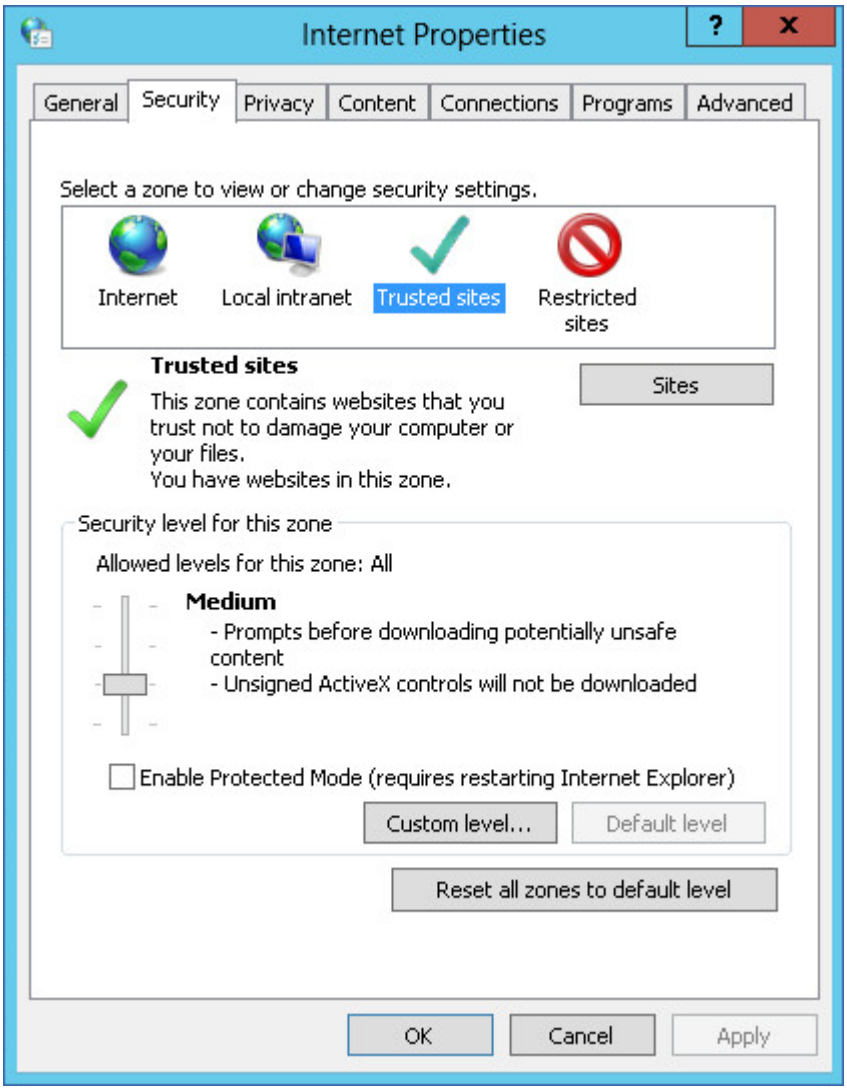
3. 按一下**[網站]**。
4. 在 **[新增此網站到區域]** 中，輸入 Cyber Protect Web 主控台登入頁面的網址，然後按一下 **[新增]**。



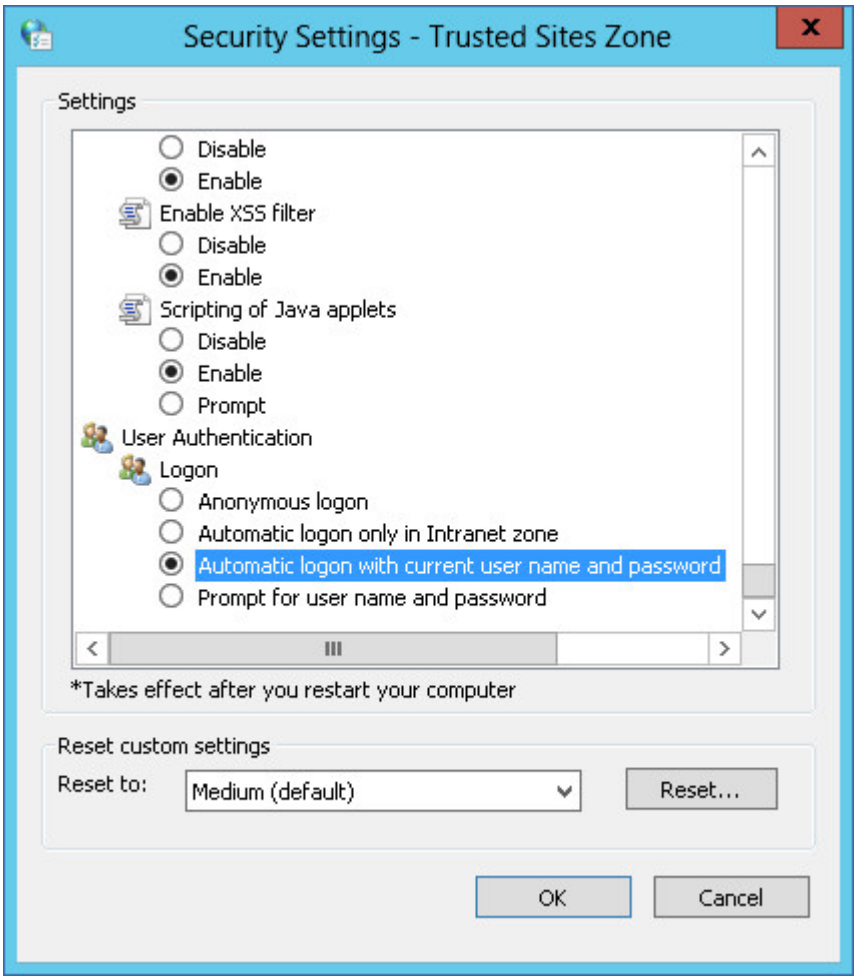
5. 按一下**[關閉]**。
6. 按一下 **[確定]**。

新增主控台到受信任網站的清單

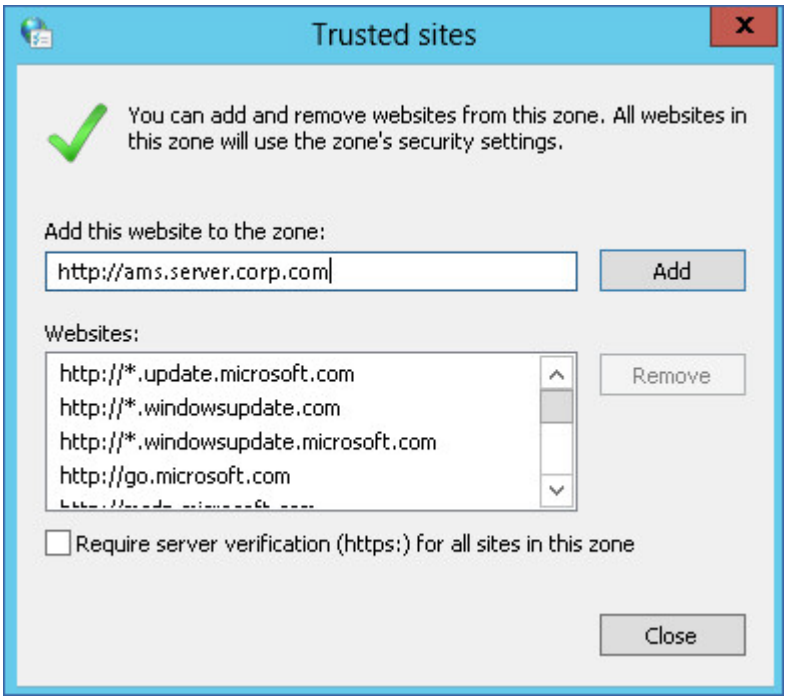
1. 進入**[控制台]** > **[網際網路選項]**。
2. 在**[安全性]**標籤上，選擇**[受信任的網站]**，然後按一下**[自訂層級]**。



3. 在**[登入]**下，選擇**[使用目前的使用者名稱與密碼自動登入]**，然後按一下**[確定]**。



4. 在**[安全性]**標籤，當**[受信任的網站]**仍選取時，按一下**[網站]**。
5. 在 **[新增此網站到區域]** 中，輸入 Cyber Protect Web 主控台登入頁面的網址，然後按一下 **[新增]**。



6. 按一下**[關閉]**。
7. 按一下 **[確定]**。

僅允許使用 HTTPS 連線到 Web 主控台

基於安全性考量，您可以透過 HTTP 通訊協定防止使用者存取 Cyber Protect Web 主控台，並僅允許 HTTPS 連線。

若要僅允許使用 HTTPS 連線到 Web 主控台

1. 在執行管理伺服器的電腦上，使用文字編輯器開啟下列設定檔案：
   - 在 Windows 中：`%ProgramData%\Acronis\ApiGateway\api_gateway.json`
   - 在 Linux 中：`/var/lib/Acronis/ApiGateway/api_gateway.json`
2. 找到以下區段：

```
"tls": {
  "auto_redirect" : false,
  "cert_file": "cert.pem",
```

3. 將 `"auto_redirect"` 值從 `false` 變更為 `true`。

   如果缺少 `"auto_redirect"` 行，請手動新增：

```
"auto_redirect": true,
```

4. 儲存 `api_gateway.json` 檔案。

重要事項

請小心謹慎，不要意外刪除設定檔中的任何逗點、括弧以及引號。

5. 如下所述，重新啟動 Acronis Service Manager 服務。

若要在 Windows 中重新啟動 Acronis Service Manager 服務

在 Windows 中

1. 在 **[開始]** 功能表中，按一下 **[執行]**，然後輸入：**cmd**
2. 按一下 **[確定]**。
3. 執行以下命令：

```
net stop asm
net start asm
```

在 Linux 中

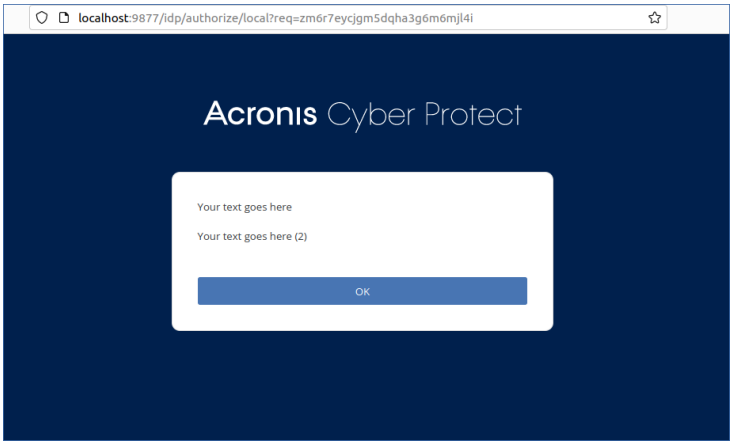
1. 開啟**終端機**。
2. 在任何目錄中執行以下命令：

```
sudo service acronis_asm restart
```

正在將自訂訊息新增至 Web 主控台

您可以將自訂訊息新增至 Cyber Protect Web 主控台。

每次登入嘗試前都會顯示此訊息。



必要條件

如果您的保護計劃套用至執行管理伺服器的電腦，請確認已停用自我保護功能。否則，您將無法編輯組態檔。

如需有關自我保護功能停用或啟用方式的詳細資訊，請參閱 "自我保護" (第 439 頁)。

若要將自訂訊息新增至 Web 主控台

在 Windows 中

1. 登入安裝管理伺服器的電腦。您的帳戶必須具備系統管理員權限。
2. 瀏覽至 %Program Files%\Acronis\AccountServer。
3. [選用] 製作 AccountServer.zip 檔案的備份副本。
4. 瀏覽至 %Program Files%\Acronis\AccountServer\AccountServer.zip\static\locale。
5. 解壓縮對應至您用於 Cyber Protect Web 主控台的 JSON 檔案。例如，如果您使用英文，則解壓縮 en.json 檔案。

   注意事項
   若要能夠編輯檔案，不只是按兩下開啟檔案，您必須解壓縮該檔案。

6. 開啟解壓縮的檔案進行編輯。您可以使用文字編輯器，例如記事本或 Notepad++。
7. 導覽至下行，然後在結尾新增逗號：

   ```
   "APP_LOGINFORM_LOGIN_BUTTON":"Log in",
   ```

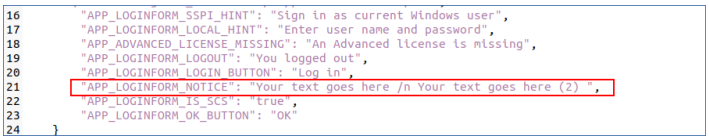
8. 在 "APP_LOGINFORM_LOGIN_BUTTON":"Log in" 行下，新增下行：

   ```
   "APP_LOGINFORM_NOTICE": "<Type your custom message here>",
   ```

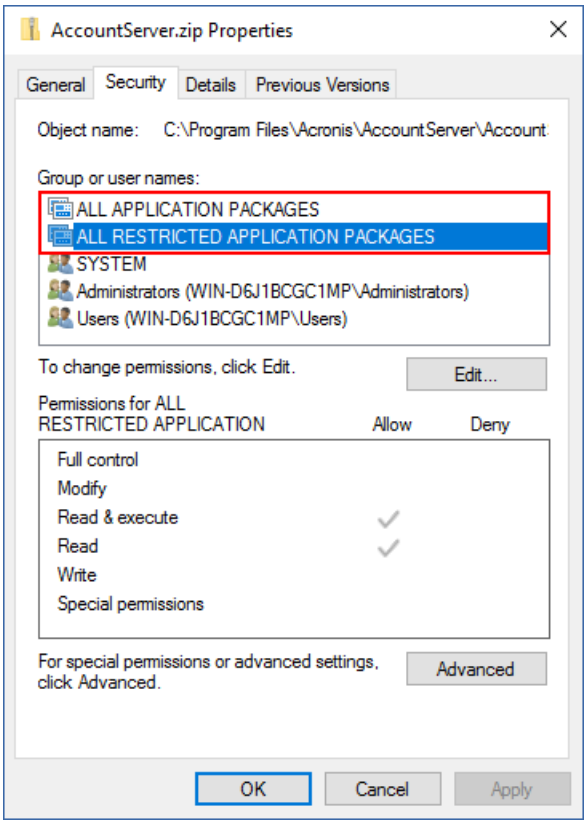
   ```
   "APP_LOGINFORM_IS_SCS": "true",
   ```

   ```
   "APP_LOGINFORM_OK_BUTTON":"OK"
   ```

   例如：

9. 儲存變更，然後將已編輯的 JSON 檔案放回 %Program Files%\Acronis\AccountServer\AccountServer.zip\static\locale。
10. 以滑鼠右鍵按一下 AccountServer.zip 檔案，然後瀏覽至 **[屬性]** > **[安全性]** 以確認 [所有應用程式套件] 和 [所有受限制的應用程式套件] 已新增至具有 **[讀取]** 和 **[讀取和執行]** 權限的 **[群組或使用者名稱]** 下。



注意事項

如果 [所有受限制的應用程式套件] 遺失，則移除該清單中的 [所有應用程式套件]，然後重新加入它。當您新增 [所有應用程式套件] 時，[所有受限制的應用程式套件] 即會在您新增時自動顯示。

11. 如所述，重新啟動 **Acronis Service Manager 服務**。

在 Linux 中

1. 登入安裝管理伺服器的電腦。
2. 瀏覽至 `/usr/lib/Acronis/AccountServer`。
3. 請確認您具備 `AccountServer.zip` 檔案的寫入權限。
4. [選用] 製作 `AccountServer.zip` 檔案的備份副本。
5. 瀏覽至 `/usr/lib/Acronis/AccountServer/static/locale`。
6. 解壓縮對應至您用於 Cyber Protect Web 主控台的 JSON 檔案。例如，如果您使用英文，則解壓縮 `en.json` 檔案。
7. 開啟解壓縮的檔案進行編輯。
8. 導覽至下行，然後在結尾新增逗號：

```
"APP_LOGINFORM_LOGIN_BUTTON":"Log in",
```

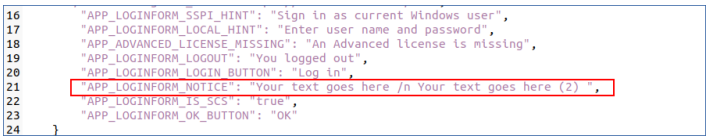
9. 在 `"APP_LOGINFORM_LOGIN_BUTTON":"Log in"` 行下，新增下行：

```
"APP_LOGINFORM_NOTICE": "<Type your custom message here>",
```

```
"APP_LOGINFORM_IS_SCS": "true",
```

```
"APP_LOGINFORM_OK_BUTTON":"OK"
```

例如：



10. 儲存變更，然後將已編輯的 JSON 檔案放回 `/usr/lib/Acronis/AccountServer/static/locale`。
11. 如所述，重新啟動 **Acronis Service Manager 服務**。

SSL 憑證設定

本節描述如何：

- 設定使用管理伺服器所產生之自我簽署安全通訊端層 (SSL) 憑證的保護代理程式。
- 將管理伺服器產生的自我簽署 SSL 憑證變更為受信任憑證授權單位發出的憑證，例如 GoDaddy、Comodo 或 GlobalSign。若執行此變更作業，則管理伺服器使用的憑證將在任何電腦上都授信。使用 HTTPS 通訊協定登入 Cyber Protect Web 主控台時，將不會出現瀏覽器安全性警示。

或者，您可以透過將所有使用者重新導向至 HTTPS，設定管理伺服器以禁止透過 HTTP 存取 Cyber Protect Web 主控台。

使用自我簽署的憑證

若要在 Windows 中設定保護代理程式

1. 在已安裝代理程式的電腦上，開啟登錄編輯程式。
2. 找到以下登錄機碼：**HKEY_LOCAL_MACHINE\Software\Acronis\BackupAndRecovery\Settings\CurlOptions.**
3. 將 **VerifyPeer** 值設定為 **0**。
4. 請確認 **VerifyHost** 值已設定為 **0**。
5. 重新啟動 Managed Machine Service (MMS)：
   a. 在 **[開始]** 功能表中，按一下 **[執行]**，然後輸入：**cmd**
   b. 按一下 **[確定]**。
   c. 執行以下命令：

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

若要在 Linux 中設定保護代理程式

1. 在已安裝代理程式的電腦上，開啟檔案 **/etc/Acronis/BackupAndRecovery.config** 以進行編輯。
2. 瀏覽到 **CurlOptions** 機碼，並將 **VerifyPeer** 的值設定為 **0**。請確認 **VerifyHost** 的值也設定為 **0**。
3. 儲存您所做的編輯。
4. 在任意目錄中執行下列命令以重新啟動 Managed Machine Service (MMS)：

```
sudo service acronis_mms restart
```

若要在 macOS 中設定保護代理程式

1. 在已安裝代理程式的電腦上，停止 Managed Machine Service (MMS)：
   a. 前往 **[應用程式]** > **[公用程式]** > **[終端機]**
   b. 執行下列命令：

```
sudo launchctl stop acronis_mms
```

2. 開啟檔案 **/Library/Application Support/Acronis/Registry/BackupAndRecovery.config** 以進行編輯。
3. 瀏覽到 **CurlOptions** 機碼，並將 **VerifyPeer** 的值設定為 **0**。請確認 **VerifyHost** 的值也設定為 **0**。
4. 儲存您所做的編輯。
5. 在終端機中執行下列命令以啟動 Managed Machine Service (MMS)：

```
sudo launchctl starts acronis_mms
```

使用受信任憑證授權單位發出的憑證

若要設定 SSL 憑證設定

1. 確保您具有以下所有項目：

如果您使用的是憑證和金鑰檔案	如果您使用的是 PFX 檔案
憑證檔案 (.pem 格式)	PFX 檔案
具有憑證私密金鑰的檔案 (格式通常為 .key)	
私密金鑰密碼 (若金鑰受密碼保護)	PFX 檔案的密碼 (若檔案受密碼保護)

2. 將檔案複製到執行管理伺服器的電腦上。
3. 在此電腦上，使用文字編輯器開啟下列設定檔案：
   - 在 Windows 中：`%ProgramData%\Acronis\ApiGateway\api_gateway.json`
   - 在 Linux 中：`/var/lib/Acronis/ApiGateway/api_gateway.json`
4. 找到以下區段：

```
"tls": {
    "cert_file": "cert.pem",
    "key_file": "key.pem",
    "passphrase": "",
```

5. 在介於 "cert_file" 行中的引號之間，指定憑證檔案或 PFX 檔案的完整路徑。

   例如：

作業系統	如果您使用的是成對的憑證和金鑰	如果您使用的是 .pfx 檔案
Windows (注意正斜線)	"cert_file":"C:/certificate/local-domain.ams.pem"	"cert_file":"C:/certificate/local-domain.ams.pfx"
Linux	"cert_file": "/home/user/local-domain.ams.pem"	"cert_file": "/home/user/local-domain.ams.pfx"

6. 在介於 "key_file" 行中的引號之間，指定包含憑證金鑰的私密金鑰檔案或 PFX 檔案的完整路徑。

   PFX 檔案通常同時包含憑證及其金鑰。在此情況下，在 "key_file" 行中，指定與在上一個步驟中相同的路徑。

   例如：

作業系統	如果您使用的是成對的憑證和金鑰	如果您使用的是 .pfx 檔案
Windows (注意正斜線)	"key_file":"C:/certificate/private.key"	"cert_file":"C:/certificate/local-domain.ams.pfx"
Linux	"key_file": "/home/user/private.key"	"cert_file": "/home/user/local-domain.ams.pfx"

7. [選用] 如果私密金鑰或 PFX 檔案受密碼保護，則在介於 "passphrase" 行中的引號之間，指定密碼。

   例如："passphrase": "my password"

注意事項

如果在您的 api_gateway.json 組態檔中缺少 "passphrase": ""，行，請手動新增。

例如：

```
"tls": {
    "cert_file": "cert.pem",
    "key_file": "key.pem",
    "passphrase": "my password",
}
```

8. 儲存 api_gateway.json 檔案。

重要事項

請小心謹慎，不要意外刪除設定檔中的任何逗點、括弧以及引號。

9. 如下所述，重新啟動 Acronis Service Manager 服務。

若要重新啟動 Acronis Service Manager 服務

在 Windows 中

1. 在 **[開始]** 功能表中，按一下 **[執行]**，然後輸入：**cmd**
2. 按一下 **[確定]**。
3. 執行以下命令：

```
net stop asm
net start asm
```

在 Linux 中

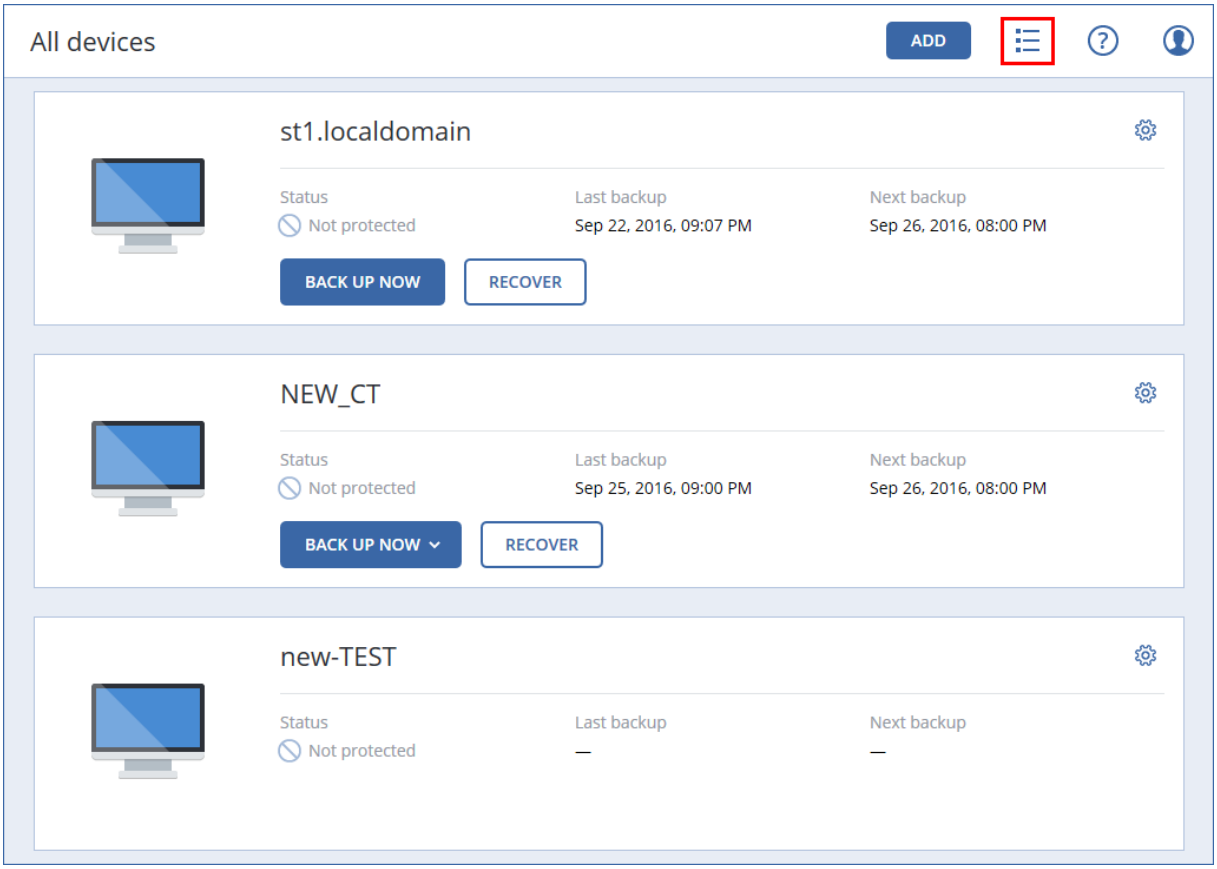
1. 開啟**終端機**。
2. 在任何目錄中執行以下命令：

```
sudo service acronis_asm restart
```

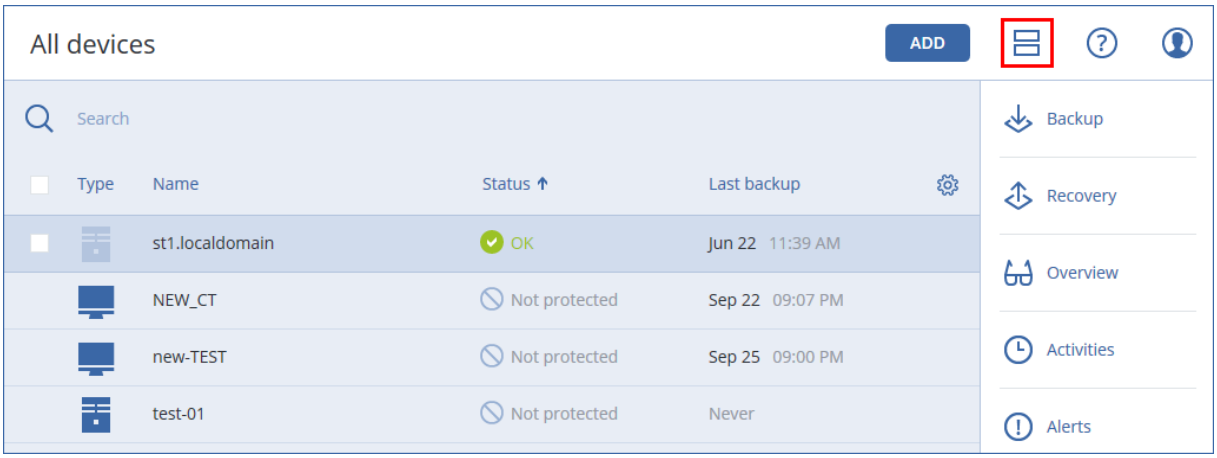
Cyber Protect Web 主控台檢視

Cyber Protect Web 主控台有兩種檢視：簡易檢視與表格檢視。如果要在這兩個檢視畫面間切換，請按一下右上角對應的圖示。

簡易檢視畫面支援數量少的電腦。



當電腦數目變多時，系統就會自動啟用表格檢視畫面。



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。

當一部電腦上線或離線時，其在 Cyber Protect Web 主控台內的狀態需要一些時間才會變更。

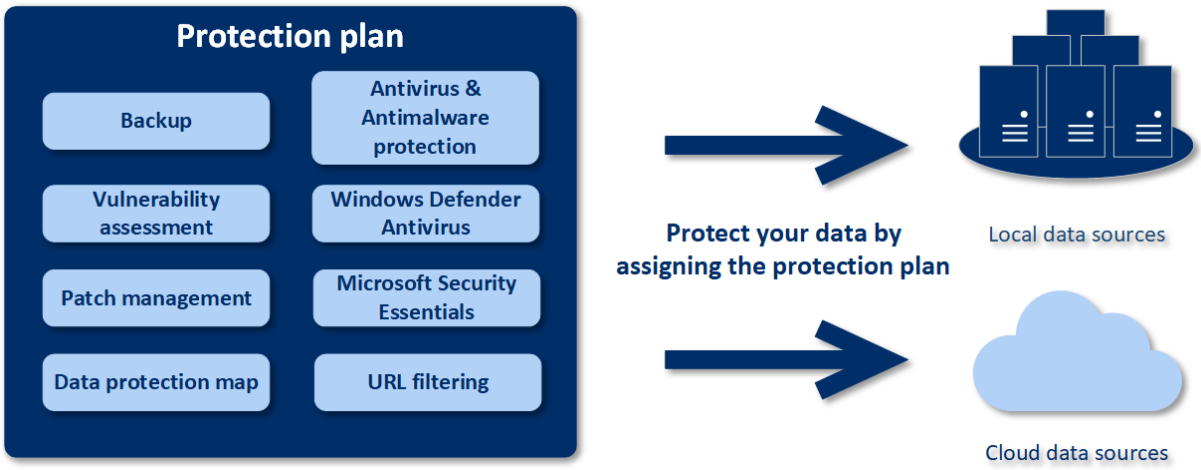
電腦狀態每分鐘檢查一次。如果此電腦上安裝的代理程式未在傳輸資料，而且連續五次檢查都沒有回應，則該電腦會顯示為離線。當電腦回應狀態檢查或開始傳輸資料時，該電腦會顯示為線上。

保護計劃和模組

保護計劃是一種結合數種資料保護模組的計劃，包括

- 備份 – 可讓您將資料來源備份到本機或雲端儲存空間。
- 防毒和反惡意程式碼保護 – 可讓您使用內建的反惡意程式碼解決方案檢查電腦。
- URL 篩選 – 可讓您透過封鎖對惡意 URL 和要下載之內容的存取來保護電腦，免受來自網際網路的威脅。
- Windows Defender 防毒軟體 – 可讓您管理 Windows Defender 防毒軟體的設定以保護您的環境。
- Microsoft Security Essentials – 可讓您管理 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 Microsoft 和第三方產品中的弱點，並對您發送通知。
- 修補程式管理 – 可讓您安裝電腦上 Microsoft 和第三方產品的修補程式和更新，以終止探索到的弱點。
- 資料保護圖 – 可讓您探索資料以監視重要檔案的保護狀態。

保護計劃可讓您完整保護您的資料來源，免受內外部威脅的影響。您可以啟用和停用不同的模組，並進行模組設定，以建立滿足各種商業需求的彈性計劃。



建立保護計劃

保護計劃可在其建立時 (或之後) 套用至多部電腦。當您建立計劃時，系統會檢查作業系統和裝置類型 (例如，工作站、虛擬機器等等)，並僅顯示適用於您裝置的那些計劃模組。

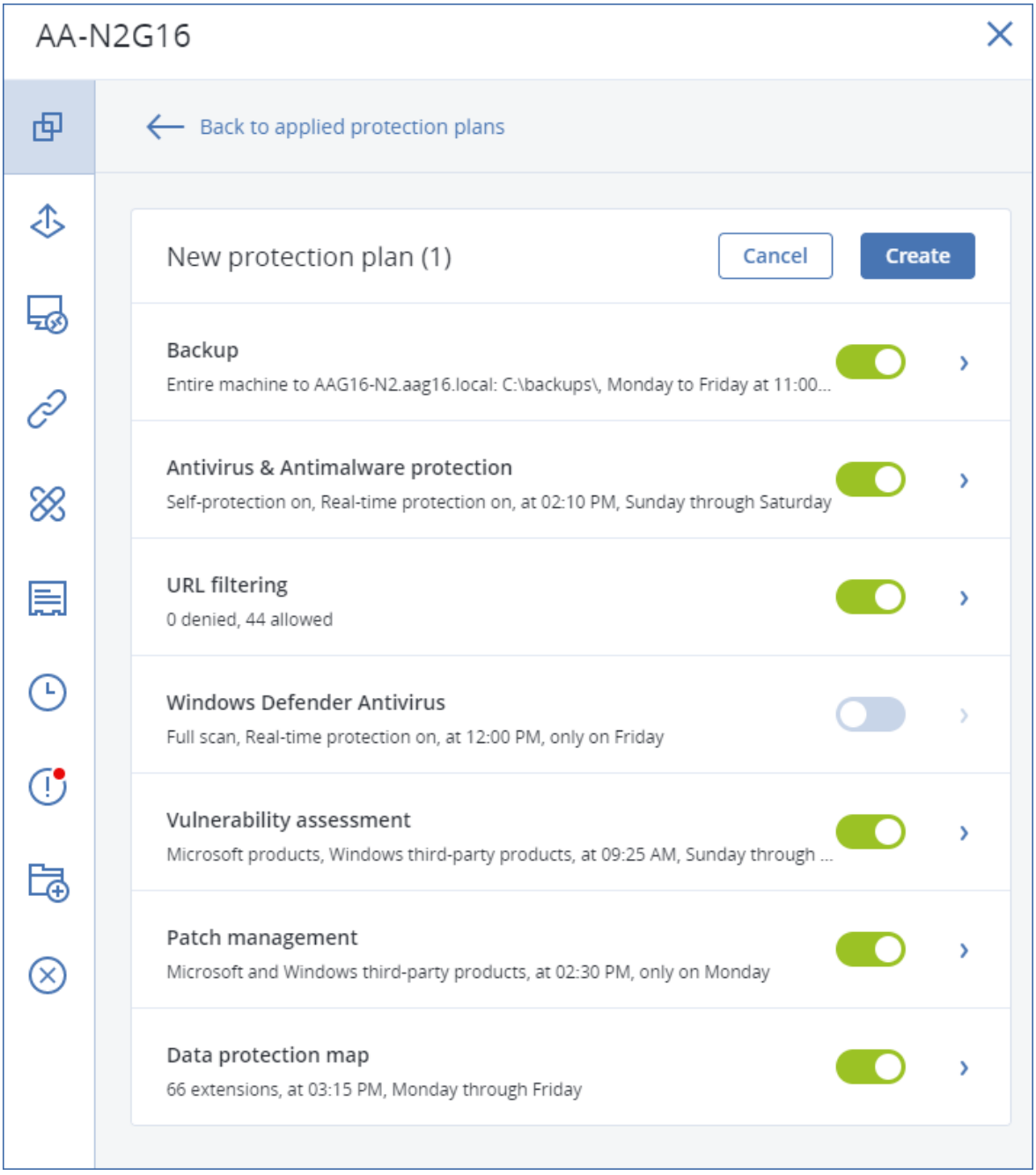
保護計劃可以透過兩種方式建立：

- 在 **[裝置]** 區段中 – 當您選擇要保護的一或多個裝置，然後為其建立計劃時。
- 在 **[計劃]** 區段中 – 當您建立一個計劃，然後選擇要套用的電腦時。

讓我們考慮第一種方式。

建立第一個保護計劃

1. 在 Cyber Protect Web 主控台中，移至 **[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]**。您將會看到具有預設設定的保護計劃。



4. [選擇性] 若要修改保護計劃名稱，按一下名稱旁邊的鉛筆圖示。
5. [選擇性] 若要啟用或停用保護計劃模組，按一下模組名稱旁邊的開關。
6. [選擇性] 若要設定模組參數，按一下保護計劃的對應區段。
7. 準備就緒後，按一下 **[建立]**。

按一下 **[立即執行]**，可以視需要執行 [備份]、[防毒和反惡意程式碼保護]、[弱點評估]、[修補程式管理] 和 [資料保護圖] 模組。

解決計劃衝突

保護計劃可以為下列狀態之一：

- **作用中** – 已指派給裝置並在其上執行的計劃。
- **非作用中** – 已指派給裝置但遭到停用而且未其上執行的計劃。

將數個計劃套用至一個裝置

您可以將數個保護計劃套用至單一裝置。因此，您將在單一裝置上獲指派不同保護計劃的組合。例如，您可以套用僅啟用 [防毒和反惡意程式碼保護] 模組的計劃，以及僅啟用 [備份] 模組的另一個計劃。只有在保護計劃沒有交集的模組時，才可以加以結合。如果在多個保護計劃中啟用相同的模組，您必須解決它們之間的衝突。

解決計劃衝突

計劃與已經套用的計劃發生衝突

當您在已經套用計劃的一或多個裝置上建立新的計劃，且已經套用的計劃與新計劃發生衝突時，可以使用下列其中一種方式解決衝突：

- 建立一個新計劃、套用該計劃，然後停用所有已經套用的衝突計劃。
- 建立一個新計劃並停用該計劃。

當您在已經套用計劃的一或多個裝置上編輯計劃，且已經套用的計劃與所做的變更發生衝突時，可以使用下列其中一種方式解決衝突：

- 將變更儲存至計劃，並停用所有已經套用的衝突計劃。
- 將變更儲存至計劃，並停用該計劃。

裝置計劃與群組計劃發生衝突

如果某個裝置包含在已獲指派群組計劃的裝置群組中，而且您嘗試將新的計劃指派給某個裝置時，則系統將會要求您透過執行下列其中一個操作來解決衝突：

- 將某個裝置從群組中移除，並將新的計劃套用至該裝置。
- 將新的計劃套用至整個群組，或編輯目前的群組計劃。

授權問題

裝置上已指派的配額必須適用於要執行、更新或套用的保護計劃。若要解決授權問題，請執行下列其中一項操作：

- 停用已指派的配額不支援的模組，然後繼續使用保護計劃。
- 手動變更已指派的配額：移至 **[裝置]** > **<特定裝置>** > **[詳細資料]** > **[服務配額]**。接著，撤銷現有的配額並指派一個新配額。

具有保護計劃的作業

如需有關如何建立保護計劃的資訊，請參閱「建立保護計劃」。

具有保護計劃的可用動作

您可以執行具有保護計劃的下列動作：

- 重新命名計劃
- 啟用/停用模組，並編輯每個模組設定
- 啟用/停用計劃

  已停用的計劃將不會在套用該計劃的裝置上執行。

  對於之後打算使用相同計劃保護相同裝置的系統管理員而言，此動作相當方便。計劃未從裝置撤銷，因此，若要還原保護，系統管理員僅需要重新啟用該計劃即可。
- 將計劃套用至裝置或裝置群組
- 從裝置撤銷計劃

  已撤銷的計劃不會再套用至裝置。

  對於不需要再次使用相同計劃快速保護相同裝置的系統管理員而言，此動作相當方便。若要還原對已撤銷計劃的保護，系統管理員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所需的裝置。
- 匯入/匯出計劃

  注意事項
  您僅能匯入在 Acronis Cyber Protect 15 中建立的保護計劃。在舊版中建立的保護計劃與 Acronis Cyber Protect 15 不相容。

- 刪除計劃

套用現有的保護計劃

1. 選擇您要保護的電腦。
2. 按一下 **[保護]**。如果已將某個保護計劃套用至選擇的電腦，請按一下 **[新增計劃]**。
3. 軟體會顯示先前建立的保護計劃。
4. 選擇您需要的保護，然後按一下 **[套用]**。

編輯保護計劃

1. 如果您要編輯所有已套用到電腦上的保護計劃，請選擇其中一部電腦。否則，選擇您要編輯保護計劃的多部電腦。
2. 按一下 **[保護]**。
3. 選擇您要編輯的保護計劃。
4. 按一下保護計劃名稱旁的省略符號圖示，然後按一下 **[編輯]**。
5. 若要修改計劃參數，按一下保護計劃面板的對應區段。
6. 按一下 **[儲存變更]**。

7. 若要變更已套用到所有電腦的保護計劃，請按一下 **[將變更套用至此保護計劃]**。否則，按一下 **[只為選擇的裝置建立新保護計劃]**。

從電腦撤銷保護計劃

1. 選擇您要從中撤銷保護計劃的電腦。
2. 按一下 **[保護]**。
3. 如果電腦已套用數個保護計劃，請選擇您要撤銷的保護計劃。
4. 按一下保護計劃名稱旁的省略符號圖示，然後按一下 **[撤銷]**。

刪除保護計劃

1. 選擇已套用您要刪除的保護計劃的任何電腦。
2. 按一下 **[保護]**。
3. 如果電腦已套用數個保護計劃，請選擇您要刪除的保護計劃。
4. 按一下保護計劃名稱旁的省略符號圖示，然後按一下 **[刪除]**。
   因此，保護計劃會從所有電腦中撤銷，並完全從 Web 介面中移除。

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。

注意事項
在內部部署中，如果管理伺服器上只有標準授權，則保護計劃無法套用到多部實體機器。每一部實體機器都必須有自己的保護計劃。

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]**。

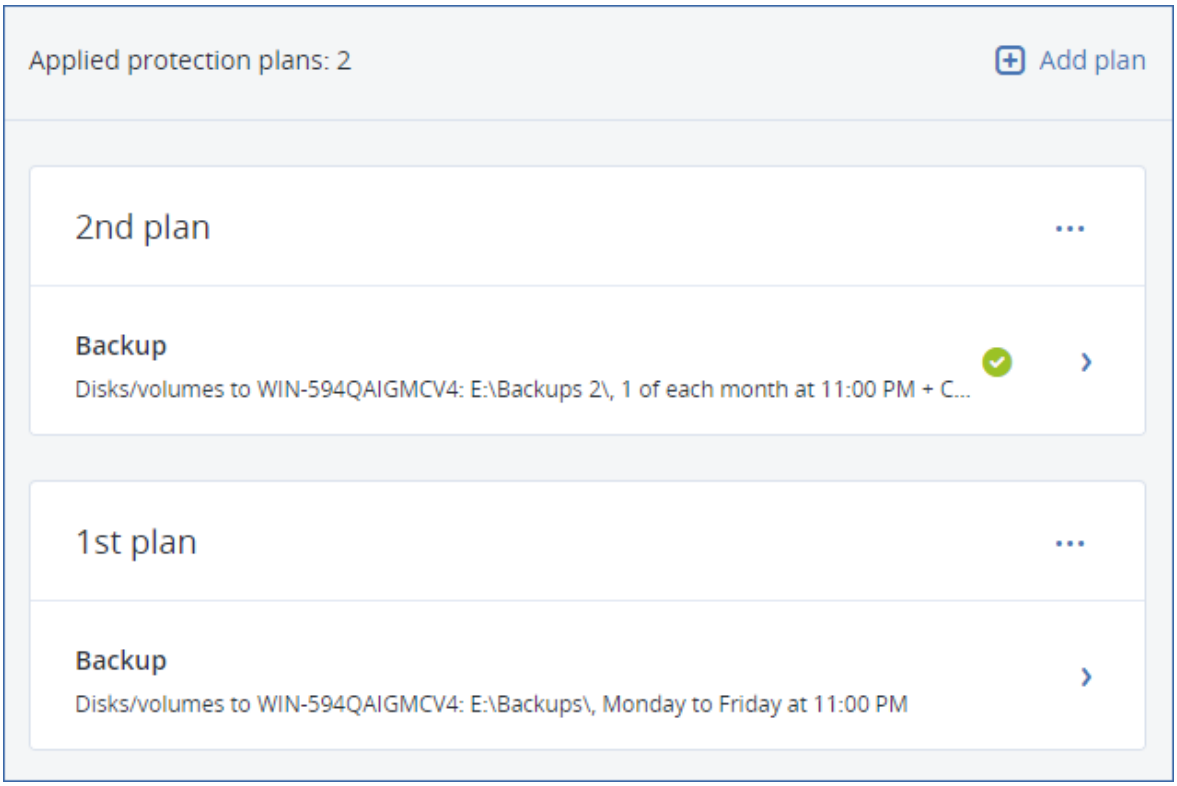
   軟體就會顯示已套用至電腦的保護計劃。如果電腦還未獲指派任何計劃，則您將會看到可以套

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. [選擇性] 若要修改保護計劃名稱，請按一下預設名稱。
5. [選擇性] 若要修改 [備份] 模組參數，請按一下保護計劃面板的對應區段。
6. [選擇性] 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]**。

備份模組速查表

重要事項
本節中所述的部分功能僅適用於內部部署。

下表摘要說明可用的 [備份] 模組參數。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 選擇方法	備份目標位置	排程 備份配置 (非針對雲端)	保留多長時間
磁碟/磁碟區 (實體機器)	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 SFTP 伺服器*	一律增量備份 (單一檔案)* 一律完整備份	按照備份存留期 (單一規則/每一組備份) 按照備份數目 按照備份大小總計*

		NFS* Secure Zone* 受管理的位置* 磁帶裝置*	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)	永久保留
磁碟/磁碟區 (虛擬機器)	原則規則 檔案篩選器	雲端 本機資料夾 網路資料夾 SFTP 伺服器* NFS* 受管理的位置* 磁帶裝置*		
檔案 (僅限實體機器)	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 SFTP 伺服器* NFS* Secure Zone* 受管理的位置* 磁帶裝置	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) 一律增量備份 (單一檔案)* 自訂 (F-D-I)	
ESXi 設定	直接選擇	本機資料夾 網路資料夾 SFTP 伺服器 NFS*		
系統狀態 (僅限在雲端部署)	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	直接選擇	雲端 本機資料夾 網路資料夾 受管理的位置* 磁帶裝置		
Exchange 資料庫	直接選擇			
Exchange 信箱	直接選擇	雲端 本機資料夾 網路資料夾 受管理的位置*	一律增量備份 (單一檔案)	
Microsoft 365 信箱	直接選擇			按照備份存留期 (單一規則/每一組備份) 按照備份數目 永久保留

* 請參閱以下限制。

限制

SFTP 伺服器與磁帶裝置

- 這些位置無法做為執行 macOS 的電腦的備份目的地。
- 這些位置無法做為應用程式感知備份的目的地。
- 當備份到這些位置時，將無法使用**一律增量備份(單一檔案)**備份配置。
- 這些位置無法使用**按照備份大小總計**保留規則。

NFS

- 在 Windows 中無法使用備份至 NFS 共用。
- 當備份到 NFS 共用時，將無法針對檔案 (實體機器) 使用 **[一律增量備份 (單一檔案)]** 備份配置。

Secure Zone

- 在 Mac 上無法建立 Secure Zone。

受管理的位置

- 不得選擇已啟用重複資料刪除或加密的受管理位置來做為目的地：
  - 如果備份配置設定為**一律增量備份(單一檔案)**
  - 如果備份格式設定為**12 版**
  - 適用於執行 Mac OS 的電腦上的磁碟層級備份
  - 備份 Exchange 信箱與 Microsoft 365 信箱。
- 在有啟用重複資料刪除的受管理地點上，無法使用**按照備份大小總計**的保留規則。

一律增量備份 (單一檔案)

- 當備份到 SFTP 伺服器或磁帶裝置上時，無法使用**一律增量備份(單一檔案)**的備份配置。
- 只有在主要備份位置為 Cloud 時，才能針對檔案 (實體機器) 使用 **[一律增量備份 (單一檔案)]** 備份配置。

依備份大小總計

- 無法使用**按照備份大小總計**保留規則：
  - 如果備份配置設定為**一律增量備份(單一檔案)**
  - 備份到 SFTP 伺服器、磁帶裝置或已啟用重複資料刪除的受管理位置。

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。

若要設定此種備份，請在 **[要備份的內容]** 中選擇 **[整部電腦]**。

重要事項

外接式磁碟機 (例如 USB 快閃磁碟機或 USB 硬碟) 不包含在 **[整部電腦]** 備份中。若要備份這些磁碟機，請設定 **[磁碟/磁碟區]** 備份。如需有關磁碟備份的詳細資訊，請參閱 "選擇磁碟/磁碟區" (第 189 頁)。

選擇磁碟/磁碟區

磁碟層級備份包含磁碟或磁碟區的封裝式複本。您可從磁碟層級備份復原個別磁碟、磁碟區、或檔案。整部電腦的備份就是其所有非卸除式磁碟的備份。

注意事項

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存檔中有無效內容。

有兩種方法可選擇磁碟/磁碟區：直接在每部電腦上選擇或使用原則規則。您可以設定檔案篩選器，將檔案排除在磁碟備份之外。

直接選擇

只有實體機器才能進行直接選擇。若要直接選擇虛擬機器上的磁碟和磁碟區，您必須在其客體作業系統上安裝保護代理程式。

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部電腦，選擇要備份的磁碟或磁碟區旁的核取方塊。
5. 按一下**[完成]**。

使用原則規則

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。

   原則規則將會套用至包含在保護計劃中的所有電腦。在電腦上開始進行備份時，如果找不到至少符合其中一項規則的任何資料，該部電腦上的備份將無法成功執行。
5. 按一下**[完成]**。

適用於 Windows、Linux 及 macOS 的規則

- `[All Volumes]` 會選擇 Windows 電腦上的所有磁碟區，以及 Linux 或 macOS 電腦上的所有已掛載磁碟區。

適用於 Windows 的規則

- 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)]` 會選擇實體電腦的所有磁碟區，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]` 可選擇開機磁碟區和系統磁碟區。這個組合是最小的資料集，可確保能從備份順利復原作業系統。
- `[BOOT+SYSTEM DISK (physical machines)]` 可選擇開機磁碟區和系統磁碟區所在磁碟的所有磁碟區。如果開機磁碟區和系統磁碟區不在相同的磁碟上，將不會選擇任何項目。此規則僅適用於實體機器。
- `[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。

適用於 Linux 的規則

- `/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，請輸入：

```
/dev/mapper/vg_1-lv1
/dev/mapper/vg-l-lv2
```

適用於 macOS 的規則

- `[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。

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，從 Windows 7 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。

選擇檔案/資料夾

檔案層級備份適用於客體系統中所安裝之代理程式備份的實體機器和虛擬機器。

檔案層級的備份不足以復原作業系統。如果您計劃只保護特定資料 (例如目前的專案)，請選擇檔案備份。這會降低備份大小，進而節省儲存空間。

注意事項
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存檔中有無效內容。

選擇檔案有兩種方法：在每部電腦上直接選擇，或透過使用原則規則。藉由設定檔案篩選，這兩種方法都可讓您的選擇結果更為精細。

直接選擇

1. 在 **[要備份的內容]** 中，選擇 **[檔案/資料夾]**。
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. 針對包含在保護計劃中的每部電腦：
   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]**。
      共用必須可從已選擇的電腦存取。

c. 瀏覽至所需的檔案/資料夾，或輸入路徑並按一下箭頭按鈕。如果看到提示，請指定共用資料夾的使用者名稱和密碼。

   不支援備份具有匿名存取權的資料夾。

d. 選擇所需的檔案/資料夾。

e. 按一下**[完成]**。

使用原則規則

1. 在 **[要備份的內容]** 中，選擇 **[檔案/資料夾]**。
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。

   原則規則將會套用至包含在保護計劃中的所有電腦。在電腦上開始進行備份時，如果找不到至少符合其中一項規則的任何資料，該部電腦上的備份將無法成功執行。
5. 按一下**[完成]**。

Windows 的選擇規則

- 檔案或資料夾的完整路徑，例如 **D:\Work\Text.doc** 或 **C:\Windows**。
- 範本：
  - `[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 (通常是 **C:\Users** 或 **C:\Documents and Settings**)。
- 環境變數：
  - `%ALLUSERSPROFILE%` 會選擇所有使用者設定檔之一般資料所在的資料夾 (通常是 **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 所在的資料夾 (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，請輸入：**%PROGRAMFILES%\Java**。

Linux 的選擇規則

- 檔案或目錄的完整路徑。例如，若要將 **file.txt** 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**。
  - `/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。
- 範本：
  - `[All Profiles Folder]` 會選擇 **/home**。這是所有使用者設定檔預設所在的資料夾。

Mac OS 的選擇規則

- 檔案或目錄的完整路徑。
- 範本：
  - [All Profiles Folder] 會選擇 **/Users**。這是所有使用者設定檔預設所在的資料夾。

範例：

- 若要將 **file.txt** 檔案備份在您的桌面，請指定 **/Users/<username>/Desktop/file.txt**，其中 <username> 代表您的使用者名稱。
- 若要備份所有使用者的主目錄，請指定 **/Users**。
- 若要備份安裝應用程式的目錄，請指定 **/Applications**。

選擇系統狀態

系統狀態備份可用於執行 Windows 7 及更高版本的機器。

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。
- 若要備份 ESXi 設定，VMware 用代理程式會在 TCP 連接埠 22 上使用 ESXi 主機的 SSH 連線。請確認您的防火牆不會封鎖此連線。
- 您必須知道 ESXi 主機上「根」帳戶的密碼。

限制

- VMware vSphere 7.0 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 [**備份**]。
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)

由於效能的緣故，備份通常會定期但以很長的時間間隔執行。如果系統突然損壞，將會失去上次備份和系統故障之間的資料變更。

[連續資料保護] 功能可讓您連續備份排程備份之間所選資料的變更：

- 透過追蹤指定之檔案/資料夾中的變更
- 透過追蹤指定的應用程式修改之檔案的變更

您可以從針對備份選擇的資料中選擇特定檔案，以進行連續資料保護。系統將會備份這些檔案的每個變更。您可以將這些檔案復原至上次變更時間。

目前，下列作業系統支援 **[連續資料保護]** 功能：

- Windows 7 和更新版本
- Windows Server 2008 R2 和更新版本

支援的檔案系統：僅限 NTFS、僅限本機資料夾 (不支援共用資料夾)。

[連續資料保護] 選項與 **[應用程式備份]** 選項不相容。

注意事項
不同版本的功能會有所不同。您的授權可能無法使用本文件中所述的部分功能。如需有關各版本隨附功能的詳細資訊，請參閱「包括雲端部署在內的Acronis Cyber Protect 15 版本比較」。

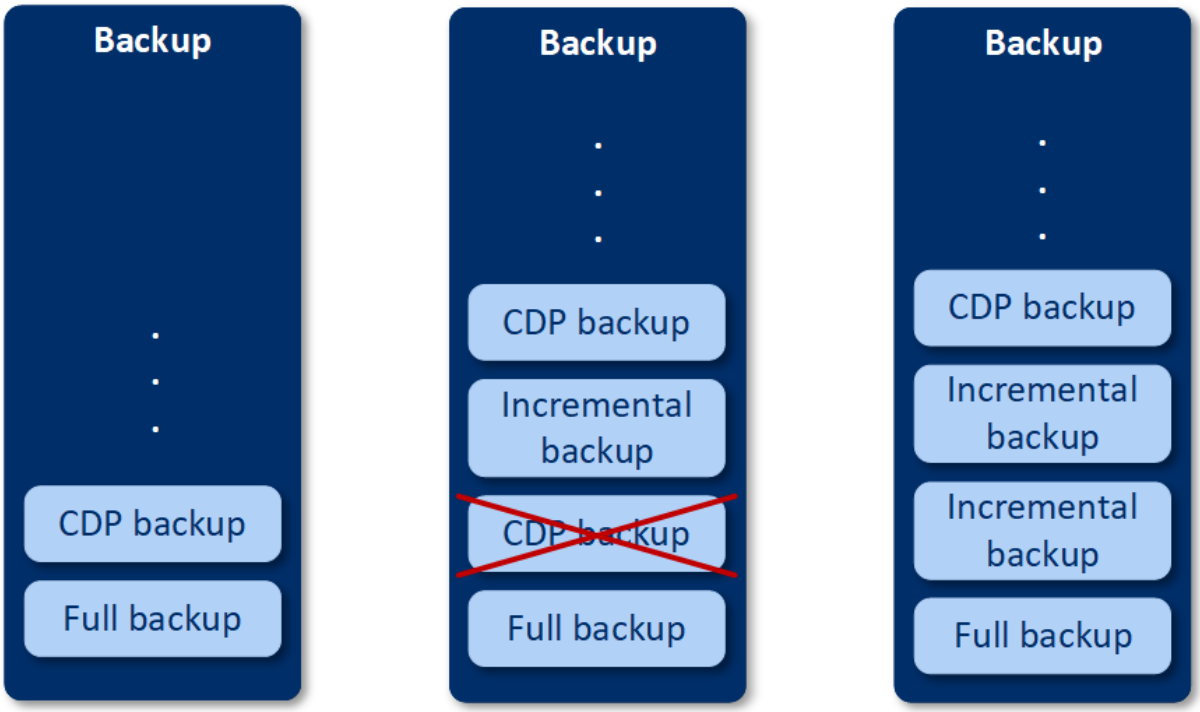
運作原理

讓我們將連續建立的備份稱為 CDP 備份。為了要建立 CDP 備份，必須先建立完整備份或增量備份。

當您在已啟用 [備份] 模組和 **[連續資料保護]** 的情況下首次執行保護計劃時，會先建立完整備份。之後，將會建立所選或已變更之檔案/資料夾的 CDP 備份。CDP 備份一律包含您所選擇的最新資料。當您對所選檔案/資料夾進行變更時，不會建立任何新的 CDP 備份，所有變更都會記錄到相同的 CDP 備份中。

進行排程的增量備份時，將捨棄 CDP 備份，而且在增量備份完成後會建立一個新的 CDP 備份。

因此，CDP 備份永遠保持為備份鏈中具有受保護檔案/資料夾最新實際狀態的最新備份。



如果您已經有一個已啟用 [備份] 模組的保護計劃，而且您決定啟用 **[連續資料保護]**，則會在啟用該選項之後立即建立 CDP 備份，因為備份鏈已經有完整備份。

連續資料保護支援的資料來源和目的地

若要讓連續資料保護正常運作，您必須針對下列資料來源指定下列項目：

要備份的內容	要備份的項目
整部電腦	必須指定檔案/資料夾或應用程式
磁碟/磁碟區	必須指定磁碟/磁碟區和檔案/資料夾或應用程式
檔案/資料夾	必須指定檔案/資料夾

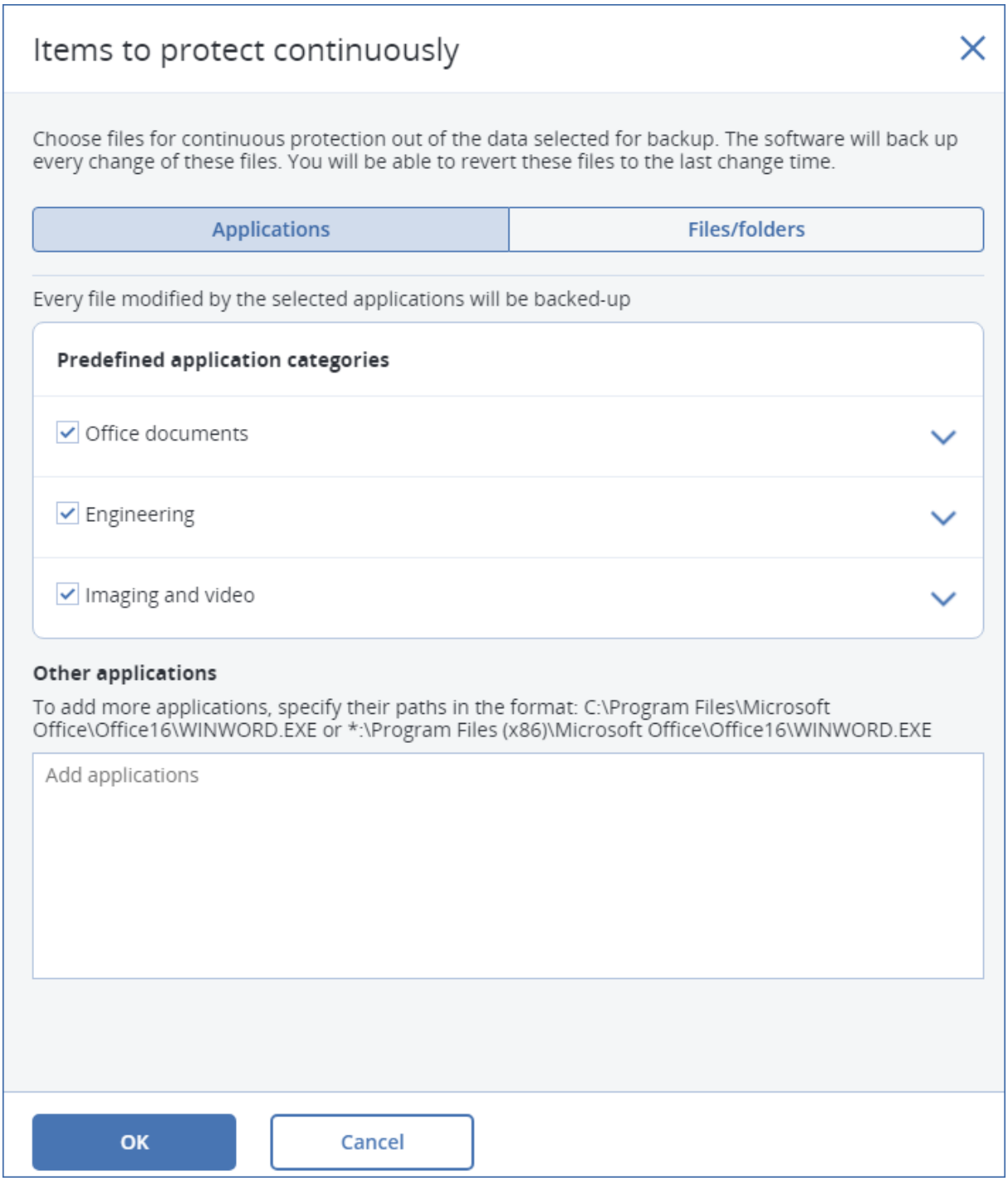
	可以指定應用程式 (非必要)

連續資料保護支援下列備份目的地：

- 本機資料夾
- 網路資料夾
- 指令碼所定義的位置
- 雲端儲存
- Acronis Cyber Infrastructure

使用連續資料保護來保護裝置

1. 在 Cyber Protect Web 主控台中，啟用 **[備份]** 模組的情況下，建立一個保護計劃。
2. 啟用 **[連續資料保護 (CDP)]** 選項。
3. 指定 **[連續保護的項目]**：
   - **應用程式** (系統將會備份所選應用程式所修改的任何檔案)。建議使用此選項保護具有 CDP 備份的 Office 文件。



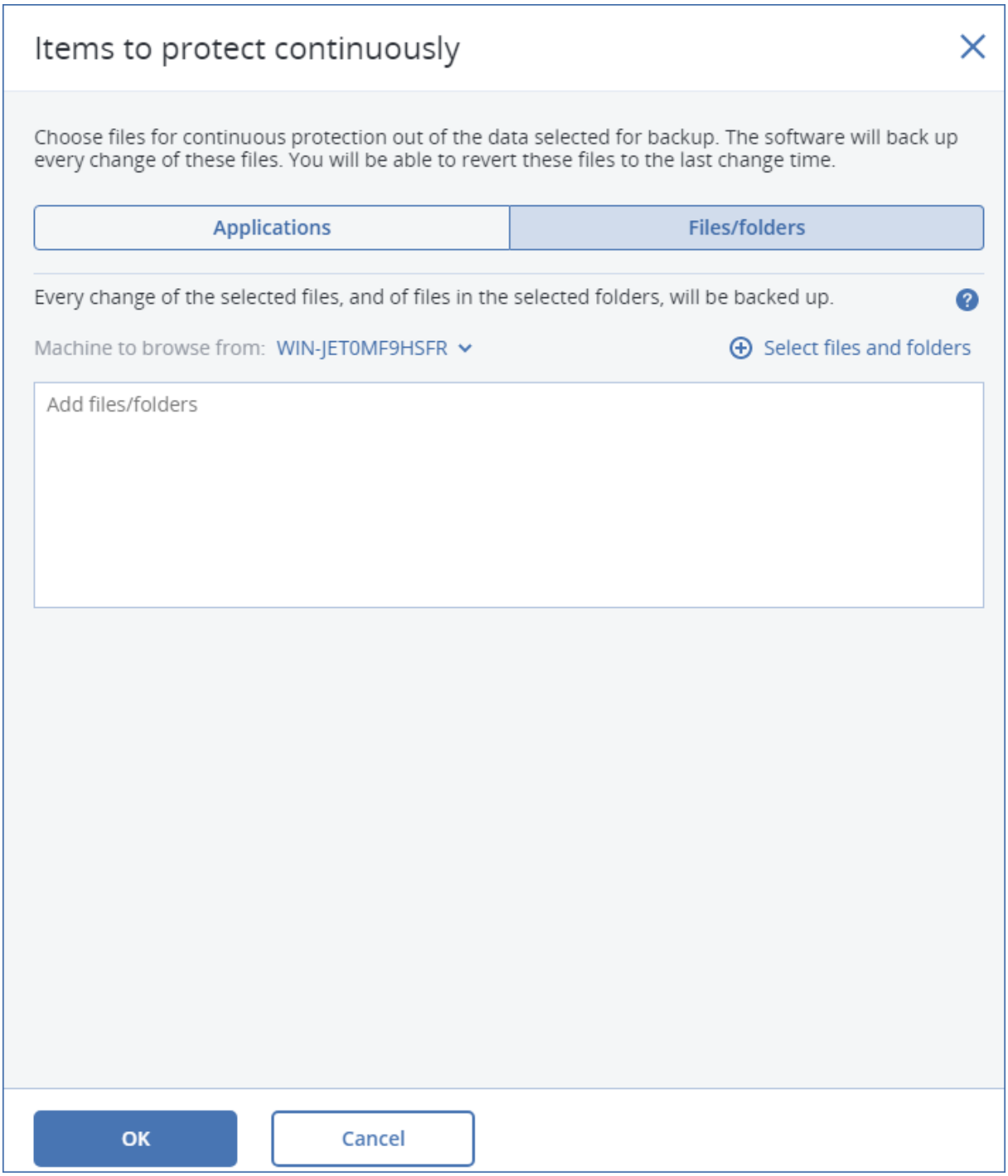
- 您可以從預先定義的類別選擇應用程式，或透過定義應用程式可執行檔的路徑來指定其他應用程式。使用下列其中一種格式：

  `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`

  OR

  `*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`

  - **檔案/資料夾** (將會備份指定之位置中修改的任何檔案)。建議使用此選項保護不斷變更的檔案和資料夾。



1. **要瀏覽的電腦** – 指定您要選擇其檔案/資料夾用於連續資料保護的電腦。
   按一下 **[選擇檔案和資料夾]**, 在指定的電腦上選擇檔案/資料夾。

   重要事項
   如果您手動指定將連續備份其檔案的整個資料夾, 請使用遮罩, 例如:
   正確的路徑:D:\Data*
   錯誤的路徑:D:\Data\

在文字欄位中，您也可以指定規則來選擇將備份的檔案/資料夾。如需有關如何定義規則的詳細資訊，請參閱「選擇檔案/資料夾」。準備就緒後，按一下 **[完成]**。

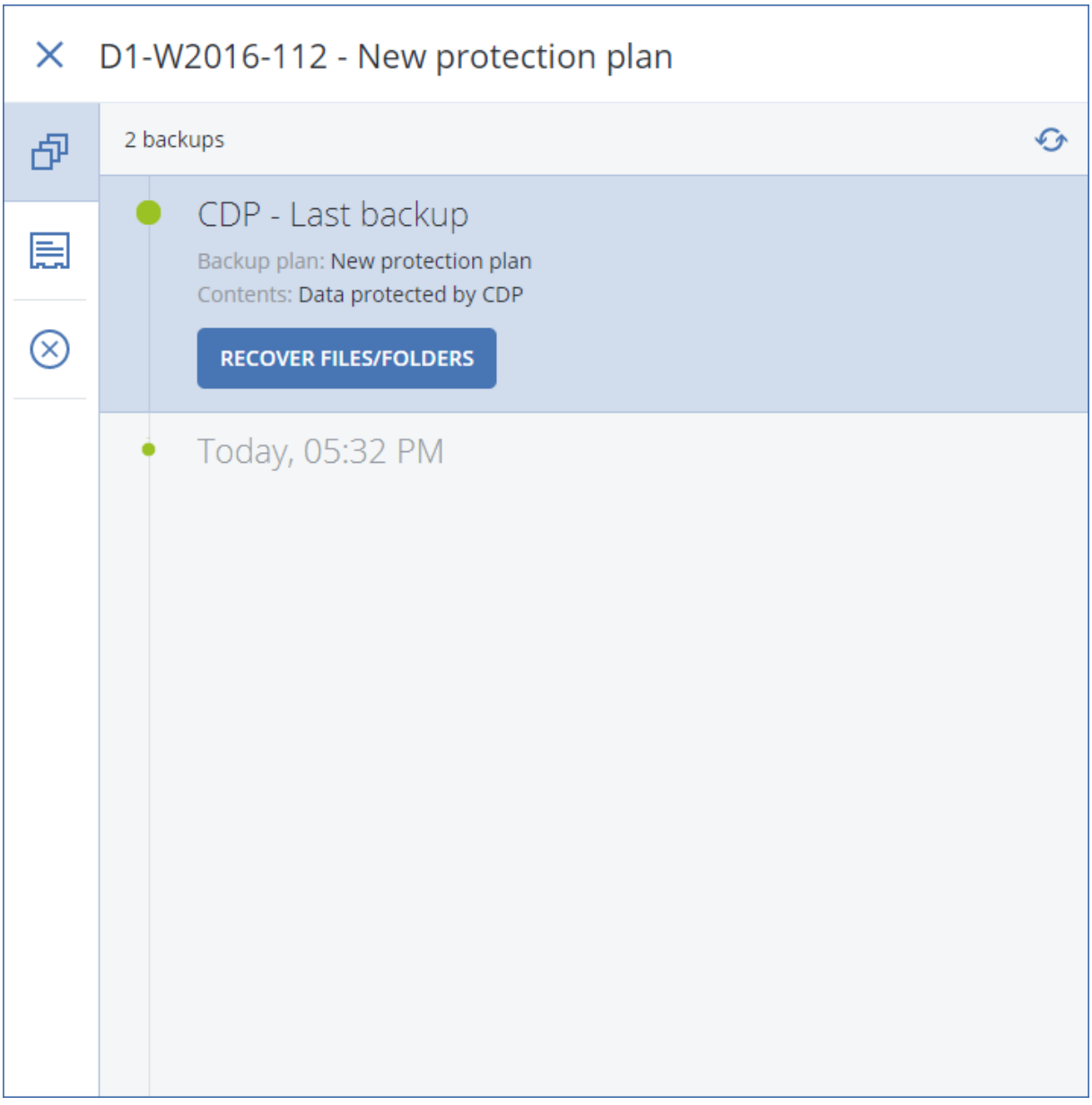
2. 按一下 **[建立]**。

因此，系統會將已啟用連續資料保護的保護計劃指派給所選電腦。第一次定期備份之後，將會連續建立具有 CDP 資料保護之最新複本的備份。系統會同時備份透過應用程式和檔案/資料夾定義的資料。

連續備份的資料會根據針對 [備份] 模組定義的保留原則加以保留。

如何區分連續保護的備份

連續備份的備份有 CDP 首碼。



如何將整部電腦復原到最新狀態

如果您想要能夠將整部電腦復原到最新狀態，可以在保護計劃的 [備份] 模組中，使用 **[連續資料保護 (CDP)]** 選項。

您可以從 CDP 備份復原整部電腦或檔案/資料夾。在第一種情況下，您將使整部電腦處於最新狀態；在第二種情況下，您將使檔案/資料夾處於最新狀態。

選擇目的地

重要事項
本節中所述的部分功能僅適用於內部部署。

若要選擇備份位置

1. 按一下**備份目標位置**。
2. 執行下列其中一項操作：
   - 選擇已使用或預先定義的備份位置
   - 按一下**新增位置**，然後指定新的備份位置。

支援的位置

- **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。
- **Acronis Cyber Infrastructure**
  Acronis Cyber Infrastructure 可以當作高度可靠的軟體定義儲存空間使用，且具有資料備援和自動自我修復功能。可以將儲存設定為一個閘道，用於在 Microsoft Azure 中或與 S3 或 Swift 相容的其中一種儲存解決方案中儲存備份。儲存還可以使用 NFS 後端。如需詳細資訊，請參閱「關於 Acronis Cyber Infrastructure」。

重要事項
備份至 Acronis Cyber Infrastructure 不適用於 macOS 電腦。

- **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 電腦上已安裝 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。
  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」。
- **SFTP**
  輸入 SFTP 伺服器名稱或地址。支援以下標記法:
  `sftp://<伺服器>`
  `sftp://<伺服器>/<資料夾>`
  輸入使用者名稱和密碼後,可瀏覽伺服器資料夾。
  在任一標記法中,您也可以指定連接埠、使用者名稱和密碼。
  `sftp://<伺服器>:<連接埠>/<資料夾>`
  `sftp://<使用者名稱>@<伺服器>:<連接埠>/<資料夾>`
  `sftp://<使用者名稱>:<密碼>@<伺服器>:<連接埠>/<資料夾>`
  如果未指定連接埠號碼,系統會使用連接埠 22。
  對於設定了無密碼之 SFTP 存取權的使用者,無法備份到 SFTP。
  不支援備份至 FTP 伺服器。

進階儲存選項

- **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);
```

- 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");
  ```

  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 Web 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。

- 下列 **VBScript** 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。

- **儲存節點**
  儲存節點是一部伺服器，其設計旨在最佳化保護企業資料所需的各種資源 (例如企業儲存容量、網路頻寬和生產伺服器 CPU 負載) 之使用。藉由組織和管理充當企業備份專用儲存空間的位置 (受管理位置)，可實現這個目標。
  您可按一下**[新增位置]** > **[儲存節點]**選擇已建立位置或建立新的位置。如需有關設定的資訊，請參閱「新增受管理的位置」。
  系統可能會提示您指定儲存節點的使用者名稱和密碼。在安裝儲存節點的電腦上的下列 Windows 群組成員，擁有儲存節點上所有受管理位置的存取權：
  - **系統管理員**
  - **Acronis ASN Remote Users**
    此群組是在安裝儲存節點時自動建立的。此群組預設是空的。您可以手動新增使用者至此群組。
- **磁帶**
  如果磁帶裝置連接到備份電腦或儲存節點，則位置清單顯示預設磁帶集區。自動建立該集區。
  您可按一下**[新增位置]** > **[磁帶]**選取預設集區或建立新集區。如需有關集區設定的資訊，請參閱「建立集區」。

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

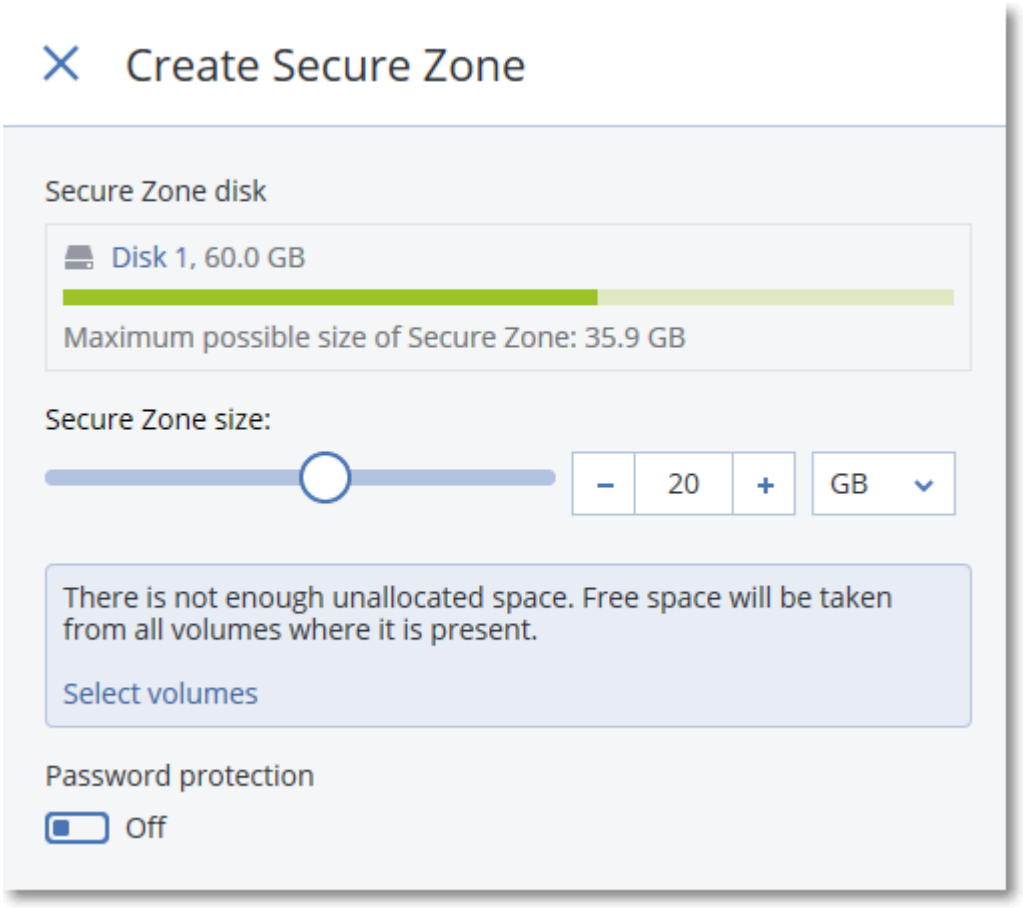
- Secure Zone 一律會在硬碟的末尾區域建立。
- 如果在磁碟末尾沒有未配置空間或未配置空間不足，但是在磁碟區之間有未配置空間，則將會移動磁碟區以便在磁碟末尾增加更多的未配置空間。
- 當集合了所有的未配置空間仍然不足，軟體將使用您選擇的磁碟區上的可用空間，成比例降低磁碟區的大小。
- 但是，在磁碟區上應該有可用空間，這樣作業系統和應用程式才能 運行；例如建立暫存檔。如果可用空間等於或低於磁碟區總大小的 25%，軟體將不會減少磁碟區的大小。僅在磁碟上所有磁碟區的可用空間都為 25% 或更低時，軟體才會繼續按比例減少磁碟區大小。

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. [選擇性步驟] 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. [選擇性步驟] 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。

關於 Acronis Cyber Infrastructure

Acronis Cyber Protect 15 支援與 Acronis Cyber Infrastructure 3.5 Update 5 或更新版本整合。

備份至 Acronis Cyber Infrastructure 不適用於 macOS 電腦。

部署

若要使用 Acronis Cyber Infrastructure，請視需要將其部署至裸機。建議至少五部實體伺服器以充分使用此產品。若您只需要閘道功能，則可以使用一個實體或虛擬伺服器，或者使用盡可能多的伺服器設定閘道叢集。

確保管理伺服器與 Acronis Cyber Infrastructure 之間的時間設定同步。Acronis Cyber Infrastructure 的時間設定可在部署期間進行設定。依預設，會啟用透過網路時間通訊協定 (NTP) 進行的時間同步。

您可以部署數個 Acronis Cyber Infrastructure 執行個體，並在同一管理伺服器上註冊它們。

登錄

在 Acronis Cyber Infrastructure Web 介面中執行註冊。Acronis Cyber Infrastructure 僅可由組織系統管理員註冊，且只能在組織內註冊。註冊之後，儲存即可對所有組織單位可用。它可以作為備份位置新增至任何單位或組織。

反向作業 (取消註冊) 則是在 Acronis Cyber Protect 介面中執行的。按一下 **[設定]** > **[儲存節點]**、按一下所需的 Acronis Cyber Infrastructure，然後按一下 **[刪除]**。

新增備份位置

每個 Acronis Cyber Infrastructure 執行個體上只有一個備份位置可以新增單位或組織。以單位層級新增的位置對此單位及組織管理員可用。以組織層級新增的位置僅對組織管理員可用。

新增位置時，您會建立並輸入其名稱。如果您需要將現有的位置加入至新的或不同的管理伺服器，請選擇 **[使用現有的位置]...** 核取方塊，按一下 **[瀏覽]**，然後從清單中選擇位置。

如果有數個 Acronis Cyber Infrastructure 執行個體是在管理伺服器註冊的，則可以在新增位置時選擇 Cyber Infrastructure 執行個體。

備份配置、作業和限制

從可開機媒體直接存取 Acronis Cyber Infrastructure 不可使用。若要使用 Acronis Cyber Infrastructure，請在管理伺服器上註冊媒體，並透過 Cyber Protect Web 主控台管理。

透過命令列介面存取 Acronis Cyber Infrastructure 不可使用。

在可用的備份配置和備份作業方面，Acronis Cyber Infrastructure 類似於雲端儲存。唯一的區別在於，在執行保護計劃期間，可以從 Acronis Cyber Infrastructure 複寫備份。

使用說明

整套 Acronis Cyber Infrastructure 說明文件可在 Acronis 網站上找到。

排程

重要事項
本節中所述的部分功能僅適用於內部部署。

排程採用安裝代理程式所在作業系統的時間設定 (包括時區)。VMware 用代理程式 (虛擬裝置) 的時區可以在代理程式的介面設定。

例如，如果保護計劃排程在 21:00 執行，並套用到不同時區的數部電腦，則每部電腦將會在本地時間 21:00 開始備份。

排程參數由備份目的地而定。

備份至雲端儲存時

依預設，由週一至週五，每天執行備份。您可以選擇執行備份的時間。

若想要變更備份頻率，請移動滑桿，然後指定備份排程。

您應該依事件排程要執行的備份，而不是依時間。若要這麼做，請在排程選擇器中選擇事件類型。如需更多資訊，請參閱「依事件排程」。

重要事項
第一個備份是完整備份，這表示它也是最耗時的。所有後續備份均為增量備份，大幅減少使用時間。

備份至其他位置時

您可以選擇預先定義備份配置或是建立自定配置。保護計劃包括備份排程和備份方法，備份配置也是其中的一部分。

在 **[備份配置]** 中選擇下列其中一項：

- **一律增量備份 (單一檔案)**
  依預設，由週一至週五，每天執行備份。您可以選擇執行備份的時間。
  若想要變更備份頻率，請移動滑桿，然後指定備份排程。
  備份使用新的 [單一檔案備份格式][1]。
  備份到磁帶裝置或 SFTP 伺服器時，無法使用此配置。

[1]新的備份格式，會將初始完整備份及後續增量備份儲存為單一的 .tib 檔案，而不是一長串的檔案。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 (例如，SFTP 伺服器) 時，無法使用單一檔案備份格式。

- **一律完整備份**

  依預設，由週一至週五，每天執行備份。您可以選擇執行備份的時間。

  若想要變更備份頻率，請移動滑桿，然後指定備份排程。

  所有備份均為完整備份。
- **每週完整備份，每日增量備份**

  依預設，由週一至週五，每天執行備份。您可以修改在星期幾與何時執行備份。

  每週建立一次完整備份。其他所有備份均為增量備份。在星期幾建立完整備份是依 **[每週備份]**選項而定 (請按一下齒輪圖示，然後按一下 **[備份選項]** > **[每週備份]**)。
- **每月完整備份、每週差異備份和每日增量備份 (GFS)**

  依預設，將從週一至週五每天執行增量備份；差異備份則將每週六執行；完整備份則將在每個月的第一天執行。您可以修改這些排程，以及執行備份的時間。

  此備份配置將在保護計劃面板上顯示為 **[自訂]** 配置。
- **自訂**

  指定完整、差異和增量備份的排程。

  在備份 SQL 資料、Exchange 資料或系統狀態時，無法使用差異備份。

無論使用任何備份配置，您都應依事件排程要執行的備份，而不是依時間。若要這麼做，請在排程選擇器中選擇事件類型。如需更多資訊，請參閱「依事件排程」。

其他排程選項

有了任何目的地，您可以執行下列作業：

- 指定備份開始條件，以便在符合條件時才執行已排程的備份。如需詳細資訊，請參閱「開始條件」。
- 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。排程停用後，除非手動啟動一項備份，否則不適用保留規則。
- 從排定的時間導入延遲。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。

  按一下齒輪圖示，然後按一下 **[備份選項]** > **[排程]**。請選擇 **[在時間視窗內分配備份開始時間]**，然後指定最大延遲。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。

  注意事項

  在雲端部署中，此選項預設為啟用，且最大延遲設為 30 分鐘。在內部部署中，所有備份預設為完全按排程開始。

- 按一下 **[顯示更多]** 以存取下列選項：
  - **如果電腦關閉，則在電腦啟動時執行遺漏的工作** (預設為停用)
  - **防止在備份期間進入睡眠或休眠模式** (預設為啟用)

    此選項僅對執行 Windows 的電腦有效。
  - **從睡眠或休眠模式中喚醒，開始進行排程的備份** (預設為停用)

此選項僅對執行 Windows 的電腦有效。當電腦關機時，此選項無效，即該選項不會使用 LAN 喚醒功能。

依據事件排程

設定保護計劃排程時，可在排程選擇器中選擇事件類型。事件發生時，備份將立即啟動。

可選擇以下一個事件：

- **自上次備份後的時間**
  這是自上次備份成功完成後 (以相同的保護計劃) 經過的時間。您可指定時間長度。

  注意事項
  由於排程依據的是成功的備份事件，因此如果備份失敗，除非操作員手動執行計劃而且成功完成，否則排程器將不會再次執行工作。

- **當使用者登入系統時**
  預設情況下，任何使用者登入後，將啟動備份。您可將任何使用者變更為特定用戶帳戶。
- **當使用者登出系統時**
  預設情況下，任何使用者登出後，將啟動備份。您可將任何使用者變更為特定用戶帳戶。

  注意事項
  系統關機時，備份不會執行，因為關機不同於登出。

- **在系統啟動時**
- **在系統關閉時**
- **發生 Windows 事件記錄中的事件時**
  您必須指定事件屬性。

下表列出在 Windows、Linux 和 macOS 下可用於不同資料的事件。

要備份的內容	自上次備份後的時間	當使用者登入系統時	當使用者登出系統時	在系統啟動時	在系統關閉時	發生 Windows 事件記錄中的事件時
磁碟/磁碟區或檔案 (實體機器)	Windows、Linux、macOS	Windows	Windows	Windows、Linux、macOS	Windows	Windows
磁碟/磁碟區 (虛擬機器)	Windows、Linux	–	–	–	–	–
ESXi 設定	Windows、Linux	–	–	–	–	–

Microsoft 365 信箱	Windows	–	–	–	–	Windows
Exchange 資料庫和信箱	Windows	–	–	–	–	Windows
SQL 資料庫	Windows	–	–	–	–	Windows

發生 Windows 事件記錄中的事件時

您可設定排程，讓備份在特定 Windows 事件被登錄在**[應用程式]**、**[安全性]** 或 **[系統]**等事件記錄時啟動。

例如，您可能希望設定一個在 Windows 發現硬碟機即將故障時自動執行資料緊急完整備份的保護計劃。

若要瀏覽事件和檢視事件屬性，請使用 **[電腦管理]** 主控台中的 **[事件檢視器]** 管理單元。您必須是 **Administrators** 群組的成員，才能開啟**安全性** 記錄 。

事件屬性

記錄名稱

指定記錄名稱。從清單中選擇一個標準記錄的名稱 (**應用程式**、**安全性**或**系統**)，或輸入一個記錄名稱，例如：**Microsoft Office 工作階段**

事件來源

指定事件來源，這通常指的是導致該事件的程式或系統元件，例如：**磁碟**

含有指定之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，如果您指定字串 **service**，則 **Service Control Manager** 和 **Time-Service** 事件來源都將觸發備份。

事件類型

指定事件類型：**錯誤**、**警告**、**資訊**、**稽核成功**，或**稽核失敗**。

事件識別碼

指定事件編號，這通常用於在同一來源的事件中識別特定類型的事件。

例如，當 Windows 探索到磁碟上的一個區塊損壞時，包含事件來源**磁碟**和事件識別碼 **7** 的**錯誤**事件發生，而當磁碟尚未準備就緒進行存取時，包含事件來源**磁碟**和事件識別碼 **15** 的**錯誤**事件發生。

範例：「損壞區塊」緊急備份

硬碟上突然出現一或多個損壞區塊，通常代表硬碟即將故障。假設您想要建立一個在此類情形發生時立即備份硬碟資料的保護計劃。

當 Windows 在硬碟上檢測到一個損壞區塊時，將在**系統**日誌中記錄帶有事件來源**磁碟**和事件編號**7**的事件；該事件的類型為**錯誤**。

建立計劃時，請在 **[排程]** 區段輸入或選擇以下內容：

- **日誌名稱**：**系統**
- **事件來源**：**磁碟**
- **事件類型**：**錯誤**
- **事件識別碼**：**7**

重要事項
為了確保這種備份在有損壞區塊的狀況下依然能夠完成，您必須使備份略過損壞區塊。若要執行此作業，請在 **[備份選項]** 中，移至 **[錯誤處理]**，然後選擇 **[忽略損壞磁區]** 核取方塊。

開始條件

這些設定讓排程器更具彈性，可讓備份工作在特定條件下執行。如果有多個條件，則必須同時符合所有條件，才能讓備份開始。當備份為手動啟動時，開始條件無效。

若要存取這些設定，請在設定保護計劃的排程時，按一下 **[顯示更多]**。

在未滿足條件(或任何多種條件)的情況下，根據備份開始條件備份選項定義排程行為。處理長時間未符合條件，進而延遲備份的情況有一定風險，您可設定時間間隔，在此時間間隔以後無論條件是否符合，備份都將執行。

下表列出在 Windows、Linux 和 macOS 下可用於不同資料的開始條件。

要備份的內容	磁碟/磁碟區或檔案 (實體機器)	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	–	–	–	–	–
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	–	–	–	–	–
符合時間間隔	Windows、Linux、macOS	Windows、Linux	–	–	–	–

時						
節省電池電力	Windows	–	–	–	–	–
不要在使用計量付費連線時開始	Windows	–	–	–	–	–
不要在連線至下列 Wi-Fi 網路時開始	Windows	–	–	–	–	–
檢查裝置 IP 位址	Windows	–	–	–	–	–

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 21:00 在電腦上執行備份，最好當使用者空閒時執行。如果到 23:00 仍有使用者活動，則強制執行備份。

- 排程：每天，每天執行。啟動時間：**21:00**。
- 條件：**使用者空閒**。
- 備份開始條件：**等到符合條件，務必在 2** 小時後啟動備份。

完成設定後，結果如下：

(1) 如果使用者在 21:00 之前變為空閒，備份將在 21:00 啟動。

(2) 如果使用者在 21:00 至 23:00 之間變為空閒，備份將在使用者變為空閒後立即啟動。

(3) 如果到 23:00 仍有使用者活動，則在 23:00 啟動備份。

備份位置的主機可用

「備份位置的主機可用」的意思是，當您選擇將備份儲存於網路，而內含存檔目的地的電腦成為可用狀態時。

此條件對於網絡資料夾、雲端儲存和儲存節點管理的位置有效。

此條件並不涵蓋位置本身的可用性 - 僅主機的可用性。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

在每個工作日 21:00 將資料備份至網路資料夾。如果此時裝載資料夾的電腦不可用（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：每日，週一至週五執行。啟動時間：**21:00**。
- 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：

(1) 如果已到 21:00，並且主機可用，則立即啟動備份。

(2) 如果已到 21:00，但主機不可用，則備份工作將在下一個工作日開始 (假設屆時主機可用)。

(3) 如果在工作日的 21:00，主機總是不可用，則備份永遠不會開始。

使用者已登出

暫停備份工作的執行，直到所有使用者都從 Windows 登出為止。

範例

每週五 20:00 執行備份，最好在所有使用者登出時。如果在 23:00 有一個使用者仍在登入，則務必執行備份。

- 排程：每週，星期五。啟動時間：**20:00**。
- 條件：**使用者已登出**。
- 備份開始條件：**等到符合條件，務必在 3** 小時後啟動備份。

結果：

(1) 如果所有使用者在 20:00 都已登出，備份工作將在 20:00 啟動。

(2) 如果最後一名使用者在 20:00 至 23:00 之間登出，備份將在該使用者登出後後立即啟動。

(3) 如果到 23:00 仍有使用者登入，則在 23:00 啟動備份。

符合時間間隔時

將備份的啟動時間限制在指定的時段。

範例

一家公司使用同一個網路連接儲存裝置上的不同位置備份使用者資料和伺服器。工作日從上午 8 點開始到下午 5 點結束。使用者資料應在使用者登出後立即備份，但不能早於下午 4:30 。公司伺服器的備份時間是每天晚間 11 點。因此，最好應該在這個時間之前備份使用者的資料，以便釋放網路頻寬。假定備份使用者資料所需時間不超過一小時，則最晚備份開始時間為 22:00。如果在指定的時段內有一個使用者仍登入在系統中，或在任何其他時間登出，則不備份該使用者的資料，亦即略過備份執行。

- 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**，從**下午 04:30:00** 至**晚間 10:00:00**。
- 備份開始條件：**略過排程備份**。

結果：

(1) 如果使用者在下午 04:30:00 和晚間 10:00:00 之間登出，備份工作將在登出後立即啟動。

(2) 如果使用者在任何其他時間登出，將略過此備份。

節省電池電力

裝置 (筆記型電腦或平板電腦) 未連線到電源時，可防止進行備份。視 [備份開始條件] 備份選項的值而定，在裝置連線到電源之後，跳過的備份將會啟動，也可能不會啟動。您可以選取下列選項：

- **不要在使用電池電力時開始**
  僅當裝置連線到電源時，才會開始備份。
- **如果電池電量高於下列設定，可在使用電池電力時開始**
  當裝置連線到電源，或電池電量高於指定值時，即會開始備份。

範例

資料在每個工作日 21:00 時備份。若裝置未連線到電源 (例如，使用者在參加會議)，則您需要跳過備份，以節省電池電力並等到使用者將裝置連線到電源。

- 排程：每日，週一至週五執行。啟動時間：21:00。
- 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：

(1) 如果已到 21:00，且裝置已連線到電源，則將立即開始備份。

(2) 如果已到 21:00，且裝置正在使用電池電力執行，則在裝置連線到電源時立即開始備份。

不要在使用計量付費連線時開始

在裝置透過使用 Windows 中設定為使用計量付費的連線來連線網際網路時，可防止進行備份 (包括對本機磁碟的備份)。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。

防止透過行動熱點進行備份的另一個方法就是，在您啟用**不要在使用計量付費連線時開始**條件時，條件**不要在連線至下列 Wi-Fi 網路時開始**會自動啟用。依預設會指定下列網路名稱：“android”、“phone”、“mobile” 和 “modem”。可以透過按一下 X 符號來刪除此清單中的這些名稱。

範例

資料在每個工作日 21:00 時備份。若裝置透過使用計量付費連線來連線網際網路 (例如，使用者差旅時)，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：每日，週一至週五執行。啟動時間：21:00。
- 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：

(1) 如果已到 21:00，而裝置未透過使用計量付費連線來連線網際網路，則將立即開始備份。

(2) 如果已到 21:00，且裝置已透過使用計量付費連線來連線網際網路，則備份將在下一個工作日開始。

(3) 如果在工作日的 21:00，裝置始終透過使用計量付費連線來連線網際網路，則備份永遠不會開始。

不要在連線至下列 Wi-Fi 網路時開始

在裝置連線至任何指定的無線網路時，可防止進行備份 (包括對本機磁碟的備份)。您可以指定 Wi-Fi 網路名稱，也稱為服務組識別元 (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，若您指定 “phone” 作為網路名稱，備份將不會在裝置連線至以下任何網路時開始：“John's iPhone”、“phone_wifi” 或 “my_PHONE_wifi”。

當裝置透過使用手機熱點連線至網際網路時，此條件有助於防止進行備份。

防止透過行動熱點進行備份的另一個方法就是，在您啟用**不要在使用計量付費連線時開始**條件時，條件**不要在連線至下列 Wi-Fi 網路時開始**會自動啟用。依預設會指定下列網路名稱：“android”、“phone”、“mobile” 和 “modem”。可以透過按一下 X 符號來刪除此清單中的這些名稱。

範例

資料在每個工作日 21:00 時備份。若裝置透過使用行動熱點來連線網際網路 (例如，筆記型電腦在網絡共享模式下進行連線)，則您需要跳過備份，並等待下一個工作日的排程開始。

- 排程：每日，週一至週五執行。啟動時間：21:00。
- 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：

(1) 如果已到 21:00，而電腦未連線至指定網路，則將立即開始備份。

(2) 如果已到 21:00，且電腦已連線至指定網路，則備份將在下一個工作日開始 。

(3) 如果在工作日的 21:00，電腦始終連線至指定網路，則備份永遠不會開始。

檢查裝置 IP 位址

若任何裝置 IP 位址在指定的 IP 位址範圍之內或之外，則可以防止進行備份 (包括對本機磁碟的備份)。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。

若使用者在海外，這一條件很有用，可以避免大量的資料傳輸費用。它還有助於防止透過虛擬私人網路 (VPN) 連線進行備份。

範例

資料在每個工作日 21:00 時備份。若裝置透過使用 VPN 通道連線企業網路 (例如，使用者在家工作)，則您需要跳過備份，等到使用者將裝置帶入辦公室。

- 排程：每日，週一至週五執行。啟動時間：21:00。
- 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：

(1) 若已到 21:00，而電腦 IP 位址未在指定範圍內，則將立即開始備份。

(2) 若已到 21:00，且電腦 IP 位址在指定範圍內，則在裝置取得非 VPN IP 位址之後立即開始備份。

(3) 若在工作日的 21:00，電腦 IP 位址始終在指定範圍內，則備份永遠不會開始。

保留規則

重要事項
本節中所述的部分功能僅適用於內部部署。

1. 按一下**保留時間**。
2. 在**清理**中選取下列其中一項：

- **根據備份時期**(預設值)

  指定保護計劃所建立之備份的保留時間。系統會預設為每個備份集[1]個別指定保留規則。如果您想要在所有備份使用單一規則，請按一下 **[改為所有備份集使用單一規則]**。
- **按照備份數目**

  指定要保留的備份數目上限。
- **按照備份大小總計**

  指定要保留的備份數目大小總計。

  此設定不適用於**一律增量備份 (單一檔案)** 備份配置或備份到 SFTP 伺服器或磁帶裝置上時。
- **永久保留備份**

3. 選擇啟動清理的時間：
   - **備份後** (預設值)

     保留規則將於建立新備份後套用。
   - **備份前**

     保留規則將於建立新備份前套用。

     備份 Microsoft SQL Server 叢集或 Microsoft Exchange Server 叢集時，此設定不可用。

您需要知道的其他事項

- 除非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，否則在所有情況下都會保留保護計劃所建立的最後一個備份。

  警告！
  如果您透過以這種方式套用保留規則來刪除您擁有的唯一備份，則如果備份失敗，您將沒有用於還原資料的備份，因為沒有可用的備份可供使用。

- 在磁帶被複寫之前，系統不會刪除儲存在磁帶上的備份資料。
- 如果根據備份配置和備份格式，各備份存儲為單獨檔案，則僅在所有依賴 (增量和差異備份) 備份的存留期到期時，才可刪除該檔案。因此需要額外的空間來儲存延後刪除的備份。此外，備份時期、備份數據或備份大小可能會超過您所指定的值。

  可透過使用「備份彙總」備份選項變更此行為。
- 保留規則是保護計劃的一部分。一旦保護計劃從電腦撤銷或刪除，或者電腦本身從管理伺服器中刪除，這些規則就不適用於電腦的備份工作。如果您不再需要備份計劃所建立的備份，請加以刪除，如 < 刪除備份 > 中所述。

[1]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]、[每日]、[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]) 選擇的星期幾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。

加密

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。

重要事項
若是遺失或忘記密碼，則無法復原加密的備份。

保護計劃中的加密

若要啟用加密，請在建立保護計劃時指定加密設定。保護計劃套用後，就無法修改加密設定。若要使用不同的加密設定，請建立新的保護計劃。

在保護計劃中指定加密設定

1. 請在保護計劃面板中，啟用 **[加密]** 開關。
2. 指定並確認加密密碼。
3. 選擇下列其中一個加密演算法：
   - **AES 128**–備份將以採用 128 位元金鑰的進階加密標準 (AES) 演算法加密。
   - **AES 192**–備份將以採用 192 位元金鑰的 AES 演算法加密。
   - **AES 256**–備份將以採用 256 位元金鑰的 AES 演算法加密。
4. 按一下 **[確定]**。

以電腦屬性加密

此選項適用於要處理多部機器備份的管理員。如果每部電腦都需要唯一的加密密碼，或是不論保護計劃加密設定為何，均需強制備份加密，請將加密設定個別儲存在每部電腦上。備份將採用 256 位元金鑰的 AES 演算法加密。

在電腦上儲存加密設定會對保護計劃造成以下影響：

- **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。即使在保護計劃設定中停用加密，仍會加密所有備份。

此選項可用於執行 VMware 用代理程式的電腦。不過，若有一個以上的 VMware 用代理程式連結於相同的 vCenter Server，則要小心謹慎。因為負載平衡的緣故，所有代理程式務必使用相同的加密設定。

儲存加密設定後，也可以依以下所述方式變更或重設。

重要事項
如果此電腦上執行的保護計劃已建立備份，變更加密設定將會使此計劃失敗。若要繼續備份，請建立新的計劃。

欲儲存加密設定在電腦上

1. 請以管理員身份 (Windows 系統) 或是 root 使用者身份 (Linux 系統) 登入。
2. 執行下列指令碼：
   - Windows 系統：<安裝路徑>**\PyShell\bin\acropsh.exe -m manage_creds --set-password** <加密密碼>

     <安裝路徑> 在這裡指的是保護代理程式的安裝路徑。其在雲端部署中預設為 **%ProgramFiles%\BackupClient**，在內部部署中為 **%ProgramFiles%\Acronis** 。
   - Linux 系統：**/usr/sbin/acropsh -m manage_creds --set-password** <加密密碼>

欲重設加密設定在電腦上

1. 請以管理員身份 (Windows 系統) 或是 root 使用者身份 (Linux 系統) 登入。
2. 執行下列指令碼：
   - Windows 系統：<安裝路徑>**\PyShell\bin\acropsh.exe -m manage_creds --reset**

     <安裝路徑> 在這裡指的是保護代理程式的安裝路徑。其在雲端部署中預設為 **%ProgramFiles%\BackupClient**，在內部部署中為 **%ProgramFiles%\Acronis** 。
   - Linux 系統：**/usr/sbin/acropsh -m manage_creds --reset**

使用 Cyber Protect 監視器變更加密設定

1. 在 Windows 或 macOS 中以管理員身份登入。
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. 執行下列其中一項操作：
   - 選擇**為此電腦設定特定的密碼**。指定並確認加密密碼。
   - 選擇 **[使用保護計劃中指定的加密設定]**。
6. 按一下 **[確定]**。

加密如何運作

AES 加密演算法以加密區塊鏈結 (CBC) 模式作業，並使用隨機產生的金鑰 (依使用者定義，大小可為 128、192 或 256 位元)。金鑰的大小越大，程式加密備份所需的時間越長，資料的安全性就越高。

然後，程式會以密碼的 SHA-256 雜湊作為金鑰，運用 AES-256 來為加密金鑰加密。密碼本身不儲存在磁碟或備份中的任何位置。密碼雜湊會用於驗證。有了此雙層安全性後，備份資料即可免於受到任何未經授權的存取，但您無法復原遺失的密碼。

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
- 若備份目的地是已啟用重複資料刪除或加密的受管理位置

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。

轉換為虛擬機器

重要事項
本節中所述的部分功能僅適用於內部部署。

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。

轉換方法

- **定期轉換**
  設定定期轉換有兩種方法:
  - **將轉換變成保護計劃的一部分**
    轉換將在每次備份之後執行(若設定為主要位置), 或在每次複寫之後執行(若設定為次要與更多位置)。
  - **建立單獨的轉換計劃**
    此方法可讓您指定單獨的轉換排程。
- **復原至新的虛擬機器**
  此方法可讓您選擇要復原的磁碟, 然後調整每個虛擬磁碟的設定。使用此方法進行單次轉換或偶爾進行轉換, 例如, 要執行實體至虛擬移轉。

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。

下表摘要說明代理程式可以建立的虛擬機器類型：

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
VMware ESXi	+	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–
VMware 工作站	+	+	+	+	–	–
VHDX 檔案	+	+	+	+	–	–
Scale Computing HC3	–	–	–	–	–	+

限制

- Windows 用代理程式、VMware 用代理程式 (Windows) 和 Hyper-V 用代理程式無法轉換儲存在 NFS 上的備份。
- 在單獨轉換計劃中，無法轉換儲存在 NFS 或 SFTP 伺服器上的備份。
- 儲存在 Secure Zone 中的備份只能由執行於相同電腦上的代理程式轉換。
- 備份只能在單獨的轉換計劃中轉換為 Scale Computing HC3 虛擬機器。
- 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。

定期轉換至 ESXi 和 Hyper-V 以及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。

定期轉換會佔用 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。

在第二種情況中，只有在執行虛擬機器時才會消耗資源。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。

在保護計劃中轉換為虛擬機器

您可以從保護計劃中的任何備份或複寫位置，設定轉換到虛擬機器。在每次備份或複寫後執行轉換。

如需有關必要條件和限制的資訊，請參閱「關於轉換，您需要知道的內容」。

若要在保護計劃中設定轉換到虛擬機器

1. 確定要執行轉換的備份位置。
2. 在保護計劃面板上，按一下此位置底下的 **[轉換為 VM]**。
3. 啟用 **[轉換]** 交換器。
4. 在**轉換為**中，選擇目標虛擬機器的類型。您可以選擇下列其中一項：
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **VMware Workstation**
   - **VHDX 檔案**
5. 執行下列其中一項操作：
   - VMware ESXi 和 Hyper-V：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. [選擇性步驟] 按一下 **[將執行轉換的代理程式]**，然後選擇代理程式。

   這可以是執行備份的代理程式 (依預設)，或是安裝於另一部電腦的代理程式。如果為第二種情況，備份必須儲存在共用位置，例如網路資料夾，以便其他電腦可以存取它們。
7. [選擇性] 若是 VMware ESXi 和 Hyper-V，您也可以執行下列步驟：
   - 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 (儲存)。
   - 變更磁碟的佈建模式。預設設定為：**[精簡]** (適用於 VMware ESXi) 和 **[動態延伸]** (適用於 Hyper-V)。
   - 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。
8. 按一下**[完成]**。

定期轉換至 VM 的運作方式

定期轉換的運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，軟體會更新現有的虛擬機器，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。如果此作業成功，就會刪除舊的機器。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已經有*完整備份*，系統會從頭開始重新建立虛擬機器，如本節先前所述。
- 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

為了能夠更新虛擬機器，軟體儲存了一些虛擬機器的中間快照。這些快照命名為 **Backup...** 和 **Replica...**，您應該保留這些名稱。不需要的快照會自動刪除。

最新的 **Replica...** 快照會對應到最近一次轉換的結果。您可以使用此快照，將虛擬機器回復為快照的狀態；例如，如果您使用虛擬機器後，想放棄所做的變更。

其他快照則是供軟體內部使用。

複寫

重要事項
本節中所述的部分功能僅適用於內部部署。

本節描述當作保護計劃一部分的備份複寫。如需建立單獨複寫計劃的資訊，請參閱 < 脫離主機資料處理 > 。

如果您啟用備份複寫，備份複寫建立後系統會立即將每個備份複製到其他位置。如果之前的備份並未複寫 (例如由於網路連線中斷)，軟體也會複寫上次成功複寫後出現的所有備份。

複寫的備份不會依存原始位置中剩下的備份，反之亦然。您可以在不存取其他位置的情況下，從任何備份復原資料。

使用範例

- **可靠的災難復原**

  使用現地 (適合立即復原) 與異地 (可保護備份免受本機存放裝置故障或自然災難影響) 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**

  為避免過度使用昂貴的存放裝置空間，您可根據保留規則刪除高速存放裝置中較舊的備份。

支援的位置

您可以*從*以下任何位置複寫備份：

- 本機資料夾
- 網路資料夾
- Secure Zone
- SFTP 伺服器
- 由儲存節點管理的位置

您可以將備份複寫*到*以下任何位置：

- 本機資料夾
- 網路資料夾
- 雲端儲存
- SFTP 伺服器
- 由儲存節點管理的位置
- 磁帶裝置

啟用備份的複寫。

1. 在保護計劃面板上，按一下 **[新增位置]**。

   [新增位置] 控制項僅在支援*從*上次選擇的備份或複寫位置進行複寫時才能使用。
2. 指定要將備份複寫到哪個位置。
3. [選擇性步驟]在 **[保留時間]** 中，如 < 保留規則 > 所述為選定的位置變更保留規則。
4. [選擇性步驟] 在 **[轉換為 VM]** 中，指定轉換為虛擬機器的設定，如 [轉換為虛擬機器]中所述。
5. [選擇性] 按一下齒輪圖示 > **[效能和備份視窗]**，然後設定所選位置的備份視窗，如「效能和備份視窗」中所述。這些設定將會定義複寫效能。
6. [選擇性步驟] 對於要複寫備份的所有位置，請重複步驟 1-5。最多支援五個連續位置，包括主要位置。

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，排程的備份將不會開始。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 301 頁)。

具有進階授權之使用者的考量

提示

您可以透過建立單獨的複寫計劃，從雲端儲存設定備份的複寫。如需更多資訊，請參閱 < 脫離主機資料處理 > 。

限制

- 不支援將備份從儲存節點管理的位置複寫到本機資料夾。本機資料夾是指建立備份的代理程式所在之電腦上的資料夾。
- 對於使用 **12 版**備份格式的備份，不支援將備份複寫至已啟用重複資料刪除的受管理位置。

作業會由哪一部電腦執行？

從任何位置複寫備份的作業是由建立備份的代理程式起始，並由以下項執行：

- 如果位置*不是*由儲存節點管理，則作業由該代理程式執行。
- 如果位置受管理，則由對應的儲存節點執行。然而，將備份從受管理位置複寫至雲端儲存的作業，則是由建立備份的代理程式執行。

如以上說明所述，唯有當裝有代理程式的電腦已開機時，作業才會執行。

在受管理位置之間複寫備份

將備份從一個受管理位置複寫到另一個受管理位置的作業，是由儲存節點執行。

如果為目標位置 (可能位於不同的儲存節點上) 啟用重複資料刪除，則來源儲存節點只會傳送未在目標儲藏庫中呈現的那些資料區塊。換言之，儲存節點會與代理程式一樣執行來源端重複資料刪除。當您在四處分散的儲存節點之間複寫資料時，如此可以節省網路流量。

手動啟動備份

1. 選擇至少已套用一項保護計劃的電腦。
2. 按一下 **[備份]**。
3. 如果已套用一個以上的保護計劃，請選擇保護計劃。
4. 執行下列其中一項操作：

- 按一下 **[立即執行]**。系統將建立增量備份。
- 如果備份配置包括數個備份方法，您可以選擇要使用的方法。按一下 **[立即執行]** 按鈕上的箭頭，然後選擇 **[完整]**、**[增量]** 或 **[差異]**。

保護計劃建立的第一個備份一律為完整備份。

備份進度會顯示在電腦的**[狀態]**欄位中。

備份選項

重要事項
本節中所述的部分功能僅適用於內部部署。

若要修改備份選項，按一下保護計劃名稱旁的齒輪圖示，然後按一下 **[備份選項]**。

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	Scale Computing	Windows
警示	+	+	+	+	+	+	+	+	+	+
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	+	+	+	+	+	+	+	+	+	+
電子郵件通知	+	+	+	+	+	+	+	+	+	+
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	+	+	+	-	-	-	-	-	-	-
檔案篩選器	+	+	+	+	+	+	+	+	+	-
檔案層級備份快照	-	-	-	+	+	+	-	-	-	-
記錄截斷	-	-	-	-	-	-	+	+	-	僅 SQL
LVM 快照	-	+	-	-	-	-	-	-	-	-
掛載點	-	-	-	+	-	-	-	-	-	-
多重分割檔快照	+	+	-	+	+	-	-	-	-	-
效能和備份視窗	+	+	+	+	+	+	+	+	+	+
實體資料運送	+	+	+	+	+	+	+	+	+	-
事前/事後命令	+	+	+	+	+	+	+	+	+	+
資料擷取前/後命令	+	+	+	+	+	+	+	-	-	+
SAN 硬體	-	-	-	-	-	-	+	-	-	-

快照										
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	+	+	+	+	+	+	+	+	+	+
磁帶管理	+	+	+	+	+	+	+	+	+	+
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。

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。

如果以下任何一下為真,則此選項*將不*生效:

- 備份目的地為磁帶裝置或雲端儲存。
- 備份配置設定為**一律增量備份(單一檔案)**。
- 備份格式設定為**12 版**。

儲存在磁帶上的備份無法合併。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。儲存在磁帶上的備份只有在覆寫或刪除磁帶時，才會從 GUI 消失。

備份檔案名稱

此選項會定義保護計劃所建立之備份檔案的名稱。

當瀏覽備份位置時，可以在檔案管理員中看到這些名稱。

什麼是備份檔案?

每個保護計劃都會在備份位置上建立一或多個檔案，此依備份配置，以及將使用哪種備份格式而定。以下表格會列出可依機器或信箱建立的檔案的清單。

	一律增量備份 (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 (傳統格式)
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)	

所有檔案都有相同的名稱，可包含或不含時間戳記或序號。建立或編輯保護計劃時，您可以定義此名稱 (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。

當您變更備份檔案名稱後，下一個備份將是完整備份，除非您指定的是相同機器上的現有備份的檔案名稱。如果是後者，則將根據保護計劃排程建立一個完整、增量或差異備份。

請注意，您可以設定讓檔案管理員無法瀏覽位置的備份檔案名稱(例如，雲端儲存或磁帶裝置) 。如果您想要在 **[備份儲存]** 索引標籤上看到自訂名稱，就可以使用這種方法。

我可以在哪裡看到備份檔案名稱?

選擇 **[備份儲存]** 索引標籤，然後選擇備份的群組。

- 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。

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**)。

預設備份檔案名稱

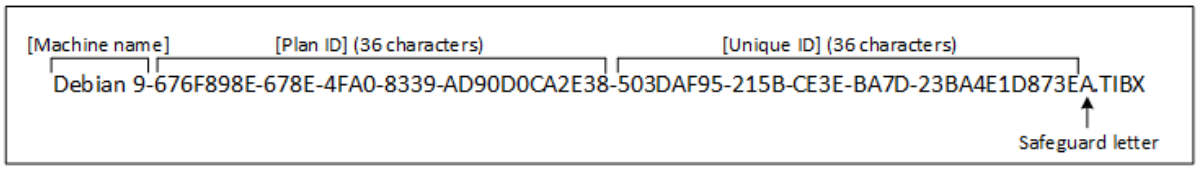
欲設備份檔案名稱為 `[Machine Name]-[Plan ID]-[Unique ID]A`。

用於信箱備份的預設備份檔案名稱為 `[Mailbox ID]_mailbox_[Plan ID]A`。

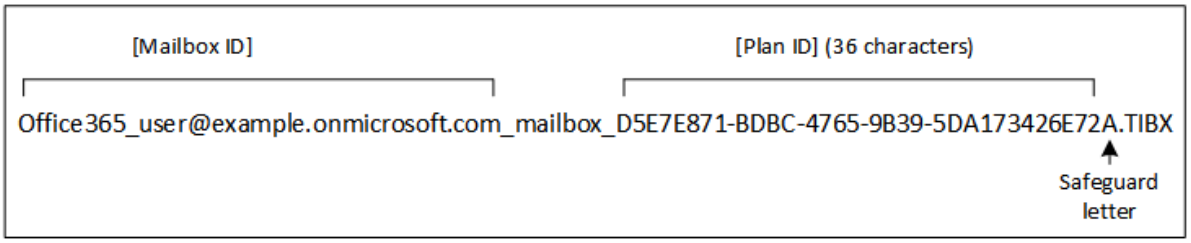
名稱包含下列變數：

- `[Machine Name]` 對於所有類型的備份資料 (Microsoft 365 信箱除外)，此變數會取代為電腦的名稱 (與 Cyber Protect Web 主控台中顯示的名稱相同)。對於 Microsoft 365 信箱，它取代為信箱使用者的主體名稱 (UPN)。
- `[Plan ID]` 此變數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]` 此變數取代為所選取電腦或信箱的唯一識別碼。重新命名電腦或變更信箱 UPN 時，此值不會變更。
- `[Mailbox ID]` 此變數取代為信箱 UPN。
- `"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。



下圖顯示信箱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
...
```

對於具有 **[一律增量 (單一檔案)]** 備份配置的 11 版格式：

```
MyBackup.xml
MyBackup.tib
```

對於具有其他備份配置的 11 版格式：

```
MyBackup.xml
MyBackup_2016_9_13_14_49_20_403F.tib
MyBackup_2016_9_14_14_43_00_221F.tib
MyBackup_2016_9_15_14_45_56_300F.tib
...
```

使用變數

除了依預設使用的變數之外，您還可以使用 [Plan name] 變數，該變數會取代為保護計劃的名稱。

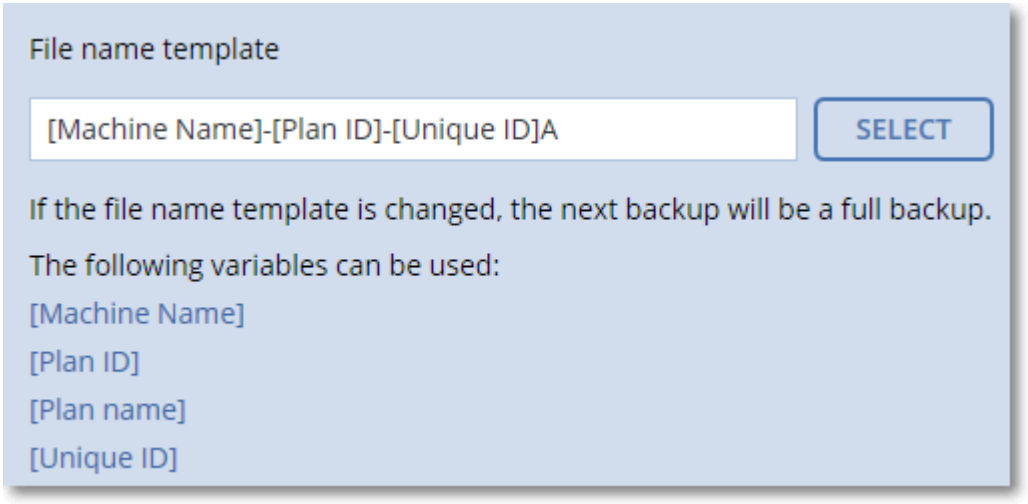
如果選擇多個電腦或信箱進行備份，則備份檔案名稱必須包含 [Machine Name]、[Mailbox ID] 或 [Unique ID] 變數。

備份檔案名稱與簡化檔案命名

使用純文字和/或變數，您可以建構與舊版 Acronis Cyber Protect 中相同的檔案名稱。然而，無法重新建構簡化的檔案名稱 — 在 12 版中，除非使用單一檔案格式，否則檔案名稱具有時間戳記。

使用範例

- **檢視使用者易記的檔案名稱**
  您想要在使用檔案管理員瀏覽備份位置時輕鬆識別備份。
- **繼續現有備份順序**
  讓我們假設保護計劃套用至單一電腦，而且您必須從 Cyber Protect Web 主控台中移除此電腦，或者必須解除安裝代理程式及其組態設定。重新新增電腦或者重新安裝代理程式之後，您可以強制保護計劃繼續備份到相同的備份及備份順序。方法是，在保護計劃的備份選項中，按一下 **[備份檔案名稱]**，然後按一下 **[選擇]** 以選擇想要的備份。
  [瀏覽] 按鈕會將備份顯示在保護計劃面板的 **[備份目標位置]** 區段中選擇的位置。它不能瀏覽此位置外部的內容。



- **從先前的產品版本升級**
  如果在升級期間未自動移轉保護計劃，請重新建立該計劃，並將其指向舊的備份檔案。如果僅選擇一部電腦以進行備份，請按一下 **[瀏覽]**，然後選擇必要的備份。如果選擇多部電腦以進行備份，請使用變數重新建立舊的備份檔案名稱。

注意事項
[選擇] 按鈕僅適用於針對單一裝置建立並套用到單一裝置的保護計劃。

備份格式

此選項會定義保護計劃所建立之備份的格式。其僅適用於使用 11 版舊版備份格式的保護計劃。在此情況下，您可以將其變更為 12 版新格式。在此變更之後，此選項會變成無法存取。

此選項對信箱備份無效。信箱備份一律使用新格式。

預設為：**自動選擇**。

您可以選擇下列其中一項：

- **自動選擇**
  除非保護計劃將備份附加至舊版產品所建立的備份，否則將使用 12 版。
- **12 版**
  在多數情況下，建議使用新格式進行快速備份和復原。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。
  使用此格式，保留規則 **[按照備份大小總計]** 無效。
- **11 版**
  為回溯相容性而保留的舊版格式。其可讓您將備份附加至舊版產品所建立的備份。
  此外，如果您希望完整備份、增量備份和差異備份是不同的檔案，請使用此格式 (搭配 **[一律增量 (單一檔案)]** 之外的任何備份配置)。
  如果備份目的地 (或者複寫目的地) 是已啟用重複資料刪除的受管理位置，或者已啟用加密的受管理位置，則會自動選擇此格式。如果您將該格式變更為 **12 版**，則備份將失敗。

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。

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。您可以使用 [備份檔案名稱] 項來定義檔案名稱。以下表格會列出可依機器或信箱建立的檔案的清單。

	一律增量備份 (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 (傳統格式)
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)	

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。
- 如果備份目的地 (或者複寫目的地) 是已啟用重複資料刪除的受管理位置，則備份將會失敗。

存檔內重複資料刪除

12 版格式支援存檔內重複資料刪除。

存檔內重複資料刪除使用用戶端重複資料刪除，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。

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，經由保護計劃建立的每個備份都會在建立後立即進行驗證。此作業是由保護代理程式所執行。

預設為：**[已停用]**。

驗證作業會計算可以從備份復原之各資料區塊的檢查碼，唯一的例外是驗證位於雲端儲存中檔案層級的備份。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。

驗證作業是個非常耗時的程序，即使是驗證檔案不大的增量或差異備份也一樣。這是因為該作業不只會驗證備份中實際包含的資料，也會驗證選擇備份時可復原的所有資料。這需要存取先前建立的備份。

雖然驗證成功表示很可能復原成功，但它並未檢查會影響復原程序的所有因素。如果要備份作業系統，我們建議您測試在可開機媒體下復原至備用硬碟，或在 ESXi 或 Hyper-V 環境下從備份執行虛擬機器。

變更區塊追蹤 (CBT)

此選項適用於虛擬機器與執行 Windows 之實體機器的磁碟層級備份。此選項也對 Microsoft SQL Server 資料庫和 Microsoft Exchange Server 資料庫的備份有效。

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

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

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]**。

較高等級的壓縮層級，表示備份程序可能會花較長時間，但最後的備份檔案佔用的空間較少。目前，[高] 和 [最大] 層級的運作方式類似。

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。

電子郵件通知

此選項可讓您設定在備份期間發生的事件的電子郵件通知。

此選項僅可用於內部部署。在雲端部署中，當建立帳戶時，每個帳戶會設定為預設設定。

預設為：**使用系統設定。**

您可以使用系統設定，或者以專屬於此計劃的自訂值覆寫它們。系統設定的設定方式如在「電子郵件通知」中所述。

重要事項
變更系統設定時，使用系統設定的所有保護計劃都將受到影響。

啟用此選項之前，請確保已進行**電子郵件伺服器**設定。

若要為保護計劃自訂電子郵件通知

1. 選擇 **[自訂此保護計劃的設定]**。
2. 在**[收件人電子郵件地址]**欄位中，輸入目的地電子郵件。您可以輸入多組地址，並以分號隔開各組地址。
3. [選擇性步驟] 在**[主旨]**，變更電子郵件通知主旨。
   您可以使用以下變數：
   - `[Alert]` - 警示摘要。
   - `[Device]` - 裝置名稱。
   - `[Plan]` - 產生該警示的計劃的名稱。
   - `[ManagementServer]` - 安裝管理伺服器的電腦的主機名稱。
   - `[Unit]` - 電腦所屬的單位的名稱。

   預設主旨是 `[Alert]` **裝置：**`[Device]` **計劃：**`[Plan]`
4. 選擇您想要接收通知的事件的核取方塊。您可以從在備份期間發生的所有警示的清單中選擇，此清單依嚴重性分組。

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: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。

例如，若網路上的備份目的地不可用或無法存取，此程式會每隔 30 秒嘗試存取目的地一次，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。

雲端儲存

如果已選取雲端儲存作為備份目的地，此選項值會自動設為 **[已啟用]**。**嘗試次數:300**。**嘗試間隔：30 秒。**

在此情況下，實際的嘗試次數是無限的，但是備份失敗之前的逾時時間的計算方式如下：(300 秒 + **嘗試間隔**) * (**嘗試次數** + 1)。

範例：

- 使用預設值，備份將在 (300 秒 + 30 秒) * (300 + 1) = 99330 秒，亦即 ~27.6 小時後失敗。
- 如果您將 **[嘗試次數]** 設定為 1 且 **[嘗試間隔]** 設定為 1 秒，則備份將在 (300 秒 + 1 秒) * (1 + 1) = 602 秒，亦即 ~10 分鐘後失敗。

如果計算後的逾時時間超過 30 分鐘，而且資料傳輸尚未開始，則實際的逾時時間會設定為 30 分鐘。

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。

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

透過使用檔案篩選器，您可以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，否則進行磁碟層級或檔案層級備份時，都可以使用檔案篩選器。

在無代理程式模式下，套用到 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) 時，檔案篩選器不適用。

啟用檔案篩選器

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. 選取 **[檔案篩選器]**。
4. 使用下面敘述的任一選項。

包含或排除符合特定條件的檔案

反向方式中可選擇兩個選項。

- **僅備份符合下列條件的檔案**
  範例：若您選取備份整台電腦，並於篩選條件中指定 **C:\File.exe**，則只會備份這個檔案。

  注意事項
  如果在 **[備份格式]** 中選擇 **[11 版]**，且備份目的地「不是」雲端儲存空間，則此篩選不適用於檔案層級備份。

- **不要備份符合以下條件的檔案**
  範例：若您選取備份整部機器，並於篩選條件中指定 **C:\File.exe**，則只會略過這個檔案。

您可以同時使用兩個選項，但較晚選取的選項會覆寫先前的選項，亦即，若您在兩個欄位中都指定了 **C:\File.exe**，那麼在備份期間就會略過這個檔案。

準則

- **完整路徑**
  指定檔案或資料夾的完整路徑，並以磁碟機代號 (備份 Windows 時) 或根目錄 (備份 Linux 或 Mac OS 時) 開頭。
  在 Windows 和 Linux/Mac OS 中，都可以在檔案或資料夾路徑中使用正斜線 (例如 **C:/Temp/File.tmp**)。在 Windows 中，您也可以使用傳統反斜線 (例如 **C:\Temp\File.tmp**)。

重要事項

如果在磁碟層級備份過程中，未正確偵測到備份電腦的作業系統，則完整路徑檔案篩選器將無法運作。針對排除篩選器，將會顯示警告。如果有包含篩選器，則備份將會失敗。

完整路徑篩選器包含磁碟機代號 (Windows) 或根目錄 (Linux 與 macOS)。例如，檔案完整路徑可能是 **C:\Temp\File.tmp**。包含磁碟機代號或根目錄的篩選器，例如 **C:\Temp\File.tmp** 或 **C:\Temp***，將會導致警告或失敗。

不包含磁碟機代號或根目錄的篩選器 (例如 **Temp*** 或 **Temp\File.tmp**) 或是以星號為開頭的篩選器 (例如 ***C:**) 將不會導致警告或失敗。不過，如果在磁碟層級備份過程中，未正確偵測到備份電腦的作業系統，則這些篩選器也會無法運作。

- **名稱**

  指定檔案或資料夾的名稱，例如 **Document.txt**，如此即可選取所有具備該名稱的檔案與資料夾。

條件不區分大小寫。例如，指定 **C:\Temp**，您會同時選取 **C:\TEMP**、**C:\temp** 等等，以此類推。

您可在準則中使用一或多個萬用字元 (*、** 和 ?)。完整路徑及檔案或資料夾名稱均可使用這些字元。

星號 (*) 會代替檔案名稱中的零個或更多個字元。例如，準則 **Doc*.txt** 符合 **Doc.txt** 和 **Document.txt** 等檔案

[僅適用於 **12 版**格式的備份] 雙星號 (**) 會代替檔案名稱及路徑中的零個或更多個字元 (包含斜線字元)。例如，準則 ****/Docs/**.txt** 符合所有 **Docs** 資料夾下的所有子資料夾內的全部 txt 檔案。

問號 (?)會代替檔案名稱中的一個字元。例如，準則 **Doc?.txt** 符合 **Doc1.txt** 和 **Docs.txt** 等檔案，但不符合檔案 **Doc.txt** 或 **Doc11.txt**

排除隱藏的檔案和資料夾

選擇此核取方塊可略過具有**隱藏**屬性 (適用於 Windows 支援的檔案系統) 或以英文句點 (.)開頭 (適用於 Linux 檔案系統，例如 Ext2 和 Ext3) 的檔案和資料夾。如果資料夾為 [隱藏]，則其所有內容 (包括未隱藏的檔案) 都將排除。

排除系統檔案和資料夾

這個選項僅適用於受 Windows 支援的檔案系統。選擇此核取方塊可略過具有**系統**屬性的檔案和資料夾。如果資料夾具有**系統**屬性，則其所有內容 (包括不具備**系統**屬性的檔案) 都將排除。

注意事項

您可以在檔案/資料夾內容中檢視檔案或資料夾的屬性，或使用 attrib 命令檢視。如需更多資訊，請參閱 Windows 的「說明及支援中心」。

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以在電腦上進行惡意活動。可能需要調查的另一種情況是,透過不同的程式竊取或變更電腦上的資料。這類活動可能需要進行調查,但只有在您在要調查的電腦上保留數位證據時才可行。遺憾的是,證據 (檔案、痕跡等) 可能會遭到刪除,或者電腦可能會變得無法使用。

稱為**鑑識資料**的備份選項可讓您收集能夠用於鑑識調查的數位證據。下列項目可以當作數位證據使用:未使用磁碟空間的快照、記憶體傾印,以及執行中處理程序的快照。**[鑑識資料]** 功能僅適用於整部電腦備份。

[鑑識資料] 選項目前僅適用於含下列作業系統版本的 Windows 電腦:

- Windows 8.1、Windows 10
- Windows Server 2012 R2 – Windows Server 2019

注意事項
• 含 [備份] 模組的保護計劃套用至電腦之後,就無法修改鑑識資料設定。若要使用不同的鑑識資料設定,請建立一個新的保護計劃。
• 對於透過 VPN 連線到網路,且無法直接存取網際網路的電腦,不支援含鑑識資料集合的備份。

支援用於含鑑識資料之備份的位置為:

- 雲端儲存
- 本機資料夾

注意事項
1.只有透過 USB 連線的外接式硬碟才支援本機資料夾。
2.不支援本機動態磁碟作為鑑識備份的位置。

- 網路資料夾

系統會自動公證含鑑識資料的備份。鑑識備份將允許調查人員分析通常不包括在定期磁碟備份中的磁碟區域。

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 Web 主控台中，移至 **[裝置]** > **[所有裝置]**。或者，您可以從 **[計劃]** 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 **[儀表板]** > **[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 Web 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

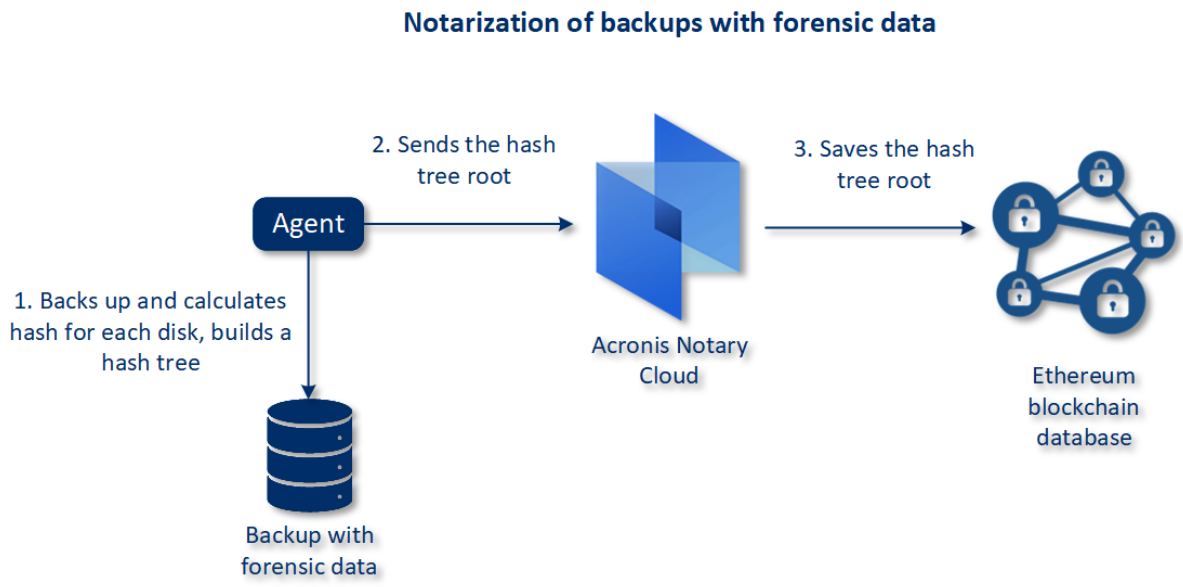
公證可讓您證明含鑑識資料的磁碟在備份後即是真實且未變更的。

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 Protect 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。其位於：`C:\Program Files\Acronis\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\Defa
  ult\<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
```

```
Output template:
```

```
GUID   Date   Date timestamp
----   ------ --------------
<guid> <date> <timestamp>
```

<guid> – 備份 GUID。

<date> – 備份的建立日期。其格式為：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   Date   Date timestamp
----   ------ --------------
516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865
516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925
```

list content

列出復原點中的內容。

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:

```
Disk     Size   Notarization status
-------- ------ --------------------
<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:

```
Disk     Size   Notary status
-------- ------ --------------
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-256 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 Web 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 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 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=密碼	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 Date Date timestamp`
	`---- ------ --------------`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`
	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。備份更快速，且不需要磁碟區群組上的未配置空間。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。

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。

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]**。
- 如果未選擇任何電腦 (如果您從 **[計劃]** > **[備份]** 頁面開始建立保護計劃，就會是這個情況)：**[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

單鍵復原可讓使用者自動復原其電腦的最新磁碟備份。這可以是整部電腦的備份，或此電腦上特定磁碟或磁碟區的備份。

系統管理員啟用此功能後，就可以在使用者的電腦上，與 Startup Recovery Manager 一起存取該功能。系統管理員僅能透過命令列界面執行此作業。若要深入瞭解如何啟用 Startup Recovery Manager 以及單鍵復原，請參閱命令列參考。

單鍵復原支援下列備份儲存空間：

1. Secure Zone
2. 網路儲存區
3. 雲端儲存

如果無法使用特定類型的儲存空間或其中沒有磁碟備份，則系統會提示使用者使用下一種類型的儲存空間。

如果在儲存空間中有多個包含磁碟備份的備份集 (亦稱為*存檔*) 可用，則單鍵復原會選擇上次更新的備份集。使用者無法選擇不同的備份集。

單鍵復原支援下列作業：

- 從最新的備份自動復原
- 從自動選擇的備份集中的特定備份 (亦稱為*復原點*) 復原

使用單鍵復原來復原電腦

必要條件

- 系統管理員已經在所選電腦上啟用單鍵復原。
- 所選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。
3. 選擇所需的單鍵復原選項：
   - 若要自動復原最新的備份，請按下鍵盤上的 1。
   - 若要復原上次更新的備份集中的其他備份，請按下鍵盤上的 2。
     - 若要選擇所需的備份 (亦稱為*復原點*)，請按一下鍵盤上的個別數字。

圖形化使用者介面隨即啟動，然後消失。復原程序會繼續進行，而不需要該介面。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。

您可以分別針對保護計劃中指定的每個位置，設定此選項。若要為複寫位置設定此選項，按一下位置名稱旁的齒輪圖示，然後按一下 **[效能和備份視窗]**。

此選項僅對備份和備份複寫程序有效。保護計劃 (驗證、轉換至虛擬機器) 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。**

啟用此選項時，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。

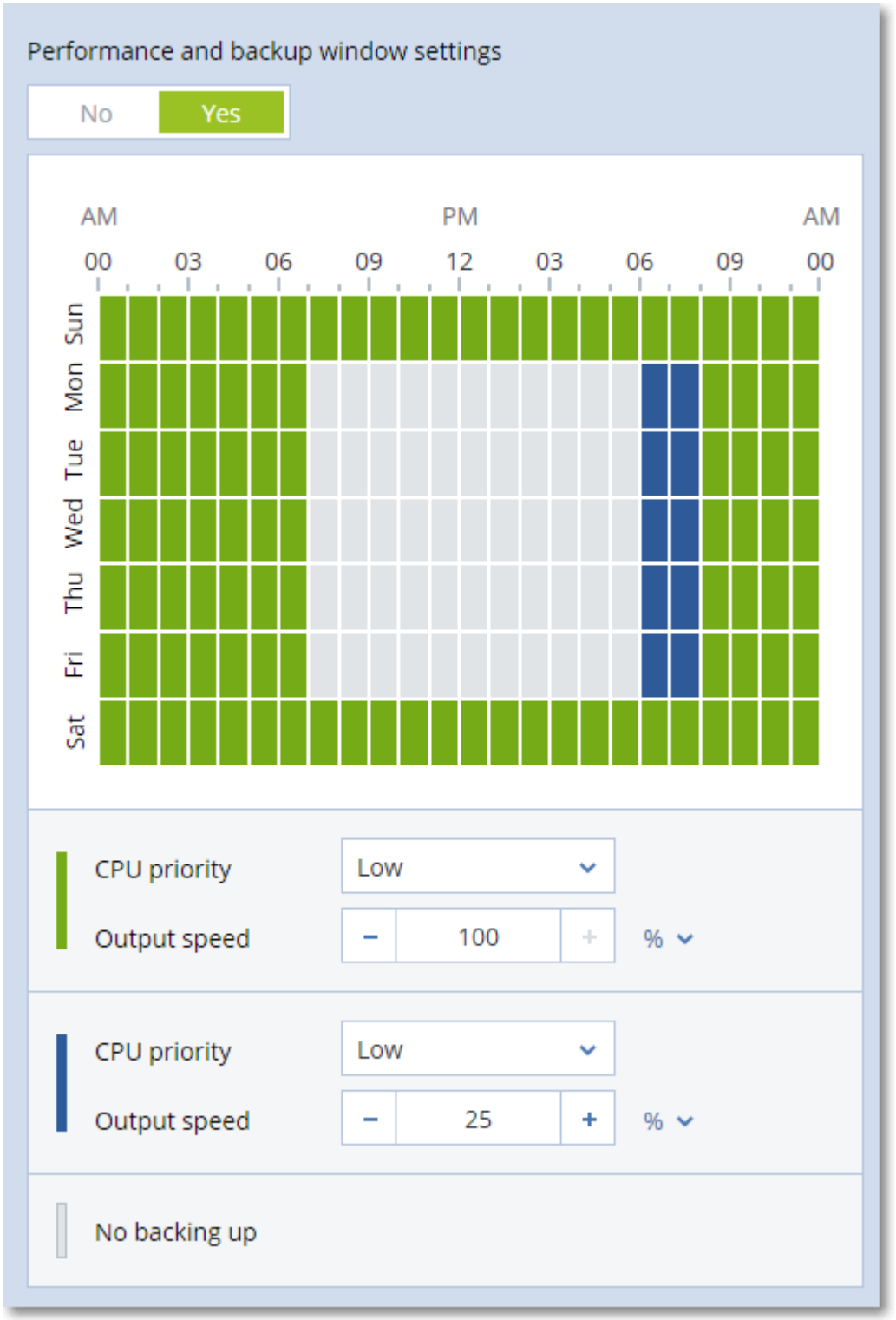
即使排程備份遭到阻止，仍然可以手動開始備份。允許備份時，將使用最近一小時的效能參數。

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：

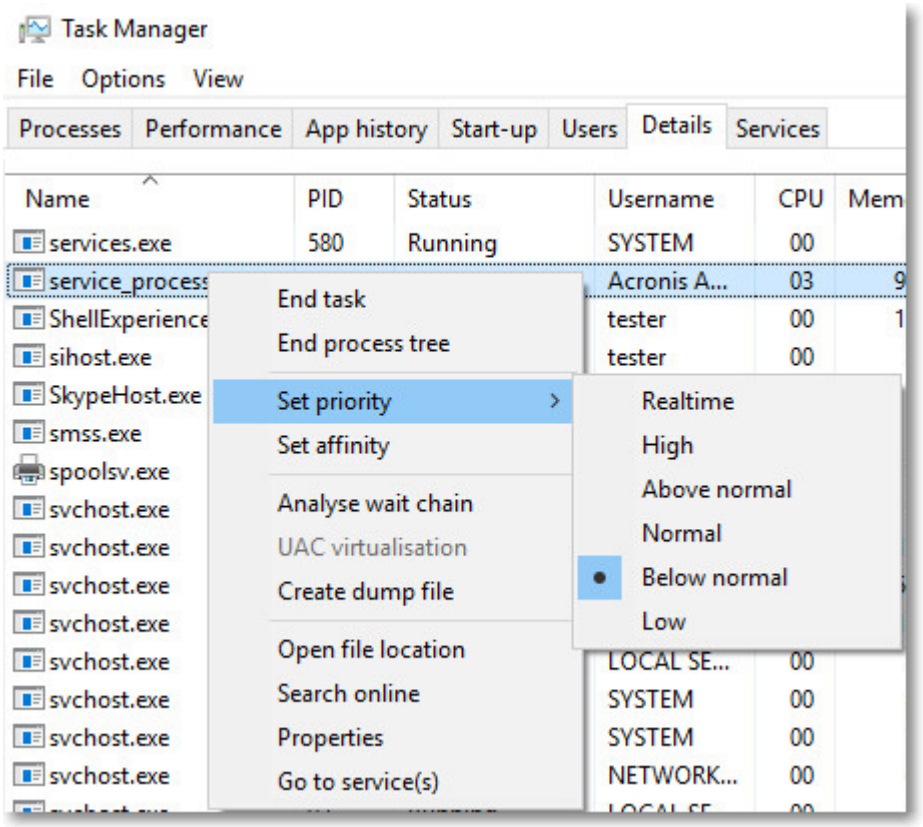
低 - 在 Windows 中，會對應至 **[低於一般]**。

一般 - 在 Windows 中，會對應至 **[一般]**。

高 - 在 Windows 中，會對應至 **[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 OS X 內備份程序的優先度等級 (**service_process**)。



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

如果備份目的地為雲端儲存，且備份格式設定為 **12 版**，則此選項有效。

此選項適用於 Windows 用代理程式、Linux 用代理程式、Mac 用代理程式、VMware 用代理程式，以及 Hyper-V 用代理程式所建立的磁碟層級備份和檔案備份。不支援在可開機媒體底下建立的備份。

此選項可決定保護計劃所建立的第一個完整備份是否將使用「實體資料運送」服務，傳送至硬碟機上的雲端儲存。後續的增量備份可以透過網路執行。

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 介面僅適用於內部部署中的組織系統管理員和雲端部署中的系統管理員。

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. 建立新的保護計劃。在此計劃中，啟用 **[實體資料運送]** 備份選項。

   您可以直接備份到磁碟機，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。

   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。

2. 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，請執行下列其中一項操作：
   - 在內部部署中：登入您的 Acronis 帳戶，然後按一下 **[實體資料運送]** 底下的 **[轉至追蹤主控台]**。
   - 在雲端部署中：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]**。
3. 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。

4. 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。

程式在執行備份後命令*之後*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。

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

此選項可讓您定義擷取資料 (即取得資料快照) 之前和之後要自動執行的命令。資料擷取將於備份程序一開始的時候執行。

以下配置說明資料擷取事前/事後命令的執行時間。

	<---------- 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		備份事後命令

如果 [磁碟區陰影複製服務] 選項已啟用，則命令執行與 Microsoft VSS 動作的順序如下所示：

[資料擷取前] 命令 -> VSS 暫停 -> 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。

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。

SAN 硬體快照

此選項對於 VMware ESXi 虛擬機器的備份有效。

預設為：**[已停用]**。

此選項決定在執行備份時是否使用 SAN 快照。

如果停用此選項，將會從 VMware 快照讀取虛擬磁碟內容。快照將保存用於整個備份期間。

如果啟用此選項，將從 SAN 快照讀取虛擬磁碟內容。系統將會建立並短暫保留 VMware 快照，以便將虛擬磁碟置於一致的狀態。如果無法從 SAN 快照讀取，備份將會失敗。

啟用此選項前，請檢查和執行列於「使用 SAN 硬體快照」中的要求。

排程

此選項會決定備份應按排程時間開始或稍有延誤，以及同時要備份的虛擬機器數目。

預設為：

- 內部部署：**完全按排程開始所有備份。**
- 雲端部署：**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**

  只有當保護計劃要套用至多部虛擬機器時，此選項才可使用。此選項會定義代理程式在執行特定保護計劃時可同時備份的虛擬機器數量。

  如果代理程式根據保護計劃，必須同時開始備份多部虛擬機器，代理程式將會選擇兩部電腦。(代理程式會嘗試比對儲存在不同存放區的虛擬機器，以最佳化備份效能。)當兩項備份作業中的任何一項完成時，代理程式會選擇第三部虛擬機器，以此類推。

  您可以變更代理程式同時備份的虛擬機器數目。最大值是 10。不過，如果代理程式執行多個時間重疊的保護計劃，則會將其選項中指定的數目相加。無論有多少保護計劃正在執行，您都可以限制代理程式可以同時備份的虛擬機器總數。

  實體機器的備份會完全按照排程時間開始進行。

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

此選項可用於**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，每日增量備份 (GFS)** 和**自訂**備份配置。

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。

預設為：**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。

磁帶管理

這些選項在備份目的地為磁帶裝置時有效。

啟用從儲存在磁帶上的磁碟備份復原檔案

預設為：**[已停用]**。

如果選擇了此核取方塊，每次備份時，軟體都會在磁帶裝置連接的電腦的硬碟上，建立補充檔案。只要這些補充檔案完整無缺，就能從磁碟備份復原檔案。當儲存相應備份的磁帶被清除、移除或覆寫時，自動刪除檔案。

補充檔案的位置如下：

- 在 Windows XP 和 Server 2003 中：**%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation**。
- 在 Windows 7 及更新版本的 Windows 中：**%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation**。
- 在 Linux 中：**/var/lib/Acronis/BackupAndRecovery/TapeLocation**。

這些補充檔案佔據的空間，視相應備份中的檔案數量而定。一個包含約 20,000 個檔案的完整磁碟備份 (典型的工作站磁碟備份)，補充檔案佔據約 150 MB 的空間。而一個包含 250,000 個檔案的伺

服器完整備份，可能產生約 700 MB 的補充檔案。因此，如果您確定不需要復原個別檔案，可以將這個核取方塊保留為清除狀態，節省磁碟空間。

如果備份期間沒有建立補充檔案，或補充檔案已被刪除，您仍然可以重新掃描儲存備份的磁帶來建立補充檔案。

每次成功備份每部電腦之後，將磁帶移回插槽

預設為：**[啟用]**。

如果您停用此選項，磁帶在磁帶作業完成後將留在磁碟機中。否則，軟體會將磁帶移回至作業前所處的插槽中。如果根據保護計劃，備份還有後續作業 (例如，備份驗證或複寫至其他位置)，磁帶將會在這些作業完成後移回至插槽中。

如果同時啟用此選項和**每部電腦備份成功後退出磁帶**選項，磁帶將會退出。

每次成功備份每部電腦之後，退出磁帶

預設為：**[已停用]**。

此核取方塊為選取狀態時，軟體會在每台電腦成功備份後退出磁帶。如果根據保護計劃，備份還有後續作業 (例如，備份驗證或複寫至其他位置)，磁帶將會在這些作業完成後退出。

建立完整備份時覆寫獨立磁帶機中的磁帶

預設為：**[已停用]**。

此選項僅適用於獨立磁帶機。此選項為啟用狀態時，每次建立完整備份時都會覆寫插入磁帶機的磁帶。

使用下列磁帶裝置和磁碟機

此選項可讓您指定保護計劃要使用的磁帶裝置和磁帶機。

磁帶集區包含連接至電腦之所有磁帶裝置的磁帶 (不論是儲存節點或安裝保護代理程式所在的電腦，或者兩者)。當您選擇磁帶集區當做備份位置時，您便直接選擇的磁帶裝置所連接的電腦。根據預設，可以透過連接到該電腦的任何磁帶裝置上的任何磁帶機，將備份寫入磁帶上。如果缺少部分裝置或磁碟機或無法運作，保護計劃將會使用可用的部分。

您可以按一下 **[僅限選取的裝置和磁碟機]**，然後從清單選擇磁帶裝置和磁帶機。選擇整台裝置，即選擇其所有磁帶機。這表示保護計劃可使用其中的任何磁碟機。如果所選裝置或磁帶機遺失或未運作中，而且也未選擇其他裝置，則備份會失敗。

藉著使用此選項，您可以控制由多個代理程式執行的備份，備份到具有多磁帶機的大型磁帶庫。例如，如果多個代理程式在相同備份時窗中備份其電腦，則可能無法啟動大型檔案伺服器的備份或檔案共用，因為代理程式佔用了所有磁帶機。假設您允許代理程式使用磁帶機 2 和 3，則磁帶機 1 會保留給備份共用的代理程式。

多重資料流

預設為：**[已停用]**。

多重資料流可讓您將資料從一個代理程式分成多個資料流，然後將那些資料流同時寫入不同磁帶。這可做到較快速的備份，而且當代理程式比磁帶機的傳輸量更高時，這特別有用。

只有當您在 **[僅限選取的裝置和磁碟機]** 選項下選擇多個磁帶機時，**[多重資料流]** 核取方塊才可用。選擇的磁碟機數目等於來自代理程式的同時資料流數目。如果在備份開始時，有任何選擇的磁碟機無法使用，備份將會失敗。

若要復原多重資料流備份或同時復原多重資料流備份和多工備份，您至少需要具備與用來建立此備份相同數目的磁碟機。

您無法變更現有保護計劃的多重資料流設定。若要使用不同的設定或變更選擇的磁帶機，請建立一個新的保護計劃。

多重資料流適用於本機連接的磁帶機，也適用於連接到儲存節點的磁帶機。

多工

預設為：**[已停用]**。

多工可讓您將來自多個代理程式的資料流寫入單一磁帶。這可更妥善地利用快速磁帶機。多工因子 (亦即傳送資料到單一磁帶的代理程式數目) 預設設定為二。您最多可增加至十。

多工對於有許多備份作業的大型環境很實用。它並不會提升單一備份的效能。

若要在大型環境中達到最快速備份，您必須分析代理程式、網路和磁帶機的傳輸量。然後，據以設定多工因子，不要過度多工。例如，如果您的代理程式每秒提供 70 Mbit 的資料，您的磁帶機每秒寫入 250 Mbit，而且您的網路沒有瓶頸，那麼請將多工因子設為三。多工因子設為四會導致過度多工，並降低備份效能。一般而言，多工因子介於二到五之間。

由於其結構緣故，多工備份的復原速度較慢。多工因子越大，復原速度越慢。不支援多個備份同時復原寫入單一多工磁帶。

您可以選擇一或多個特定磁帶機進行多工，或者在任何可用的磁帶機使用多工選項。本機連結的磁帶機無法使用多工。

您無法變更現有保護計劃的多工設定。若要使用不同的設定，請建立新的保護計劃。

在保護計劃中，可以做到下列多重資料流與多工組合：

- **多重資料流與多工選項皆已清除。**
  每個代理程式傳送資料到單一磁帶機。
- **只選擇多重資料流選項。**
  每個代理程式同時傳送資料到至少兩個磁帶機。
- **只選擇多工選項。**
  每個代理程式傳送資料到一部同時接受來自多個代理程式之資料流的磁帶機。一部磁帶機可接受的資料流數量上限設定於保護計劃內，而且無法即時修改。
- **多重資料流與多工選項皆已選擇。**
  每個代理程式至少傳送資料到兩部同時接受來自多個代理程式之資料流的磁帶機。

一部磁帶機一次只能寫入一種類型的備份 (多工或非多工)，端視哪一個保護計劃先開始而定。

在選擇用於備份的磁帶集區中使用磁帶組

預設為:**[已停用]**。

一個集區中的磁帶可以分組為所謂的**磁帶組**。

如果此選項保留為停用,資料會備份在屬於某個集區的所有磁帶上。如果此選項處於啟用狀態,可根據預先定義或自訂規則分離備份。

- **為每部電腦使用不同的磁帶組** (選擇一個規則:**備份類型**、**裝置類型**、**裝置名稱**、**月份中的日期**、**一週中的日期**、**一年中的月份**、**年**、**日期**)

  如果選擇此變數,則可根據預先定義的規格組織磁帶組。例如,對於一週的每天,您可使用不同磁帶組,或將每台電腦的備份儲存至不同的磁帶組上。
- **指定磁帶組的自訂規則**

  如果選擇此變數,則可指定組織磁帶組的自身規則。規則可包括以下變數:

變數語法	變數說明	變數數值
[Resource Name]	每部電腦的備份都會儲存在不同的磁帶組上。	在管理伺服器上登錄的電腦名稱。
[Backup Type]	完整、增量及差異備份將儲存在不同的磁帶組上。	full, inc, diff
[Resource Type]	各型別電腦的備份都會儲存在不同的磁帶組上。	Server essentials, Server, Workstation, Physical machine, VMware Virtual Machine, Virtual-PC Virtual Machine, Virtual Server Virtual Machine, Hyper-V Virtual Machine, Parallels Virtual Machine, XEN Virtual Machine, KVM Virtual Machine, RHEV Virtual Machine, Parallels Cloud Virtual Machine
[Day]	建立於一個月每天的備份都會儲存在不同的磁帶組上。	01、02、03 31
[Weekday]	建立於一週每天的備份都會儲存在不同的磁帶組上。	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
[Month]	建立於一年每月期間的備份都會儲存在不同的磁帶組上。	January, February, March, April, May, June, July, August, September, October, November, December
[Year]	建立於一年期間的備份都會儲存在不同的磁帶組上。	2017、2018

- 例如,如果將規則指定為 [Resource Name]-[Backup Type],則對於套用保護計劃的每台電腦的各完整備份、增量備份和差異備份,需要有不同的磁帶組。

您也可以指定各磁帶的磁帶組。在這種情況下，軟體將先在其磁帶組值與保護計劃中指定的運算式值一致的磁帶上寫入備份。然後，如有必要，將從同一集區取出其他磁帶。之後，如果集區可補充，則使用**可用磁帶**集區中的磁帶。

例如，如果將磁帶組 Monday 指定用於磁帶 1，將 Tuesday 指定用於磁帶 2 等，並在備份選項中指定 [Weekday]，在一週的相應日期使用對應的磁帶。

工作失敗處理

已排定的保護計劃執行失敗時，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。

預設為：**[已停用]**。

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 > 。

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)

此選項僅對 Windows 作業系統有效。

此選項定義了磁碟區陰影複製服務 (VSS) 提供者是否必須在即將開始備份時通知 VSS 感知應用程式。這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。資料一致性也可反過來確保應用程式復原至其正確狀態並在復原後立即可作業。

預設為：**[啟用]**。**自動選擇快照提供者**。

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、軟體快照提供者與 Microsoft 軟體陰影複製提供者。
- **使用 Microsoft 軟體陰影複製提供者**
  備份應用程式伺服器 (Microsoft Exchange Server、Microsoft SQL Server、Microsoft SharePoint 或 Active Directory) 時，建議您選擇此選項。

如果您的資料庫與 VSS 不相容，請停用此選項。此選項的快照擷取較快速，但對於在擷取快照時尚未完成其交易的應用程式，其資料一致性無法獲得保證。您可以使用資料擷取事先/事後命令，以確保在一致的狀態下備份資料。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；而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
如果啟用此選項，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**。

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) 的記錄將於每次順利進行完整、增量或差異磁碟層級備份後截斷。

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。

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。若要擷取靜止快照，備份軟體會使用 VMware Tools 或 Hyper-V 整合服務，將 VSS 套用到虛擬機器內。

預設為：**[啟用]**。

若啟用此選項，則會在擷取快照前完成截斷虛擬機器內執行的所有 VSS 感知應用程式。若擷取靜止快照的嘗試次數達到 [錯誤處理] 選項中所指定的重新嘗試次數後仍然失敗，且應用程式備份遭到停用，則會擷取非靜止快照。若啟用應用程式備份，備份會失敗。

若停用此選項，則會擷取非靜止快照。虛擬機器會以「衝突一致性」狀態來進行備份。建議您一律將此選項維持在啟用狀態，即使是未執行 VSS 感知應用程式的虛擬機器也是如此。否則，即使是在擷取的備份中也無法保證檔案系統的一致性。

注意事項
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 工具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。

復原內容	復原方法
實體機器 (Windows 或 Linux)	使用 Web 介面 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 或 Scale Computing HC3)	使用 Web 介面 使用可開機媒體
ESXi 設定	使用可開機媒體
檔案/資料夾	使用 Web 介面 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 Web 介面
SQL 資料庫	使用 Web 介面
Exchange 資料庫	使用 Web 介面
Exchange 信箱	使用 Web 介面
Microsoft 365 信箱	使用 Web 介面
Oracle 資料庫	使用 Oracle Explorer 工具

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

作業系統的備份影像可能會受到惡意程式碼感染，而且可能會重新感染復原後的電腦。

安全復原可讓您在復原過程中，使用整合式反惡意程式碼掃描和惡意程式碼刪除，防止這類感染再次發生。

限制：

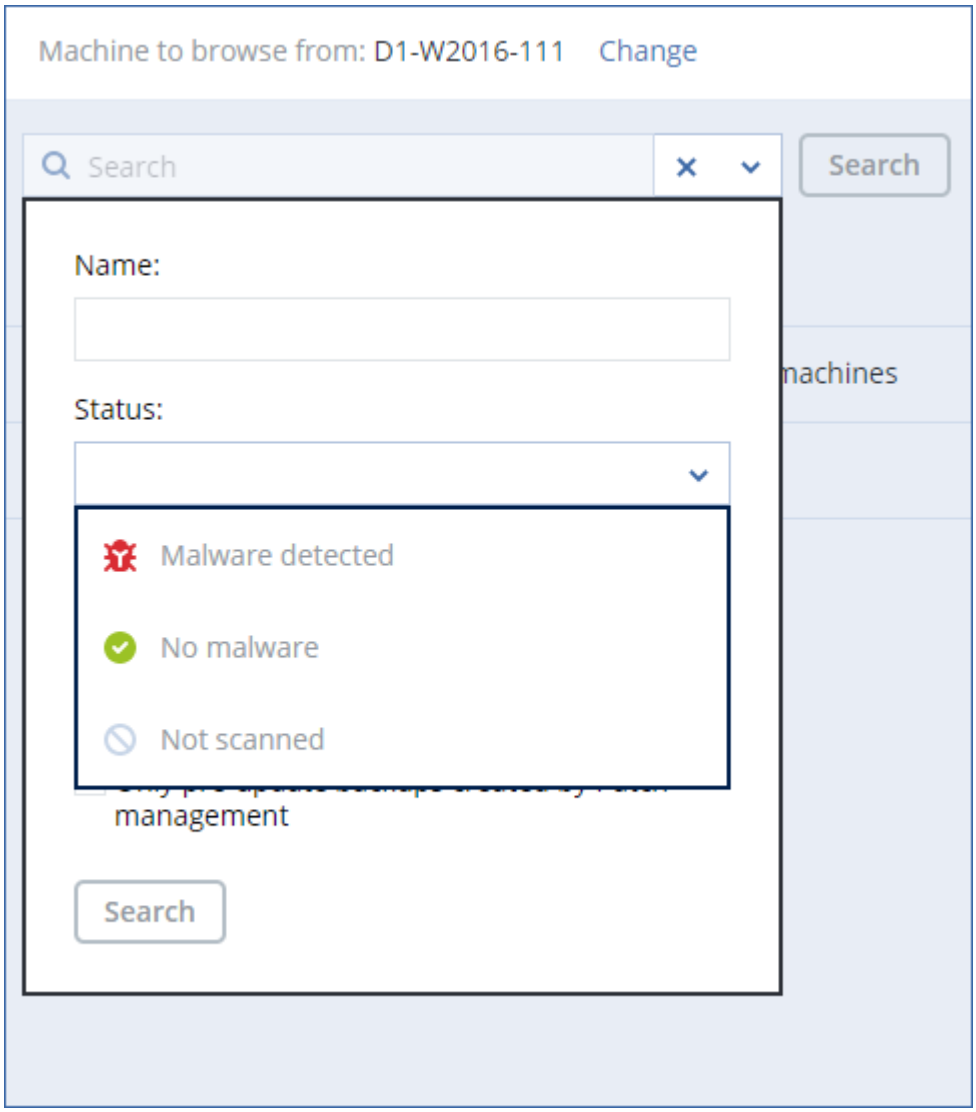
- 只有電腦內已安裝 Windows 用代理程式的實體或虛擬 Windows 機器支援安全復原。
- 僅支援備份 **[整部電腦]** 或 **[磁碟/磁碟區]** 類型。
- 只有具有 NTFS 檔案系統的磁碟區才受到支援。非 NTFS 磁碟分割將會在不經過反惡意程式碼掃描的情況下復原。
- 連續資料保護 (CDP) 備份不支援安全復原。電腦將會根據上次定期備份進行復原，但 CDP 備份中沒有資料。若要復原 CDP 資料，請執行 **[檔案/資料夾]** 復原。

運作原理

如果您在復原過程中啟用 [安全復原] 選項，則系統將會執行下列操作：

1. 掃描映像備份中的惡意程式碼，並標示受感染的檔案。備份會獲指派下列其中一個狀態：
   - **無惡意程式碼** – 在掃描期間，備份中找不到惡意程式碼。
   - **偵測到惡意程式碼** – 在掃描期間，備份中找到惡意程式碼。
   - **未掃描** – 未掃描備份中的惡意程式碼。
2. 將備份復原至選定的電腦。
3. 刪除偵測到的惡意程式碼。

您可以使用 **[狀態]** 參數篩選備份。



建立可開機媒體

可開機媒體為 CD、DVD、USB 快閃磁碟機，或其他可讓您執行代理程式的卸除式媒體，而不需作業系統的協助。可開機媒體的主要用途是復原無法啟動的作業系統。

我們極度建議當您開始使用磁碟層級備份時，就馬上建立及測試可開機媒體。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 中建立可開機媒體

1. 下載可開機媒體 ISO 檔。若要下載檔案，請按一下右上角的帳戶圖示 > **[下載]** > **[可開機媒體]**。
2. 執行下列任何一項作業：
   - 使用 ISO 檔燒錄 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]，而 Win32DiskImager 適用於 BIOS 電腦。在 Linux 中，應使用 dd 公用程式。

- 以 CD/DVD 光碟機將 ISO 檔連接至您要復原的虛擬機器。

此外，您可以使用 Bootable Media Builder 建立可開機媒體。

若要在 Mac OS 中建立可開機媒體

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。

復原電腦

復原實體機器

本節說明如何使用 Cyber Protect Web 主控台來復原實體機器。

如果您需要復原下列任一個項目，請使用可開機媒體，而不要使用 Cyber Protect Web 主控台：

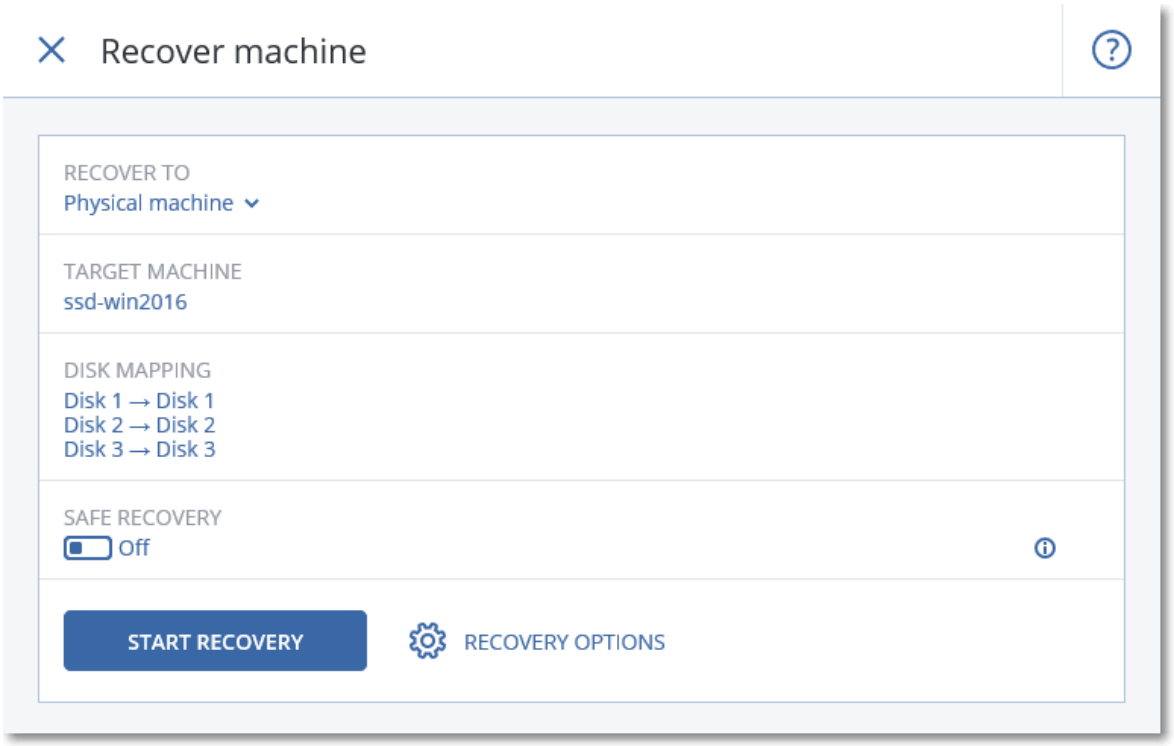
- macOS 作業系統
- 裸機或離線電腦上的任何作業系統
- 邏輯磁碟區 (Linux 中邏輯磁碟區管理器所建立的磁碟區) 的結構。媒體可讓您自動重新建立邏輯磁碟區結構。

復原作業系統以及復原使用 BitLocker 或 CheckPoint 加密的磁碟區都必須重新啟動。如需詳細資訊，請參閱 "使用重新啟動復原" (第 276 頁)。

如果要復原實體機器

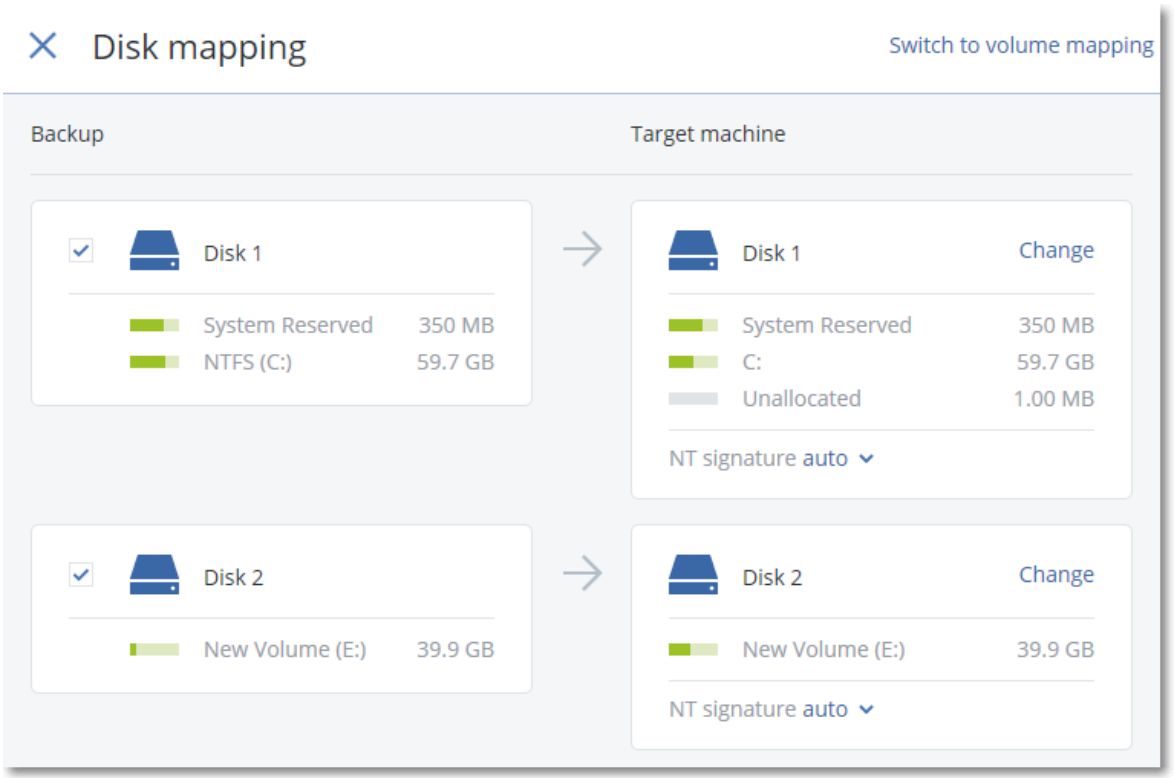
1. 選擇已備份的電腦。
2. 按一下 **[復原]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。
   如果電腦處於離線狀態，復原點就不會顯示。執行下列任何一項作業：
   - 如果備份位置是雲端或共用儲存 (即可被其他代理程式存取)，按一下 **[選擇電腦]**，選擇在線上的目標電腦，然後選擇復原點。
   - 在 [備份儲存] 索引標籤上選擇復原點。
   - 如 < 使用可開機媒體復原磁碟 > 所述來復原電腦。
4. 按一下 **[復原]** > **[整部機器]**。
   軟體會自動將備份的磁碟對應到目標電腦的磁碟。

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，可以透過按一下 **[磁碟對應]** 手動重新對應磁碟。

   此外，在對應區段中，您可以選擇要復原的個別磁碟或磁碟區。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. [選擇性] 啟用 **[安全復原]** 開關以掃描備份中的惡意程式碼。如果偵測到惡意程式碼，將會在備份中標示出來，並在復原程序完成後立即刪除。

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。

將實體機器復原為虛擬機器

您可以將實體機器的備份復原為虛擬機器。

如果至少在您的環境中為相關目標 Hypervisor 安裝一個代理程式，並在管理伺服器上註冊，才能復原至虛擬機器。例如，復原至 VMware ESXi 需要在環境中安裝 VMware 用代理程式，並在管理伺服器上註冊。

有些選項僅適用於雲端部署。

如需有關實體至虛擬機器移轉 (P2V) 之支援路徑的詳細資訊，請參閱 "電腦移轉" (第 433 頁)。

注意事項
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和磁碟區" (第 276 頁) 中所述復原電腦。
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。

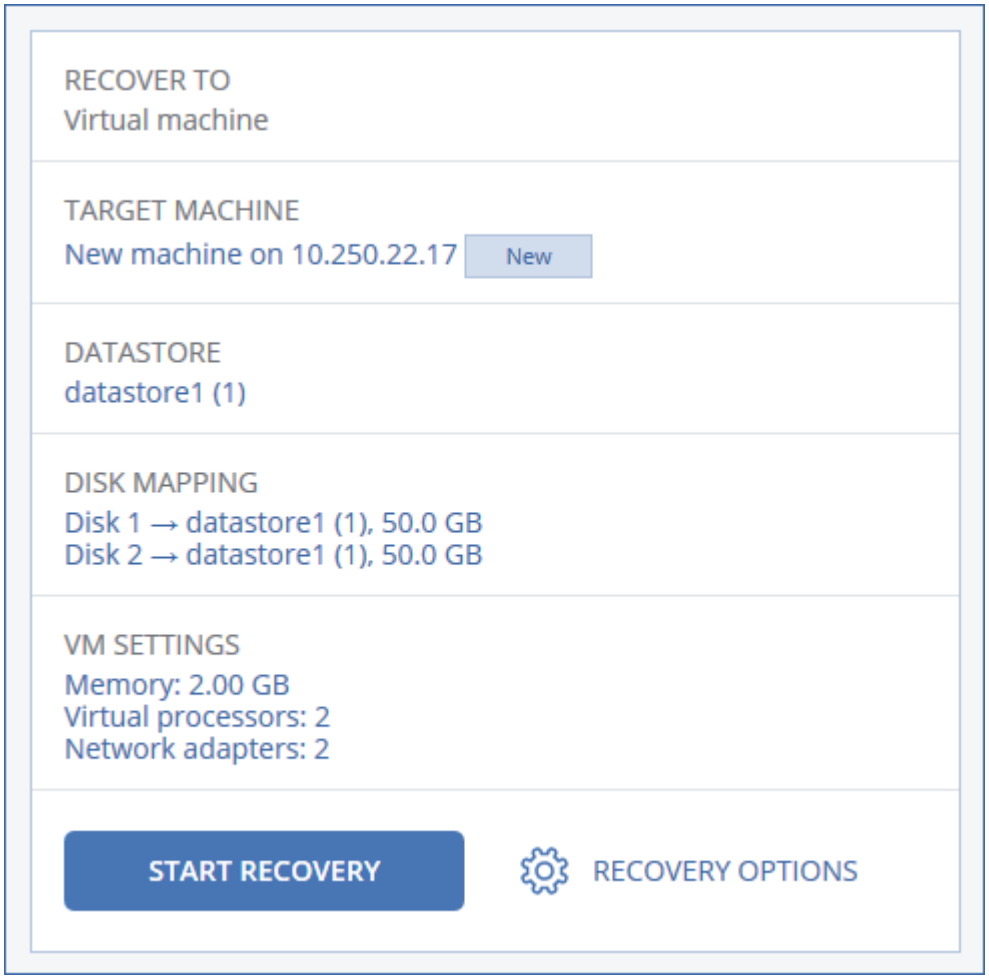
      注意事項
      必須至少在您的環境中為該 Hypervisor 安裝一個代理程式，並在管理伺服器上註冊。

   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]**，然後選擇 **[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。
8. [選用] [復原至新電腦時] 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)。
- 若要選擇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]**。在對應區段中，您可以選擇要復原的個別磁碟。

  注意事項
  如果您要復原 Virtuozzo 容器或 Virtuozzo Hybrid Infrastructure 虛擬機器，您無法變更這些設定。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]**。

- [適用於 VMware ESXi、Hyper-V、Virtuozzo 和 Red Hat Virtualization/oVirt] 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]**。



9. 按一下 **[開始復原]**。
10. [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

您可以將虛擬機器的備份復原為實體機器或另一部虛擬機器。

如果至少在您的環境中為相關目標 Hypervisor 安裝一個代理程式，並在管理伺服器上註冊，才能復原至虛擬機器。例如，復原至 VMware ESXi 需要在環境中安裝 VMware 用代理程式，並在管理伺服器上註冊。

有些選項僅適用於雲端部署。

如需有關虛擬至實體 (V2P) 或虛擬至虛擬 (V2V) 機器移轉之支援路徑的詳細資訊，請參閱 "電腦移轉" (第 433 頁)。

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。

重要事項
當您對另一部機器進行復原時，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]**)。

如果要復原虛擬機器

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. [復原至實體機器時] 在 **[復原至]** 中，選擇 **[實體機器]**。
   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 "復原實體機器" (第 270 頁) 中的步驟 4。否則，我們建議您使用可開機媒體來執行虛擬至實體 (V2P) 移轉。
4. [選用] 預設會將原始機器選為目標電腦。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。

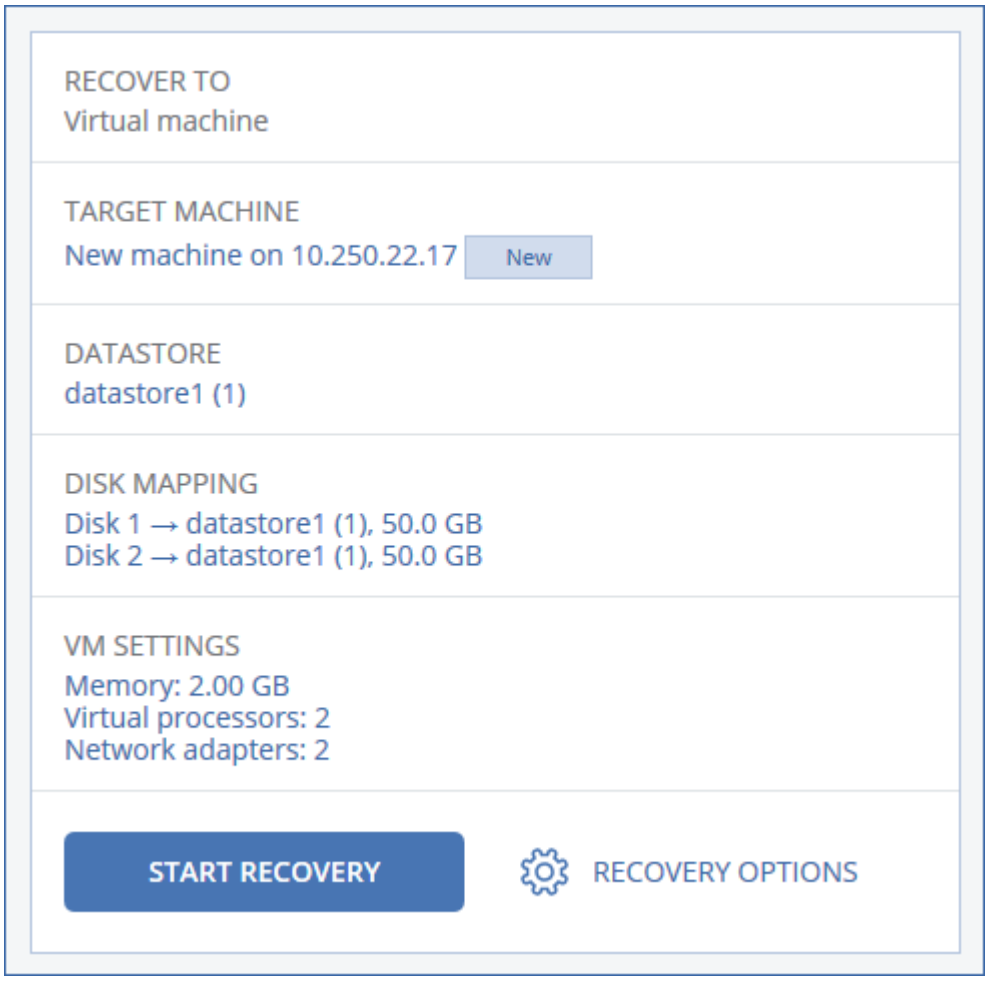
      注意事項
      必須至少在您的環境中為該 Hypervisor 安裝一個代理程式，並在管理伺服器上註冊。

   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，然後指定新電腦名稱，或選擇現有目標電腦。
   d. 按一下 **[確定]**。
5. [若是 Virtuozzo Hybrid Infrastructure] 按一下 **[VM 設定]**，然後選擇 **[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。

6. [選用] [復原至新電腦時] 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)。
   - 若要選擇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]**。在對應區段中，您可以選擇要復原的個別磁碟。

     注意事項
     如果您要復原 Virtuozzo 容器或 Virtuozzo Hybrid Infrastructure 虛擬機器，您無法變更這些設定。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]**。

   - [適用於 VMware ESXi、Hyper-V、Virtuozzo 和 Red Hat Virtualization/oVirt] 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]**。



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

當您復原下列項目時需要重新啟動：

- 作業系統
- BitLocker 或 CheckPoint 加密的磁碟區

重要事項
已備份的加密磁碟區會被當作未加密復原。

需求

- 復原加密的磁碟區時，會要求相同的電腦上有一個未加密的磁碟區，而且此磁碟區的可用空間至少為 1 GB。否則，復原將會失敗。
- 復原加密的系統磁碟區不需要採取其他任何動作。若要復原加密的非系統磁碟區，您必須先將其鎖定，例如，透過開啟此磁碟區上的檔案。否則，復原將會在未重新啟動的情況下繼續，因此 Windows 可能無法辨識復原後的磁碟區。

疑難排解

如果復原失敗，而且您的電腦重新啟動，並出現 [無法從磁碟分割取得檔案的錯誤]，請停用 [安全開機]。如需有關操作方式的詳細資訊，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和磁碟區

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" (第 269 頁)。

若要使用可開機媒體復原磁碟或磁碟區

1. 使用可開機媒體將目標電腦開機。
2. [僅適用於 macOS] 若要將 APFS 格式化的磁碟區復原至非原始電腦或裸機，則要手動重新建立原始磁碟組態：
   a. 按一下 **[磁碟公用程式]**。
   b. 重新建立原始磁碟組態。如需說明，請參閱 https://support.apple.com/guide/disk-utility/welcome。
   c. 按一下 **[磁碟公用程式]** > **[結束磁碟公用程式]**。

   注意事項
   自 macOS 11 Big Sur 開始，系統磁碟區無法備份及復原。若要復原可開機的 macOS 系統，您必須復原資料磁碟區，然後在其上安裝 macOS。

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 位址和連接埠。否則，請跳過此步驟。

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。
   - 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。

   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 **[磁碟]** 或 **[磁碟區]**，然後選擇要復原的項目。按一下 **[確定]** 以確認您的選擇。

   重要事項
   如果備份電腦有動態磁碟或邏輯磁碟區 (LVM)，請選擇 **[磁碟區]**。
10. 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。
11. [僅適用於 macOS] 若要將 APFS 格式化的資料磁碟區復原成可開機的 macOS 系統，請在 **[macOS 安裝區段]** 中，保持選擇 **[在復原的 macOS 資料磁碟區上安裝 macOS]** 核取方塊。
    復原之後，系統會重新開機，並且自動開始安裝 macOS。您需要有網際網路連線，讓安裝程式下載必要檔案。
    如果不需要將 APFS 格式化的資料磁碟區復原成可開機系統，請清除 **[在復原的 macOS 資料磁碟區上安裝 macOS]** 核取方塊。您稍後仍可將此磁碟區設為可開機，方法是在其上手動安裝 macOS。
12. [僅適用於 Linux] 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。
    c. 確認選擇項目。
13. [選擇性步驟] 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

使用 Web 介面復原檔案

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。執行下列其中一項操作：
   - [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，或使用搜尋以取得所需檔案和資料夾的清單。

   您可以使用一或多個萬用字元 (* 和 ?)。有關如何使用萬用字元的詳細資訊，請參閱「檔案篩選器」。

   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。
8. 按一下 **[復原]**。

   在**復原至**中，您可以看到以下之一：
   - 原始包含您想要復原的檔案的電腦 (如果代理程式安裝在此電腦上)。
   - 已安裝 VMware 用代理程式、Hyper-V 用代理程式或 Scale Computing HC3 用代理程式的電腦 (如果檔案源自於 ESXi、Hyper-V 或 Scale Computing HC3 虛擬機器)。

   這是要執行復原的目標電腦。您可以視需要選擇其他電腦。
9. 在**[路徑]**中，選擇復原目的地。您可以選擇下列其中一項：
   - 原始位置 (在復原至原始電腦時)
   - 目標電腦上的本機資料夾

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。

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

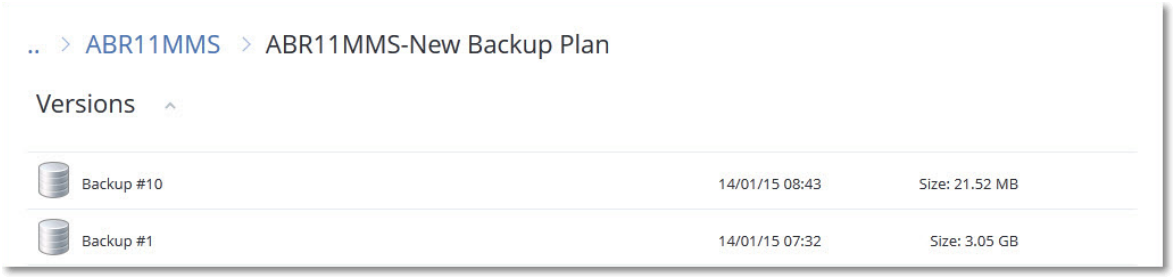
您可瀏覽雲端儲存、檢視備份內容，然後下載您所需的檔案。

限制

- 無法瀏覽系統狀態、SQL 資料庫與 Exchange 資料庫的備份。
- 為獲得更佳的下載體驗，一次下載不超過 100 MB。若要從雲端快速擷取更大量的資料，請使用檔案復原程序。

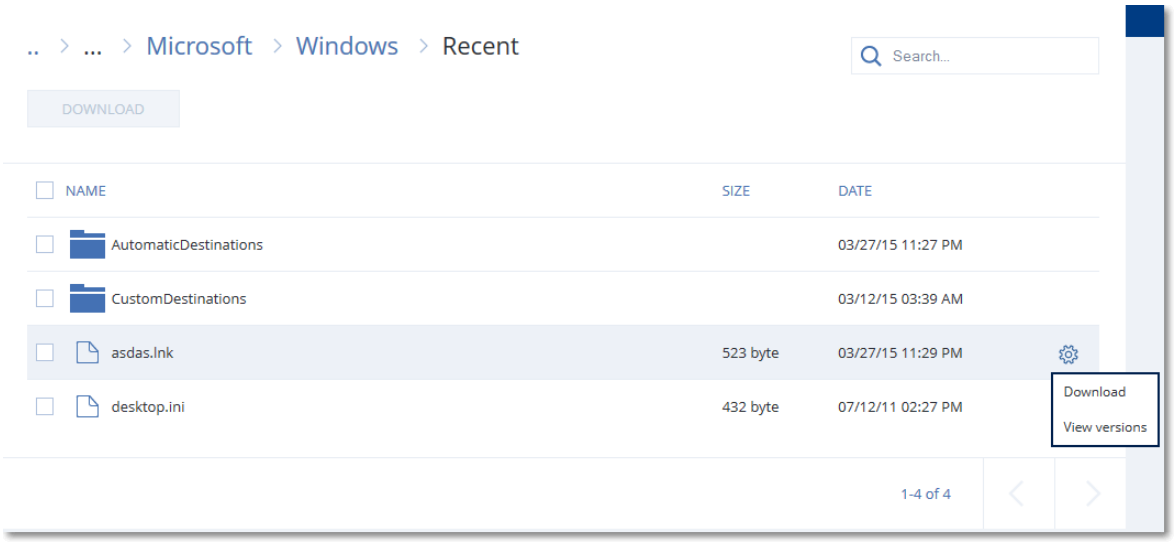
如果要從雲端儲存下載檔案

1. 選擇已經備份的電腦。
2. 按一下 **[復原]** > **[更多復原方式...]** > **[下載檔案]**。
3. 輸入已指派備份電腦之帳戶的認證。
4. [瀏覽磁碟層級備份時] 在 **[版本]** 下按一下您要復原檔案的來源備份。



[瀏覽檔案層級備份時] 您可在下個步驟中，在已選擇檔案右邊的齒輪圖示下選擇備份日期與時間。系統預設會從最新的備份復原檔案。

5. 瀏覽至所需的資料夾，或使用搜尋以取得所需檔案的清單。



6. 選擇需復原之項目的核取方塊，然後按一下 **[下載]**。
   如果只選擇一個檔案，系統會依檔案現狀下載檔案。否則，系統會將選擇的資料存檔為 .zip 檔。
7. 選擇儲存資料的目的地位置，然後按一下 **[儲存]**。

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

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」節步驟 1 - 6 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 位址和連接埠。否則，請跳過此步驟。

4. 在歡迎畫面上，按一下 **[復原]**。
5. 按一下 **[選擇資料]**，然後按一下 **[瀏覽]**。
6. 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。
   - 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。

   按一下 **[確定]** 以確認您的選擇。
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. 在 **[備份內容]** 中選擇 **[資料夾/檔案]**。
9. 選擇您要復原的資料。按一下 **[確定]** 以確認您的選擇。
10. 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。
11. [選擇性步驟] 按一下 **[復原選項]** 以指定額外的設定。
12. 按一下**[確定]**開始復原。

注意事項

當您在 Linux 可開機媒體和 WinPE 可開機媒體下重新掃描和復原時，磁帶位置需要大量空間，而且可能不適合 RAM。若是 Linux，您必須掛載另一個位置，才能將資料儲存在磁碟或共用上。請參閱 Acronis Cyber Backup Advanced：變更 TapeLocation 資料夾 (KB 27445)。若是 Windows PE，則目前沒有因應措施。

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。
- 您用來瀏覽備份的電腦必須已安裝保護代理程式。
- 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+。
- 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。

復原系統狀態

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 < 建立可開機媒體 > 。

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。
   - [選擇性步驟] 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. [選擇性步驟] 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. [選擇性步驟] 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 HC3	Windows
備份驗證	+	+	+	+	+	+	+	+	+
開機模式	+	-	-	-	-	-	-	+	-
檔案日期與時間	-	-	-	+	+	+	+	-	-
錯誤處理	+	+	+	+	+	+	+	+	+
檔案排除	-	-	-	+	+	+	+	-	-
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	-	-	-	-	-	-	-	+	-
"磁帶管理" (第 292 頁) > 使用磁碟快取加快復原速度	-	-	-	+	+	+	-	-	-
Windows 事件日誌	+	-	-	+	-	-	-	僅 Hyper-V	+
復原後開啟電源	-	-	-	-	-	-	+	-	-

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]**。

驗證作業會計算備份中所儲存之各資料區塊的檢查碼。唯一的例外是驗證位於雲端儲存中檔案層級的備份。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。

驗證作業是個非常耗時的程序，即使是驗證檔案不大的增量或差異備份也一樣。這是因為該作業不只會驗證備份中實際包含的資料，也會驗證選擇備份時可復原的所有資料。這需要存取先前建立的備份。

注意事項
驗證適用於位於 Acronis 資料中心且由 Acronis 合作夥伴所提供的雲端儲存空間。

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)。

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。

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。這會加速資料復原到與備份相同的磁碟，尤其是如果磁碟的磁碟區配置沒有變更的話。資料會在資料區塊層級進行比較。

對於實體機器，在區塊層級處比較資料是一項耗時作業。若與備份儲存的連線速度很快，那復原整個磁碟的時間將比計算資料差異所需的時間要少。因此，我們建議您僅在與備份儲存的連線速度緩慢時 (例如，在將備份儲存在雲端儲存或遠端網路資料夾上時)，啟用此選項。

復原實體機器之後，預設取決於備份位置：

- 若備份位置為雲端儲存，則預設為：**[啟用]**。
- 對於其他備份位置，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。

磁帶管理

您可以使用下列磁帶管理復原選項。

使用磁碟快取加快復原速度

預設為：**[已停用]**。

當您從影像存檔復原檔案時，強烈建議您使用 **[使用磁碟快取加快復原速度]** 選項。否則，還原作業可能要花很多時間。透過這個選項，系統會依序執行磁帶讀取，而不會中斷和倒帶。

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 用代理程式或 Scale Computing HC3 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、Hyper-V 用代理程式或 Scale Computing HC3 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]**。

復原後開啟電源

在可開機媒體下作業時，此選項有效。

預設為：**[已停用]**。

此選項可將電腦開機至復原的作業系統，不需要使用者介入。

災難復原

此功能僅在 Acronis Cyber Protect 雲端部署中可用。如需此功能的詳細描述，請參閱 https://www.acronis.com/support/documentation/DisasterRecovery/index.html#43224.html。

備份的相關作業

備份儲存索引標籤

[備份儲存] 索引標籤會顯示曾經在管理伺服器上登錄的所有電腦的備份。其中包括離線電腦及不再登錄的電腦。

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。在雲端部署中，系統管理員可以代表屬於相同群組及其子群組的任何帳戶檢視備份。**[可瀏覽的電腦]** 可間接選擇此帳戶。**[備份儲存]** 索引標籤會顯示曾以與此電腦所登錄之相同帳戶，進行登錄的所有電腦之備份。

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。

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，建議您匯出備份或使用備份複寫，而非手動移動備份檔案。

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. [選擇性步驟] 請按一下 **[可瀏覽的電腦]** 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 **[可瀏覽的電腦]** 中指定其他電腦。

4. 按一下 **[顯示備份]**。
5. 選擇復原點。

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。此方式也可透過利用 SharePoint Explorer 來對 Microsoft SharePoint 資料執行細微復原。
- **離線病毒清理**

  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。一旦錯誤修正完成，系統就會建立新的增量備份，並從該備份復原系統。

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。預設情況下，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. 用滑鼠右鍵按一下要掛載的磁碟區，然後按下列任一選項：

- **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)。

- **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. 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

驗證是檢視從備份中復原資料的可能性的作業。有關此作業的更多資訊，請參閱 "驗證" (第 302 頁)。

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 295 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獨立複本。原始備份保持不變。匯出作業可讓您從增量和差異備份鏈中分離特定備份，以快速復原，寫入卸除式或卸離式媒體，或用於其他用途。

匯出作業的結果一律是完整備份。如果您要將整個備份鏈複寫到其他位置並保留多個復原點，請使用備份複寫計劃。

匯出備份的備份檔案名稱取決於備份格式選項：

- 若是具有任何備份配置的 **12 版**格式，備份檔案名稱會與原始備份的檔案名稱相同，但序號除外。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。
- 若是具有 **[一律增量 (單一檔案)]** 備份配置的 **11 版**格式，備份檔案名稱會與原始備份的備份檔案名稱完全相符。如果相同備份鏈中的多個備份匯出到相同的位置，則每個匯出作業都會覆寫先前匯出的備份。
- 若是具有其他備份配置的 **11 版**格式，備份檔案名稱會與原始備份的檔案名稱相同，但時間戳記除外。匯出備份的時間戳記會對應到執行匯出的時間。

匯出備份會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。
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

警告！
當備份遭到刪除時，其所有資料也會遭到永久清除。已刪除的資料無法復原。

若要刪除線上且存在 Cyber Protect Web 主控台中的電腦備份

1. 在 **[所有裝置]** 索引標籤上，選擇您要刪除其備份的電腦。
2. 按一下 **[復原]**。
3. 選擇您要刪除的備份之位置。
4. 執行下列其中一項操作：
   - 欲刪除單一備份，請選擇要刪除的備份，按一下齒輪圖示，然後按一下 **[刪除]**。
   - 欲刪除已選擇位置裡的所有備份，請按一下 **[全部刪除]**。
5. 確認選項無誤。

欲刪除任何電腦的備份

1. 在 **[備份儲存]** 索引標籤上，選擇您要刪除備份的位置。
   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. 選擇群組
3. 執行下列其中一項操作：
   - 欲刪除單一備份，請按一下 **[顯示備份]**，選擇要刪除的備份，按一下齒輪圖示，然後按一下 **[刪除]**。
   - 如果要刪除選擇的群組，請按一下 **[刪除]**。
4. 確認選項無誤。

若要從雲端儲存空間直接刪除備份

1. 登入雲端儲存空間，如 < 從雲端儲存空間下載檔案 > 中所述。
2. 按一下您要刪除其備份的電腦名稱。
   軟體會顯示一或多個備份群組。
3. 按一下對應到您想要刪除之備份群組的齒輪圖示。
4. 按一下 **[移除]**。
5. 確認作業。

「計劃」索引標籤

利用 Advanced 授權，您可以透過使用 **[計劃]** 索引標籤管理保護計劃和其他計劃。

[計劃] 索引標籤的各區段包含特定類型的所有計劃。以下區段可用：

- **保護**
- **備份掃描**
- **備份複寫**
- **驗證**
- **清理**
- **轉換成 VM**
- **VM 複寫**
- **可開機媒體**。此區段會顯示針對從可開機媒體開機的電腦而建立的保護計劃，且僅能套用至這類電腦。

在各區段，您可建立、編輯、停用、啟用、刪除、啟動及監視計劃的執行。

複製與停止僅適用於保護計劃。與從 **[裝置]** 索引標籤停止備份不同的是，停止保護計劃將會在套用此計劃的所有裝置上停止備份。如果多個裝置的備份開始時間分配在某個時間範圍內，那麼停止保護計劃將會停止執行中的備份或防止啟動備份。

您也可將計劃匯出至檔案並匯入先前匯出的計劃。

脫離主機資料處理

保護計劃的大部分操作 (如複寫、驗證和套用保留規則) 都由執行備份的代理程式執行。這會給運行代理程式的電腦增加額外的工作負載，即使備份過程完成後也如此。

將反惡意程式碼掃描、複寫、驗證、清理和轉換計劃從保護計劃中分離，可讓您靈活處理以下操作：

- 選擇其他代理程式執行這些操作
- 將這些操作安排在非高峰時段，以最大限度地減少網路頻寬消耗
- 如果設置一個專用代理程式不在您的計劃之內，則將這些操作挪到工作時間外執行

如果您使用的是儲存節點，則在同一台電腦上安裝專用代理程式是明智之選。

備份和 VM 複寫計劃會採用執行代理程式之電腦的時間設定，脫離主機資料處理計劃則根據管理伺服器電腦的時間設定執行。

備份掃描計劃

支援的位置

您可以在下列位置中掃描備份中是否有惡意程式碼：**[雲端儲存空間]**、**[本機資料夾]** 和 **[網路資料夾]**。只有安裝在已掃描電腦上的代理程式可以存取 **[本機資料夾]** 位置。

如需有關備份掃描及其限制的詳細資訊，請參閱「備份的反惡意程式碼掃描」。

建立備份掃描計劃

1. 在 Cyber Protect Web 主控台中，按一下 **[計劃]** > **[備份掃描]**。
2. 按一下 **[建立計劃]**。
3. [選擇性] 若要修改計劃名稱，請按一下預設名稱旁的鉛筆圖示。
4. 選擇掃描代理程式。
5. 選擇要掃描的備份位置或個別備份。
   您可以一次選擇多個備份位置。若要在一個計劃中包含多個個別備份，您需要逐一新增備份。
6. [如果選擇 **[雲端儲存空間]** 或 **[網路資料夾]**] 如果出現提示，請提供存取備份儲存空間的認證。
7. [如果選擇加密備份] 提供存取備份的密碼。如果選擇一個儲藏庫或多個加密備份，則您可以指定單一密碼。如果特定備份的密碼不正確，將會顯示警示。系統只會掃描提供正確密碼的備份。
8. 設定掃描的排程。
9. 準備就緒後，按一下 **[建立]**。

因此便會建立備份掃描計劃。

備份複寫

支援的位置

下表摘述備份複寫計劃支援的備份位置。

備份位置	支援作為來源	支援作為目標
雲端儲存	+	+
本機資料夾	+	+
網路資料夾	+	+
NFS 資料夾	–	–
Secure Zone	–	–
SFTP 伺服器	–	–
受管理的位置*	+	+
磁帶裝置	–	+

* 檢查主題 "具有進階授權之使用者的考量" (第 225 頁) 中所述的限制。

若要建立備份複寫計劃

1. 按一下 **[計劃]** > **[備份複寫]**。
2. 按一下 **[建立計劃]**。
   軟體會顯示新的計劃範本。
3. [選擇性步驟] 若要修改計劃名稱，請按一下預設名稱。
4. 按一下 **[代理程式]**，然後選擇將執行複寫的代理程式。

您可以選擇具有來源與目標備份位置存取權的任何代理程式。

5. 按一下 **[要複寫的項目]**，然後選擇此計劃將複寫的備份。

   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。
6. 按一下 **[目的地]**，然後指定目標位置。
7. [選擇性步驟]在 **[如何複寫]** 中，選擇要複寫的備份。您可以選擇下列其中一項：
   - **所有備份** (預設值)
   - **僅限完整備份**
   - **僅限最後一個備份**
8. [選擇性步驟] 按一下 **[排程]**，然後變更排程。
9. [選擇性步驟] 按一下 **[保留規則]**，然後如「保留規則」中所述指定目標位置的保留規則。
10. 如果 **[要複寫的項目]** 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。
11. [選擇性步驟] 若要修改計劃選項，請按一下齒輪圖示。
12. 按一下 **[建立]**。

驗證

驗證是檢視從備份中復原資料的可能性的作業。

備份位置驗證會驗證位置儲存的所有備份。

運作原理

驗證計劃提供兩種驗證方法。若選擇這兩種方法，作業將連續執行。

- **計算備份中所儲存之各資料區塊的總和檢查碼**

  如需透過計算總合檢查碼進行驗證的相關資訊，請參閱「備份驗證」。
- **從備份執行虛擬機器**

  此方法僅適用於包含作業系統的磁盤層級備份。若要使用此方法，您需要 ESXi 或 Hyper-V 主機以及用於管理此主機的保護代理程式 (VMware 用代理程式或 Hyper-V 用代理程式)。

  代理程式從備份執行虛擬機器，然後連線至 VMware Tools 或 Hyper-V Heartbeat Service，以確保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的備份數目為何，執行驗證的代理程式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並執行下一個虛擬機器。

如果驗證失敗，您可以在 **[概觀]** 標籤的 **[活動]** 區段上向下鑽研詳細資料。

支援的位置

下表摘述驗證計劃支援的備份位置。

備份位置	計算總和檢查碼	執行 VM
雲端儲存	+	+
本機資料夾	+	+
網路資料夾	+	+
NFS 資料夾	–	–
Secure Zone	–	–
SFTP 伺服器	–	–
受管理的位置	+	+
磁帶裝置	+	–

若要建立新的驗證計劃

1. 按一下**計劃** > **驗證**。
2. 按一下 **[建立計劃]**。
   軟體會顯示新的計劃範本。
3. [選擇性步驟] 若要修改計劃名稱，請按一下預設名稱。
4. 按一下**代理程式**，然後選擇將執行驗證的代理程式。
   如果要透過從備份執行虛擬機器而進行驗證，則選擇 VMware 用代理程式或 Hyper-V 用代理程式。否則，您可以選擇登錄於管理伺服器且具有備份位置存取權的任何代理程式。
5. 按一下 **[要驗證的項目]**，然後選擇此計劃將驗證的備份。
   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。
6. [選擇性步驟] 在 **[要驗證的內容]** 中，選擇要驗證的備份。您可以選擇下列其中一項：
   - **所有備份**
   - **僅限最後一個備份**
7. [選擇性步驟] 按一下 **[如何驗證]**，然後選擇下列任何方法：
   - **總和檢查碼驗證**
     軟體將計算備份中所儲存之各資料區塊的檢查碼。
   - **以虛擬機器的形式執行**
     軟體將從每個備份執行虛擬機器。
8. 若您已選擇**以虛擬機器的形式執行**：
   a. 按一下 **[目標電腦]**，然後選擇虛擬機器類型 (ESXi 或 Hyper-V)、主機和電腦名稱範本。
      預設名稱為 **[電腦名稱]_validate**。
   b. [選擇性步驟] 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。
   c. [選用] 變更磁碟的佈建模式。

預設設定為：**[精簡]**(適用於 VMware ESXi) 和 **[動態延伸]**(適用於 Hyper-V)。

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。

注意事項

[VM 活動訊號] 開關一律啟用，以透過從備份執行虛擬機器，來驗證由客體作業系統 (VMware Tools 或 Hyper-V 整合服務) 中 Hypervisor 工具回報之虛擬機器的活動訊號狀態。此開關專為將來版本而設計，所以您無法與之互動。

9. [選用] 按一下 **[排程]**，然後變更排程。
10. 如果 **[要驗證的項目]** 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。
11. [選用] 要修改計劃選項，請按一下齒輪圖示。
12. 按一下 **[建立]**。

清理

清理作業會根據保留規則刪除過期的備份。

支援的位置

清理計劃支援除了 NFS 資料夾、SFTP 伺服器及 Secure Zone 之外的所有備份位置。

若要建立新的清理計劃

1. 按一下 **[計劃]** > **[清理]**。
2. 按一下 **[建立計劃]**。

軟體會顯示新的計劃範本。

3. [選擇性步驟] 若要修改計劃名稱，請按一下預設名稱。
4. 按一下 **[代理程式]**，然後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。

5. 按一下 **[要清理的項目]**，然後選擇此計劃將清理的備份。

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。

6. [選擇性步驟] 按一下 **[排程]**，然後變更排程。
7. [選擇性步驟] 按一下 **[保留規則]**，然後如 < 保留規則 > 中所述指定保留規則。
8. 如果 **[要清理的項目]** 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。
9. [選擇性步驟] 若要修改計劃選項，請按一下齒輪圖示。
10. 按一下 **[建立]**。

轉換為虛擬機器

您可以針對轉換至虛擬機器建立個別的計劃，並以手動或排程的方式，執行此計劃。

如需有關必要條件和限制的資訊，請參閱「關於轉換，您需要知道的內容」。

若要建立轉換至虛擬機器的計劃

1. 按一下 **[計劃]** > **[轉換為 VM]**。
2. 按一下 **[建立計劃]**。
   軟體會顯示新的計劃範本。
3. [選擇性步驟] 若要修改計劃名稱，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。您可以選擇下列其中一項：
   - **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，每次轉換成 VHDX 的檔案都會覆寫在上次轉換期間建立的目標位置中的 VHDX 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。
   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. [選擇性步驟] 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. [選擇性步驟] 若要修改計劃選項，請按一下齒輪圖示。
14. 按一下 **[建立]**。

可開機媒體

重要事項
本節中所述的部分功能僅適用於內部部署。

可開機媒體

可開機媒體是一種實體媒體 (CD、DVD、USB 快閃磁碟機，或電腦 BIOS 支援作為開機裝置的其他卸除式媒體)，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 (WinPE) 中執行保護代理程式。

可開機媒體最常用於：

- 復原無法啟動的作業系統
- 存取和備份損毀的系統中未損壞的資料
- 在裸機上部署作業系統
- 在裸機上建立基本或動態磁碟區
- 逐一磁區備份採用不支援的檔案系統的磁碟
- 離線備份因為資料遭到執行中應用程式鎖定或限制存取等而無法線上備份的任何資料。

您也可以從 Acronis PXE 伺服器、Windows Deployment Services (WDS) 或遠端安裝服務 (RIS) 使用網路開機，以便為電腦開機。這些裝有上傳可開機元件的伺服器也可視為一種可開機媒體。您可以使用相同的精靈，建立可開機媒體或設定 PXE 伺服器或 WDS/RIS。

建立可開機媒體或下載現成的可開機媒體？

您可以使用 Bootable Media Builder，為 Windows、Linux 或 macOS 電腦，建立自己的可開機媒體 (Linux 型或 WinPE 型)。若是完整功能的可開機媒體，則需要指定您的 Acronis Cyber Protect 授權金鑰。如果沒有這個金鑰，您的可開機媒體將僅能夠執行復原作業。

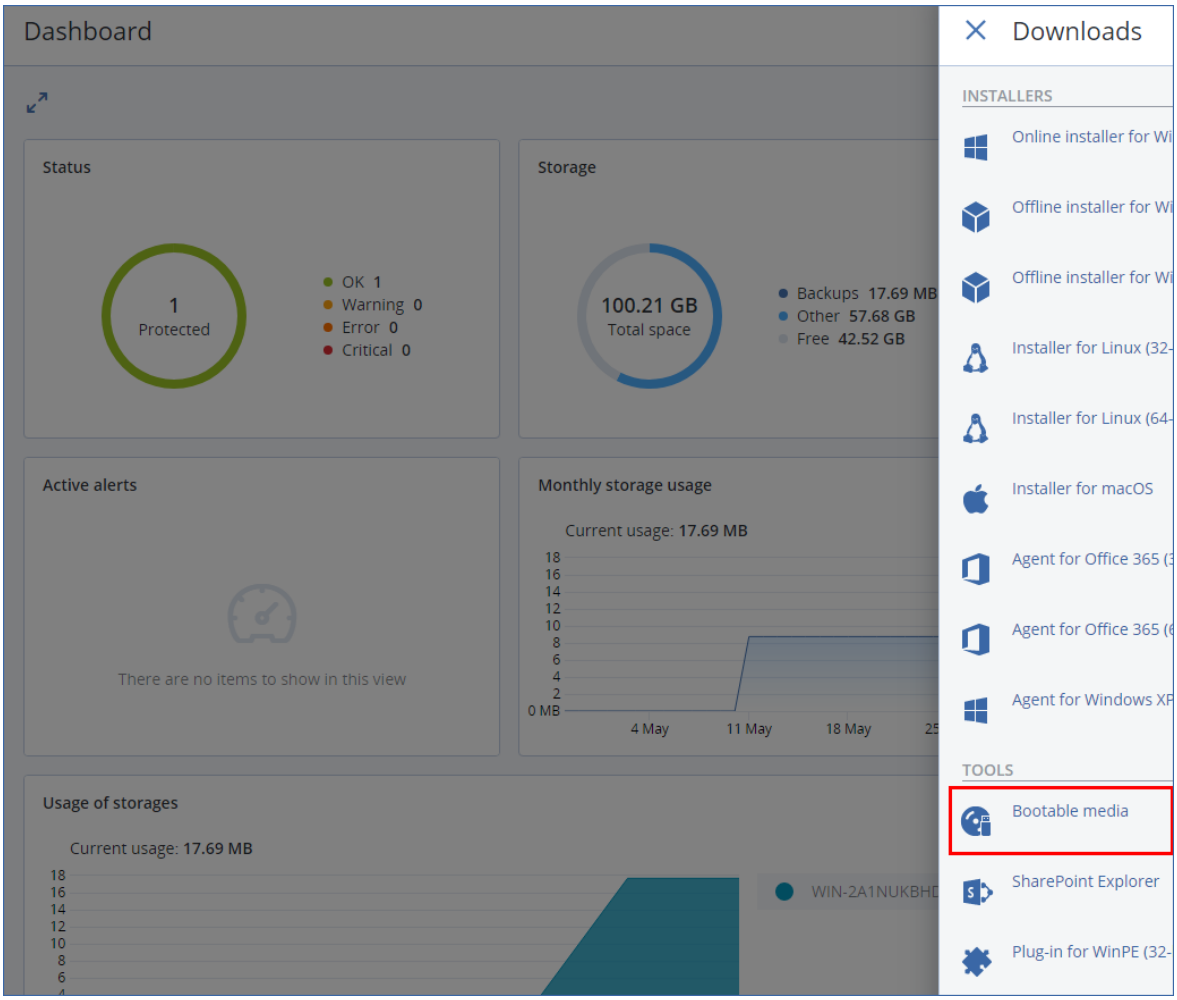
注意事項
可開機媒體不支援混合式磁碟機。

此外，您可以下載現成的可開機媒體 (僅限 Linux 型)。您僅能將下載的可開機媒體用於復原作業，以及存取 Acronis Universal Restore。您無法備份資料、驗證或匯出備份、管理磁碟，或搭配該可開機媒體使用指令碼。下載的可開機媒體不適用於 macOS 電腦。

注意事項
現成的可開機媒體不支援儲存節點、磁帶位置和 SFTP 位置。如果您想要在內部部署中使用這些儲存位置，必須使用 Bootable Media Builder 建立自己的可開機媒體。請參閱 https://kb.acronis.com/content/61566。

若要下載現成的可開機媒體

1. 在 Cyber Protect Web 主控台中，按一下右上角的帳戶圖示，然後按一下 **[下載]**。
2. 選擇 **[可開機媒體]**。



您可以將下載的 ISO 檔案燒錄到 CD/DVD，或使用線上提供的其中一個免費工具，建立可開機的 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。

如果無法存取 Cyber Protect Web 主控台，您可以在 Acronis 客戶入口網站中，從您的帳戶下載現成的可開機媒體：

1. 移至 https://account.acronis.com。
2. 找出 Acronis Cyber Protect，然後按一下 **[下載]**。
3. 在開啟的頁面上，找出 **[其他下載]**，然後按一下 **[可開機媒體 ISO (適用於 Windows 和 Linux)]**。

Linux 或 WinPE 可開機媒體？

Linux

Linux 型可開機媒體包含以 Linux 核心為基礎的可開機保護代理程式。代理程式可在任何 PC 相容硬體上開機並執行作業，包括裸機和帶有已損壞的或不支援檔案系統的電腦。這些作業可以從本機

或遠端的 Cyber Protect Web 主控台設定並控制。

Linux 媒體硬體所支援的清單可在下列位址取得：http://kb.acronis.com/content/55310。

WinPE 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 Acronis 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。

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 可開機媒體，在 Windows 預先安裝環境中使用 Acronis Cyber Protect 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。
- 基於 PE 之可開機媒體有助於克服某些與 Linux 相關之可開機媒體問題，如僅支援特定 RAID 控制器或特定級別的 RAID 陣列。以 WinPE 2.x 及更新版本為基礎的媒體可讓您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。
- 若某台電腦是透過 PE 可開機媒體開機，您就無法選擇 CD、DVD 或藍光光碟 (BD) 等光學媒體作為備份目的地。

可開機媒體組建

Bootable Media Builder 是建立可開機媒體的專用工具。僅適用於內部部署。

Bootable Media Builder 依預設會在您安裝管理伺服器的時候加以安裝。您可以在任何執行 Windows 或 Linux 的電腦上單獨安裝媒體建立器。支援的作業系統與對應之代理程式的作業系統相同。

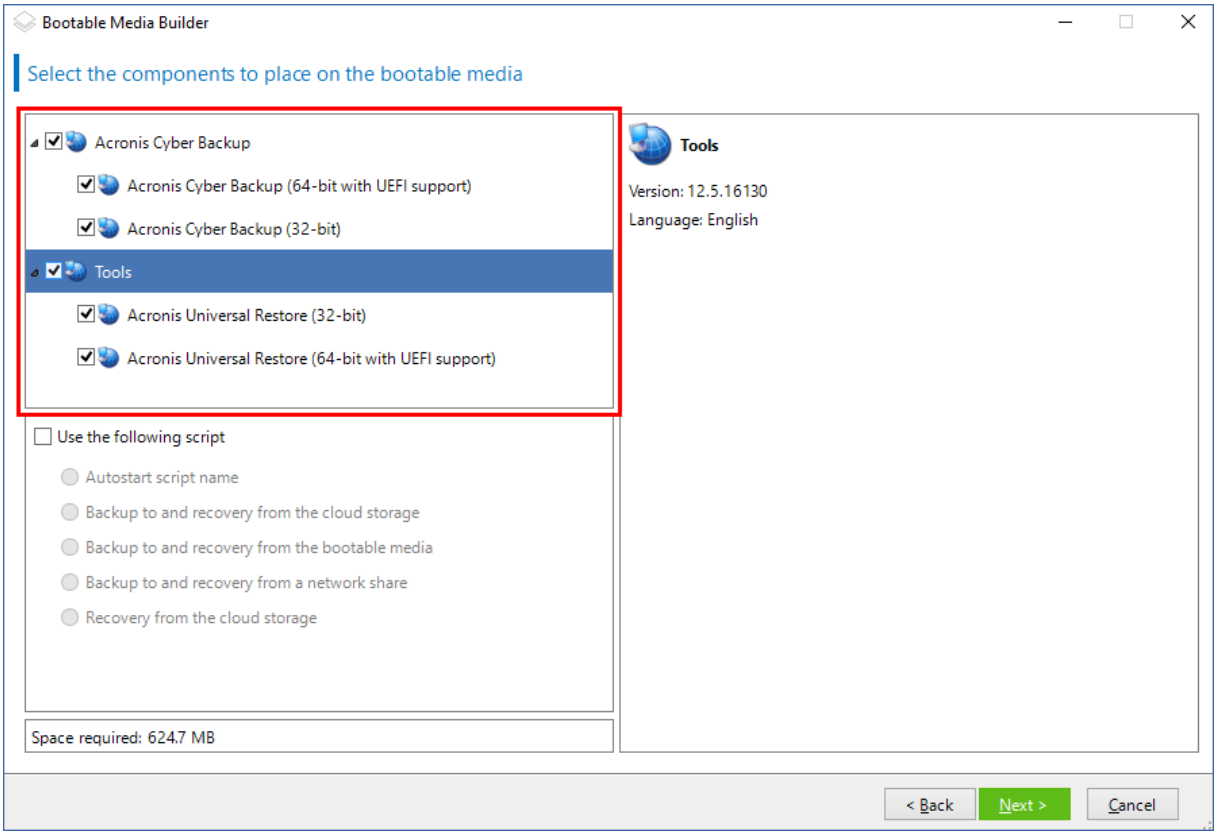
為何使用媒體建立器？

可供在 Cyber Protect Web 主控台中下載的現成可開機媒體僅可用於復原。此媒體是以 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。

- 媒體建立器可讓您建立具有備份功能的自訂、完整功能的 Linux 和 WinPE 可開機媒體。
- 除了建立實體可開機媒體之外，您可以將其元件上傳至 Windows Deployment Services (WDS)，並使用網路開機。
- 現成的可開機媒體不支援儲存節點、磁帶位置和 SFTP 位置。如果您想要在本機內部部署中使用這些儲存位置，必須使用 Bootable Media Builder 建立自己的可開機媒體。請參閱 https://kb.acronis.com/content/61566。

32 位元或 64 位元?

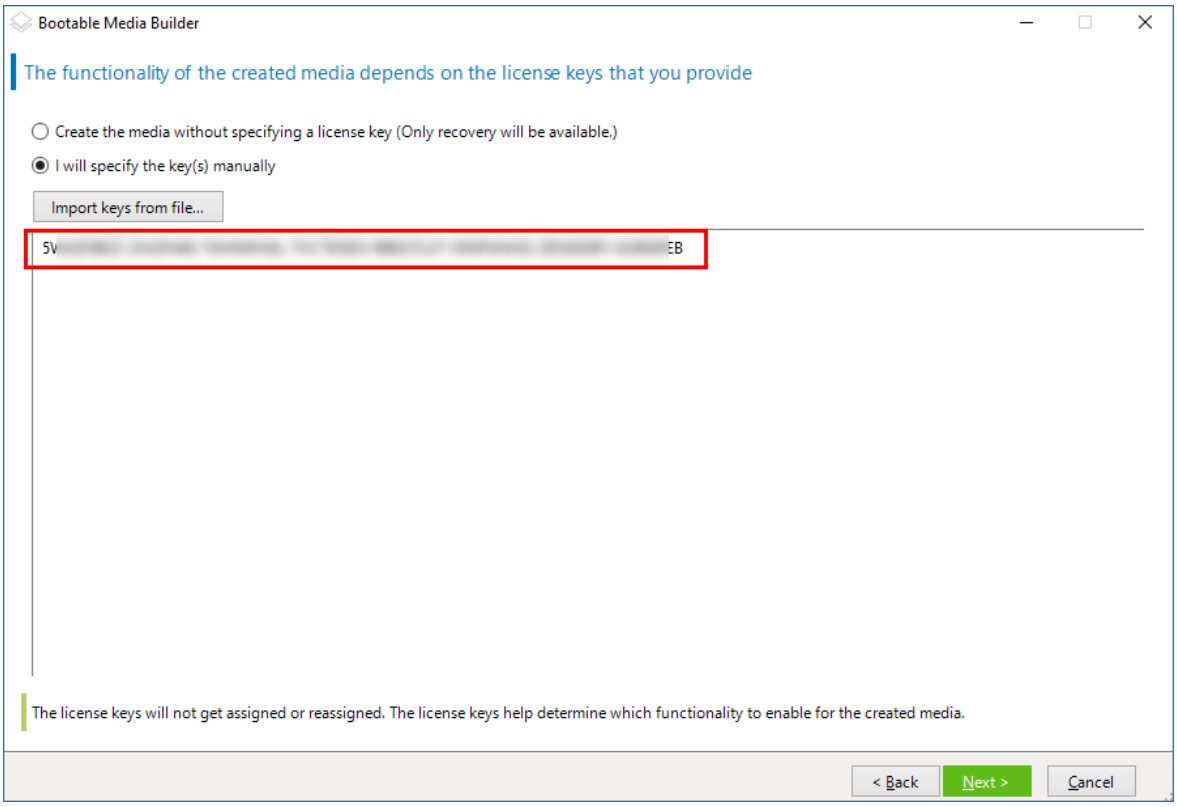
Bootable Media Builder 會建立包含 32 位元及 64 位元元件的媒體。在大多數的情況下，使用整合可延伸韌體介面 (UEFI) 的電腦需要有 64 位元的媒體才能開機。



Linux 可開機媒體

若要建立 Linux 可開機媒體

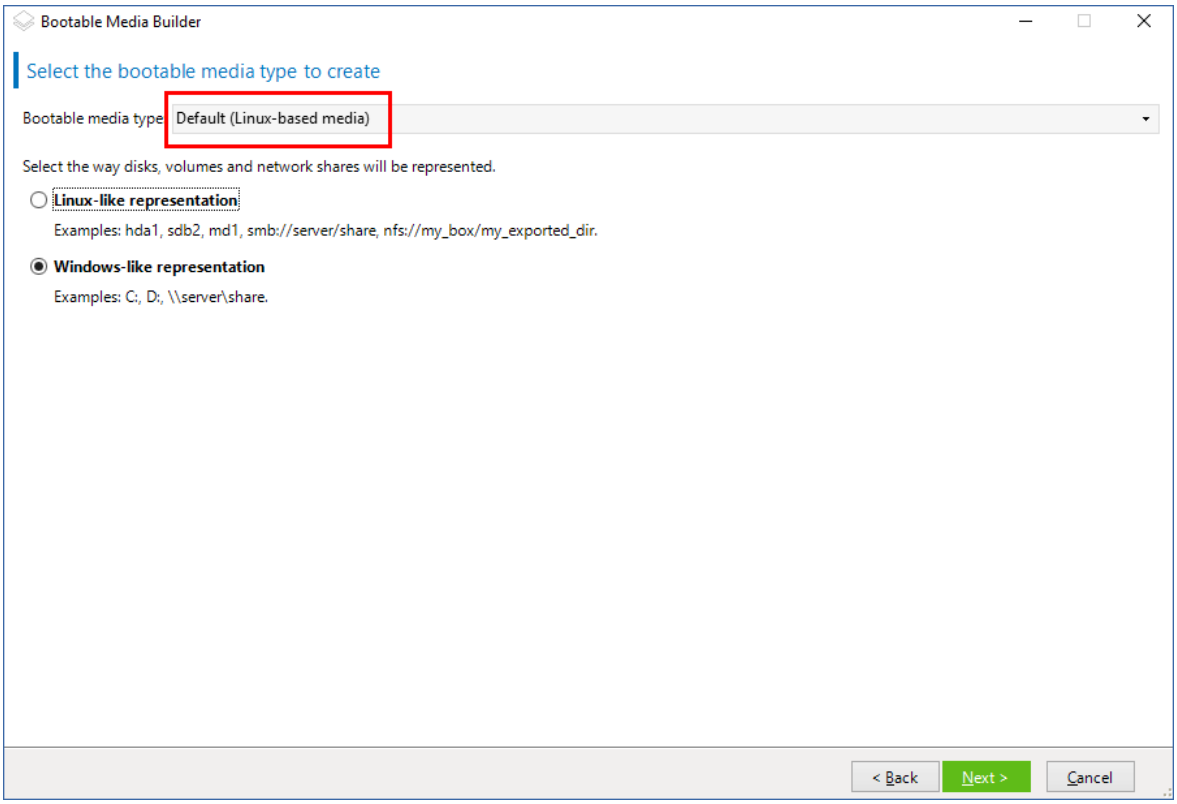
1. 啟動 **Bootable Media Builder**。
2. 若要建立完整功能的可開機媒體，請指定 Acronis Cyber Protect 授權金鑰。此金鑰用於確定將包含在可開機媒體中的功能。系統將不會從任何電腦撤銷授權。
   如果您未指定授權金鑰，所產生的可開機媒體僅能用於復原作業。



3. 請選擇**可開機媒體類型：預設（Linux 媒體）**。

   選擇表示磁碟區和網路資源的方式：

   - 採用類似 Linux 磁碟區表示方式的媒體，會將磁碟區顯示為以下格式：hda1 和 sdb2。這種媒體在進行復原前，會先試圖重建 MD 裝置和邏輯 (LVM) 磁碟區。
   - 採用類似 Windows 磁碟區表示方式的媒體，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 (LDM) 磁碟區。



4. 指定 Linux 核心的參數。使用空格分隔多個參數。

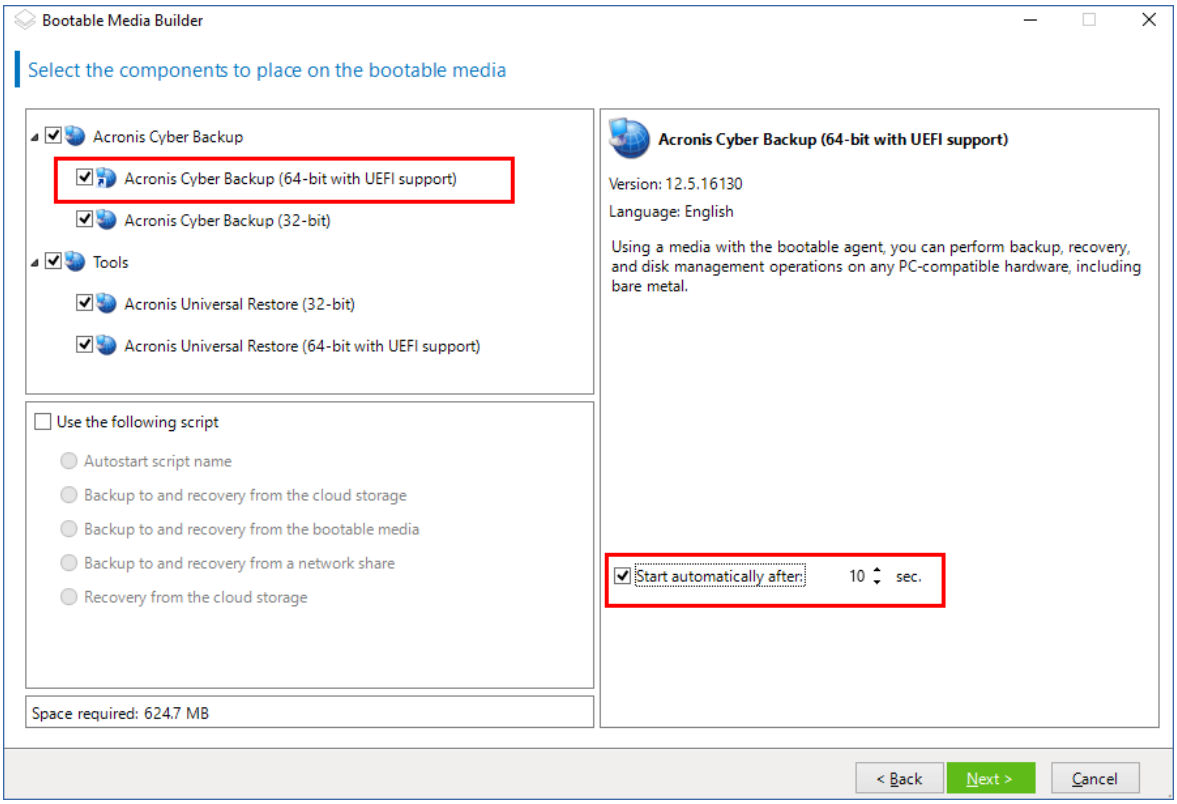
   例如，為了能夠在每次媒體啟動時選擇可開機代理程式的顯示模式，請輸入：**vga=ask**

   如需有關可用參數的詳細資訊，請參閱核心參數。
5. [選擇性步驟] 選擇將在可開機媒體中使用的語言。
6. 選擇要放在媒體上的元件：Acronis Cyber Protect 可開機代理程式和/或 Universal Restore (如果您打算在相異硬體上還原系統)。

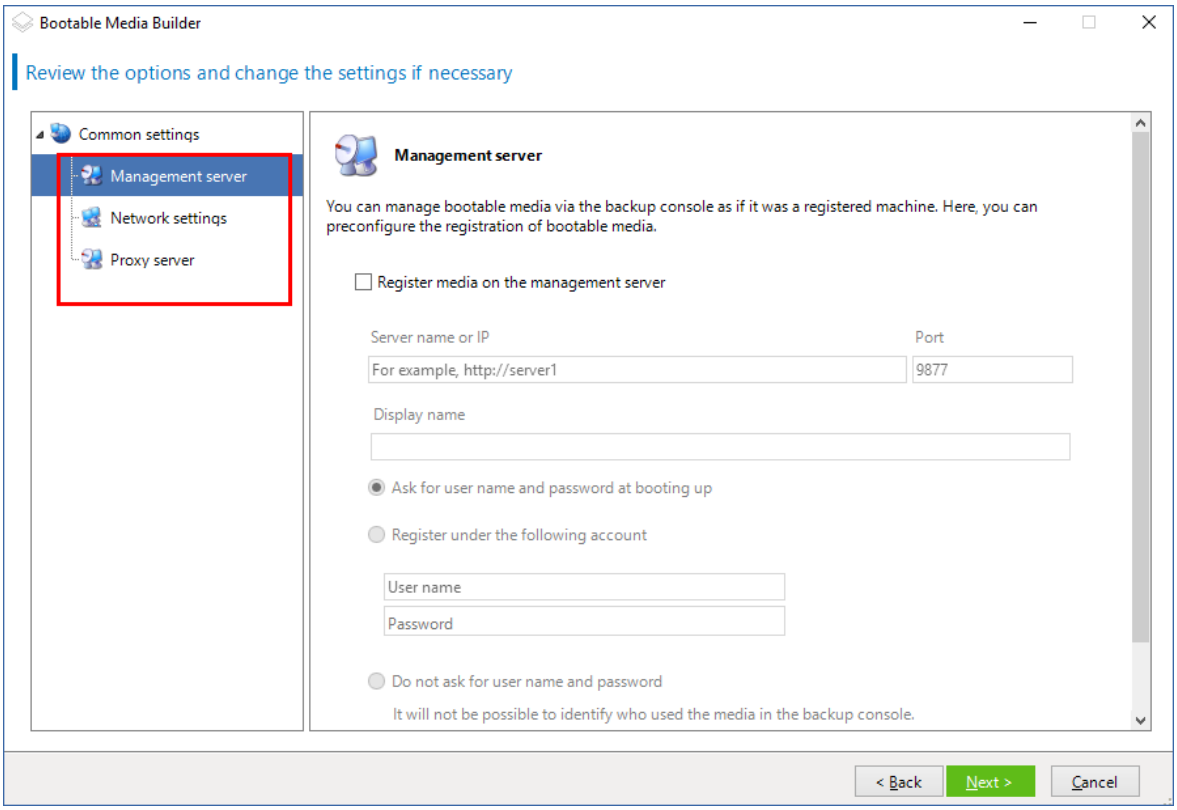
   可開機代理程式可讓您在任何 PC 相容硬體 (包括裸機) 上執行備份、復原及磁碟管理作業。

   Universal Restore 可讓您啟動復原至相異硬體或虛擬機器的作業系統。此工具會針對對於啟動作業系統極為關鍵的裝置 (例如存放控制器、主機板或晶片組)，尋找並安裝驅動程式。
7. [選擇性] 指定開機功能表的逾時間隔，以及逾時的時候將自動啟動的元件。方法是，按一下左上窗格中所需的元件，然後設定其間隔。從 WDS/RIS 開機時，這可讓您自動現場作業。

   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。



8. [選擇性步驟] 如果您想要自動化可開機代理作業，請選擇**使用以下指令碼**核取方塊。然後，選擇指令碼之一並指定指令碼參數。
9. [選擇性步驟] 選擇在開機時要如何在管理伺服器上登錄媒體。如需有關註冊設定的詳細資訊，請參閱管理伺服器。



10. [選擇性步驟] 指定網路設定：要指派給電腦網路介面卡的 TCP/IP 設定。如需詳細資訊，請參閱 "網路設定" (第 322 頁)。
11. [選擇性步驟] 指定網路連接埠：可開機代理程式接聽傳入連線所使用的 TCP 連接埠。
12. 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. 選擇媒體類型。您可以：
    - 建立 ISO 影像。接著，您可以將其燒錄到 CD/DVD；將其用於建立可開機的 USB 快閃磁碟機；或將其連線到虛擬機器。
    - 建立 ZIP 檔案。
    - 將選擇的元件上傳至 Acronis PXE 伺服器。
    - 將選擇的元件上傳至 WDS/RIS。
14. [選擇性步驟] 新增 Windows 系統驅動程式供 Universal Restore 使用。若新增 Universal Restore 至媒體，且已選擇除了 WDS/RIS 以外的媒體，就會出現這個視窗。
15. 若顯示提示，請指定 WDS/RIS 的主機名稱 /IP 位址和認證，或是指定到媒體 ISO 檔案的路徑。
16. 在摘要畫面中檢查您的設定，然後按一下 **[繼續]**。

核心參數

此視窗可讓您指定 Linux 核心的一個或多個參數。啟動可開機媒體時，這些參數將自動套用。

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。

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**

與一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。

建立可開機媒體時預設會指定此參數，但您可以在開機功能表中移除此參數。

若沒有此參數，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

如果希望可開機媒體執行一組判定作業，可指定指令碼，同時在可開機媒體建立器中建立媒體。每次媒體開機時，將執行此指令碼，而不是顯示使用者介面。

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：

- 備份至雲端存儲和從雲儲存復原 (**entire_pc_cloud**)
- 備份至可開機媒體和從可開機媒體復原 (**entire_pc_local**)
- 備份至網路共用和從網路共用復原 (**entire_pc_share**)
- 從雲端存放區復原 (**golden_image**)

腳本可在安裝了可開機媒體建立程式之電腦上的以下目錄中找到：

- 在 Windows 中：%**ProgramData%\Acronis\MediaBuilder\scripts**
- 在 Linux 中：**/var/lib/Acronis/MediaBuilder/scripts/**

備份至雲端存儲和從雲儲存復原

此腳本可將電腦備份至雲端儲存，或從其使用此腳本在雲端儲存中所建立的最近備份復原該電腦。開始時，腳本將提示使用者在備份、復原和啟動使用者介面之間進行選擇。

在可開機媒體開機程式中，指定以下腳本參數：

1. 雲端儲存的使用者名稱和密碼。
2. [選擇性步驟] 腳本用於加密或存取備份的密碼。

備份至可開機媒體和從可開機媒體復原

此腳本可將電腦備份至可開機媒體，或從其使用此腳本在相同媒體中所建立的最近備份復原該電腦。開始時，腳本將提示使用者在備份、復原和啟動使用者介面之間進行選擇。

在可開機媒體開機程式中，指定腳本用於加密或存取備份的密碼。

備份至網路共用和從網路共用復原

此腳本可將電腦備份至網路共用，或從其位於網路共用的最近備份復原該電腦。開始時，腳本將提示使用者在備份、復原和啟動使用者介面之間進行選擇。

在可開機媒體開機程式中，指定以下腳本參數：

1. 網路共用路徑。
2. 網絡共用的使用者名稱和密碼。
3. [選擇性步驟] 備份檔案名稱。預設值為 **[自動備份]**。如果您希望腳本將備份附加到現有備份，或者從採用非預設名稱的備份復原，則將預設值更改為此備份的檔案名稱。

   尋找備份檔案名稱

   a. 在 Cyber Protect Web 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。
4. [選擇性步驟] 腳本用於加密或存取備份的密碼。

從雲端存放區復原

此腳本將從位於雲端儲存中的最近備份復原該電腦。開始時，腳本將提示使用者指定：

1. 雲端儲存的使用者名稱和密碼。
2. 密碼（如果備份已加密）。

建議您在此雲端儲存帳戶下僅儲存一台電腦的備份。否則，如果另一台電腦的備份比當前電腦的備份更新，腳本將選擇較新的電腦的備份。

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	字串	是	要在可開機媒體建立程式中顯示的指令碼名稱。
description	字串	否	要在可開機媒體建立程式中顯示的指令碼說明。
timeout	編號	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	字串	是	**<script_file>.sh** 中使用的變數名稱。
type	字串	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	字串	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	編號 (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)	編號	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)	編號	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	編號	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。

spinner)			
items (僅限 enum)	字串陣列	是	下拉式清單的值。
required (針對 string、multiString、password 和 enum)	編號	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。

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。

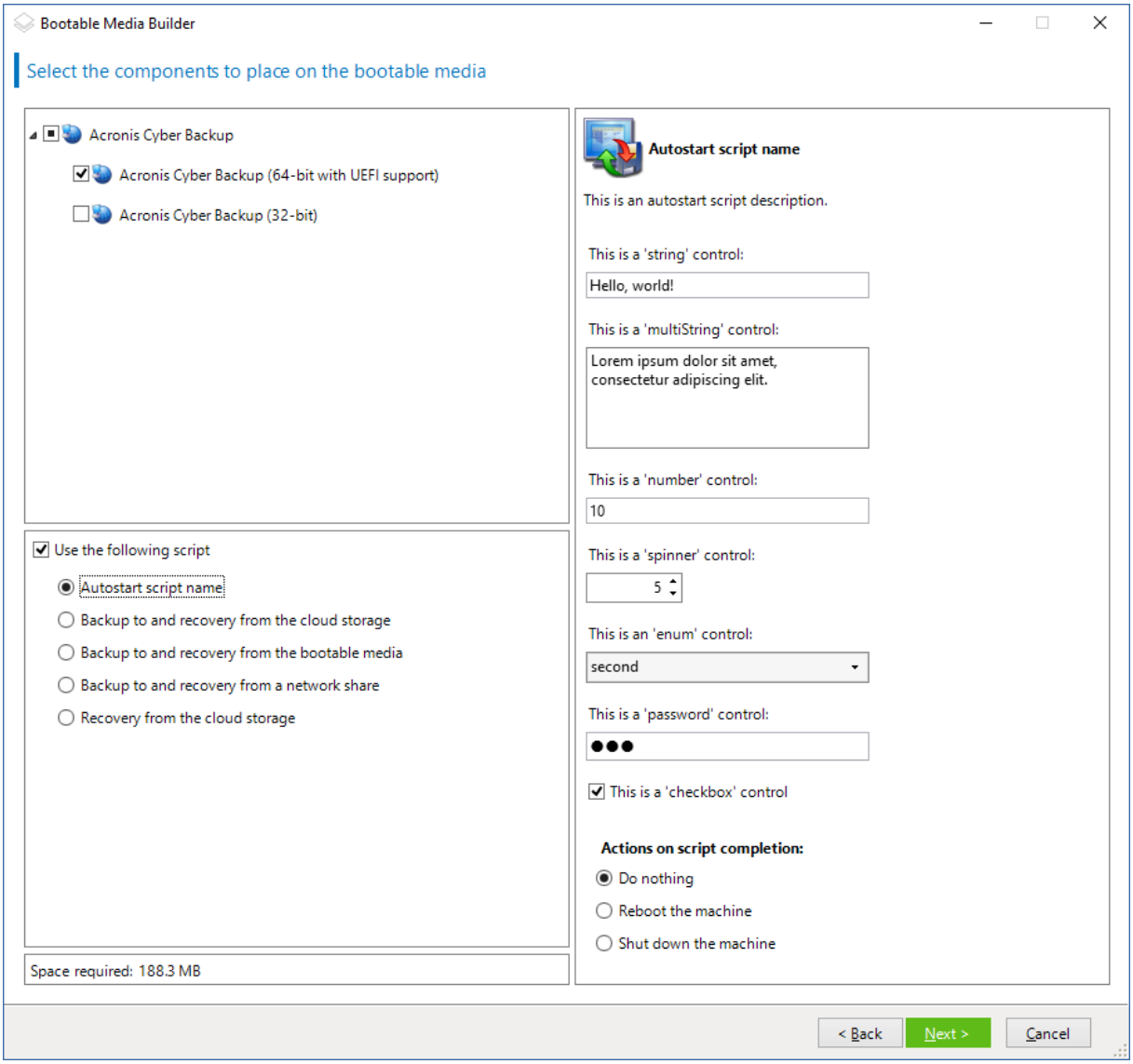
下方的樣本 **autostart.json** 包含可用來設定 **<script_file>.sh** 之變數的所有可能控制類型。

```
{
        "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
    }
```

```
        }
}
```

這是它在可開機媒體建立程式中的顯示方式。



管理伺服器

建立可開機媒體時，您可選擇在管理伺服器上預設定媒體註冊。

註冊媒體可讓您將媒體當作已登錄電腦，以透過 Cyber Protect Web 主控台進行管理。除了方便遠端存取，這還讓系統管理員能夠跟蹤在可啟動媒體下執行的所有作業。作業都記錄在 **[活動]** 中，因此可以查看何人何時開始操作。

如果沒有預設定註冊，在從媒體啟動電腦後仍然可以註冊該媒體。

在管理伺服器上預設定註冊

1. 選取 **[在管理伺服器上註冊媒體]** 核取方塊。
2. 在 **[伺服器名稱或 IP]** 指定已安裝管理伺服器的電腦的名稱或 IP 位址。您可以使用下列其中一種格式：
   - `http://`<伺服器>。例如，`http://10.250.10.10` 或 `http://server1`
   - <IP 地址>。例如，`10.250.10.10`
   - <主機名稱>。例如，`server1` 或 `server1.example.com`
3. 在 **[連接埠]** 中，指定 Web 瀏覽器用來存取管理伺服器的連接埠。預設值為 9877。
4. 在 **[顯示名稱]** 中，指定要在 Cyber Protect Web 主控台中顯示的此電腦的名稱。如果將此欄位留空，則顯示名稱將設定為以下其中一種：
   - 如果之前在管理伺服器上註冊了該電腦，則其將擁有相同的名稱。
   - 否則，將使用該電腦的完整網域名稱 (FQDN) 或 IP 地址。
5. 選擇用於在管理伺服器上註冊媒體的帳戶。您可以選取下列選項：
   - **開機時要求使用者名稱與密碼**

     每次從媒體啟動電腦時都必須提供認證。

     為成功註冊，帳戶必須位於管理伺服器系統管理員 (**[設定]** > **[帳戶]**) 的清單中。在 Cyber Protect Web 主控台中，根據給予指定帳戶的權限，媒體將顯示在組織下或特定單位下。

     在可開機媒體介面中，可以透過按一下 **[工具]** > **[在管理伺服器上註冊媒體]**，變更使用者名稱和密碼。
   - **使用下列帳戶註冊**

     每次從媒體啟動電腦時，會自動註冊電腦。

     您指定的帳戶必須位於管理伺服器系統管理員 (**[設定]** > **[帳戶]**) 的清單中。在 Cyber Protect Web 主控台中，根據給予指定帳戶的權限，媒體將顯示在組織下或特定單位下。

     在可開機媒體介面中，*無法*變更註冊參數。

網路設定

建立可開機媒體時，您可選擇預設定該可開機代理程式將使用的網路連線。下列參數可預設定：

- IP 位址
- 子網路遮罩
- 閘道
- DNS 伺服器
- WINS 伺服器。

當可開機代理程式在電腦上啟動時，該組態將套用於電腦的網路介面卡 (NIC)。若尚未預設定設定，代理程式將使用 DHCP 自動組態。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

您可為多達 10 個網路介面卡預設定 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 NIC 時，其設定被選中儲存在該媒體上。每個現有 NIC 的 MAC 位址也將儲存在該媒體上。

除 MAC 位址外，您可變更任何設定；或在必要時為不存在的 NIC 設定進行設定。

一旦可開機代理程式在伺服器上啟動，它將檢索可用 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頂端。

可開機代理程式為每個已知的 NIC 指定適合的設定，透過其 MAC 位址識別 NIC。在設定包含已知 MAC 位址的 NIC 後，將從上部未指定的 NIC 開始為剩餘的 NIC 指定您為不存在的 NIC 所指定的設定。

您可為任何電腦自訂可開機媒體，而不僅限於在之上建立了媒體的電腦。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 則位於下一個插槽，依此類推。當可開機代理程式在該電腦上啟動時，它將無法找到具有已知 MAC 位址的 NIC 並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。可為此連線進行自動組態。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。

網路埠

建立可開機媒體時，您可選擇預設定可開機代理程式監聽從 acrocmd公用程式傳入連線的網路連接埠。您有下列選擇：

- 預設連接埠
- 當前使用的連接埠
- 新連接埠 (輸入連接埠號)

若該連接埠尚未預設定，代理程式將使用連接埠號 (9876)。

Universal Restore 的驅動程式

建立可開機媒體時，您可選擇將 Windows 驅動程式新增至媒體。Universal Restore 會使用這些驅動程式來啟動已移轉至相異硬體的 Windows。

您將可設定 Universal Restore：

- 在媒體上搜索最適合目標硬體的驅動程式
- 獲得您從媒體上明確指定的大型存放驅動程式。如果目標硬體具有用於硬碟的特定大型存放控制器 (如 SCSI、RAID 或光纖通道介面卡)，則這一選擇非常必要。

這些驅動程式將被置於可開機媒體上的可見 [驅動程式] 資料夾中。驅動程式並未載入到目標電腦的 RAM 中，因此在 Universal Restore 的整個作業過程中，媒體必須保持插入或連線狀態。

當您建立卸除式媒體、其 ISO 或卸離式媒體 (如快閃磁碟機) 時，將能夠為可開機媒體新增驅動程式。無法在 WDS/RIS 上傳驅動程式。

只能以群組形式，透過新增 INF 檔案或包含此類檔案的資料夾，將驅動程式新增至清單。無法從 INF 檔案中選擇單個驅動程式，但是媒體建立器可為您顯示檔案內容。

若要新增驅動程式：

1. 按一下 **[新增]**，並瀏覽至 INF 檔案或包含 INF 檔案的資料夾。
2. 選擇 INF 檔案或資料夾。
3. 按一下 **[確定]**。

只能以群組形式，透過移除 INF 檔案從清單中移除驅動程式。

若要移除驅動程式：

1. 選擇 INF 檔案。
2. 按一下 **[移除]**。

WinPE 可開機媒體

Bootable Media Builder 提供將 Acronis Cyber Protect 與 WinPE 整合在一起的兩種方法：

- 重新建立含外掛程式的 PE ISO。
- 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 Acronis 外掛程式新增至 WIM 檔案。

您不需要任何額外的準備，就可以建立 WinRE 型 PE 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 PE 影像。

WinRE 型 PE 影像

下列作業系統支援建立 WinRE 型影像：

- Windows 7 (64 位元)
- Windows 8、8.1、10 (32 位元及 64 位元)
- Windows Server 2012、2016、2019 (64 位元)

PE 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 for Windows 10)

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。

WinPE 4 及更新版本的 PE 影像需要約 1 GB 的 RAM 才能運作。

注意事項

磁碟管理功能不適用於 Windows PE 4.0 和更新版本的可開機媒體。因此，Windows 7 和更舊的作業系統支援磁碟管理。若要在 Windows 8 和更新版本上執行磁碟管理作業，您需要安裝 Acronis Disk Director。如需詳細資訊，請參閱此 KB 文章：https://kb.acronis.com/content/47031。

準備工作：WinPE 2.x 與 3.x

若要能建立或修改 PE 2.x 或 3.x 影像，請在已安裝 Windows 自動化安裝套件 (WAIK) 的電腦上安裝 Bootable Media Builder。如果您沒有具備 AIK 的電腦，請依以下方式準備：

準備具備 AIK 的電腦

1. 下載並安裝 Windows 自動化安裝套件。

   Windows Vista (PE 2.0) 用自動化安裝套件 (AIK)：

   http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=en

   Windows Vista SP1 與 Windows Server 2008 (PE 2.1) 用自動化安裝套件 (AIK)：

   http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=en

   Windows 7 (PE 3.0) 用自動化安裝套件 (AIK)：

   http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=en

   Windows 7 SP1 (PE 3.1) 用自動化安裝套件 (AIK) 補充：

   http://www.microsoft.com/download/en/details.aspx?id=5188

   您可以在上述連結中找到安裝的系統需求。
2. 選擇性步驟：將 WAIK 燒錄成 DVD 或複製到快閃磁碟機。
3. 從此套件中安裝 Microsoft .NET Framework (NETFXx86 或 NETFXx64，視硬體而定)。
4. 從此套件中安裝 Microsoft Core XML (MSXML) 5.0 或 6.0 Parser。
5. 從此套件中安裝 Windows AIK。
6. 在相同電腦上安裝 Bootable Media Builder。

建議您詳讀 Windows AIK 隨附的說明文件。若要取得說明文件，請從 [開始] 功能表選擇 **[Microsoft Windows AIK] -> [文件]**。

準備工作：WinPE 4.0 及更新版本

若要能夠建立或修改 PE 4 或更新版本影像，請在已安裝 Windows 評定及部署套件 (ADK) 的電腦上安裝 Bootable Media Builder。如果您沒有具備 ADK 的電腦，請依以下方式準備：

準備具備 ADK 的電腦

1. 下載評定及部署套件的安裝程式。

   適用於 Windows 8 (PE 4.0) 的評定及部署套件 (ADK)：http://www.microsoft.com/zh-tw/download/details.aspx?id=30652。

適用於 Windows 8.1 (PE 5.0) 的評定及部署套件 (ADK): http://www.microsoft.com/zh-TW/download/details.aspx?id=39982。

適用於 Windows 10 (PE for Windows 10) 的評定及部署套件 (ADK): https://msdn.microsoft.com/en-us/windows/hardware/dn913721%28v=vs.8.5%29.aspx。

您可以在上述連結中找到安裝的系統需求。

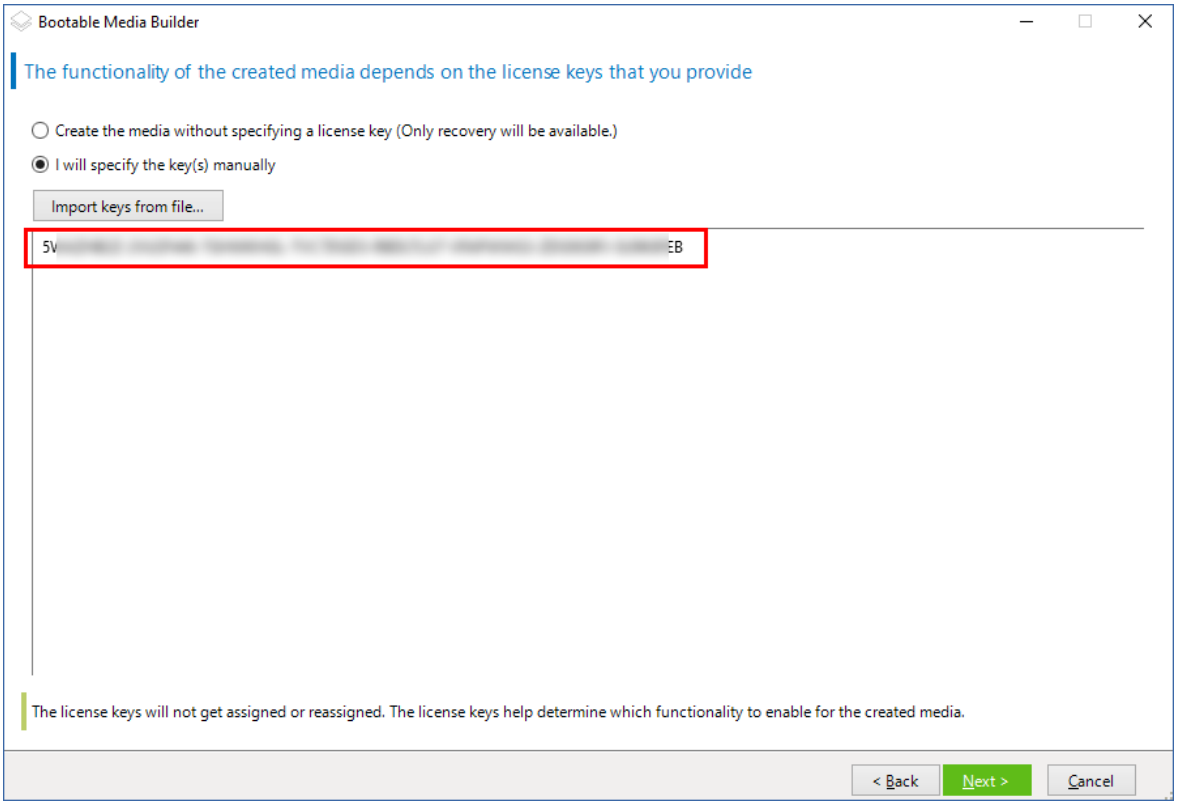
2. 在電腦上安裝評定及部署套件。
3. 在相同電腦上安裝 Bootable Media Builder。

將 Acronis 外掛程式新增至 WinPE

若要將 Acronis 外掛程式新增至 WinPE:

1. 啟動 Bootable Media Builder。
2. 若要建立完整功能的可開機媒體，請指定 Acronis Cyber Protect 授權金鑰。此金鑰用於確定將包含在可開機媒體中的功能。系統將不會從任何電腦撤銷授權。

   如果您未指定授權金鑰，所產生的可開機媒體僅能用於復原作業。



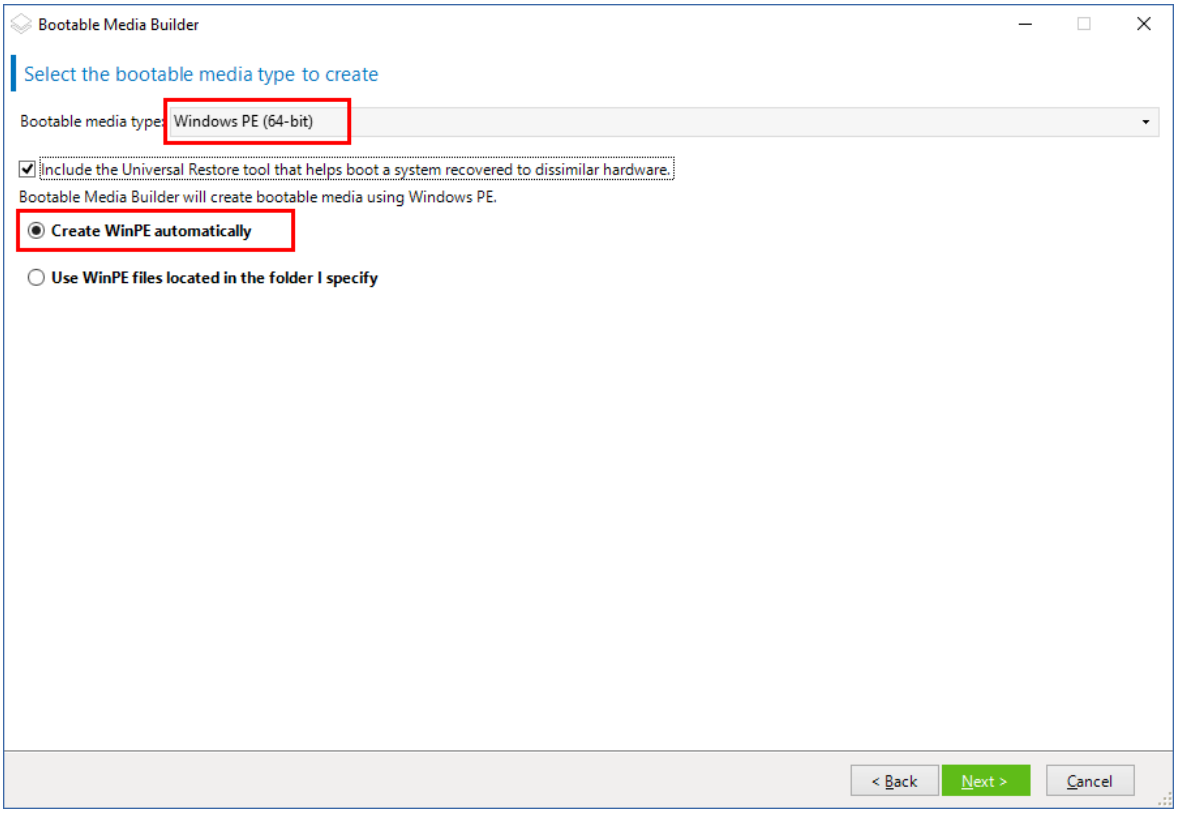
3. 請選擇**可開機媒體類型:Windows PE** 或 **可開機媒體類型:Windows PE(64 位元)**。使用整合可延伸韌體介面 (UEFI) 的電腦需要有 64 位元的媒體才能開機。

   如果您選擇了**可開機媒體類型:Windows PE**，請先進行以下操作:

   - 按一下**下載 WinPE(32 位元)外掛程式**。
   - 儲存外掛程式到 **%PROGRAM_FILES%\Acronis\BootableComponents\WinPE32**。

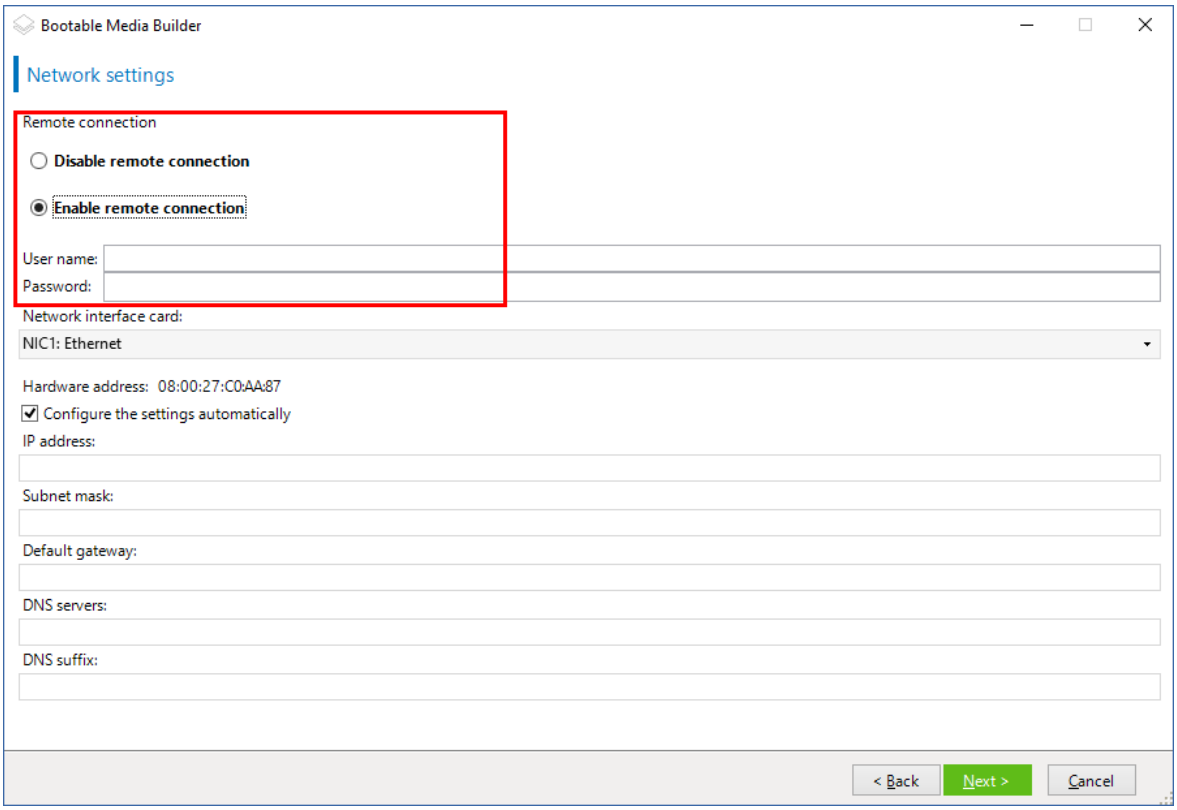
   如果您打算將作業系統復原至相異硬體或虛擬機器，並且希望確保系統的開機能力，請選擇**包含 Universal Restore 工具...**核取方塊。
4. 選擇**自動建立 WinPE**。

軟體將執行適當的指令碼，並前往下一視窗。



5. 選擇將在可開機媒體中使用的語言。
6. 選擇啟用或停用遠端連線至從媒體開機的電腦。如果啟用，且 acrocmd 公用程式是在不同的電腦上執行，請輸入要在命令列中指定的使用者名稱與密碼。您也可以將這些欄位留空，如此就可以在不需要認證的情況下，透過命令列介面進行遠端連線。

   當您在 Cyber Protect Web 主控台的管理伺服器上註冊媒體時，也將需要這些認證。



7. 請為電腦網路卡指定網路設定，或選擇 DHCP 自動設定。

注意事項

網路設定僅適用於 Acronis Cyber Protect 15 個 Advanced 和 Acronis Cyber Protect 15 個 Backup Advanced 授權。如需詳細的功能比較，請參閱這篇知識庫文章。

8. [選擇性步驟] 選擇在開機時要如何在管理伺服器上登錄媒體。如需有關註冊設定的詳細資訊，請參閱管理伺服器。
9. 選擇性步驟：指定要新增至 Windows PE 的 Windows 驅動程式。

   電腦開機進入 Windows PE 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 發行版本，請新增 32 位元驅動程式；若您使用 64 位元 WinPE 發行版本，請新增 64 位元驅動程式。

   此外，您也能在設定 Universal Restore for Windows 時指向新增的驅動程式。若是 Universal Restore，請依據您計劃要復原的 Windows 作業系統為 32 位元還是 64 位元，來新增 32 位元或 64 位元的驅動程式。

   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 媒體中的每個驅動程式重複此程序。
10. 選擇要建立 ISO 或 WIM 影像，或是將媒體上傳到伺服器 (WDS 或 RIS)。
11. 指定產生的影像檔的完整路徑，包括檔案名稱在內，或指定伺服器並提供使用者名稱與密碼以存取該伺服器。
12. 在摘要畫面中檢查您的設定，然後按一下 **[繼續]**。

13. 使用第三方工具將 .ISO 燒錄到 CD 或 DVD，或準備一個可開機的快閃磁碟機。

電腦開機進入 WinPE 時，代理程式將自動啟動。

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:\AcronisMedia.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。

如需自訂 Windows PE 2.x 和 3.x 的更多資訊，請參閱《Windows 預先安裝環境使用者手冊 (Winpe.chm)》。您可在 Microsoft TechNet Library 中找到自訂 Windows PE 4.0 及更新版本的資訊。

連線到從媒體開機的電腦

一旦電腦從可開機媒體開機，電腦終端機將顯示一個啟動視窗，帶有從 DHCP 獲得或根據預設值設定的 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]**。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。

於工作階段期間所做的變更會在電腦重新開機後遺失。

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]**。

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]**。

遠端連線

若要從遠端連接至媒體，請如 < 在管理伺服器上登錄媒體 > 中所述，將其登錄在管理伺服器上。

在管理伺服器上註冊媒體

註冊可開機媒體可讓您將媒體當作已登錄電腦，以透過 Cyber Protect Web 主控台進行管理。這適用於所有可開機媒體，無需考慮開機方式 (實體媒體、Startup Recovery Manager、Acronis PXE Server、WDS 或 RIS)。但是，無法註冊在 macOS 中建立的可開機媒體。

只有在管理伺服器上新增了至少一個 Acronis Cyber Protect Advanced 授權的情況下，才可以註冊媒體。

您可以從媒體 UI 註冊媒體。

可以在可開機媒體開機程式的[管理伺服器]選項中預先設定註冊參數。如果已預先設定所有註冊參數，則媒體將自動出現在 Cyber Protect Web 主控台中。如果預先設定了某些參數，則以下程式中的某些步驟可能不可用。

從媒體 UI 註冊媒體

您可以使用 [可開機媒體建立程式] 來下載或建立媒體。

從媒體 UI 註冊媒體

1. 從媒體啟動電腦。
2. 執行下列其中一項操作：
   - 在啟動視窗中，在 **[管理伺服器]** 下，按一下 **[編輯]**。
   - 在可開機媒體介面中，按一下 **[工具]** > **[在管理伺服器上註冊媒體]**。
3. 在 **[註冊位置]** 指定已安裝管理伺服器的電腦的名稱或 IP 位址。您可以使用下列其中一種格式：
   - `http://`<伺服器>。例如，`http://10.250.10.10` 或 `http://server`
   - <IP 地址>。例如，`10.250.10.10`
   - <主機名稱>。例如，`server` 或 `server.example.com`
4. 在 **[使用者名稱]** 和 **[密碼]** 中，提供位於管理伺服器系統管理員 (**[設定]** > **[帳戶]**) 清單中帳戶的認證。在 Cyber Protect Web 主控台中，根據給予指定帳戶的權限，媒體將顯示在組織下或特定單位下。
5. 在 **[顯示名稱]** 中，指定要在 Cyber Protect Web 主控台中顯示的此電腦的名稱。如果將此欄位留空，則顯示名稱將設定為以下其中一種：
   - 如果之前在管理伺服器上註冊了該電腦，則其將擁有相同的名稱。
   - 否則，將使用該電腦的完整網域名稱 (FQDN) 或 IP 地址。
6. 按一下 **[確定]**。

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備份和復原作業類似。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，將可用代號指派給磁碟區。

   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
   建議您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. 使用可開機媒體建立的備份具有簡化的檔案名稱。唯有備份新增至使用標準檔案命名方式的現有存檔，或目的地不支援簡化的檔案名稱時，才會將標準名稱指派給這些備份。
4. 以類似 Linux 磁碟區表示的可開機媒體無法將備份寫入 NTFS 格式的磁碟區。如有需要，可切換至以類似 Windows 磁碟區表示的媒體。若要切換可開機媒體磁碟區表示方式，按一下 **[工具]** > **[變更磁碟區表示方式]**。
5. 無法排程工作。如果您需要重複作業，則需要從頭開始設定。
6. 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。
7. 集中儲藏庫不會顯示在 **[存檔]** 視窗的資料夾樹狀目錄中。

   若要存取受管理儲藏庫，請在 **[路徑]** 欄位中輸入下列字串：

   bsp://node_address/vault_name/

   若要存取一個不受管理的集中化儲藏庫，請鍵入該儲藏庫資料夾的完整路徑。

   在輸入存取認證之後，您將會看到位於該儲藏庫中的存檔清單。

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，並將適當的模式編號 (在上述範例中為 **vga=0x318**) 輸入 **[核心參數]** 視窗。

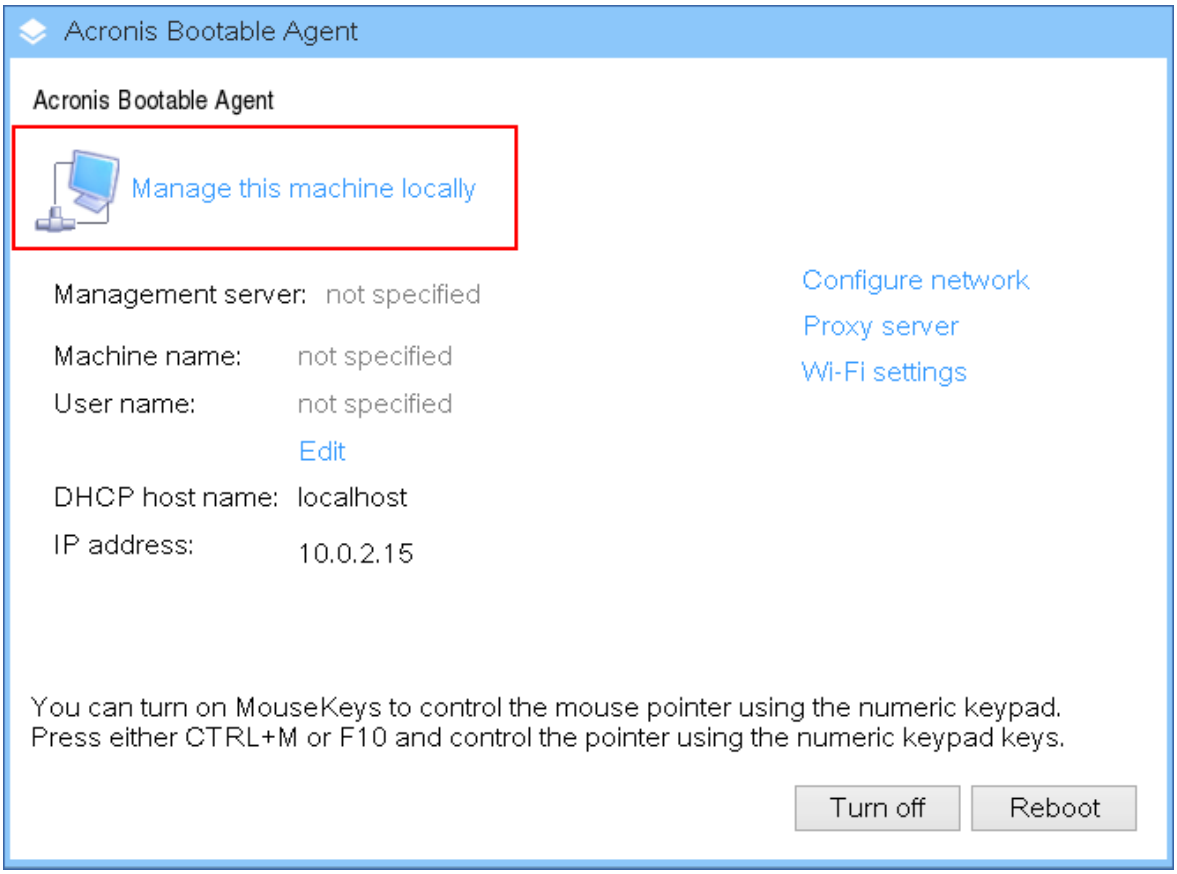
使用內部部署可開機媒體備份

您可以僅利用您使用 Bootable Media Builder 建立，並使用您的 Acronis Cyber Protect 授權金鑰建立的可開機媒體備份資料。如需有關如何建立可開機媒體的詳細資訊，請分別參閱 Linux 可開機媒體或 Windows-PE 可開機媒體。

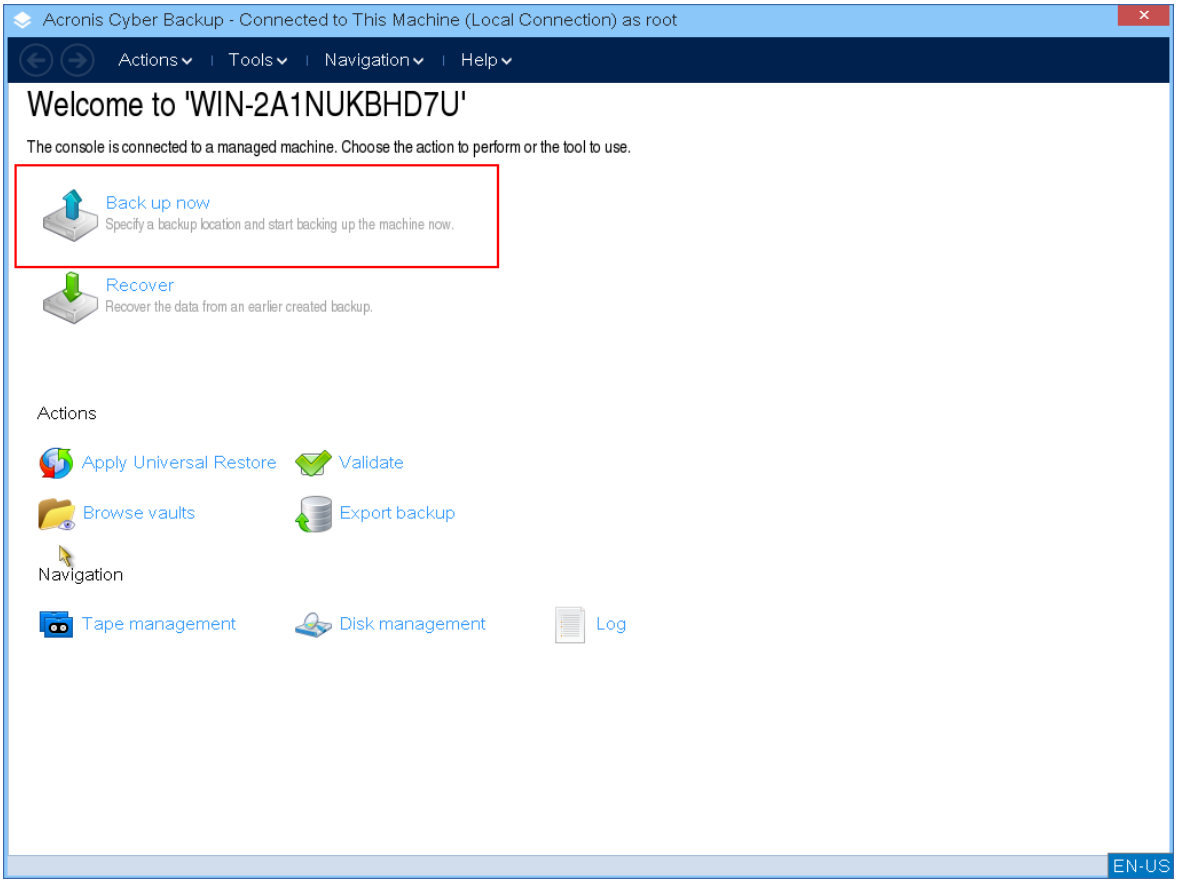
若要在可開機媒體下備份資料

1. 從 Acronis 可開機救援媒體開機。

2. 若要備份本機電腦，按一下 **[在本機管理這部電腦]**。若是遠端連線，請參閱在管理伺服器上註冊媒體。



3. 按一下 **[立即備份]**。

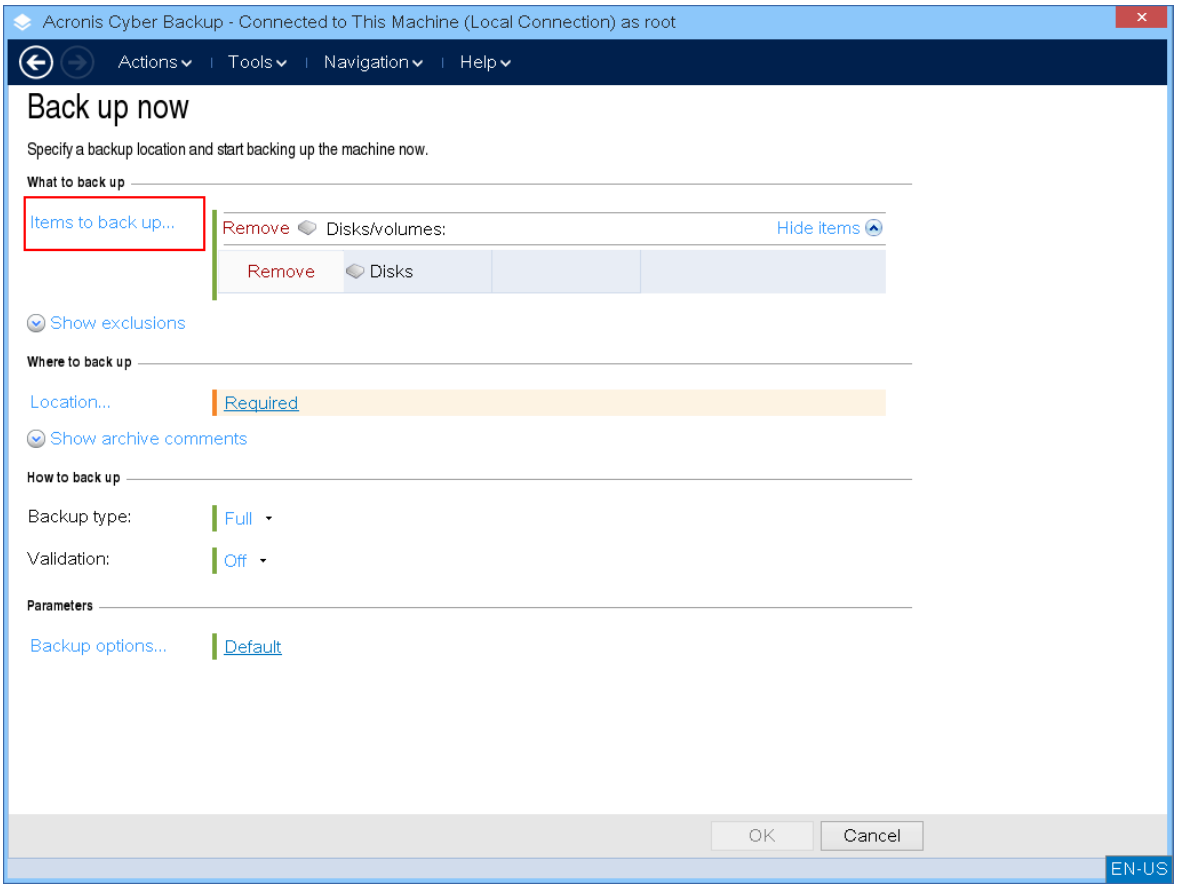


4. 系統會自動選擇電腦的所有非卸除式磁碟進行備份。若要變更將備份的資料，按一下 **[要備份的項目]**，然後選擇所需的磁碟或磁碟區。

   選擇要備份的資料時，您可能會看到下列訊息：「*無法直接選擇此電腦。電腦上已安裝了舊版代理程式。請使用原則規則選擇此電腦以進行備份。*」這是 GUI 問題，您可以安心地忽略。繼續選擇您要備份的個別磁碟或磁碟區。

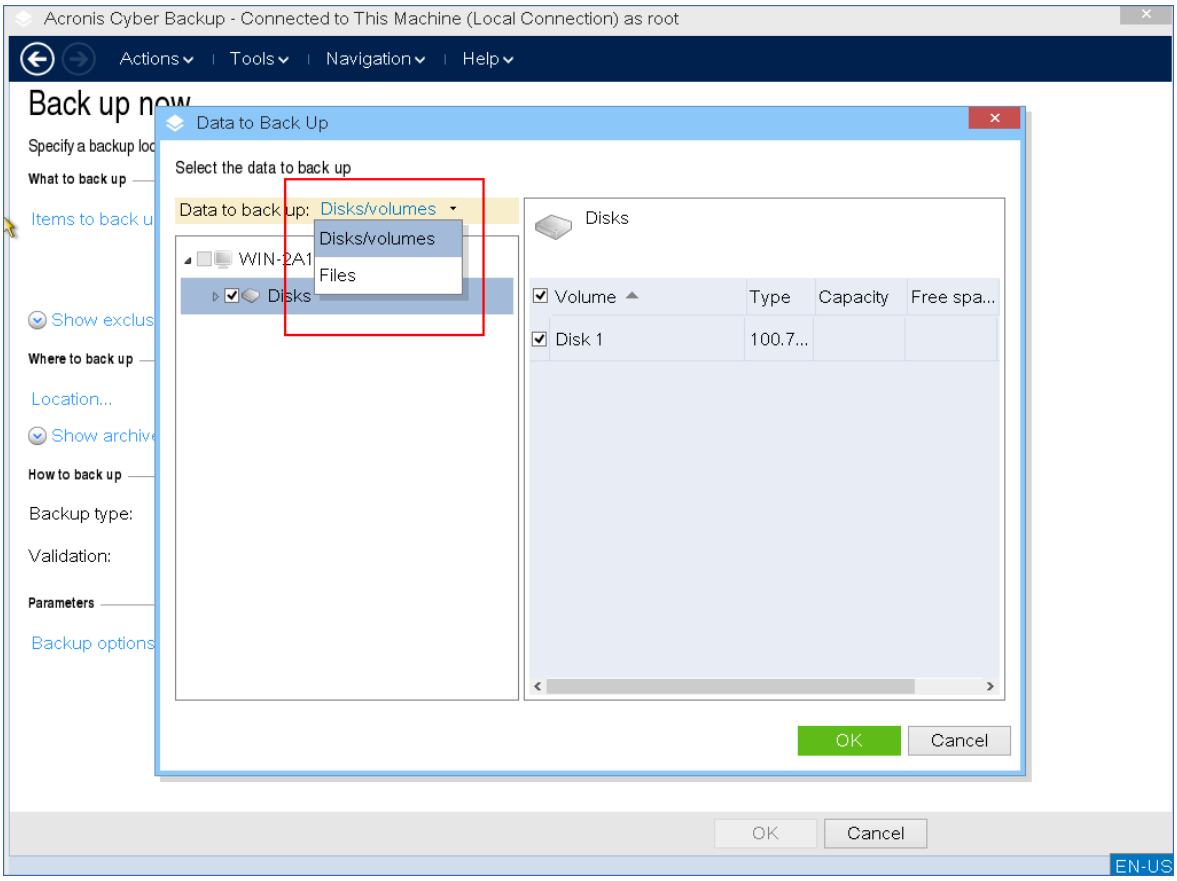
   注意事項

   使用 Linux 可開機媒體時，您可能會看到不同於 Windows 中所看到的磁碟機代號。請試著透過磁碟機或磁碟分割的大小或標籤來識別。

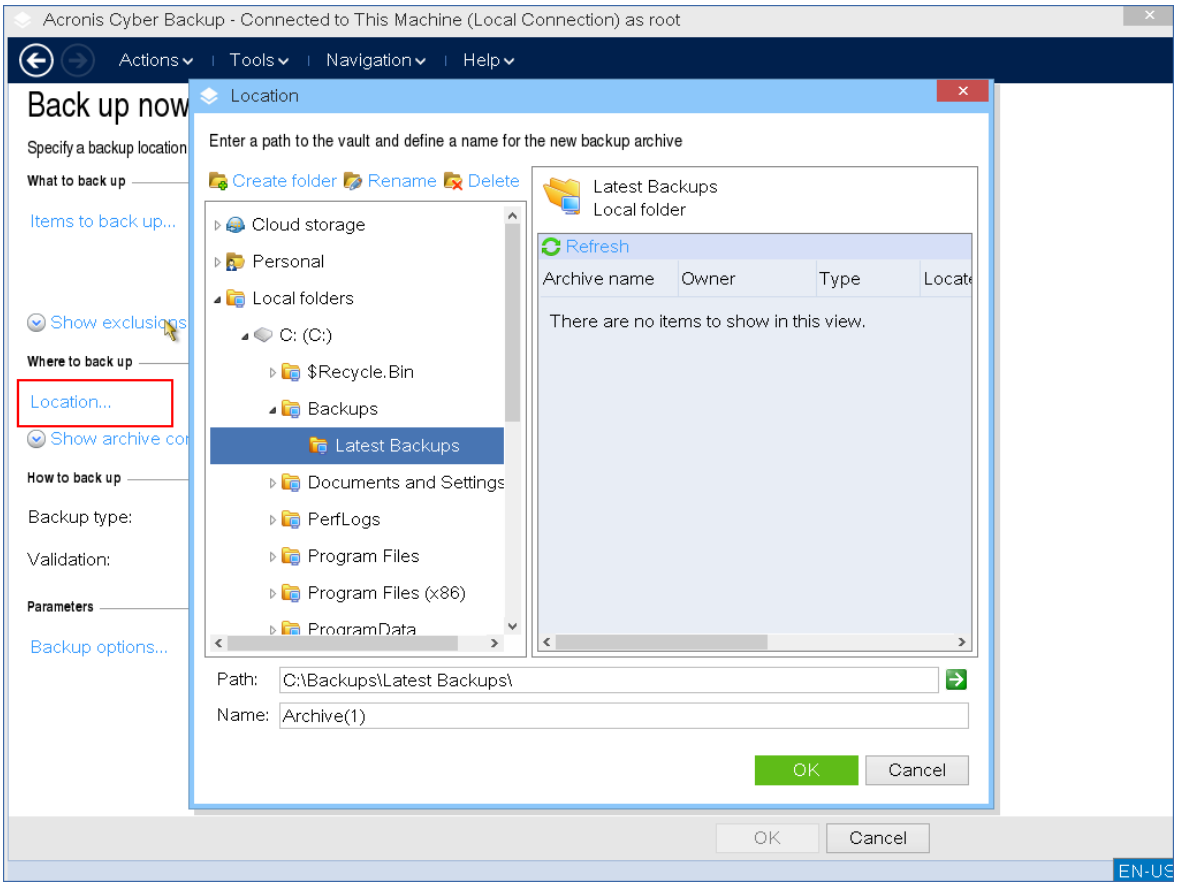


5. 如果您需要備份檔案或資料夾而不是磁碟，請在 **[要備份的資料]** 中，切換到 **[檔案]**。

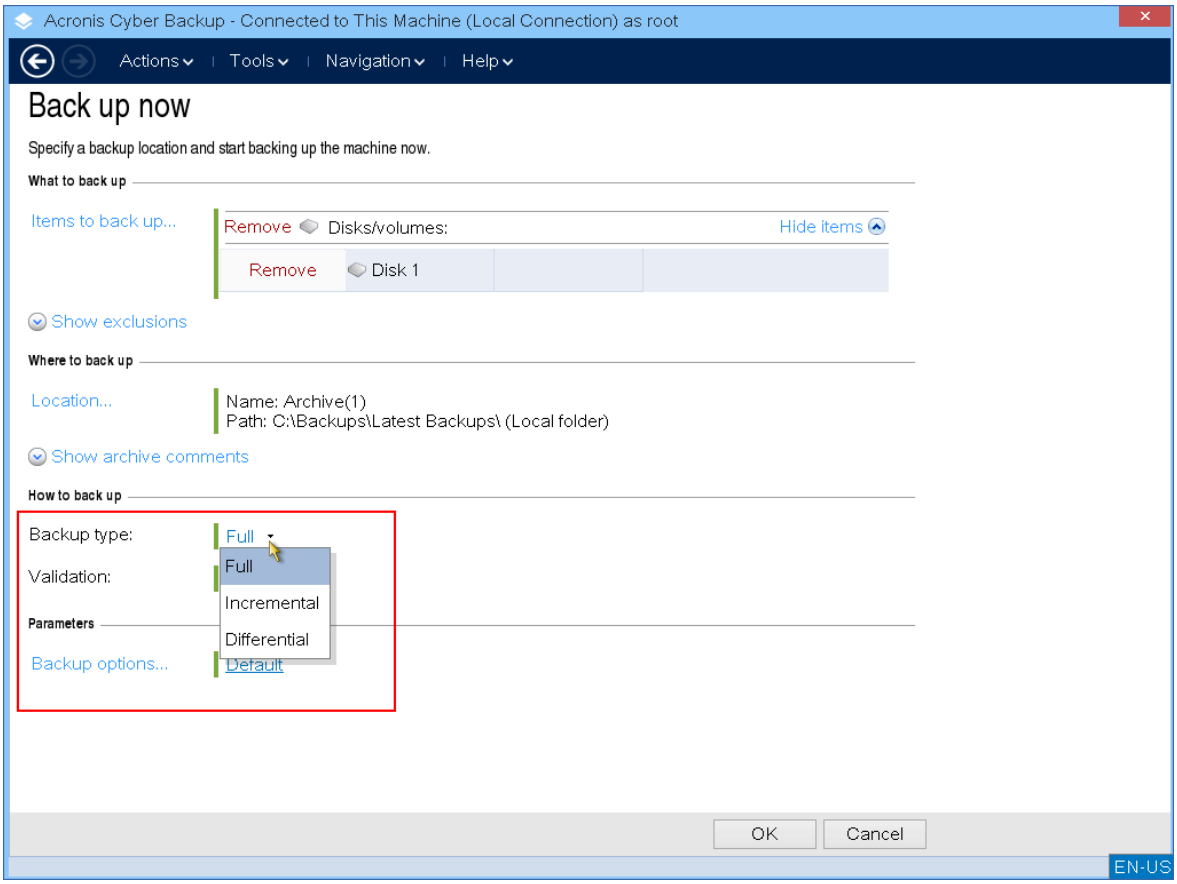
   在可開機媒體下，僅能使用磁碟/磁碟分割和檔案/資料夾備份。其他備份類型 (例如，資料庫備份) 則僅能在執行中的作業系統下使用。



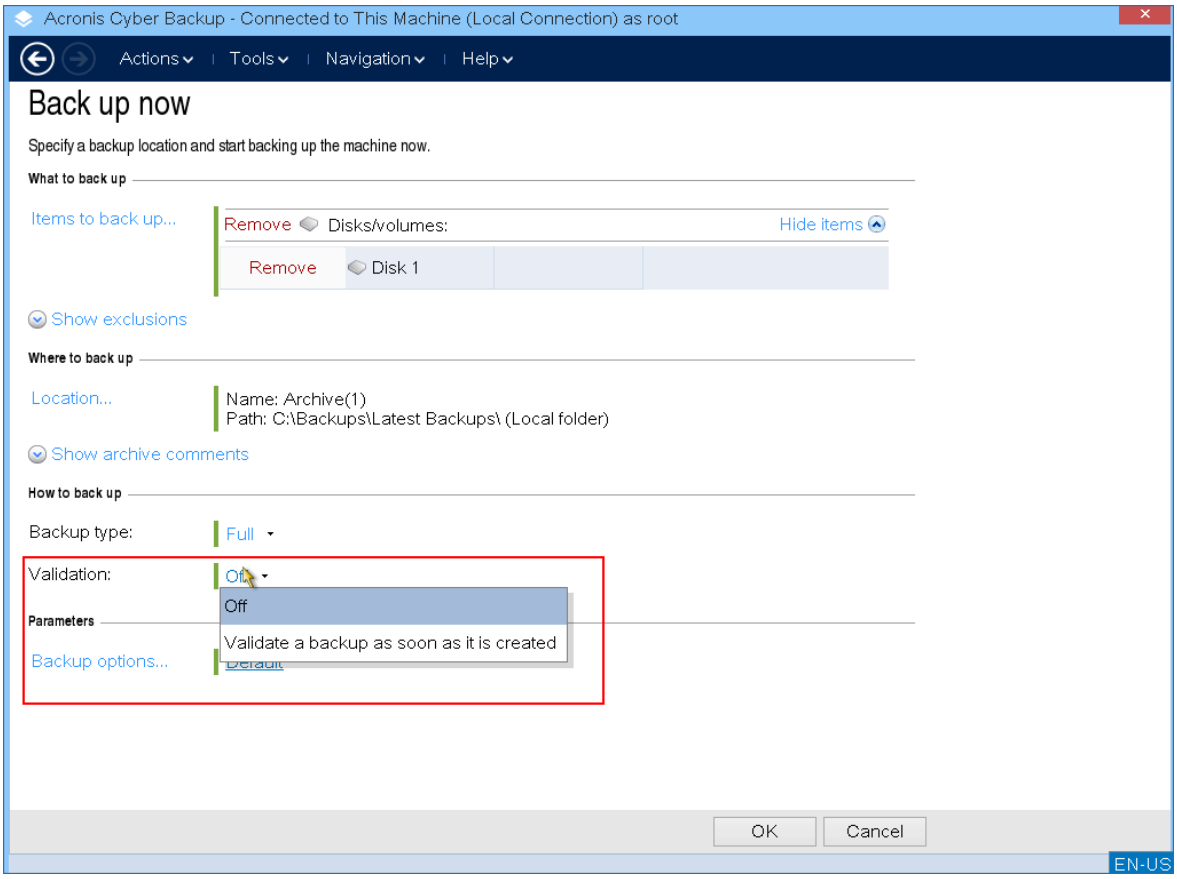
6. 按一下 **[位置]**, 選擇將儲存備份的位置。



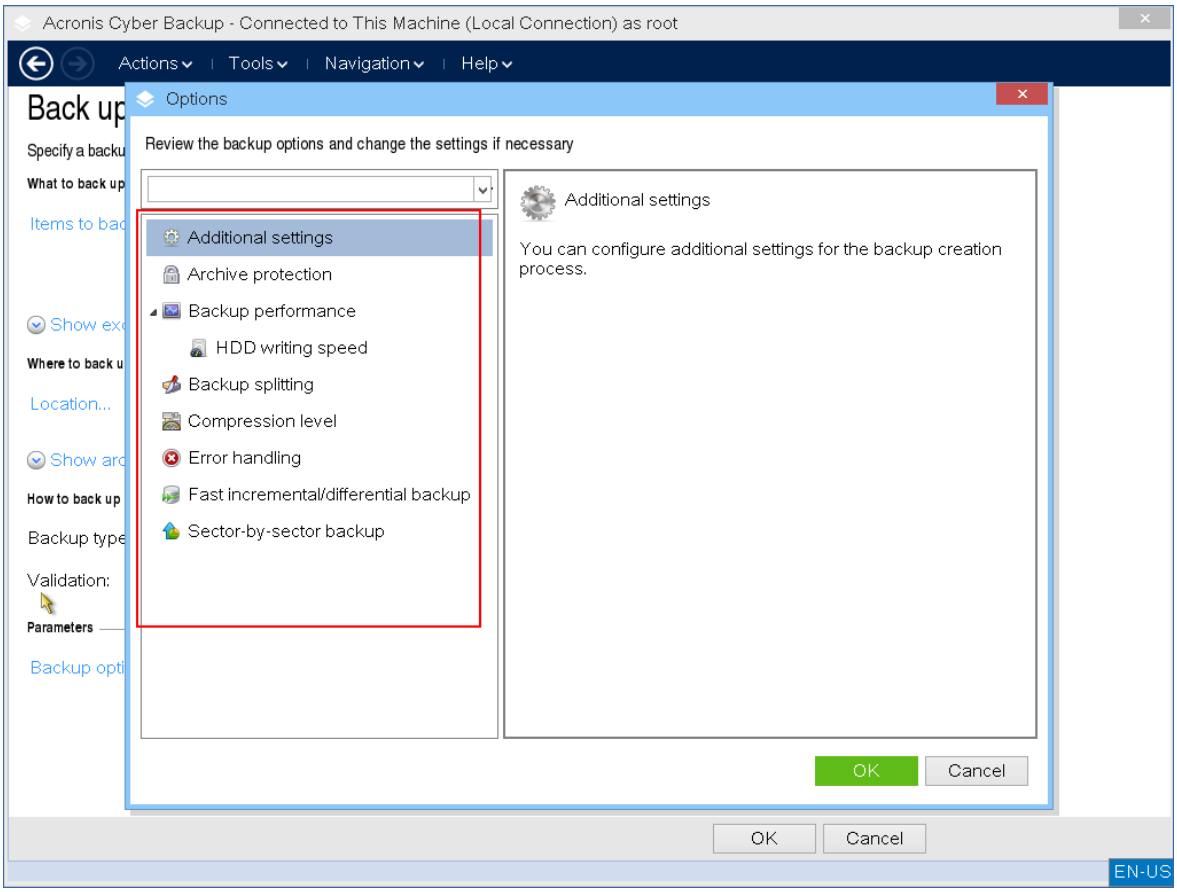
7. 為您的備份指定位置和名稱。
8. 指定備份類型。如果這是此位置中的第一個備份，將建立完整備份。如果您繼續進行一系列的備份，可以選擇 **[增量]** 或 **[差異]**，以節省空間。如需有關備份類型的詳細資訊，請參閱 https://kb.acronis.com/content/1536。



9. [選擇性] 如果您想要驗證備份檔案，選擇 **[備份建立後立即驗證]**。



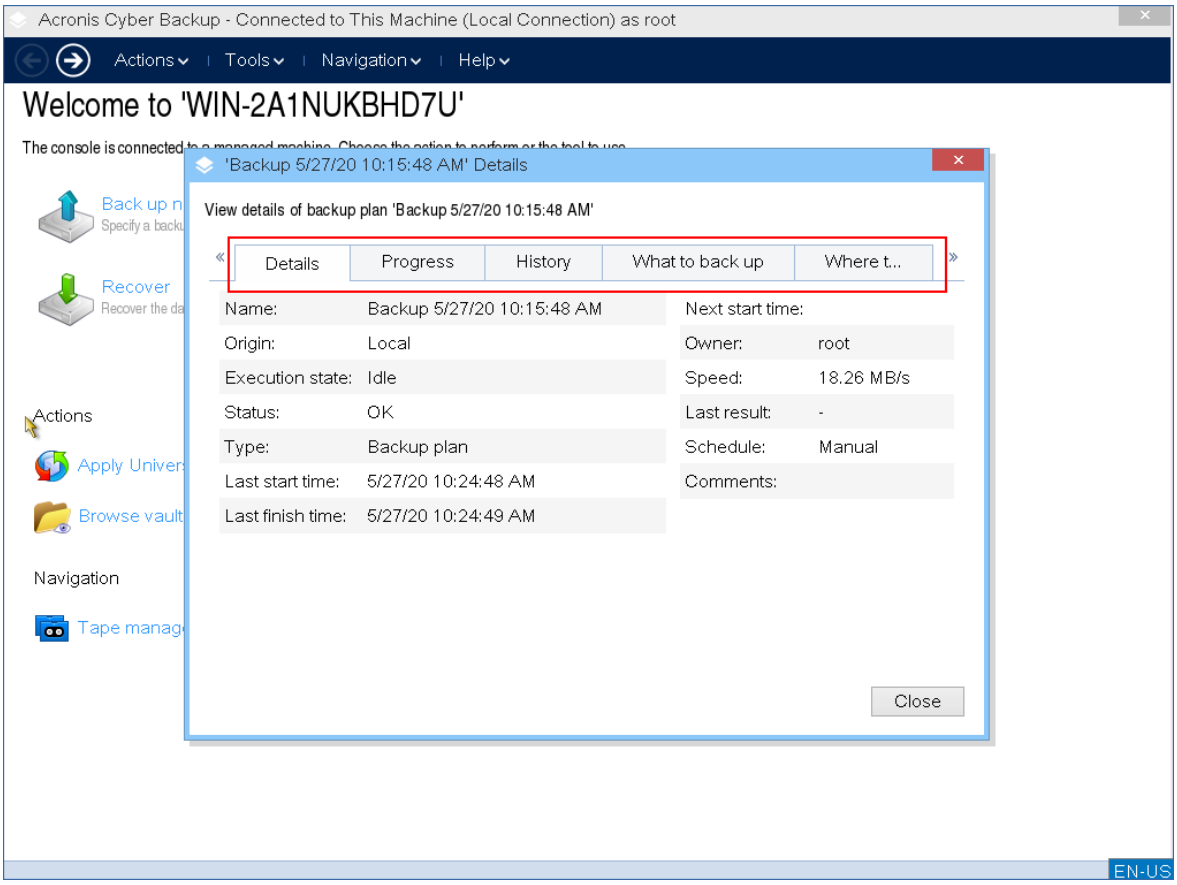
10. [選擇性] 指定您可能需要的備份選項，例如，備份檔案的密碼、備份分割或錯誤處理。



11. 按一下 **[確定]** 開始備份。

    可開機媒體會讀取磁碟中的資料、將其壓縮為 .tib 檔案，然後將這個檔案寫入所選位置。它不會建立磁碟快照，因為沒有執行中的應用程式。

12. 您可以在出現的視窗中檢查備份工作狀態，以及關於備份的其他資訊。

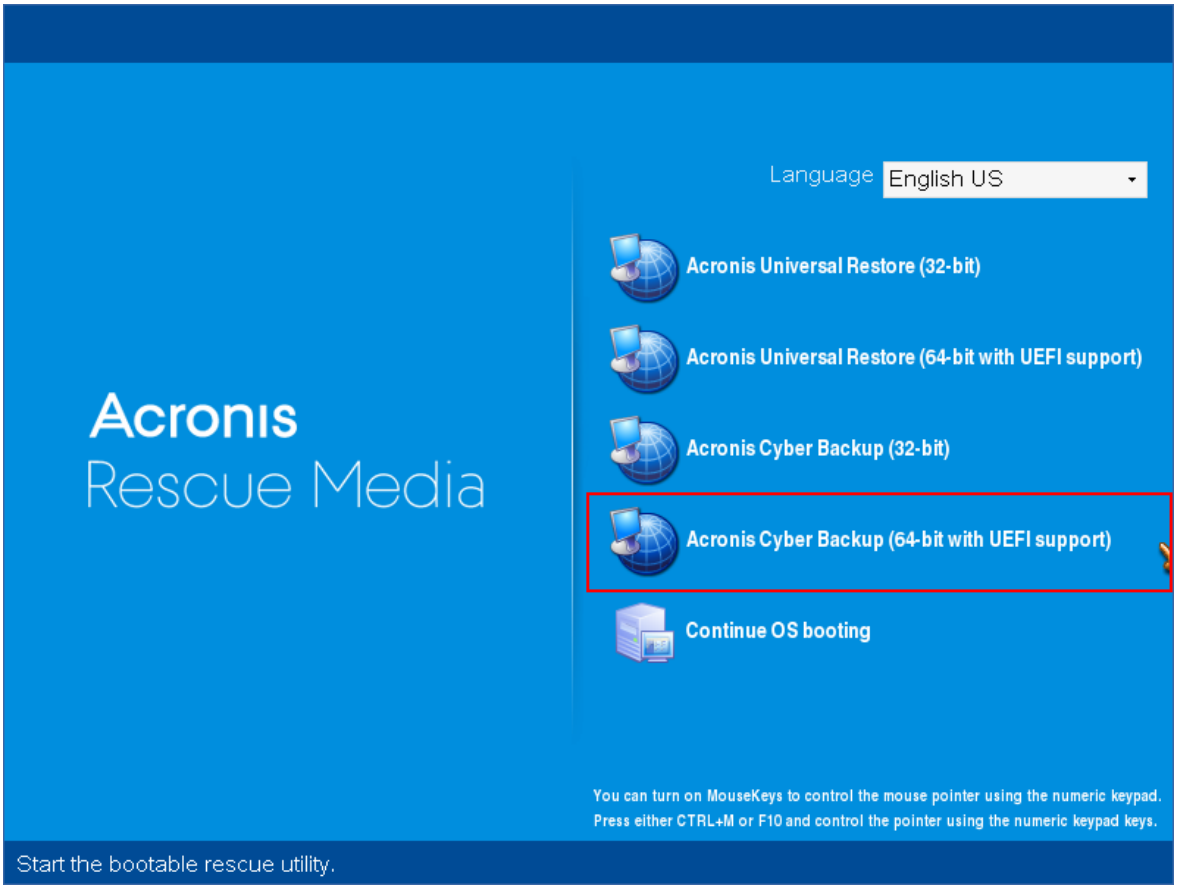


使用內部部署可開機媒體復原

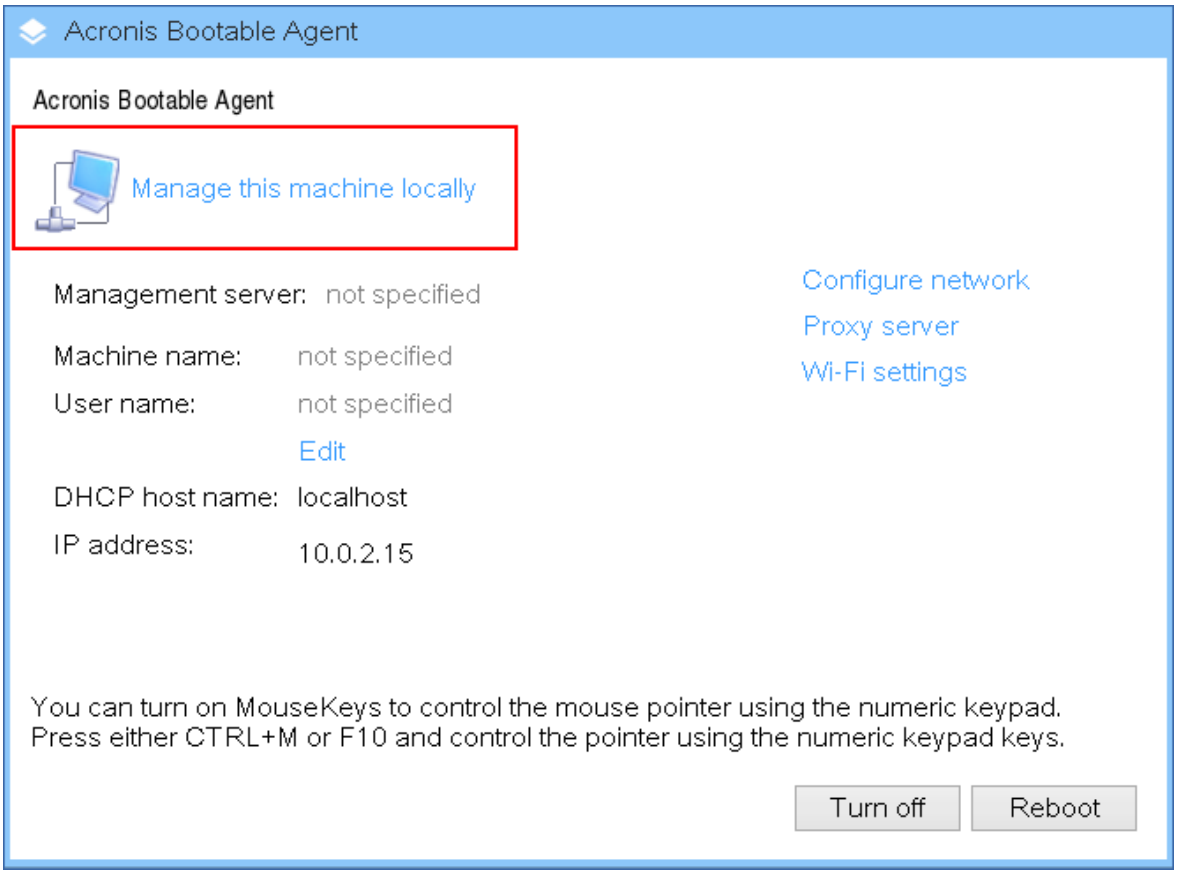
使用 Bootable Media Builder 建立的可開機媒體以及下載的現成可開機媒體都可以使用復原作業。

若要在可開機媒體下復原資料

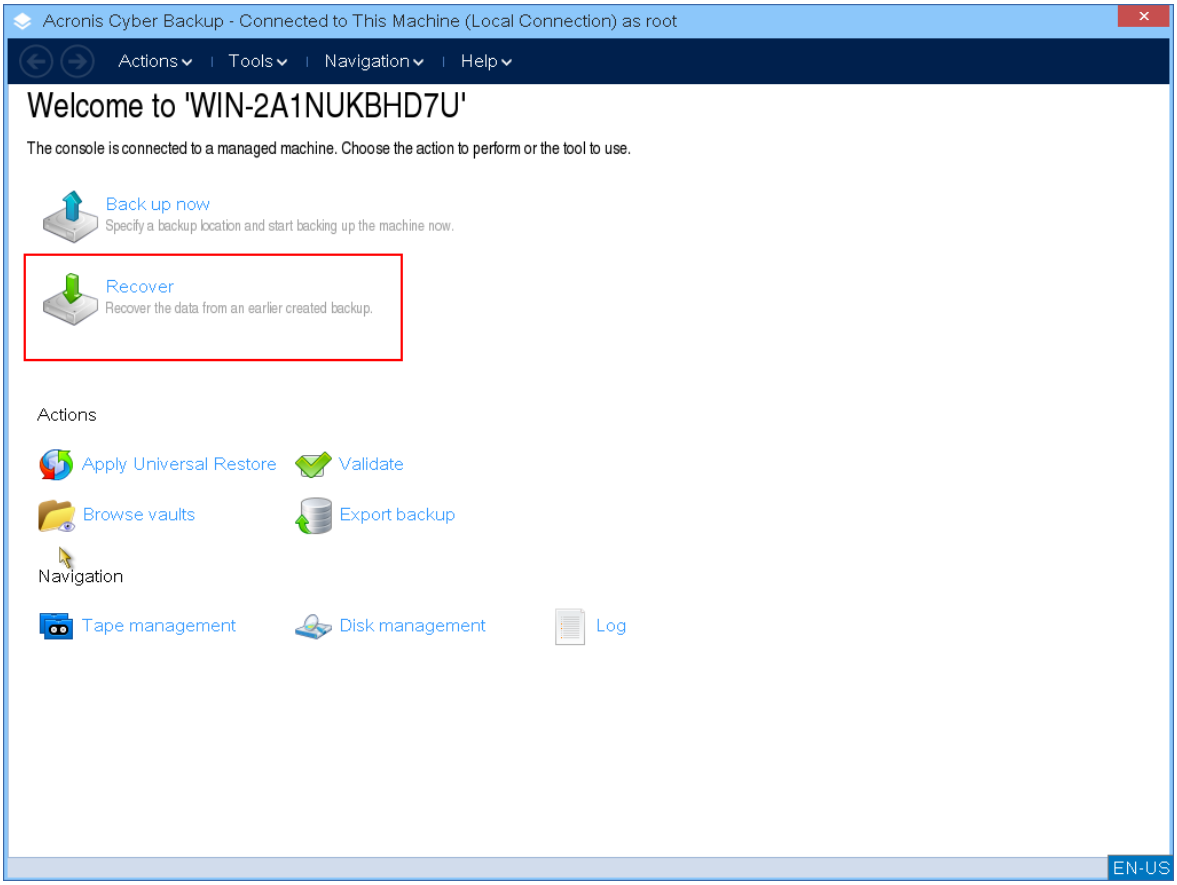
1. 從 Acronis 可開機救援媒體開機。



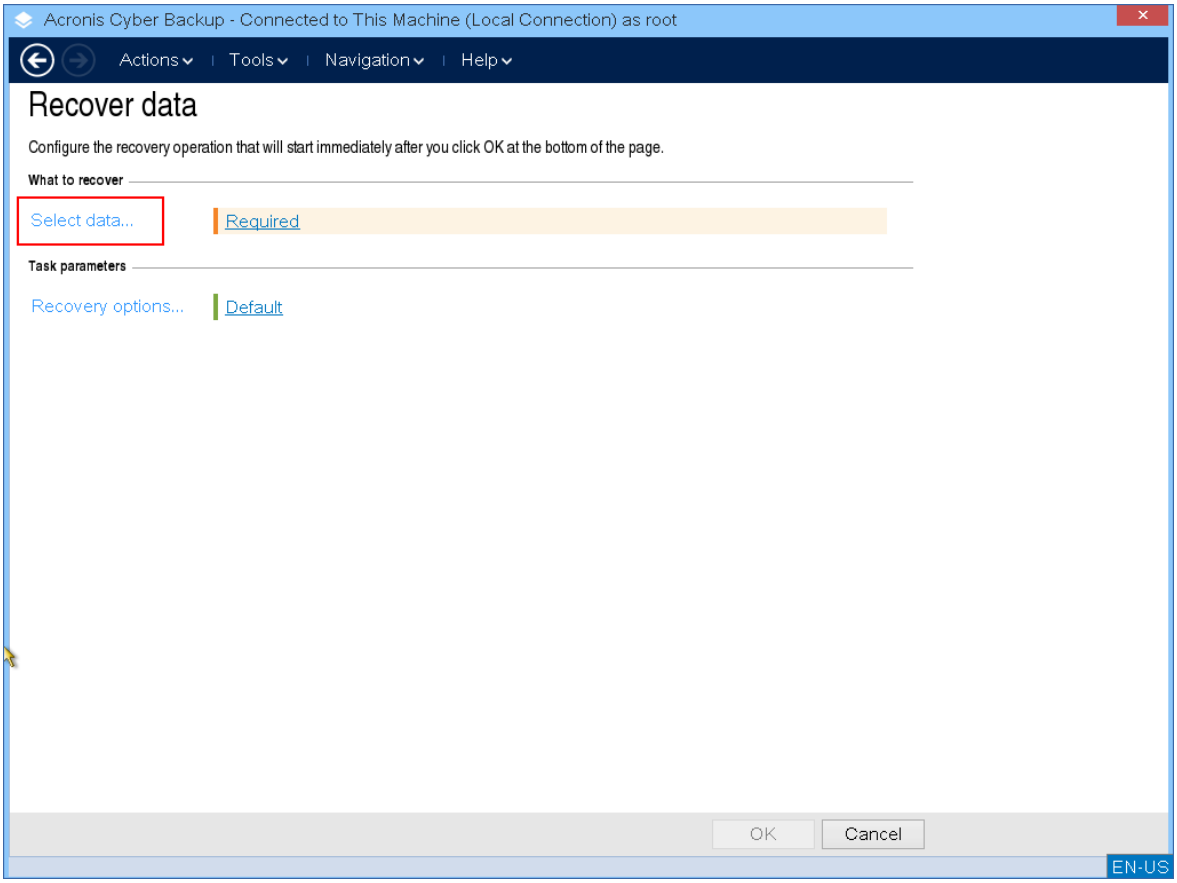
2. 若要將資料復原到本機電腦，按一下 **[在本機管理這部電腦]**。若是遠端連線，請參閱在管理伺服器上註冊媒體。



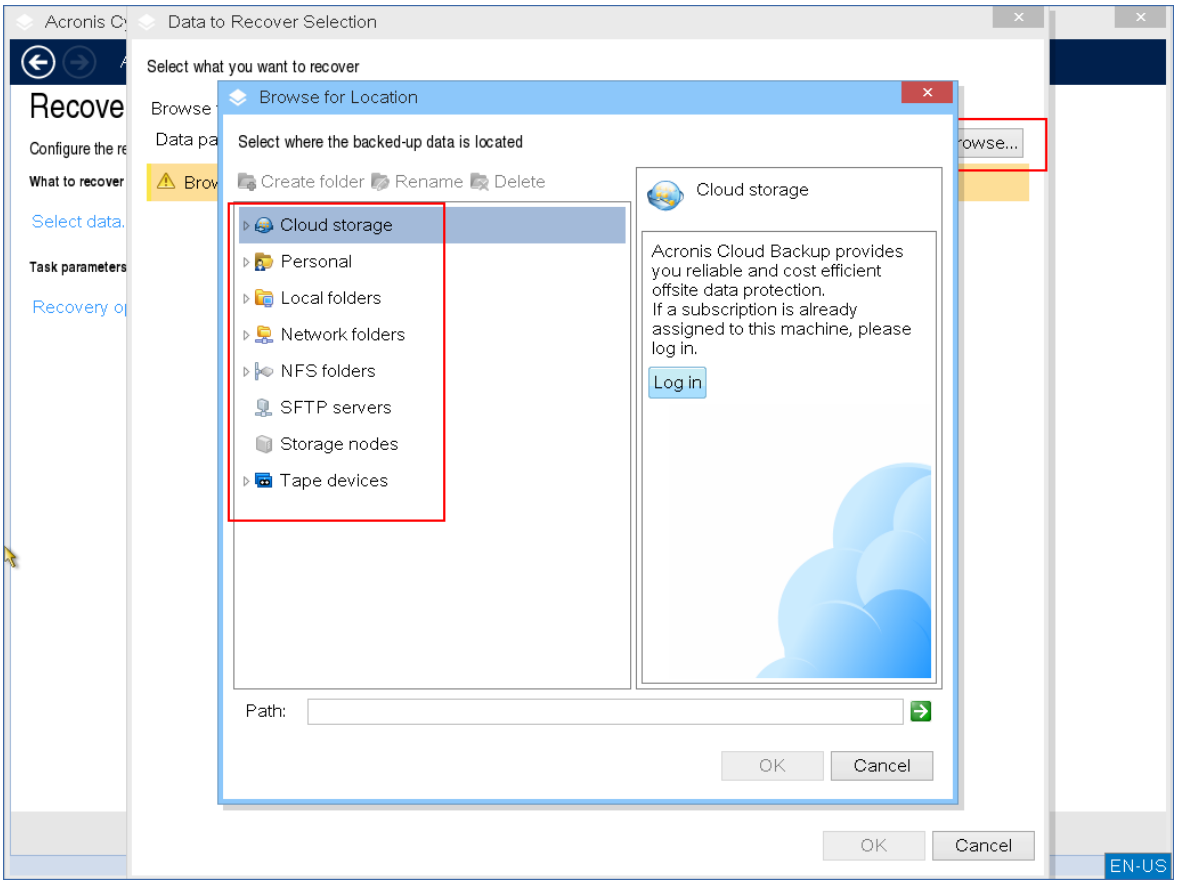
3. 按一下 **[復原]**。



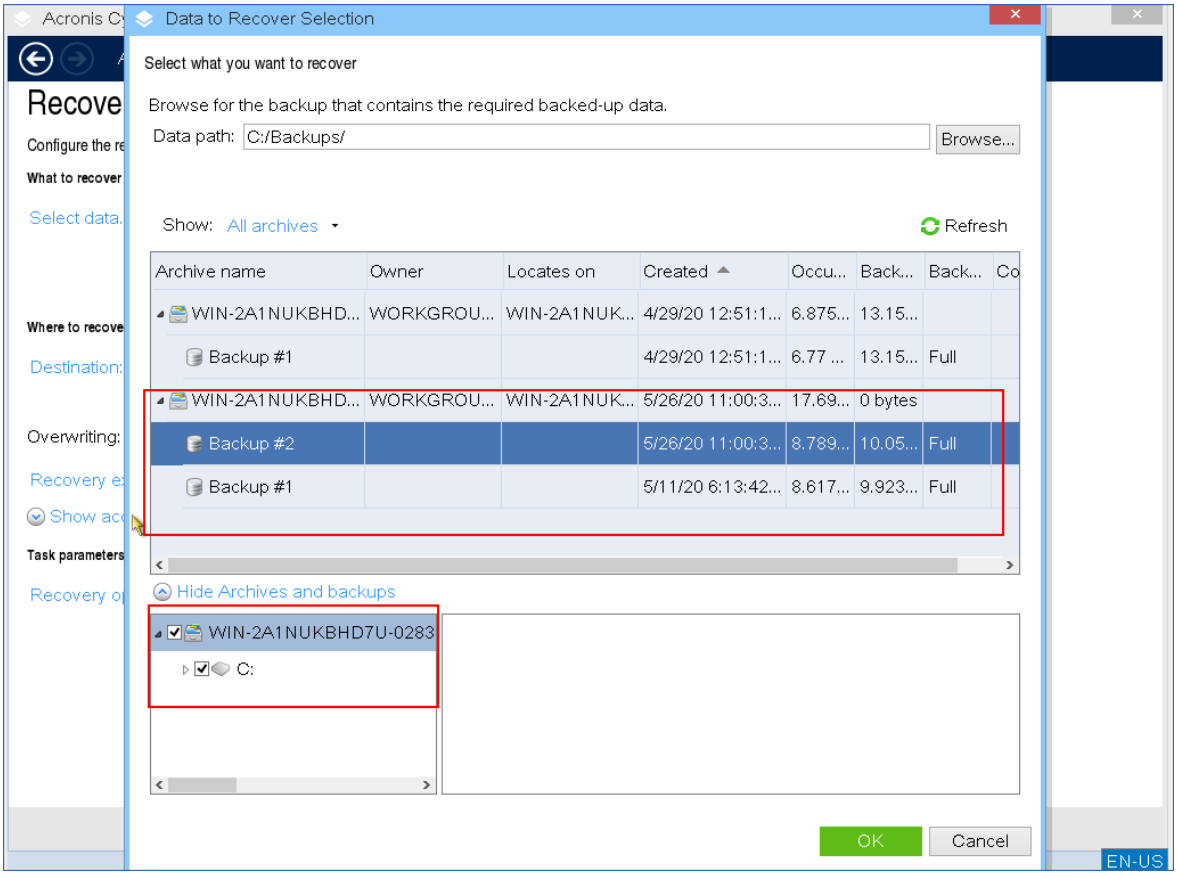
4. 在 **[復原內容]** 中，按一下 **[選擇資料]**。



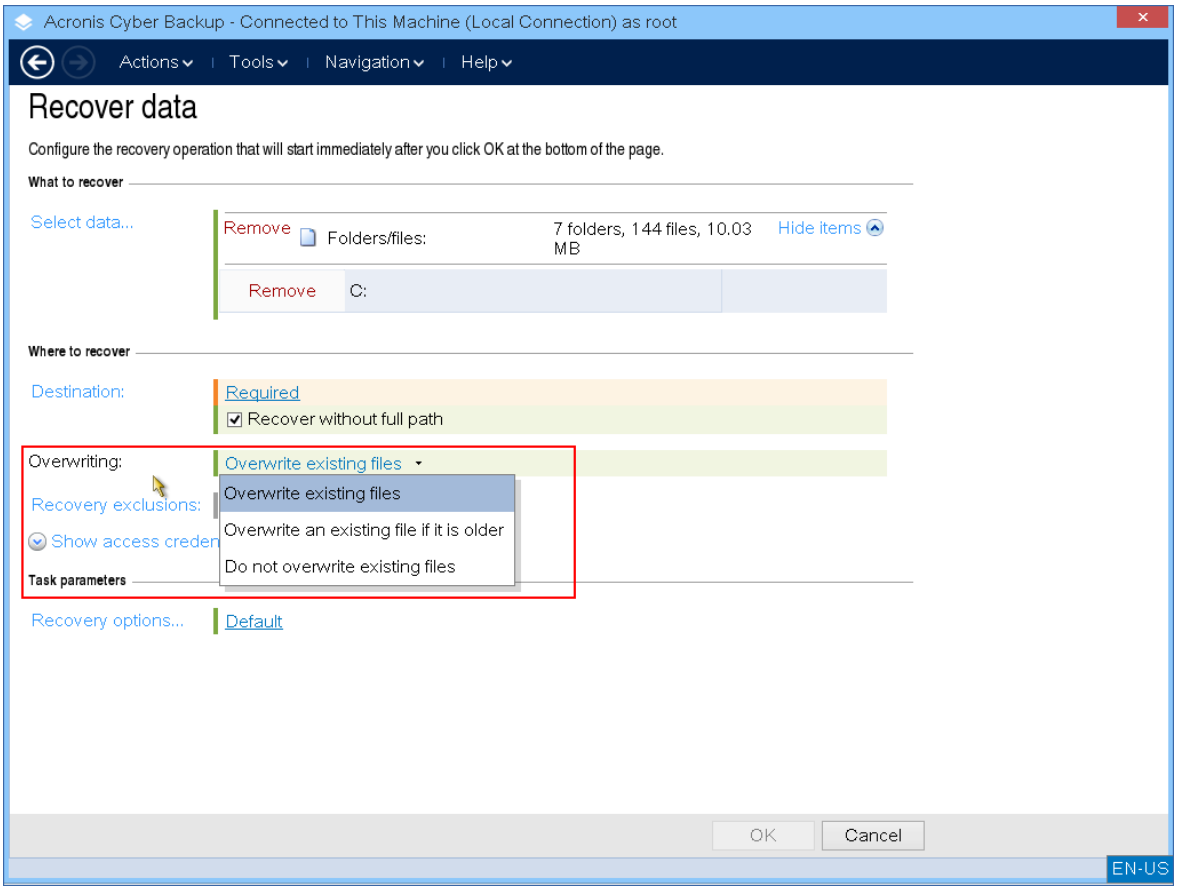
5. 按一下 **[瀏覽]**，然後選擇備份位置。



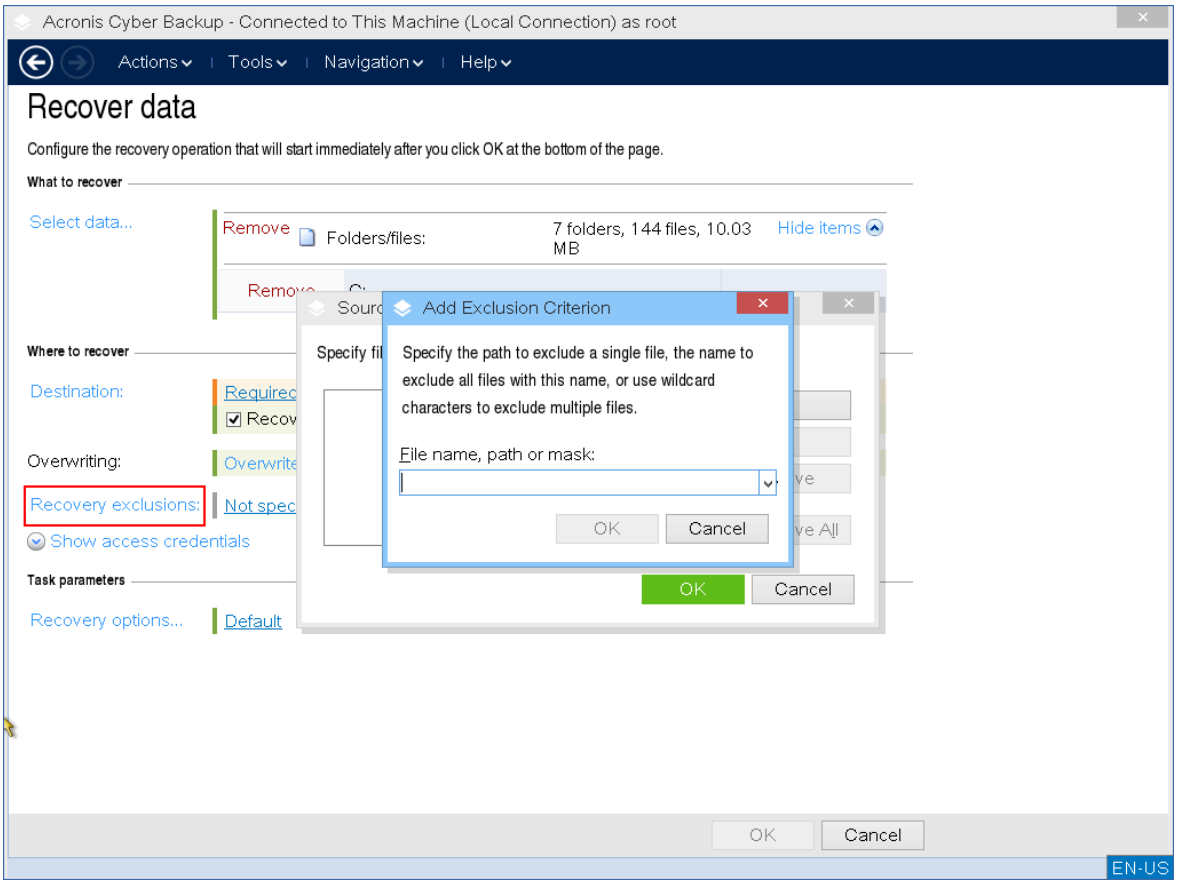
6. 選擇您要復原的來源備份檔案。



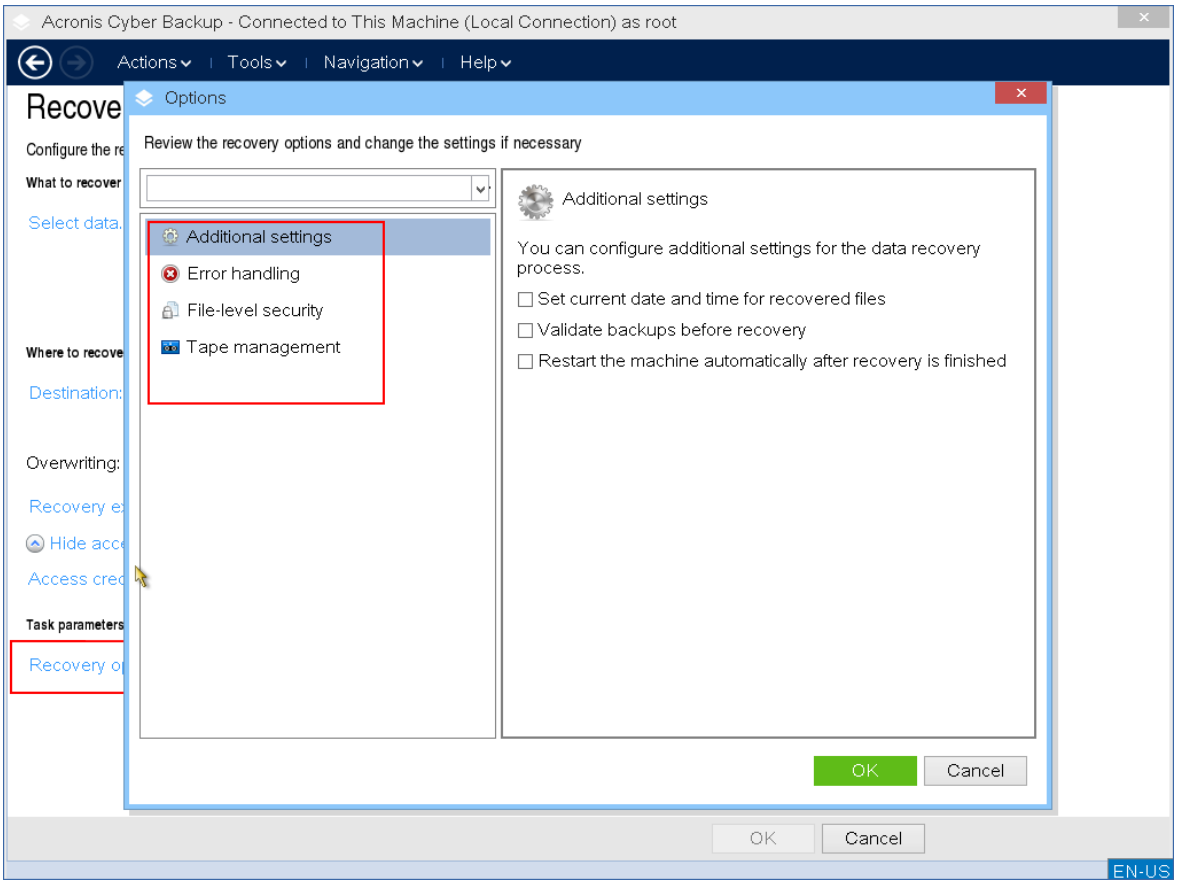
7. 在左下方窗格中，選擇您要復原的磁碟機/磁碟區 (或檔案/資料夾)，然後按一下 **[確定]**。
8. [選擇性] 設定覆寫規則。



9. [選擇性] 設定復原排除。



10. [選擇性] 設定復原選項。



11. 檢查您的設定是否正確，然後按一下 **[確定]**。

注意事項
若要將資料復原到相異硬體，您必須使用 Acronis Universal Restore。
當備份位於 Acronis Secure Zone 時，無法使用 Acronis Universal Restore。

具有可開機媒體的磁碟管理

您可以利用 Acronis 可開機媒體準備磁碟/磁碟區組態，以便復原使用 Acronis Cyber Protect 備份的磁碟區影像。

有時在磁碟區經過備份並且其影像放置於安全的儲存裝置中後，電腦磁碟組態可能因 HDD 更換或硬體遺失而變更。在這種狀況下，您可以重新建立所需的磁碟組態，以便將磁碟區影像完全「按照原狀」復原，或以您認為必要的一些磁碟或磁碟區結構變更復原。

為避免可能的資料遺失，請採取所有必要的預防措施。

重要事項
在磁碟和磁碟區上進行的所有作業都有一定的資料損毀風險。必須非常小心地在系統、可開機或資料磁碟區上執行作業，以免開機過程或硬碟資料儲存出現任何可能的問題。
對硬碟和磁碟區進行作業需要花費一些時間，在這個程序中，斷電、不小心關閉電腦或意外按下 Reset 按鈕都可能導致磁碟區損毀和資料遺失。

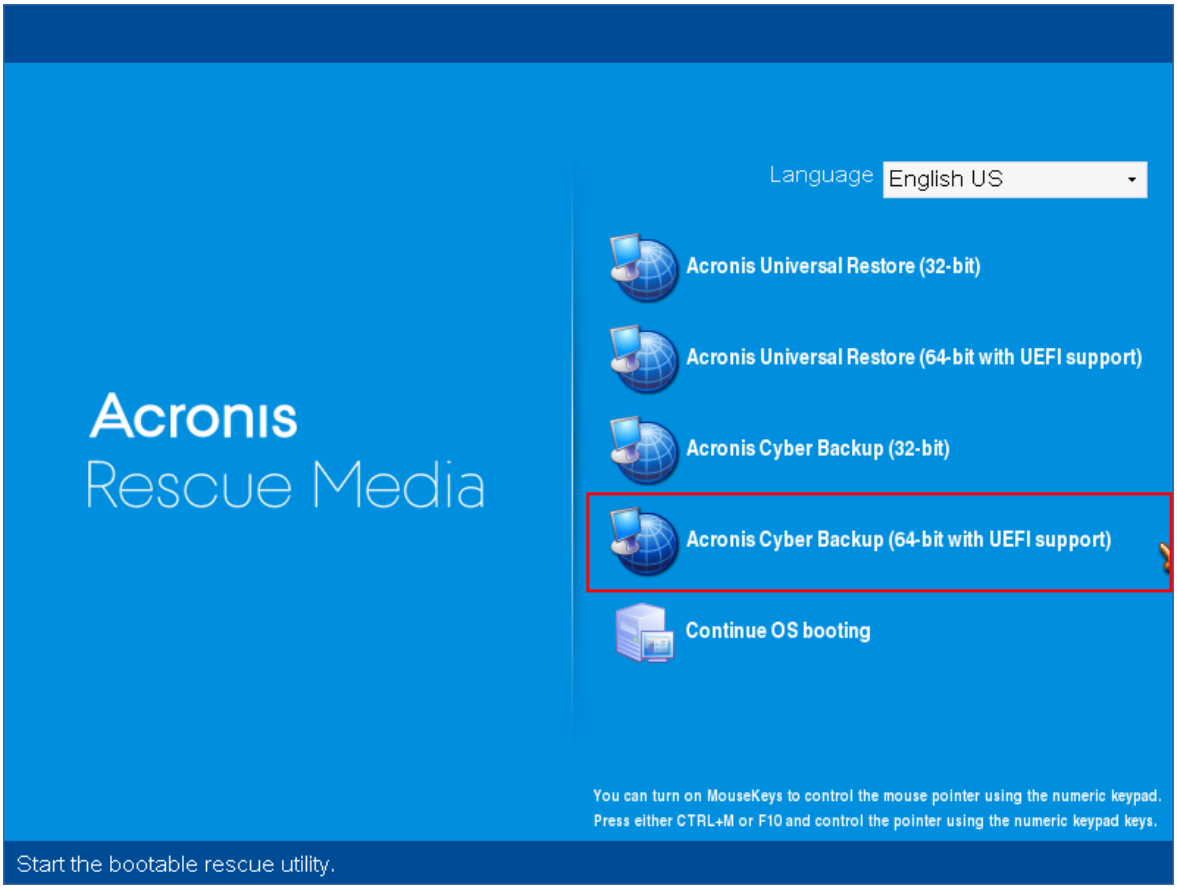
您可以在裸機、無法開機的電腦或非 Windows 系統的電腦上執行磁碟管理作業。您將需要一個您使用 Bootable Media Builder 建立，並使用您的 Acronis Cyber Protect 授權金鑰的可開機媒體。如需有關如何建立可開機媒體的詳細資訊，請分別參閱 Linux 可開機媒體或 Windows-PE 可開機媒體。

注意事項

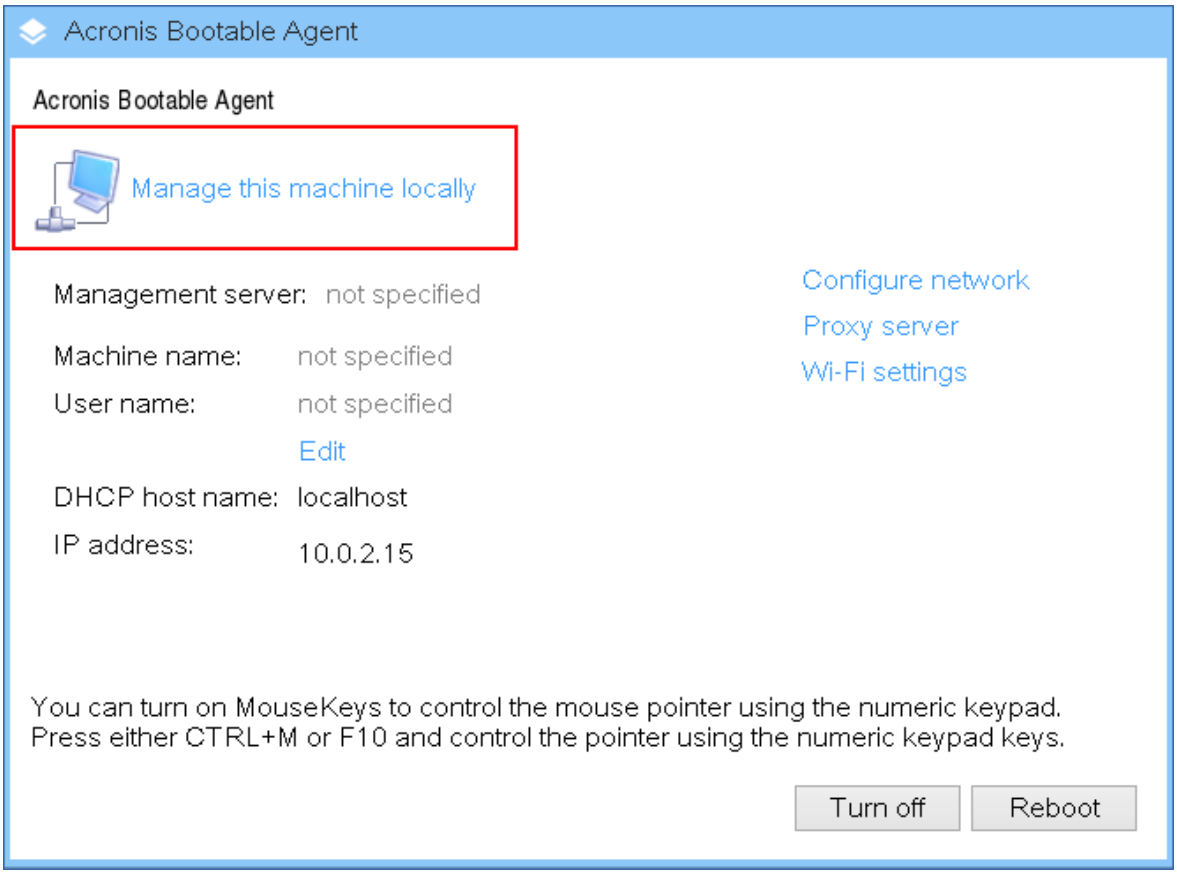
磁碟管理功能不適用於 Windows PE 4.0 和更新版本的可開機媒體。因此，Windows 7 和更舊的作業系統支援磁碟管理。若要在 Windows 8 和更新版本上執行磁碟管理作業，您需要安裝 Acronis Disk Director。如需詳細資訊，請參閱此 KB 文章：https://kb.acronis.com/content/47031。

若要執行磁碟管理作業

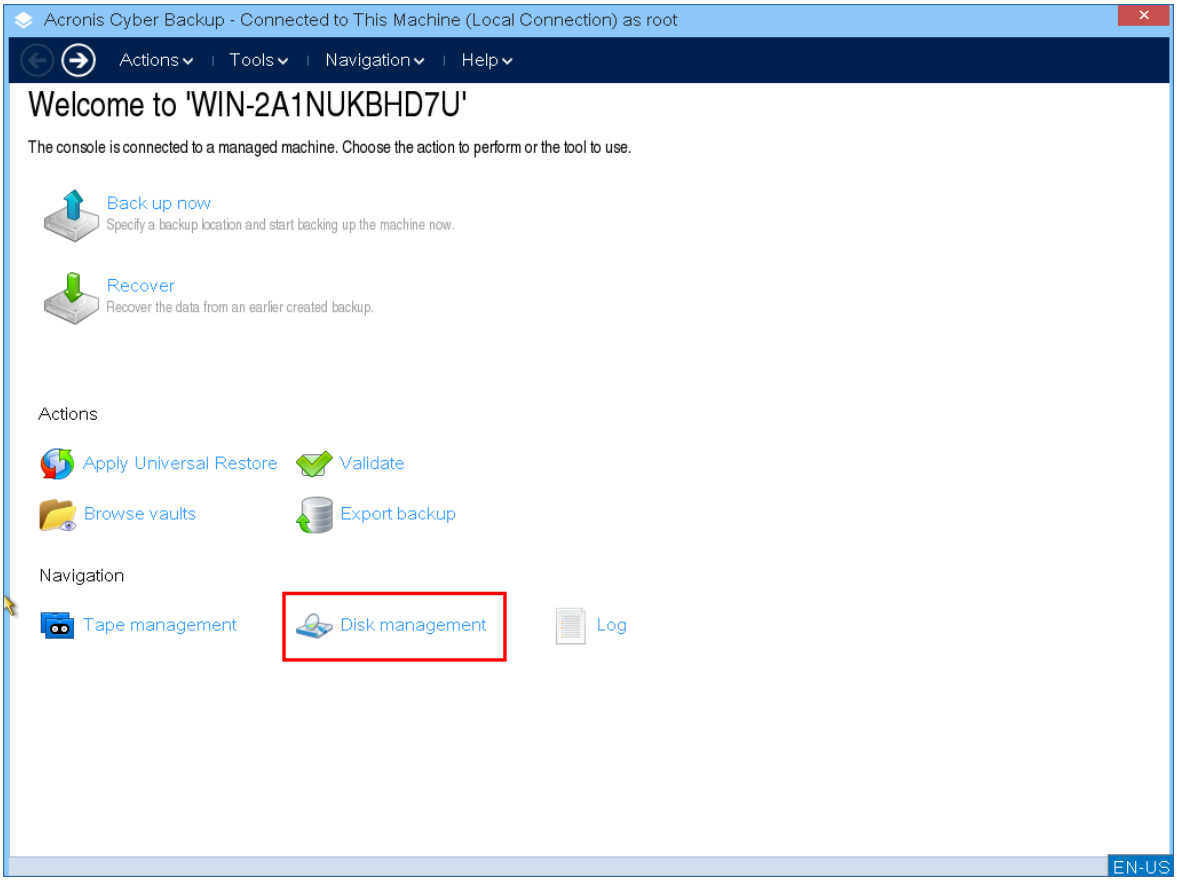
1. 從 Acronis 可開機救援媒體開機。



2. 若要在本機電腦上作業，按一下 **[在本機管理這部電腦]**。若是遠端連線，請參閱在管理伺服器上註冊媒體。



3. 按一下 **[磁碟管理]**。



注意事項
如果在電腦上設定儲存空間，則可開機媒體下的磁碟管理作業可能無法正確運作。

支援的檔案系統

可開機媒體支援使用下列檔案系統進行磁碟管理：

- FAT 16/32
- NTFS

如果您需要在採用不同檔案系統的磁碟區上執行作業，請使用 Acronis Disk Director。它提供了更多的工具和公用程式，可用於管理具有以下檔案系統的磁碟和磁碟區：

- FAT 16/32
- NTFS
- Ext2
- Ext3
- HFS+
- HFSX
- ReiserFS
- JFS
- Linux SWAP

基本預防措施

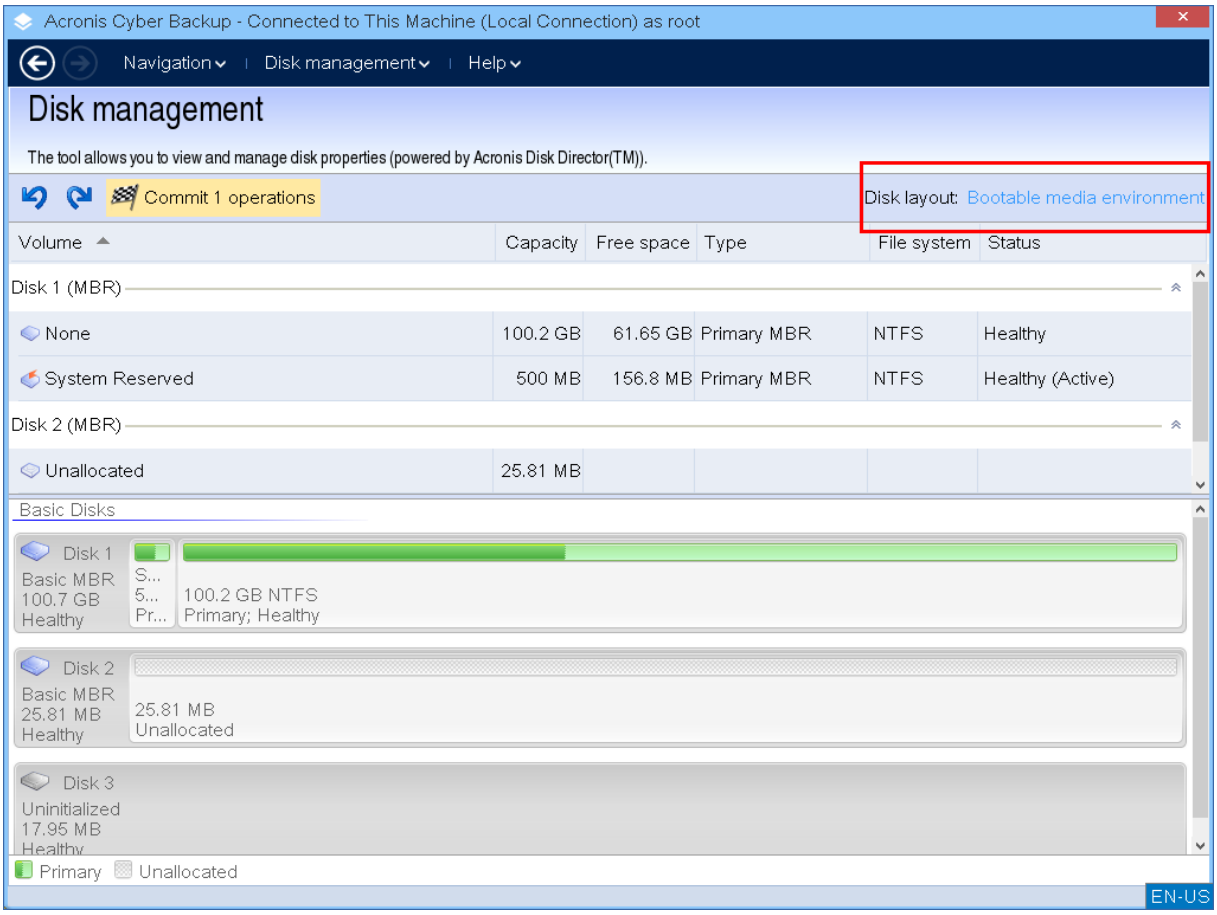
若要避免可能的磁碟和磁碟區結構損毀或資料遺失，請採取所有必要的預防措施並遵循下列指導方針進行：

1. 請備份要在其上建立或管理磁碟區的磁碟。將您最重要的資料備份至其他硬碟、網路共用或卸除式媒體，這可讓您安心地在磁碟區上作業，因為知道您的資料非常安全。
2. 測試您的磁碟，確保其功能完好並且沒有損毀的磁區或檔案系統錯誤。
3. 當執行其他具有低層級磁碟存取的軟體時，請勿執行任何磁碟/磁碟區作業。

為磁碟管理選擇作業系統

在擁有兩個或兩個以上作業系統的電腦上，磁碟和磁碟區的表示依據目前執行的作業系統而定。相同的磁碟區在不同的作業系統下可能會有不同的代號。

當您執行磁碟管理作業時，必須針對將顯示的作業系統指定磁碟配置。方法是，按一下 **[磁碟配置]** 標籤旁的作業系統名稱，然後在開啟的視窗中選擇所需的作業系統。



磁碟作業

您可以利用可開機媒體，執行下列磁碟管理作業：

- 磁碟初始化 - 初始化新增到系統的新硬體
- 基本磁碟複製 - 將來源基本 MBR 磁碟中的完整資料轉移到目標磁碟
- 磁碟轉換：MBR 至 GPT - 將 MBR 分割表轉換為 GPT
- 磁碟轉換：GPT 至 MBR - 將 GPT 分割表轉換為 MBR
- 磁碟轉換：基本至動態 - 將基本磁碟轉換為動態磁碟
- 磁碟轉換：動態至基本 - 將動態磁碟轉換為基本磁碟

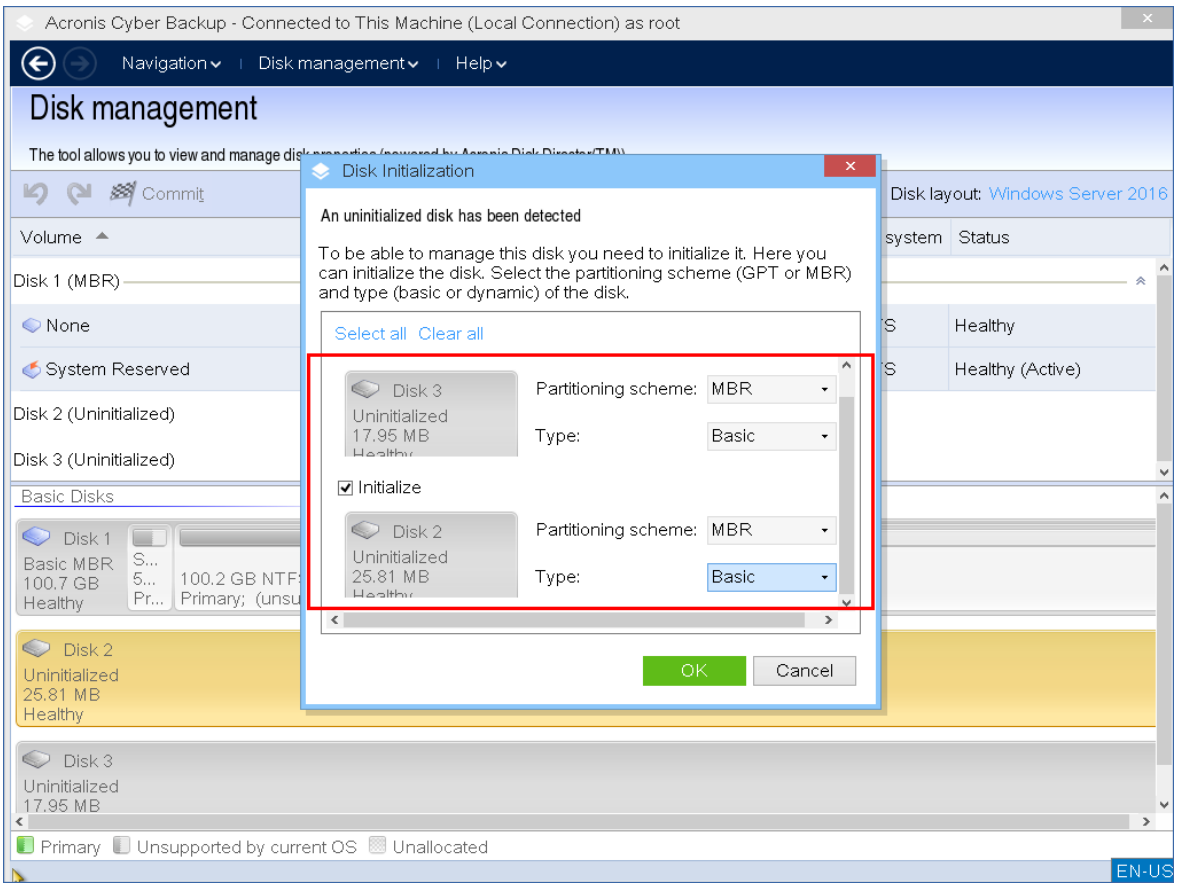
磁碟初始化

可開機媒體會將未初始化的磁碟顯示為一個帶有灰色圖示的灰色區塊，由此表示系統無法使用該磁碟。

若要初始化磁碟

1. 以滑鼠右鍵按一下所需的磁碟，然後按一下 **[初始化]**。
2. 在 **[磁碟初始化]** 視窗中，設定磁碟分割配置 (MBR 或 GPT) 和磁碟類型 (基本或動態)。
3. 按一下 **[確定]**，您將新增待執行的磁碟初始化作業。
4. 若要完成新增的作業，請認可該作業。若未認可作業就退出程式，將會取消該作業。

5. 初始化後，磁碟空間仍處於未配置的狀態。若要能夠使用該空間，您需要在其上建立一個磁碟區。



基本磁碟複製

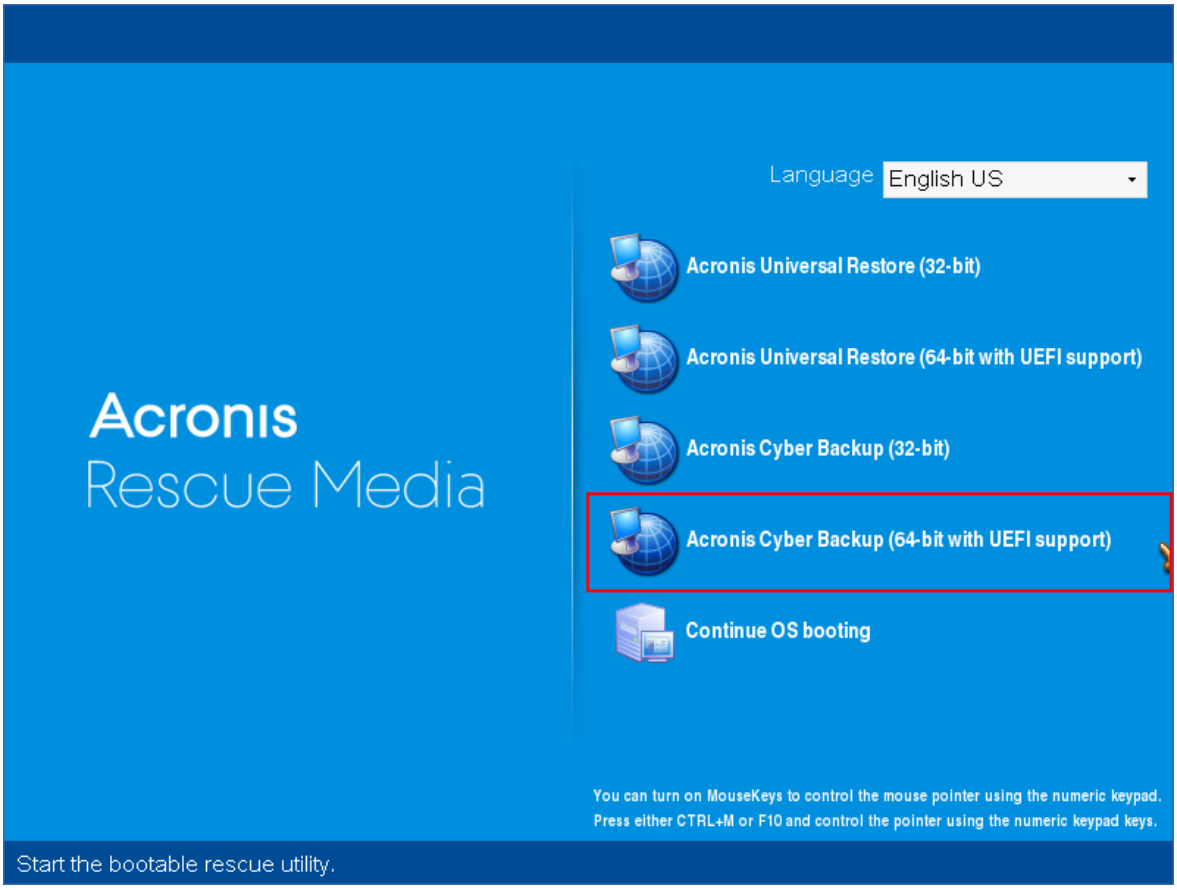
您可以使用完整功能的 Linux 可開機媒體，複製基本 MBR 磁碟。磁碟複製不適用於您可以下載的現成可開機媒體，也不適用於使用授權金鑰建立的可開機媒體。

注意事項

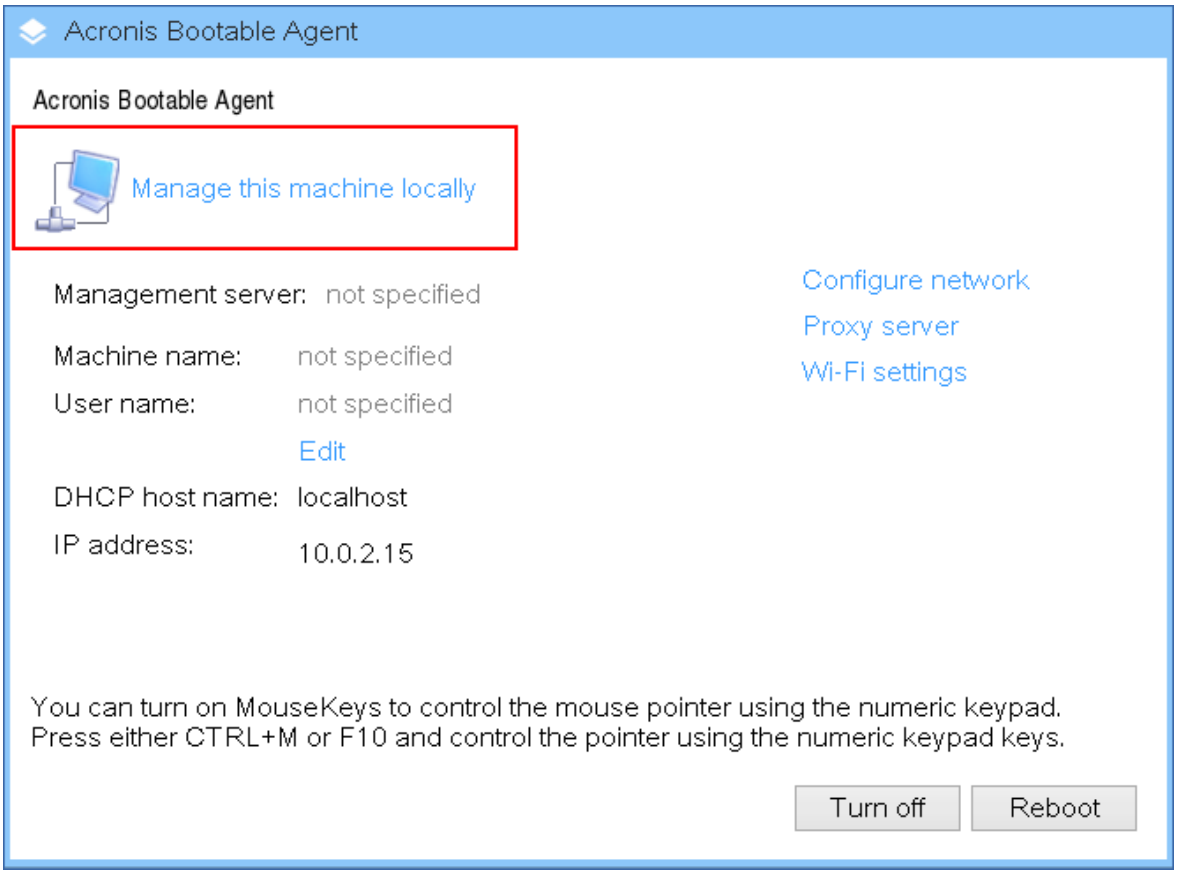
您也可以使用 Acronis Cyber Protect 命令列公用程式複製磁碟。

若要在可開機媒體下複製基本磁碟

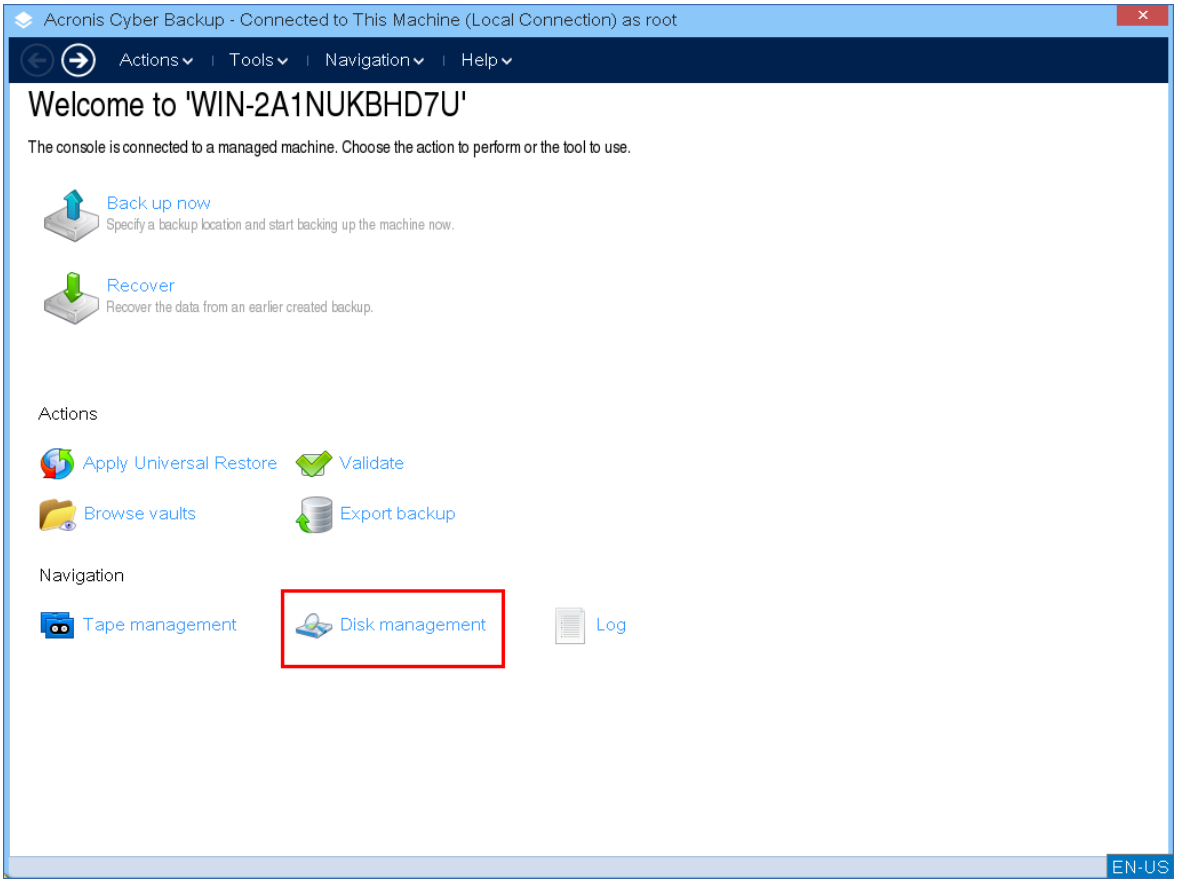
1. 從 Acronis 可開機救援媒體開機。



2. 若要複製本機電腦的磁碟，按一下 **[在本機管理這部電腦]**。若是遠端連線，請參閱在管理伺服器上註冊媒體。

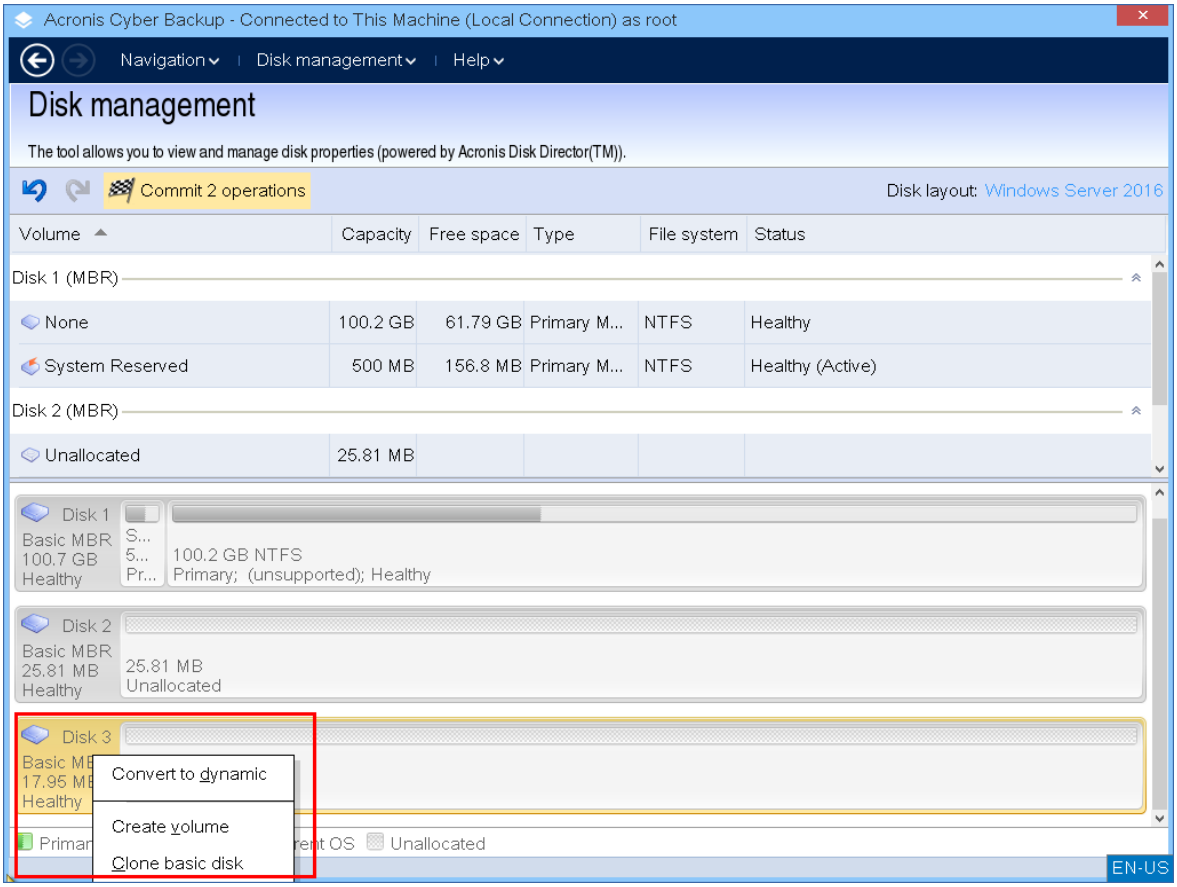


3. 按一下 **[磁碟管理]**。

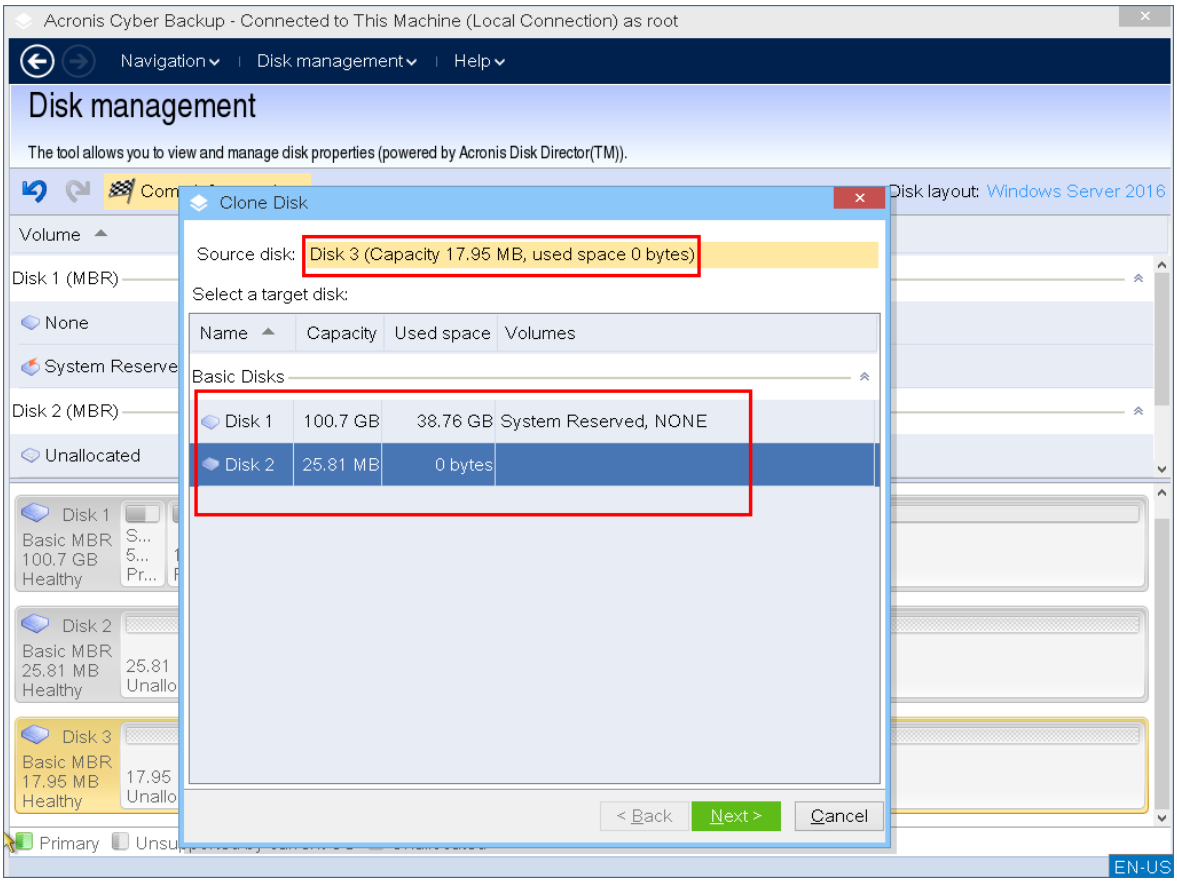


4. 可用的磁碟隨即顯示。以滑鼠右鍵按一下您要複製`的磁碟，然後按一下 **[複製基本磁碟]**。

注意事項
您可以僅複製整個磁碟。磁碟分割複製無法使用。



5. 可能的目標磁碟清單隨即顯示。如果目標磁碟夠大，足以容納來源磁碟中的所有資料，而不會造成任何損失，則此程式可讓您該目標磁碟。選擇目標磁碟，然後按 **[下一步]**。

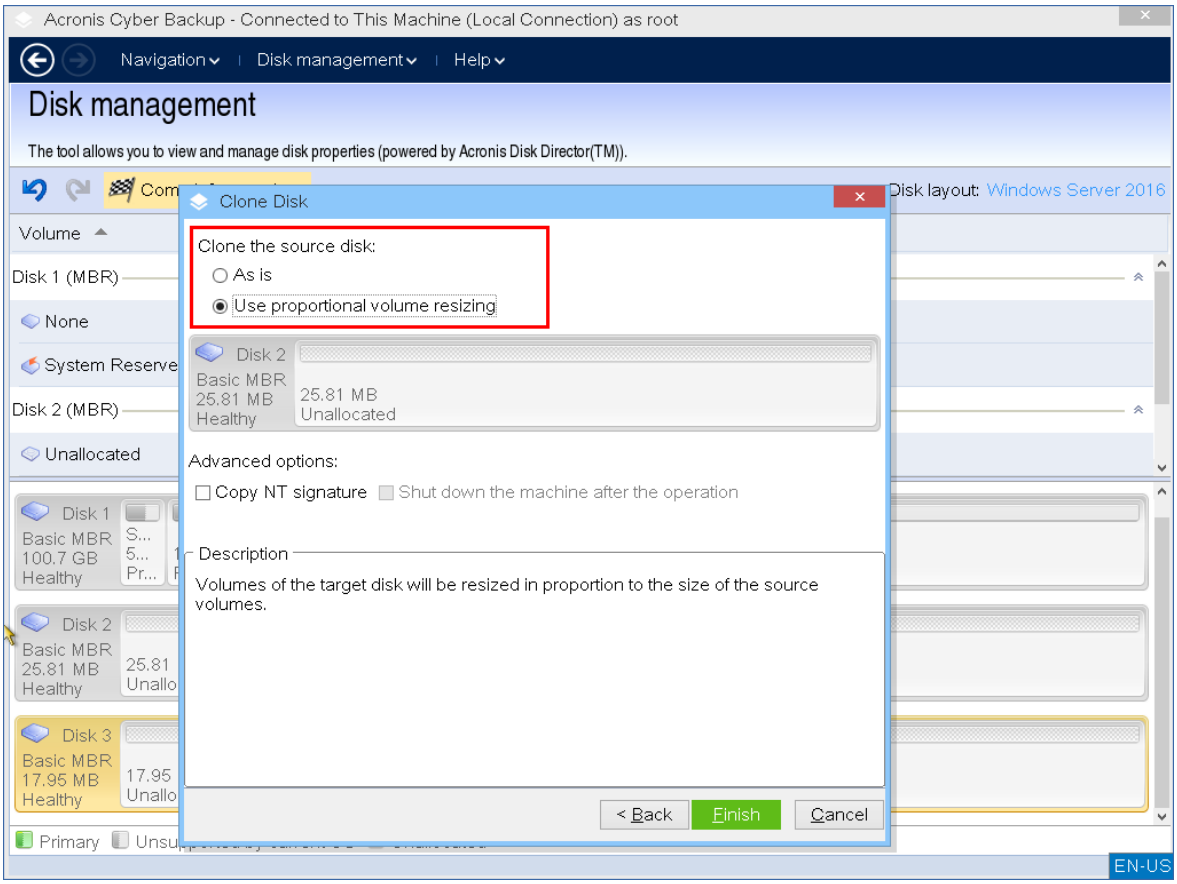


如果目標磁碟比較大，您可以依原樣複製磁碟，或按比例調整來源磁碟磁碟區大小 (預設選項)，以避免在目標磁碟上留下未配置空間。

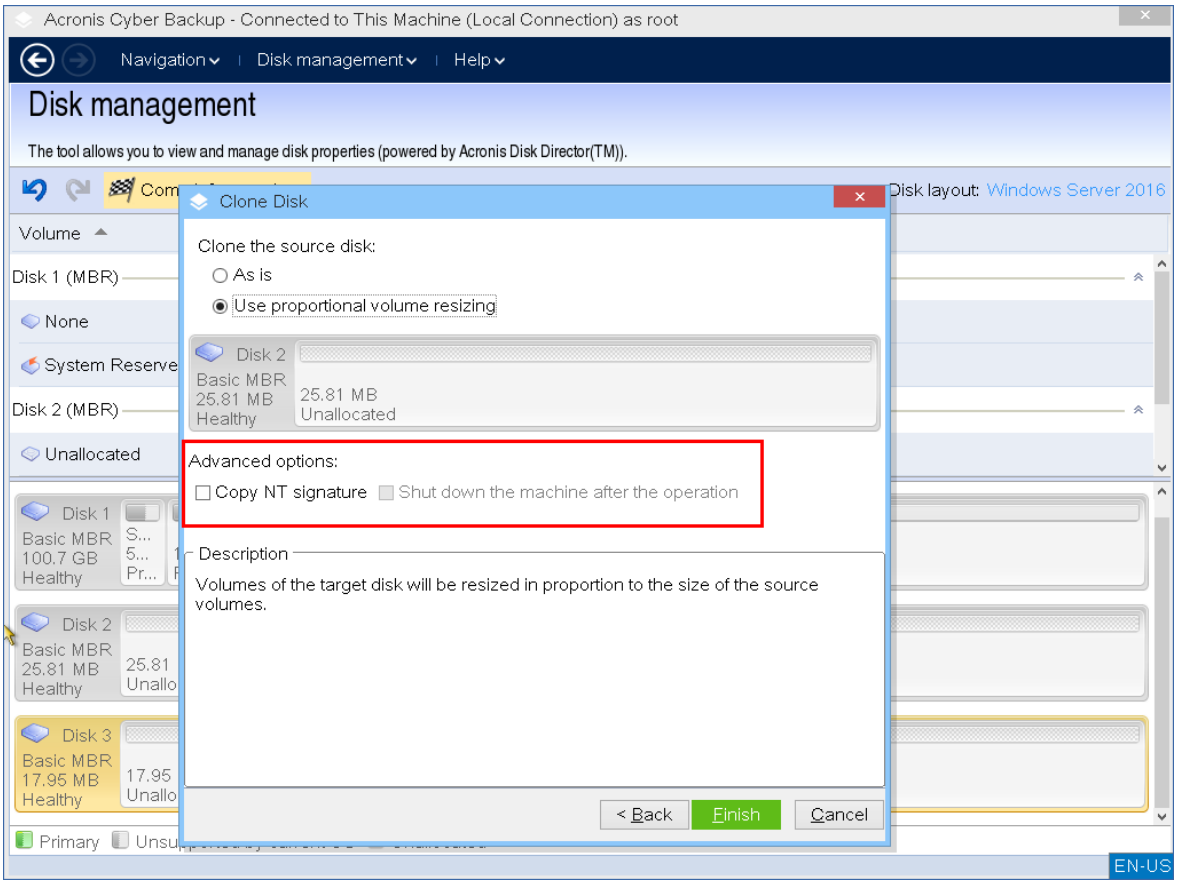
如果目標磁碟比較小，則僅能使用按比例調整大小。如果即使是使用按比例調整大小還是無法進行安全複製，您將無法繼續此作業。

重要事項

如果目標磁碟上有資料，您將會看到警告：「*所選的目標磁碟不為空。將覆寫其磁碟區上的資料。*」如果您繼續，目前在目標磁碟上的所有資料都將遺失，無法挽回。



6. 選擇是否要複製 NT 簽章。



如果您要複製含有系統磁碟區的磁碟，需要在目標磁碟磁碟區上確保作業系統可開機。這表示作業系統必須具備與磁碟 NT 簽章相符的系統磁碟區資訊 (例如，磁碟區代號)，此類資訊保留在 MBR 磁碟記錄中。但是，在一個作業系統下，具有相同 NT 簽章的兩個磁碟無法正常運作。

如果電腦上有兩個帶有相同 NT 簽章的磁碟並且含有一個系統磁碟區，在啟動時，作業系統將從第一個磁碟執行，並發現第二個磁碟上有相同的簽章，然後自動產生唯一的新 NT 簽章，並將其指派給第二個磁碟。如此一來，第二個磁碟上的所有磁碟區都將失去其代號、所有路徑都將不再有效，而且程式也找不到其檔案。該磁碟上的作業系統將無法開機。

若要保留系統在目標磁碟磁碟區上的可開機屬性，您可以：

a. **複製 NT 簽章** – 為目標磁碟提供與登錄機碼相符，且也將在目標磁碟上複製的來源磁碟 NT 簽章。

   方法是，選擇 **[複製 NT 簽章]** 核取方塊。

   您將會收到警告：*「如果硬碟上有作業系統，再次啟動電腦前，請從電腦上解除安裝來源或目標硬碟機。否則，作業系統將從第一個磁碟上啟動，而第二個磁碟上的作業系統將無法開機。」*

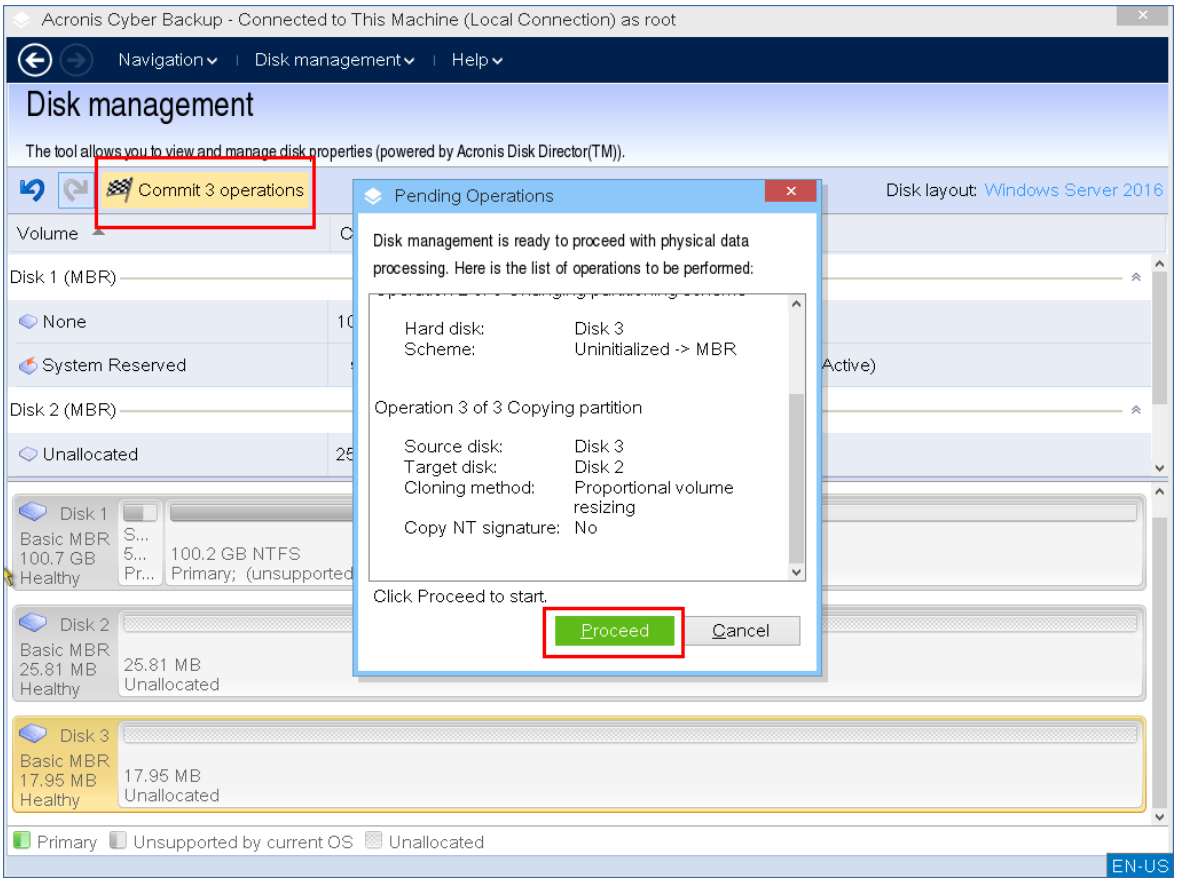
   將自動選擇並停用 **[作業後關閉電腦]** 核取方塊。

b. **保留 NT 簽章** – 保留舊目標磁碟簽章，並根據簽章更新作業系統。

   方法是，必要時，按一下以清除 **[複製 NT 簽章]** 核取方塊。

   將自動清除 **[作業後關閉電腦]** 核取方塊。

7. 按一下 **[完成]** 以新增待執行的磁碟複製作業。
8. 按一下 **[認可]**，然後在 **[待執行作業]** 視窗中按一下 **[繼續]**。若未認可作業就退出程式，將會取消該作業。



9. 如果您選擇複製 NT 簽章，請等到作業完成且電腦關閉，然後從電腦上中斷連接來源或目標硬碟機。

磁碟轉換：MBR 至 GPT

在下列情況下，可以將 MBR 基本磁碟轉換為 GPT 基本磁碟：

- 您需要在一個磁碟上有 4 個以上的主要磁碟區。
- 您需要更高的磁碟可靠性，以防止任何可能的資料銷毀。

重要事項
如果基本 MBR 磁碟上的開機磁碟區有目前執行中的作業系統，則無法轉換為 GPT。

若要將基本 MBR 磁碟轉換為基本 GPT 磁碟

1. 以滑鼠右鍵按一下您要複製`的磁碟，然後按一下 **[轉換為 GPT]**。
2. 按一下 **[確定]**，即可新增一個將 MBR 磁碟轉換為 GPT 磁碟的待執行作業。
3. 若要完成新增的作業，請認可該作業。若未認可作業就退出程式，將會取消該作業。

注意事項

GPT 分割磁碟會在分割區域的末尾保留一定的空間用作備份區域，這用來儲存 GPT 標題和分割表的副本。如果磁碟已滿，而且無法自動減少磁碟區大小，將 MBR 磁碟轉換為 GPT 磁碟的作業將會失敗。

該作業是不可逆的。如果您有一個屬於 MBR 磁碟的主要磁碟區，而且您先將磁碟轉換為 GPT 磁碟，然後再轉換回 MBR 磁碟，則該磁碟區將變成邏輯磁碟區，而且無法當作系統磁碟區使用。

動態磁碟轉換：MBR 至 GPT

可開機媒體不支援動態磁碟 MBR 至 GPT 的直接轉換。但是，您可以執行下列轉換來達到此目的：

1. 使用 **[轉換為基本磁碟]** 作業來執行 MBR 磁碟轉換：動態至基本。
2. 基本磁碟轉換：使用 **[轉換為 GPT]** 作業來執行 MBR 至 GPT 轉換。
3. 使用 [轉換為動態磁碟] 作業來執行 GPT **磁碟轉換：基本至動態**。

磁碟轉換：GPT 至 MBR

如果您打算安裝不支援 GPT 磁碟的作業系統，可以將 GPT 磁碟轉換為 MBR 磁碟。

重要事項

如果基本 GPT 磁碟上的開機磁碟區有目前執行中的作業系統，則無法轉換為 MBR。

若要將 GPT 磁碟轉換為 MBR 磁碟

1. 以滑鼠右鍵按一下您要複製`的磁碟，然後按一下 **[轉換為 MBR]**。
2. 按一下 **[確定]** 即可新增一個將 GPT 磁碟轉換為 MBR 磁碟的待執行作業。
3. 若要完成新增的作業，請認可該作業。若未認可作業就退出程式，將會取消該作業。

注意事項

操作後，此磁碟上的磁碟區將會變成邏輯磁碟區。此變更是不可逆的。

磁碟轉換：基本至動態

在下列情況下，您可能想要將基本磁碟轉換為動態磁碟：

- 打算將磁碟當作動態磁碟群組的一部分使用
- 想要為資料儲存提高磁碟可靠性

若要將基本磁碟轉換為動態磁碟

1. 以滑鼠右鍵按一下您要轉換`的磁碟，然後按一下 **[轉換為動態磁碟]**。
2. 按一下 **[確定]**。

轉換將會立即執行，而且必要時，您的電腦將會重新開機。

注意事項
動態磁碟將佔用實體磁碟的最後空間來儲存資料庫，包括各動態磁碟區的四個層級的描述(磁碟區-組件-分割-磁碟)。如果在轉換為動態磁碟期間，基本磁碟已滿，無法自動減少其磁碟區的大小，作業將會失敗。
轉換含有系統磁碟區的磁碟需要一些時間，而且在這個程序中，斷電、不小心關閉電腦或意外按下 Reset 按鈕都可能導致喪失開機能力。

與 Windows 磁碟管理員相反，該程式可確保執行作業後磁碟上的**離線作業系統**可開機。

磁碟轉換：動態至基本

您可能希望將動態磁碟轉換回基本磁碟，例如，如果您要使用不支援動態磁碟的作業系統。

若要將動態磁碟轉換為基本磁碟：

1. 以滑鼠右鍵按一下您要轉換`的磁碟，然後按一下 **[轉換為基本磁碟]**。
2. 按一下 **[確定]**。

轉換將會立即執行，而且必要時，您的電腦將會重新開機。

注意事項
此作業不適用於含有跨距磁碟區、等量磁碟區或 RAID-5 磁碟區的動態磁碟。

轉換完成後，磁碟空間的最後 8Mb 將被保留，供日後從基本磁碟轉換至動態磁碟的作業使用。在某些情況下，可能的未配置空間與建議的最大磁碟區大小可能有所不同 (例如，當一個鏡像的大小建立另一個鏡像的大小，或磁碟空間的最後 8Mb 為日後從基本磁碟轉換為動態磁碟而保留時)。

注意事項
轉換含有系統磁碟區的磁碟需要花費一些時間，而且在這個程序中，斷電、不小心關閉電腦或意外按下 Reset 按鈕都可能導致喪失開機能力。

與 Windows 磁碟管理員相反，此程式可確保：

- 當磁碟具有**含資料**的磁碟區 (用於簡單和鏡像磁碟區) 時，可將動態磁碟安全地轉換為基本磁碟
- 在多開機系統中，在作業期間**離線**的系統的開機能力

磁碟區作業

您可以利用可開機媒體，在磁碟區上執行下列作業：

- 建立磁碟區 - 建立新磁碟區
- 刪除磁碟區 - 刪除所選磁碟區
- 設定為使用中 - 將所選磁碟區設定為使用中，讓電腦能夠使用安裝在該磁碟區上的作業系統開機
- 變更代號 - 變更所選磁碟區的代號
- 變更標籤 - 變更所選磁碟區的標籤
- 格式化磁碟區 - 格式化含有檔案系統的磁碟區

動態磁碟區的類型

簡單磁碟區

用一個實體磁碟上的可用空間建立的磁碟區。它可包括磁碟的一或數個區域，實際上是由 [邏輯磁碟管理器] (LDM) 聯合在一起。這既無法提升額外的可靠性或速度，也無法提供額外的大小。

跨距磁碟區

在可用磁碟空間上建立的磁碟區，這些磁碟空間是來自於幾個實體磁碟，由 LDM 以虛擬方式連結在一起。最多可將 32 個磁碟包含在一個磁碟區中，從而克服了硬體大小的限制。但即使只有一個磁碟發生故障，所有的資料都將遺失。此外，如果不破壞整個磁碟區，則無法移除跨距磁碟區的任何部分。因此，跨距磁碟區無法提供額外的可靠性或更佳的 I/O 傳輸速率。

等量磁碟區

也稱為 RAID 0 的磁碟區，包含同等大小的資料條帶，可跨磁碟區中的各磁碟寫入。這意味著，若要建立等量磁碟區，您需要兩個或更多的動態磁碟。等量磁碟區中的磁碟不必完全相同，但是在您要納入磁碟區的各個磁碟上必須有未使用的空間。磁碟區大小將取決於最小空間的大小。通常，存取等量磁碟區上的資料要比存取單個實體磁碟上的相同資料更快，因為 I/O 分散在多個磁碟上。

建立等量磁碟區旨在提升效能，而不是提高可靠性，因為其不包含冗餘資訊。

鏡像磁碟區

具有容錯能力的磁碟區，也稱為 RAID 1，其資料會在兩個相同的實體磁碟上複製。一個磁碟上的所有資訊會複製到另一個磁碟上，以提供資料冗餘。幾乎任何磁碟區都可以建立鏡像，包括系統和開機磁碟區，而如果其中一個磁碟故障，仍可從剩餘的磁碟存取資料。遺憾的是，使用鏡像磁碟區時，硬體大小和效能的限制更高。

鏡像等量磁碟區

一種具有容錯能力的磁碟區，有時也稱為 RAID 1+0，結合了等量配置的高速 I/O 傳輸速度和鏡像類型冗餘的優勢。但仍具有鏡像架構固有的缺點，磁碟對磁碟區大小比率較低。

RAID-5

一種具有容錯能力的磁碟區，其資料以等量方式儲存於由三個或更多磁碟組成的陣列中。其磁碟不必完全相同，但是磁碟區中各磁碟上的可用未配置空間的區塊必須大小相同。同位 (失敗後可用於重建資料的計算值) 也以等量方式儲存於磁碟陣列，而且，它一律會儲存在不同的磁碟上，而非資料本身。若實體磁碟故障，此故障磁碟上 RAID-5 磁碟區的部分可透過剩餘資料及同位重新建立。RAID-5 磁碟區不但能提供可靠性，且因為磁碟對磁碟區大小比率高於鏡像磁碟區，而能夠克服實體磁碟的大小限制。

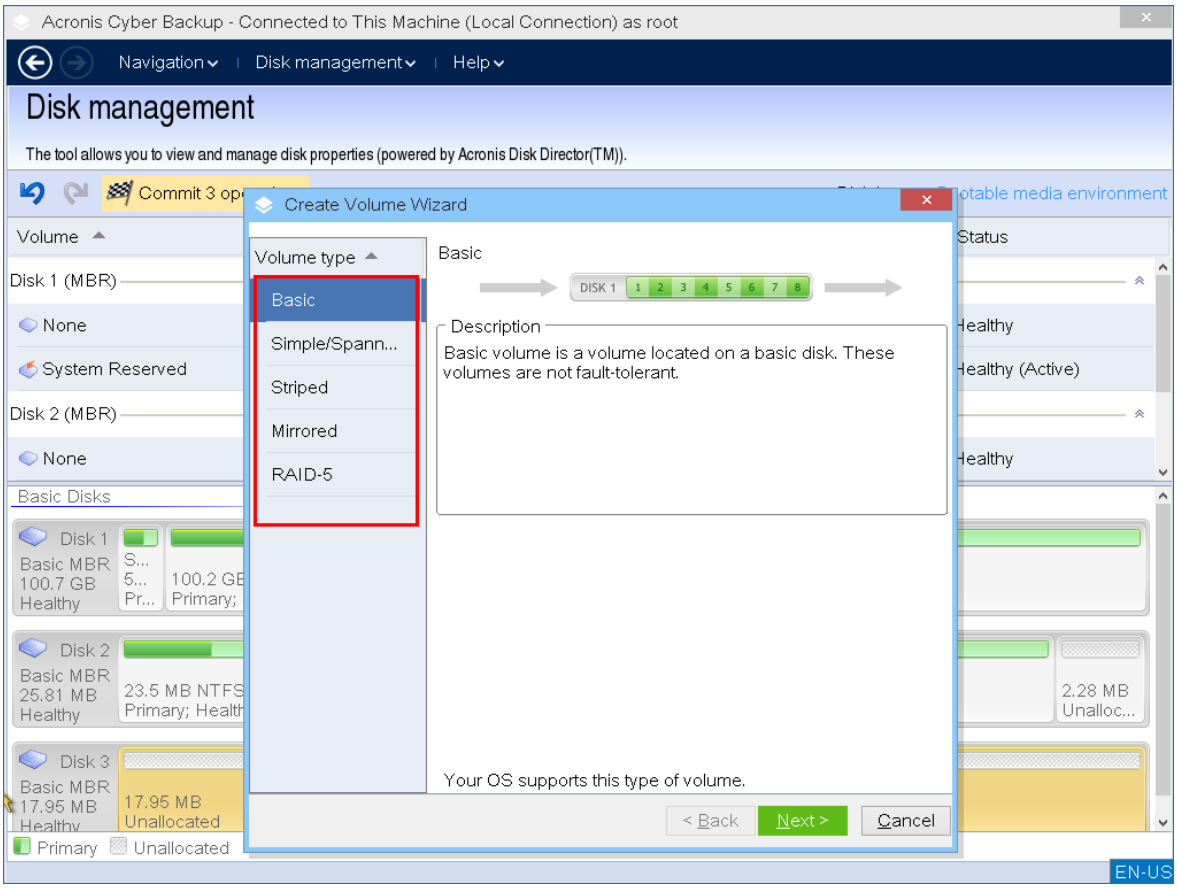
建立磁碟區

您可能需要一個新磁碟區來：

- 以「完全按原樣」的設定，復原先前儲存的備份複本
- 分開儲存類似檔案的集合，例如，在單獨的磁碟區上儲存 MP3 集合或視訊檔案
- 在特殊磁碟區上儲存其他磁碟區/磁碟的備份 (影像)
- 在新磁碟區上安裝新的作業系統 (或交換檔)
- 將新硬體新增至電腦

若要建立磁碟區

1. 以滑鼠右鍵按一下磁碟中任何未配置空間，然後按一下 **[建立磁碟區]**。**[建立磁碟區]** 精靈隨即開啟。



2. 選擇磁碟區類型。您可以選取下列選項：
   - 基本
   - 簡單/跨距
   - 等量
   - 鏡像
   - RAID-5

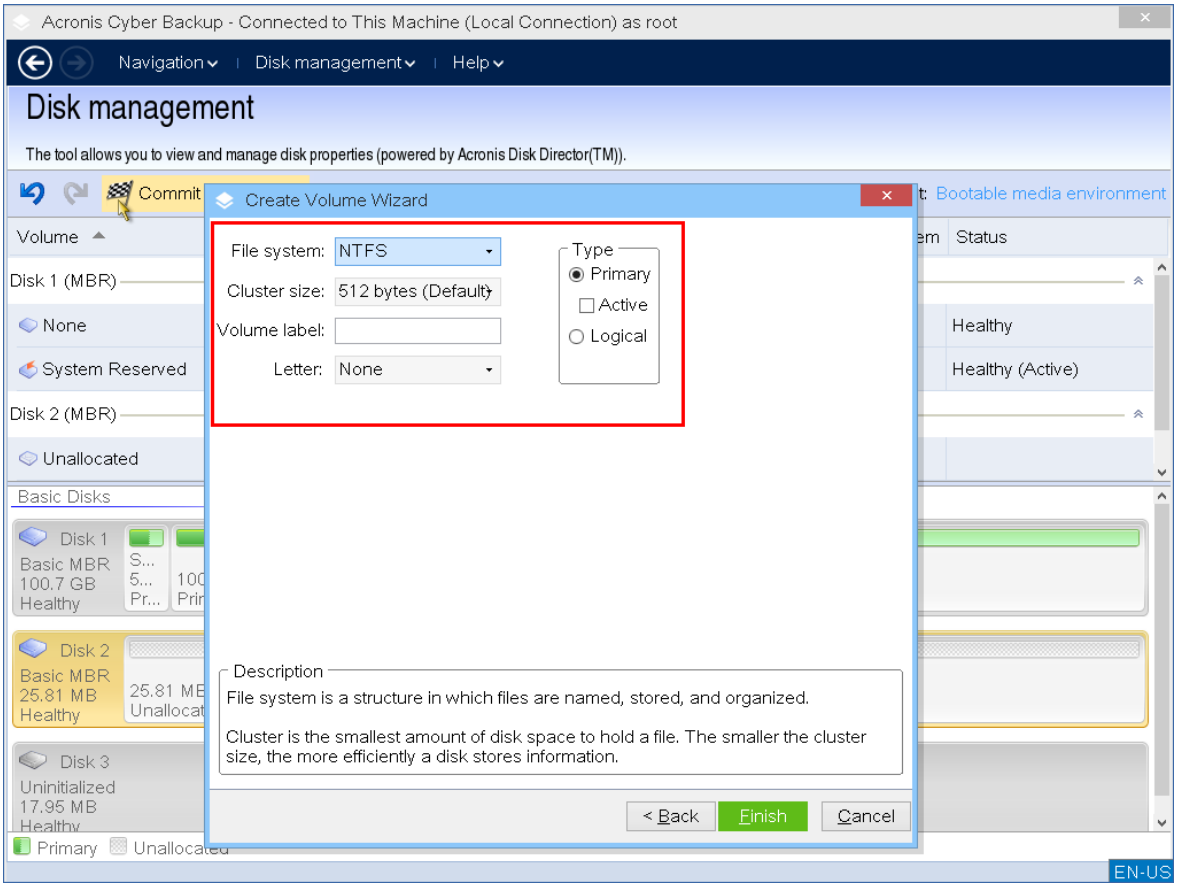
   如果目前的作業系統不支援所選的磁碟區類型，您將收到一個警告，而且 **[下一步]** 按鈕將遭到停用。您必須選擇另一種磁碟區類型，才能繼續。

3. 指定未配置空間或選擇目的地磁碟。
   - 若是基本磁碟區，請在所選磁碟上指定未配置空間。
   - 若是簡單/跨距磁碟區，選擇一或多個目的地磁碟。
   - 若是鏡像磁碟區，選擇兩個目的地磁碟。
   - 若是等量磁碟區，選擇兩個或多個目的地磁碟。
   - 若是 RAID-5 磁碟區，選擇三個目的地磁碟

   如果您要建立**動態**磁碟區，並選擇一個或數個**基本**磁碟作為其目的地，您將收到一個警告，指出所選磁碟將自動轉換為動態磁碟。
4. 設定磁碟區大小。

   最大值通常會反映最大可能的未配置空間。在某些情況下，建議的最大值可能有所不同，例如，當一個鏡像的大小建立另一個鏡像的大小，或磁碟空間的最後 8Mb 為日後從基本磁碟轉換為動態磁碟而保留時。

   如果磁碟上的未配置空間比磁碟區大，您可以在該磁碟上選擇新基本磁碟區的位置。
5. 設定磁碟區選項。



您可以指派磁碟區 **[代號]**(預設為字母表的第一個可用字母)，還可以選擇性地指派 **[標籤]**(預設為 [無])。您也必須指定 **[檔案系統]** 和 **[叢集大小]**。

可能的檔案系統選項包括：

- FAT16 (如果磁碟區大小已設為超過 2 GB，則停用)
- FAT32 (如果磁碟區大小已設為超過 2 TB，則停用)

- NTFS
- 保留磁碟區為未格式化狀態。

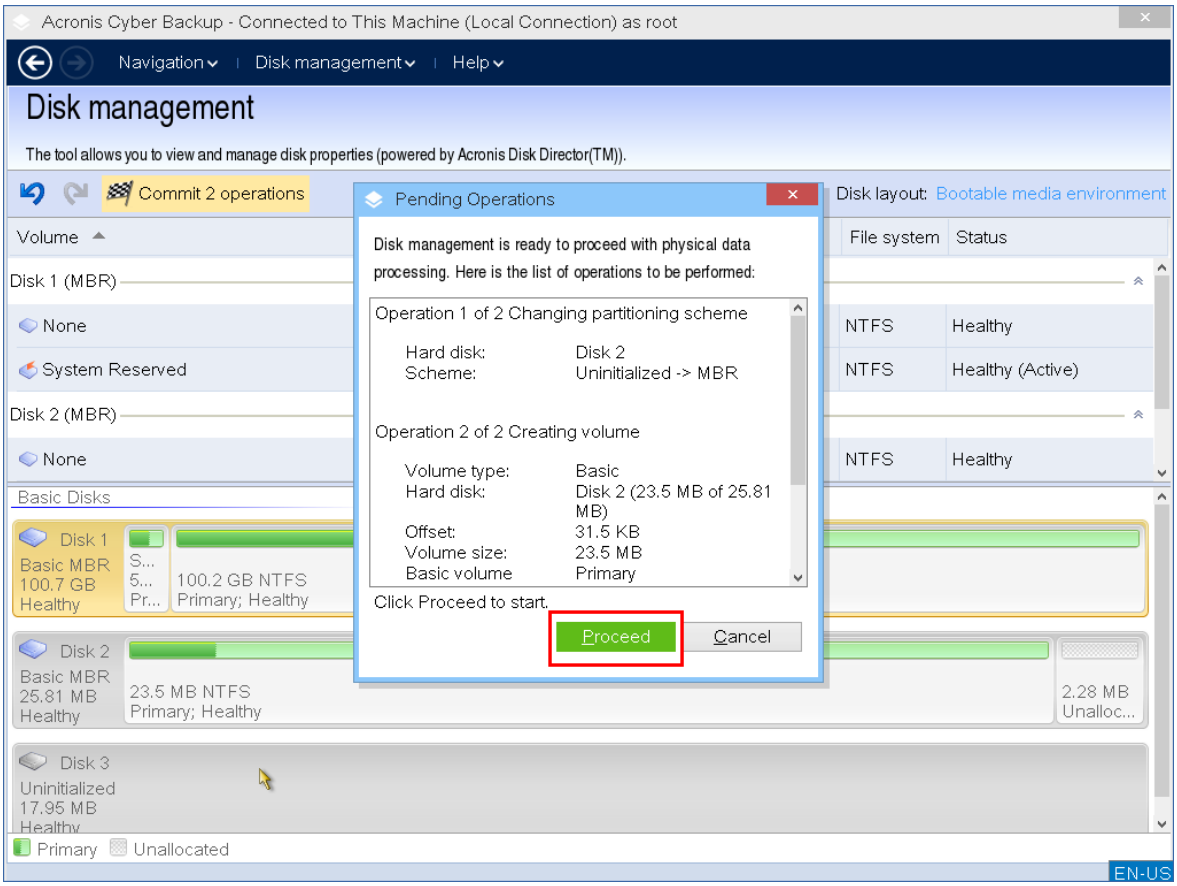
  設定叢集大小時，您可以在每個檔案系統預設的數量範圍內選擇任何數目。預設的建議叢集大小最適合具備所選檔案系統的磁碟區。如果您為 FAT16/FAT32 設定 64K 的叢集大小，或為 NTSF 設定 8KB-64KB 的叢集大小，Windows 可以掛載該磁碟區，但有些程式 (如安裝程式) 可能會錯誤地計算其磁碟空間。

  如果您要建立一個可以成為系統磁碟區的基本磁碟區，您也可以選擇磁碟區類型：**主要 (使用中主要)** 或 **[邏輯]**。通常，當您想要將作業系統安裝到磁碟區時，選擇 **[主要]**。如果您要在這個磁碟區上安裝在電腦啟動時開機的作業系統，則選擇 **[使用中]** (預設) 值。如果未選擇 **[主要]** 按鈕，**[使用中]** 選項將處於非使用中狀態。如果該磁碟區用於資料儲存，選擇 **[邏輯]**。

  注意事項

  一個基本磁碟可包含最多四個主要磁碟區。如果它們已經存在，磁碟將必須轉換為動態磁碟，否則 **[使用中]** 和 **[主要]** 選項將遭到停用，您將只能選擇 **[邏輯]** 磁碟區類型。

6. 按一下 **[認可]**，然後在 **[待執行作業]** 視窗中按一下 **[繼續]**。若未認可作業就退出程式，將會取消該作業。



刪除磁碟區

若要刪除磁碟區

1. 以滑鼠右鍵按一下您要刪除的磁碟區。
2. 按一下 **[刪除磁碟區]**。

注意事項
此磁碟區上的所有資訊將會遺失，無法挽回。

3. 按一下 **[確定]**，您將新增待執行的磁碟區刪除作業。
4. 若要完成新增的作業，請認可該作業。若未認可作業就退出程式，將會取消該作業。

刪除磁碟區後，其空間會新增到未配置空間中。您可以將其用於建立新磁碟區或變更另一個磁碟區的類型。

設定啟動磁碟區

如果您有幾個主磁碟區，必須指定一個作為開機磁碟區。為此，您可將一個磁碟區設為啟動磁碟區。一個磁碟上只能有一個使用中磁碟區。

若要將磁碟區設定為使用中：

1. 以滑鼠右鍵按一下基本 MBR 上所需的主要磁碟區，然後按一下 **[標記為使用中]**。
   如果系統中沒有其他啟動磁碟區，將新增設定啟動磁碟區的擱置作業。如果系統中有另一個使用中磁碟區，您將收到一個警告，指出先前的使用中磁碟區必須先設定為被動。

注意事項
由於設定新的使用中磁碟區，先前的使用中磁碟區代號可能會變更，而且部分已安裝的程式可能會停止執行。

2. 按一下 **[確定]**，您將新增待執行的設定使用中磁碟區作業。

注意事項
即使新的使用中磁碟區上有作業系統，在某些狀況下，電腦也無法從該磁碟區開機。您必須確認將新磁碟區設為啟動磁碟區。

3. 若要完成新增的作業，請認可該作業。若未認可作業就退出程式，將會取消該作業。

變更磁碟區代號

啟動時，Windows 作業系統會指定硬碟的磁碟區代號 (C:、D:等)。應用程式和作業系統使用這些代號來找到磁碟區上的檔案和資料夾。連接另一個磁碟及在現有磁碟上建立或刪除磁碟區，可能會變更您的系統組態。因此，某些應用程式可能停止正常運作，或者可能無法自動找到並開啟使用者檔案。為了避免這種狀況，您可手動變更作業系統自動指定的磁碟區代號。

若要變更作業系統指派給磁碟區的代號

1. 以滑鼠右鍵按一下所需的磁碟區，然後按一下 **[變更代號]**。
2. 在 **[變更代號]** 視窗中，選擇一個新代號。
3. 按一下 **[確定]**，您將新增待執行的磁碟區代號指派作業。
4. 若要完成新增的作業，請認可該作業。若未認可作業就退出程式，將會取消該作業。

變更磁碟區標籤

磁碟區標籤是一項可選用屬性。這是為了便於識別而指定給磁碟區的名稱。

若要變更磁碟區標籤

1. 以滑鼠右鍵按一下所需的磁碟區，然後按一下 **[變更標籤]**。
2. 在 **[變更標籤]** 視窗的文字欄位中，輸入新的標籤。
3. 按一下 **[確定]**，您將新增待執行的變更磁碟區標籤作業。
4. 若要完成新增的作業，請認可該作業。若未認可作業就退出程式，將會取消該作業。

格式化磁碟區

您可能會希望格式化磁碟區來變更磁碟區的檔案系統，以達到下列目的：

- 節省額外的空間，而這些空間由於 FAT16 或 FAT32 檔案系統上的叢集大小而流失
- 快速且或多或少可靠地銷毀此磁碟區上的資料

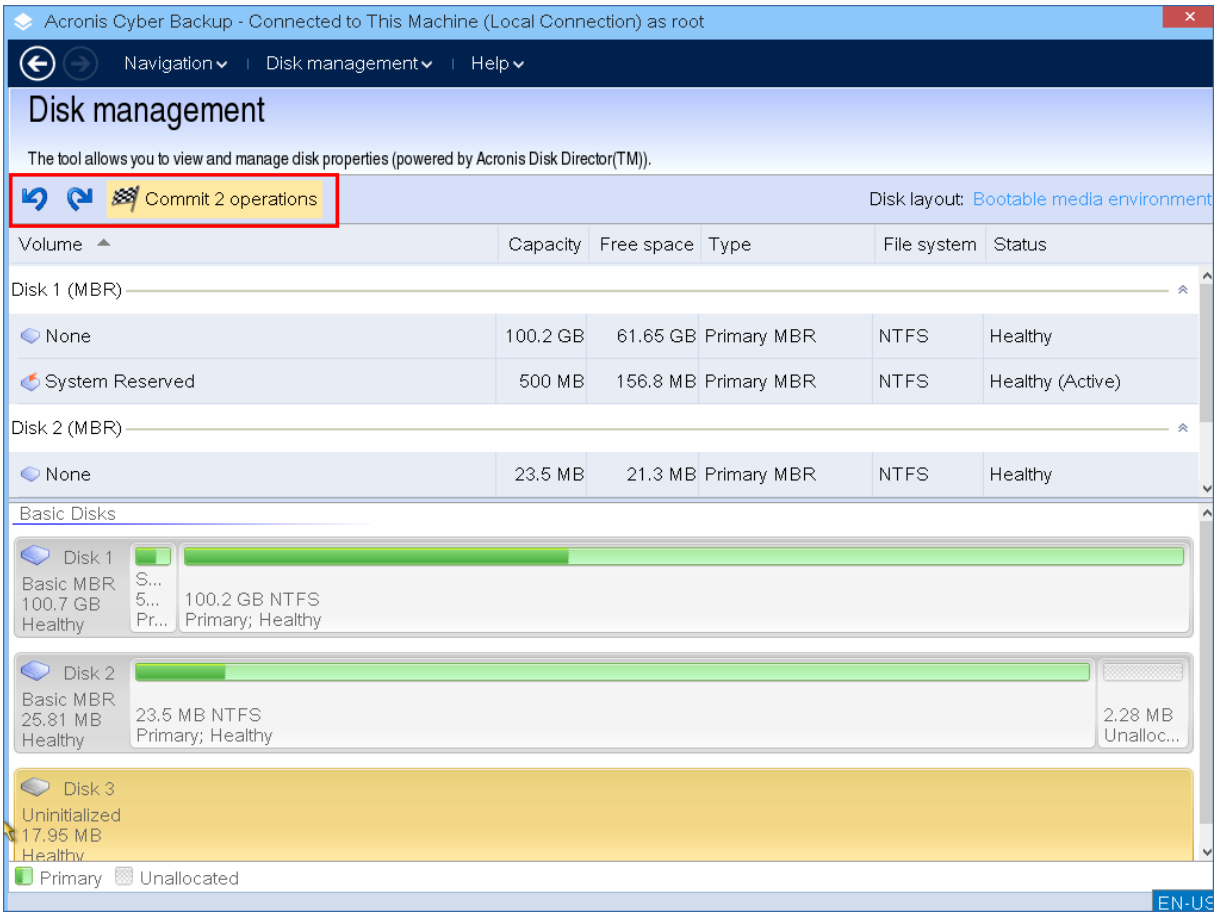
若要格式化磁碟區：

1. 以滑鼠右鍵按一下所需的磁碟區，然後按一下 **[格式化]**。
2. 選擇叢集大小和檔案系統。可能的檔案系統選項包括：
   - FAT16 (如果磁碟區大小已設為超過 2 GB，則停用)
   - FAT32 (如果磁碟區大小已設為超過 2 TB，則停用)
   - NTFS
3. 按一下 **[確定]**，您將新增待執行的格式化磁碟區作業。
4. 若要完成新增的作業，請認可該作業。若未認可作業就退出程式，將會取消該作業。

擱置作業

在您發出並確認 **[認可]** 命令之前，所有作業都會被視為待執行。因此，您可以控制所有規劃的作業、再次確認預定的變更，以及在必要時於執行之前取消任何作業。

[磁碟管理] 檢視中的工具列上有圖示可用於待執行作業的 **[復原]**、**[取消復原]** 和 **[認可]** 動作。這些動作也可以從 **[磁碟管理]** 功能表啟動。



所有規劃的作業將新增至擱置作業清單。

[復原] 動作可讓您復原清單中最近的作業。清單不是空白時，您可以使用該動作。

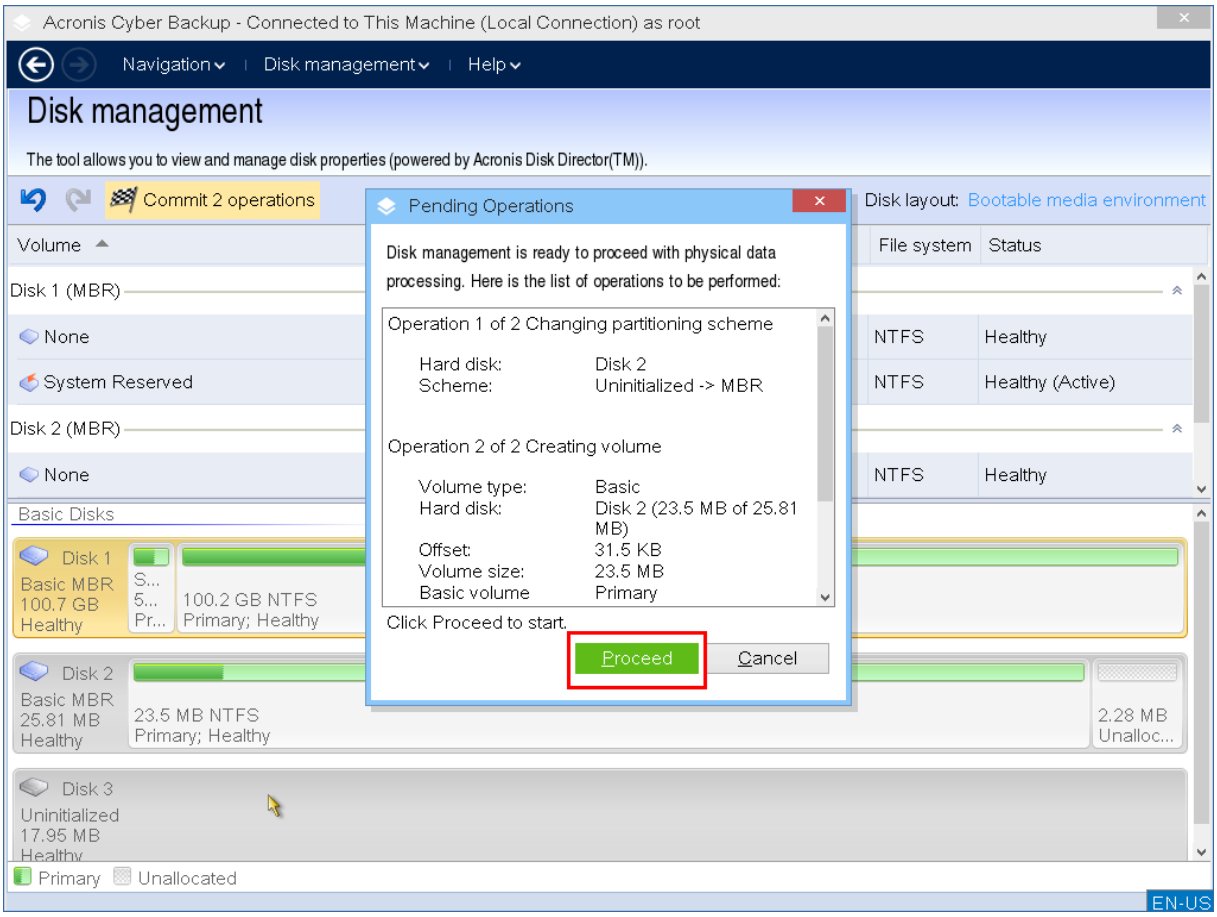
[取消復原] 動作可讓您恢復已復原的最後一個待執行作業。

[認可] 動作可將您轉至 **[待執行作業]** 視窗，您可在此檢視待執行作業清單。

若要啟動執行，按一下 **[繼續]**。

注意事項
選擇 **[繼續]** 作業後，您將無法復原任何動作或作業！

如果您不想要以認可繼續，按一下 **[取消]**。那麼，待處理作業清單不會有任何變更。若未認可待執行作業就退出程式也會取消這些作業。



可開機媒體的相關遠端作業

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 "在管理伺服器上註冊媒體"(第 330 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]** 中。

您可以使用 Web 介面，從遠端管理媒體。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。

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。

   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"(第 240 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 286 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 "復原實體機器" (第 270 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 286 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。

設定 iSCSI 和裝置

本節描述在可開機媒體下運作時，如何設定網際網路小型電腦系統介面 (iSCSI) 裝置。執行以下步驟後，您將可以使用這些裝置，就像它們本端連接到使用可開機媒體開機的電腦一樣。

iSCSI 目標伺服器（或 **目標入口**）是代管 iSCSI 裝置的伺服器。**iSCSI 目標**是目標伺服器上的元件；此元件會共用裝置並列出已被允許存取裝置的起始端。**iSCSI 起始端**是電腦上的一個元件；此元件可提供電腦與 iSCSI 目標之間的互動。在具備可開機媒體的電腦上，當設定對 iSCSI 裝置的存取時，您必須指定裝置的 iSCSI 目標入口，以及目標中所列的 iSCSI 起始端之一。若目標共用了數個裝置，則將會存取所有這些裝置。

要在 Linux 可開機媒體上新增 iSCSI 裝置

1. 按一下**[工具]** > **[設定 iSCSI/NDAS 裝置]**。
2. 按一下 **[新增主機]**。
3. 指定 IP 位址、iSCSI 目標入口的連接埠，以及任何容許存取該裝置的 iSCSI 起始端的名稱。
4. 如果主機需要驗證，則為其指定使用者名稱與密碼。
5. 按一下 **[確定]**。
6. 從清單中選擇 iSCSI 目標，然後按一下 **[連線]**。
7. 若在 iSCSI 目標設定中啟用 CHAP 驗證，則會提示您提供認證以存取 iSCSI 目標。指定與 iSCSI 目標設定相同的使用者名稱和目標密碼。按一下 **[確定]**。
8. 按一下 **[關閉]** 以關閉視窗。

要在 PE 可開機媒體上新增 iSCSI 裝置

1. 按一下**[工具]** > **[執行 iSCSI 安裝程式]**。
2. 按一下**[探查]**標籤。
3. 在 **[目標入口]** 下，按一下 **[新增]**，然後指定 IP 位址以及 iSCSI 目標入口的連接埠。按一下 **[確定]**。
4. 分別按一下 **[一般]** 標籤以及 **[變更]**，然後指定任何容許存取該裝置的 iSCSI 起始端的名稱。
5. 分別按一下 **[目標]** 標籤以及 **[重新整理]**，然後從清單中選擇 iSCSI 目標，再按一下 **[連線]**。按一下 **[確定]** 以連線至 iSCSI 目標。
6. 若在 iSCSI 目標設定中啟用 CHAP 驗證，則會出現 **[驗證失敗]** 錯誤。在此種情況下，分別按一下 **[連線]** 以及 **[進階]**，選擇 **[啟用 CHAP 登入]** 核取方塊，隨後指定與 iSCSI 目標設定相同的使用者名稱和目標密碼。按一下 **[確定]** 關閉視窗，然後按一下 **[確定]** 以連線至 iSCSI 目標。
7. 按一下 **[確定]** 關閉視窗。

Startup Recovery Manager

Startup Recovery Manager 是位於您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。

Startup Recovery Manager 對行動使用者尤為方便。如果發生故障，請將電腦重新開機，並等待出現「**按下 F11，執行 Acronis Startup Recovery Manager...**」的提示，然後按下 F11。程式將會啟動，

接著您便可以執行復原。在已安裝 GRUB 開機載入器的電腦上，從開機功能表中選擇 Startup Recovery Manager，而不是在重新開機期間按下 F11。

外出時，您也可以使用 Startup Recovery Manager 備份。

若要使用 Startup Recovery Manager，您必須將其啟用。因此，您要啟用開機過程中的提示 **[按下 F11，執行 Acronis Startup Recovery Manager]** (或者，如果您要使用 GRUB 開機載入器，請將 **[Startup Recovery Manager]** 項目新增至 GRUB 功能表)。

注意事項
若要在系統磁碟區未加密的電腦上啟用 Startup Recovery Manager，該電腦至少要有 100 MB 的可用空間。如果復原作業需要重新啟動電腦，則需要另外 100 MB 的可用空間。

如果電腦至少有一個其他非加密磁碟區，您可以在具有 BitLocker 加密磁碟區的電腦上，啟用 Startup Recovery Manager。未加密的磁碟區必須至少有 500 MB 的可用空間。如果復原作業需要重新啟動電腦，則電腦必須有另外 500 MB 的可用空間。

重要事項
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。

除非使用 GRUB 開機載入器，並將其安裝在主開機記錄 (MBR) 中，否則啟動 Startup Recovery Manager 會使用其本身的開機程式碼覆寫 MBR。因此，如果您有安裝第三方開機載入器，可能需要重新啟用這類開機載入器。

在 Linux 中使用 GRUB 以外 (例如 LILO) 的開機載入器時，請考慮在啟用 Startup Recovery Manager 之前，將其安裝至 Linux 根 (或 boot) 磁碟分割開機記錄中，而不要安裝在 MBR 中。否則，在啟動之後需要以手動方式重新組態該開機載入程式。

啟動 Startup Recovery Manager

在執行 Windows 用代理程式或 Linux 用代理程式的電腦上，您可以在 Cyber Protect Web 主控台中啟用 Startup Recovery Manager。

若要在 Cyber Protect Web 主控台中啟用 Startup Recovery Manager

1. 選擇您要在其上啟用 Startup Recovery Manager 的電腦。
2. 按一下**[詳細資料]**。
3. 啟用 **Startup Recovery Manager** 開關。
4. 請等待軟體啟用 Startup Recovery Manager。

若要在沒有代理程式的電腦上啟用 Startup Recovery Manager

1. 從可開機媒體將機器開機
2. 按一下 **[工具]** > **[啟用 Startup Recovery Manager]**。
3. 請等待軟體啟用 Startup Recovery Manager。

停用 Startup Recovery Manager

若要停用Startup Recovery Manager，請重複啟用程序，然後選擇對應的相反動作。停用可停用開機過程中的提示 **[按下 F11，執行 Acronis Startup Recovery Manager]**(或 GRUB 中的功能表項目)。

如果 Startup Recovery Manager 未啟用，當其無法開機時，您將需要執行以下一項作業來復原系統：

- 從個別的可開機媒體將機器開機
- 從 PXE 伺服器或 Microsoft 遠端安裝服務 (RIS) 使用網路開機

Acronis PXE Server

Acronis PXE Server 可讓您透過網路將電腦開機至 Acronis 可開機元件。

網路開機：

- 減少讓現場技術人員將可開機媒體安裝至必須開機的系統中的需求
- 在群組作業期間，相比使用實體可開機媒體，減少了啟動多台電腦所需的時間。

您可以使用 Acronis Bootable Media Builder 將可開機元件上傳至 Acronis PXE Server。要上傳可開機元件，請啟動可開機媒體建立程式，然後依「Linux 可開機媒體」中所述的逐步說明操作。

若您的網路上有動態主機控制通訊協定 (DHCP) 伺服器，您就可以從 Acronis PXE Server 將多部電腦開機。然後，已開機的電腦的網路介面將自動獲取 IP 位址。

限制：

Acronis PXE Server 不支援 UEFI 開機載入器。

安裝 Acronis PXE 伺服器

安裝 Acronis PXE 伺服器

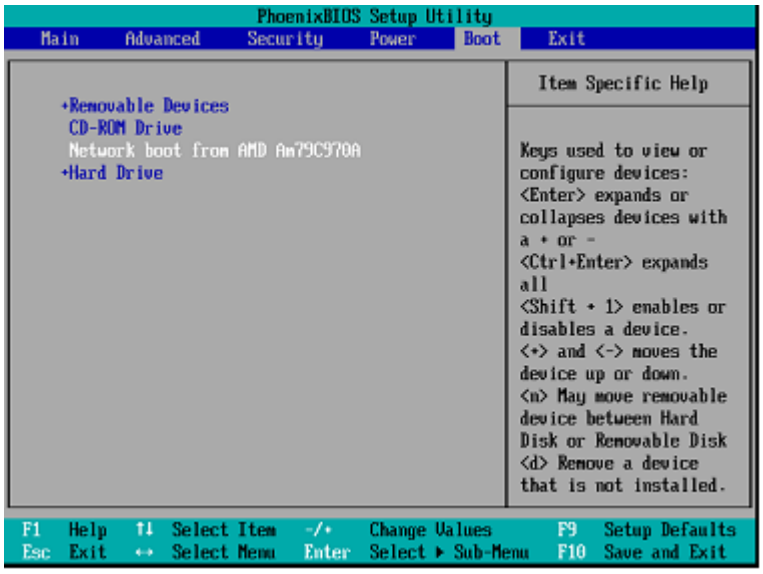
1. 以系統管理員身分登入，並啟動 Acronis Cyber Protect 安裝程式。
2. [選擇性步驟]：若要變更安裝程式的語言，請按一下 **[設定語言]**。
3. 接受授權合約和隱私權聲明的條款，然後按一下 **[下一步]**。
4. 按一下**[自訂安裝設定]**。
5. 在**[要安裝的項目]**旁，按一下**[變更]**。
6. 選擇 **[PXE 伺服器]** 核取方塊。如果不想在此電腦上安裝其他元件，請清除元件對應的核取方塊。按一下**[完成]** 以繼續。
7. 選擇性步驟：變更安裝設定。
8. 按一下**[安裝]** 以開始安裝。
9. 安裝完成後，請按一下**[關閉]**。

安裝後，Acronis PXE 伺服器將以服務的形式立即執行。稍後它會在每個系統重新啟動時自動啟動。您可採用與其他 Windows 服務相同的方式停止和啟動 Acronis PXE 伺服器。

設定電腦從 PXE 開機

對裸機而言，電腦的 BIOS 支援網路開機已經足夠。

在硬碟有作業系統的電腦上，BIOS 則必須經過設定，使網路介面卡成為第一個開機裝置，或至少是優先於硬碟裝置的開機裝置。以下範例顯示其中一個合理的 BIOS 設定。如果您沒有插入可開機媒體，電腦將從網路開機。



在有些 BIOS 版本中，您必須在啟用網路介面卡後將變更儲存至 BIOS 中，這樣介面卡才會顯示在開機裝置清單中。

如果硬體有多張網路介面卡，請確定 BIOS 支援的介面卡已插入網路線。

跨子網路運作

若要讓 Acronis PXE Server 能夠在另一個子網路中運作 (跨交換器)，請設定交換器以轉送 PXE 流量。PXE 伺服器 IP 位址的設定是依每一介面為基礎，並使用 IP 協助程式功能進行，就和 DHCP 伺服器的位址一樣。如需詳細資訊，請參閱：https://docs.microsoft.com/en-us/troubleshoot/mem/configmgr/boot-from-pxe-server。

保護行動裝置

備份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備份應用程式：

- iOS 10.3 和更新版本 (iPhone、iPod 和 iPad)
- Android 5.0 和更新版本

可備份的內容

- 連絡人
- 相片
- 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。如果此設定已開啟：
  - 若是 Android 7.0 或更新版本，備份應用程式會自動即時偵測新資料，並將其上傳到雲端。
  - 若是 Android 5 和 6，它會每三小時檢查一次變更。您可以在應用程式設定中關閉連續備份功能。
- **[僅使用 Wi-Fi]** 選項在應用程式設定中預設為啟用狀態。如果此設定已開啟，則只會在有 Wi-Fi 連線時，備份應用程式才會備份資料。如果失去 Wi-Fi 連線，備份程序將不會起動。若要讓應用程式也使用行動數據連線，請將此選項關閉。
- 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，備份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)。如果此設定已開啟，則只會在您的裝置電池電力充足時，備份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。此選項適用於 Android 8 或更新版本。
- 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 Web 主控台，將相片、影片或連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。

- 在備份應用程式中，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 Web 主控台。
- [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。

何處取得備份應用程式

1. 在行動裝置上開啟瀏覽器，然後移至 https://backup.acronis.com/。
2. 使用您的帳戶登入。
3. 按一下**[所有裝置]** > **[新增]**。
4. 在**[行動裝置]**下選擇裝置類型。
   視乎裝置類型，您將被重新導向至 App Store 或 Google Play Store。
5. [僅適用於 iOS 裝置] 按一下 **[獲取]**。
6. 按一下 **[安裝]** 以安裝備份應用程式。

如何開始備份資料

1. 開啟應用程式。
2. 使用您的帳戶登入。

點選 **[設定]** 可建立第一個備份。

1. 選擇您要備份的資料類別。系統預設為全選所有類別。
2. [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]**。
3. 點選**[備份]**。
4. 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

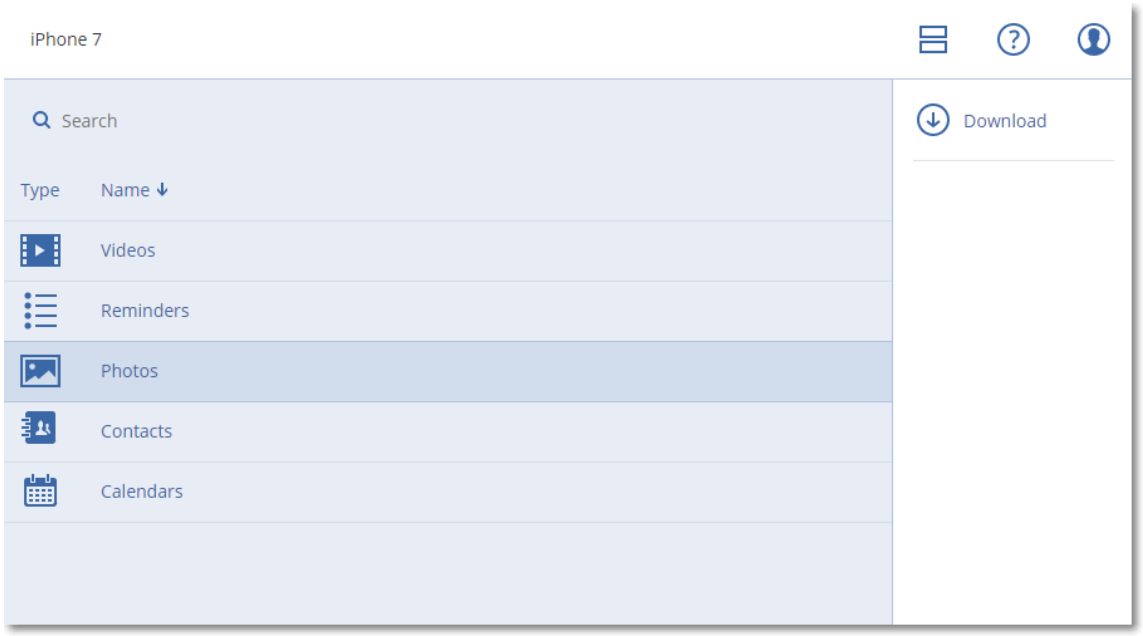
1. 開啟備份應用程式。
2. 點選 **[瀏覽]**。
3. 點選裝置名稱。
4. 執行下列其中一項操作：

- 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。

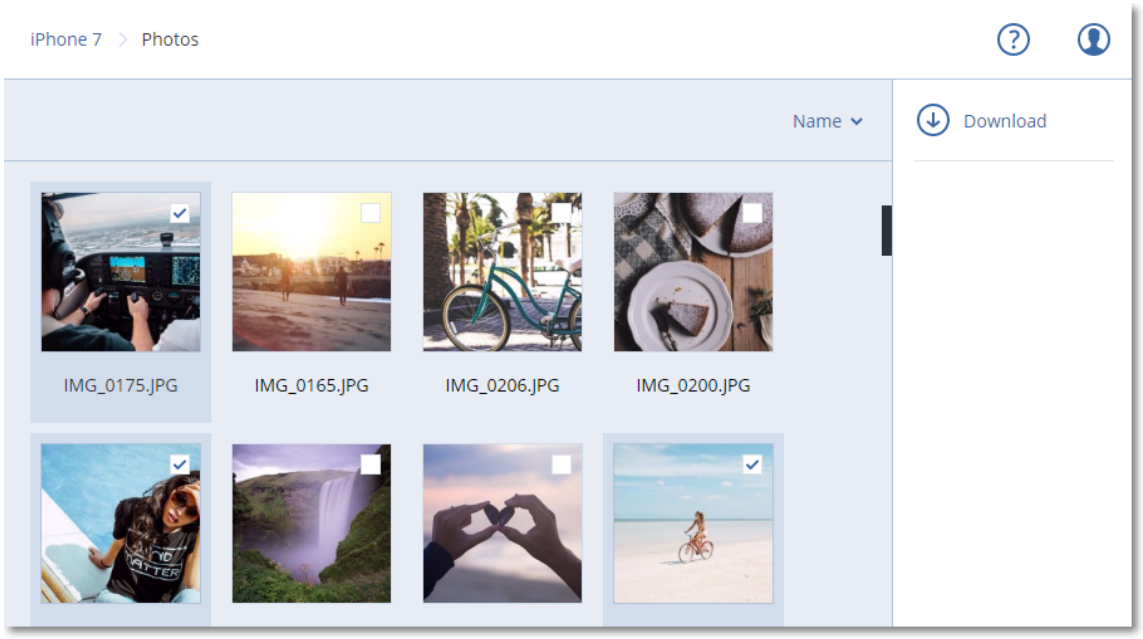
5. 執行下列其中一項操作：
   - 若要復原單一資料項目，請點選此項目。
   - 若要復原多個資料項目，點選 **[選擇]**，然後點選所需資料項目的核取方塊。
6. 點選 **[復原]**。

如何透過 Cyber Protect Web 主控台檢閱資料

1. 在電腦上開啟瀏覽器，並輸入 Cyber Protect Web 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 Microsoft 應用程式

重要事項
本節中所述的部分功能僅適用於內部部署。

保護 Microsoft SQL Server 和 Microsoft Exchange Server

有兩種方法可以保護這些應用程式：

- **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。

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 資料庫的 15%。或者，您可以先變更暫存檔的位置，然後再建立 Exchange 備份，如 https://kb.acronis.com/content/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：

- 若是實體機器，請確保已啟用 [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。

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。
- 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 > 中所述的設定 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)」。
   - 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 > 中所述的設定 Exchange 用代理程式，則可以選擇要備份的信箱。
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)

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。

   注意事項
   在其中一個節點上安裝該代理程式後，軟體將在 **[裝置]** > **[Microsoft SQL]** > **[資料庫]** 下顯示 AAG 及其節點。若要在剩餘節點上安裝適用於 SQL 的代理程式，請選擇 AAG，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]**。

2. 選擇要設為備份的 AAG 或資料庫，如「選擇 SQL 資料庫」中所述。
   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)

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。

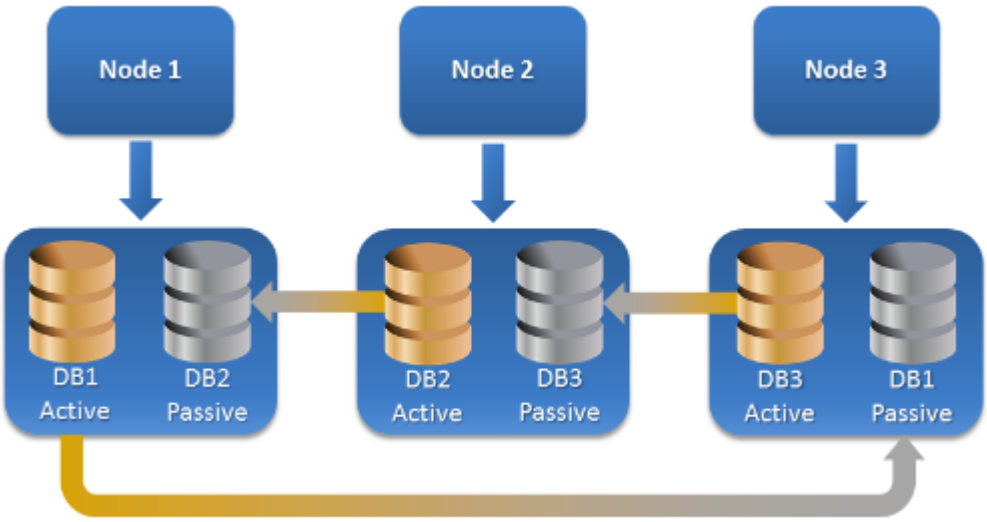
叢集感知備份

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 Web 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，如「選擇 Exchange Server 資料」中所述選擇 DAG。
2. 設定「叢集備份模式」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. 請遵循「復原 Exchange 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。

應用程式感知備份

實體機器、ESXi 虛擬機器和 Hyper-V 虛擬機器中可以使用應用程式感知磁碟層級備份。

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：

1. 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。
2. 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。
3. 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」。
4. 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

若是執行 Windows Server 2022 的 Hyper-V 虛擬機器，則在無代理程式模式下不支援應用程式感知備份，亦即，當 Hyper-V 用代理程式執行備份時。若要保護這些電腦上的 Microsoft 應用程式，請在客體作業系統內安裝 Windows 用代理程式。

VMware 用代理程式 (虛擬裝置) 和 VMware 用代理程式 (Linux) 可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。若要從這些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。

其他需求列在 "必要條件" (第 380 頁) 和 "應用程式感知備份所需的使用者權限" (第 388 頁) 中。

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：

  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。
- 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。

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 原則，您必須在設定應用程式感知備份時，提供內建網域系統管理員 (DOMAIN\Administrator) 的認證。

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。

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. [選擇性步驟] 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 [**備份**]。

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

本節說明如何從資料庫備份和應用程式感知備份復原。

如果 SQL 用代理程式已安裝在執行執行個體的電腦上，您可以將 SQL 資料庫復原至 SQL Server 執行個體。

如果您使用的是 Windows 驗證，您將需要在電腦上提供 **[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，您將需要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。

或者，您可以將資料庫復原為檔案。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，這項功能即可派上用場。如 < 附加 SQL Server 資料庫 > 中所述，您可以將 SQL 資料庫檔案附加至 SQL Server 執行個體。

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。

系統資料庫的復原方式和使用者資料庫大致相同。系統資料庫復原方式的特點請見 < 系統資料庫復原 > 。

將 SQL 資料庫復原至SQL Server 執行個體

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。
   - 從資料庫備份復原時，按一下 **[裝置]** > **[Microsoft SQL]**，然後選擇所要復原的資料庫。
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 SQL 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 SQL 資料庫的目標電腦。
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]** > **[SQL 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]**> **[將資料庫復原為執行個體]**。
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。您可以選擇復原資料庫至其他 SQL Server 執行個體 (在相同機器上執行)。

若要在相同的執行個體中復原為不同的資料庫：

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. [選擇性步驟] [不適用於復原至其原始執行個體的資料庫作為新的資料庫] 若要在復原後變更資料庫狀態，按一下資料庫名稱，然後選擇下列其中一個狀態：

   - **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。

7. 按一下 **[開始復原]**。

復原進度會顯示在 **[活動]** 索引標籤上。

將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。
   - 從資料庫備份復原時，按一下 **[裝置]** > **[Microsoft SQL]**，然後選擇所要復原的資料庫。
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 SQL 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。

   依照上述動作任一而選擇瀏覽的電腦，將成為復原 SQL 資料庫的目標電腦。
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]** > **[SQL 資料庫]**，選擇要復原的資料庫，然後按一下 **[作為檔案復原]**。
   - 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。

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

本節說明如何從資料庫備份、應用程式感知備份以及信箱備份，來復原 Exchange 信箱和信箱項目。信箱或信箱項目可以復原至即時 Exchange Server 或 Microsoft 365。

下列項目可以復原：

- 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 383 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。

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

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 信箱" (第 401 頁)。

復原信箱

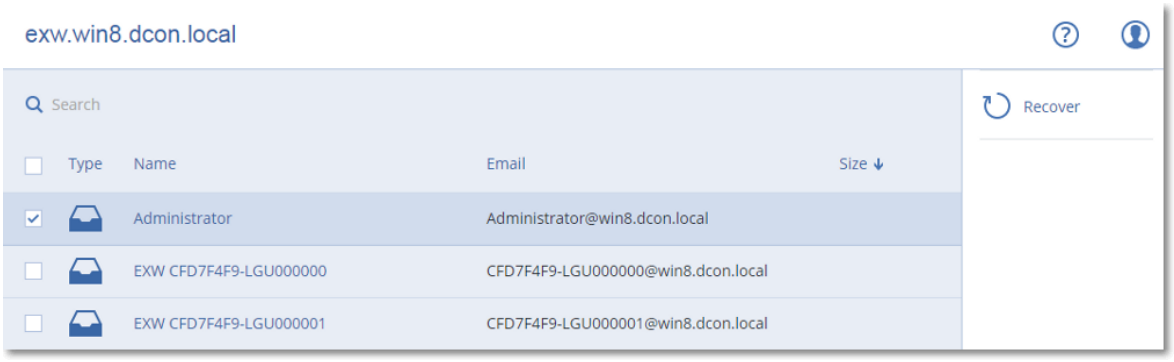
若要從應用程式感知備份或資料庫備份復原信箱

1. [僅在從資料庫備份復原至 Microsoft 365 時] 如果 Office 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：
   - 若組織中沒有 Office 365 用代理程式，則在已備份的電腦 (或在有相同 Microsoft Exchange Server 版本的另一部電腦) 上安裝 Office 365 用代理程式。
   - 若組織中已安裝 Office 365 用代理程式，則從已備份電腦 (或有相同 Microsoft Exchange Server 版本的另一部電腦) 上，將程式庫複製到裝有 Office 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 Office 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。
9. 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。
   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 "所需的使用者權限" (第 389 頁) 中。
10. [選擇性步驟] 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 Office 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：
   - 若組織中沒有 Office 365 用代理程式，則在已備份的電腦 (或在有相同 Microsoft Exchange Server 版本的另一部電腦) 上安裝 Office 365 用代理程式。

- 若組織中已安裝 Office 365 用代理程式，則從已備份電腦 (或有相同 Microsoft Exchange Server 版本的另一部電腦) 上，將程式庫複製到裝有 Office 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。

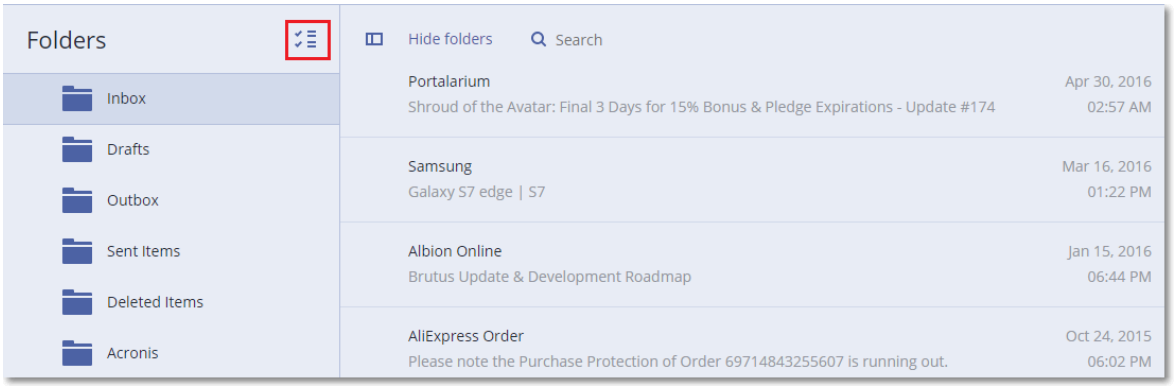
   您可以選取下列搜尋選項。不支援萬用字元。
   - 電子郵件訊息：依主題、寄件者、收件者及日期搜尋。
   - 事件：依主題及日期搜尋。
   - 工作：依主題及日期搜尋。
   - 連絡人：依姓名、電子郵件地址和電話號碼搜尋。

   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 Office 365]**。

   若要復原至 Exchange Server，保留**復原至**中的 **Microsoft Exchange** 預設值。

10. [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。

    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 "所需的使用者權限" (第 389 頁) 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 Office 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 Microsoft 365 信箱

重要事項

本節適用於 Acronis Cyber Protect 的內部部署。如果您使用的是雲端部署，請參閱 https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-microsoft-365-data.html。

如需有關授權選項的詳細資訊，請參閱 Acronis Cyber Backup for Microsoft 365 授權。

為什麼要備份 Microsoft 365 信箱？

雖然 Microsoft 365 屬於雲端服務，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，您可保留 Microsoft 365 信箱的本機副本。

復原

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。

復原功能僅限於 Microsoft 365 或即時 Exchange Server 中執行。

將信箱復原至現有的 Microsoft 365 信箱時，系統會覆寫符合 ID 的現有項目。將信箱復原至現有的 Exchange Server 信箱時，現有項目會保持原樣。復原的項目會放置其旁邊。

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。

限制

- 將保護計劃套用至超過 500 個信箱可能會降低備份效能。若要保護大量信箱，請建立數個保護計劃，並排程這些計劃在不同的時間執行。
- 封存信箱 (**就地封存**) 無法進行備份。
- 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]**、**[探索保留]**、**[行事曆記錄]**) 不包含在信箱備份中。

- 無法復原至新的 Microsoft 365 信箱。您須先手動建立新的 Microsoft 365 使用者，然後將項目復原至此使用者的信箱。
- 不支援復原至不同的 Microsoft 365 組織。
- Exchange Server 可能不支援 Microsoft 365 所支援的某些項目類型或屬性。復原至 Exchange Server 時將略過這些項目類型或屬性。

新增 Microsoft 365 組織

若要新增 Microsoft 組織，您需要知道您的應用程式 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。

新增 Microsoft 365 組織

1. 在已連線至網際網路的 Windows 電腦上安裝 Office 365 用代理程式。組織內只能有一個 Office 365 用代理程式。
2. 在 Cyber Protect Web 主控台中，按一下 **[Microsoft Office 365]**。
3. 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。
4. 按一下 **[登入]**。

因此，貴組織的資料項目會出現在 Cyber Protect Web 主控台的 **[Microsoft Office 365]** 索引標籤上。

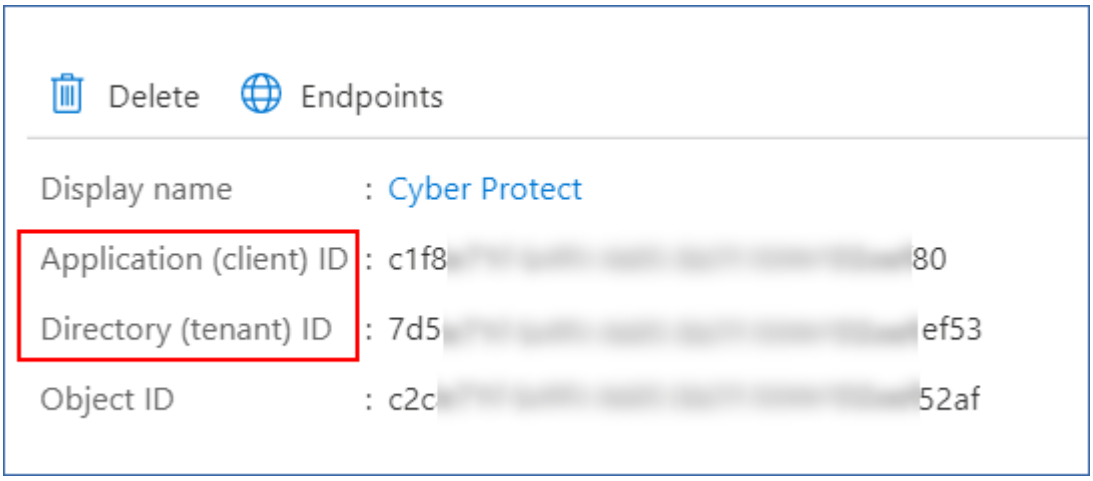
取得應用程式 ID 和應用程式密碼

若要為 Microsoft 365 使用新型驗證，您需要在 Azure Active Directory 中建立自訂應用程式，並為其授予特定的 API 權限。因此，您將取得您需要在 Web 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**。

若要在 Azure Active Directory 中建立應用程式

1. 以系統管理員身分，登入 Azure 入口網站。
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 Protect。
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 Azure 入口網站中，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)。



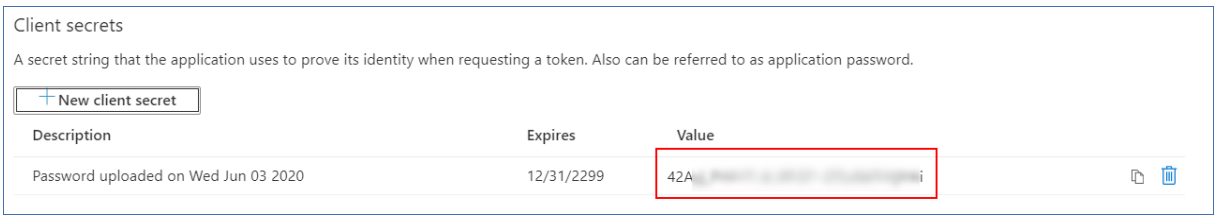
如需有關如何在 Azure 入口網站中建立應用程式的詳細資訊，請參閱 Microsoft 文件。

若要為您的應用程式授予所需的 API 權限

1. 在 Azure 入口網站中，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 Azure 入口網站中，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. 在 Cyber Protect Web 主控台中，前往 **[裝置]** > **[Microsoft Office 365]**。
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。
5. 按一下 **[登入]**。

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。

選取信箱

1. 在 Cyber Protect Web 主控台中，前往 **[裝置]** > **[Microsoft Office 365]**。
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. [僅在復原至 Exchange Server 時] 確保有一個 Exchange 使用者，其登入名稱與要復原信箱之使用者的使用者名稱相同。若沒有，則建立使用者。查看 "對於使用者帳戶的要求" (第 395 頁) 中對此使用者要求的完整清單。
2. 在 Cyber Protect Web 主控台中，前往 **[裝置]** > **[Microsoft Office 365]**。
3. 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]**。
4. 選擇復原點請注意，復原點是依照位置進行篩選。
5. 請按一下**[復原]** > **[信箱]**。
6. 若要復原至 Exchange Server，請在 **[復原至]** 中選擇 **[Microsoft Exchange]**。如 "復原信箱" (第 396 頁) 中所述，繼續復原作業，從步驟 9 開始。此程序無需執行更多步驟。
   若要復原至 Microsoft 365，請保留 **[復原至]** 中的 **[Microsoft Office 365]** 預設值。
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]**。

復原信箱項目

1. [僅在復原至 Exchange Server 時] 確保有一個 Exchange 使用者，其登入名稱與要復原信箱之使用者的使用者名稱相同。若沒有，則建立使用者。查看 "對於使用者帳戶的要求" (第 395 頁) 中對此使用者要求的完整清單。
2. 在 Cyber Protect Web 主控台中，前往 **[裝置]** > **[Microsoft Office 365]**。

3. 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]**。
4. 選擇復原點請注意，復原點是依照位置進行篩選。
5. 按一下**[復原]** > **[電子郵件訊息]**。
6. 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： 
7. 按一下 **[復原]**。
8. 若要復原至 Exchange Server，請在 **[復原至]** 中選擇 **[Microsoft Exchange]**。
   若要復原至 Microsoft 365，請保留 **[復原至]** 中的 **[Microsoft Office 365]** 預設值。
9. [僅在復原至 Exchange Server 時] 若要選擇或變更目標電腦，按一下 **[具有 Microsoft Exchange Server 的目標電腦]**。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。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。
   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 "所需的使用者權限" (第 389 頁) 中。
10. **[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。
11. [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。
12. 按一下 **[開始復原]**。

保護 Google Workspace 資料

此功能僅在 Acronis Cyber Protect 雲端部署中可用。如需此功能的詳細描述，請參閱 https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-google-workspace-data.html。

保護 Oracle 資料庫

對 Oracle Database 的保護詳述於另一個文件中：https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_OracleBackup_whitepaper.pdf。

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。

建議您執行此臨時虛擬機器三天。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

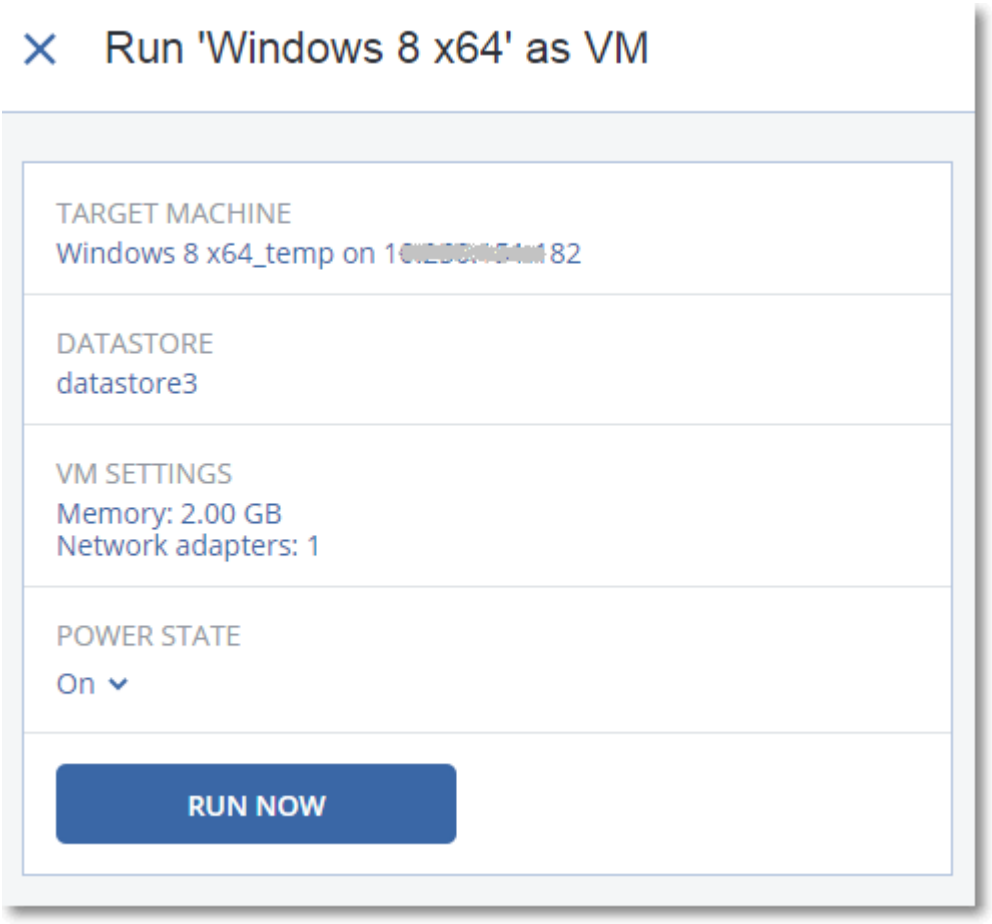
- **災難復原**
  立即讓故障電腦複本上線。
- **測試備份**
  從備份執行電腦並確保客體 OS 和應用程式均運作正常。
- **存取應用程式資料**
  在電腦執行時，使用應用程式原生管理工具存取和擷取所需的資料。

必要條件

- 必須在網路保護服務中至少註冊一個 VMware 用代理程式或 Hyper-V 用代理程式。
- 備份可以儲存在網路資料夾、儲存節點或已安裝 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。虛擬機器無法從儲存在 SFTP 伺服器、磁帶裝置或 Secure Zone 的備份執行。
- 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. [選擇性] 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. [選擇性] 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. [選擇性] 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. [選擇性] 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。

刪除電腦

我們不建議直接在 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. [選擇性步驟] 請指定新的電腦名稱。
4. [選擇性步驟] 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。

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。

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. 選擇性步驟：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. [選擇性] 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. [選擇性] 按一下齒輪圖示以修改複寫選項。
8. 按一下**[套用]**。
9. [選擇性] 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. [選擇性] 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. [選擇性] 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. [選擇性步驟] 變更虛擬機器的名稱。
5. [選擇性] 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. [選擇性] 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. 選擇性步驟: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. [選擇性] 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]**。

變更區塊追蹤 (CBT)

此選項與備份選項 [變更區塊追蹤 (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。

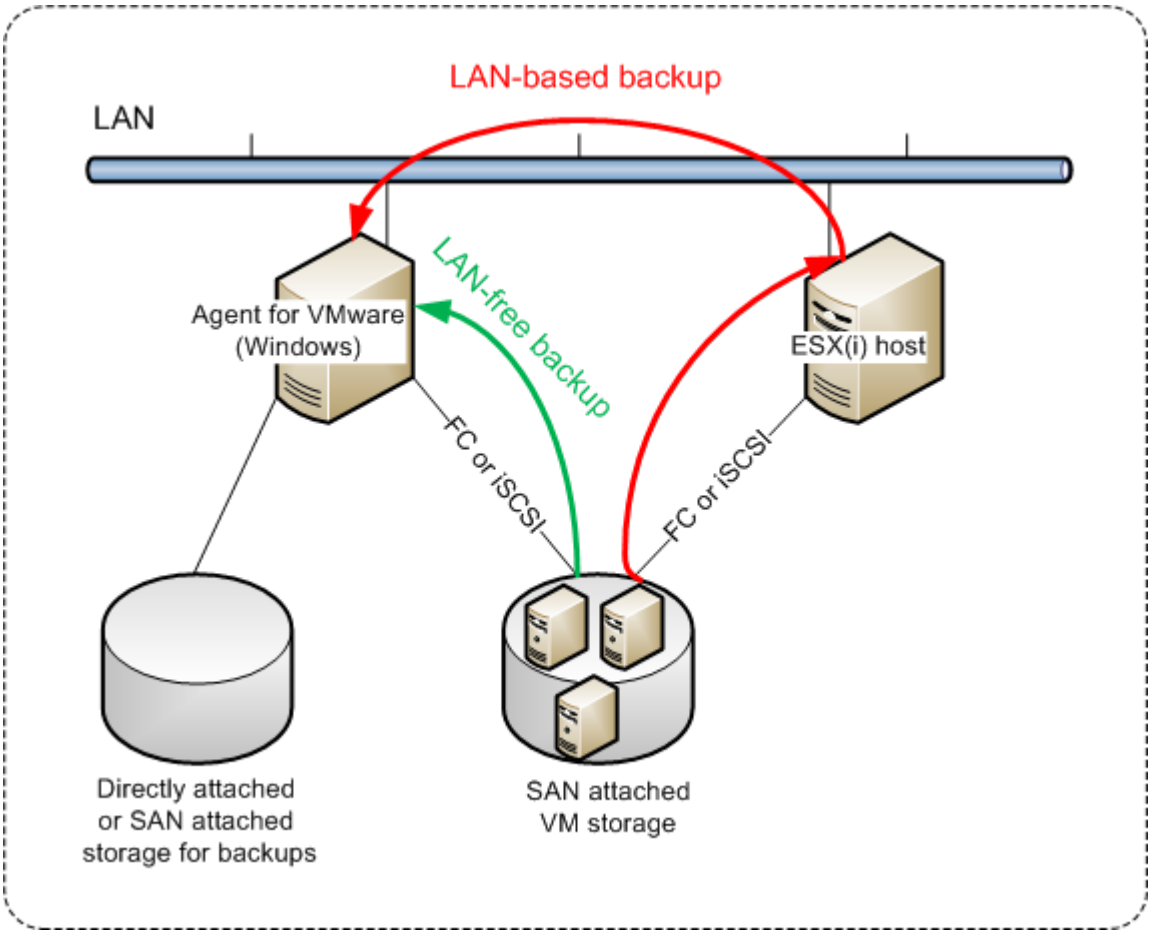
如此一來，軟體將會繼續更新複本。所有複寫將會增量。

不透過 LAN 備份

如果您的生產 ESXi 主機負載繁重，而不適合執行虛擬裝置，不妨在 ESXi 基礎架構外的實體機器上安裝 VMware 用代理程式 (Windows)。

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。

     要避免 LUN 初始化，將在 VMware 用代理程式 (Windows) 安裝期間自動將 **SAN 原則**設定為**全部離線**。

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。

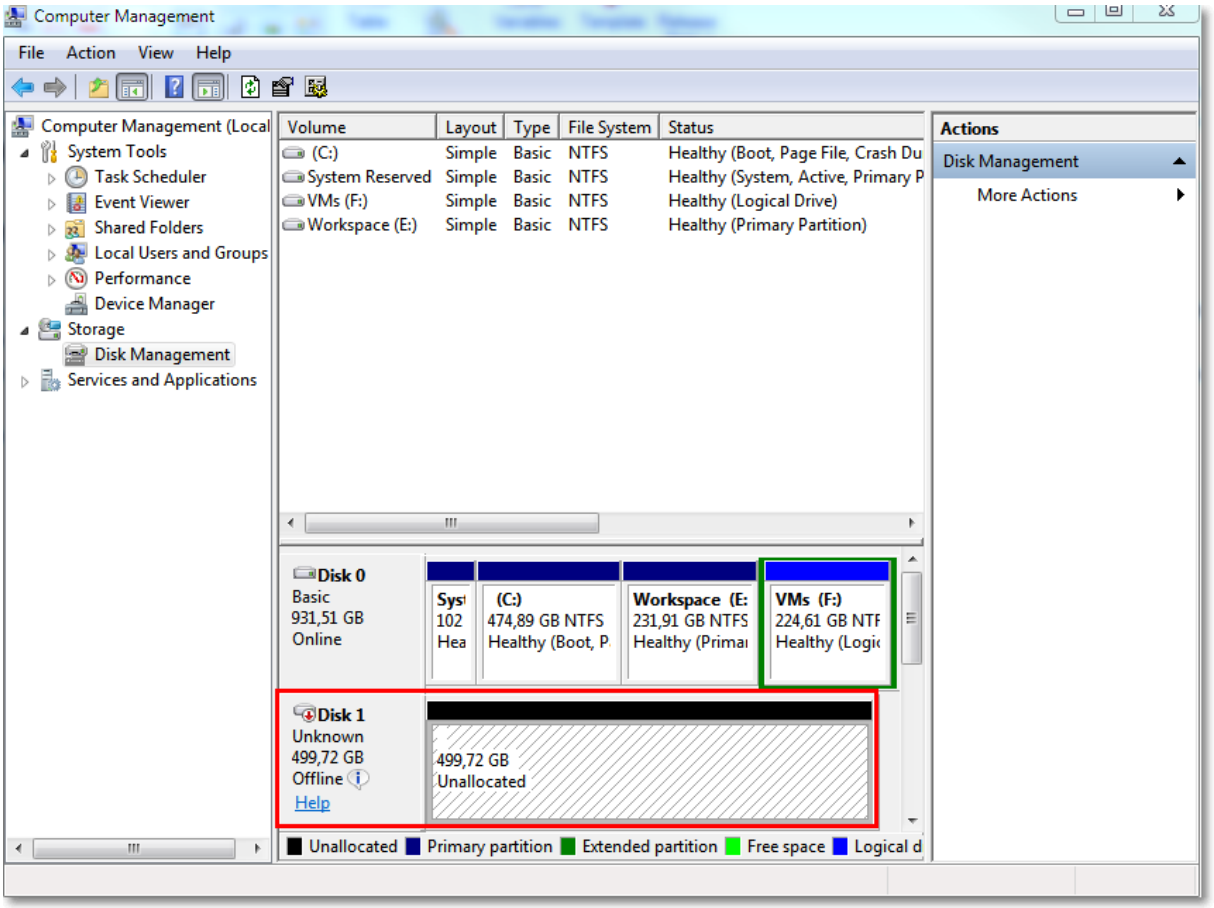
設定 iSCSI 起始端

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 SAN 硬體快照

如果 VMware vSphere 將存放區域網路 (SAN) 儲存系統作為資料存放區，則在執行備份時可啟用 VMware (Windows) 代理程式以使用 SAN 硬體快照。

重要事項
僅支援 NetApp SAN 儲存。

為何使用 SAN 硬體快照？

VMware 用代理程式需要虛擬機器快照才可建立一致的備份。由於代理程式從快照讀取虛擬磁碟內容，所以快照必須保存用於整個備份期間。

預設情況下，代理程式使用 ESXi 主機建立的原生 VMware 快照。保存快照時，虛擬磁碟檔案處於唯讀狀態，且主機將完成的所有變更寫入單獨的差異檔案中。備份過程完成後，主機刪除快照，即將差異檔案與虛擬磁碟檔案合併。

維護和刪除快照均會影響虛擬機器效能。如果進行大量的虛擬磁碟和快速資料變更，則這些作業的完成需很長時間，在該時間內，效能可能會降低。在極端情況下，如果多台電腦同時備份，則增長的差異檔案幾乎可能填滿資料存放區，並導致所有虛擬機器關機。

您可透過將快照卸載到 SAN 減少 hypervisor 資源使用率。在這種情況下，作業序列如下：

1. ESXi 在備份過程開始時取 VMware 快照，以使虛擬磁碟處於一致狀態。
2. SAN 建立包含虛擬機器及其 VMware 快照的磁碟區或 LUN 硬體快照。此作業通常需要幾秒鐘。
3. ESXi 刪除 VMware 快照。VMware 用代理程式從 SAN 硬體快照讀取虛擬磁碟內容。

由於 VMware 快照僅維持幾秒鐘，故虛擬機器效能下降最小化。

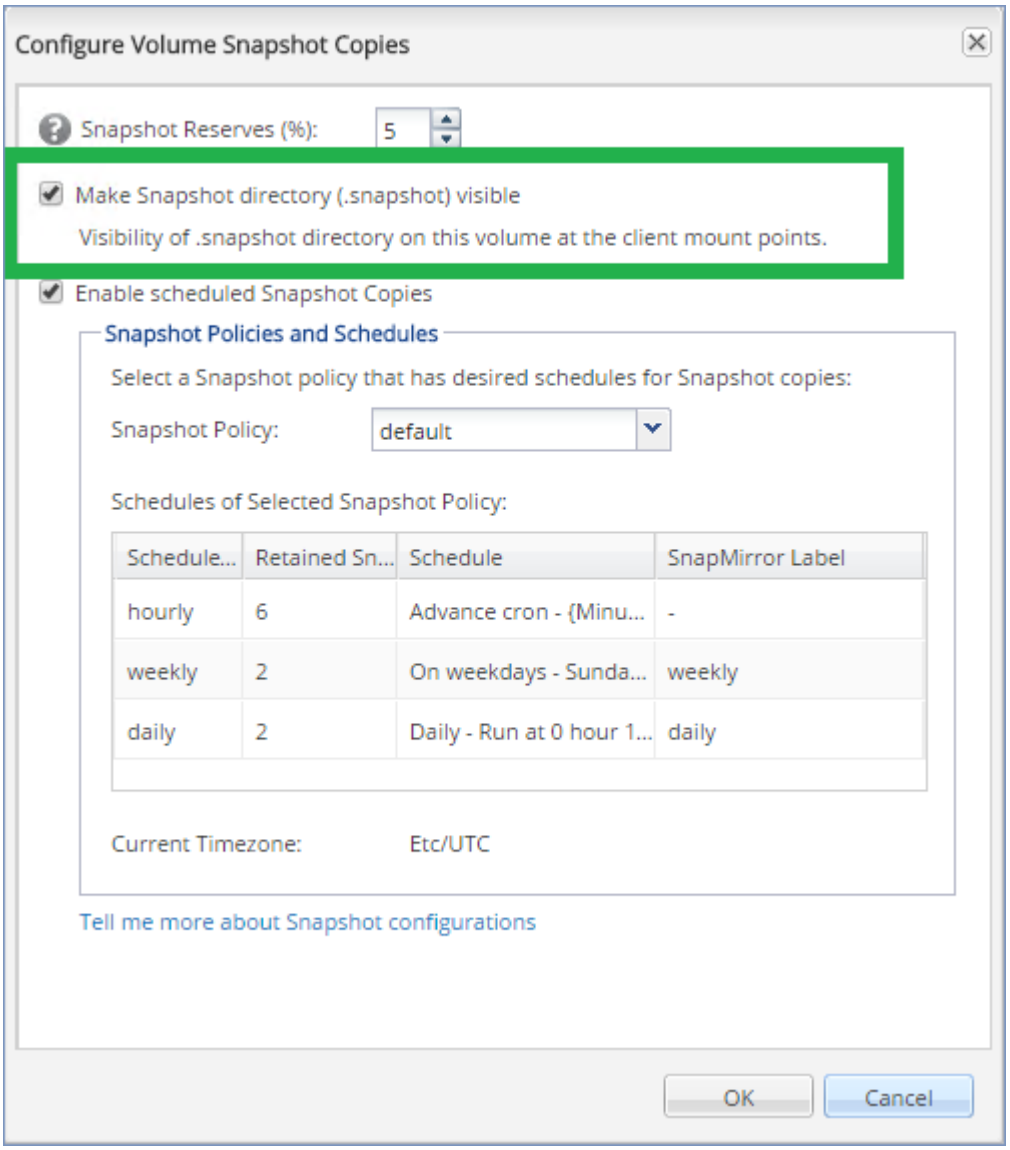
使用 SAN 硬體快照時需要什麼？

備份虛擬機器時，如果要使用 SAN 硬體快照，請確保符合以下所有條件：

- NetApp SAN 儲存符合「NetApp SAN 儲存要求」中所述的要求。
- 執行 VMware 用代理程式 (Windows) 的電腦配置如「配置執行 VMware 用代理程式的電腦」中所述。
- SAN 存放區在在管理伺服器上登錄。
- [如果存在並未參與上述登錄的 VMware 用代理程式] 位於 SAN 存放區的虛擬機器被指派給已啟用 SAN 的代理程式，如「虛擬機器繫結」中所述。
- 在保護計劃選項中啟用 [SAN 硬體快照] 備份選項。

NetApp SAN 存放區要求

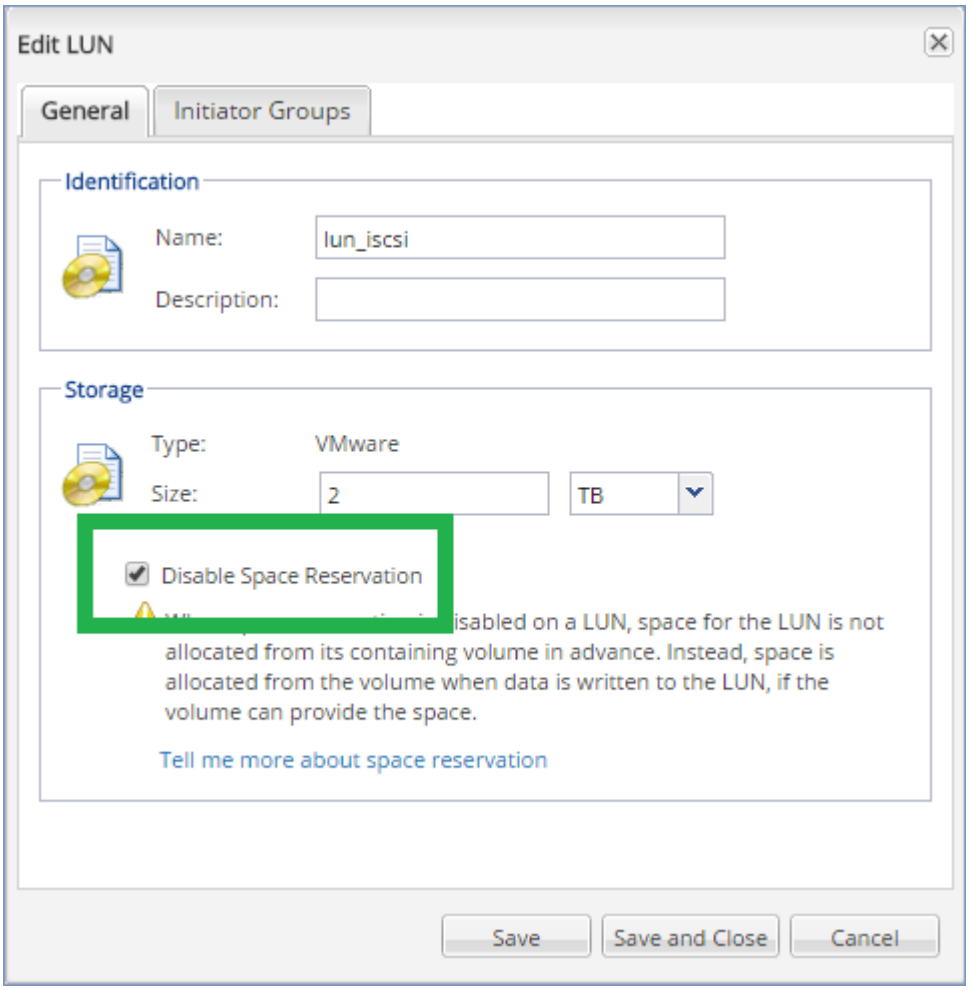
- SAN 存放區必需用作 NFS 或 iSCSI 資料存放區。
- SAN 必須在 **Clustered Data ONTAP (cDOT)**模式下運行 Data ONTAP 8.1 或更新版本。不支援 **7-mode** 模式
- 在 NetApp OnCommand System Manager 中，必須為資料存放區所在磁碟區選取 **[快照副本]**> **[設定]** > **[使快照目錄 (.snapshot) 可見]** 核取方塊。



- [適用於 NFS 資料儲存] 必須在建立資料儲存時指定的儲存虛擬機器 (SVM) 上啟用從 Windows NFSv3 用戶端存取 NFS 共用。可以透過以下命令啟用存取權限：

```
vserver nfs modify -vserver [SVM name] -v3-ms-dos-client enable
```

  如需詳細資訊，請參閱 NetApp 最佳實踐文件：https://kb.netapp.com/support/s/article/ka21A0000000k89QAA/top-windows-nfsv3-0-issues-workarounds-and-best-practices
- [針對 iSCSI 資料存放區] 在 NetApp OnCommand System Manager 中，必須為資料存放區所在的 iSCSI LUN 選取 **[停用空間保留]** 核取方塊。



設定執行 VMware 用代理程式的電腦

根據 SAN 儲存體是用作 NFS 還是 iSCSI 資料存放區，請參閱下方對應的小節。

設定 iSCSI Initiator

確保符合以下所有條件：

- 已安裝 Microsoft iSCSI 啟動器。
- Microsoft iSCSI 啟動器服務啟動類型設為 **[自動]** 或 **[手動]**。可以在 **[服務]** 嵌入式管理單元中完成此動作。
- iSCSI 啟動器的設定方式如 < LAN-free 備份 > 的範例區段中所述。

設定 NFS 用戶端

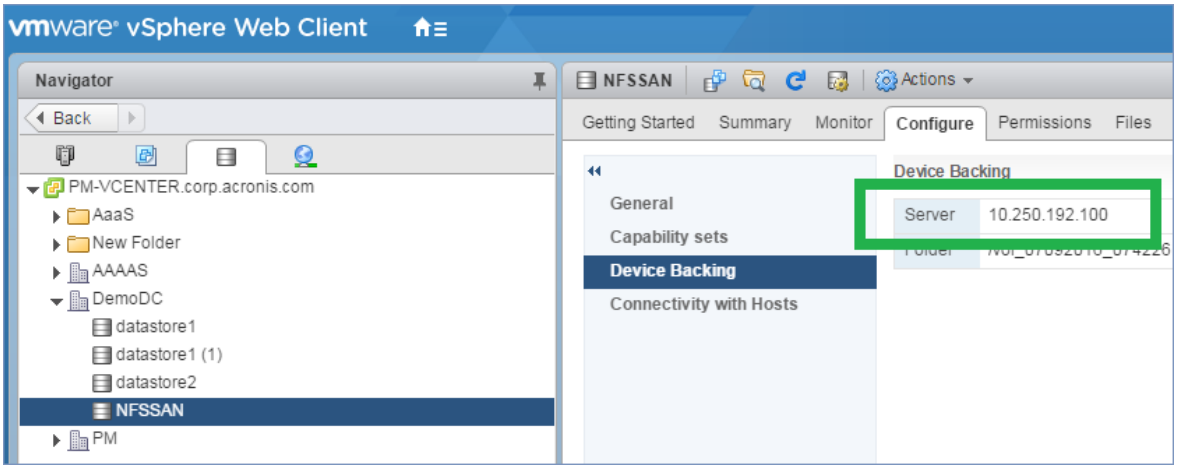
確保符合以下所有條件：

- 已安裝 Microsoft **Services for NFS** (在 Windows Server 2008 中) 或 **Client for NFS** (在 Windows Server 2012 以及更新版本中)。
- NFS 用戶端設為匿名存取。這可以由下列操作來完成：

a. 開啟 [登錄編輯程式]。
b. 找到以下登錄機碼：**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default**
c. 在此機碼中，建立新 **DWORD** 值 (名為 **AnonymousUID**)，並將其值資料設為 0。
d. 在同一機碼中，建立新 **DWORD** 值 (名為 **AnonymousGID**)，並將其值資料設為 0。
e. 重新啟動電腦。

在管理伺服器上註冊 SAN 存放區

1. 請按一下**[設定]** > **[SAN 存放區]**。
2. 按一下**[新增存放區]**。
3. [選擇性步驟] 在 **[名稱]** 中，變更儲存名稱。
   名稱可能會顯示在 **[SAN 存放區]**索引標籤上。
4. 在 **[主機名稱或 IP 位址]** 中，指定建立資料存儲時指定的 NetApp 存儲虛擬機器(SVM，也稱為檔案管理員)。
   若要在 VMware vSphere Web 用戶端中查找所需資訊，請選擇該資料存放區，然後按一下 **[設定]** > **[裝置支援]**。主機名稱或 IP 位址顯示在 **[伺服器]** 欄位中。



5. 請在 **[使用者名稱]** 及 **[密碼]** 中指定 SVM 系統管理員認證。

重要事項
指定的帳戶必須是 SVM 上的本機系統管理員，而不是整個 NetApp 系統管理的管理員。

可以指定現有的使用者或建立新使用者。若要建立新用戶，在 NetApp OnCommand System Manager 中，瀏覽到 **[設定]** > **[安全]** > **[使用者]**，然後建立一個新用戶。

6. 選擇一或多個將會獲得此 SAN 裝置讀取權限的 VMware 用代理程式 (Windows)。
7. 按一下 **[新增]**。

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:**。

虛擬機器繫結

本節概述管理伺服器如何組織 VMware vCenter 內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，管理伺服器會使用相同的演算法重新分配虛擬機器。

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。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，指派給代理程式的虛擬機器會分配給剩餘的代理程式。然而，如果代理程式損毀，或未手動從 vSphere 刪除代理程式，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。
- 如果您正在使用 SAN 硬體快照，則需手動繫結。繫結 VMware 用代理程式 (Windows)，對此，使用位於 SAN 資料存放區的電腦配置 SAN 硬體快照。
- 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。

VM 移轉支援

本節說明虛擬機器在 vSphere 環境中移轉時的預期結果，包括 vSphere 叢集所屬 ESXi 主機之間的移轉。

vMotion

vMotion 將虛擬機器狀態和組態移至其他主機，而電腦磁碟則保持在共用存放區的相同位置。

- VMware 用代理程式的 vMotion (虛擬裝置) 不受支援且已遭到停用。
- 備份期間，虛擬機器的 vMotion 會遭到停用。移轉完成後將會繼續執行備份。

Storage vMotion

Storage vMotion 會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。

- VMware 用代理程式的 Storage vMotion (虛擬裝置) 不受支援且已遭到停用。
- 備份期間，虛擬機器的 Storage vMotion 會遭到停用。移轉後將會繼續執行備份。

管理虛擬化環境

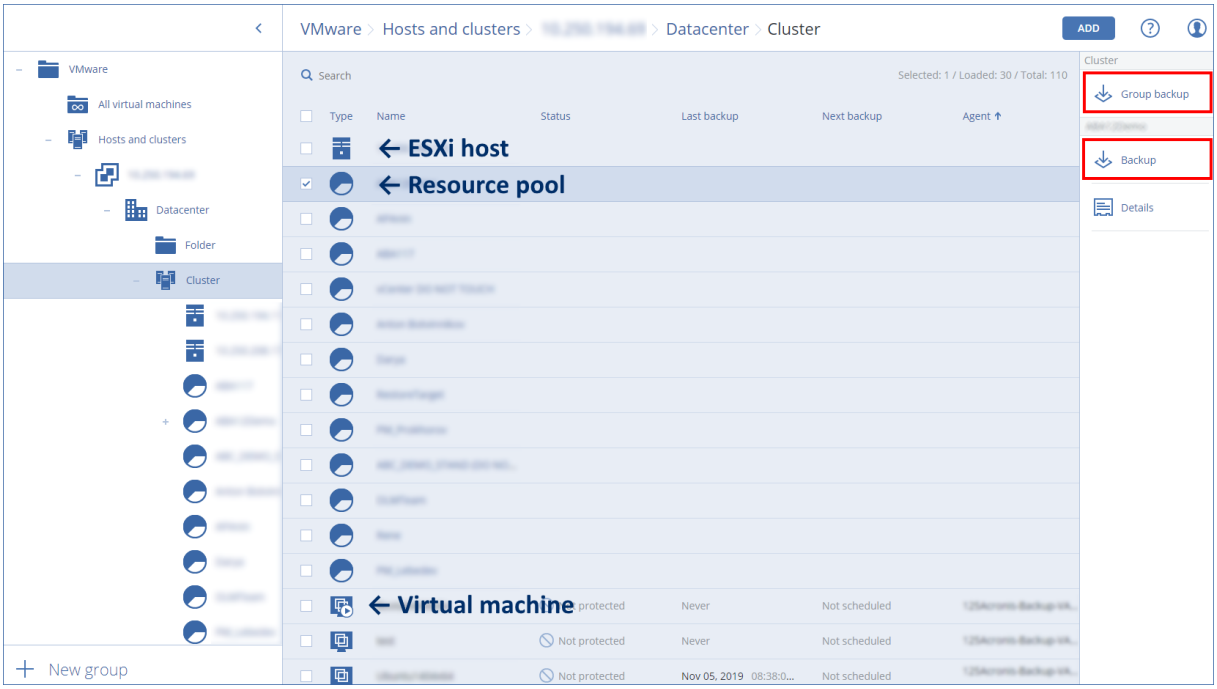
您可以使用原生的呈現方式檢視 vSphere、Hyper-V 及 Virtuozzo 環境。一旦已安裝並登錄對應的代理程式之後，**[VMware]**、**[Hyper-V]** 或 **[Virtuozzo]** 索引標籤就會出現在 **[裝置]** 底下。

在 **[VMware]** 索引標籤中，您可以備份下列 vSphere 基礎架構物件：

- 資料中心
- 資料夾
- 叢集
- ESXi 主機
- 資源集區

其中每個基礎架構物件都如同虛擬機器的群組物件般運作。當您將保護計劃套用至其中任何群組物件時，將會備份其中所有的虛擬機器。您可以按一下 **[備份]** 來備份所選群組電腦，或按一下 **[群組備份]** 來保護所選群組所屬的父群組電腦。

例如，您已經選擇叢集，然後選擇其中的資源集區。如果您按一下 **[備份]**，將會備份所選資源集區中包含的所有虛擬機器。如果您按一下 **[群組備份]**，將會備份叢集中包含的所有虛擬機器。



您可以變更 vCenter Server 或單機 ESXi 主機的存取認證，而不用重新安裝代理程式。

變更 vCenter Server 或 ESXi 主機存取認證

1. 在**[裝置]**下，按一下 **VMware**。
2. 按一下**[主機與叢集]**。
3. 在**主機與叢集**清單（位於**主機與叢集**樹狀結構的右側）中，選擇在 VMware 代理程式安裝期間指定的 vCenter Server 或單機 ESXi 主機。
4. 按一下**[詳細資料]**。

5. 在**[認證]**下，按一下使用者名稱。
6. 指定新的存取認證，然後按一下 **[確定]**。

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 - 必要權限

本節說明 ESX 虛擬機器操作，以及虛擬裝置部署所需的權限。

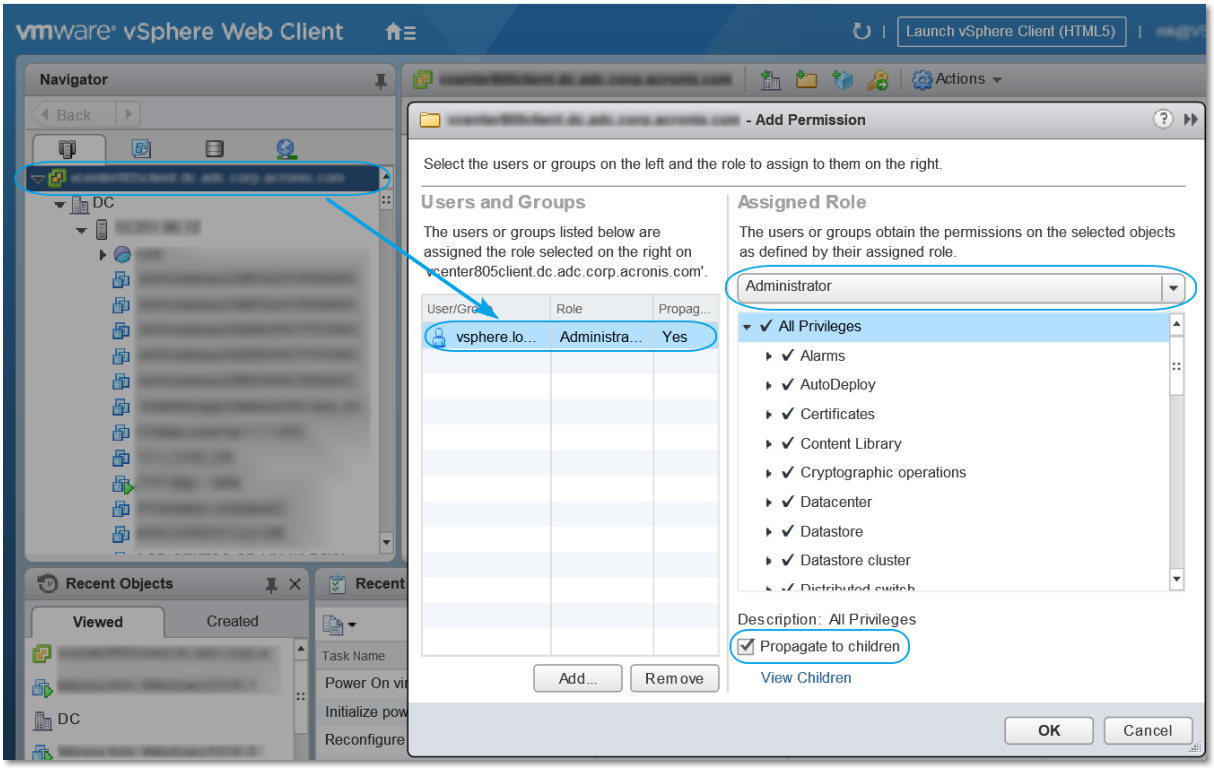
注意事項
ESXi 主機上必須安裝 vStorage API，才能啟用虛擬機器備份。請參閱 https://kb.acronis.com/content/14931。

若要使用 vCenter 物件 (例如虛擬機器、ESXi 主機、叢集、vCenter 等等) 執行任何作業，VMware 用代理程式會在 vCenter 或 ESXi 主機上，使用使用者提供的 vSphere 認證進行驗證。VMware 用代理程式用於連線至 vSphere 的 vSphere 帳戶必須擁有從 vCenter 層級開始所有 vSphere 基礎架構所有層級所需的權限。

安裝或設定 VMware 用代理程式時，請使用所需的權限指定 vSphere 帳戶。若您日後需要變更帳戶，請參閱 管理虛擬化環境〉一節。

若要將權限指派給 vCenter 層級的 vSphere 使用者，請執行下列操作：

1. 登入 vSphere Web 用戶端。
2. 在 vCenter 上按一下滑鼠右鍵，然後按一下 **[新增權限]**。
3. 選擇或加入擁有所需角色的新使用者 (新角色必須包含下表中所有所需的權限)。
4. 選擇 **[傳播至子項]** 選項。



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	VA 部署
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	授權	+	+	+	+	
	停用方式	+	+	+		
	啟用方式	+	+	+		
	管理自訂屬性	+	+	+		
	設定自訂屬性	+	+	+		

主機 > 組態	VM 自動啟動設定					+
	儲存磁碟分割組態				+	
主機 > 清查	修改叢集					+
主機 > 本機作業	建立 VM				+	+
	刪除 VM				+	+
	重新設定 VM				+	+
網路	指派網路		+	+	+	+
資源	指派 VM 至資源集區		+	+	+	+
	匯入					+
虛擬機器> 設定	新增現有磁碟	+	+		+	
	新增新磁碟		+	+	+	+
	新增或移除裝置		+		+	+
	進階	+	+	+		+
	變更 CPU 數量		+			
	磁碟變更追蹤	+		+		
	磁碟租賃	+		+		
	記憶體		+			
	移除磁碟	+	+	+	+	
	重新命名		+			
	設定註解				+	
	設定		+	+	+	
[虛擬機器] > [客體作業]	客體作業程式執行	+**				+
	客體作業查詢	+**				+
	客體作業修改	+**				
虛擬機器 > 互動	取得客體控制票證 (適用於 vSphere 4.1 及 5.0)				+	+
	設定 CD 媒體		+	+		

	主控台互動					+
	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		+	+	+	+
	移動					+
	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 或更新版本)	**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。

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. 在管理伺服器上登錄所有代理程式。

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到*新的* Hyper-V 虛擬機器時，或在保護計劃中對 Hyper-V 虛擬機器進行轉換時，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。

[排程備份] 選項會定義代理程式在執行特定保護計劃時，可同時備份的虛擬機器數量。

當多個保護計劃的時間重疊時，則會將其備份選項中指定的數目相加。即使所產生的總數在程式設計上限制為 10，計劃重疊還是可能會影響備份效能，並使主機和虛擬機器存放區超載。

您可以進一步減少 VMware 用代理程式或 Hyper-V 用代理程式可以同時備份的虛擬機器總數。

若要限制 VMware 用代理程式 (Windows) 或 Hyper-V 用代理程式可以備份的虛擬機器總數

1. 在執行代理程式的電腦上，建立新文字文件，然後在文字編輯器 (例如「記事本」) 中開啟此文件。
2. 複製以下各行並貼到檔案中：

```
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. 執行下列作業以重新啟動代理程式：
   a. 在 **[開始]** 功能表中，按一下 **[執行]**，然後輸入：**cmd**
   b. 按一下 **[確定]**。
   c. 執行以下命令：

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

若要限制 VMware 用代理程式 (虛擬裝置) 或 VMware 用代理程式 (Linux) 可以備份的虛擬機器總數

1. 在執行代理程式的電腦上，啟動命令殼層：
   - **VMware 用代理程式 (虛擬裝置):** 在虛擬裝置 UI 中時，按下 CTRL+SHIFT+F2。
   - **VMware 用代理程式 (Linux):** 以 root 使用者的身分，登入執行 Acronis Cyber Protect 裝置的電腦。密碼與 Cyber Protect Web 主控台的密碼相同。
2. 使用文字編輯器 (例如 **vi**) 開啟檔案 **/etc/Acronis/MMS.config**。
3. 找到以下區段：

   ```
   <key name="SimultaneousBackupsLimits">
       <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
   </key>
   ```

4. 將 `10` 取代為您想要設定之限制的十進位值。
5. 儲存檔案。
6. 重新啟動代理程式：
   - **VMware 用代理程式 (虛擬裝置):** 執行 `reboot` 命令。
   - **VMware 用代理程式 (Linux):** 執行下列命令：

     ```
     sudo service acronis_mms restart
     ```

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 虛擬機器***	**Virtuozzo 容器***	**Virtuozzo Hybrid Infrastructure 虛擬機器***	**Scale Computing HC3 虛擬機器**	**RHV/oVirt 虛擬機器***
實體電腦	+	+	+	-	-	+	+	+
VMware ESXi 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*	+	+	+	-	-	+	+	+

* 僅適用於雲端部署。

如需執行移轉的指示，請參閱下列章節：

- 實體到虛擬 (P2V) - "將實體機器復原為虛擬機器" (第 272 頁)
- 虛擬到虛擬 (V2V) - "復原虛擬機器" (第 274 頁)
- 虛擬到實體 (V2P) - "復原虛擬機器" (第 274 頁) 或 "使用可開機媒體復原磁碟和磁碟區" (第 276 頁)

雖然可以從 Web 介面執行 V2P 移轉，但在特定案例中我們建議您使用可開機媒體。有些時候，您可能會想使用媒體來移轉到 ESXi 或 Hyper-V。

媒體可讓您進行下列動作：

- 針對含有邏輯磁碟區 (LVM) 的 Linux 電腦，執行 P2V 和 V2P 移轉。使用 Linux 用代理程式或可開機媒體建立要復原的備份和可開機媒體。
- 提供系統開機所必要的特定硬體驅動程式。

Windows Azure 和 Amazon EC2 虛擬機器

若要備份 Windows 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，您在雲端部署中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 Windows 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 Windows Azure 或 Amazon EC2 虛擬機器，請依照以下步驟執行。

將電腦復原為 Windows Azure 或 Amazon EC2 虛擬機器

1. 從 Windows 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。

網路需求

安裝在備份電腦上的代理程式，必須能夠在網路上與管理伺服器進行通訊。

內部部署

- 若代理程式和管理伺服器均安裝在 Azure/EC2 雲端上，則所有電腦都會位在相同的網路中。您不需要進行額外的動作。
- 若管理伺服器位在 Azure/EC2 雲端外，則在雲端的電腦將無網路存取至安裝管理伺服器的本機網路。欲啟用安裝在這些電腦上的代理程式，與管理伺服器進行通訊，則必須建立虛擬私人網路 (VPN) 以連結本機 (現場) 和雲端 (Azure/EC2) 網路。如需如何建立 VPN 的說明，請參閱下列文章：

  Amazon EC2：http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#vpn-create-cgw

  Windows Azure：https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

雲端部署

在雲端部署中，管理伺服器是位在某個 Acronis 資料中心，因此代理程式可以到達。您不需要進行額外的動作。

保護 SAP HANA

SAP HANA 的保護詳述於可在 https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_SAP_HANA_whitepaper_en-US.pdf 取得的另一份文件。

反惡意程式碼和 Web 保護

Cyber Protect 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 Windows Defender 防毒軟體的管理。

防毒和反惡意程式碼保護

[防毒和反惡意程式碼保護] 模組可讓您保護 Windows 和 macOS 電腦，免受所有最近的惡意程式碼威脅的影響。請注意，macOS 電腦不支援屬於反惡意程式碼保護一部分的 Active Protection 功能。查看支援的反惡意程式碼功能完整清單：作業系統支援的功能。

在 Windows Security Center 中支援並註冊 Acronis Cyber Protect。

如果您的電腦在將 [防毒和反惡意程式碼保護] 模組套用至電腦時，已經受到第三方防毒解決方案保護，則系統將會產生一個警示，並停止即時保護，以防止潛在的相容性和效能問題。您將需要停用或解除安裝第三方防毒解決方案，才能啟用完整功能的 Acronis Cyber Protect 防毒和反惡意程式碼保護。

您可以使用下列反惡意程式碼功能：

- 在即時保護和按需模式下偵測檔案中的惡意程式碼 (適用於 Windows、macOS)
- 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)
- 將危險的檔案移到隔離區
- 將受信任的公司應用程式新增到白名單中

[防毒和反惡意程式碼保護] 模組為您提供兩種類型的掃描：

- 即時保護掃描
- 按需惡意程式碼掃描

即時保護掃描

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。

您可以選擇以下其中一個掃描類型：

- 主動即時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，主動且不斷地掃描的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/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。

按需惡意程式碼掃描

反惡意程式碼掃描是根據排程執行的。

您可以在 **[儀表板]** > **[概觀]** > [最近受影響] 桌面小工具中，監視反惡意程式碼掃描的結果。

防毒和反惡意程式碼保護設定

若要瞭解如何使用 [防毒和反惡意程式碼保護] 模組建立保護計劃，請參閱「建立保護計劃」。

您可以針對 [防毒和反惡意程式碼保護] 模組指定下列設定。

Active Protection

Active Protection 可保護系統免受勒索軟體和加密貨幣採礦惡意程式碼的攻擊。勒索軟體會將檔案加密，並要求贖金才會提供加密金鑰。加密採礦惡意程式碼會在背景執行數學計算，從而竊取處理能力和網路流量。

在 Acronis Cyber Protect Cyber Backup 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 Acronis Cyber Protect Protect 版本中，Active Protection 是 [防毒和反惡意程式碼保護] 模組的一部分。

Active Protection 適用於執行下列作業系統的電腦：

- 桌面作業系統：Windows 7 Service Pack 1 和更新版本
  在執行 Windows 7 的電腦上，確認已安裝適用於 Windows 7 的更新 (KB2533623)。
- 伺服器作業系統：Windows Server 2008 R2 和更新版本。

必須在機器上安裝 Windows 代理程式。

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，並執行設定所指定的額外操作。

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。

預設設定：**[啟用]**。

Active Protection 設定

在**與偵測相關的動作**中，選擇當偵測到勒索軟體活動時，軟體將採取的動作，然後按一下**[完成]**。

您可以選擇下列其中一項：

- **僅通知**
  軟體將產生有關於此程序的警示。
- **停止程序**
  軟體將產生警示，並停止程序。

- **使用快取回復**
  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：**使用快取回復**。

網路資料夾保護

[保護對應為本機磁碟機的網路資料夾] 選項會定義防毒和反惡意程式碼保護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。

此選項適用於透過 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。但是會儲存到此選項設定中指定的資料夾。預設資料夾為 **C:\ProgramData\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：**[啟用]**。

伺服器端保護

此選項會定義防毒和反惡意程式碼保護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：**[已停用]**。

設定受信任和已封鎖連線

在 **[受信任]** 索引標籤上，您可以指定能夠修改任何資料的連線。您必須定義使用者名稱與 IP 位址。

在 **[已封鎖]** 索引標籤上，您可以指定將無法修改任何資料的連線。您必須定義使用者名稱與 IP 位址。

自我保護

自我保護可避免對軟體自身的程序、登錄檔記錄、可執行檔與組態檔案、Secure Zone，以及位於本機資料夾的備份進行未經授權的變更。我們不建議停用此功能。

預設設定：**[啟用]**。

允許程序修改備份

[允許特定程序修改備份] 選項會在啟用 **[自我保護]** 時生效。

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。

此選項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。

如果停用此選項，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。

如果啟用此選項，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]**。

加密採礦程序偵測

此選項會定義防毒和反惡意程式碼保護是否會偵測潛在的加密採礦惡意程式碼。

加密採礦惡意程式碼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。建議您將加密採礦惡意程式碼加入至 **[有害的程序]** 清單以防止其執行。

預設設定：**[啟用]**。

加密採礦程序偵測設定

選擇當偵測到加密採礦活動時，軟體將採取的動作，然後按一下 **[完成]**。您可以選擇下列其中一項：

- **僅通知**
  此軟體會針對懷疑有加密採礦活動的程序產生警示。
- **停止程序**
  此軟體會產生警示並停止懷疑有加密採礦活動的程序。

預設設定：**停止程序**。

隔離

隔離是一個資料夾，用於將可疑 (可能受感染) 或可能危險的檔案保留在隔離的位置。

在下列時間後移除隔離的檔案 – 定義將移除隔離檔案的天數。

預設設定：**30 天**。

行為偵測

Acronis Cyber Protect 會使用行為啟發法識別惡意程序以保護您的系統：此軟體會將程序執行的動作鏈與惡意行為模式資料庫中記錄的動作鏈進行比較。因此，此軟體會透過惡意程式碼的典型行為，偵測新的惡意程式碼。

預設設定：**[啟用]**。

行為偵測設定

在 **[偵測到時採取的動作]** 中，選擇當偵測到惡意程式碼活動時，軟體將採取的動作，然後按一下 **[完成]**。

您可以選擇下列其中一項：

- **僅通知**
  此軟體將會針對懷疑有惡意程式碼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惡意程式碼活動的程序。

- **隔離**
  此軟體將會產生警示、停止程序，然後將可執行檔移到隔離資料夾。

預設設定：**隔離**。

即時保護

即時保護會在系統開機期間，不斷地檢查電腦系統中是否有病毒和其他威脅。

預設設定：**[啟用]**。

針對即時保護設定偵測到時採取的動作

在 **[偵測到時採取的動作]** 中，選擇當偵測到病毒或其他惡意威脅時，軟體將採取的動作，然後按一下 **[完成]**。

您可以選擇下列其中一項：

- **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**
  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。

預設設定：**隔離**。

設定即時保護的掃描模式

在 **[掃描模式]** 中，選擇當偵測到病毒或其他惡意威脅時，軟體將採取的動作，然後按一下 **[完成]**。

您可以選擇下列其中一項：

- **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。

預設設定：**智慧型主動即時掃描**。

排程掃描

您可以啟用 **[排程掃描]** 設定，根據將會檢查其中是否有惡意程式碼的電腦，定義排程。

偵測到時採取的動作：

- **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。

預設設定：**隔離**。

掃描類型:

- **完整**
  相較於快速掃描，完成完整掃描所需的時間更長，因為每個檔案都將經過檢查。
- **快速**
  快速掃描僅會掃描電腦上通常會駐留惡意程式碼的一般區域。
- **自訂**
  自訂掃描會檢查系統管理員為保護計劃所選擇的檔案/資料夾。

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]** 掃描。

預設設定：

- 已排程 **[快速]** 和 **[完整]** 掃描。
- **[自訂]** 掃描預設為停用狀態。

使用下列事件，排程工作執行：

- **依時間排程** – 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。

預設設定：**依時間排程**。

排程類型：

- **每月** – 選擇執行工作的月份以及該月的週數或日期。
- **每日** – 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。

預設設定：**每天**。

開始時間 – 選擇執行工作的明確時間。

在日期範圍內執行 – 設定一個範圍，已設定的排程將在該範圍內生效。

開始條件 – 定義必須同時符合，工作才能執行的所有條件。

反惡意程式碼掃描的開始條件與 [備份] 模組的開始條件類似，詳述於 "開始條件" (第 211 頁) 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 之間執行。

- **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。

僅掃描新的和變更的檔案 – 將僅掃描新建立和修改的檔案。

預設設定：**[啟用]**。

排程 **[完整掃描]** 時，您有另外兩個選項：

- **掃描存檔檔案**

  預設設定：**[啟用]**。
  - **遞迴深度上限**

    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。

    預設設定：**16**。
  - **大小上限**

    要掃描之存檔檔案的大小上限。

    預設設定：**無限制**。
- **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，快閃磁碟機和外接式硬碟)
  - **CD/DVD**

排除

為了將啟發式分析所使用的資源減至最少，並消除所謂的誤報，當受信任的程式被視為勒索軟體時，您可以定義以下的設定：

在 **[受信任]** 索引標籤上，您可以指定：

- 絕不會被視為惡意程式碼的程序。由 Microsoft 簽署的程序一律受到信任。
- 將不會監視發生檔案變更的資料夾。
- 將不會執行排程掃描的檔案和資料夾。

在 **[已封鎖]** 索引標籤上，您可以指定：

- 將一律遭封鎖的程序。只要在電腦上啟用了 Active Protection，這些程式就無法啟動。
- 將封鎖其中任何程序的資料夾。

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`。

指定資料夾時，您可以使用萬用字元 * 與 ?。星號 (*) 會代替零個或更多個字元。問號 (?)會代替一個字元。無法使用環境變數，例如 `%AppData%`。

預設設定：預設沒有定義任何排除項目。

URL 篩選

請參閱 URL 過濾功能以取得詳細說明。

Active Protection

在 Acronis Cyber Protect Cyber Backup 版本中，Active Protection 是保護計劃中的獨立模組。此模組具有以下設定：

- 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

在 Acronis Cyber Protect Protect 版本中，Active Protection 是 [防毒和反惡意程式碼保護] 模組的一部分。

Active Protection 適用於執行下列作業系統的電腦：

- 桌面作業系統：Windows 7 Service Pack 1 和更新版本
  在執行 Windows 7 的電腦上，確認已安裝適用於 Windows 7 的更新 (KB2533623)。
- 伺服器作業系統：Windows Server 2008 R2 和更新版本。

必須在機器上安裝 Windows 代理程式。

若要深入瞭解 Active Protection 及其設定，請參閱 "防毒和反惡意程式碼保護設定" (第 438 頁)。

Windows Defender 防毒軟體

Windows 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。

[Windows Defender 防毒軟體] 模組可讓您透過 Cyber Protect Web 主控台，設定 Windows 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 Windows Defender 防毒軟體的電腦。

排程掃描

指定排程掃描的排程。

掃描模式：

- **完整** – 除了在快速掃描期間掃描的項目之外，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 Windows Defender 防毒軟體排程設定的詳細資訊，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** – 清理電腦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** – 從電腦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 Windows 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電腦上安裝或執行。

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 Windows 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 Windows Defender 防毒軟體使用者介面。您可以透過 Cyber Protect Web 主控台管理 Windows Defender 防毒軟體原則。
- **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 Windows 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 Windows Defender 防毒軟體排除項目設定的詳細資訊，請參閱 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings。

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 Web 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 的電腦。

Microsoft Security Essentials 設定與 Microsoft Windows Defender 防毒軟體幾乎相同，但是沒有即時保護設定，而且無法透過 Cyber Protect Web 主控台定義排除項目。

URL 篩選

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] 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。您可以封鎖對可能含有惡意內容之網站的存取。

URL 篩選也可讓您控制網路使用量以符合外部法規或公司內部政策。您可以針對超過 40 個網站類別，設定不同的存取原則。

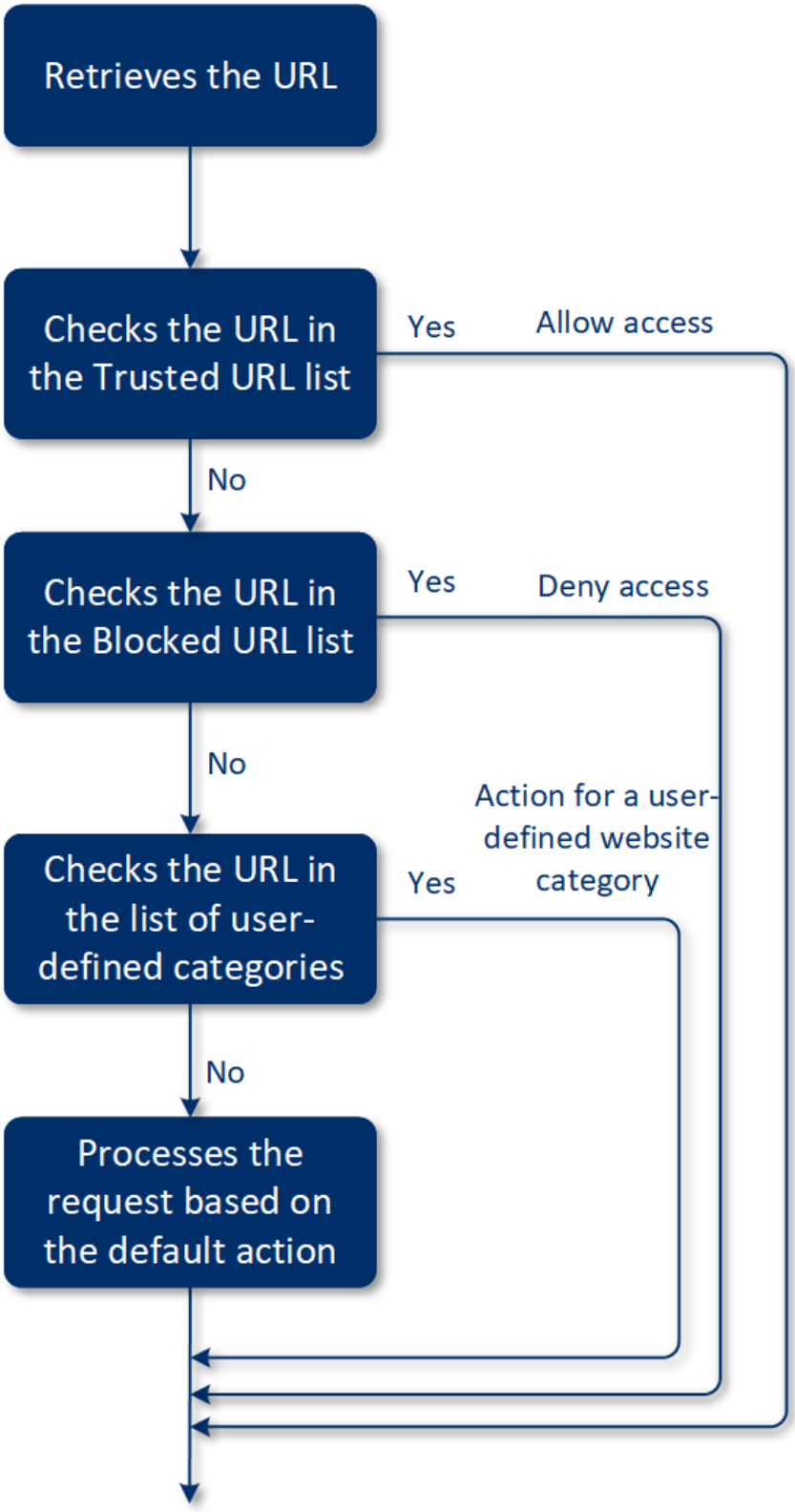
目前，保護代理程式將會檢查 Windows 電腦上的 HTTP 和 HTTPS 連線。

URL 篩選功能需要有網際網路連線才能運作。

注意事項
如果同時使用 URL 篩選和也使用 URL 篩選的第三方防毒解決方案，則可能發生衝突。您可以透過 Windows Security Center 判斷已安裝的防毒解決方案的狀態。
如果發生相容性或效能問題，請解除安裝第三方解決方案或停用保護計劃中的 URL 篩選模組

運作原理

使用者可以按一下連結，或在瀏覽器的網址列中輸入 URL。攔截器會取得 URL，並將其傳送到保護代理程式中。保護代理程式會剖析 URL、檢查資料庫，然後將結果傳回攔截器。如果 URL 遭到禁止，攔截器會封鎖對該 URL 的存取，並通知使用者，指出無法看到此內容。



若要設定 URL 篩選

1. 在啟用 [URL 篩選] 模組的情況下，建立一個保護計劃。
2. 設定 URL 篩選設定 (請參閱以下內容)。
3. 將保護計劃指派給您想要的電腦。

若要檢查已遭到封鎖的 URL，請移至 **[儀表板]** > **[警示]**。

URL 篩選設定

您可以針對 [URL 篩選] 模組設定下列設定。

惡意網站存取

指定當使用者嘗試開啟惡意網站時將執行的動作：

- **封鎖** – 系統將封鎖對惡意網站的存取，並將產生一個警示。
- **一律詢問使用者** – 要求使用者選擇繼續存取網站或返回。

要篩選的類別

您可以設定其存取原則的網站類別有 44 個。預設允許存取所有類別的網站。

	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	**政府機構**	此類別涵蓋政府網站，包括政府機構、大使館和辦公室網站。
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。建議使用此類別搭配社交網路類別。
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**	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

	間	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。

如果您啟用 **[顯示依類別封鎖之 URL 的所有通知]** 核取方塊，系統匣中將會顯示依類別封鎖之 URL 的通知。如果某個網站有數個子網域，則系統也會為其產生通知，因此這個數量可能很大。

排除

已知為安全的 URL 可以新增到受信任 URL 的清單中。代表威脅的 URL 可以新增到已封鎖 URL 的清單中。

若要將 URL 新增至清單

1. 在保護計劃的 [URL 篩選] 模組中，按一下 **[排除項目]**。
2. 選擇所需的清單：**[受信任]** 或 **[已封鎖]**。

3. 按一下 **[新增]**。
4. 指定 URL 或 IP 位址，然後按一下核取標記。

   URL 排除項目的範例：

   - 如果您將 xyz.com 新增為受信任/未受信任，根據您要新增的位置，xyz.com 網域中的所有位址都將被視為受信任或未受信任。
   - 如果您要新增特定網域，您可以將 **mail.xyz.com** 新增為受信任/未受信任，這不會讓所有的 **xyz.com** 位址都變成受信任或未受信任。
   - 如果您要將 IPv4 新增為受信任/未受信任，則必須使用下列格式才會有效：**20.53.203.50**。
   - 如果您要同時新增多個 URL 排除項目，請務必在新的一行上新增每個項目：

     acronis.com

     mail.xyz.com

     20.53.203.50

隔離

[隔離] 是電腦硬碟上的一個特殊隔離資料夾，防毒和反惡意程式碼保護所偵測到的可疑檔案會放入其中，以防進一步散播威脅。

[隔離] 可讓您檢閱所有電腦中可疑而且可能危險的檔案，並決定要將其移除或還原。如果電腦從系統中移除，就會自動移除隔離的檔案。

檔案如何進入隔離資料夾？

1. 您設定保護計劃，並為受感染的檔案定義預設動作，也就是置於 [隔離]。
2. 系統在排程或主動即時掃描期間會偵測惡意檔案，並將其置於安全的資料夾 - [隔離]。
3. 系統會更新電腦上的隔離清單。
4. 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清理檔案。

管理隔離的檔案

若要管理隔離的檔案，移至 **[反惡意程式碼保護]** > **[隔離]**。您將會看到一份清單，其中包含所有電腦中的隔離檔案。

名稱	描述
檔案	檔案名稱。
隔離日期	檔案置於 [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	據以將可以檔案置入 [隔離] 的保護計劃。

您對隔離的檔案有兩個可能的動作：

- **刪除** – 從電腦永久移除隔離的檔案。
- **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。

電腦上的隔離位置

隔離檔案的預設位置為：

若是 Windows 電腦：`%ProgramData%\%product_name%\Quarantine`

若是 Mac/Linux 電腦：`/usr/local/share/%product_name%/quarantine`

公司白名單

重要事項
企業白名單要求在管理伺服器上安裝掃描服務。

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。

Cyber Protect 可以將此流程自動化：[防毒和反惡意程式碼保護] 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掃描效能。

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。

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" (第 300 頁) 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 Web 主控台中，移至 **[反惡意程式碼保護]** > **[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 Web 主控台中，移至 **[反惡意程式碼保護]** > **[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

若要防止從備份還原受感染的檔案，您可以掃描備份中是否有惡意程式碼。只有 Windows 作業系統支援備份掃描。它僅適用於 Cyber Protect Management Server 上已安裝掃描服務的情況。

若要掃描備份中的惡意程式碼，請建立備份掃描計劃。

注意事項
基於安全性和效能，建議您使用指定的電腦進行掃描。此電腦將可存取經過掃描的所有備份。

您可以在儀表板上的「備份掃描詳細資料」桌面小工具中，檢查掃描的結果。此外，您可以在 **[備份儲存]** > **[位置]** > **<備份名稱>** 中查看備份狀態。如果未執行備份掃描，則備份會處於 **[未掃描]** 狀態。執行備份掃描之後，備份狀態會更新為：

- **無惡意程式碼**
- **偵測到惡意程式碼**

限制

- 只有 **[整部電腦]** 或 **[磁碟/磁碟區]** 類型的備份可以掃描惡意程式碼。
- 僅掃描具有 GPT 和 MBR 磁碟分割之 NTFS 檔案系統的磁碟區。
- 支援的備份位置包括：**[雲端儲存空間]**、**[本機資料夾]** 和 **[網路資料夾]**。
- 可以選擇包含連續資料保護 (CDP) 復原點的備份，但是這些復原點將排除在掃描之外。僅將掃描一般復原點。
- 選擇 CDP 備份對整部電腦進行安全復原時，將會在沒有 CDP 復原點中資料的情況下，安全地復原電腦。若要復原 CDP 資料，請執行 **[檔案/資料夾]** 復原。

協同作業和通訊應用程式的保護

Zoom、Cisco Webex Meetings 和 Microsoft Teams 現在廣泛用於視訊/網路會議和通訊。Cyber Protect 可讓您保護您的協同作業工具。

Zoom、Cisco Webex Meetings 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 Web 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. [選擇性] 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

弱點評估和修補程式管理

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。您可以使用保護計劃中的 [弱點評估] 模組掃描電腦中的弱點，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。

執行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 458 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 459 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。

執行 Windows 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 458 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，將命令傳送到保護代理程式以執行弱點評估掃描。
3. 代理程式會接收命令、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. 您可以使用這項資訊，決定必須修正哪些找到的弱點。

您可以在 **[儀表板]** > **[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 Microsoft 作業系統的協力廠商產品支援弱點評估。

支援的 Microsoft 產品

桌面作業系統

- Windows 7 (企業版、專業版、旗艦版)
- Windows 8
- Windows 8.1
- Windows 10

伺服器作業系統

- 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 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Exchange Server 2013
- Microsoft Sharepoint Server 2016
- Microsoft Sharepoint Server 2016

Windows 支援的協力廠商產品

Cyber Protect 支援各種協力廠商應用程式的弱點評估和修補，包括協同作業工具和 VPN 用戶端，這些應用程式對於遠端工作情況至關重要。

如需 Windows 支援的協力廠商產品的完整清單，請參閱 https://kb.acronis.com/content/62853。

支援的 Linux 產品

下列 Linux 發行版本和版本支援弱點評估：

- Virtuozzo 7.0.11
- Virtuozzo 7.0.10 (320)

- Virtuozzo 7.0.9 (539)
- Virtuozzo 7.0.8 (524)
- CentOS 7.x
- Acronis Cyber Infrastructure 3.x
- Acronis Storage 2.4.0
- Acronis Storage 2.2.0

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" (第 179 頁)。您可以依排程或視需要執行弱點評估掃描 (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 支援的協力廠商產品的詳細資訊，請參閱 https://kb.acronis.com/content/62853。
- 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：

使用下列事件，排程工作執行：

- **依時間排程** – 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。

預設設定：**依時間排程**。

排程類型：

- **每月** – 選擇執行工作的月份以及該月的週數或日期。
- **每日** – 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。

預設設定：**每天**。

開始時間 – 選擇執行工作的明確時間。

在日期範圍內執行 – 設定一個範圍，已設定的排程將在該範圍內生效。

開始條件 – 定義必須同時符合，工作才能執行的所有條件。

反惡意程式碼掃描的開始條件與 [備份] 模組的開始條件類似，詳述於 "開始條件" (第 211 頁) 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 之間執行。
- **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。

1. 在 Cyber Protect Web 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 460 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 **[儀表板]** > **[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 Web 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 460 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 **[儀表板]** > **[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可用修補程式的弱點，以及沒有建議之修補程式的弱點。您可以使用篩選功能，僅顯示具有可用修補程式的弱點。

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： • **嚴重**：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 Web 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. 選擇要安裝的修補程式。按 **[下一步]**。
4. 選擇您要安裝修補程式所在的電腦。

5. 選擇是否要在修補程式安裝之後重新啟動電腦：
   - **否** – 修補程式安裝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。
   - **是** – 修補程式安裝後將一律起始重新開機。但是，您可以指定延遲時間。

   在備份完成之前，請不要重新開機 – 如果備份程序正在執行，電腦重新開機將會延遲，直到備份完成為止。
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

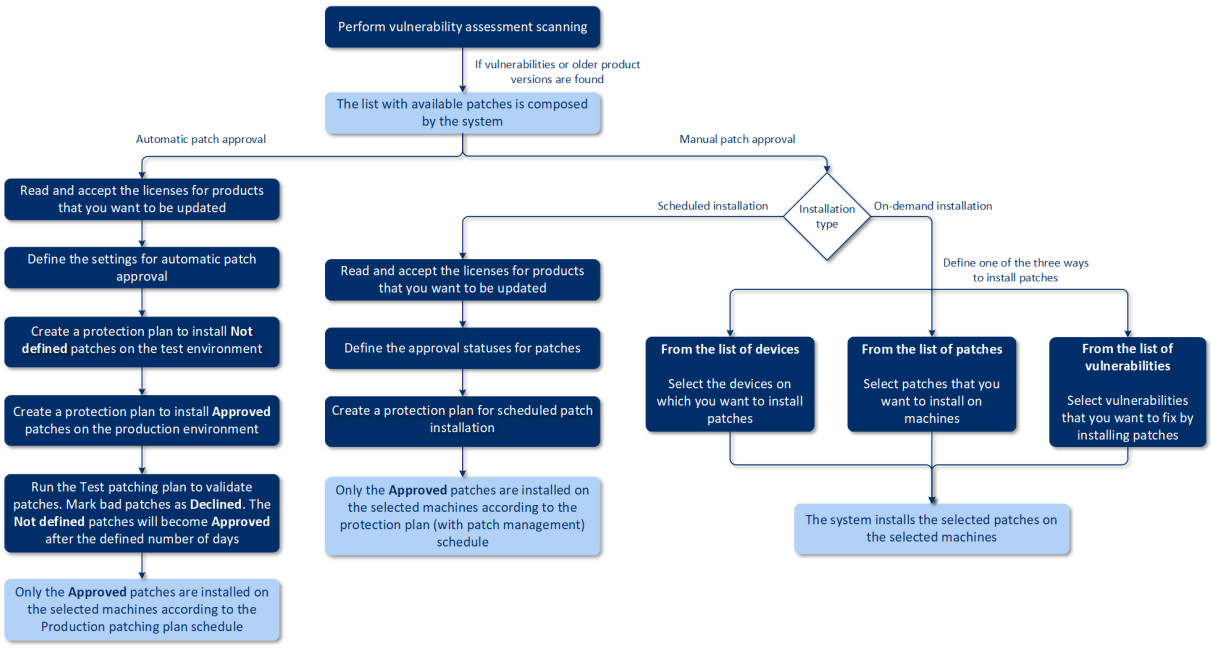
使用修補程式管理功能可：

- 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，精確地定義要套用的修補程式：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
- 定義要在安裝修補程式後套用的重新開機選項

Cyber Protect 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。

運作原理

您可以設定自動或手動核准修補程式。在以下的配置中，您可以同時看到自動和手動修補程式核准工作流程。



1. 首先，您必須在啟用 **[弱點評估]** 模組的情況下，使用保護計劃，至少執行一個弱點評估掃描。執行掃描後，[找到的弱點] 和 [可用的修補程式] 的清單是由系統組成。
2. 接著，您可以設定自動核准修補程式或使用手動核准修補程式方法。
3. 定義如何安裝修補程式 – 根據排程或視需要。根據您的喜好設定，可以透過三種方式完成按需修補程式安裝：
   - 移至修補程式清單 (**[軟體管理]** > **[修補程式]**)，然後安裝所需的修補程式。
   - 移至弱點清單 (**[軟體管理]** > **[弱點]**)，然後開始也包含修補程式安裝的修復程序。
   - 移至裝置清單 (**[裝置]** > **[所有裝置]**)、選擇您要更新的特定電腦，然後在其上安裝修補程式。

您可以在 **[儀表板]** > **[概觀]** > **[修補程式安裝歷史記錄]** 桌面小工具中，監視修補程式安裝的結果。

修補程式管理設定

若要瞭解如何使用 [修補程式管理] 模組建立保護計劃，請參閱「建立保護計劃」。您可以使用保護計劃，指定 Microsoft 產品和其他適用於 Windows OS 的第三方產品的哪些更新會自動安裝在定義的電腦上。

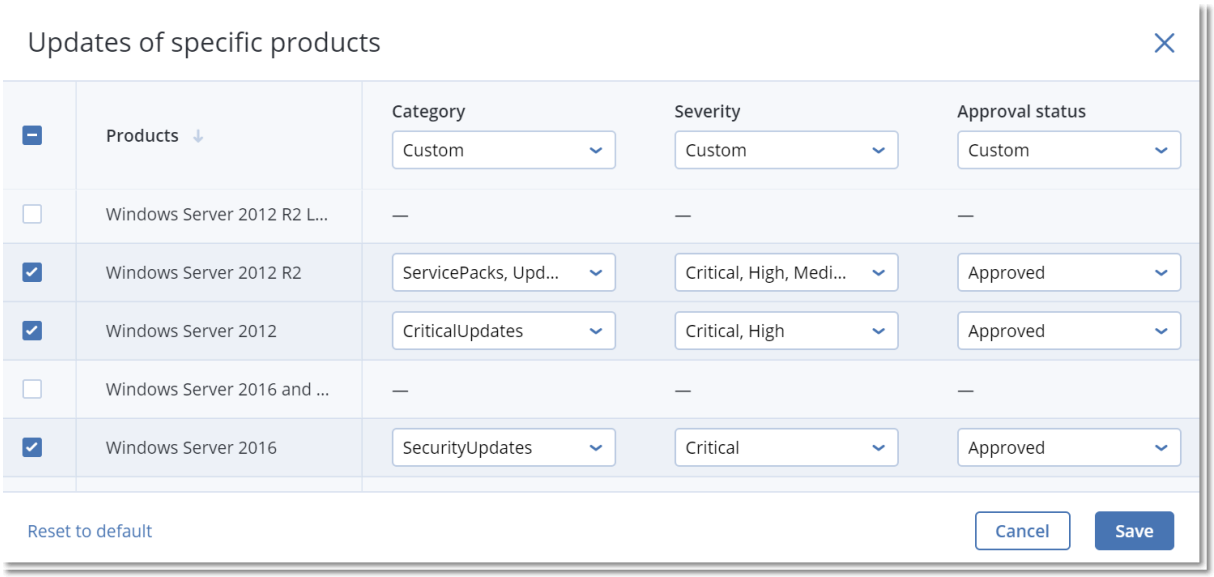
您可以針對 [修補程式管理] 模組指定下列設定。

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。

選擇要安裝的更新：

- **所有更新**
- **僅限安全性更新和重大更新**
- **特定產品更新**：您可以為不同的產品定義自訂設定。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。

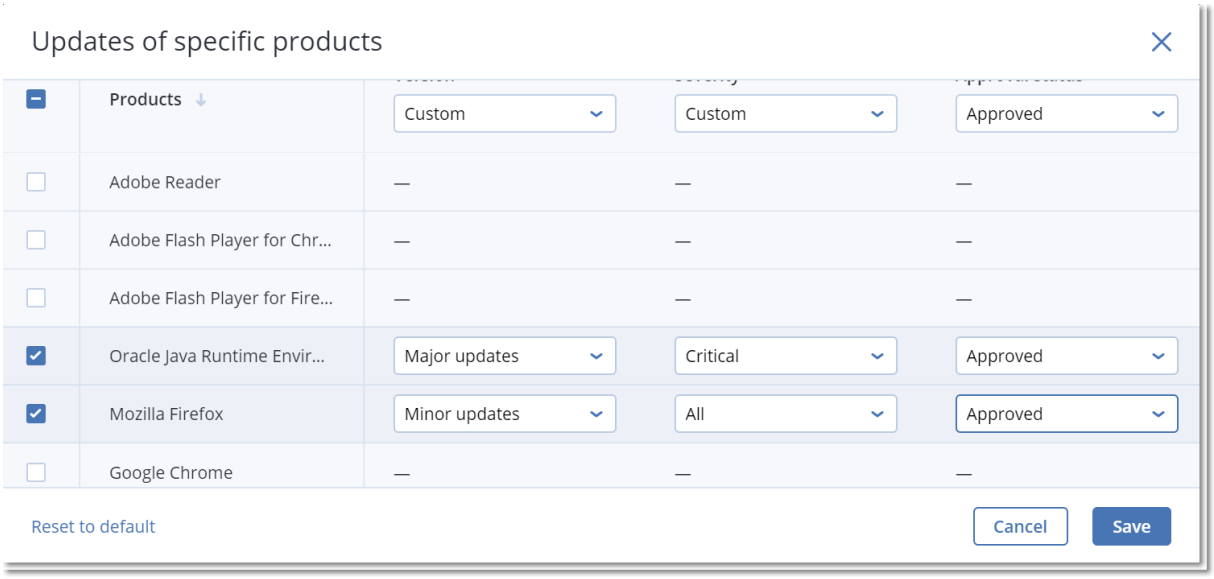


Windows 協力廠商產品

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 第三方產品]** 選項。

選擇要安裝的更新：

- **[僅限主要更新]** 可讓您安裝最新可用的更新版本。
- **[僅限次要更新]** 可讓您安裝次要的更新版本。
- **特定產品更新**：您可以為不同的產品定義自訂設定。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。



排程

根據將在所選電腦上安裝的更新，定義排程。

使用下列事件，排程工作執行：

- **依時間排程** – 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。

預設設定：**依時間排程**。

排程類型：

- **每月** – 選擇執行工作的月份以及該月的週數或日期。
- **每日** – 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。

預設設定:**每天**。

開始時間 – 選擇執行工作的明確時間。

在日期範圍內執行 – 設定一個範圍,已設定的排程將在該範圍內生效。

開始條件 – 定義必須同時符合,工作才能執行的所有條件。

反惡意程式碼掃描的開始條件與 [備份] 模組的開始條件類似,詳述於 "開始條件" (第 211 頁) 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 之間執行。
- **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。

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。萬一修補程式安裝失敗,如此將可讓您回復到先前的狀態。若要讓 **[更新前備份]** 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 **[更新前備份]** 選項。

管理修補程式清單

弱點評估完成之後,您將會在 **[軟體管理]** > **[修補程式]** 中找到可用的修補程式。

名稱	描述
名稱	修補程式的名稱
嚴重性	修補程式的嚴重性: • **嚴重** • **高** • **中** • **低** • **無**
廠商	修補程式的廠商
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。
Microsoft KB	如果是適用於 Microsoft 產品的修補程式，則會提供 KB 文章 ID
發佈日期	發佈修補程式的日期
電腦	受影響電腦的數量
核准狀態	核准狀態主要是自動核准案例所需，而且能夠在保護計劃中定義要依狀態安裝的更新。 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 • **未定義** – 修補程式狀態不清楚，應該進行驗證
授權合約	• 閱讀並接受 • 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
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

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。讓我們來看看運作方式的範例。

運作原理

您應該有兩個環境:測試和實際運作。測試環境用於測試修補程式安裝並確保它們不會破壞任何功能。在測試環境上測試修補程式安裝之後,您可以將這些安全的修補程式自動安裝在實際運作環境上。

設定自動核准修補程式

設定自動核准修補程式

1. 針對您打算更新其產品的每個廠商,您必須閱讀並接受授權合約。否則,將無法自動安裝修補程式。
2. 設定自動核准的設定。
3. 利用已啟用的 **[修補程式管理]** 模組,準備保護計劃 (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 **[未定義]**。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。
4. 利用已啟用的 **[修補程式管理]** 模組,準備保護計劃 (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]**。
5. 執行「測試修補」計劃並檢查結果。沒有問題的這些電腦的核准狀態可以保留為 **[未定義]**,而正確運作之電腦的狀態必須設定為 **[已拒絕]**。
6. 根據在 **[自動核准]** 選項中設定的天數,**[未定義]** 的這些修補程式將會變成 **[已核准]**。
7. 啟動「實際運作修補」計劃時,實際運作電腦上只會安裝 **[已核准]** 的修補程式。

手動步驟如下所列。

步驟 1。針對您要更新的產品,閱讀並接受授權合約

1. 在 Cyber Protect Web 主控台中,移至 **[軟體管理]** > **[修補程式]**。
2. 選擇修補程式,然後閱讀並接受授權合約。

步驟 2。設定自動核准的設定

1. 在 Cyber Protect Web 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]** 選項,並指定天數。也就是說,在從第一次嘗試安裝修補程式起的指定天數之後,狀態為 **[未定義]** 的修補程式將會自動變成 **[已核准]**。

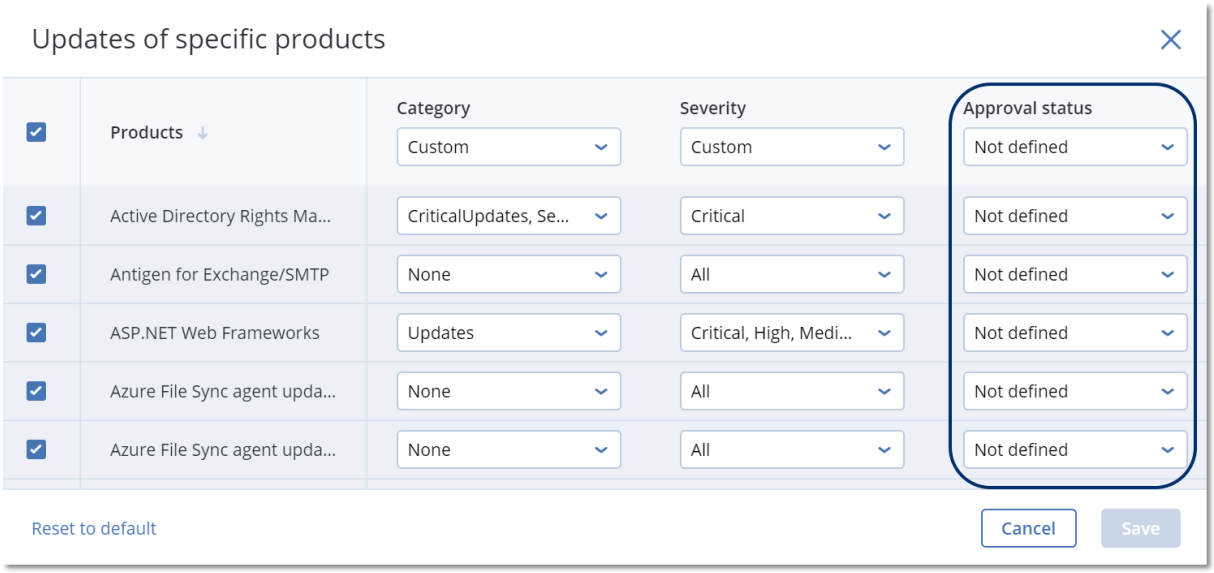
例如，您指定 10 天。您對測試電腦執行「測試修補」計劃，並安裝修補程式。您將這些破壞電腦的修補程式標示為 **[已拒絕]**，而其餘的修補程式則保留為 **[未定義]**。10 天之後，**[未定義]** 狀態中的修補程式將會自動切換為 **[已核准]**。

4. 啟用 **[自動接受授權合約]** 選項。若要在修補程式安裝期間，這是自動接受授權所需，無須使用者確認。

步驟 3。準備測試修補保護計劃

1. 在 Cyber Protect Web 主控台中，移至 **[計劃]** > **[保護]**。
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「修補程式管理設定」。

重要事項
針對要更新的所有產品，將 **[核准狀態]** 定義為 **[未定義]**。更新時，代理程式僅會將 **[未定義]** 修補程式安裝在測試環境中的所選電腦上。

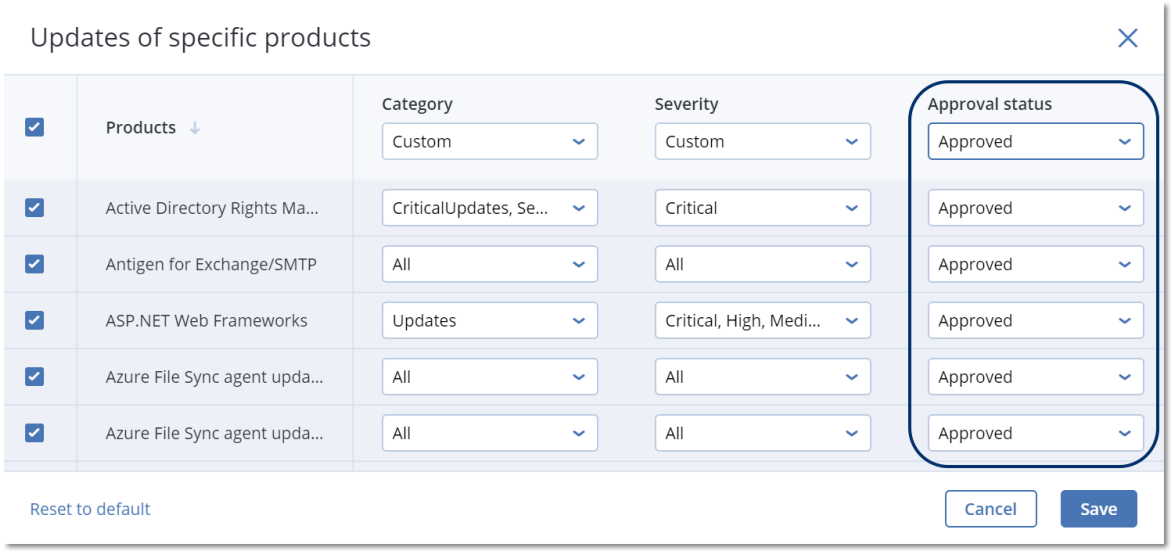


步驟 4。準備實際運作修補保護計劃

1. 在 Cyber Protect Web 主控台中，移至 **[計劃]** > **[保護]**。
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「修補程式管理設定」。

重要事項
針對要更新的所有產品，將 **[核准狀態]** 定義為 **[已核准]**。更新時，代理程式僅會將 **[已核准]** 修補程式安裝在實際運作環境中的所選電腦上。

注意事項



步驟 5。執行「測試修補」保護計劃並檢查結果

1. 執行「測試修補」保護計劃 (依排程或視需要)。
2. 之後，檢查哪些已安裝的修補程式安全，哪些不安全。
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]**。

手動核准修補程式

手動核准修補程式程序如下：

1. 在 Cyber Protect Web 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，然後閱讀並接受授權合約。
3. 針對您核准安裝的修補程式，將 **[核准狀態]** 設定為 **[已核准]**。
4. 在啟用 [修補程式管理] 模組的情況下，建立一個保護計劃。您可以設定排程，或者在 [修補程式管理] 模組設定中，按一下 **[立即執行]**，即可視需要啟動計劃。

因此，只有核准的修補程式將會安裝在所選電腦上。

按需修補程式安裝

根據您的喜好設定，可以透過三種方式完成按需修補程式安裝：

- 移至修補程式清單 (**[軟體管理]** > **[修補程式]**)，然後安裝所需的修補程式。
- 移至弱點清單 (**[軟體管理]** > **[弱點]**)，然後開始也包含修補程式安裝的修復程序。
- 移至裝置清單 (**[裝置]** > **[所有裝置]**)、選擇您要更新的特定電腦，然後在其上安裝修補程式。

讓我們考慮從修補程式清單中安裝修補程式：

1. 在 Cyber Protect Web 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. 選擇您要安裝的修補程式，然後按一下 **[安裝]**。
4. 選擇必須安裝修補程式的電腦。
5. 定義在安裝修補程式之後，是否起始重新開機：
   - **永不** – 安裝修補程式後絕不會起始重新開機。
   - **如有需要** – 只有在需要套用修補程式時，才會進行重新開機。
   - **一律** – 安裝修補程式後將一律起始重新開機。您一律可以指定重新開機延遲。

   在備份完成之前，請不要重新開機 – 如果備份程序正在執行，電腦重新開機將會延遲，直到備份完成為止。
6. 按一下 **[安裝修補程式]**。

所選修補程式將會安裝在所選電腦上。

清單中的修補程式存留時間

若要將修補程式清單保持在最新狀態，請前往 **[軟體管理]** > **[修補程式]** > **[設定]**，然後指定 **[清單存留期]** 選項。

[清單中的存留時間] 選項可定義偵測到的可用修補程式要在修補程式清單中保留的時間長度。一般而言，如果修補程式已成功安裝在偵測到缺少修補程式的所有電腦上或經過定義的時間，則將從清單中刪除該修補程式。

- **永遠** – 修補程式永遠保留在清單中。
- **7 天** – 首次安裝經過 7 天之後，將會移除該修補程式。

  例如，您有兩部必須安裝修補程式的電腦。一部電腦在線上，另一部則離線。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，將會移除該修補程式。

智慧型保護

威脅饋送

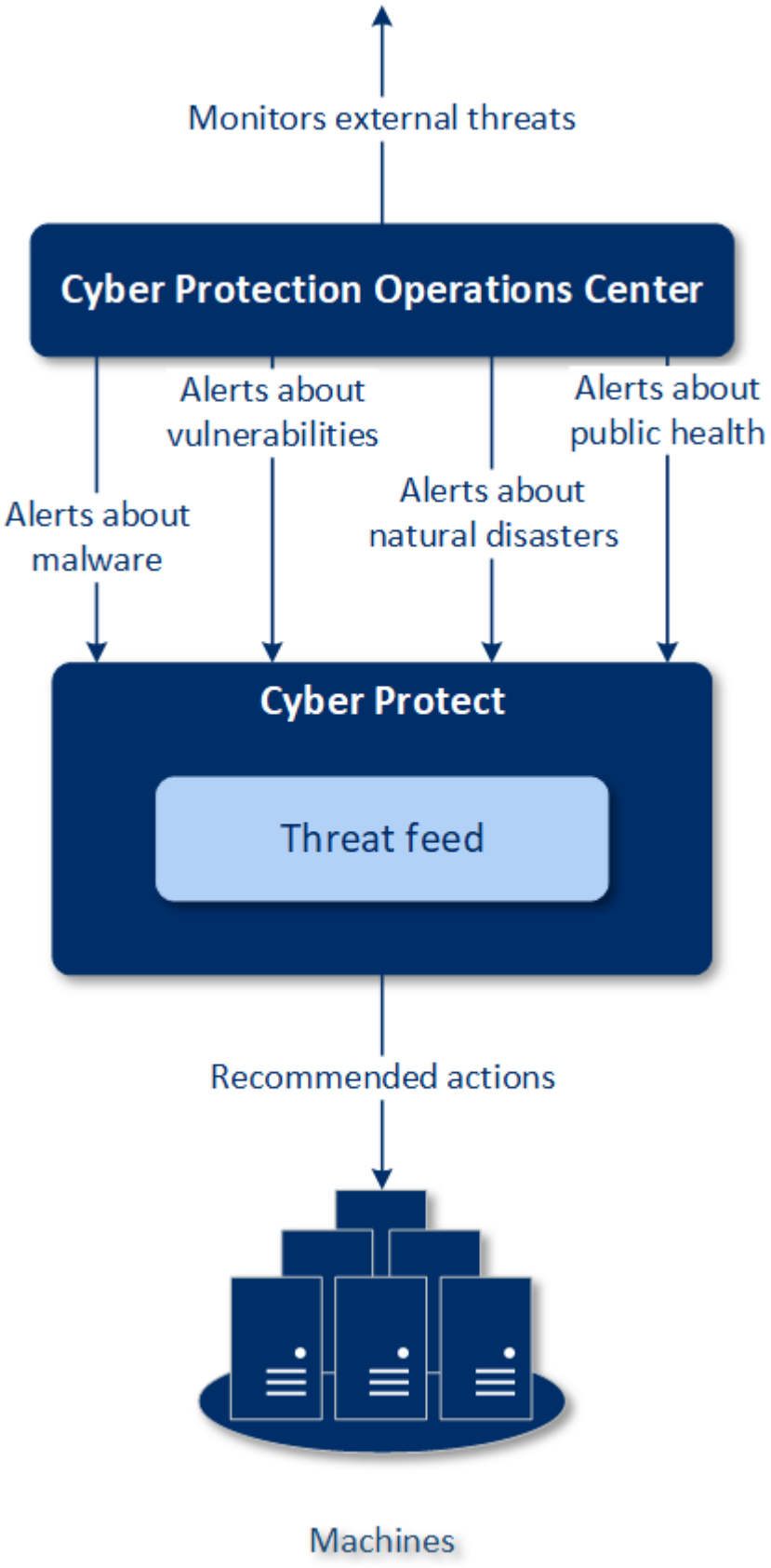
Acronis 網路保護營運中心 (CPOC) 會產生僅傳送至相關地理區域的安全性警示。這些安全性警示所提供的資訊包括惡意程式碼、弱點、自然災害、公共衛生，以及可能會影響資料保護的其他類型全球事件。威脅摘要會通知您所有潛在威脅，並可讓您預防這些威脅。

您可以利用安全專家所提供的一些特定動作，解決安全性警示。有一些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。

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 Web 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 Web 主控台中，移至 **[儀表板]** > **[威脅摘要]** 以檢查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，然後選擇必須套用這些動作的電腦。可以建議下列動作：

- **弱點評估** – 掃描所選電腦中的弱點
- **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
- **備份受保護或未受保護的電腦** – 備份受保護/未受保護的電腦

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

在下列期間之後，將會自動清除威脅摘要警示：

- 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，您要在啟用 [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 Web 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詳細資訊，請按一下此裝置的名稱。

   您將根據副檔名和位置，看到未受保護檔案的清單。您可以依副檔名篩選此清單。
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。

使用下列事件，排程工作執行：

- **依時間排程** – 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。

預設設定：**依時間排程**。

排程類型：

- **每月** – 選擇執行工作的月份以及該月的週數或日期。
- **每日** – 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。

預設設定：**每天**。

開始時間 – 選擇執行工作的明確時間。

在日期範圍內執行 – 設定一個範圍，已設定的排程將在該範圍內生效。

開始條件 – 定義必須同時符合，工作才能執行的所有條件。

反惡意程式碼掃描的開始條件與 [備份] 模組的開始條件類似，詳述於 "開始條件" (第 211 頁) 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 之間執行。
- **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。

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，將不會檢查其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。

遠端桌面存取

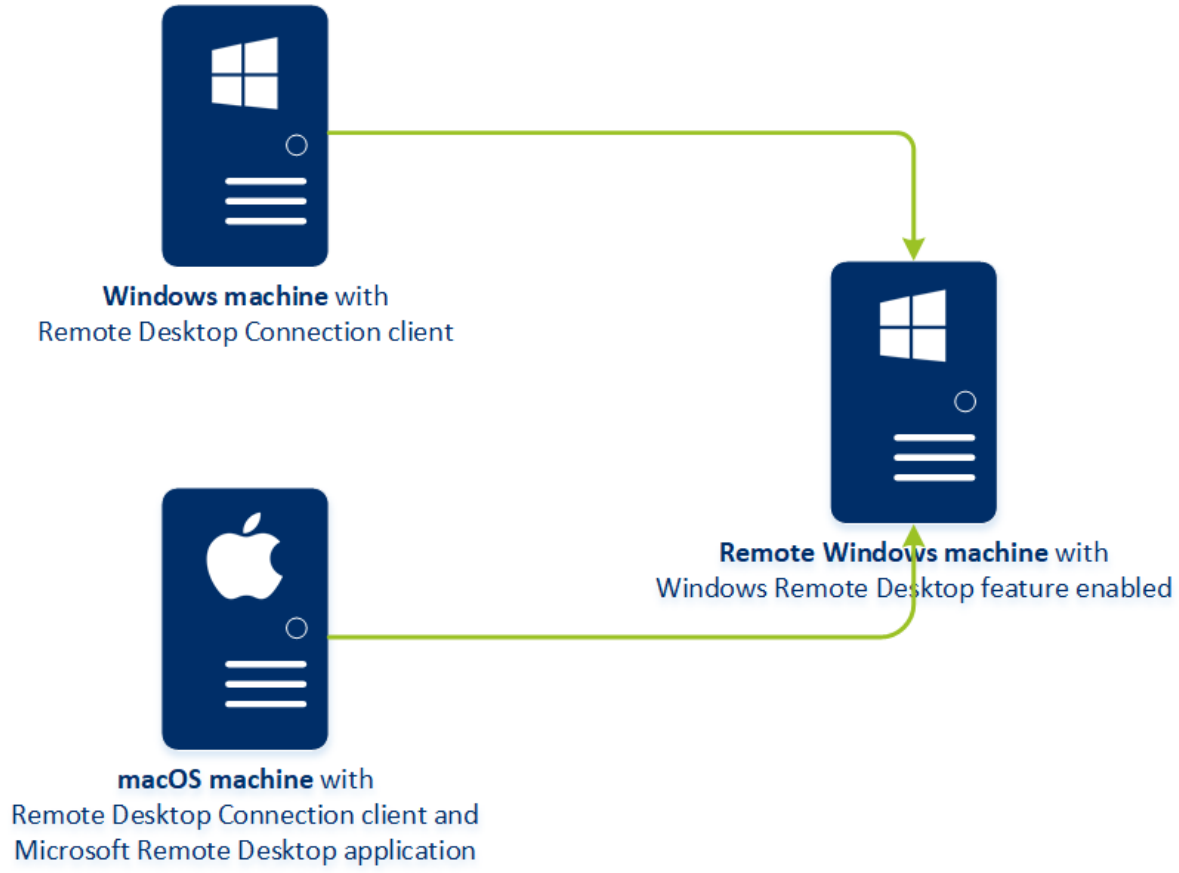
遠端存取 (RDP 和 HTML5 用戶端)

Cyber Protect 為您提供遠端存取功能。您可以直接從 Web 主控台遠端連線並管理使用者電腦。如此可讓您輕鬆地協助使用者解決其電腦上的問題。

必要條件：

- 遠端電腦上已安裝保護代理程式，且已在管理伺服器上註冊。
- 電腦已獲指派適當的 Cyber Protect 授權。
- Remote Desktop Connection Client 已安裝在初始化連線所在的電腦上。
- 初始化 RDP 連線的電腦必須能夠依其主機名稱，存取管理伺服器。DNS 設定必須正確設定，或者管理伺服器主機名稱必須置於主機檔案中。

遠端連線可以從 Windows 和 macOS 電腦上建立。



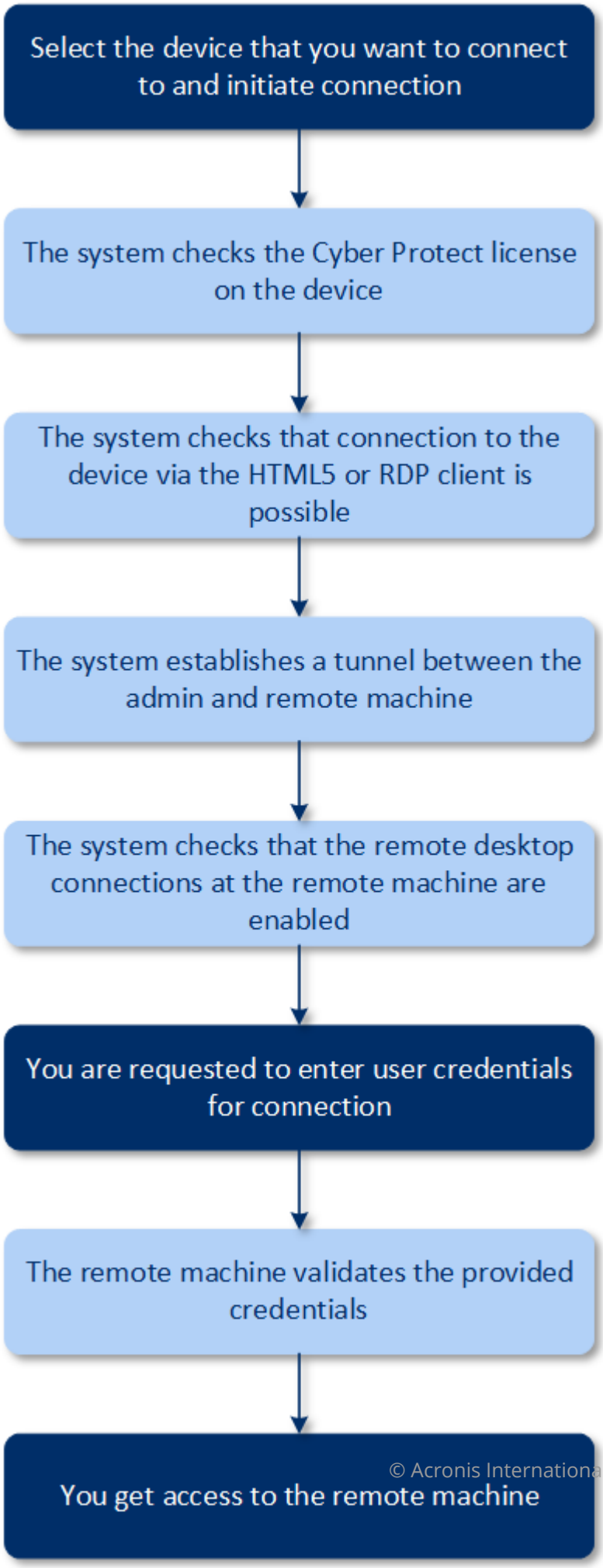
遠端存取功能可透過可用的 Windows 遠端桌面功能，用於連線至 Windows 電腦。這就是為什麼無法對 Windows 10 Home 或 macOS 系統進行遠端存取的原因。

若要建立從 macOS 電腦到遠端電腦的連線，請確認 macOS 電腦上已安裝下列應用程式：

- Remote Desktop Connection Client
- Microsoft Remote Desktop 應用程式

運作原理

當您嘗試連線至遠端電腦時，系統會先檢查此電腦是否有 Cyber Protect 授權。接著，系統會檢查是否可以透過 HTML5 或 RDP 用戶端連線。您透過 RDP 或 HTML5 用戶端起始連線。系統會建立一個與遠端電腦的通道，並檢查是否已在遠端電腦上啟用遠端桌面連線。接著，您要輸入認證，然後在驗證後，您就可以存取遠端電腦。



如何連線至遠端電腦

若要連線至遠端電腦，請執行以下操作：

1. 在 Cyber Protect Web 主控台中，移至 **[裝置]** > **[所有裝置]**。
2. 按一下您要從遠端連線到哪個電腦，然後按一下 **[網路保護桌面]** > **[透過 RDP 用戶端連線]** 或 **[透過 HTML5 用戶端連線]**。

   注意事項
   只有在 Linux 電腦上安裝管理伺服器的情況下，才能使用透過 HTML5 用戶端連線。

3. [選擇性，僅適用於透過 RDP 用戶端連線] 下載並安裝 Remote Desktop Connection Client。起始與遠端電腦的連線。
4. 指定用來存取遠端電腦的登入和密碼，然後按一下 **[連線]**。

結果，您連線至遠端電腦，而且可以管理該電腦。

共用遠端連線

在家裡工作的員工可能需要存取其辦公室電腦，但是您的組織可能還沒有設定 VPN 或其他工具，以進行遠端連線。Cyber Protect 可讓您與您的使用者共用 RDP 連結，從而讓他們從遠端存取他們的電腦。

若要啟用共用遠端連線功能

1. 在 Cyber Protect Web 主控台中，移至 **[設定]** > **[保護]** > **[遠端連線]**。
2. 選擇 **[共用遠端桌面連線]** 核取方塊。

因此，當您在 Cyber Protect Web 主控台中選擇裝置時，新選項 **[共用遠端連線]** 將會出現。

若要與您的使用者共用遠端連線

1. 在 Cyber Protect Web 主控台中，移至 **[裝置]** > **[所有裝置]**。
2. 選擇您要提供遠端連線的裝置。
3. 按一下 **[共用遠端連線]**。
4. 按一下 **[取得連結]**。在開啟的視窗中，複製所產生的連結。此連結可以與需要遠端存取裝置的使用者共用。此連結的有效期限為 10 小時。

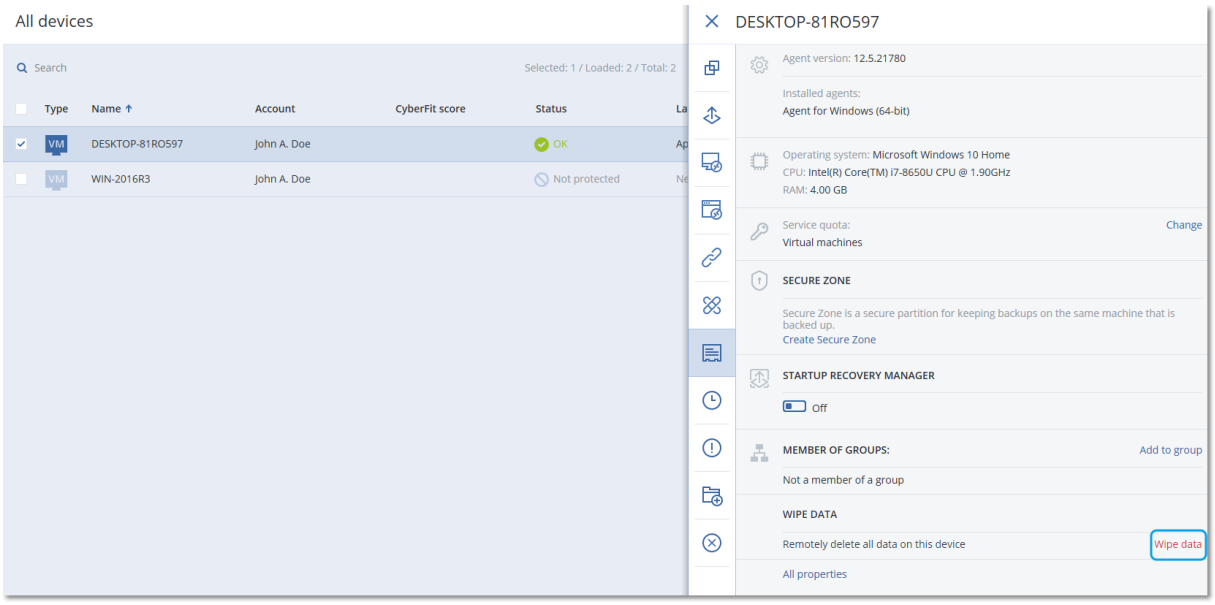
取得連結之後，您可以透過電子郵件或與其他通訊方式，共用該連結。共用連結的使用者必須按一下該連結，然後選擇連線類型：

- 透過 RDP 用戶端連線。
  此連線將會提示下載並安裝 Remote Connection Client。
- 透過 HTML5 用戶端連線。
  此連線不需要在使用者電腦上安裝任何 RDP 用戶端。使用者將會被重新導向到登入畫面，而且必須輸入用來存取電腦的認證。

遠端抹除

遠端抹除可讓 Cyber Protect 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 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 Web 主控台中，移至 **[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 **[儀表板]** > **[活動]** 中檢查抹除程序以及啟動者的詳細資料。

各 Device 群組

裝置群組的設計旨在方便您管理大量已註冊裝置。

您可以將保護計劃套用至群組。一旦群組中顯示新的裝置，裝置會變成由計劃進行保護。如果從群組移除裝置，則裝置將不再由計劃進行保護。套用至群組的計劃無法從群組成員撤銷，只能從群組本身撤銷。

只能將相同類型的裝置新增至群組。例如，在 **Hyper-V** 下，您可以建立一組 Hyper-V 虛擬機器。在 **[包含代理程式的電腦]** 下，您可以建立一個已安裝代理程式之電腦的群組。在 **[所有裝置]** 底下，您無法建立群組。

單一裝置可以是多個群組的成員。

內建群組

在註冊裝置後，該裝置會顯示在 **[裝置]** 索引標籤上的其中一個內建根目錄群組中。

根目錄群組*無法*進行編輯或刪除。您*無法*將計劃套用至根目錄群組。

部分根目錄群組包含內建子根目錄群組。這些群組*無法*進行編輯或刪除。然而，您*可以*將計劃套用至子根目錄內建群組。

自訂群組

因為電腦的角色各不相同，因此使用單一保護計劃保護內建群組中的所有裝置可能無法產生令人滿意的效果。每個部門都有專屬的備份資料；有些資料需要經常備份，其他資料則是每年備份兩次。因此，您可能需要建立適用於不同電腦群組的各種保護計劃。在這種情況下，請考慮建立自訂群組。

自訂群組可以包含一或多個巢狀群組。您可以編輯或刪除任何自訂群組。自訂群組包含以下類型：

- **靜態群組**

  靜態群組包含手動新增的電腦。除非您明確新增或刪除電腦，否則靜態群組內容永遠不會變更。

  範例：您為財務部建立了自訂群組，並將會計的電腦手動新增至此群組。將保護計劃套用至該群組之後，會計的電腦會變成受到保護。如果聘用了新的會計，您可手動向該群組新增新的電腦。
- **動態群組**

  動態群組包含根據建立群組時指定的搜尋條件自動新增的電腦。動態群組內容會自動變更。只要電腦符合指定的條件，就會一直保留在該群組中。

  範例 1：屬於財務部的電腦的主機名稱稱包含「財務」一詞。您將部分電腦名稱指定為群組成員條件並將保護計劃套用至該群組。如果聘用了新的會計，在註冊新電腦時，會立即向該群組添加新電腦，因此實現自動保護。

  範例 2：財務部形成了一個獨立的 Active Directory 組織單位 (OU)。您將財務 OU 指定為群組成員條件並將保護計劃套用至該群組。如果聘用了新的會計，在註冊新電腦並添加到 OU 時 (不論何者先執行)，會立即向該群組添加新電腦，因此實現自動保護。

建立靜態群組

1. 按一下 **[裝置]**，然後選擇包含您要為其建立動態群組之裝置的內建群組。
2. 在您想要建立群組的群組旁的齒輪圖示按一下。
3. 按一下 **[新增群組]**。
4. 指定群組名稱，然後按一下 **[確定]**。
   新群組會顯示在群組樹狀目錄中。

新增裝置到靜態群組

1. 按一下 **[裝置]**，然後選擇您想要新增到群組的一個或多個裝置。
2. 按一下**[新增到群組]**。
   軟體會顯示可新增所選取裝置的群組的樹狀結構。
3. 如果您想要建立新群組，請進行以下操作。否則，請跳過此步驟。
   a. 選擇您要在其中建立群組的群組。
   b. 按一下 **[新增群組]**。
   c. 指定群組名稱，然後按一下 **[確定]**。
4. 選擇您想要新增群組的群組，然後按一下**[完成]**。

將裝置新增至靜態群組的另一種方式是選取群組，然後按一下 **[新增裝置]**。

建立動態群組

1. 按一下 **[裝置]**，然後選擇包含您要為其建立動態群組之裝置的群組。
2. 透過使用搜尋欄位來搜尋裝置。您可以使用下述多個屬性和運算子。
3. 按一下搜尋欄位旁邊的 **[另存新檔]**。

   注意事項
   部分屬性不支援建立群組。請參閱以下「搜尋查詢」一節中的表格。

4. 指定群組名稱，然後按一下 **[確定]**。

搜尋查詢

下表摘要說明您可用於搜尋查詢的可用屬性。

屬性	含義	搜尋查詢範例	支援建立群組
name	• 實體機器的主機名稱 • 虛擬機器的名稱 • 資料庫名稱	name = 'en-00'	是

屬性	含義	搜尋查詢範例	支援建立群組
	• 信箱的電子郵件地址		
parameters.MacAddress	MAC 位址。	parameters.MacAddress LIKE '00-22-4D-50-25-E5'	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
	如果在註解欄位中有手動新增文字，則會停用與 Windows 描述自動同步。若要再次啟用，請清除您已經新增的註解。
	若要為您的裝置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：
	`net stop mms`
	`net start mms`
	若要檢視註解，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：
		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
	• 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** 如果在註解欄位中有手動新增文字，則會停用與 Windows 描述自動同步。若要再次啟用，請清除您已經新增的註解。 • 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]**。		

屬性	含義	搜尋查詢範例	支援建立群組
ip	IP 位址 (僅適用於實體機器)。	ip RANGE ('10.250.176.1','10.250.176.50')	是
cpuArch	CPU 架構。 可能的值: • 'x64' • 'x86'	cpuArch = 'x64'	是
memorySize	RAM 的大小, 以 MB 為單位。	memorySize < 1024	是
cpuName	CPU 名稱。	cpuName LIKE '%XEON%'	是
insideVm	內部具有代理程式的虛擬機器。 可能的值: • true • false	insideVm = true	是
tzOffset	電腦時區偏移 (分鐘)。	tzOffset = 120	是
parameters.Architecture	作業系統架構。 可能的值: • 'x86' • 'x64'	parameters.Architecture = 'x86'	是
osName	作業系統名稱。	osName LIKE '%Windows XP%'	是
osType	作業系統類型。 可能的值: • 'windows' • 'linux' • 'macosx'	osType IN ('linux', 'macosx')	是
osProductType	作業系統產品類型。 可能的值: • 'dc' 代表網域控制站。 • 'server' • 'workstation'	osProductType = 'server'	是

屬性	含義	搜尋查詢範例	支援建立群組
virtualType	虛擬機器類型。 可能的值： • '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	virtualType = 'vmwesx'	是
osSp	作業系統 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。	osVersionMminor = 1	是
isOnline	電腦可用性。 可能的值： • true • false	isOnline = true	否
tenant	裝置隸屬於之單位的名稱。	tenant = 'Unit 1'	是
tenantId	裝置隸屬於之單位的識別碼。 若要取得單位 ID，請在 **[裝置]** 下，選擇裝置，按一下 **[詳細資料]** > **[所有內容]**。ID 會顯示在 ownerId 欄位中。	tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'	是
state	裝置狀態。 可能的值：	state = 'backup'	否

屬性	含義	搜尋查詢範例	支援建立群組
	• 'idle' • 'interactionRequired' • 'canceling' • 'backup' • 'recover' • 'install' • 'reboot' • 'failback' • 'testReplica' • 'run_from_image' • 'finalize' • 'failover' • 'replicate' • 'createAsz' • 'deleteAsz' • 'resizeAsz'		
status	資源狀態。 可能的值： • 'notProtected' • 'ok' • 'warning' • 'error' • 'critical'	status = 'ok'	否
protectedByPlan	由保護計劃保護的裝置具有給定 ID。 若要取得計劃 ID，請按一下 **[計劃]** > **[備份]**，選取該計劃，按一下 **[狀態]** 欄中的圖表，然後按一下某個狀態。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

屬性	含義	搜尋查詢範例	支援建立群組
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
ou	屬於指定 Active Directory 組織單位的電腦。	ou IN ('RnD', 'Computers')	是
id	裝置 ID。 若要取得裝置 ID，請在 **[裝置]** 下，選擇裝置，按一下 **[詳細資料]** > **[所有內容]**。ID 會顯示在 [ID] 欄位中。	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	是
lastBackupTime	上次成功備份的日期和時間。 格式為 'YYYY-MM-DD HH:MM'。	lastBackupTime > '2022-03-11' lastBackupTime <= '2022-03-11 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 >= '2022-03-11'	否
nextBackupTime	下次備份的時間。 格式為 'YYYY-MM-DD HH:MM'。	nextBackupTime >= '2022-08-11'	否
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。 若要取得保護代理程式 ID，請在 **[裝置]** 下，選擇電腦、按一下 **[詳細資料]** > **[所有內容]**。使用 agent 屬性的 "id" 值。	hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	是

屬性	含義	搜尋查詢範例	支援建立群組
resourceType	資源類型。 可能的值： • 'machine' • 'virtual_machine.vmwesx' • 'virtual_machine.mshyperv' • 'virtual_machine.rhev' • 'virtual_machine.kvm' • 'virtual_machine.xen'	resourceType = 'machine' resourceType in ('mssql_aag_database', 'mssql_database')	是
hasAsz	在具有 Acronis Secure Zone 的實體機器上的保護代理程式。 可能的值： • true • false	hasAsz=true	是
chassis	電腦機箱類型。 可能的值： • unknown • laptop • desktop • server • other	chassis='laptop'	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 = 2020-02-20 表示搜尋結果將包含自 lastBackupTime >= 2020-02-20 00:00 到 lastBackup time <= 2020-02-20 23:59:59 這段間隔的所有備份

運算子

下表摘述可用的運算子。

運算子	含義	範例
AND	邏輯接合運算子。	name like 'en-00' AND tenant = 'Unit 1'

運算子	含義	範例
OR	邏輯分離運算子。	state = 'backup' OR state = 'interactionRequired'
IN (<value1>,... <valueN>)	此運算子用來測試表示式是否符合值清單中的任何值。	osType IN ('windows', 'linux')
NOT	邏輯否定運算子。	NOT(osProductType = 'workstation')
NOT IN (<value1>,... <valueN>)	此運算子與 IN 運算子相反。	NOT osType IN ('windows', 'linux')
LIKE '萬用字元模式'	此運算子用來測試表示式是否符合萬用字元模式。 系統可能會使用下列萬用字元運算子： • * 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_'
RANGE(<starting_value>, <ending_value>)	此運算子用來測試表示式是否在值範圍內 (含兩個值)。	ip RANGE ('10.250.176.1','10.250.176.50')
= or ==	等於運算子。	osProductType = 'server'
!= 或 <>	不等於運算子。	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'
<	小於運算子。	memorySize < 1024
>	大於運算子。	diskSize > 300GB
<=	小於或等於運算子。	lastBackupTime <= '2022-05-11 00:15'
>=	大於或等於運算子。	nextBackupTime >= '2022-09-11'

將保護計劃套用到群組

1. 按一下 **[裝置]**，然後選擇包含您要套用保護計劃之群組的內建群組。
   軟體會顯示一個子群組清單。
2. 選擇您要套用保護計劃的群組。
3. 按一下 **[群組備份]**。
   軟體會顯示可以套用至群組之保護計劃的清單。
4. 執行下列其中一項操作：
   - 展開現有的保護計劃，然後按一下 **[套用]**。
   - 按一下 **[新建]**，然後建立一個新的保護計劃，如「備份」中所述。

監控與報告

[概觀] 儀表板可讓您監視受保護基礎架構的目前狀態。

[報告] 區段可讓您產生關於受保護基礎架構的按需報告和排程報告。只有使用 Advanced 授權才可以使用此區段。

概觀儀表板

[概觀] 儀表板提供許多可自訂的桌面小工具，供概覽您受保護的基礎結構。您可以從超過 20 個動態小工具中進行選擇，顯示為圓餅圖、表格、圖形、長條圖和清單。它們帶有可按一下的元素，可讓您調查問題並進行疑難排解。系統會每五分鐘更新一次桌面小工具中的資訊。

您也可以利用 Advanced 授權，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。若要透過電子郵件傳送儀表板，請確保已進行 **[電子郵件伺服器]** 設定。

可用的桌面小工具端視您的 Cyber Protect 版本而定。預設的桌面小工具如下所列：

桌面小工具	可用性	描述
網路保護	不適用於 Cyber Backup 版本	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。
保護狀態	適用於所有版本	顯示所有電腦目前的保護狀態。
活動	適用於所有版本	顯示指定期間內執行之活動的摘要。
作用中警示摘要	適用於所有版本	依警示類型和嚴重性，顯示作用中警示的摘要。
修補程式安裝狀態	不適用於 Cyber Backup 版本	顯示依修補程式安裝狀態分組的電腦數目。
遺漏的更新 (依類別)	不適用於 Cyber Backup 版本	依類別顯示遺漏的更新數目。
磁碟健全狀況狀態	不適用於 Cyber Backup 版本	依磁碟的狀態顯示其數目。
裝置	適用於所有版本	顯示有關您環境中裝置的詳細資訊。
作用中警示詳細資訊	適用於所有版本	顯示有關作用中警示的詳細資訊。
現有的弱點	適用於所有版本	顯示環境中作業系統和應用程式現有的弱點，以及受影響的電腦。
修補程式安裝歷史記錄	不適用於 Cyber Backup 版本	顯示有關已安裝之修補程式的詳細資訊。
最近受影響	適用於所有版本	顯示有關最近受感染電腦的詳細資訊。
位置摘要	適用於所有版本	顯示有關備份位置的詳細資訊。

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鉛筆圖示。編輯動態小工具之後, 按一下 **[完成]**。

重新排列儀表板上的動態小工具

按一下桌面小工具的名稱可拖放它們。

´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。

移除動態小工具

按一下動態小工具名稱旁的 X 符號。

Cyber Protection

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

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。

探索到的電腦

此桌面小工具會顯示在指定的時間範圍內發現之電腦的清單。

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。
- 在 NVMe 磁碟機上，只有透過 Windows API 傳達 SMART 資料的磁碟機支援磁碟健全狀況監控。需要直接從磁碟機讀取 SMART 資料的 NVMe 磁碟機不支援磁碟健全狀況監控。

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。
- **嚴重**
  磁碟健全狀況介於 0% 到 30% 之間。
- **正在計算磁碟資料**
  正在計算目前的磁碟狀態和預測

運作原理

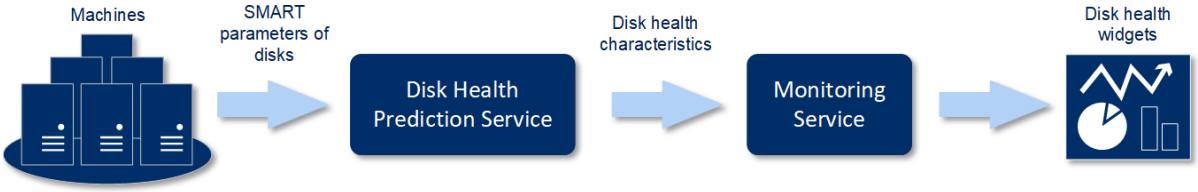
磁碟健全狀況預測服務使用以 AI 為基礎的預測模型。

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)。

   預測期間一律是一個月。
3. 監控服務會收到這些特徵，然後在 Cyber Protect Web 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 Web 主控台中提供的下列桌面小工具內。

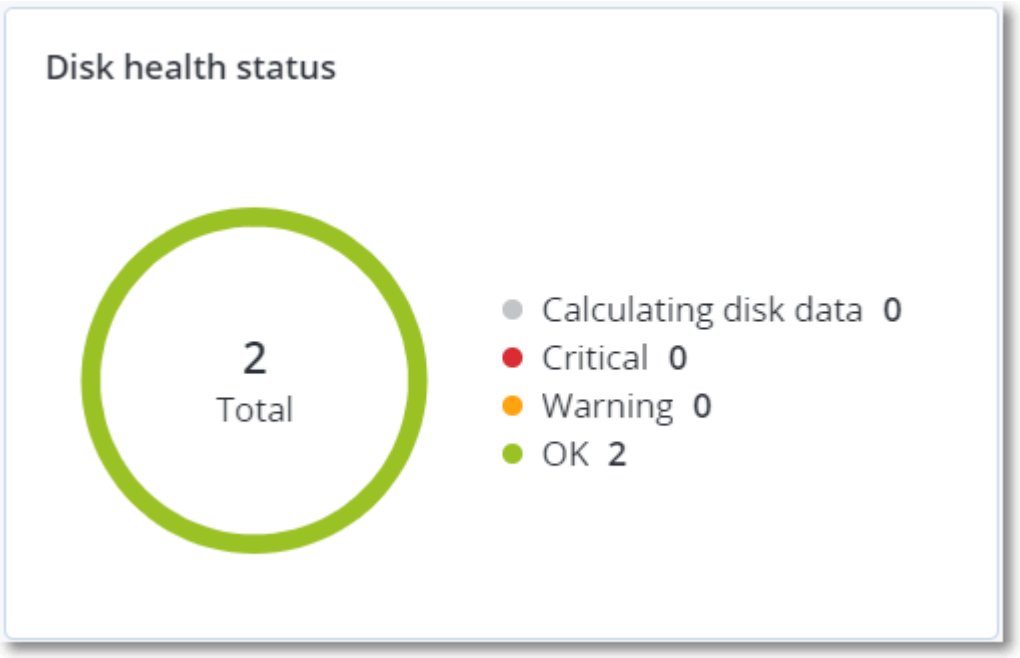
- **磁碟健全狀況概觀**是一個樹狀圖桌面小工具，其中包含可以透過查找切換的兩個詳細資料層級。
  - 電腦層級

    針對所選組織單位中所有電腦的磁碟狀態，顯示摘要資訊。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。當磁碟健全狀況狀態從 **[警告]** 變更為 **[嚴重]** 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

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組織單位/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：

- **嚴重** – 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) 的儀表板上找到。

將滑鼠暫留在有顏色的區塊上可以查看未受保護檔案數目及其位置的詳細資訊。若要保護這些檔案，按一下 **[保護所有檔案]**。

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
- 嚴重：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

此桌面小工具會依修補程式安裝狀態顯示修補程式摘要。

修補程式安裝歷史記錄

此桌面小工具會顯示有關電腦上已安裝之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

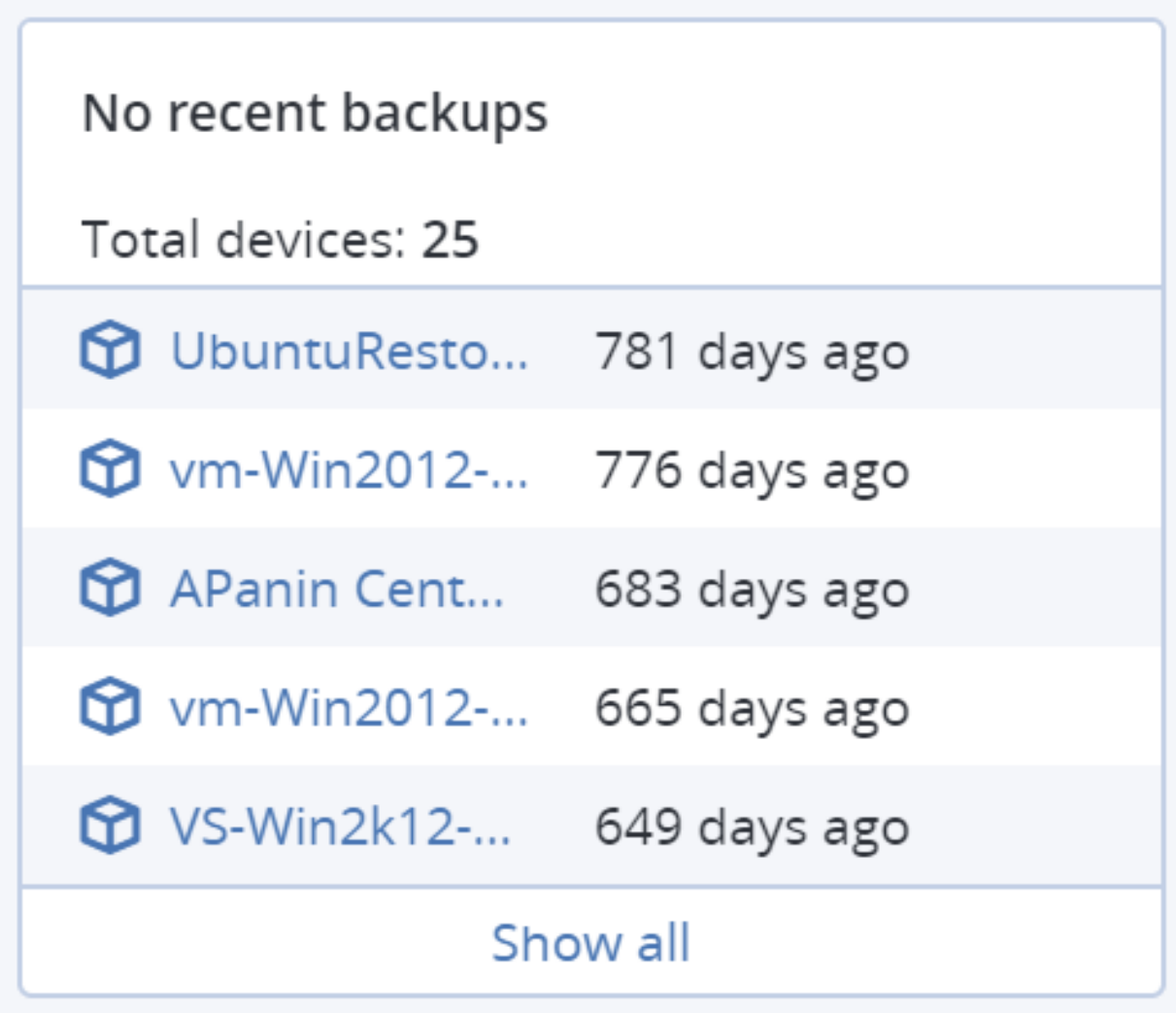
此桌面小工具僅適用於管理伺服器上已安裝掃描服務的情況。此桌面小工具會顯示有關備份中偵測到之威脅的詳細資訊。

最近受影響

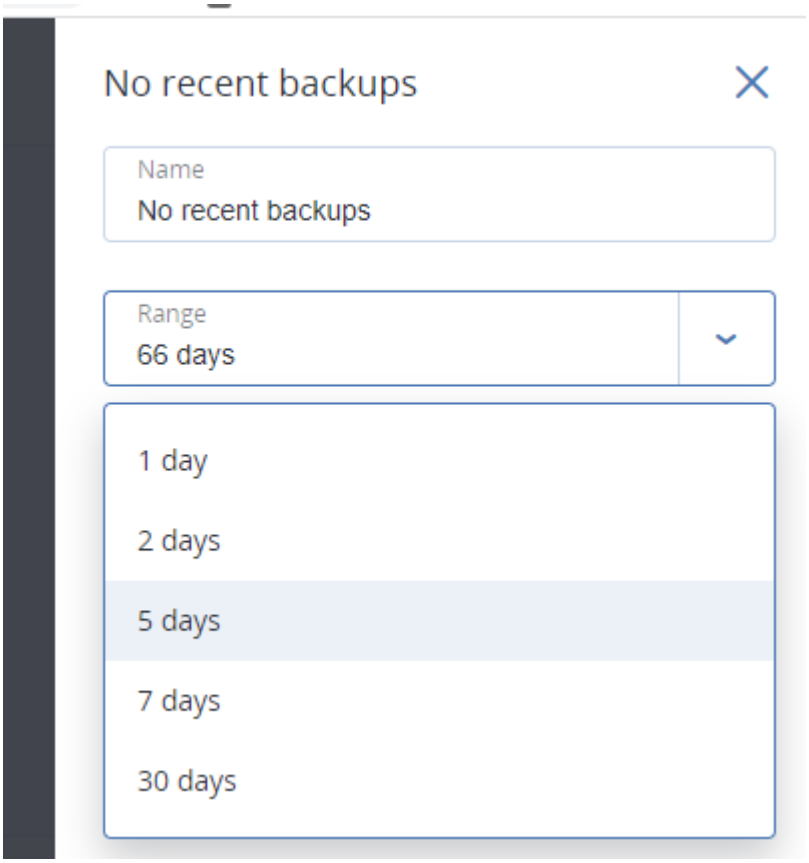
此桌面小工具會顯示有關最近受感染電腦的詳細資訊。您可以在這裡找到偵測到的威脅以及受感染檔案數目的相關資訊。

無最近備份

此桌面小工具會顯示已套用保護計劃的工作負載，其上次成功備份日期早於桌面小工具設定中指定的時間範圍。



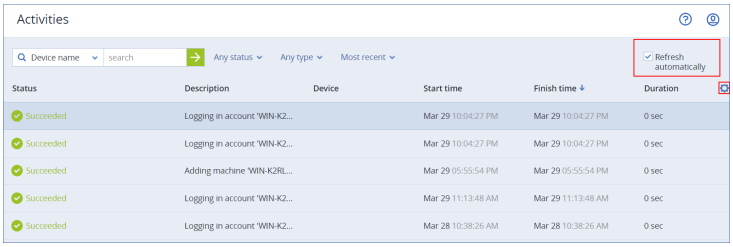
根據預設，當您新增此桌面小工具時，其會顯示過去 5 天的資訊。您可以使用下拉式功能表選擇另一個期間，或手動輸入天數。您可以輸入的天數上限為 180。



活動索引標籤

[活動] 索引標籤提供過去 90 天內活動的概觀。

若要自訂 **[活動]** 索引標籤中的檢視，請按一下齒輪圖示並選取您要檢視的欄。若要即時查看活動進度，請選擇 **[自動重新整理]** 核取方塊。請注意，經常更新多個活動可能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**
  這是執行該活動的電腦。
- **啟動者**
  這是啟動該活動的帳戶。

您也可以依下列屬性篩選活動：

- **狀態**
  例如，成功、失敗、進行中或已取消。
- **類型**
  例如，套用計劃、刪除備份、安裝軟體更新等。
- **時間**
  例如，最近的活動、最近 24 小時的活動，或是預設保留期內特定一段時間中的活動。

若要變更預設保留期，請編輯 task_manager.yaml 組態檔。

若要變更保留期

1. 在執行管理伺服器的電腦上，使用文字編輯器開啟下列設定檔案：
   - 在 Windows 中：`%Program Files%\Acronis\TaskManager\task_manager.yaml`
   - 在 Linux 中：`/usr/lib/Acronis/TaskManager/task_manager.yaml`
2. 找到以下區段：

```
database:
  connection-string:""
  run-cleanup-at:"23:59"
  cleanup-batch-size:10
  max-cleanup-retries:10
  log-queries:false
  max-transaction-retries: 10
  shards:
   - connection-string: sqlite://task-manager.sqlite
     days-to-keep: 90
     space: "default"
     key: "00000000-0000-0000-0000-000000000000"
```

3. 視需要編輯 days-to-keep 行。
   例如：

```
days-to-keep:30
```

   注意事項
   您可以根據需求變更保留期。增加保留期會降低管理伺服器的效能。

4. 如所述，重新啟動 **Acronis Service Manager 服務**。

報告

您可以使用預先定義的報告或建立自訂報告。報告可能包含任何一組儀表板桌面小工具。

您僅能為您所管理的單位設定報告。

可透過電子郵件傳送報告或按排程下載報告。要透過電子郵件傳送報告，請確保已進行**電子郵件伺服器**設定。如果您要透過使用第三方軟體處理報告，請排程將報告以 .xlsx 格式儲存到特定資料夾中。

可用的報告端視您的 Cyber Protect 版本而定。預設報告如下所列：

報告名稱	可用性	描述
警示	Cyber Backup Advanced Cyber Protect Advanced	顯示指定的期間內發生的警示。
備份掃描詳細資料	Cyber Protect Advanced	顯示備份中偵測到的威脅的詳細資訊。
備份	Cyber Backup Advanced Cyber Protect Advanced	顯示目前備份和復原點的詳細資料。
目前狀態	Cyber Backup Advanced Cyber Protect Advanced	顯示您環境的目前狀態。
每日活動	Cyber Backup Advanced Cyber Protect Advanced	顯示指定的期間內執行之活動的摘要。
資料保護圖	Cyber Protect Advanced	顯示電腦上所有重要檔案之數目、大小、位置與保護狀態的詳細資訊。
偵測到的威脅	Cyber Backup Advanced Cyber Protect Advanced	按照遭封鎖的威脅數目，顯示受影響電腦的詳細資料，以及狀況良好與易受攻擊電腦的相關資訊。
探索到的電腦	Cyber Backup Advanced Cyber Protect Advanced	顯示組織網路中找到的所有電腦。
磁碟健全狀況預測	Cyber Protect Advanced	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	Cyber Backup Advanced Cyber Protect Advanced	顯示環境中作業系統和應用程式現有的弱點，以及受影響的電腦。

授權	Cyber Backup Advanced Cyber Protect Advanced	顯示可用授權的摘要。
位置	Cyber Backup Advanced Cyber Protect Advanced	顯示指定的期間備份位置的使用狀況統計資料。
修補程式管理摘要	Cyber Protect Advanced	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	Cyber Backup Advanced Cyber Protect Advanced	顯示指定的期間受保護裝置的摘要。
磁帶活動	Cyber Backup Advanced Cyber Protect Advanced	顯示過去 24 小時內使用之磁帶的清單。
每週各項活動	Cyber Backup Advanced Cyber Protect Advanced	顯示指定期間內執行之活動的摘要。

基本報告作業

- 若要檢視報告，請按一下其名稱。
- 如需有關報告的其他操作，請按一下省略符號圖示 (...)。
  從報告內也可以使用相同操作。

若要新增報告

1. 按一下 **[新增報告]**。
2. 執行下列其中一項操作：
   - 若要新增預先定義的報告，請按一下其名稱。
   - 若要新增自訂報告，按一下 **[自訂]**。名稱為 **Custom** 的新報告隨即新增到報告清單中。開啟此報告並在其中新增桌面小工具。
3. [選擇性步驟] 拖曳動態小工具將它們重新排列。
4. [選擇性步驟] 如下所述，編輯報告。

若要編輯報告

1. 按一下報告名稱旁的省略符號圖示 (...), 然後按一下 **[設定]**。
2. 編輯報告。您可以:
   - 重新命名報告
   - 變更報告內所含所有動態小工具的時間範圍
   - 排程以 .pdf 和/或 .xlsx 格式透過電子郵件傳送報告。
3. 按一下 **[儲存]**。

若要排程報告

1. 選取報告, 然後按一下**排程**。
2. 啟用**傳送排定報告**開關。
3. 選取是否透過電子郵件傳送報告, 或將其儲存至資料夾, 或兩者。根據您的選擇, 指定電子郵件地址、資料夾路徑或兩者。
4. 選取報告格式:.pdf、.xlsx 或兩者。
5. 選取報告期間:1 天、7 天或 30 天。
6. 選取傳送或儲存報告的日期和時間。
7. 按一下 **[儲存]**。

匯出和匯入報告結構

您可將報告結構(widget 和排程設定集) 匯出並匯入 .json 檔案中。在管理伺服器重新安裝或將報告結構複製到其他管理伺服器的情況下, 這可能較為有用。

要匯出報告結構, 請選取報告, 然後按一下**匯出**。

要匯入報告結構, 請按一下**建立報告**, 然後按一下**匯入**。

傾印報告資料

您可將傾印報告資料儲存至 .csv 檔案。傾印包括所有自訂時間範圍的報告資料(不篩選) 。

軟體即時產生資料傾印。如果指定了很長時間, 則該動作可能需要很長時間。

要傾印報告資料

1. 請選取報告, 然後按一下**開啟**。
2. 按一下右上角的省略符號圖示 (...), 然後按一下 **[傾印資料]**。
3. 在**位置**中, 指定 .csv 檔案的資料夾路徑。
4. 在**時間範圍**中, 指定時間範圍。
5. 按一下 **[儲存]**。

設定警示的安全性

警示是對實際或潛在問題發出警告的訊息。您可以透過各種方式使用警示:

- **[概觀]** 標籤的 **[警示]** 區段可讓您透過監視現行警示, 快速識別及解決問題。
- 在 **[裝置]** 下, 裝置狀態衍生自警示。**[狀態]** 欄可讓您過濾具有問題的裝置。

- 設定 [電子郵件通知] 時，您可以選擇哪些警示將觸發通知。

警示可以擁有以下嚴重性之一：

- **嚴重**
- **錯誤**
- **警告**

您可以如下所述使用警示設定檔案，變更警示的嚴重性或完全停用警示。此作業需要重新啟動管理伺服器。

變更警示的嚴重性不會影響已產生的警示。

警示設定檔案

設定檔案位於執行管理伺服器的電腦上。

- 在 Windows 中：`<installation_path>`**\AlertManager\alert_manager.yaml**
  其中，`<installation_path>` 是管理伺服器的安裝路徑。預設為：**%ProgramFiles%\Acronis** 。
- 在 Linux 中：**/usr/lib/Acronis/AlertManager/alert_manager.yaml**

該檔案結構化為 YAML 文件。每個警示都是 `alertTypes` 清單中的一個元素。

`name` 機碼可識別警示。

`severity` 機碼可定義警示嚴重性。它必須具有以下其中一個值：`critical`、`error` 或 `warning`。

選用的 `enabled` 機碼可定義啟用還是停用警示。其值必須是 `true` 或 `false`。預設 (不含此機碼) 啟用所有警示。

若要變更警示的嚴重性或停用警示

1. 在安裝管理伺服器的電腦上，使用文字編輯器開啟 **alert_manager.yaml** 檔案。
2. 找出您要變更或停用的警示。
3. 執行下列其中一項操作：
   - 若要變更警示嚴重性，請變更 `severity` 機碼的值。
   - 若要停用警示，請加入 `enabled` 機碼，然後將其值設定為 `false`。
4. 儲存檔案。
5. 如下所述重新啟動管理伺服器服務。

若要在 Windows 中重新啟動管理伺服器服務

1. 在 **[開始]** 功能表中，按一下 **[執行]**，然後輸入：**cmd**
2. 按一下 **[確定]**。
3. 執行以下命令：

```
net stop acrmngsrv
net start acrmngsrv
```

若要在 Linux 中重新啟動管理伺服器服務

1. 開啟**終端機**。
2. 在任何目錄中執行以下命令：

```
sudo service acronis_ams restart
```

進階儲存選項

磁帶裝置

以下章節詳細說明如何將磁帶裝置用於儲存備份。

什麼是磁帶裝置?

磁帶裝置這個通用術語是指磁帶庫或獨立磁帶機。

磁帶庫 (自動磁帶庫) 是由以下部分組成的高容量存放裝置:

- 一或多部磁帶機
- 用來載入磁帶的多個 (最多可達數千個) 插槽
- 用於在插槽與磁帶機之間移動磁帶的一或多部換帶機 (自動機制)。

磁帶庫也可能包含其他元件, 例如條碼閱讀器或條碼印表機。

自動上帶機是一種特殊的磁帶庫。包含一部磁帶機、數個插槽、一部換帶機及一個條碼閱讀器 (可選)。

獨立磁帶機 (亦稱為**串流磁帶機**) 包含一個插槽, 一次只能載入一個磁帶。

磁帶支援概觀

保護代理程式可以將資料直接備份至磁帶裝置, 亦可透過儲存節點, 將資料備份至磁帶裝置。不論是哪種情況, 磁帶裝置皆為全自動作業。當您將具備多部磁帶機的磁帶裝置附加至儲存節點時, 可以同時備份多個代理程式至磁帶。

與 RSM 和第三方軟體的相容性

與第三方軟體的共存性

若電腦已安裝含專屬磁帶管理工具的第三方軟體, 則無法在該電腦上使用磁帶。若要在此類電腦上使用磁帶, 您必須解除安裝或停用第三方磁帶管理軟體。

與 Windows 卸除式存放裝置管理員 (RSM) 互動

保護代理程式及儲存節點不使用 RSM。偵測磁帶裝置時, 會從 RSM 停用裝置 (除非其他軟體正在使用該裝置)。只要您希望使用磁帶裝置, 就必須確定沒有使用者或第三方軟體在 RSM 中啟用該裝置。如果磁帶裝置已在 RSM 中啟用, 請重複磁帶裝置偵測。

支援的硬體

Acronis Cyber Protect 支援外部 SCSI 裝置。外部 SCSI 裝置意指連至光纖通道或使用 SCSI、iSCSI、Serial Attached SCSI (SAS) 介面的裝置。此外, Acronis Cyber Protect 支援 USB 連接的磁帶裝置。

在 Windows 中，即使未安裝磁帶裝置之換帶裝置的驅動程式，Acronis Cyber Protect 也能備份至磁帶裝置。這類磁帶裝置在 **[裝置管理員]** 中會顯示為 **[不明的媒體換帶裝置]**。但是，您必須安裝該裝置磁碟機的驅動程式。在 Linux 中及可開機媒體下，若沒有驅動程式，即無法備份至磁帶裝置。

不保證能辨識 IDE 或 SATA 等介面的裝置。這取決於作業系統是否安裝正確的驅動程式。

若要瞭解是否支援您的特定裝置，請使用硬體相容性工具，如 http://kb.acronis.com/content/57237 中所述。歡迎您將有關測試結果的報告傳送至 Acronis。確認支援的硬體會列在硬體相容性清單中：https://go.acronis.com/acronis-cyber-protect-advanced-tape-hcl。

磁帶管理資料庫

會將所有附加到電腦的磁帶裝置的相關資訊儲存在磁帶管理資料庫中。預設的資料庫路徑如下：

- 在 Windows XP/Server 2003 中：`%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\ARSM\Database`。
- 在 Windows 7 及更新版本的 Windows 中：`%PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database`。
- 在 Linux 中：`/var/lib/Acronis/BackupAndRecovery/ARSM/Database`。

資料庫大小取決於儲存於磁帶中的備份數量，每一百個備份約等於 10 MB。如果磁帶庫包含數千個備份，資料庫可能會很大。在此情況下，您可能要將磁碟資料庫儲存於不同磁碟區上。

在 Windows 中調整資料庫位置：

1. 停止 Removable Storage Management 服務。
2. 將所有檔案從預設位置移至新的位置。
3. 找到登錄機碼 `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings`。
4. 在登錄值 `ArsmDmlDbProtocol` 中指定新的位置路徑。字串最多可能包含 32765 個字元。
5. 啟動 Removable Storage Management 服務。

在 Linux 中調整資料庫位置：

1. 停止 `acronis_rsm` 服務。
2. 將所有檔案從預設位置移至新的位置。
3. 使用文字編輯器開啟設定檔案 `/etc/Acronis/ARSM.config`。
4. 找出此行：`<value name="ArsmDmlDbProtocol" type="TString">`。
5. 變更此行下方的路徑。
6. 儲存檔案。
7. 啟動 `acronis_rsm` 服務。

TapeLocation 資料夾

`TapeLocation` 資料夾包含來自磁帶上備份之所有磁碟區的檔案系統中繼資料快取。

`TapeLocation` 的預設資料夾路徑為：

- 在 Windows XP/Server 2003 中：`%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation`

- 在 Windows 7 和更新版本中：`%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation`
- 在 Linux 中：`/var/lib/Acronis/BackupAndRecovery/TapeLocation`

`TapeLocation` 資料夾大小大約是磁帶上儲存的所有備份大小的 0,5-1%。對於已啟用檔案復原選項的磁碟層級備份，`TapeLocation` 資料夾大小可能會稍微大一點，端視備份檔案數量而定。

寫入至磁帶所使用的參數

磁帶寫入參數 (區塊大小和快取大小) 可讓您微調軟體以達到最大效能。寫入磁碟同時需要這兩個參數，但通常您只需要調整區塊大小。最佳值取決於磁帶裝置類型以及要備份的資料，例如檔案數量及其大小。

注意事項
當軟體從磁帶讀取時，它會使用寫入至磁帶時所使用的相同區塊大小。如果磁帶裝置不支援這個區塊大小，讀取將會失敗。

這些參數是在連接磁帶裝置的每台電腦上設定的。它可以是安裝代理程式或儲存節點所在的電腦。在執行 Windows 的電腦上，設定是在登錄中執行；在 Linux 電腦上，則是在設定檔案 **/etc/Acronis/BackupAndRecovery.config** 中進行。

在 Windows 中，建立個別的登錄機碼及其 DWORD 值。在 Linux 中，在設定檔案的結尾、`</registry>` 標籤的正前方加上以下文字：

```
<key name="TapeLocation">
     <value name="WriteCacheSize" type="Dword">
          "value"
     </value>
     <value name=DefaultBlockSize" type="Dword">
          "value"
     </value>
</key>
```

DefaultBlockSize

這是寫入至磁帶時所使用的區塊大小 (位元組)。

*可能的值：*0、32、64、128、256、512、1024、2048、4096、8192、16384、32768、65536、131072、262144、524288、1048576。

如果值為 0，或者如果沒有參數，則會以下列方式決定區塊大小：

- 在 Windows 中，此值擷取自磁帶裝置驅動程式。
- 在 Linux 中，此值為 **64 KB**。

*登錄機碼 (在執行 Windows 的電腦上)：***HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\DefaultBlockSize**

/etc/Acronis/BackupAndRecovery.config 中的一行 (在執行 Linux 的電腦上)：

```
<value name=DefaultBlockSize" type="Dword">
     "value"
</value>
```

如果磁帶機不接受指定的值，軟體會將該值除以二，直到達到適用的值為止，或直到該值達到 32 位元組為止。如果找不到適用的值，軟體會將指定的值乘以二，直到達到適用的值為止，或直到該值達到 1 MB 為止。如果磁帶機不接受任何值，備份將會失敗。

WriteCacheSize

這是寫入至磁帶時所使用的緩衝區大小 (位元組)。

*可能的值:*0、32、64、128、256、512、1024、2048、4096、8192、16384、32768、65536、131072、262144、524288、1048576，但是不小於 **DefaultBlockSize** 參數值。

如果值為 0，或者如果沒有參數，則緩衝區大小為 **1 MB**。如果作業系統不支援這個值，軟體會將該值除以二，直到找到適用的值為止，或直到達到 **DefaultBlockSize** 參數值為止。如果找不到作業系統支援的值，備份將會失敗。

登錄機碼 (在執行 Windows 的電腦上):
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\WriteCacheSize

/etc/Acronis/BackupAndRecovery.config 中的一行 (在執行 Linux 的電腦上):

```
<value name="WriteCacheSize" type="Dword">
     "value"
</value>
```

如果您指定一個作業系統不支援的非零的值，備份將會失敗。

磁帶相關備份選項

您可以設定 **[磁帶管理]** 備份選項來判斷:

- 是否要啟用從儲存在磁帶上的磁碟層級備份復原檔案。
- 保護計劃完成後是否將磁帶返回插槽。
- 備份完成後是否退出磁帶。
- 是否每次完整備份均使用一個可用磁帶。
- 建立完整備份時是否覆寫磁帶 (僅適用於獨立磁帶機)。
- 是否使用磁帶組區分所使用的磁帶，例如，用於在一週不同日期所建立的備份，或不同電腦型別的備份。

並行作業

Acronis Cyber Protect 可同時對磁帶裝置中不同的元件執行作業。在使用磁帶機的作業期間 (備份、復原、重新掃描或清除)，您可以啟動使用換帶裝置的作業 (移動磁帶至其他插槽或退出磁帶)，反之

亦然。如果磁帶庫有一部以上的磁碟機，您也可以在使用其中一部磁帶機作業的時候，啟動使用另一部磁帶機的作業。例如，多台電腦可以使用同一磁帶庫的不同磁帶機同時進行備份或復原。

偵測新磁帶裝置的作業可以與任何作業同時執行。清查時，除了偵測新磁帶裝置之外，無法執行其他作業。

無法並行執行的作業會排入佇列。

限制

以下是磁帶裝置使用上的限制：

1. 電腦從基於 Linux 的 32 位可啟動媒體啟動時，不支援磁帶裝置。
2. 無法將以下資料類型備份到磁帶：Microsoft 365 信箱、Microsoft Exchange 信箱。
3. 無法建立實體電腦和虛擬機器的應用程式感知備份。
4. 在 Mac OS 中，僅支援至受管理磁帶位置的檔案層級備份。
5. 磁帶上的備份無法合併。因此，備份到磁帶時，**一律增量備份**備份配置不可用。
6. 磁帶上的備份無法執行重複資料刪除。
7. 如果磁帶中有非刪除備份，或在其他磁帶有依存備份，軟體就無法自動覆寫這個磁帶。
   此規則唯一的例外是當啟用「建立完整備份時覆寫獨立磁帶機中的磁帶」選項時。
8. 如果復原程序需要作業系統重新開機，您就無法在作業系統中從儲存於磁帶的備份復原。您必須使用可開機媒體執行這類復原。
9. 您可以驗證儲存在磁帶上的任何備份，但您無法選取整個磁帶位置或磁帶裝置進行驗證。
10. 受管理的磁帶位置無法以加密保護。而是加密您的備份。
11. 軟體無法將一個備份同時寫入多個磁帶，或是同時將多個備份透過同一部磁帶機寫入同一個磁帶。
12. 不支援使用網路資料管理通訊協定 (NDMP) 的裝置。
13. 不支援條碼印表機。
14. 不支援線性磁帶檔案系統 (LTFS) 格式化磁帶。

由舊版 Acronis 產品所寫入之磁帶的可讀性

下表摘要說明由 Acronis True Image Echo、Acronis True Image 9.1、Acronis Backup & Recovery 10、Acronis Backup & Recovery 11、Acronis Backup 11.5、11.7 和 12.5 產品系列所寫入之磁帶在 Acronis Cyber Protect 中的可讀性。該表格同時也說明由 Acronis Cyber Protect 各元件所寫入之磁帶的相容性。

您可以對 Acronis Backup 11.5、11.7 和 12.5 建立的重新掃描備份附加增量備份和差異備份。

	在裝有下列元件之電腦本機連接的磁帶裝置上，可讀取的磁帶為			
	Acronis Cyber Protect 可開機媒體	Acronis Cyber Protect Windows 用	Acronis Cyber Protect Linux 用	Acronis Cyber Protect 儲存節點

				代理程式	代理程式	
藉由右列元件在本機連接的磁帶裝置(磁帶機或磁帶庫)上寫入的磁帶	可開機媒體	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	-
	Windows 用代理程式	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	-
	Linux 用代理程式	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	-
透過右列元件在磁帶裝置上寫入的磁帶	備份伺服器	9.1	-	-	-	-
		Echo	-	-	-	-
	儲存節點	ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	+

磁帶裝置入門

備份電腦至直接附加的磁帶裝置

必要條件

- 磁帶裝置已根據製造廠商的說明附加至電腦。
- 電腦上已安裝保護代理程式。

備份前

1. 將磁帶載入磁帶裝置。
2. 登入 Cyber Protect Web 主控台。
3. 在**[設定]** > **[磁帶管理]**中，展開機器節點，然後按一下**[磁帶裝置]**。
4. 請確保有顯示所連接的磁帶裝置。如果沒有，請按一下**[偵測裝置]**。
5. 執行磁帶清查：
   a. 按一下磁帶裝置名稱。
   b. 按一下 **[清查]** 偵測載入的磁帶。保持**[完整清查]**為開啟。請勿開啟**移動未識別或匯入的磁帶到「可用磁帶」集區**。按一下**[立即開始清查]**。
   結果。所載入的磁帶已經移動到適當的集區，如在「清查中」區段所指定的。

   注意事項
   對整個磁帶裝置執行完整清查可能需要很長的時間。

   c. 如果所載入的磁帶傳送到**未識別的磁帶**或**匯入的磁帶**集區，且您想要使用它們進行備份，請以手動方式移動此類磁帶到**可用的磁帶**集區。

   注意事項
   傳送到 **[已匯入的磁帶]** 集區的磁帶內含 Acronis 軟體所寫入的備份。移動此類磁帶到**[可用的磁帶]**集區之前，請確保您已經不需要這些備份。

備份

依「備份」一節中所述的方式，建立保護計劃。指定備份位置時，請選擇**磁帶集區 'Acronis'**。

結果

- 若要存取將建立備份的位置，請按一下 **[備份儲存]** > **[磁帶集區 'Acronis']**。
- 包含備份的磁帶將移動到**Acronis**集區。

備份到附加至儲存節點的磁帶裝置

必要條件

- 儲存節點將登錄到管理伺服器上。
- 磁帶裝置已根據製造廠商的說明附加至儲存節點。

備份前

1. 將磁帶載入磁帶裝置。
2. 登入 Cyber Protect Web 主控台。
3. 按一下**[設定]** > **[磁帶管理]**，使用儲存節點名稱展開節點，然後按一下**[磁帶裝置]**。
4. 請確保有顯示所連接的磁帶裝置。如果沒有，請按一下**[偵測裝置]**。
5. 執行磁帶清查：
   a. 按一下磁帶裝置名稱。
   b. 按一下 **[清查]** 偵測載入的磁帶。保持**[完整清查]**為開啟。請勿開啟**移動未識別或匯入的磁帶到「可用磁帶」集區**。按一下**[立即開始清查]**。
   結果。所載入的磁帶已經移動到適當的集區，如在「清查中」區段所指定的。

   注意事項
   對整個磁帶裝置執行完整清查可能需要很長的時間。

   c. 如果所載入的磁帶傳送到**未識別的磁帶**或**匯入的磁帶**集區，且您想要使用它們進行備份，請以手動方式移動此類磁帶到**可用的磁帶**集區。

   注意事項
   傳送到 **[已匯入的磁帶]** 集區的磁帶內含 Acronis 軟體所寫入的備份。移動此類磁帶到**[可用的磁帶]**集區之前，請確保您已經不需要這些備份。

   d. 決定您是否要備份到 **Acronis** 集區或建立新的集區。
   詳細資料。擁有多個集區可讓您為每個機器，或您公司的每個部門使用個別的磁帶組。您可以使用多個集區，避免透過不同保護計劃所建立的備份在同一個磁帶上相互混淆。
   e. 如果所選取的集區可以在需要時從**可用的磁帶**集區中使用磁帶，請跳過此步驟。
   否則，請從**可用的磁帶**集區移動磁帶到所選取的集區。
   提示。要瞭解某個集區是否可從**可用的磁帶**集區使用磁帶，請按一下集區並按一下**資訊**。

備份

依「備份」一節中所述的方式，建立保護計劃。指定備份位置時，請選擇所建立的磁帶集區。

結果

- 要存取將建立備份的位置，請按一下**[備份]**，然後按一下所建立的磁帶集區的名稱。
- 包含備份的磁帶將被移動到所選取的集區。

進一步的磁帶庫使用訣竅

- 您不需要在每次載入新的磁帶時都執行完整清查。為節省時間，請依「快速與完整清查的組合」下的「清查中」區段所述的程序操作。
- 您可以在相同的磁帶儲藏庫中建立集區，並選擇任何一個做為備份的目的地。

在作業系統中從磁帶裝置復原

若要在作業系統中從磁帶裝置復原：

1. 登入 Cyber Protect Web 主控台。
2. 按一下 **[裝置]**，然後選擇已備份的電腦。
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。
5. 軟體將會顯示 復原所需磁帶的清單。缺少的磁帶會顯示為灰色。如果您的磁帶裝置有空的插槽，請將這些磁帶載入該裝置。
6. 設定 其他復原設定。
7. 按一下 **[開始復原]** 開始復原作業。
8. 如果任何所需的磁帶因某些原因而未載入，軟體將會顯示訊息，其中包含所需磁帶的識別碼。執行下列作業：
   a. 載入磁帶。
   b. 執行快速清查。
   c. 按一下 **[概觀]** > **[活動]**，然後按一下具有 **[需要互動]** 狀態的復原活動。
   d. 按一下 **[顯示詳細資料]**，然後按一下 **[重試]** 繼續復原。

如果我看不到儲存在磁帶上的備份，該怎麼辦？

這可能意味著包含磁帶內容的資料庫因某些原因而遺失或損毀。

若要還原資料庫，請執行下列作業：

1. 執行快速清查。

   警告！
   清查期間，請勿打開**將無法識別且匯入的磁帶移至「可用磁帶」集區**。如果打開此開關，您可能會丟失所有備份。

2. 重新掃描 **[無法識別的磁帶]** 集區。如此一來，您將取得載入磁帶的內容。
3. 如果有任何偵測到的備份延續到其他尚未重新掃描的磁帶中，請在出現提示時載入這些磁帶，然後重新掃描這些磁帶。

從本機附加的磁帶裝置在可開機媒體下復原

若要從本機附加的磁帶裝置在可開機媒體下復原：

1. 將復原所需的磁帶載入磁帶裝置。
2. 從可開機媒體啟動電腦。
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. 如果磁帶裝置連接使用 iSCSI 介面，請按 [設定 iSCSI 和 NDAS 設備] 所述設定該設備。
5. 按一下 **[磁帶管理]**。
6. 按一下 **[清查]**。
7. 在 **[要清查的物件]**中，選擇磁帶裝置。
8. 按一下 **[開始]** 開始清查。
9. 清查完成後，請按一下 **[關閉]**。
10. 按一下 **[動作]** > **[復原]**。
11. 按一下 **[選擇資料]**，然後按一下 **[瀏覽]**。
12. 展開 **[磁帶裝置]**，然後選擇所需裝置。系統會提示您確認重新掃描。按一下 **[是]**。
13. 選取**無法識別的磁帶**集區。
14. 選擇要重新掃描的磁帶。若要選擇集區的所有磁帶，請選擇 **[磁帶名稱]** 欄標頭旁的核取方塊。
15. 如果磁帶含有受密碼保護的備份，請選擇對應的核取方塊，然後在 **[密碼]** 方塊中指定用於備份的密碼。如果您未指定密碼，或密碼不正確，則無法偵測到備份。請記得這一點，遇到重新掃描後找不到任何備份的情形，可以考量是否為上述原因。

    提示。如果磁帶含有受到不同密碼保護的數個備份，您就需要依次指定每個密碼，重複進行多次重新掃描。
16. 按一下 **[開始]** 以開始重新掃描。如此一來，您將取得載入磁帶的內容。
17. 如果有任何偵測到的備份延續到其他尚未重新掃描的磁帶中，請在出現提示時載入這些磁帶，然後重新掃描這些磁帶。
18. 重新掃描完成後，請按一下 **[確定]**。
19. 在 **[存檔檢視]** 中，選擇包含欲復原資料的備份，然後選擇您要復原的資料。按一下 **[確定]** 之後，**[復原資料]** 頁面將會顯示復原所需磁帶的清單。缺少的磁帶會顯示為灰色。如果您的磁帶裝置有空的插槽，請將這些磁帶載入該裝置。
20. 設定 其他復原設定。
21. 按一下**[確定]**開始復原。
22. 如果任何所需的磁帶因某些原因而未載入，軟體將會顯示訊息，其中包含所需磁帶的識別碼。執行下列作業：
    a. 載入磁帶。
    b. 執行快速清查。
    c. 按一下 **[概觀]** > **[活動]**，然後按一下具有 **[需要互動]** 狀態的復原活動。
    d. 按一下 **[顯示詳細資料]**，然後按一下 **[重試]** 繼續復原。

在可開機媒體下從附加至儲存節點的磁帶裝置復原

若要在可開機媒體下從附加至儲存節點的磁帶裝置復原：

1. 將復原所需的磁帶載入磁帶裝置。
2. 從可開機媒體啟動電腦。
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. 按一下 **[復原]**。
5. 按一下 **[選擇資料]**，然後按一下 **[瀏覽]**。
6. 在 **[路徑]** 方塊中，輸入 bsp://<儲存節點地址>/<集區名稱>/，其中 <儲存節點地址> 是包含所需備份之儲存節點的 IP 位址，而 <集區名稱> 則是磁帶集區的名稱。按一下 **[確定]**，然後指定集區的認證。
7. 選擇備份，然後選擇您要復原的資料。按一下 **[確定]** 之後，**[復原資料]** 頁面將會顯示復原所需磁帶的清單。缺少的磁帶會顯示為灰色。如果您的磁帶裝置有空的插槽，請將這些磁帶載入該裝置。
8. 設定 其他復原設定。
9. 按一下**[確定]**開始復原。
10. 如果任何所需的磁帶因某些原因而未載入，軟體將會顯示訊息，其中包含所需磁帶的識別碼。執行下列作業：
    a. 載入磁帶。
    b. 執行快速清查。
    c. 按一下 **[概觀]** > **[活動]**，然後按一下具有 **[需要互動]** 狀態的復原活動。
    d. 按一下 **[顯示詳細資料]**，然後按一下 **[重試]** 繼續復原。

磁帶管理

偵測磁帶裝置

偵測磁帶裝置時，備份軟體會尋找附加至電腦的磁帶裝置，然後將其相關資訊置於磁帶管理資料庫。系統會從 RSM 停用偵測到的磁帶裝置。

通常，只要將磁帶裝置附加到已安裝產品的電腦，就會立即偵測到。然而，在以下情況下，您可能需要偵測磁帶裝置：

- 附加或重新附加磁帶裝置後。
- 在附加磁帶裝置的電腦上安裝或重新安裝備份軟體後。

若要偵測磁帶裝置

1. 按一下**[設定]** > **[磁帶管理]**。
2. 選擇磁帶裝置所連接的電腦。
3. 按一下 **[偵測裝置]**。您會看到連線的磁帶裝置、其磁碟機和插槽。

磁帶集區

備份軟體使用磁帶集區，亦即磁帶的邏輯群組。軟體包含下列預先定義的磁帶集區：**無法識別的磁帶**、**已匯入的磁帶**、**可用磁帶**和 **Acronis**。此外，您也可以建立您自己的自訂集區。

Acronis 集區和自訂集區也當成備份位置。

預先定義的集區

無法識別的磁帶

此集區包含第三方應用程式寫入的磁帶。若要寫入到此類磁帶，您需要將這些磁帶明確移動到 **可用磁帶**集區。您僅能將磁帶從此集區移到**可用磁帶**集區，無法移到任何其他集區。

已匯入的磁帶

此集區包含由 Acronis Cyber Protect 在附加於另一個儲存節點或代理程式的磁帶裝置中寫入的磁帶。若要寫入到此類磁帶，您需要將這些磁帶明確移動到 **可用磁帶**集區。您僅能將磁帶從此集區移到**可用磁帶**集區，無法移到任何其他集區。

可用磁帶

此集區包含可用 (空的) 磁帶。您可以手動將磁帶從其他集區移到此集區。

當您將磁帶移動至**可用磁帶**集區時，軟體會將其標示為空的。如果磁帶內含備份，則會使用 圖示加以標示。軟體啟動覆寫磁帶時，將從資料庫中移除備份的相關資料。

Acronis

當您不想自行建立集區時，軟體預設會使用此集區進行備份。此集區通常適用於具有少量磁帶的單一磁帶機。

自訂集區

如果您想要區分不同資料的備份，您需要建立數個集區。例如，您不妨建立多個自訂集區，以區別：

- 來自公司不同部門的備份
- 來自不同電腦的備份
- 系統磁碟區和使用者資料的備份。

集區相關作業

建立集區

若要建立集區：

1. 按一下**[設定]** > **[磁帶管理]**。
2. 選取電腦或您的磁帶裝置所附加的儲存節點，然後按一下機器下的**[磁帶集區]**。
3. 按一下 **[建立集區]**。
4. 指定集區名稱。
5. [選擇性步驟] 清除 **[自動從「可用磁帶」集區取得磁帶...]** 核取方塊。若清除該核取方塊，則只有在特定時間點加入新集區的磁帶才會用於備份。
6. 按一下 **[建立]**。

編輯集區

您可以編輯 **Acronis** 集區或您自訂集區的參數。

若要編輯集區：

1. 按一下**[設定]** > **[磁帶管理]**。
2. 選取電腦或您的磁帶裝置所附加的儲存節點，然後按一下機器下的**[磁帶集區]**。
3. 選擇所需的集區，然後按一下 **[編輯集區]**。
4. 您可以變更集區名稱或設定。如需有關集區設定的詳細資訊，請參閱「建立集區」一節。
5. 按一下**[儲存]**儲存變更。

刪除集區

您只能刪除自訂集區。預先定義的磁帶集區 (**[無法識別的磁帶]**、**[已匯入的磁帶]**、**[可用磁帶]** 及 **Acronis**) 無法刪除。

注意事項
刪除集區之後，不要忘記編輯將集區作為備份位置的保護計劃。否則，這些保護計劃將失敗。

若要刪除集區：

1. 按一下**[設定]** > **[磁帶管理]**。
2. 選取電腦或您的磁帶裝置所附加的儲存節點，然後按一下機器下的**[磁帶集區]**。
3. 選擇所需的集區，然後按一下 **[刪除]**。
4. 選擇欲刪除的集區在刪除後，該集區中的磁帶要移至哪個集區。
5. 按一下 **[確定]**，以刪除集區。

磁帶的相關作業

移至其他插槽

您可以在下列情況下使用此作業：

- 您需要從磁帶裝置中同時取出數個磁帶。
- 您的磁帶裝置沒有郵件插槽，而要退出的磁帶位於非卸離式磁帶匣的插槽中。

您需要將磁帶移至單一插槽磁帶匣的插槽，然後手動退出磁帶匣。

若要將磁帶移至其他插槽

1. 按一下**[設定]** > **[磁帶管理]**。
2. 選取電腦或您的磁帶裝置所附加的儲存節點，然後按一下機器下的**[磁帶集區]**。
3. 按一下包含必要磁帶的集區，然後選擇所需的磁帶。
4. 按一下 **[搬移到插槽]**。
5. 選擇所選擇的磁帶要移至哪個新插槽。
6. 按一下 **[搬移]** 開始作業。

移至其他集區

此作業可讓您將一或多個磁帶從一個集區移動到另一個集區。

當您將磁帶移動至**可用磁帶**集區時，軟體會將其標示為空的。如果磁帶內含備份，則會使用  圖示加以標示。軟體啟動覆寫磁帶時，將從資料庫中移除備份的相關資料。

特定磁帶類型注意事項

- 有防寫保護及單次寫入限制的 WORM (單寫多讀) 磁帶無法移動至 **[可用磁帶]** 集區。
- 清理磁帶一律顯示於 **[無法識別的磁帶]** 集區，無法移動至其他集區。

若要將磁帶移動至其他集區

1. 按一下**[設定]** > **[磁帶管理]**。
2. 選取電腦或您的磁帶裝置所附加的儲存節點，然後按一下機器下的**[磁帶集區]**。
3. 按一下包含必要磁帶的集區，然後選擇所需的磁帶。
4. 按一下 **[搬移到集區]**。
5. 選擇性步驟：如果您要為選擇的磁帶建立另一個集區，請按一下 **[新集區]**。執行建立集區一節說明的動作。
6. 選擇磁帶移動的目標集區。
7. 按一下 **[搬移到]** 儲存變更。

注意事項
如果您的磁帶上有可還原備份，而您將磁帶移到另一個集區，請在完成移動作業之後，確認重新整理備份儲存下的儲藏庫。不論原始備份目的地為何，第二個集區都提供備份。

清查

清查作業會偵測載入磁帶裝置的磁帶，並為沒有名稱的磁帶指派名稱。

清查法

有兩種清查方法。

快速清查

代理程式或儲存節點掃描磁帶以獲得條碼。使用條碼可以讓軟體快速地將磁帶歸回其先前所在的集區。

選擇此方法可識別附加到相同電腦之相同磁帶裝置所用的磁帶。其他磁帶將會歸到 **[無法識別的磁帶]** 集區。

如果您的磁帶庫沒有條碼讀取器，所有磁帶都會歸到 **[無法識別的磁帶]** 集區。為識別您的磁帶，請執行完整清查，或依照本節稍後的說明結合快速與完整清查。

完整清查

代理程式或儲存節點讀取之前寫入的標籤，並分析其他關於已載入磁帶內容的資訊。選擇此方法可識別空的磁帶，以及相同軟體在任何磁帶裝置與任何電腦上寫入的磁帶。

下表顯示完整清查後磁帶的傳送目的地集區。

磁帶的使用者...	磁帶的讀取者...	磁帶的傳送目的地集區...
代理程式	相同的代理程式	磁帶先前的所在位置
	其他代理程式	**已匯入的磁帶**
	儲存節點	**已匯入的磁帶**
儲存節點	相同的儲存節點	磁帶先前的所在位置
	其他儲存節點	**已匯入的磁帶**
	代理程式	**已匯入的磁帶**
第三方備份應用程式	代理程式或儲存節點	**無法識別的磁帶**

特定類型的磁帶會傳送至特定集區：

磁帶類型	磁帶的傳送目的地集區...
空磁帶	**可用磁帶**
空白的防寫保護磁帶	**無法識別的磁帶**
清理磁帶	**無法識別的磁帶**

快速清查可套用至所有磁帶裝置。快速清查可套用至所有磁帶裝置、個別磁帶機或插槽。如果是獨立磁帶機，則即使選擇了快速清查，仍會始終執行完整清查。

結合快速與完整清查

對整個磁帶裝置執行完整清查可能需要很長的時間。如果您只需要清查一些磁帶，請依下列方式繼續：

1. 執行磁帶裝置快速清查。
2. 按一下 **[無法識別的磁帶]** 集區。尋找要清查的磁帶，並記錄它們所使用的插槽。
3. 執行這些插槽的完整清查。

清查的後續作業

如果您要備份至 **[無法識別的磁帶]** 或 **[已匯入的磁帶]** 集區中的磁帶，請將其移動至 **[可用磁帶]** 集區，然後再移動至 **Acronis** 集區或自訂集區。如果您要的備份目的地集區為可補充集區，則您可以將磁帶留在 **[可用磁帶]** 集區。

如果您要從置於 **[無法識別的磁帶]** 或 **[已匯入的磁帶]** 集區中的磁帶進行復原，則需要重新掃描該磁帶。如此一來，該磁帶將移至與您在重新掃描期間移至的集區，而儲存在磁帶上的備份將出現在該位置。

動作順序

1. 按一下**[設定]** > **[磁帶管理]**。
2. 選擇磁帶設備所連接的電腦，然後選擇要清查的磁帶設備。
3. 按一下 **[清查]**。
4. [選擇性步驟] 若要選擇快速清查請關閉**[完整清查]**。
5. [選擇性步驟] 打開**將無法識別且已匯入的磁帶移至 [可用磁帶] 集區**。

   警告！
   只有當您完全確定儲存在磁帶上的資料可以覆寫時，才應該啟用此開關。

6. 按一下 **[立即開始清查]** 開始清查。

重新掃描

磁帶內容的相關資訊儲存在專用資料庫中。重新掃描作業會讀取磁帶的內容，並在資料庫中的資訊不符合磁帶上所儲存資料時更新資料庫。作業完成後所偵測到的備份會置於指定集區中。

您可以於單一作業內重新掃描特定集區內的磁帶。您只能選擇線上磁帶進行此作業。

若要重新掃描包含多重資料流備份的磁帶或同時包含多重資料流和多工備份的磁帶，您至少需要具備與用來建立此備份相同數目的磁碟機。這種備份無法透過獨立磁帶機重新掃描。

執行重新掃描：

- 如果儲存節點或受管理電腦的資料庫遺失或損壞。
- 如果資料庫中的磁帶相關資訊已過期 (例如，其他儲存節點或代理程式已修改磁帶內容)。
- 在可開機媒體下工作時，取得存取權以存取磁帶上儲存的備份。
- 如果誤從資料庫移除磁帶的相關資訊。重新掃描已移除的磁帶時，儲存在其上的備份會重新出現在資料庫中，並可供資料復原之用。
- 如果您已手動或透過保留規則從磁帶中刪除備份，但您希望那些備份可供存取以進行資料復原。重新掃描此類磁帶之前，請先將其退出、從資料庫中移除其相關資訊，然後再次將磁帶插入磁帶裝置。

若要重新掃描磁帶

1. 按一下**[設定]** > **[磁帶管理]**。
2. 選取電腦或您的磁帶裝置所附加的儲存節點，然後按一下電腦下的**磁帶裝置**。
3. 選取您載入磁帶的磁帶裝置。
4. 執行快速清查。

   注意事項
   在清查期間，請勿啟用**將無法識別且已匯入的磁帶移至 [可用磁帶] 集區**開關。

5. 選取**無法識別的磁帶**集區。這是快速清查後大部分磁帶的傳送目的地集區。也可重新掃描任何其他集區。
6. [選擇性]要僅重新掃描個別磁帶，請選取。

7. 按一下**重新掃描**。
8. 請選取新偵測到的備份將放置在哪個集區。
9. 必要時，請選取**[啟用從儲存在磁帶上的磁碟備份復原檔案]**核取方塊。

   詳細資料。如果選取此核取方塊，軟體將會在磁帶裝置所連接電腦的硬碟中，建立特別的補充檔案。只要這些補充檔案完整無缺，就能從磁碟備份復原檔案。如果磁帶包含應用程式感知備份，請務必選取該核取方塊。否則，您將無法從這些備份復原應用程式資料。
10. 如果磁帶包含受密碼保護的存檔，請選取對應對應的核取方塊，然後指定備份密碼。如果您未指定密碼，或密碼不正確，則無法偵測到備份。請記得這一點，遇到重新掃描後找不到任何備份的情形，可以考量是否為上述原因。

    提示。如果磁帶含有受到不同密碼保護的備份，您就需要依次指定每個密碼，重複進行多次重新掃描。
11. 按一下**開始重新掃描**開始重新掃描。

結果。選擇的磁帶移至所選集區。儲存在磁帶上的備份可在此集區中找到。如果一個備份分散在數個磁帶中，必須等到所有內含備份的磁帶都重新掃描完成後，備份才會出現在集區中。

重新命名

軟體偵測到新磁帶時，會自動以下列格式將名稱指派給磁帶：**磁帶 XXX**，其中 **XXX** 是不重複的編號。軟體會依照順序指派磁帶的編號。重新命名作業可讓您手動變更磁帶的名稱。

若要重新命名磁帶

1. 按一下**[設定]** > **[磁帶管理]**。
2. 選取電腦或您的磁帶裝置所附加的儲存節點，然後按一下機器下的**[磁帶集區]**。
3. 按一下包含必要磁帶的集區，然後選擇所需的磁帶。
4. 按一下 **[重新命名]**。
5. 輸入選定磁帶的新名稱。
6. 按一下 **[重新命名]** 儲存變更。

清除

清除磁帶時，會完全刪除儲存在磁帶上的所有備份，並從資料庫移除這些備份的相關資訊。但是，磁帶本身的相關資訊會保留在資料庫中。

清除進行後，位於 **[無法識別的磁帶]** 或 **[已匯入的磁帶]** 集區的磁帶會移至 **[可用磁帶]** 集區。位於任何其他集區的磁帶則不會移動。

若要清除磁帶

1. 按一下**[設定]** > **[磁帶管理]**。
2. 選取電腦或您的磁帶裝置所附加的儲存節點，然後按一下機器下的**[磁帶集區]**。
3. 按一下包含必要磁帶的集區，然後選擇所需的磁帶。
4. 按一下 **[清除]**。系統會提示您確認作業。
5. 選擇清除方法：[快速] 或 [完整]。

6. 按一下 **[清除]** 開始作業。

詳細資料。無法取消清除作業。

退出

若要從磁帶庫成功退出磁帶，磁帶庫必須有郵件插槽，而且該插槽不能由使用者或其他軟體鎖定。

若要退出磁帶

1. 按一下**[設定]** > **[磁帶管理]**。
2. 選取電腦或您的磁帶裝置所附加的儲存節點，然後按一下機器下的**[磁帶集區]**。
3. 按一下包含必要磁帶的集區，然後選擇所需的磁帶。
4. 按一下 **[退出]**。軟體將會提示您提供磁帶描述。建議您描述磁帶未來的實體保存位置。在復原期間，軟體將會顯示此描述，以便您便能輕鬆找到磁帶。
5. 按一下 **[退出]** 開始作業。

手動或自動退出磁帶後，建議在磁帶上寫上其名稱。

移除

移除作業會從資料庫刪除選定磁帶上所儲存備份的相關資訊和磁帶本身的相關資訊。

您只能移除離線 (已退出) 的磁帶。

若要移除磁帶

1. 按一下**[設定]** > **[磁帶管理]**。
2. 選取電腦或您的磁帶裝置所附加的儲存節點，然後按一下機器下的**[磁帶集區]**。
3. 按一下包含必要磁帶的集區，然後選擇所需的磁帶。
4. 按一下 **[移除]**。系統會提示您確認作業。
5. 按一下 **[確定]** 移除磁帶。

如果磁帶誤遭移除，應該怎麼辦？

和清除後的磁帶不同的是，已移除磁帶中的資料實際上不會刪除。因此，您可以讓儲存在這類磁帶上的備份再次成為可用狀態。若要這麼做：

1. 將磁帶載入磁帶裝置。
2. 執行快速清查以偵測磁帶。

   注意事項
   在清查期間，請*勿*啟用**將無法識別且已匯入的磁帶移至 [可用磁帶] 集區**開關。

3. 執行重新掃描，以比對儲存在磁帶上的資料和資料庫。

指定磁帶組

透過該作業，您可指定磁帶的磁帶組。

磁帶組即在一個集區內的一組磁帶。

不同於在其中可使用變數的備份選項中指定磁帶組，在這裡，您盡可指定一個字串值。

如果希望軟體按照特定規則備份特定磁帶 (例如，如果希望將週一備份儲存到磁帶 1 上，週二備份儲存到磁帶 2 上等)，請執行此作業。對於各所需磁帶，指定特定磁帶組，然後在備份選項中指定同一磁帶組或使用適當變數。

對於上例，請指定用於磁帶 1 的磁帶組 Monday、用於磁帶 2 的磁帶組 Tuesday 等。在備份選項中，請指定 [Weekday]。在這種情況下，在一週的相應日期使用適當磁帶。

若要指定一個或數個磁帶的磁帶組

1. 按一下**[設定]** > **[磁帶管理]**。
2. 選取電腦或您的磁帶裝置所附加的儲存節點，然後按一下機器下的**[磁帶集區]**。
3. 按一下包含必要磁帶的集區，然後選擇所需的磁帶。
4. 按一下**[磁帶組]**。
5. 輸入磁帶組名稱。如果已指定另一磁帶組用於所選磁帶，則將會被替換。如果要排除磁帶組中的磁帶但不指定另一個磁帶組，則刪除現有磁帶組名稱。
6. 按一下**[儲存]**儲存變更。

儲存節點

儲存節點是一部伺服器，其設計旨在最佳化保護企業資料所需的各種資源 (例如企業儲存容量、網路頻寬和生產伺服器 CPU 負載) 之使用。藉由組織和管理充當企業備份專用儲存空間的位置 (受管理位置) 可達到這個目標。

Acronis Storage Node 的主要用途是允許集中存取磁帶機或磁帶媒體櫃，例如，將多個裝置中的資料備份和復原至相同的磁帶機或磁帶媒體櫃 (磁帶上的受管儲藏庫) 中。

另一個使用案例是啟用進階重複資料刪除功能，其中多個裝置中的資料必須針對彼此進行重複資料刪除，並儲存在單一位置 (已啟用重複資料刪除的受管儲藏庫)。

安裝儲存節點與目錄服務

在安裝儲存節點之前，確保電腦符合系統需求。

我們建議您將儲存節點與目錄服務安裝在不同的電腦上。用於執行目錄服務之電腦的系統需求，詳述於 "編目最佳作法" (第 533 頁) 中。

若要安裝儲存節點及/或目錄服務

1. 以系統管理員身分登入，並啟動 Acronis Cyber Protect 安裝程式。
2. [選擇性步驟]:若要變更安裝程式的語言，請按一下 **[設定語言]**。
3. 接受授權合約和隱私權聲明的條款，然後按一下 **[下一步]**。
4. 按一下 **[安裝保護代理程式]**。
5. 按一下**[自訂安裝設定]**。
6. 在**[要安裝的項目]** 旁，按一下**[變更]**。
7. 選擇要安裝的元件：

- 若要安裝儲存節點，選擇**[儲存節點]**核取方塊。自動選擇 **[Windows 用代理程式]** 核取方塊。
- 若要安裝目錄服務，選擇**[目錄服務]**核取方塊。
- 如果不想在此電腦上安裝其他元件，請清除元件對應的核取方塊。

按一下**[完成]** 以繼續。

8. 指定將註冊元件的管理伺服器：
   a. 在 **Acronis Cyber Protect Management Server** 旁邊，按一下 **[指定]**。
   b. 指定已安裝管理伺服器的電腦的名稱或 IP 位址。
   c. 指定管理伺服器系統管理員的認證或註冊權杖。
      如需有關如何產生註冊權杖的詳細資訊，請參閱 "步驟 1：產生註冊權杖" (第 157 頁)。
   d. 按一下**[完成]**。
9. 若出現提示，則選擇具有儲存節點及/或目錄服務的電腦是新增至組織，還是其中一個單位。
   如果您管理多個單位或具有至少一個單位的組織，則會出現此提示。否則，電腦將以無訊息方式新增至您管理的單位或組織中。如需更多資訊，請參閱「管理員與單位」。
10. [選擇性步驟] 如「自訂安裝設定」中所述變更其他安裝設定。
11. 按一下**[安裝]** 以開始安裝。
12. 安裝完成後，請按一下**[關閉]**。

使用 Acronis Cyber Protect 15 Update 4 更新目錄服務

Acronis Cyber Protect 15 Update 4 使用新版本的目錄服務。新版本與舊版建立的目錄資料不直接相容。

在更新至 Acronis Cyber Protect 15 Update 4 的過程中，可將此資料手動移轉至新版本的目錄服務。或者，也可以略過移轉，稍後再重新建立目錄服務。重新建立目錄資料所需的時間比移轉更多。

若要移轉目錄資料

1. 在安裝目錄服務所在的電腦上，執行 Acronis Cyber Protect 安裝程式。
2. 接受授權合約和隱私權聲明的條款，然後按一下 **[下一步]**。
3. 選擇 **[我瞭解]** 核取方塊，然後按一下 **[更新]**。
4. 選取 **[指定暫存資料夾]** 核取方塊。
5. 指定將要匯出目錄資料的目的地資料夾。
   匯出的資料已加密。移轉完成後，會自動刪除暫存資料夾。
6. 按一下**[完成]**。

若要略過移轉目錄資料

1. 在安裝目錄服務所在的電腦上，執行 Acronis Cyber Protect 安裝程式。
2. 接受授權合約和隱私權聲明的條款，然後按一下 **[下一步]**。
3. 選擇 **[我瞭解]** 核取方塊，然後按一下 **[更新]**。
4. 清除 **[指定暫存資料夾]** 核取方塊。
5. 按一下**[完成]**。
6. 確認選擇項目。

結果是，在更新至 Acronis Cyber Protect 15 Update 4 之後，現有的目錄資料將會變成無法使用。若要重新建立目錄資料，請執行備份。

注意事項

如果目錄服務、儲存節點和管理伺服器是在不同電腦上執行，請確認將它們全部更新至 Acronis Cyber Protect 15 Update 4，更新順序如下：

1. 管理伺服器
2. 儲存節點
3. 目錄服務

新增受管理的位置

可以組織受管理的位置：

- 在本機資料夾內：
  - 在儲存節點本機的硬碟上
  - 在作業系統會認為是本機連接裝置的 SAN 儲存裝置上
- 在網路資料夾內：
  - 在 SMB/CIFS 共用上
  - 在作業系統會認為是網路資料夾的 SAN 儲存裝置上
  - 在 NAS 上
- 在連接到儲存節點的本機磁帶裝置上。

  磁帶位置是以磁帶集區的形式建立。依預設，將存在一個磁帶集區。若有必要，您可以建立其他的磁帶集區，如此區段的稍後部分中所述。

若要在本機或網路資料夾內建立受管理的位置

1. 執行下列其中一項操作：
   - 按一下 **[備份儲存]** > **[新增位置]**，然後按一下 **[儲存節點]**。
   - 建立保護計劃時，按一下 **[備份位置]** > **[新增位置]**，然後按一下 **[儲存節點]**。
   - 按一下 **[設定]** > **[儲存節點]**，選擇將管理位置的儲存節點，然後按一下 **[新增位置]**。
2. 在**[名稱]**中，指定位置的唯一的名稱。「唯一」意味著不得有受相同儲存節點管理的另一個相同名稱的位置。
3. [選擇性步驟] 選擇將管理位置的儲存節點。若您選擇了步驟 1 中的最後一個選項，則將無法變更儲存節點。
4. 選擇代理程式將用來存取位置的儲存節點名稱或 IP 位址。

   依預設，會選擇儲存節點名稱。如果 DNS 伺服器無法解析名稱為 IP 位址，而造成存取失敗，則需變更此設定。之後若要變更此設定，請按一下 **[備份儲存]** > 位置 > **[編輯]**，然後變更 **[位址]** 欄位值。
5. 輸入資料夾路徑或瀏覽所需資料夾。
6. 按一下**[完成]**。軟體將檢查對該特定資料夾的存取權限。
7. [選擇性步驟] 在位置中啟用備份重複資料刪除功能。

   重複資料刪除可以消除重複的磁碟區塊，來減少備份流量及縮小儲存在位置內的備份大小。

如需有關重複資料刪除限制的詳細資訊，請參閱「重複資料刪除限制」。

8. [僅在啟用重複資料刪除時] 指定或變更**重複資料刪除資料庫路徑**欄位值。

   這必須是儲存節點本機硬碟上的資料夾。為了改善系統效能，我們建議您在不同的磁碟上建立重複資料刪除資料庫與受管理位置。

   如需重複資料刪除資料庫的相關資訊，請參閱「重複資料刪除最佳作法」。
9. [選擇性步驟] 選擇是否要使用加密來保護位置。任何寫入到該位置的內容都將被加密，而任何從其中讀取的內容也將由儲存節點使用儲存在儲存節點的位置專屬的加密金鑰，以透通的方式解密。

   有關加密的更多資訊，請參閱「位置加密」。
10. [選擇性] 選擇是否要為儲存在位置中的備份編目。資料目錄能讓您輕鬆找到所需的資料版本，並選擇該版本進行復原。

    當管理伺服器上已登錄數個編目服務時，您可以選擇將對儲存在位置的備份進行編目的服務。您稍後可以啟用或停用編目，如「如何啟用或停用編目」。
11. 按一下**[完成]**以建立位置。

在磁帶裝置上建立受管理的位置

1. 按一下 **[備份儲存]** > **[新增位置]**，或在建立保護計劃時，按一下 **[備份位置]** > **[新增位置]**。
2. 按一下**[磁帶]**。
3. [選擇性步驟] 選擇將管理位置的儲存節點。
4. 請依「建立集區」中所述的步驟操作，從步驟 4 開始。

注意事項
依預設，代理程式使用儲存節點名稱，以存取受管理的磁帶位置。若要使代理程式使用儲存節點 IP 位址，按一下 **[備份儲存]** > 位置 > **[編輯]**，然後變更 **[位址]** 欄位值。

重複資料刪除

重複資料刪除限制

常見限制

加密的備份無法進行重複資料刪除。如果您要同時使用重複資料刪除和加密，請將備份保留為未加密狀態，並將其導向至同時啟用重複資料刪除和加密的位置。

磁碟層級備份

如果磁碟區的配置單位大小 (也稱為叢集大小或區塊大小) 不能被 4 KB 整除，軟體就不會對磁碟區塊執行重複資料刪除。

注意事項
大部分 NTFS 和 ext3 磁碟區的配置單位大小為 4 KB。因此您可以對這類磁碟區進行區塊層級的重複資料刪除。其他允許區塊層級重複資料刪除的配置單位大小包括 8 KB、16 KB 和 64 KB 等。

檔案層級備份

如果檔案經過加密，就無法對檔案執行重複資料刪除。

重複資料刪除和 NTFS 資料流

在 NTFS 檔案系統中，一個檔案可能有一或多組相關聯的其他資料，這通常稱為*替代資料流*。

備份這類檔案時，其替代資料流也會一併獲得備份。但是，即使檔案本身經過重複資料刪除處理，軟體也不會對替代資料流執行重複資料刪除。

重複資料刪除最佳作法

重複資料刪除是一項取決於許多因素的複雜程序。

以下為影響重複資料刪除速度的最重要因素：

- 存取重複資料刪除資料庫的速度
- 儲存節點的 RAM 容量
- 在儲存節點上建立的重複資料刪除位置數量。

若要提高重複資料刪除效能，請參考以下建議。

將重複資料刪除資料庫和重複資料刪除位置放在不同的實體裝置上

重複資料刪除資料庫會儲存儲藏庫中所儲存全部項目的雜湊值，但無法進行重複資料刪除的項目除外，例如加密的檔案。

若要提高重複資料刪除資料庫的存取速度，資料庫和位置必須位於不同的實體裝置上。

最佳作法是分別為位置和資料庫配置專用的裝置。如果無法這麼做，至少避免將位置或資料庫放在與作業系統相同的磁碟上。原因在於，作業系統會執行大量硬碟讀寫作業，這會大幅減慢重複資料刪除速度。

選擇重複資料刪除資料庫的磁碟

- 資料庫必須位於固定式磁碟機上。請勿嘗試將重複資料刪除資料庫置於外部可卸離式磁碟機上。
- 若要將資料庫的存取時間減至最少，請將其儲存在直接連接的磁碟機上，而非儲存在掛載的網路磁碟區上。網路延遲可能會大幅降低重複資料刪除效能。
- 您可以透過以下公式估算重複資料刪除資料庫所需的磁碟空間：

$$S = U * 90 / 65536 + 10$$

其中，

S 是磁碟大小 (GB)

U 是重複資料刪除資料存放區中預計會存放的唯一資料量 (GB)

例如，如果重複資料刪除資料存放區中預計會存放 U=5 TB 的唯一資料量，則重複資料刪除資料庫需要的可用空間至少為：

S = 5000 * 90 / 65536 +10 = 17 GB

選擇重複資料刪除位置的磁碟

為避免資料遺失，建議使用 RAID 10、5 或 6。不建議使用 RAID 0，因為該設定不容錯。不建議使用 RAID 1，因其速度較慢。本機磁碟或 SAN，兩者均可使用。

每 1 TB 的唯一資料，40 至 160 MB 的 RAM

當達到此限制值時，重複資料刪除將會停止，但備份和復原將會繼續工作。若要向儲存節點新增更多 RAM，在下一次備份之後，重複資料刪除將會回復。一般而言，擁有的 RAM 越多，您可以儲存的唯一資料量就越多。

每個儲存節點上只有一個重複資料刪除位置

強烈建議您在一個儲存節點上僅建立一個重複資料刪除位置。否則，所有可用的 RAM 磁碟區可能會按照位置的數量等比例分配。

缺乏競爭資源的應用程式

具有儲存節點的電腦不應執行需要很多系統資源的應用程式，例如資料庫管理系統 (DBMS) 或企業資源規劃 (ERP) 系統。

多核心處理器，具備至少 2.5 GHz 的時脈

建議您使用至少 4 核心、時脈至少 2.5 GHz 的處理器。

位置中有足夠的可用空間

儲存至位置後，在目標端進行重複資料刪除作業所需的可用空間，和備份資料佔用的空間一樣大。若不在來源端進行壓縮或重複資料刪除，這個數值會等於在備份作業期間備份的原始資料大小。

高速 LAN

建議使用 1-Gbit 的 LAN。這可讓軟體同時執行 5-6 個含重複資料刪除的備份作業，且速度不會大幅減慢。

備份多部內容相似的電腦之前，先備份一部具有代表性的電腦

備份內容相似的多台電腦之前，建議您先備份一台電腦，並等候備份資料編列索引完畢。之後，由於重複資料刪除的效率提高，因此其他電腦的備份速度便可加快。由於第一部電腦的備份已編列索引，因此大多數資料已進入重複資料刪除資料儲存區。

在不同時間備份不同的電腦

如果您備份大量電腦，請將備份作業分散到不同的時間執行。方法是，建立多個不同排程的保護計劃。

位置加密。

若您使用加密保護位置，寫入節點的所有內容都將會加密，而從中讀取的所有內容都將由儲存節點以節點上儲存的特定位置加密金鑰來透明解密。如果儲存媒體被盜或由未經授權的人員存取，罪犯將因無法存取儲存節點而無法解密位置內容。

此加密與保護計劃所指定且由代理程式執行的備份加密無關。如果備份已加密，則儲存節點端加密將套用於代理程式執行的加密之上。

若要使用加密保護位置

1. 指定並確認要用於產生加密金鑰的文字 (密碼)。
   文字會區分大小寫。只有將位置連接至其他儲存節點時，才會要求您輸入此文字。
2. 選擇下列其中一個加密演算法：
   - **AES 128**–位置內容將以採用 128 位元金鑰的進階加密標準 (AES) 演算法加密。
   - **AES 192**–位置內容將以採用 192 位元金鑰的 AES 演算法加密。
   - **AES 256**–位置內容將以採用 256 位元金鑰的 AES 演算法加密。
3. 按一下 **[確定]**。

AES 加密演算法以加密區塊鏈結 (CBC) 模式作業，並使用隨機產生的金鑰 (依使用者定義，大小可為 128、192 或 256 位元)。金鑰大小愈大，程式就要更長的時間加密位置中儲存的備份，而備份也將更安全。

之後，會以所選文字的 SHA-256 雜湊作為金鑰，使用 AES-256 來加密加密金鑰。文字本身並不會儲存在磁碟上；文字雜湊會用於驗證。有了這兩層安全保護，備份即可免於未經授權的存取，但如果文字遺失，則無法復原。

編目

資料目錄

資料目錄能讓您輕鬆找到所需的資料版本，並選擇該版本進行復原。資料目錄會顯示啟用編目所在受管理位置中儲存的資料。

只有在管理伺服器上註冊至少一個目錄服務時，**[目錄]** 區段才會出現在 **[備份儲存]** 索引標籤下方。如需安裝目錄服務的相關資訊，請參閱「安裝儲存節點及目錄服務」。

只有組織管理員能夠看見 **[目錄]** 區段。

限制

只有實體機器的磁碟與檔案層級備份以及虛擬機器的備份支援編目。

目錄中無法顯示下列資料：

- 加密備份中的資料。
- 備份至磁帶裝置的資料

- 備份至雲端儲存的資料。
- 由 Acronis Cyber Protect 12.5 之前產品版本備份的資料

選擇復原用的備份資料

1. 按一下 **[備份儲存]** > **[目錄]**。
2. 當管理伺服器上已登錄數個編目服務時，選擇將對儲存在位置的備份進行編目的服務。

   注意事項
   若要查看哪個服務編目位置，請在 **[備份儲存]** > **[位置]** > **[位置]** 中選擇該位置，然後按一下 **[詳細資料]**。

3. 軟體即會顯示備份至由選定目錄服務編目之受管理位置的電腦。
   透過瀏覽或使用搜尋，選擇要復原的資料。
   - **瀏覽**
     按兩下電腦，檢視其中所包含的已備份磁碟、磁碟區、資料夾及檔案。
     若要復原磁碟，請選擇標記有以下圖示的磁碟： 
     若要復原磁碟區，請按兩下包含有磁碟區的磁碟，然後選擇該磁碟區。
     若要復原檔案及資料夾，請瀏覽其所在的磁碟區。您可以瀏覽標記有資料夾圖示的磁碟區： 
   - **搜尋**
     在搜尋欄位中，輸入有助於識別所需資料項目的資訊 (可以是電腦名稱、檔案或資料夾名稱、或磁碟標籤)，然後按一下 **[搜尋]**。
     您可以使用星號 (*) 和問號 (?) 作為萬用字元。
     搜尋完成後，您將看到其名稱與您輸入的值完全或部分相符的備份資料項目的清單。
4. 依預設，會將資料還原至最新的可能時間點。如果選擇單一項目，則可以使用 **[版本]** 按鈕，選擇復原點。
5. 選擇所需資料後，執行下列其中一項操作：
   - 按一下 **[復原]**，然後設定復原作業的參數，如 < 復原 > 中所述。
   - [僅適用於檔案/資料夾] 如果您要將檔案儲存為 .zip 檔案，請按一下 **[下載]**，選擇儲存資料的位置，然後按一下 **[儲存]**。

編目最佳作法

若要提高編目效能，請依照以下建議。

安裝

我們建議您將目錄服務與儲存節點安裝在不同的電腦上。否則，這些元件將競爭 CPU 和 RAM 資源。

如果在管理伺服器上登錄數個儲存節點，則一個目錄服務足夠，除非編列索引或搜尋效能降低。例如，如果您注意到編目全天候執行 (意味著編目活動之間沒有暫停)，請在單獨的電腦上安裝多個目

錄服務。然後，移除部分受管理位置，並使用新的目錄服務重新建立。這些位置中儲存的備份將保持完整。

系統需求

參數	最小值	建議值
CPU 核心數目	2	4 個和以上
RAM	8 GB	16 GB 和以上
硬碟	7200 rpm HDD	SSD
具有儲存節點的電腦與具有目錄服務的節點之間的網路連線	100 Mbps	1 Gbps

如何啟用或停用編目

如果為受管理位置啟用編目，一旦建立備份之後，導向至位置的每個備份內容就會加入至備份目錄。

您可以在新增受管理的位置時啟用編目，也可以稍後啟用。一旦啟用編目之後，儲存在位置中且先前還未編目的所有備份都將在下次備份至位置之後編目。

編目程序可能很耗時，特別是在要將大量電腦備份至相同的位置時。您可以隨時停用編目。在停用完成之前建立之備份的編目。新建立的備份將不會編目。

若要為現有的位置設定編目

1. 按一下 **[備份儲存]** > **[位置]**。
2. 按一下 **[位置]**，然後選擇您要設定編目所在的受管理位置。
3. 按一下 **[編輯]**。
4. 啟用或停用 **[目錄服務]** 開關。
5. 按一下**[完成]**。

系統設定

這些設定僅可用於內部部署。

若要存取這些設定，請按一下 **[設定]** > **[系統設定]**。

只有組織管理員能夠看見 **[系統設定]** 區段。

電子郵件通知

您可以設定通用於從管理伺服器寄送的所有電子郵件通知的全域設定。

在[預設備份選項]中，您可以針對在備份期間發生的事件覆寫這些設定。在此情況下，全域設定將對除備份以外的作業生效。

當建立保護計劃時，您可以選擇要使用哪些設定：全域設定，或在預設備份選項中所指定的設定。您還可以專屬於此計劃的自訂值覆寫它們。

重要事項
變更全域電子郵件通知設定時，使用全域設定的所有保護計劃都會受到影響。

設定這些設定之前，請確保已經設定了**電子郵件伺服器**設定。

要設定全域電子郵件通知設定

1. 按一下**[設定]** > **[系統設定]** > **[電子郵件通知]**。
2. 在**[收件人電子郵件地址]**欄位中，輸入目的地電子郵件。您可以輸入多組地址，並以分號隔開各組地址。
3. [選擇性步驟] 在**[主旨]**，變更電子郵件通知主旨。
   您可以使用以下變數：
   - `[Alert]` - 警示摘要。
   - `[Device]` - 裝置名稱。
   - `[Plan]` - 產生該警示的計劃的名稱。
   - `[ManagementServer]` - 安裝管理伺服器的電腦的主機名稱。
   - `[Unit]` - 電腦所屬的單位的名稱。

   預設主旨是 `[Alert]` **裝置：**`[Device]` **計劃：**`[Plan]`
4. [選擇性步驟] 選擇 **作用中的警示的相關每日摘要**核取方塊，然後進行以下操作：
   a. 指定要傳送摘要的時間。
   b. [選擇性步驟] 選擇**不要傳送「無作用中警示」訊息**核取方塊。
5. [選擇性步驟] 選擇將在電子郵件通知中使用的語言。
6. 選擇您想要接收通知的事件的核取方塊。您可以從所有可能的警示的清單中選擇，此清單依嚴重性分組。
7. 按一下 **[儲存]**。

電子郵件伺服器

您可以指定一個電子郵件伺服器，用來從管理伺服器傳送電子郵件通知。

若要指定電子郵件伺服器

1. 按一下**[設定]** > **[系統設定]** > **[電子郵件伺服器]**。
2. 在**[電子郵件服務]**中，選擇下列其中一項：
   - **自訂**
   - **Gmail**
   - **Yahoo Mail**
   - **Outlook.com**
3. [僅適用於自訂電子郵件服務] 指定下列設定：
   - 在**[SMTP 伺服器]**中，輸入外送郵件伺服器 (SMTP) 的名稱。
   - 在**[SMTP 連接埠]**中，設定外送郵件伺服器的連接埠。連接埠預設為 25。
   - 請選擇要使用 SSL 或 TLS 加密。選擇 **[無]** 以停用加密。
   - 如果 SMTP 伺服器需要驗證，選擇 **[SMTP 伺服器需要驗證]** 核取方塊，然後指定將用於傳送訊息的帳戶認證。如果您不確定 SMTP 伺服器是否有要求驗證，請連絡您的網路系統管理員或電子郵件服務供應商以取得協助。
4. [僅針對 Gmail、Yahoo Mail 及 Outlook.com] 指定將用於傳送訊息的帳戶認證。
5. [僅限自訂電子郵件服務] 在**[寄件者]**中，輸入寄件者的名稱。此名稱將會顯示在電子郵件通知的**[寄件者]**欄位中。如果將此欄位留空，訊息將會包含步驟 3 或 4 中指定的帳戶。
6. 選擇性步驟：按一下**[傳送測試訊息]**，檢查電子郵件通知在指定設定下是否正確運作。輸入要傳送測試訊息的目標電子郵件地址。

安全性

使用這些選項來加強 Acronis Cyber Protect 內部部署的安全性。

在以下時間之後登出非作用中的使用者

此選項可讓您指定因使用者未動作而自動登出的逾時。當設定逾時剩下一分鐘時，軟體會提示使用者保持登入。否則，使用者將會登出，並失去所有未儲存的變更。

預設為：**[啟用]。逾時：10 分鐘。**

顯示目前使用者上次登入的通知

此選項可顯示使用者上次成功登入的日期與時間、自上次成功登入後的驗證失敗次數，以及上次成功登入的 IP 位址。此資訊會在每次使用者登入時顯示在畫面底部。

預設為：**[已停用]**。

發出本機密碼或網域密碼到期的警告

此選項可顯示使用者存取 Acronis Cyber Protect Management Server 的密碼到期時間。這是本機或網域密碼，使用者使用該密碼登入安裝管理伺服器的電腦。密碼到期時間會顯示在畫面底部和左上角的帳戶功能表中。

預設為：**[已停用]**。

更新

此選項會定義 Acronis Cyber Protect 是否在組織系統管理員每次登入 Cyber Protect Web 主控台時檢查新版本。

預設為：**[啟用]**。

若停用此選項，管理員可按照「檢查軟體更新」中所述手動檢查更新。

預設備份選項

對於管理伺服器上的所有保護計劃，備份選項的預設值都相同。組織系統管理員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建立的所有保護計劃。

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. 以組織系統管理員的身份，登入 Cyber Protect Web 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]**。

保護設定

若要設定保護設定，請移至 Cyber Protect Web 主控台中的 **[設定]** > **[保護]**。

如需有關特定設定和程序的詳細資訊，請參閱本節中對應的主題。

更新保護定義

根據預設，所有保護代理程式都可以連線至網際網路，並下載下列元件的更新：

- 反惡意程式碼
- 弱點評估
- 修補程式管理

具有 [更新者] 角色的代理程式

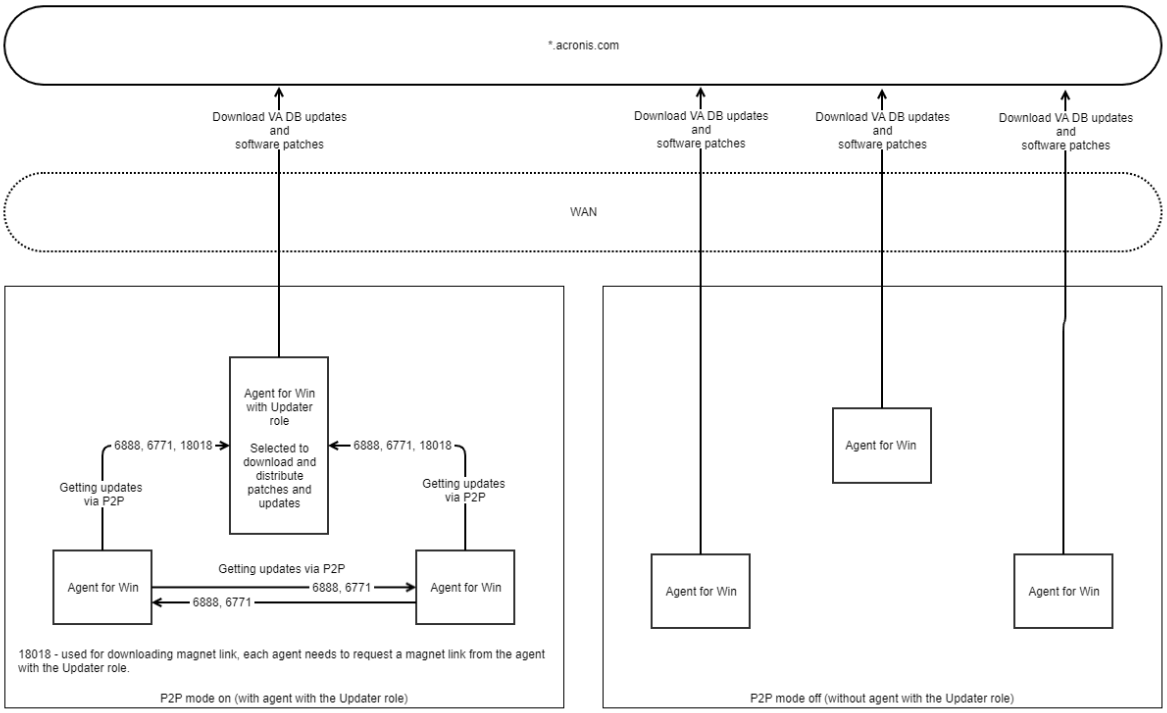
系統管理員可以在環境中選擇一或多個保護代理程式，並為其指派 [更新者] 角色，以便將網路頻寬流量降至最低。因此，專用的代理程式將會連線至網際網路，並下載更新。其他所有代理程式將會使用對等技術連線至專用的更新程式代理程式，然後從中下載更新。

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。

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。

您可以將 [更新者] 角色指派給環境中的多個代理程式。因此，如果具有 [更新者] 角色的代理程式離線，具有此角色的其他代理程式可以當作更新的保護定義來源。

下圖說明用於下載保護更新的選項。在左側，代理程式會獲指派 [更新者] 角色。該代理程式可以連線到網際網路下載保護更新，且其對等代理程式可以連線到 Updater 代理程式取得最新的更新。在右側，沒有代理程式獲指派 [更新者] 角色，因此所有代理程式都可以連線到網際網路下載保護更新。



準備 [更新者] 角色的電腦

1. 在執行具有 [更新者] 角色的代理程式所在電腦上，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 服務。
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] 角色指派給代理程式

1. 在 Cyber Protect Web 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。

排程更新

您可以排程自動更新所有代理程式上的保護定義，或是手動在所選代理程式上更新。

若要排程自動更新

1. 在 Cyber Protect Web 主控台中，移至 **[設定]** > **[保護]** > **[保護定義更新]**。
2. 選擇 **[排程]**。

3. 在 **[排程類型]** 中，選擇下列其中一項：
   - **每日**

     選擇在一週的哪幾天更新保護定義。

     在 **[開始時間]** 中，選擇更新開始的時間。
   - **每小時**

     為更新設定細微排程。

     在 **[執行週期]** 中，設定更新的週期。

     在 **[開始]** 中...在 **[結束]** 中，為更新設定特定的時間範圍。

若要手動更新保護定義

1. 在 Cyber Protect Web 主控台中，移至 **[設定]** > **[代理程式]**。
2. 選擇您要對其代理程式更新保護定義所在的電腦，然後按一下 **[更新定義]**。

變更下載位置

保護定義會先下載到電腦上的預設暫存資料夾中，然後再儲存到 Acronis 程式資料夾中。

若要變更用於下載的預設資料夾

1. 在管理伺服器電腦上，開啟 `atp-database-mirror.json` 檔案進行編輯。

   您可以在下列位置找到此檔案：
   - Windows：`%programdata%\Acronis\AtpDatabaseMirror\`
   - Linux：`/var/lib/Acronis/AtpDatabaseMirror/`
2. 將 `"enable_user_config"` 的值變更為 `true`。

   ```
   {
   "sysconfig":
   {
   ...
   "enable_user_config": true
   }
   ...
   }
   ```
3. 在管理伺服器電腦上，開啟 `config.json` 檔案進行編輯。

   您可以在下列位置找到此檔案：
   - Windows：`%programdata%\Acronis\AtpDatabaseMirror\`
   - Linux：`/var/lib/Acronis/AtpDatabaseMirror/`
4. 新增下行：`"mirror_temp_dir": "<path_to_new_download_location>"`

   例如：

   ```
   {
           "mirror_temp_dir":"C:\\temp"
   }
   ```

路徑可以是 AppData 資料夾的絕對路徑或相對路徑。
如果無法建立資料夾，或管理伺服器無法寫入資料夾，將會使用預設位置。

快取儲存選項

快取的資料儲存在下列位置：

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

您可以設定排程來清除過期的快取資料，並設定其大小的限制。您可以針對含非更新程式代理程式的電腦以及含更新程式代理程式的電腦，設定不同的限制。

最新保護定義的來源

您可以從下列位置下載最新的保護定義：

- **雲端**
  保護代理程式會連線到網際網路，然後從 Acronis Cloud 下載最新的保護定義。根據預設，在管理伺服器上註冊的所有代理程式都會檢查更新並加以散佈。如需有關具有 [更新者] 角色之代理程式的詳細資訊，請參閱 "更新保護定義" (第 538 頁)。
- **Cyber Protect Management Server**
  選擇此選項時，代理程式不需要存取網際網路。它們只要連線到儲存保護定義所在的管理伺服器即可。但是，管理伺服器必須連線到網際網路，才能下載最新的保護定義。
- **自訂 Web 伺服器**
  此選項適用於疑難排解和測試用途，或用於氣隙環境。如需詳細資訊，請參閱 "在氣隙環境中更新保護定義" (第 542 頁)。通常只有在 Acronis 支援團隊指示時，您才需要選擇此選項。

遠端連線

啟用遠端連線時，**[透過 RDP 用戶端連線]** 和 **[透過 HTML5 用戶端連線]** 選項會出現在 Cyber Protect Web 主控台中，右側功能表的 **[網路保護桌面]** 底下。當您在 **[裝置]** 索引標籤上選擇工作負載時，右側功能表隨即開啟。

啟用或停用遠端連線會影響貴組織的所有使用者。

若要啟用遠端連線

1. 在 Cyber Protect Web 主控台中，移至 **[設定]** > **[保護]**。
2. 按一下 **[遠端連線]**，然後啟用 **[遠端桌面連線]** 開關。

此外，您可以啟用遠端連線共用。您可以透過此選項，產生一個允許從遠端存取所選工作負載的連結。您可以與其他使用者共用這些連結。

若要啟用遠端連線共用

1. 在 Cyber Protect Web 主控台中，移至 **[設定]** > **[保護]**。
2. 選擇 **[共用遠端桌面連線]** 核取方塊。

結果，**[共用遠端連線]** 選項將會出現在 Cyber Protect Web 主控台中，右側功能表的 **[網路保護桌面]** 底下。

在氣隙環境中更新保護定義

Acronis Cyber Protect 支援在氣隙環境中更新保護定義。

若要在氣隙環境中更新保護定義

1. 在您的氣隙環境外，安裝另一部可存取網際網路的管理伺服器。
   如需有關操作方式的詳細資訊，請參閱 "安裝管理伺服器" (第 74 頁)。
2. 將保護定義從線上管理伺服器複製到卸除式磁碟機，然後將定義轉移到氣隙環境中的 HTTP 伺服器。
   如需有關此步驟的詳細資訊，請參閱 "將定義下載到線上管理伺服器" (第 542 頁) 和 "將定義轉移到 HTTP 伺服器" (第 543 頁)。
3. 在氣隙管理伺服器上，將HTTP 伺服器設定為更新的保護定義來源。
   如需有關此步驟的詳細資訊，請參閱 "在氣隙管理伺服器上設定定義來源" (第 544 頁)。

將定義下載到線上管理伺服器

安裝可以存取網際網路的另一個管理伺服器之後，下載最新的保護定義，並將其複製到卸除式磁碟機，例如 USB 快閃記憶體或外接式硬碟。

若要下載並複製保護定義

1. 在具有線上管理伺服器的電腦上，將 `AtpDatabaseMirror` 資料夾複製到您選擇的位置，例如桌面或 `Temp` 資料夾。
   您可以在下列位置找到 `AtpDatabaseMirror` 資料夾：
   - Windows：`%ProgramData%\Acronis\`
   - Linux：`/usr/lib/Acronis/`
2. 開啟 `atp_database_mirror.json` 檔案進行編輯。您可以在下列位置找到此檔案：
   - Windows：`%Program Files%\Acronis\AtpDatabaseMirror`

     注意事項
     在 Windows 中，此資料夾與上一個步驟中的資料夾不同。

   - Linux：`/usr/lib/Acronis/AppDatabaseMonitor`
3. 編輯 `atp_database_mirror.json` 檔案，如下所示：
   a. 將 `"enable_appdata_as_root"` 的值變更為 `false`。
   b. 將 `"local_path"` 所有項目的值變更為您要儲存保護定義所在位置的絕對路徑。
4. 將變更儲存在 `atp_database_mirror.json` 檔案中。
5. 在具有線上管理伺服器的電腦上，使用下列命令停止 **Acronis Management Server** 服務：

- Windows (命令提示字元):

```
sc stop AcrMngSrv
```

- Linux (終端機):

```
sudo systemctl stop acronis_ams.service
```

6. 在您複製到所選位置的 AtpDatabaseMirror 資料夾中，使用下列命令啟動 AtpDatabaseMirror 工具：
   - Windows (命令提示字元):

```
atp_database_mirror.exe -config atp_database_mirror.json
```

   - Linux (終端機):

```
sudo ./atp_database_mirror -config atp_database_mirror.json
```

   當所有更新都下載到您在 "local_path" 中指定的資料夾時，下行會出現在 [命令提示字元] 或 [終端機] 視窗中：

```
standing by for 1m0s
```

7. 按下 CTRL+C，停止 AtpDatabaseMirror 工具。
8. 將此檔案從您在 "local_path" 中指定的資料夾複製到卸除式磁碟機。

接下來，您必須將檔案從卸除式磁碟機複製到您氣隙環境中的 HTTP 伺服器。您可以使用氣隙管理伺服器作為 HTTP 伺服器。如需詳細資訊，請參閱 "將定義轉移到 HTTP 伺服器" (第 543 頁)。

將定義轉移到 HTTP 伺服器

若要在氣隙環境中散佈保護定義，您需要專用的 HTTP 伺服器。您可以使用氣隙管理伺服器作為 HTTP 伺服器。

若要將保護定義轉移到 HTTP 伺服器

1. 在您將執行 HTTP 伺服器所在的電腦上，將保護定義複製到您選擇的資料夾。
2. 從您複製保護定義所在的資料夾，啟動 HTTP 伺服器。
   例如，您可以使用 Python 並執行下列命令：

```
python -m http.server 8080
```

   注意事項
   您可以使用您慣用的任何 HTTP 伺服器。

3. 從您複製保護定義所在的資料夾，開啟下列 update-index.json 檔案進行編輯：
   - ./ngmp/update-index.json
   - ./vapm/update-index.json

4. 在兩個 update-index.json 檔案中，編輯所有 products > os > arch > components > versions > url 欄位，如下所示：
   a. 在 [IP] 和 [連接埠] 值中，設定 HTTP 伺服器的 IP 位址和連接埠。
   b. 請不要變更路徑的其他部分。
   例如，"url": "http://192.168.1.10:8080/ngmp/win64/ngmp.zip"，其中 192.168.1.10 是 HTTP 伺服器的 IP 位址，8080 是其連接埠。請不要變更 /ngmp/win64/ngmp.zip 部分。
5. 在兩個 update-index.json 檔案中儲存您所做的編輯。

接下來，您必須在氣隙管理伺服器上設定保護定義的來源。如需詳細資訊，請參閱 "在氣隙管理伺服器上設定定義來源" (第 544 頁)。

在氣隙管理伺服器上設定定義來源

設定 HTTP 伺服器之後，您必須在氣隙管理伺服器上設定該伺服器，作為保護定義的來源。

若要在氣隙管理伺服器上設定保護定義來源

1. 在氣隙管理伺服器的 Cyber Protect Web 主控台中，移至 **[設定]** > **[保護]** > **[保護定義更新]**。
2. 選擇 **[定義]**。
3. 選擇 **[自訂]**，然後指定下列路徑：

- 若是**防毒和反惡意程式碼定義**：
  `http://<IP address of your HTTP server>:8080/scanner`
- 若是**進階偵測定義**：
  `http://<IP address of your HTTP server>:8080/ngmp`
- 若是**弱點評估和修補程式管理定義**：
  `http://<IP address of your HTTP server>:8080/vapm`

因此，氣隙環境中的代理程式將會從您的 HTTP 伺服器下載保護定義。

管理使用者帳戶與組織單位

內部部署

此區段中所述的功能，僅限組織管理員使用。

若要存取這些設定，按一下 **[設定]** > **[帳戶]**。

單位與系統管理帳戶

若要管理單位與系統管理帳戶，請在 Cyber Protect Web 主控台中，移至 **[設定]** > **[帳戶]**。**[帳戶]** 面板會顯示 **[組織]** 群組，且包含單位的樹狀結構 (如果有的話)，以及在所選階層層級的系統管理帳戶清單。

單位

當您安裝管理伺服器時，將自動建立**組織**群組。使用 Acronis Cyber Protect 進階授權，您可以建立稱為單位的子群組，這些群組通常會對應到組織的單位或部門，且可以新增系統管理帳戶到單位。如此一來，您就可以委派保護管理給其存取權限被嚴格限制為相對應單位的其他人員。如需有關如何建立單位的資訊，請參閱 "建立單位" (第 548 頁)。

每個單位都可以有子單位。上層單位的系統管理帳戶在所有子單位中都有相同權限。**[組織]** 群組是最上層的上層單位，而且此層級的系統管理帳戶在其所有單位中都有相同權限。

系統管理帳戶

可以登入 Cyber Protect Web 主控台的任何帳戶都是系統管理帳戶。

在 Cyber Protect Web 主控台中，任何系統管理帳戶皆可檢視或管理此單位階層層級或以下的任何事項。例如，*組織*中的系統管理帳戶擁有此最高層級的存取權，因此也擁由此組織所有單位的存取權，而特定*單位*中的系統管理帳戶則只擁有此單位及其子單位的存取權。

哪些帳戶可以是系統管理帳戶?

如果管理伺服器是安裝在包含於 Active Directory 網域的 Windows 機器內，您可將系統管理權限授予本機使用者，或是 Active Directory 網域樹系內的使用者和使用者群組。

依預設，管理伺服器會與 Active Directory 網域控制站建立受 SSL/TLS 保護的連線。如果這是不可能的，則不會建立任何連線。但是，您可以透過編輯 `auth-connector.json5` 檔案來允許不安全的連線。

若要使用安全連線，請確認已針對 Active Directory 設定 LDAP over SSL (LDAPS)。

若要針對 Active Directory 設定 LDAP

1. 在網域控制站上，建立並安裝符合 Microsoft 需求的 LDAP 憑證。
   如需有關如何執行這些作業的詳細資訊，請參閱 Microsoft 文件中的透過第三方認證機構啟用 LDAP over SSL。

2. 在網域控制站上，開啟 **Microsoft Management Console**，並在 **[憑證 (本機電腦)]** > **[個人]** > **[憑證]** 底下確認憑證存在。
3. 重新啟動網域控制站。
4. 確認已啟用 LDAP。

若要允許至網域控制站的不安全連線

1. 登入安裝管理伺服器的電腦。
2. 開啟 `auth-connector.json5` 檔案進行編輯。

   `auth-connector.json5` 檔案位於 `%APPDATA%\Acronis\AuthConnector` 中。
3. 瀏覽至 **[sync]** 區段，並在每個 **"connectionMode"** 行中，將 **"ssl_only"** 取代為 **"auto"**。

   在 **auto** 模式中，如果無法建立 TLS 連線，則會建立不安全連線。
4. 如所述，重新啟動 **Acronis Service Manager 服務**。

注意事項
如果管理伺服器不包含於 Active Directory 網域中，或者如果是安裝在 Linux 電腦上，則您只能將系統管理權限授予本機使用者或群組。

若要瞭解如何新增系統管理帳戶至管理伺服器，請參閱 "新增系統管理帳戶" (第 548 頁)。

系統管理帳戶角色

每個系統管理帳戶皆獲指派一個角色，該角色具備特定工作所必需的預先定義權限。系統管理帳戶角色如下：

- **系統管理員**
  此角色提供對組織或單位的完整系統管理存取權。
- **唯讀**
  此角色提供對 Cyber Protect Web 主控台的唯讀存取權。其僅允許收集系統報告之類的診斷資料。唯讀角色不允許瀏覽備份或瀏覽備份信箱的內容。
- **稽核員**
  此角色提供對 Cyber Protect Web 主控台中 **[活動]** 索引標籤的唯讀存取權。如需有關此索引標籤的詳細資訊，請參閱 "活動索引標籤" (第 501 頁)。此角色不允許收集或匯出任何資料，包括管理伺服器的系統資訊。

此角色的任何變更都會顯示在 **[活動]** 索引標籤上。

角色的繼承

上層單位中的角色會由其子單位所繼承。如果在上層單位和子單位中相同的使用者帳戶獲指派不同的角色，則該帳戶將有兩個角色。

此外，角色可以明確地指派給特定使用者帳戶，也可以從使用者群組繼承。因此，使用者帳戶可以同時擁有一個專門指派的角色和一個繼承的角色。

如果某個使用者帳戶有不同的角色 (獲指派和/或繼承), 則可以存取物件並執行其中任何角色所允許的動作。例如, 如果某個使用者帳戶同時擁有獲指派的唯讀角色以及繼承的系統管理員角色, 則將擁有系統管理員權限。

重要事項
在 Cyber Protect Web 主控台中, 只會顯示針對目前單位明確地指派的角色。與繼承角色的任何可能差異均不會顯示。強烈建議您將系統管理員角色、唯讀和稽核員角色指派給不同的帳戶或群組, 才能避免繼承角色可能會發生的問題。

預設系統管理員

在 Windows 中

當在機器上安裝管理伺服器時, 會發生以下情況:

- 在該機器上建立**Acronis Centralized Admins** 使用者群組。
  在網域控制器上, 群組的名稱為 *DCNAME* **$ Acronis Centralized Admins**。在這裡, *DCNAME* 代表網域控制器的 NetBIOS 名稱。
- **Administrators** 群組的所有成員都會被新增到**Acronis Centralized Admins** 群組。如果電腦位於非網域控制站的網域中, 則會排除本機l (非網域) 使用者。在網域控制站上, 沒有非網域使用者。
- **Acronis Centralized Admins** 與 **Administrators** 群組將被新增到管理伺服器, 並成為**組織系統管理員**。如果電腦位於非網域控制站的網域中, 則不會新增 **[系統管理員]** 群組, 如此一來, 本機 (非網域) 使用者就不會變成組織系統管理員。

您可以從組織管理員的清單中刪除**管理員**群組。然而, 無法刪除 **AcronisCentralized Admins**。在罕見的情況下, 如果所有組織系統管理員都已經遭到刪除, 您可以將帳戶新增到 Windows 中的 **Acronis Centralized Admins** 群組, 然後再使用此帳戶登入 Cyber Protect Web 主控台。

在 Linux 中

當管理伺服器安裝在電腦上時, **root** 使用者會作為**組織管理員**新增至管理伺服器。

如稍後部分中所述, 您可以將其他 Linux 使用者新增至管理伺服器系統管理員清單中, 然後從此清單中刪除 **root** 使用者。在罕見的情況下, 若所有組織系統管理員都已遭到刪除, 您可以重新啟動 `acronis_asm` 服務。因此, **root** 使用者將會自動再次新增為組織管理員。

多個單位中的系統管理帳戶

一個帳戶可獲授予任何數量的單位中的系統管理權限。針對此類帳戶, 以及組織層級的組織系統管理帳戶, Cyber ProtectWeb 主控台上會顯示單位選擇器。透過使用此選擇器, 此帳戶可以個別地檢視及管理每個單位。

對組織內所有單位都有權限的帳戶, 對組織沒有權限。必須以明確的方式, 將組織層級的系統管理帳戶新增到**組織**群組。

如何使用機器來部署單位

當管理員透過網頁界面來新增機器時，機器將新增到受管理員管理的單位。如果管理員管理多個單位，則機器將新增到在單位選擇器中所選擇的單位。因此，管理員必須在按一下**新增**前選擇單位。

當在本機安裝代理程式時，管理員必須提供其認證。機器將新增到受管理員管理的單位。如果管理員管理多個單位，安裝程式會提示選擇要新增機器的單位。

新增系統管理帳戶

注意事項
Standard 和 Essentials 版本中不提供此功能。

若要新增帳戶

1. 按一下 **[設定]** > **[帳戶]**。
   軟體將顯示管理伺服器管理員的清單，以及單位的樹狀結構(若有)。
2. 選擇**[組織]**，或選擇您想要新增管理員的單位。
3. 按一下 **[新增帳戶]**。
4. 在**[網域]**中，選擇包含您想要新增的使用者帳號的網域。若管理伺服器未包含在 Active Directory 網域，或安裝在 Linux 中，則只能新增本機使用者。
5. 搜尋使用者名稱或使用者群組名稱。
6. 按一下位於使用者或群組名稱旁的 "+"。
7. 選擇帳戶的角色。
8. 針對您要新增的所有使用者或群組，重複步驟 4-6。
9. 完成後，按一下 **[完成]**。
10. [僅在 Linux 中] 新增使用者名稱至 Acronis 模組的插入式驗證模組 (PAM) 組態，如下所述。

若要新增使用者名稱至 Acronis 的 PAM 組態

此程序適用於 Linux 電腦上與 Acronis Cyber Protect 多合一裝置中執行的管理伺服器。

1. 在執行管理伺服器的電腦上，以 root 使用者身分使用文字編輯器開啟檔案 **/etc/security/acronisagent.conf**。
2. 在此檔案中，鍵入您新增作為管理伺服器系統管理員的使用者名稱，一行一個。
3. 儲存並關閉檔案。

建立單位

1. 按一下 **[設定]** > **[帳戶]**。
2. 軟體將顯示管理伺服器管理員的清單，以及單位的樹狀結構(若有)。
3. 選取 **[組織]**，或者選取新單位的上層單位。
4. 按一下 **[建立單位]**。
5. 指定新單位的名稱，然後按一下 **[建立]**。

雲端部署

可在管理入口網站中管理使用者帳戶與組織單位。若要存取管理入口網站，請在登入 Cyber Protection 服務時按一下 **[管理入口網站]**，或按一下右上角的  圖示，然後按一下 **[管理入口網站]**。僅具有管理專用權的使用者才能存取此入口網站。

如需管理使用者帳戶和組織單位的相關資訊，請參閱《管理入口網站系統管理員指南》。若要存取此文件，請在管理入口網站中按一下問號圖示。

本節提供與管理網路保護服務相關的其他資訊。

配額

配額可讓您限制使用者使用服務的能力。若要設定配額，選擇 **[使用者]** 標籤上的使用者，然後按一下 **[配額]** 區段中的鉛筆圖示。

超過配額時，系統會發送一則通知到使用者的電子郵件地址。若未設定配額超額，則該配額會視為「軟」。這意味著不會套用使用網路保護服務的限制。

您還可以指定配額超額。超額可允許使用者超過指定值的配額。超過超額時，會套用使用網路保護服務的限制。

備份

您可已指定雲端儲存空間配額、本機備份配額，以及允許使用者保護的電腦/裝置/信箱數量上限。您可以選擇下列配額：

- **雲端儲存**
- **工作站**
- **伺服器**
- **Windows Server Essentials**
- **虛擬主機**
- **通用**

  此配額可用來代替以上所列四個配額中的任一個：工作站、伺服器、Windows Server Essentials、虛擬主機。
- **行動裝置**
- **Microsoft 365 信箱**
- **本機備份**

只要至少套用了一個保護計劃，電腦/裝置/信箱就會被視為受到保護。第一次備份後，行動裝置將變成受保護狀態。

當超過雲端儲存空間配額超額時，備份則無法成功執行。當超過一些裝置的超額時，使用者無法將保護計劃套用至更多裝置。

[本機備份] 配額會限制使用雲端基礎架構建立的本機備份大小總計。無法針對此配額設定超額。

災難復原

這些配額是由服務供應商套用到整個公司的。公司系統管理員可在管理入口網站中檢視配額和使用狀況，但無法為使用者設定配額。

- **災難復原儲存空間**

  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，或新增/延伸現有主要伺服器的磁碟。如果超過此配額的超額，則無法啟動容錯移轉，或只啟動已停止的伺服器。執行中的伺服器會繼續執行。

  當配額已停用時，會刪除所有伺服器。Web 主控台上已經沒有 **[雲端復原網站]** 索引標籤。
- **計算點**

  此配額會限制主要伺服器和復原伺服器在計費期間消耗的 CPU 和 RAM 資源。如果達到此配額的超額，則會關閉所有主要伺服器和復原伺服器。除非下一個計費期間開始，否則不能使用這些伺服器。預設的計費期間為一個完整曆月。

  當配額遭到停用時，不論計費期間，都無法使用伺服器。
- **公共 IP 位址**

  此配額會限制可指派給主要伺服器和復原伺服器的公共 IP 位址數量。如果達到此配額的超額，則無法為更多伺服器啟用公共 IP 位址。您可以透過清除伺服器設定中的 **[公共 IP 位址]** 核取方塊，禁止某個伺服器使用公共 IP 位址。然後，您可以允許其他伺服器使用公共 IP 位址，這通常不會是同一個位址。

  當配額遭到停用時，使用公共 IP 位址的所有伺服器都會停止，因此會變成無法從網際網路連線。
- **雲端伺服器**

  此配額會限制主要伺服器和復原伺服器的總數。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。

  當此配額遭到停用時，伺服器會顯示在 Cyber Protect Web 主控台中，但是唯一可行的操作是 **[刪除]**。
- **網際網路存取**

  此配額會啟用或停用從主要伺服器和復原伺服器的網際網路存取。

  當此配額停用時，主要伺服器和復原伺服器會立即與網際網路中斷連線。伺服器屬性內的 **[網際網路存取]** 開關會清除且停用。

通知

若要變更使用者的通知設定，選擇 **[使用者]** 標籤上的使用者，然後按一下**[設定]** 區段中的鉛筆圖示。您可以選擇下列通知設定：

- **配額過度使用通知** (預設為啟用)

  已超出配額的相關通知
- **已排程的使用報告**

  在每個月的第一天傳送的下述使用報告。
- **失敗通知**、**警告通知**和**成功通知** (預設為啟用)

關於每個裝置的保護計劃執行結果以及災難復原作業結果的通知。

- **作用中警示的相關每日摘要** (預設為啟用)

  摘要會通知失敗的備份、遺漏的備份與其他問題。摘要將於 10:00 傳送(資料中心時間)。若此時沒有出現任何問題,則不會傳送摘要。

所有通知將傳送至使用者的電子郵件地址。

報告

使用網路保護服務的相關報告包含下列關於組織或單位的資料:

- 依照單位、使用者、裝置類型分類的備份大小。
- 依照單位、使用者、裝置類型分類之受保護裝置的數量。
- 依照單位、使用者、裝置類型分類的價格。
- 備份大小總計。
- 受保護裝置的總數。
- 總價。

命令列參考

命令列介面是一個獨立文件，可在 https://www.acronis.com/en-us/support/documentation/AcronisCyberProtect_15_Command_Line_Reference/index.html 上取得。

疑難排解

本節說明如何將代理程式記錄檔儲存為 .zip 檔。如果因不明原因備份失敗，此檔案可幫助技術支援人員判別問題所在。

收集記錄檔

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電腦，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電腦，然後按一下 **[詳細資料]**。
2. 按一下 **[收集系統資訊]**。
3. 如果 Web 瀏覽器出現提示，請指定要儲存檔案的位置。

辭彙表

S

Startup Recovery Manager

位於系統磁碟上的可開機代理程式經過修改，且已設定為在開機過程中按下 F11 時啟動。Startup Recovery Manager 不需要救援媒體或網路連線，即可啟動可開機救援公用程式。Startup Recovery Manager 特別適用於行動使用者。如果發生故障，使用者可重新啟動電腦，在出現 [按 F11 執行 Startup Recovery Manager...] 提示時按 F11，就能以與使用普通可開機媒體相同的方法執行資料復原。限制：需要重新啟用除 Windows 載入器和 GRUB 以外的載入器。

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。

受

受管理的位置

由儲存節點管理的備份位置。實際上，受管理的位置可位於網路共用、SAN、NAS 上、儲存節點的本機硬碟上或儲存節點本機連接的磁帶庫中。儲存節點會為存放在受管理位置中的每一個備份執行清理與驗證 (如果這些包含在保護計劃中)。您可指定儲存節點將執行的其他作業 (重複資料刪除、加密)。

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。

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]、[每日]、[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]) 選擇的星期幾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

新的備份格式，會將初始完整備份及後續增量備份儲存為單一的 .tib 檔案，而不是一長串的檔案。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 (例如，SFTP 伺服器) 時，無法使用單一檔案備份格式。

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。

索引

W

一

工

已

不

什

仍

允

元

內

公

伺

位

何

作

刪

即

快

我

更

步

每

計

重

限

修

哪

容

弱

效

核

格

缺

記

退

配

惡

提

智

最

減

測

無

登

發

等

結

虛