

網路保護

22.04



目錄

1 Cyber Protection 服務版本和子版本	17
1.0.1 Cyber Protect 版本	17
1.0.2 Cyber Backup 版本	17
1.0.3 版本比較	17
1.0.4 災難復原附加元件	18
2 作業系統支援的 Cyber Protect 功能。	19
3 軟體需求	25
3.1 支援的網頁瀏覽器	25
3.2 支援的作業系統和環境	25
3.2.1 Windows 用代理程式	25
3.2.2 SQL 用代理程式、Active Directory 用代理程式、Exchange 用代理程式 (適用於資料庫備份及應用程式感知備份)	26
3.2.3 資料洩漏防禦用代理程式	26
3.2.4 File Sync & Share 用代理程式	26
3.2.5 Exchange 用代理程式 (適用於信箱備份)	26
3.2.6 Microsoft 365 用代理程式	27
3.2.7 適用於 Oracle 的代理程式	27
3.2.8 MySQL/MariaDB 用代理程式	27
3.2.9 Linux 用代理程式	27
3.2.10 Mac 用代理程式	28
3.2.11 VMware 用代理程式 (虛擬裝置)	29
3.2.12 VMware 用代理程式 (Windows)	29
3.2.13 Hyper-V 用代理程式	29
3.2.14 Virtuozzo 用代理程式	29
3.2.15 Virtuozzo Hybrid Infrastructure 用代理程式	29
3.2.16 Scale Computing HC3 用代理程式	30
3.2.17 oVirt 用代理程式	30
3.2.18 Cyber Protect 監視器	30
3.3 支援的 Microsoft SQL Server 版本	30
3.4 支援的 Microsoft Exchange Server 版本	30
3.5 支援的 Microsoft SharePoint 版本	30
3.6 受支援的 Oracle 資料庫版本	31
3.7 支援的 SAP HANA 版本	31
3.8 支援的 MySQL 版本	31
3.9 支援的 MariaDB 版本	31

3.10 支援的虛擬化平台	31
3.10.1 限制	35
3.11 與加密軟體的相容性	36
3.11.1 一般安裝規則	37
3.11.2 使用 Secure Zone 的方法	37
3.11.3 一般備份規則	37
3.11.4 軟體特定的復原程序	37
4 支援的檔案系統	38
4.0.1 重複資料刪除	39
5 啟用帳戶	40
5.1 雙重驗證機制	40
5.1.1 假如...	41
6 存取 Cyber Protection 服務	42
7 安裝軟體	43
7.1 我需要哪種代理程式?	43
7.2 代理程式的系統需求	45
7.3 準備	46
7.3.1 步驟 1	46
7.3.2 步驟 2	46
7.3.3 步驟 3	46
7.3.4 步驟 4	47
7.3.5 步驟 5	47
7.3.6 步驟 6	48
7.4 Linux 套件	48
7.4.1 所需的套件是否已安裝?	49
7.4.2 從存放庫安裝套件	49
7.4.3 手動安裝套件	50
7.5 Proxy 伺服器設定	51
7.5.1 在 Windows 中	51
7.5.2 在 Linux 中	52
7.5.3 在 macOS 中	53
7.5.4 在可開機媒體中	54
7.6 安裝 Cyber Protection 代理程式	54
7.6.1 下載 Cyber Protection 代理程式	55
7.6.2 在 Windows 中安裝 Cyber Protection 代理程式	55
7.6.3 在 Linux 中安裝 Cyber Protection 代理程式	56
7.6.4 在 macOS 中安裝 Cyber Protection 代理程式	58

7.6.5 變更 Windows 電腦上的登入帳戶	59
7.6.6 動態安裝與解除安裝元件	60
7.7 自動安裝或解除安裝	61
7.7.1 Windows 中的自動安裝或解除安裝	61
7.7.2 Linux 中的自動安裝或解除安裝	67
7.7.3 在 macOS 中自動安裝和解除安裝	72
7.8 手動註冊電腦	74
7.8.1 包含特殊字元或空格的密碼	77
7.9 自動探索電腦	77
7.9.1 必要條件	78
7.9.2 自動探索運作方式	78
7.9.3 遠端安裝代理程式的運作方式	80
7.9.4 自動探索和手動探索	80
7.9.5 管理探索到的電腦	84
7.9.6 疑難排解	85
7.10 部署 VMware 用代理程式 (虛擬裝置)	86
7.10.1 在您開始之前	86
7.10.2 部署 OVF 範本	86
7.10.3 設定虛擬裝置	87
7.11 正在部署 Scale Computing HC3 用代理程式 (虛擬裝置)	88
7.11.1 在您開始之前	88
7.11.2 部署 QCOW2 範本	89
7.11.3 設定虛擬裝置	90
7.11.4 Scale Computing HC3 用代理程式 – 必要角色	91
7.12 部署 Virtuozzo Hybrid Infrastructure 用代理程式 (虛擬裝置)	92
7.12.1 在您開始之前	92
7.12.2 在 Virtuozzo Hybrid Infrastructure 中設定網路	93
7.12.3 在 Virtuozzo Hybrid Infrastructure 中設定使用者帳戶	93
7.12.4 部署 QCOW2 範本	96
7.12.5 設定虛擬裝置	96
7.13 正在部署 oVirt 用代理程式 (虛擬裝置)	100
7.13.1 在您開始之前	100
7.13.2 部署 OVA 範本	101
7.13.3 設定虛擬裝置	102
7.13.4 oVirt 用代理程式 – 所需角色和連接埠	104
7.14 透過群組原則部署代理程式	104
7.14.1 必要條件	104

7.14.2 步驟 1:產生註冊權杖	105
7.14.3 步驟 2:建立 .mst 轉換和解壓縮安裝套件	106
7.14.4 步驟 3:設定群組原則物件	106
7.15 更新代理程式	107
7.15.1 手動更新代理程式	107
7.15.2 自動更新代理程式	109
7.16 防止未經授權者解除安裝或修改代理程式	110
7.17 解除安裝代理程式	111
7.17.1 在 Windows 中	111
7.17.2 在 Linux 中	112
7.17.3 在 macOS 中	112
7.17.4 移除 VMware 用代理程式 (虛擬裝置)	112
7.17.5 從服務主控台移除電腦	112
7.18 保護設定	113
7.18.1 元件自動更新	113
7.18.2 依排程更新 Cyber Protection 定義	114
7.18.3 視需要更新 Cyber Protection 定義	114
7.18.4 快取儲存空間	114
7.18.5 遠端連線	114
7.19 變更電腦的服務配額	115
7.20 安裝在您環境中的 Cyber Protection 服務	116
7.20.1 安裝在 Windows 中的服務	116
7.20.2 安裝在 macOS 中的服務	116
8 服務主控台	117
9 管理工作負載	120
9.1 各 Device 群組	120
9.1.1 內建群組	120
9.1.2 自訂群組	120
9.1.3 建立靜態群組	121
9.1.4 新增裝置到靜態群組	121
9.1.5 建立動態群組	121
9.1.6 將保護計劃套用到群組	127
10 多租用戶支援	128
11 保護計劃和模組	129
11.1 建立保護計劃	129
11.2 預設保護計劃	130
11.2.1 預設計劃選項	131

11.3 解決計劃衝突	134
11.3.1 將數個計劃套用至一個裝置	134
11.3.2 解決計劃衝突	134
11.4 具有保護計劃的作業	135
12 電腦的 #CyberFit 分數	137
12.1 運作原理	137
12.1.1 #CyberFit 評分機制	137
12.2 執行 #CyberFit 分數掃描	140
13 備份與復原	142
13.1 備份	142
13.2 保護計劃速查表	143
13.3 選擇要備份的資料	145
13.3.1 選擇整部機器	145
13.3.2 選擇磁碟/磁碟區	146
13.3.3 選擇檔案/資料夾	148
13.3.4 選擇系統狀態	150
13.3.5 選擇 ESXi 設定	150
13.4 連續資料保護 (CDP)	151
13.4.1 運作原理	151
13.4.2 支援的資料來源	153
13.4.3 支援的目的地	153
13.4.4 設定 CDP 備份	154
13.5 選擇目的地	155
13.5.1 進階儲存選項	155
13.5.2 關於 Secure Zone	156
13.6 排程	159
13.6.1 備份配置	159
13.6.2 其他排程選項	160
13.6.3 依據事件排程	161
13.6.4 開始條件	163
13.7 保留規則	168
13.7.1 您需要知道的其他事項	169
13.8 複寫	169
13.8.1 使用範例	169
13.8.2 支援的位置	170
13.9 加密	171
13.9.1 保護計劃中的加密	171

13.9.2 以電腦屬性加密	171
13.9.3 加密如何運作	172
13.10 公證	173
13.10.1 如何使用公證	173
13.10.2 運作原理	173
13.11 手動啟動備份	173
13.12 預設備份選項	174
13.13 備份選項	174
13.13.1 備份選項的可用性	174
13.13.2 警示	177
13.13.3 備份合併	177
13.13.4 備份檔案名稱	178
13.13.5 備份格式	181
13.13.6 備份驗證	182
13.13.7 變更區塊追蹤 (CBT)	183
13.13.8 叢集備份模式	183
13.13.9 壓縮層級	184
13.13.10 錯誤處理	185
13.13.11 快速增量/差異備份	186
13.13.12 檔案篩選器	186
13.13.13 檔案層級備份快照	187
13.13.14 鑑識資料	188
13.13.15 記錄截斷	196
13.13.16 LVM 快照	196
13.13.17 掛載點	197
13.13.18 多重磁碟區快照 (M)	197
13.13.19 效能和備份時窗	198
13.13.20 實體資料運送	200
13.13.21 事前/事後命令	202
13.13.22 資料擷取前/後命令	203
13.13.23 排程	205
13.13.24 逐一磁區備份	206
13.13.25 分割	206
13.13.26 工作失敗處理	207
13.13.27 工作開始條件	207
13.13.28 磁碟區陰影複製服務 (VSS)	207
13.13.29 虛擬機器的磁碟區陰影複製服務 (VSS)	208

13.13.30 每週備份	209
13.13.31 Windows 事件日誌	209
13.14 復原	209
13.14.1 復原快速鍵清單	209
13.14.2 安全復原	211
13.14.3 復原電腦	212
13.14.4 準備驅動程式	220
13.14.5 檢查是否能在可開機環境中存取驅動程式	220
13.14.6 驅動程式自動搜尋	220
13.14.7 仍要安裝的大型存放驅動程式	221
13.14.8 復原檔案	222
13.14.9 復原系統狀態	227
13.14.10 復原 ESXi 設定	227
13.14.11 復原選項	228
13.15 備份的相關作業	234
13.15.1 備份儲存索引標籤	234
13.15.2 從備份掛載磁碟區	236
13.15.3 驗證備份	237
13.15.4 匯出備份	238
13.15.5 刪除備份	238
13.16 保護 Microsoft 應用程式	240
13.16.1 保護 Microsoft SQL Server 和 Microsoft Exchange Server	240
13.16.2 保護 Microsoft SharePoint	240
13.16.3 保護網域控制站	240
13.16.4 復原應用程式	240
13.16.5 必要條件	241
13.16.6 資料庫備份	243
13.16.7 應用程式感知備份	248
13.16.8 信箱備份	249
13.16.9 復原 SQL 資料庫	251
13.16.10 復原 Exchange 資料庫	253
13.16.11 復原 Exchange 信箱和信箱項目	255
13.16.12 變更 SQL Server 或 Exchange Server 存取認證	261
13.17 保護行動裝置	261
13.17.1 支援的行動裝置	261
13.17.2 可備份的內容	261
13.17.3 須知事項	262

13.17.4 何處取得 Cyber Protect 應用程式	262
13.17.5 如何開始備份資料	262
13.17.6 如何將資料復原至行動裝置	263
13.17.7 如何透過服務主控台檢閱資料	263
13.18 保護託管的 Exchange 資料	264
13.18.1 哪些項目可以備份?	264
13.18.2 可以復原哪些項目?	265
13.18.3 選取信箱	265
13.18.4 復原信箱和信箱項目	266
13.19 保護 Microsoft 365 資料	268
13.19.1 為什麼要備份 Microsoft 365 資料?	268
13.19.2 Microsoft 365 用代理程式	268
13.19.3 限制	269
13.19.4 所需的使用者權限	270
13.19.5 Microsoft 365 授權報告	270
13.19.6 使用本機安裝的 Office 365 用代理程式	270
13.19.7 使用雲端 Microsoft 365 用代理程式	273
13.20 保護 Google Workspace 資料	293
13.20.1 Google Workspace 保護是什麼意思?	293
13.20.2 所需的使用者權限	293
13.20.3 關於備份排程	293
13.20.4 限制	293
13.20.5 新增 Google Workspace 組織	294
13.20.6 建立個人 Google Cloud 專案	294
13.20.7 保護 Gmail 資料	297
13.20.8 保護 Google 雲端硬碟檔案	301
13.20.9 保護共用磁碟機檔案	304
13.20.10 公證	307
13.21 保護 Oracle 資料庫	308
13.22 保護 SAP HANA	308
13.23 保護 MySQL 和 MariaDB 資料	309
13.23.1 設定應用程式感知備份	310
13.23.2 從應用程式感知備份復原資料	310
13.24 保護網站和託管伺服器	314
13.24.1 保護網站	314
13.24.2 保護 Web 託管伺服器	317
13.25 虛擬機器的特殊作業	317

13.25.1 從備份執行虛擬機器(立即復原)	317
13.25.2 於 VMware vSphere 中進行作業	321
13.25.3 備份叢集 Hyper-V 虛擬機器	337
13.25.4 限制同時備份的虛擬機器總數。	337
13.25.5 電腦移轉	338
13.25.6 Microsoft Azure 和 Amazon EC2 虛擬機器	340
14 災難復原	341
14.1 關於 Cyber Disaster Recovery Cloud	341
14.1.1 主要功能	341
14.2 軟體需求	341
14.2.1 支援的作業系統	341
14.2.2 支援的虛擬化平台	342
14.2.3 限制	342
14.3 Cyber Disaster Recovery Cloud 試用版產品	343
14.4 計算點	343
14.5 設定災難復原功能	344
14.6 建立災難復原保護計劃	345
14.6.1 編輯復原伺服器預設參數	346
14.6.2 雲端網路基礎架構	347
14.7 設定連線	347
14.7.1 網路概念	347
14.7.2 初始連線設定	357
14.7.3 必要條件	359
14.7.4 網路管理	364
14.7.5 必要條件	376
14.8 設定復原伺服器	377
14.8.1 建立復原伺服器	377
14.8.2 容錯移轉的運作方式	379
14.8.3 容錯回復的運作方式	383
14.8.4 使用加密備份	388
14.8.5 使用 Microsoft Azure 虛擬機器進行操作	389
14.9 設定主要伺服器	389
14.9.1 建立主要伺服器	389
14.9.2 主要伺服器的操作	391
14.10 管理雲端伺服器	391
14.11 雲端伺服器的防火牆規則	392
14.11.1 設定雲端伺服器的防火牆規則	393

14.11.2 檢查雲端防火牆活動	395
14.12 備份雲端伺服器	395
14.13 編排 (Runbook)	396
14.13.1 為什麼使用 Runbook?	396
14.13.2 建立 Runbook	396
14.13.3 Runbook 的相關作業	398
15 反惡意程式碼和 Web 保護	400
15.1 防毒和反惡意程式碼保護	400
15.1.1 反惡意程式碼功能	400
15.1.2 反惡意程式碼功能	400
15.1.3 掃描類型	400
15.1.4 防毒和反惡意程式碼保護設定	401
15.2 Cyber Backup Standard 版本中的 Active Protection	411
15.2.1 Cyber Backup Standard 中的 Active Protection 設定	411
15.3 URL 篩選	415
15.3.1 運作原理	415
15.3.2 URL 篩選設定工作流程	417
15.3.3 URL 篩選設定	417
15.4 Microsoft Defender 防毒軟體與 Microsoft Security Essentials	422
15.4.1 排程掃描	422
15.4.2 預設動作	423
15.4.3 即時保護	423
15.4.4 進階	424
15.4.5 排除	424
15.5 隔離	424
15.5.1 檔案如何進入隔離資料夾?	425
15.5.2 管理隔離的檔案	425
15.5.3 電腦上的隔離位置	425
15.6 隨選自助服務自訂資料夾	426
15.7 公司白名單	426
15.7.1 自動新增至白名單	426
15.7.2 手動新增至白名單	426
15.7.3 將隔離的檔案新增到白名單	427
15.7.4 白名單設定	427
15.7.5 檢視白名單中關於項目的詳細資料	427
15.8 備份的反惡意程式碼掃描	427
15.8.1 如何在雲端設定備份掃描	428

16 進階保護	429
16.1 進階版資料洩漏防禦	429
16.1.1 建立資料流程原則和原則規則	429
16.1.2 在保護計劃中啟用進階版資料洩漏防禦	437
16.1.3 自動偵測目的地	440
16.1.4 敏感資料定義	440
16.1.5 資料洩漏防禦事件	445
16.1.6 概觀儀表板上的進階版資料洩漏防禦桌面小工具	447
17 協同作業和通訊應用程式的保護	448
18 弱點評估和修補程式管理	449
18.1 弱點評估	449
18.1.1 支援的 Microsoft 和第三方產品	449
18.1.2 支援的 Apple 和協力廠商產品	451
18.1.3 支援的 Linux 產品	451
18.1.4 弱點評估設定	452
18.1.5 適用於 Windows 電腦的弱點評估	453
18.1.6 Linux 電腦的弱點評估	453
18.1.7 適用於 macOS 裝置的弱點評估	454
18.1.8 管理找到的弱點	454
18.2 修補程式管理	455
18.2.1 運作原理	456
18.2.2 修補程式管理設定	457
18.2.3 管理修補程式清單	459
18.2.4 自動核准修補程式	460
18.2.5 手動核准修補程式	463
18.2.6 按需修補程式安裝	463
18.2.7 清單中的修補程式存留時間	464
19 軟體清查	465
19.1 啟用軟體清查掃描	465
19.2 手動執行軟體清查掃描	465
19.3 瀏覽軟體清查	466
19.4 檢視單一裝置的軟體清查	468
20 硬體清查	469
20.1 啟用硬體清查掃描	469
20.2 手動執行硬體清查掃描	470
20.3 瀏覽硬體清查	470
20.4 檢視單一裝置的硬體	472

21 遠端桌面存取	474
21.1 遠端存取 (RDP 和 HTML5 用戶端)	474
21.1.1 運作原理	475
21.1.2 如何連線至遠端電腦	475
21.1.3 如何執行遠端協助工作階段	476
21.2 與使用者共用遠端連線	476
22 遠端抹除	478
23 智慧型保護	479
23.1 威脅饋送	479
23.1.1 運作原理	479
23.1.2 刪除所有警示	481
23.2 資料保護圖	482
23.2.1 運作原理	482
23.2.2 管理偵測到的未受保護檔案	482
23.2.3 資料保護圖設定	482
24 加強安全性模式	485
24.1 限制	485
24.2 設定加密密碼	485
24.3 變更加密密碼	486
24.4 復原備份	486
25 不可變動儲存空間	487
25.1 限制	487
25.2 啟用和停用固定儲存空間	487
25.3 存取固定儲存空間中已刪除的備份	488
26 裝置控制	489
26.0.1 使用資料洩漏防禦用代理程式搭配 Hyper-V 的限制	490
26.1 使用裝置控制	491
26.1.1 啟用或停用裝置控制	491
26.1.2 在 macOS 上啟用裝置控制模組	491
26.1.3 檢視或變更存取設定	493
26.1.4 從存取控制排除裝置子類別	494
26.1.5 從存取控制排除個別 USB 裝置	494
26.1.6 檢視裝置控制警示	496
26.2 存取設定	496
26.2.1 作業系統通知和服務警示	500
26.3 裝置類型允許名單	500
26.4 USB 裝置允許名單	502

26.4.1 USB 裝置資料庫	503
26.5 從存取控制排除程序	505
26.6 裝置控制警示	507
26.6.1 動作欄位值	508
27 [管理] 索引標籤	510
27.1 保護計劃	510
27.2 雲端應用程式的備份計劃	511
27.3 備份掃描計劃	511
27.3.1 限制	511
27.4 脫離主機資料處理	512
27.4.1 備份複寫	512
27.4.2 驗證	513
27.4.3 清理	515
27.4.4 轉換為虛擬機器	516
28 Cyber Protect 監視器	520
29 可開機媒體	521
29.1 自訂或現成的可開機媒體?	521
29.2 Linux 型或 WinPE/WinRE 型可開機媒體?	521
29.2.1 Linux	521
29.2.2 WinPE/WinRE 型	521
29.3 建立實體可開機媒體	522
29.4 可開機媒體組建	522
29.4.1 為什麼要使用 Bootable Media Builder?	522
29.4.2 32 位元或 64 位元?	523
29.4.3 Linux 可開機媒體	523
29.4.4 最上層物件	527
29.4.5 變數物件	527
29.4.6 控制類型	528
29.4.7 WinPE 型和 WinRE 型可開機媒體	530
29.4.8 註冊可開機媒體	533
29.4.9 網路設定	534
29.5 連線到從可開機媒體開機的電腦	534
29.5.1 本機連線	534
29.5.2 進行網路設定	535
29.6 可開機媒體的相關作業	535
29.6.1 設定顯示模式	536
29.6.2 復原	536

29.7 Startup Recovery Manager	536
30 監控	538
30.1 概觀儀表板	538
30.2 [活動] 儀表板	539
30.3 網路保護	539
30.4 保護狀態	540
30.4.1 探索到的電腦	540
30.5 依電腦分類的 #CyberFit 分數	541
30.6 磁碟健全狀況監控	541
30.6.1 運作原理	542
30.6.2 磁碟健全狀況桌面小工具	543
30.6.3 磁碟健全狀況狀態警示	545
30.7 資料保護圖	545
30.8 弱點評估桌面小工具	546
30.8.1 易受攻擊的電腦	546
30.8.2 現有的弱點	547
30.9 修補程式安裝桌面小工具	547
30.9.1 修補程式安裝狀態	547
30.9.2 修補程式安裝摘要	548
30.9.3 修補程式安裝歷史記錄	548
30.9.4 遺漏的更新 (依類別)	548
30.10 備份掃描詳細資料	549
30.11 最近受影響	549
30.11.1 下載最近受影響工作負載的資料	550
30.12 雲端應用程式	550
30.13 軟體清查桌面小工具	551
30.14 硬體清查桌面小工具	552
31 報告	554
31.0.1 新增報告	555
31.0.2 編輯報告	555
31.0.3 排程報告	556
31.0.4 匯出和匯入報告結構	557
31.0.5 下載報告	557
31.0.6 傾印報告資料	557
31.1 根據桌面小工具類型回報的資料	557
32 內部部署管理伺服器的授權管理	560
33 疑難排解	561

34 附錄 A. 站台對站台 OpenVPN - 其他資訊	562
辭彙表	569
索引	573

1 Cyber Protection 服務版本和子版本

重要事項

本主題包含舊版授權模型的相關資訊。如果您不使用這些版本作為舊版設定的一部分，請略過此資訊。

本節包含使用隨 Acronis Cyber Cloud 21.02 和更舊版本中授權模型提供的服務、版本和產品項目。這些產品項目和版本仍然受到支援，而且可以視需要，為租用用戶設定，但是不建議，現在已被視為舊版。

注意事項

可提供給您的服務、版本和產品項目繼承自適用於您父租用用戶的產品項目。如果某個產品項目不適用於建立您帳戶的合作夥伴，該產品項目將無法供您使用，而且您無法為您的合作夥伴或客戶啟用該產品項目。

如需新產品項目的相關資訊，請參閱 "進階保護" (第 429 頁)。

提供下列版本：

- Cyber Protect
- Cyber Backup

1.0.1 Cyber Protect 版本

此版本按工作負載授權，亦即，根據受保護電腦的數目，而不考慮備份資料的大小。

在 Cyber Protect 版本中，提供下列子版本：

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

1.0.2 Cyber Backup 版本

此版本按 GB 授權，亦即，根據備份資料的大小，而不考慮受保護電腦的數目。

在 Cyber Backup 版本中，沒有子版本，僅提供 Cyber Backup Standard 產品項目。

1.0.3 版本比較

可用功能的數量和範圍取決於 Cyber Protection 服務的版本。如需每個版本和子版本的功能間的詳細比較，請參閱[比較 Acronis Cyber Protection 版本](#)。

1.0.4 災難復原附加元件

Disaster Recovery 附加元件提供專為對復原時間目標 (RTO) 有高要求的公司而設計的復原功能。此附加元件只能搭配 Cyber Protect 版本使用。

注意事項

Disaster Recovery 附加元件無法搭配 Cyber Protect Essentials 子版本使用。

2 作業系統支援的 Cyber Protect 功能。

注意事項

本主題包含所有 Cyber Protect 功能以及支援這些功能的作業系統的相關資訊。部分功能可能需要額外的授權，端視適用的授權模型而定。

下列作業系統支援 Cyber Protect 功能：

- Windows: Windows 7 Service Pack 1 和更新版本、Windows Server 2008 R2 Service Pack 1 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 6.10、7.8+、CloudLinux 6.10、7.8+、Ubuntu 16.04.7+，其中加號指的是這些發行版本的次要版本。

其他 Linux 發行版和版本可能會受到支援，但尚未經過測試。

- macOS: 10.13.x 和更新版本 (僅支援防毒和反惡意程式碼保護，以及裝置控制)。macOS 10.15 和更新版本或 macOS 11.2.3 和更新版本支援裝置控制功能。

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

注意事項

只有在啟用 [進階反惡意程式碼保護] 時，才支援適用於 Linux 和 macOS 的反惡意程式碼保護。

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、Virtuozzo Hybrid Infrastructure 用代理程式、Scale Computing 用代理程式或 oVirt 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
預設保護計劃			
遠端工作者	是	否	否
辦公室工作者 (第三方防毒軟體)	是	否	否
辦公室工作者 (Cyber Protect 防毒軟體)	是	否	否
Cyber Protect Essentials (僅適用於 Cyber Protect Essentials 版本)	是	否	否
鑑識備份			
收集記憶體傾印	是	否	否
執行中程序的快照	是	否	否

Cyber Protect 功能	Windows	Linux	macOS
公證本機映像鑑識備份	是	否	否
公證雲端映像鑑識備份	是	否	否
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
Active Protection			
程序插入偵測	是	否	否
從本機快取自動復原受影響的檔案	是	是	是
Acronis 備份檔案的自我防衛	是	否	否
Acronis 軟體的自我防衛	是	否	是 (僅限 Active Protection 和防惡意程式碼元件)
受信任/遭到封鎖的程序管理	是	否	是
程序/資料夾排除	是	是	是
根據程序行為 (基於 AI) 進行勒索軟體偵測	是	否	否
根據程序行為進行加密採礦程序偵測	是	否	否
外接磁碟機保護 (HDD、快閃磁碟機、SD 卡)	是	否	是
網路資料夾保護	是	是	是
伺服器端保護	是	否	否
Zoom、Cisco Webex、Citrix Workspace 和 Microsoft Teams 保護	是	否	否
防毒和反惡意程式碼保護			

Cyber Protect 功能	Windows	Linux	macOS
完全整合的 Active Protection 功能	是	否	否
即時反惡意軟體防護	是	是, 啟用 [進階反惡意程式碼] 時	是, 啟用 [進階反惡意程式碼] 時
包含本機特徵比對偵測的進階即時反惡意程式碼保護	是	是	是
針對可攜式可執行檔進行靜態分析	是	否	是*
按需反惡意程式碼掃描	是	是**	是
網路資料夾保護	是	是	否
伺服器端保護	是	否	否
掃描存檔檔案	是	否	是
掃描卸除式磁碟機	是	否	是
僅掃描新的和已變更的檔案	是	否	是
檔案/資料夾排除	是	是 否	是***
程序排除	是	否	否
行為分析引擎	是	否	是 在 Apple Silicon 處理器 (例如 Apple M1) 上不支援
預防利用	是	否	否
隔離	是	是	是
隔離區自動清理	是	否	是
URL 篩選 (http/https)	是	否	否
全公司的白名單	是	否	是
Microsoft Defender 防毒軟體管理	是	否	否
Microsoft Security Essentials 管理	是	否	否
透過 Windows Security Center 註冊並管理防毒和反惡意程式碼保護	是	否	否
弱點評估			
作業系統及其原生應用程式的弱點評估	是	是****	是

Cyber Protect 功能	Windows	Linux	macOS
適用於協力廠商應用程式的弱點評估	是	否	是
修補程式管理			
修補程式自動核准	是	否	否
修補程式自動安裝	是	否	否
修補程式測試	是	否	否
修補程式手動安裝	是	否	否
修補程式排程	是	否	否
故障移轉修補: 安裝修補程式作為保護計劃一部分之前備份電腦	是	否	否
如果備份正在執行, 則取消電腦重新開機	是	否	否
資料保護圖			
可調整的重要檔案定義	是	否	否
掃描電腦以尋找未受保護的檔案	是	否	否
未受保護的位置概觀	是	否	否
能夠從資料保護圖桌面小工具啟動保護動作 ([保護所有檔案] 動作)	是	否	否
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			
映像備份的反惡意程式碼掃描是備份計劃的一部分	是	否	否
掃描雲端的映像備份中是否有惡意程式碼	是	否	否
加密備份的惡意程式碼掃描	是	否	否
安全復原			
在復原過程中, 使用防毒和反惡意程式	是	否	否

Cyber Protect 功能	Windows	Linux	macOS
碼保進行反惡意程式碼掃描			
加密備份的安全復原	是	否	否
遠端桌面連線			
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
遠端協助	是	否	否
#CyberFit 分數			
#CyberFit 分數狀態	是	否	否
#CyberFit 分數獨立工具	是	否	否
#CyberFit 分數建議	是	否	否
資料洩漏防禦			
裝置控制	是	否	是 不支援 ARM CPU 架構
管理選項			
宣傳 Cyber Protect 版本的追加銷售案例	是	是	是
網頁型集中式與遠端管理主控台	是	是	是
保護選項			
遠端抹除 (僅限 Windows10)	是	否	否
Cyber Protect Monitor			
Cyber Protect 監視器應用程式	是	否	是
Zoom 的保護狀態	是	否	否
Cisco Webex 的保護狀態	是	否	否
Citrix Workspace 的保護狀態	是	否	否
Microsoft Teams 的保護狀態	是	否	否
軟體清查			
軟體清查掃描	是	否	是
軟體清查監視	是	否	是

Cyber Protect 功能	Windows	Linux	macOS
硬體清查			
硬體清查掃描	是	否	是
硬體清查監視	是	否	是

* 只有在 macOS 上的排程掃描才支援針對可攜式可執行檔進行靜態分析。

** Linux 上的按需掃描不支援開始條件。

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

**** 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。

3 軟體需求

3.1 支援的網頁瀏覽器

Cyber Protection Web 主控台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
- 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。

3.2 支援的作業系統和環境

3.2.1 Windows 用代理程式

此代理程式包括用於防毒及防惡意程式碼保護和 URL 篩選的元件。有關作業系統支援的功能的詳細資訊, 請參閱 "作業系統支援的 Cyber Protect 功能。" (第 19 頁)。

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

注意事項

若要搭配 Windows 7 使用 Cyber Protection, 您必須安裝以下 Microsoft 更新, 然後再安裝 Cyber Protection 代理程式：

- [Windows 7 Extended Security Updates \(ESU\)](#)
- [KB4474419](#)
- [KB4490628](#)

有關所需更新的詳細資訊, 請參閱[本知識庫文章](#)。

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

- Windows Server 2012/2012 R2 – 所有版本
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 – Home、Pro、Education、Enterprise、IoT Enterprise 以及 LTSC (前身為 LTSB) 版
- Windows Server 2016 – 所有安裝選項，Nano Server 除外
- Windows Server 2019 – 所有安裝選項，Nano Server 除外
- Windows 11 – 所有版本
- Windows Server 2022 – 所有安裝選項，Nano Server 除外

注意事項

* 若要搭配此版本的 Windows 使用 Cyber Protection，必須在安裝代理程式之前，先從 Microsoft 安裝 SHA2 程式碼簽署支援更新 ([KB4474419](#))。

如需有關與 SHA2 程式碼簽署支援更新相關的資訊，請參閱這篇[知識庫文章](#)。

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

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

3.2.3 資料洩漏防禦用代理程式

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

注意事項

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

注意事項

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

3.2.4 File Sync & Share 用代理程式

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

3.2.5 Exchange 用代理程式 (適用於信箱備份)

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

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

3.2.6 Microsoft 365 用代理程式

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

3.2.7 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)

3.2.8 MySQL/MariaDB 用代理程式

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

3.2.9 Linux 用代理程式

此代理程式包括用於防毒及防惡意程式碼保護和 URL 篩選的元件。有關作業系統支援的功能的詳細資訊, 請參閱 "作業系統支援的 Cyber Protect 功能。" (第 19 頁)。

重要事項

在核心版本 4.17 和更新版本上, 不支援 Active Protection 和即時保護。

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 Cyber Protection 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步調查。

使用 2.6.9 到 5.16 核心程序及 2.3.4 或更高版本 Linux，包括以下 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*
- 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
- 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*
- CentOS Stream 8
- Oracle Linux 5.x、6.x、7.x、8.0、8.1、8.2、8.3、8.4* – 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*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*
- AlmaLinux 8.4*
- 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`

* 僅支援 4.18 到 5.16 之間的核心

3.2.10 Mac 用代理程式

此代理程式包括用於防毒及防惡意程式碼保護和 URL 篩選的元件。有關作業系統支援的功能的詳細資訊，請參閱 "作業系統支援的 Cyber Protect 功能。" (第 19 頁)。

支援 x64 和 ARM 架構 (用於 Apple Silicon 處理器，例如 Apple M1)*。

- 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

* 反惡意程式碼保護、硬體清查以及軟體清查在搭載 Apple Silicon 處理器的 Mac 上都需要使用 Rosetta 2。

3.2.11 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

3.2.12 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。

3.2.13 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 – 所有安裝選項, Nano Server 除外

3.2.14 Virtuozzo 用代理程式

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

3.2.15 Virtuozzo Hybrid Infrastructure 用代理程式

Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5

3.2.16 Scale Computing HC3 用代理程式

Scale Computing Hypercore 8.8, 8.9, 9.0

3.2.17 oVirt 用代理程式

Red Hat Virtualization 4.2, 4.3, 4.4

3.2.18 Cyber Protect 監視器

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

3.3 支援的 Microsoft SQL Server 版本

- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

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

3.4 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。

3.5 支援的 Microsoft SharePoint 版本

Cyber Protection 支援下列 Microsoft SharePoint 版本：

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1

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

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

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

3.6 受支援的 Oracle 資料庫版本

- Oracle 資料庫 11g 版，所有版本
- Oracle Database 12c 版，所有版本

僅支援單個執行個體組態。

3.7 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。

3.8 支援的 MySQL 版本

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

3.9 支援的 MariaDB 版本

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

3.10 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 Cyber Protection 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 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 Workstation VMware ACE VMware Player		+
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, 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Scale Computing		
Scale Computing Hypercore 8.8, 8.9, 9.0	+	+
Citrix		
Citrix XenServer/Citrix Hypervisor 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 8.0, 8.1,		僅限完全虛擬化 (亦即 HVM) 的客體。不支援半虛擬化 (亦即

8.2		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	+	+
核心虛擬機器 (KVM)		+
由 Red Hat Enterprise Linux 7.6、7.7 或 CentOS 7.6、7.7 上執行的 oVirt 4.3 所管理的核心虛擬機器 (KVM)	+	+
由 Red Hat Enterprise Linux 8.x 或 CentOS Stream 8.x 上執行的 oVirt 4.4 所管理的核心虛擬機器 (KVM)	+	+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle Virtualization Manager (以 oVirt 為基礎)*** 4.3	+	+
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		
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		
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。

***Oracle Virtualization Manager 受到 [oVirt 用代理程式](#) 的支援。

3.10.1 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：

- 從 Virtuozzo 進行的 P2V 移轉、V2P 移轉，以及 V2V 移轉。使用 Linux 用代理程式建立要復原的備份和可開機媒體。
- 從 Linux 用代理程式建立的備份執行虛擬機器。

- **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 虛擬機器：(在 VMware vSphere 6.5 中推出) 虛擬機器復原為新的虛擬機器後，會停用**安全開機**。完成復原後，可手動啟用此選項。此限制適用於 VMware。
- Hyper-V 虛擬機器：針對所有 GEN2 VM，[安全開機] 會在虛擬機器復原為新的虛擬機器或現有的虛擬機器之後遭到停用。

- VMware vSphere 7.0 不支援 **ESXi 設定備份**。

3.11 與加密軟體的相容性

透過檔案層級加密軟體加密的資料無備份和復原限制。

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

您可對採用以下磁碟層級加密軟體加密的資料進行備份：

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

若要確保可靠的磁碟層級復原，請遵循一般規則和特定軟體的建議。

3.11.1 一般安裝規則

強烈建議先安裝加密軟體，再安裝保護代理程式。

3.11.2 使用 Secure Zone 的方法

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

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

3.11.3 一般備份規則

您可以在作業系統中執行磁碟層級備份。

3.11.4 軟體特定的復原程序

Microsoft BitLocker 磁碟機加密

復原由 BitLocker 加密的系統：

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

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

McAfee 端點加密和 PGP 全磁碟機加密

您只能使用可開機媒體復原加密的系統磁碟分割。

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

<https://support.microsoft.com/kb/2622803>

4 支援的檔案系統

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

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

檔案系統	支援			限制
	代理程式	Windows 和 Linux 可開機媒體	Mac 可開機媒體	
FAT16/32	所有代理程式	+	+	無限制
NTFS		+	+	
ext2/ext3/ext4		+	-	
HFS+	Mac 用代理程式	-	+	- 支援從 Mac OS High Sierra 10.13 開始 - 復原至非原始電腦或裸機時，應手動重新建立磁碟組態。
APFS		-	+	
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		+	-	
ReFS	所有代理程式	+	+	- 無法從磁碟備份中排除檔案 - 無法啟用快速增量/差異備份 - 復原期間無法調整磁碟區大小
XFS		+	+	
Linux swap	Linux 用代理程式	+	-	無限制
exFAT	所有代理程式	+ 如果備份是儲存在 exFAT 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 (例如 Btrfs) 的磁碟機時, 軟體會自動切換至「逐一磁區」模式。以下任何檔案系統均可進行逐一磁區備份:

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

如果檔案系統不符合這些要求, 備份便會失敗。

4.0.1 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。

5 啟用帳戶

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

- **您的登入。**這是您用來登入的使用者名稱。您的登入也會顯示在帳戶啟用頁面上。
- **帳戶啟用按鈕。**按一下該按鈕，然後設定帳戶的密碼。請確保密碼長度至少 9 個字元。

如果您的系統管理原已經啟用雙重驗證機制，系統將會提示您[為帳戶設定雙重驗證機制](#)。

5.1 雙重驗證機制

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

為您的帳戶設定雙重身份驗證的一次性代碼是根據裝置的目前時間和 Cyber Protection 服務提供的密碼，而產生 QR 碼或字母數字代碼。在首次登入期間，您必須將此密碼輸入到驗證應用程式中。

若要為您的帳戶設定雙重驗證機制

當您的組織管理員已啟用雙重身份驗證時，您可以也必須為您的帳戶設定雙重身份驗證。如果在登入 Cyber Protection 服務主控台時啟用了雙重身份驗證，則必須在目前工作階段過期時對其進行設定。

必要條件：

- 已為您的組織啟用雙重身份驗證。
- 已將您登出 Cyber Protection 服務主控台。

1. 選擇第二要素裝置。

最常見的是行動電話，但是您也可以使用平板電腦、筆記型電腦或桌上型電腦。

2. 確保裝置時間設定正確，並反映目前的實際時間，確保裝置在一段時間不用後自行鎖定。

3. 在裝置上安裝驗證應用程式。建議的應用程式為 Google Authenticator 或 Microsoft Authenticator。

4. 前往 Cyber Protection 服務主控台登入頁面並設定密碼。

服務主控台會顯示 QR 碼和英數字代碼。

5. 以任何便利的方式儲存 QR 碼和英數字代碼(例如，印出畫面、寫下代碼，或在雲端儲存空間儲存螢幕擷取畫面)。如果您遺失第二要素裝置，您將可以使用這些代碼，重設雙重驗證機制。

6. 開啟驗證應用程式，然後執行下列其中一項操作：

- 掃描 QR 碼
- 將英數字代碼手動輸入到應用程式中

驗證應用程式會產生一個一次性代碼。每 30 秒鐘將會產生一個新代碼。

7. 返回服務主控台登入頁面，然後輸入所產生的代碼。

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

下次登入時，您可以選取 **[信任此瀏覽器...]** 核取方塊。如果您這麼做，當您在這部電腦上使用此瀏覽器登入時，將不需要一次性代碼。

5.1.1 假如...

...我遺失了第二要素裝置？

如果您有信任的瀏覽器，您將能夠使用此瀏覽器登入。但是，當您有新的裝置時，請使用新裝置和已儲存的 QA 碼或英數字代碼，重複上述程序的步驟 1-3 和 6-7。

如果您還未儲存該代碼，請要求系統管理員或服務供應商為您的帳戶重設雙重驗證機制，然後使用新裝置重複上述程序的步驟 1-3 和 6-7。

...我想要變更第二要素裝置？

登入時，按一下 **[重設雙重驗證機制設定]** 連結、輸入一次性代碼以確認操作，然後使用新裝置重複上述程序。

6 存取 Cyber Protection 服務

如果您已啟用帳戶，則可登入 Cyber Protection 服務。

若要登入 **Cyber Protection** 服務

1. 請移至 Cyber Protection 服務登入頁面。
2. 輸入登入，然後按一下 **[下一步]**。
3. 輸入密碼，然後按一下 **[下一步]**。
4. 如果您在 Cyber Protection 服務中擁有系統管理員角色，請按一下 **[網路保護]**。
不具備系統管理員角色的使用者會直接登入服務主控台。

服務主控台的逾時期限對於作用中工作階段而言為 24 小時，對於閒置工作階段而言則為 1 小時。

重設密碼

1. 請移至 Cyber Protection 服務登入頁面。
2. 輸入登入，然後按一下 **[下一步]**。
3. 按一下 **[忘記密碼?]**
4. 按一下 **[傳送]**，確認您需要進一步的指示。
5. 依照您收到的電子郵件中的指示進行。
6. 設定您的新密碼。請確保密碼長度至少 8 個字元。

您可以按一下右上角的帳戶圖示，以變更 Web 介面的語言。

如果 **[網路保護]** 不是您訂閱的唯一服務，可以切換服務，方法是，使用右上角的  圖示。系統管理員也可以使用此圖示切換到管理入口網站。

如果您已訂閱任何 Cyber Protection 版本，可以從服務主控台傳送有關產品的意見反應。在左導覽功能表中，按一下 **[傳送意見反應]**、填寫欄位、附加檔案 (如果有的話)，然後按一下 **[傳送]**。

7 安裝軟體

7.1 我需要哪種代理程式？

選擇代理程式，視您要備份的內容而定。下表摘要說明可協助您做出決定的資訊。

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

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

在 Linux 中，Oracle 用代理程式和 Virtuozzo 用代理程式需要也安裝 Linux 用代理程式 (64 位元)。這三個代理程式共用一個安裝程式。

您要備份什麼內容？	要安裝哪一個代理程式？	要安裝在哪裡？
實體機器		
執行 Windows 的實體機器	Windows 用代理程式	在將進行備份的機器上。
執行 Linux 的實體機器	Linux 用代理程式	
執行 macOS 的實體機器	Mac 用代理程式	
應用程式		
SQL 資料庫	SQL 用代理程式	在執行 Microsoft SQL Server 的電腦上。
MySQL 資料庫	MySQL/MariaDB 用代理程式	在執行 MySQL Server 的電腦上。
MariaDB 資料庫	MySQL/MariaDB 用代理程式	在執行 MariaDB Server 的電腦上。
Exchange 資料庫	Exchange 用代理程式	在執行 Microsoft Exchange Server 信箱角色的電腦上。*
Microsoft 365 信箱	Microsoft 365 用代理程式	在已連線至網際網路的 Windows 電腦上。 視所需的功能而定，您不一定需要安裝 Microsoft 365 用代理程式。如需詳細資訊，請參閱「 保護 Microsoft 365 資料 」。
Microsoft 365 OneDrive 檔案和 SharePoint Online 網站	—	只有雲端上安裝的代理程式才能備份此資料。如需詳細資訊，請參閱「 保護 Microsoft 365 資料 」。
Google Workspace Gmail 信	—	只有雲端上安裝的代理程式才能備份此資料。如需

箱、Google 雲端硬碟檔案和共用磁碟機檔案		詳細資訊，請參閱「 保護 Google Workspace 」。
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 (虛擬裝置)	在 Scale Computing HC3 主機上。
Red Hat Virtualization 虛擬機器 (受 oVirt 管理)	oVirt 用代理程式 (虛擬裝置)	在 Red Hat Virtualization 主機上。
Virtuozzo 虛擬機器和容器 ***	Virtuozzo 用代理程式	在 Virtuozzo 主機上。
Virtuozzo Hybrid Infrastructure 虛擬機器	Virtuozzo Hybrid Infrastructure 用代理程式	在 Virtuozzo Hybrid Infrastructure 主機上。
裝載於 Amazon EC2 主機上的虛擬機器	與實體機器相同 *****	在將進行備份的機器上。
裝載於 Windows Azure 主機上的虛擬機器		
Citrix XenServer 虛擬機器		
Red Hat Virtualization (RHV/RHEV)		
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。如需詳細指示，請參閱「VMware 用代理程式 - 不透過 LAN 備份」。

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

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

7.2 代理程式的系統需求

代理程式	安裝所需的磁碟空間
Windows 用代理程式	1.2 GB
Linux 用代理程式	2 GB
Mac 用代理程式	1 GB
SQL 用代理程式和 Windows 用代理程式	1.2 GB
Exchange 用代理程式和 Windows 用代理程式	1.3 GB
資料洩漏防禦用代理程式	500 MB
Microsoft 365 用代理程式	500 MB
Active Directory 用代理程式和 Windows 用代理程式	2 GB
VMware 用代理程式和 Windows 用代理程式	1.5 GB
Hyper-V 用代理程式和 Windows 用代理程式	1.5 GB
Virtuozzo 用代理程式和 Linux 用代理程式	1 GB
Virtuozzo Hybrid Infrastructure 用代理程式	700 MB
Oracle 用代理程式和 Windows 用代理程式	2.2 GB

Oracle 用代理程式和 Linux 用代理程式	2 GB
MySQL/MariaDB 用代理程式和 Linux 用代理程式	2 GB

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

注意事項

備份到超大的備份集 (4 TB 以上) 時, 可能會進一步增加 RAM 使用量。

可開機媒體或重新啟動以進行磁碟復原, 需至少 1 GB 的記憶體。

7.3 準備

7.3.1 步驟 1

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

7.3.2 步驟 2

請確認您的硬碟上有足夠的可用空間, 才能安裝代理程式。如需有關所需空間的詳細資訊, 請參閱"代理程式的系統需求" (第 45 頁)。

7.3.3 步驟 3

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

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

若要在本機儲存安裝程式, 請使用 **[新增裝置]** 頁面底部的連結, 下載包含在 Windows 中安裝之所有代理程式的套件。提供 32 位元和 64 位元套件。這些套件可讓您自訂要安裝的元件清單。這些套件也可讓您進行自動安裝, 例如透過群組原則。〈透過群組原則部署代理程式〉中已說明此進階情況。

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

Linux 和 macOS 中的安裝是從一般安裝程式執行。

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

7.3.4 步驟 4

Cyber Protect 功能需要使用 Microsoft Visual C++ 2017 可轉散發套件。請確認已在電腦上安裝該可轉散發套件，或在安裝代理程式前加以安裝。安裝 Microsoft Visual C++ 後，可能需要重新啟動。您可以在以下網址找到 Microsoft Visual C++ 可轉散發套

件：<https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows>。

7.3.5 步驟 5

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

- **443** 和 **8443** 這些連接埠用於存取服務主控台、註冊代理程式、下載憑證、使用者授權，以及從雲端儲存下載檔案。
- **7770...7800** 代理程式使用這些連接埠與備份管理伺服器進行通訊。
- **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](#)」一節，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

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

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

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

Downloader 元件所需的連接埠

Downloader 元件負責將更新提供給電腦，並將其分配給其他 Downloader 執行個體。它可以代理程式模式下執行，在此模式下，其電腦能夠變成 Downloader 代理程式。Downloader 代理程式會從

網際網路下載更新，並作為將更新分配給其他電腦的來源。Downloader 需要使用下列連接埠才能運作。

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

7.3.6 步驟 6

在您打算安裝網路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。

變更網路保護代理程式所使用的連接埠

網路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，變更網路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\aaakore.yaml

7.4 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。

7.4.1 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。

7.4.2 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	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。

	elfutils-libelf-devel	
	perl	執行下列命令： <pre>yum install perl</pre>
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： <pre>yum install perl</pre>
Ubuntu Debian	linux-headers linux-image gcc make perl	執行以下命令： <pre>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</pre>
SUSE Linux OpenSUSE	kernel-source gcc make perl	<pre>sudo zypper install kernel-source sudo zypper install gcc sudo zypper install make sudo zypper install perl</pre>

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。

7.4.3 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。

7.5 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。

7.5.1 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 登錄編輯程式 5.00 版

[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。
9. 在文字編輯器中開啟檔案 **%programdata%\Acronis\Agent\etc\aaakore.yaml**。
10. 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
```

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

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

14. 使用下列命令，重新啟動代理程式：

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

7.5.2 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="Tdwor" >"1"</value>
  <value name="Host" type="TString">"位址"</value>
  <value name="Port" type="Tdwor" >"連接埠"</value>
  <value name="Login" type="TString">"登入"</value>
  <value name="Password" type="TString">"密碼"</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. 在文字編輯器中開啟檔案 **/opt/acronis/etc/aakore.yaml**。
 7. 找出 **env** 區段，或建立該區段並加入下列幾行：

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

8. 將 proxy_login 和 proxy_password 取代為 Proxy 伺服器認證，並將 proxy_address:port 取代為 Proxy 伺服器的位址和連接埠號碼。
 9. 使用下列命令，重新啟動 aakore 服務：
- ```
sudo service aakore restart
```
10. 在任意目錄中執行下列命令以重新啟動代理程式：

```
sudo service acronis_mms restart
```

## 7.5.3 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. 複製以下幾行並貼到檔案中

```
<?xml version="1.0" ?>
<registry name="Global">
```

```
<key name="HttpProxy">
 <value name="Enabled" type="Tdword">"1"</value>
 <value name="Host" type="TString">"proxy.company.com"</value>
 <value name="Port" type="Tdword">"443"</value>
 <value name="Login" type="TString">"proxy_login"</value>
 <value name="Password" type="TString">"proxy_password"</value>
</key>
</registry>
```

3. 將 proxy.company.com 取代為您的 Proxy 伺服器主機名稱/IP 位址，並將 443 取代為連接埠號碼的十進位值。
4. 如果您的 Proxy 伺服器需要驗證，請將 proxy\_login 和 proxy\_password 取代為 Proxy 伺服器認證。否則，請從檔案中刪除這幾行。
5. 儲存檔案。
6. 如果尚未安裝保護代理程式，您可以現在安裝。
7. 在文字編輯器中開啟檔案 **/Library/Application Support/Acronis/Agent/etc/aakore.yaml**。
8. 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
```

9. 將 proxy\_login 和 proxy\_password 取代為 Proxy 伺服器認證，並將 proxy\_address:port 取代為 Proxy 伺服器的位址和連接埠號碼。
10. 前往 **[應用程式]>[公用程式]>[終端機]**
11. 使用下列命令，重新啟動 aakore 服務：

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

12. 使用下列命令，重新啟動代理程式：

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

## 7.5.4 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。

## 7.6 安裝 Cyber Protection 代理程式

您可以在執行「[支援的作業系統和環境](#)」中所列任何作業系統的電腦上安裝代理程式。支援 Cyber Protect 功能的作業系統列在「[作業系統支援的 Cyber Protect 功能](#)」中。

## 7.6.1 下載 Cyber Protection 代理程式

安裝代理程式之前，您必須從服務主控台下載其安裝檔案。

### 若要在將工作負載新增至保護時下載代理程式

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

### 若要下載代理程式供之後使用

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

## 7.6.2 在 Windows 中安裝 Cyber Protection 代理程式

### 必要條件

在您打算保護的電腦上，下載所需的代理程式。請參閱 "下載 Cyber Protection 代理程式" (第 55 頁)。

### 若要安裝 Windows 用代理程式

1. 確定電腦已連線到網際網路。
2. 以系統管理員身分登入並啟動安裝程式。
3. [可選] 按一下 **[自訂安裝設定]**，並進行適當的變更 (如有需要):
  - 變更要安裝的元件 (例如，停用 Cyber Protection 監視器或命令列工具的安裝，或安裝反惡意程式碼保護和 URL 篩選用代理程式)。

---

#### 注意事項

在 Windows 電腦上，反惡意程式碼保護和 URL 篩選功能需要安裝反惡意程式碼保護和 URL 篩選用代理程式。如果在其保護計劃中啟用 **[防毒和反惡意程式碼保護]** 或 **[URL 篩選]** 模組，則會為受保護的工作負載自動安裝該代理程式。

---

- 變更在 Cyber Protection 服務中註冊電腦的方法。您可以從 **[使用服務主控台]** (預設) 切換到 **[使用認證]** 或 **[使用註冊權杖]**。
  - 變更安裝路徑。
  - 變更將執行代理程式服務所用的使用者帳戶。如需詳細資訊，請參閱「[變更 Windows 電腦上的登入帳戶](#)」。
  - 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。
  7. 如果您在步驟 3 中保留預設的註冊方法 **[使用服務主控台]**，則請等到註冊畫面出現，然後再繼續進行下一個步驟。否則，您不需要再進行任何動作。
  8. 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，登入服務主控台、檢閱註冊詳細資訊，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。
- 

#### 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服務主控台的帳戶。

- 使用命令列手動註冊電腦。如需有關操作方式的詳細資訊，請參閱「[手動註冊電腦](#)」。
9. [如果是以其租用戶處於加強安全性模式下的帳戶註冊代理程式] 設定加密密碼。

## 7.6.3 在 Linux 中安裝 Cyber Protection 代理程式

### 必要條件

- 在您打算保護的電腦上，下載所需的代理程式。請參閱 "下載 Cyber Protection 代理程式" (第 55 頁)。
- 若要安裝 Linux 用代理程式，您需要至少 2 GB 的可用磁碟空間。

### 安裝 Linux 用代理程式

1. 確定電腦已連線到網際網路。
2. 以 root 使用者身分執行安裝檔案。  
 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 Cyber Protection 服務中註冊電腦的預設方法，請使用下列其中一個參數，執行安裝檔案：
  - --register-with-credentials – 要求在安裝期間輸入使用者名稱和密碼
  - --token=STRING – 使用註冊權杖
  - --skip-registration – 略過註冊
3. 選擇要安裝的代理程式的核取方塊。您可以選取下列代理程式：
  - Linux 用代理程式
  - Virtuozzo 用代理程式
  - 適用於 Oracle 的代理程式
  - MySQL/MariaDB 用代理程式
 Virtuozzo 用代理程式、Oracle 用代理程式和 MySQL/MariaDB 用代理程式需要也安裝 Linux 用代理程式 (64 位元)。
4. 如果您在步驟 2 中保留預設的註冊方法，則請繼續進行下一個步驟。否則，請輸入 Cyber Protection 服務的使用者名稱與密碼，或等到電腦使用權杖註冊為止。
5. 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，登入服務主控台、檢閱註冊詳細資訊，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。

---

#### 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服務主控台的帳戶。

- 使用命令列手動註冊電腦。如需有關操作方式的詳細資訊，請參閱「[手動註冊電腦](#)」。



6. [如果是以其租用戶處於加強安全性模式下的帳戶註冊代理程式] 設定加密密碼。
7. 如果在電腦上啟用 UEFI 安全開機，您會在安裝後收到您需要重新啟動系統的通知。請務必記住應該使用的密碼 (根使用者或 "acronis" 的密碼)。

---

#### 注意事項

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

---

8. 安裝完成後，請執行下列其中一項操作：
  - 如果系統在上一個步驟中提示您重新啟動系統，按一下 **[重新啟動]**。  
在系統重新啟動期間，選擇 MOK (機器擁有者金鑰) 管理、選擇 **[註冊 MOK]**，然後使用上一個步驟中建議的密碼，註冊金鑰。
  - 否則，請按一下 **[結束]**。

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

## 7.6.4 在 macOS 中安裝 Cyber Protection 代理程式

### 必要條件

在您打算保護的電腦上，下載所需的代理程式。請參閱 "下載 Cyber Protection 代理程式" (第 55 頁)。

### 若要安裝 *Mac* 用代理程式 (x64 或 ARM64)

1. 確定電腦已連線到網際網路。
2. 按兩下安裝檔案 (.dmg)。
3. 請等候作業系統掛載安裝磁碟影像。
4. 按兩下 **[安裝]**。
5. 如果您的網路中已啟用 Proxy 伺服器，請按一下功能表列中的 **[保護代理程式]**、按一下 **[Proxy 伺服器設定]**，然後指定 Proxy 伺服器主機名稱/IP 位址、連接埠和認證。
6. 若畫面顯示提示，請提供系統管理員認證。
7. 按一下 **[繼續]**。
8. 等到註冊畫面出現為止。
9. 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，登入服務主控台、檢閱註冊詳細資訊，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。



---

### 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服務主控台的帳戶。

- 使用命令列手動註冊電腦。如需有關操作方式的詳細資訊，請參閱「[手動註冊電腦](#)」。

10. [如果是以其租用戶處於加強安全性模式下的帳戶註冊代理程式] 設定加密密碼。

11. 如果您的 macOS 版本為 Mojave 10.14.x 或更新版本，則對保護代理程式授予完成磁碟存取權，才能啟用備份作業。

如需相關指示，請參閱將「[完整磁碟存取](#)」權限授予網路保護代理程式 (64657)。

## 7.6.5 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。

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。

## 7.6.6 動態安裝與解除安裝元件

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

- 反惡意程式碼保護和 URL 篩選用代理程式 - 操作反惡意程式碼保護和 URL 篩選功能時所需。
- 資料洩漏防禦用代理程式 - 操作裝置控制功能時所需。
- Acronis 網路保護服務 - 操作反惡意程式碼保護時所需。

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

- 防毒和反惡意程式碼保護
- URL 篩選
- 裝置控制

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

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

- 備份
- 復原

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

## 7.7 自動安裝或解除安裝

### 7.7.1 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 104 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]**。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 105 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。  
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在「[自動安裝或解除安裝參數](#)」中有所說明。

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](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=<元件清單>

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    |
|------------------|--------------|---------------|--------------|
| AgentFeature     |              | 32 位元 / 64 位元 | 適用於代理程式的核心元件 |
| MmsMspComponents | AgentFeature | 32 位          | 適用於備份的核      |

|                        |                        |                    |                                      |
|------------------------|------------------------|--------------------|--------------------------------------|
|                        |                        | 元/64<br>位元         | 心元件                                  |
| BackupAndRecoveryAgent | MmsMspComponents       | 32 位<br>元/64<br>位元 | Windows 用代理<br>程式                    |
| AmpAgentFeature        | BackupAndRecoveryAgent | 32 位<br>元/64<br>位元 | 反惡意程式碼和<br>URL 篩選用代理<br>程式           |
| DlpAgentFeature        | BackupAndRecoveryAgent | 32 位<br>元/64<br>位元 | 資料洩漏防禦用<br>代理程式                      |
| SasAgentFeature        | TrayMonitor            | 32 位<br>元/64<br>位元 | File Sync & Share<br>用代理程式           |
| ArxAgentFeature        | MmsMspComponents       | 32 位<br>元/64<br>位元 | Exchange 用代理<br>程式                   |
| ArsAgentFeature        | BackupAndRecoveryAgent | 32 位<br>元/64<br>位元 | SQL 用代理程式                            |
| ARADAgentFeature       | BackupAndRecoveryAgent | 32 位<br>元/64<br>位元 | Active Directory<br>用代理程式            |
| ArxOnlineAgentFeature  | MmsMspComponents       | 32 位<br>元/64<br>位元 | Microsoft 365 用<br>代理程式              |
| OracleAgentFeature     | BackupAndRecoveryAgent | 32 位<br>元/64<br>位元 | 適用於 Oracle 的<br>代理程式                 |
| AcronisESXSupport      | BackupAndRecoveryAgent | 64 位<br>元          | VMware ESX(i) 用<br>代理程式<br>(Windows) |
| HyperVAgent            | BackupAndRecoveryAgent | 32 位<br>元/64<br>位元 | Hyper-V 用代理程<br>式                    |
| CommandLineTool        |                        | 32 位<br>元/64<br>位元 | 命令列工具                                |
| TrayMonitor            | AgentFeature           | 32 位               | Cyber Protect 監                      |

|                                     |  |                    |         |
|-------------------------------------|--|--------------------|---------|
|                                     |  | 元/64<br>位元         | 視器      |
| BackupAndRecoveryBootableComponents |  | 32 位<br>元/64<br>位元 | 可開機媒體組建 |

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。

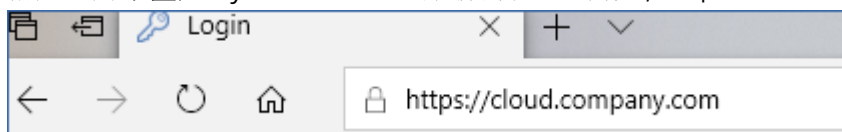
如果未指定此參數，則產品語言將由您的系統語言定義，但前提是該語言在上述清單中。否則，產品語言將設定為 [英文] (en)。

## 註冊參數

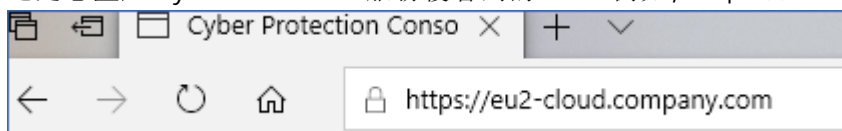
REGISTRATION\_ADDRESS

這是 Cyber Protection 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 Protection 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 Protection 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 and REGISTRATION\_PASSWORD

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

## REGISTRATION\_PASSWORD\_ENCODED

在 Cyber Protection 服務中註冊代理程式所使用之帳戶的密碼 (以 base64 編碼)。如需有關如何將密碼編碼的詳細資訊, 請參閱[「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。您可以在服務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> and 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> and ESX\_PASSWORD=<password>  
用於存取 vCenter Server 或 ESXi 主機的認證。

## HTTP\_PROXY\_ADDRESS=<IP address> and 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> and 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。

## SKIP\_SHA2\_KB\_CHECK={0,1}

如果值為 0, 或者未指定參數, 安裝程式將會檢查電腦上是否安裝 Microsoft 的 SHA2 程式碼簽署支援更新 ([KB4474419](#))。如果找不到更新, 安裝將會失敗。

此檢查只會在需要 SHA2 程式碼簽署支援更新的作業系統上執行。若要查看需要此更新的作業系統, 請參閱 "支援的作業系統和環境" (第 25 頁)。

## 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。

ANTI\_TAMPER\_PASSWORD=<password>

解除安裝受密碼保護之 Windows 用代理程式或修改其元件所需的密碼。

## 範例

- 安裝 Windows 用代理程式、反惡意程式碼和 URL 篩選用代理程式、命令列工具和 Cyber Protection 監視器。使用使用者名稱和密碼, 在 Cyber Protection 服務中登錄電腦。

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,AmpAgentFeature,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 Cyber Protection Monitor。在 Windows 中, 為代理程式服務建立一個新的登入帳戶。使用權杖, 在 Cyber Protection 服務中登錄電腦。

```
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 Cyber Protection 監視器。使用使用者名稱和以 base64 編碼的密碼, 在 Cyber Protection 服務中登錄電腦。

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



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

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

- 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
```

## 7.7.2 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：

```
<套件名稱> -a <參數 1> ... <參數 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：

```
<套件名稱> -a --options-file=<檔案的路徑>
```

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=}<元件清單>`

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

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

若無此參數，則將安裝以上所有元件。

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

`.i686` 安裝套件僅包含 BackupAndRecoveryAgent。

`{-a | --auto}`

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

`{-t | --strict}`

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

`{-n|--nodeps}`

在安裝期間將會忽略缺少所需的 Linux 套件。

`{-d|--debug}`

在詳細模式下寫入安裝記錄。

`--options-file=<位置>`

安裝參數將會從文字檔案而非命令列讀取。

`--language=<語言 ID>`

產品語言。可用的值如下：en、bg、cs、da、de、es、fr、hu、id、it、ja、ko、ms、nb、nl、pl、pt、pt\_BR、ru、fi、sr、sv、tr、zh、zh\_TW。

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

## 註冊參數

指定下列其中一個參數：

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

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

- `--token=<權杖>`

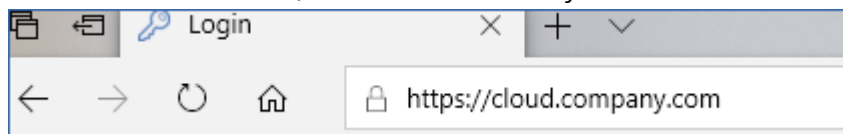
註冊權杖是由 12 個字元組成的序列，並以連字號分成三個區段。您可以在服務主控台中產生一個註冊權杖，如「[透過群組原則部署代理程式](#)」中所述。

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

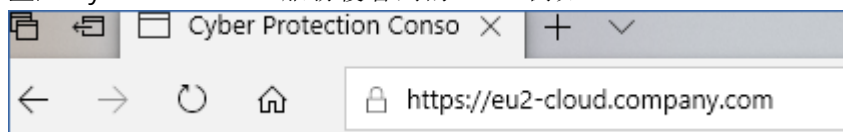
- `{-C|--rain=<服務位址>`

Cyber Protection 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 Protection 服務的位址。例如：



不過，當您使用 `{-C|--rain=<}</code> 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 Protection 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 Protection 服務中註冊代理程式所使用之帳戶的使用者名稱和密碼。這不得是合作夥伴系統管理員帳戶。

- `--skip-registration`

如果您需要安裝代理程式，但是您打算稍後在 Cyber Protection 服務中註冊該代理程式，請使用此參數。如需有關操作方式的詳細資訊，請參閱[「手動註冊電腦」](#)。

## 其他參數

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

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

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

HTTP Proxy 伺服器的認證。如果伺服器需要驗證，請使用這些參數。

`--tmp-dir=<位置>`

指定安裝期間存放暫存檔的資料夾。預設資料夾為 **/var/tmp**。

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

即使您的系統可能已經存在可轉散發程式庫，也將在安裝期間使用。

`--skip-prereq-check`

將不會檢查是否已安裝編譯 snapapi 模組所需的套件。

`--force-weak-snapapi`

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

`--skip-svc-start`

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

## 資訊參數

`{-?|--help}`

顯示參數說明。

`--usage`

顯示命令使用的簡要說明。

`{-v|--version}`

顯示安裝套件版本。

`--product-info`

顯示產品名稱和安裝套件版本。

`--snapapi-list`

顯示可用的現成 snapapi 模組。

`--components-list`

顯示安裝程式元件。

## 舊版功能的參數

這些參數與舊版元件 `agent.exe` 相關。

`{-e|--ssl=}<路徑>`

指定用於 SSL 通訊之自訂憑證檔案的路徑。

`{-p|--port=}<連接埠>`

指定 `agent.exe` 接聽連線的連接埠。預設連接埠為 9876。

## 解除安裝參數

`{-u|--uninstall}`

解除安裝產品。

`--purge`

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

## 範例

- 安裝 Linux 用代理程式但不註冊。

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

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

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

- 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
```

## 7.7.3 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 Cyber Protection 代理程式。

### 若要下載安裝檔案 (.dmg)

- 在服務主控台中，移至 **[裝置] > [所有裝置]**。
- 按一下 **[新增]**，然後按一下 **[Mac]**。

### 安裝 Mac 用代理程式

- 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。

- 掛載 .dmg 檔案。

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

在這裡，<dmg\_file> 是安裝檔案的名稱。例如，**Cyber\_Protection\_Agent\_for\_MAC\_x64.dmg**。

- 執行安裝程式。

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

- 卸離安裝檔案 (.dmg)。

```
hdiutil detach <dmg_root>
```

## 範例

- ```
mkdir mydirectory
```

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

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

```
hdiutil detach mydirectory
```

若要註冊 **Mac** 用代理程式

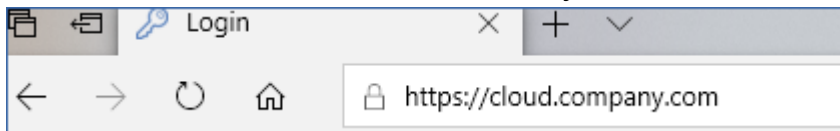
執行下列其中一項操作：

- 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 -a <Cyber Protection 服
務位址> -t cloud -u <使用者名稱> -p <密碼> -o register
```

其中：

<Cyber Protection 服務位址> 是您用來登入 Cyber Protection 服務的位址。例如：



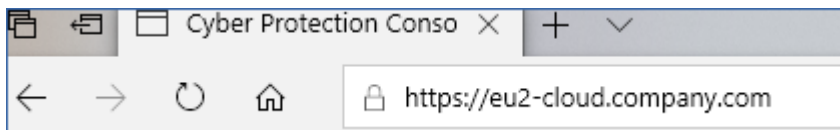
<使用者名稱> 和 <密碼> 是註冊代理程式所使用之帳戶的認證。這不得是合作夥伴的系統管理員帳戶。

- 使用註冊權杖註冊代理程式。

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -a <Cyber Protection 服
務位址> -t cloud -o register --token <權杖>
```

註冊權杖是由 12 個字元組成的序列，並以連字號分成三個區段。您可以在服務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 Protection 服務後看到的 URL。例如：



範例

使用使用者名稱與密碼註冊。

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

使用權杖註冊。

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

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。

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
```

7.8 手動註冊電腦

除了在代理程式安裝期間，於 Cyber Protection 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

若要使用使用者名稱和密碼註冊電腦，請執行下列命令。

在 Windows 中

以目前帳戶的身分註冊電腦所使用的命令：

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

以另一個帳戶的身分註冊電腦所使用的命令範本：

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

命令範例：

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


在 Linux 中

以目前帳戶的身分註冊電腦所使用的命令：

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

以另一個帳戶的身分註冊電腦所使用的命令範本：

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

命令範例：

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

在 macOS 中

以目前帳戶的身分註冊電腦所使用的命令：

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

以另一個帳戶的身分註冊電腦所使用的命令範本：

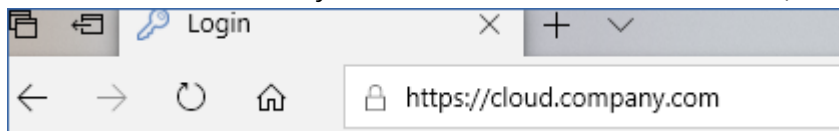
```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <service address> -u <user name> -p <password>
```

命令範例：

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

注意事項

請使用註冊代理程式所使用之特定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。服務位址是您用來登入 Cyber Protection 服務的 URL。例如, <https://cloud.company.com>：



或者, 您可以使用註冊權杖註冊電腦。若要這麼做, 請執行下列命令。

在 Windows 中

命令範本：

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud  
-a <服務位址> --token <權杖>
```

命令範例：

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

在 Linux 中

命令範本：

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <服務位  
址> --token <權杖>
```

命令範例：

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

在 macOS 中

命令範本：

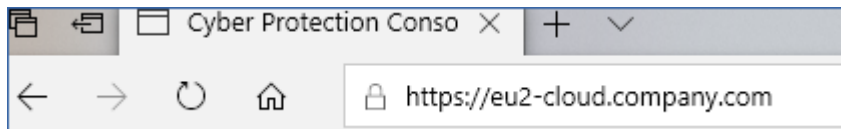
```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"  
-o register -t cloud -a <服務位址> --token <權杖>
```

命令範例：

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

注意事項

當您使用註冊權杖時，必須指定確實的資料中心位址。這是您登入 Cyber Protection 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>。

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

執行下列命令：

在 Windows 中

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

在 Linux 中

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

在 macOS 中

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

7.8.1 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。

例如，在 Windows 中，執行此命令。

命令範本：

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud  
-a <服務位址> -u <使用者名稱> -p "<密碼>"
```

命令範例：

```
"%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。

例如，在 Windows 中，執行此命令。

命令範本：

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud  
-a <服務位址> -u <使用者名稱> -b -p <編碼的密碼>
```

命令範例：

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

7.9 自動探索電腦

透過自動探索，您可以：

- 偵測 Active Directory 網域或區域網路中的機器，自動安裝保護代理程式並自動註冊機器。
- 在多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。

7.9.1 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 (不支援 Windows XP) 的機器支援遠端安裝代理程式。若要在執行 Windows Server 2012 R2 的電腦上進行遠端安裝，該電腦上必須已安裝 [Windows 更新 KB2999226](#)。

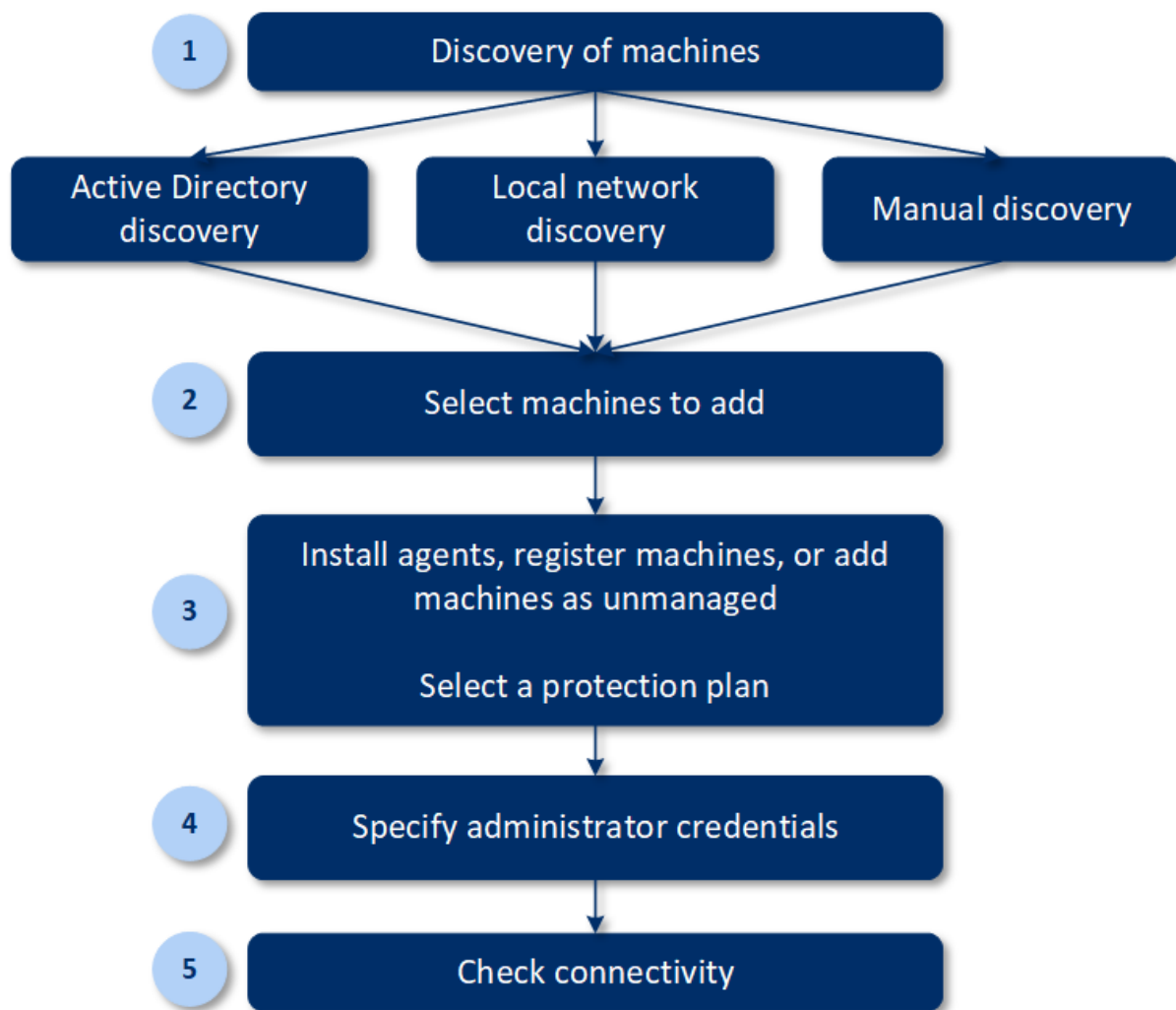
7.9.2 自動探索運作方式

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 (簡短的/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：

- 在機器上安裝保護代理程式和其他元件, 並在服務主控台註冊。
- 在服務主控台註冊機器(如果已安裝了保護代理程式)。
- 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服務主控台註冊的機器。

4. 提供所選電腦的系統管理員認證。

5. 請確認您可以使用提供的認證來連線到電腦。

Cyber Protection 服務主控台顯示的機器分為以下類別：

- **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。

7.9.3 遠端安裝代理程式的運作方式

1. 探索代理程式會使用探索精靈中指定的主機名稱、IP 位址和系統管理員認證來連線到目標電腦，然後將 `web_installer.exe` 檔案上傳到那些電腦上。
2. `web_installer.exe` 檔案會以自動模式在目標電腦上執行。
3. Web 安裝程式會從雲端擷取其他套件，然後透過 `msiexec` 命令將其安裝到目標電腦上。
4. 在安裝完成之後，將在雲端註冊元件。

7.9.4 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. 在服務主控台中，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. 選擇在探索之後必須執行的動作：

- **安裝代理程式並登錄電腦。**您可以按一下 **[選擇元件]**，選擇要在電腦上安裝的元件。如需詳細資訊，請參閱 "選擇要安裝的元件" (第 83 頁)。

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 Protection 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。您將可以在主控台中檢視電腦，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] **登錄電腦的使用者** – 選擇要為其登錄電腦之單位或下級單位的使用者。

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。如果您要定義一些自訂系統管理員認證，則您應該手動做一些額外的準備，如以下的「為自訂系統管理員啟用代理程式的遠端安裝」所述。

11. 系統會檢查所有電腦的連線。如果與部分電腦的連線失敗，可以變更這些電腦的認證。

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

準備電腦以進行遠端安裝

1. 要在執行 Windows 7 或更高版本的遠端電腦成功安裝，必須在該機器上停用 **[控制面板] > [資料夾選項] > [檢視] > [使用共用精靈]** 選項。
2. 若要在非 Active Directory 網域成員的遠端電腦上成功安裝，必須在該電腦上停用使用者帳戶控制 (UAC)。如需有關停用方式的詳細資訊，請參閱「[使用者帳戶控制 \(UAC\) 的需求](#)」>「若要停用 UAC」。
3. 根據預設，您需要有內建系統管理員帳戶的認證，才能在任何 Windows 電腦上進行遠端安裝。若要使用其他系統管理員帳戶的認證執行遠端安裝，必須停用使用者帳戶控制 (UAC) 遠端限制。如需有關停用方式的詳細資訊，請參閱「[使用者帳戶控制 \(UAC\) 的需求](#)」>「若要停用 UAC 遠端限制」。
4. 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：前往 **[控制面板] > [Windows 防火牆] > [網路和共用中心] > [變更進階共用設定]**。
5. Cyber Protection 使用 TCP 連接埠 445、25001 和 43234 進行遠端安裝。

當您啟用**[檔案及印表機共用]**時，會自動開放連接埠 445。連接埠 43234 和 25001 會透過 Windows 防火牆自動開啟。如果您使用不同的防火牆，請確定這三個連接埠都已開啟 (新增至例外)，以便讓內送和外送要求通過。

遠端安裝完成之後，連接埠 25001 會透過 Windows 防火牆自動關閉。若您想要在未來遠端更新代理程式，則必須將連接埠 445 和 43234 保留為開啟狀態。在每次更新期間，會透過 Windows 防火牆自動開放和關閉連接埠 25001。若使用不同的防火牆，則所有三個連接埠均將保留為開啟狀態。

使用者帳戶控制 (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**

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	
資料洩漏防禦用代理程式	此代理程式可讓您在保護計劃下的電腦上, 限制使用者對本機和重新導向的週邊裝置、連接埠以及剪貼簿的存取。如果選擇, 則要安裝。
反惡意程式碼和 URL 篩選	此元件可在保護計劃中啟用 [防毒和反惡意程式碼保護] 模組和 [URL 篩選] 模組。即使您選擇不安裝, 如果在電腦的保護計劃中啟用以上任何模組, 之後還是會自動安裝。
Hyper-V 用代理程式	此代理程式會備份 Hyper-V 虛擬機器, 而且將會安裝在 Hyper-V 主機上。如果選擇並在電腦上偵測到 Hyper-V 角色, 則要安裝。
SQL 用代理程式	此代理程式會備份 SQL Server 資料庫, 而且將會安裝在執行 Microsoft SQL Server 的電腦上。如果選擇並在電腦上偵測到應用程式, 則要安裝。

Exchange 用代理程式	此代理程式會備份 Exchange 資料庫和信箱，而且將會安裝在執行 Microsoft Exchange Server 信箱角色的電腦上。如果選擇並在電腦上偵測到應用程式，則要安裝。
Active Directory 用代理程式	此代理程式會備份 Active Directory 網域服務的資料，而且將會安裝在網域控制站上。如果選擇並在電腦上偵測到應用程式，則要安裝。
VMware 用代理程式 (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。
Microsoft 365 用代理程式	此代理程式會將 Microsoft 365 信箱備份到本機目的地，而且將會安裝在 Windows 電腦上。如果選擇，則要安裝。
適用於 Oracle 的代理程式	此代理程式會備份 Oracle 資料庫，而且將會安裝在執行 Oracle Database 的電腦上。如果選擇，則要安裝。
Cyber Protection 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。 支援 Windows 7 Service Pack 1 和更新版本，以及 Windows Server 2008 R2 Service Pack 1 和更新版本。

7.9.5 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 Protection 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。

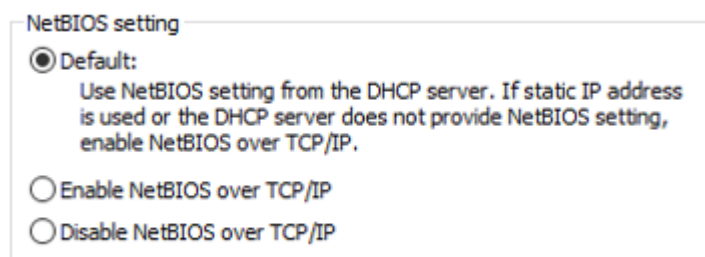
在電腦上安裝保護代理程式之後，這些電腦將會顯示在 **[裝置] > [具有代理程式的電腦]** 區段中。

若要檢查您的保護狀態，移至 **[監控] > [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。

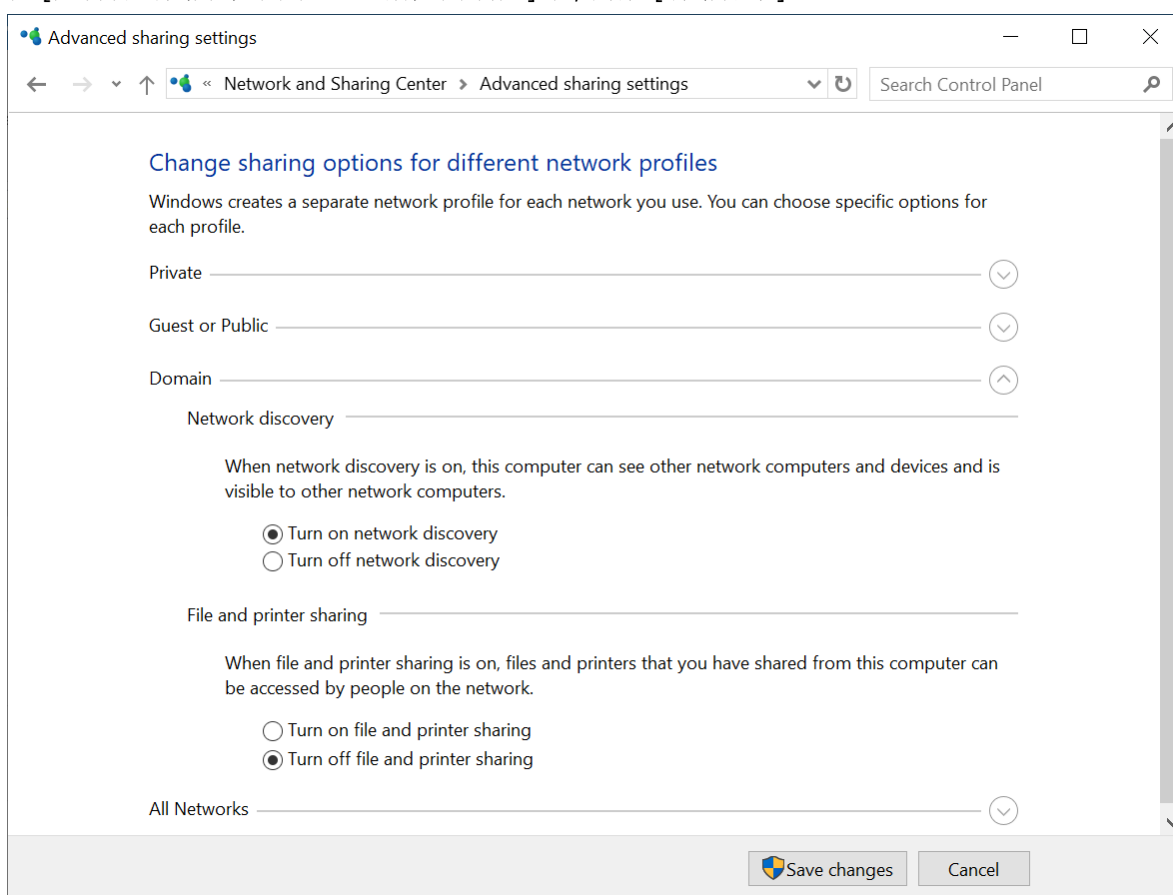
7.9.6 疑難排解

如果您對自動探索功能有任何問題，請嘗試檢查下列項目：

- 檢查是透過 TCP/IP 啟用 NetBIOS 還是設為預設值。



- 在 **[控制台\網路和共用中心\進階共用設定]** 中，開啟 **[網路探索]**。



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

7.10 部署 VMware 用代理程式 (虛擬裝置)

7.10.1 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。

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】。

7.10.2 部署 OVF 範本

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

7.10.3 設定虛擬裝置

1. 在 vSphere Client 中, 顯示 **[清查]**, 以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. 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。
3. 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。

4. 在 **[代理程式選項]** 的 **[管理伺服器]** 中, 按一下**[變更]**。
 - a. 在 **[伺服器名稱/IP]** 中, 選取 **[雲端]**。軟體會顯示 Cyber Protection 服務位址。除非特別指示, 否則請不要變更此位址。
 - b. 在 **[使用者名稱]** 和 **[密碼]** 中, 指定 Cyber Protection 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。
5. 在**[虛擬機器]** 下, 在**[時區]** 中, 按一下**[變更]**。選擇您所在位置の時區, 以確保排程作業在適當時間執行。
6. **[選擇性]** 新增本機儲存空間。

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。

7. **[如果您的網路中已啟用 Proxy 伺服器]** 設定 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。

注意事項

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

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

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

7.11 正在部署 Scale Computing HC3 用代理程式 (虛擬裝置)

7.11.1 在您開始之前

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

代理程式的系統需求

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

裝置虛擬磁碟的大小為 9 GB。

我需要多少個代理程式?

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

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

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

檢查哪個代理程式管理特定的機器

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

7.11.2 部署 QCOW2 範本

1. 請登入您的 Cyber Protection 帳戶。
2. 按一下 **[裝置]** > **[所有裝置]** > **[新增]** > **[Scale Computing HC3]**。
.zip 封存將會下載到您的電腦中。
3. 解壓縮 .zip 存檔，然後將 .qcow2 檔案和 .xml 檔案儲存到名為 **ScaleAppliance** 的資料夾中。
4. 將 **ScaleAppliance** 資料夾上傳到網路共用，並確認 Scale Computing HC3 叢集可以存取該資料夾。
5. 以獲指派 **[VM 建立/編輯]** 角色的系統管理員身分，登入 Scale Computing HC3 叢集。如需有關操作 Scale Computing HC3 虛擬機器所需角色的詳細資訊，請參閱 "Scale Computing HC3 用代理程式 - 必要角色" (第 91 頁)。
6. 在 Scale Computing HC3 Web 介面中，從 **ScaleAppliance** 資料夾匯入虛擬機器範本。
 - a. 按一下 **[匯入 HC3 VM]** 圖示。
 - b. 在 **[匯入 HC3 VM]** 視窗中，指定下列內容：
 - 新虛擬機器的名稱。
 - **ScaleAppliance** 資料夾所在的網路共用。
 - 存取此網路共用所需的使用者名稱和密碼。
 - **[選用]** 新虛擬機器的網域標籤。
 - 網路共用上的 **ScaleAppliance** 資料夾路徑。
 - c. 按一下 **[匯入]**。

部署完成後，您必須設定虛擬裝置。如需有關設定方式的詳細資訊，請參閱 "設定虛擬裝置" (第 90 頁)。

注意事項

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

7.11.3 設定虛擬裝置

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

若要設定虛擬設備

1. 登入您的 Scale Computing HC3 帳戶。
2. 選擇您需要設定的裝置虛擬機器，然後按一下 **[主控台]** 圖示。
3. 在 **[eth0]** 欄位中，設定裝置的網路介面。
請確認自動指派的 DHCP 位址 (如果有的話) 在您虛擬機器所使用的網路內有效，或手動指派這些位址。可能有一或多個介面需要設定，端視裝置所使用的網路數量而定。
4. 在 **[Scale Computing]** 欄位中，按一下 **[變更]** 以指定 Scale Computing HC3 叢集位址以及存取該位址所使用的認證：
 - a. 在 **[伺服器名稱/IP]** 欄位中，輸入叢集的 DNS 名稱或 IP 位址。
 - b. 在 **[使用者名稱]** 和 **[密碼]** 欄位中，輸入 Scale Computing HC3 系統管理員帳戶的認證。
請確保此帳戶具備操作 Scale Computing HC3 虛擬機器所需的角色。如需有關這些角色的詳細資訊，請參閱 "Scale Computing HC3 用代理程式 - 必要角色" (第 91 頁)。
 - c. [選用] 按一下 **[檢查連線]** 以確保提供的認證正確無誤。
 - d. 按一下 **[確定]**。
5. 在 **[Management Server]** 欄位中，按一下 **[變更]** 以指定 Cyber Protection 服務位址以及存取該位址所使用的認證。
 - a. 在 **[伺服器名稱/IP]** 欄位中，選擇 **[雲端]**，然後指定 Cyber Protection 服務位址。
 - b. 在 **[使用者名稱]** 和 **[密碼]** 欄位中，輸入您的帳戶在 Cyber Protection 服務中的認證。
 - c. 按一下 **[確定]**。
6. [選用] 在 **[名稱]** 欄位中，按一下 **[變更]** 以變更虛擬裝置的預設名稱，亦即 **localhost**。此名稱會顯示在 Cyber Protection 服務主控台中。
7. [選擇性] 在 **[時間]** 欄位中，按一下 **[變更]**，然後選擇您所在位置的時區，以確保排程作業在適當時間執行。
8. [如果您的網路中已啟用 Proxy 伺服器] 設定 Proxy 伺服器。
 - a. 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。

注意事項

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

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

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

保護 Scale Computing HC3 叢集中的虛擬機器

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

7.11.4 Scale Computing HC3 用代理程式 – 必要角色

本節說明 Scale Computing HC3 虛擬機器操作所需的角色。

作業	角色
備份虛擬機器	備份 VM 建立/編輯 VM 刪除
復原至現有的虛擬機器	備份 VM 建立/編輯

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

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

7.12.1 在您開始之前

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

注意事項

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

代理程式的系統需求

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

2 個 vCPU 搭配 4 GB 的 RAM (中等類別) 非常適合而且足以適用於大多數作業。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 GB 的 RAM，才能提升備份效能。

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 multiple 代理程式。

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

當代理程式間負載不平衡的情況達到 20% 的程度時，就會進行自動重新分配。新增或移除機器或代理程式時，可能會發生這種情況。例如，您發現需要更多代理程式來增進處理能力，而且您要將額外的虛擬裝置部署到叢集。管理伺服器會指派最適合的虛擬機器給新的代理程式。舊代理程式的

負載將會減少。當您從管理伺服器移除代理程式時，指派給代理程式的機器會在剩餘的代理程式之間重新分配。但是，如果代理程式損毀，或未手動從 Virtuoizzo Hybrid Infrastructure 節點刪除代理程式，就不會發生這種情況。只有在當您從 Cyber Protection Web 介面移除這種代理程式後，才會開始重新分配。

檢查哪個代理程式管理特定的機器

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

限制

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

7.12.2 在 Virtuoizzo Hybrid Infrastructure 中設定網路

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

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

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

如需有關設定網路的詳細資訊，請參閱 Virtuoizzo 文件中的[計算叢集的需求](#)。

7.12.3 在 Virtuoizzo Hybrid Infrastructure 中設定使用者帳戶

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

若要授予存取預設網域中所有專案的權限

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

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

2. 使用環境檔案授權其他 OpenStack 命令：

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

3. 執行以下命令：

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

在這裡，<使用者名稱> 是 Virtuzo Hybrid Infrastructure 帳戶，且在預設網域中具備【系統管理員】角色。虛擬裝置將會使用此帳戶，備份和還原預設網域底下的任何子專案中的虛擬機器。

範例

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

若要在不同於預設網域的網域中管理虛擬機器的備份，請也執行下列命令。

若要授予存取不同網域中所有專案的權限

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

在這裡，<網域名稱> 是 <使用者名稱> 帳戶將可存取之專案的網域。

範例

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

授予對專案的存取權之後，請檢查指派給帳戶的角色。

若要檢查已指派的角色

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

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

範例

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

Role	User	Project	Domain
admin	johndoe@Default		MyNewDomain
compute	johndoe@Default		Default
domain_admin	johndoe@Default		Default
domain_admin	johndoe@Default		Default

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

若要檢查指派給所有專案中帳戶的有效角色, 請也執行下列命令。

若要檢查所有專案中的有效角色

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

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

範例

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

Role	User	Project	Domain
domain_admin	johndoe@Default		Default
compute	johndoe@Default	admin@Default	
compute	johndoe@Default	service@Default	
domain_admin	johndoe@Default	admin@Default	
domain_admin	johndoe@Default	service@Default	
project_user	johndoe@Default	service@Default	
member	johndoe@Default	service@Default	
reader	johndoe@Default	service@Default	
project_user	johndoe@Default	admin@Default	
member	johndoe@Default	admin@Default	
reader	johndoe@Default	admin@Default	
project_user	johndoe@Default		Default
member	johndoe@Default		Default
reader	johndoe@Default		Default

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

7.12.4 部署 QCOW2 範本

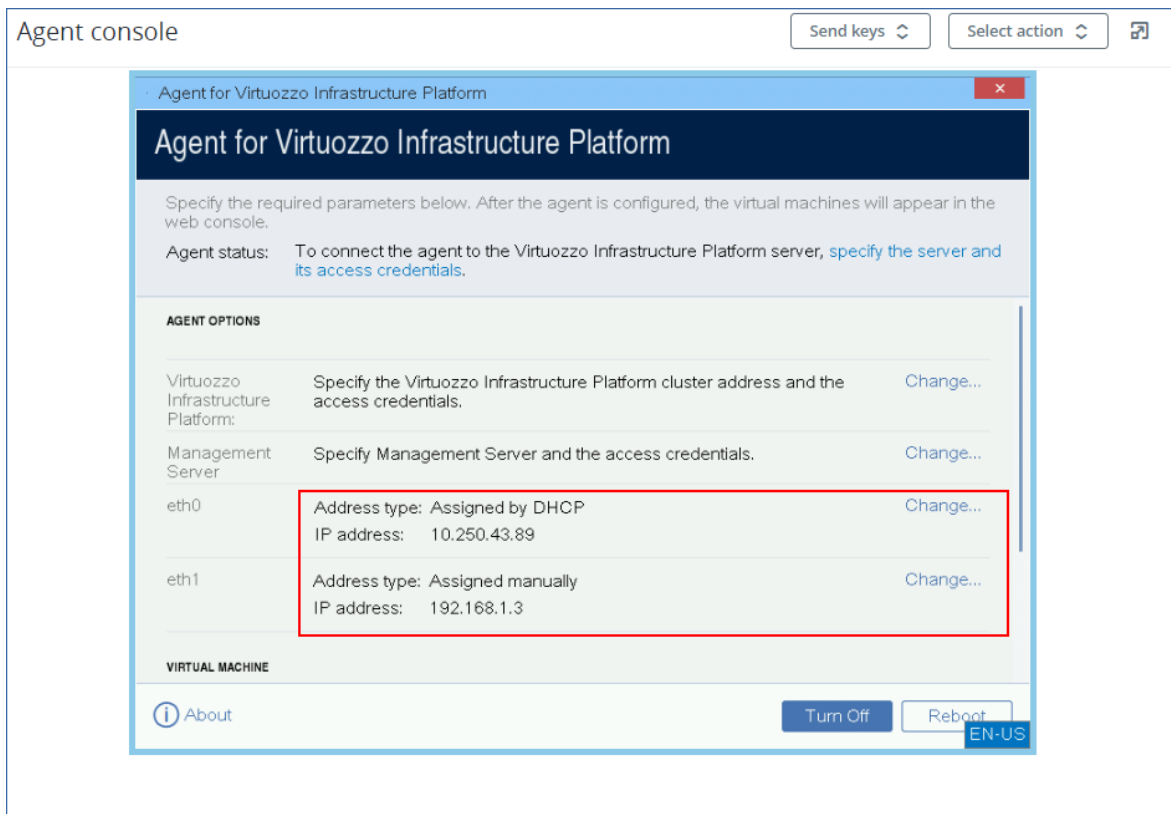
1. 請登入您的 Cyber Protection 帳戶。
2. 按一下 **[裝置] > [所有裝置] > [新增] > [Virtuozzo Hybrid Infrastructure]**。
.zip 封存將會下載到您的電腦中。
3. 解壓縮 .zip 封存。其中包含一個 .qcow2 影像檔案。
4. 登入您的 Virtuozzo Hybrid Infrastructure 帳戶。
5. 將 .qcow2 影像檔案新增到 Virtuozzo Hybrid Infrastructure 計算叢集，如下所示：
 - 在 **[計算] > [虛擬機器] > [影像]** 索引標籤上，按一下 **[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

7.12.5 設定虛擬裝置

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

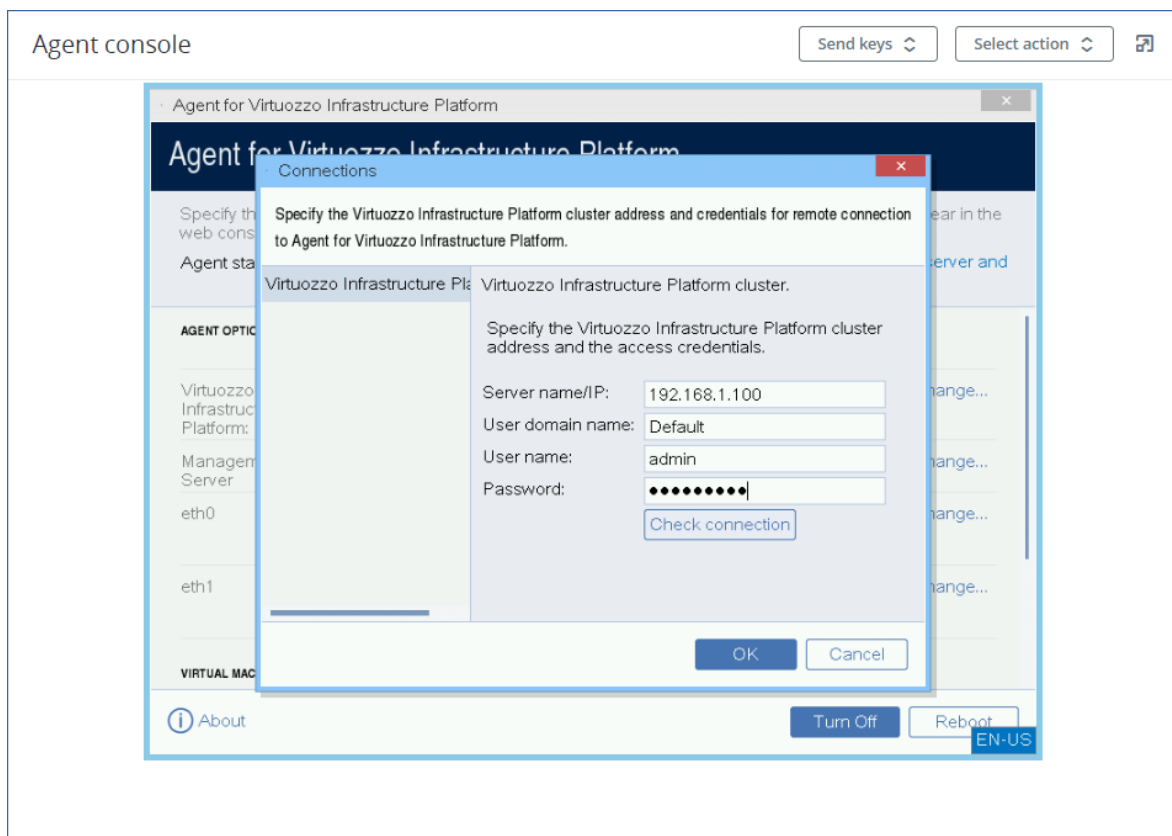
若要設定虛擬設備

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

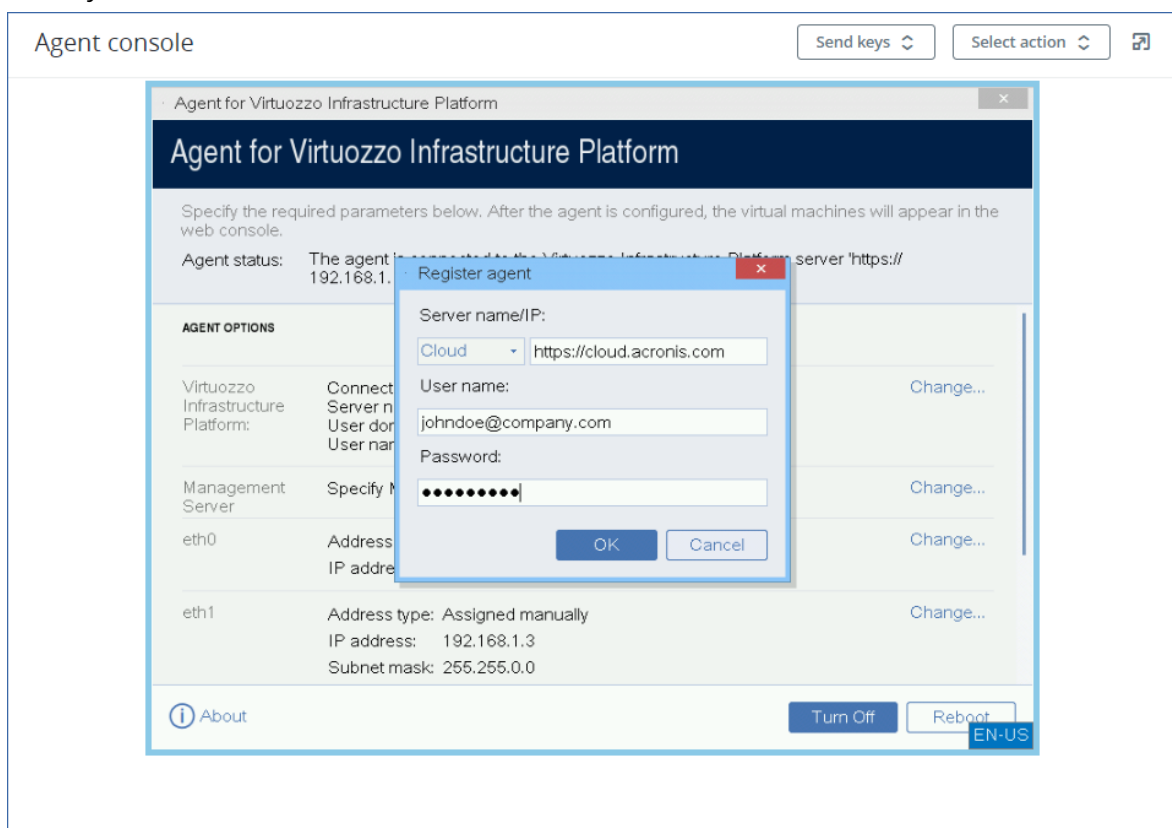


4. 指定 Virtuozzo 叢集位址和認證：

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



5. 指定 Cyber Protection 管理伺服器位址和認證以存取它。



6. [如果您的網路中已啟用 Proxy 伺服器] 設定 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="Tdwor">"1"</value>
  <value name="Host" type="TString">"ADDRESS"</value>
  <value name="Port" type="Tdwor">"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。

注意事項

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

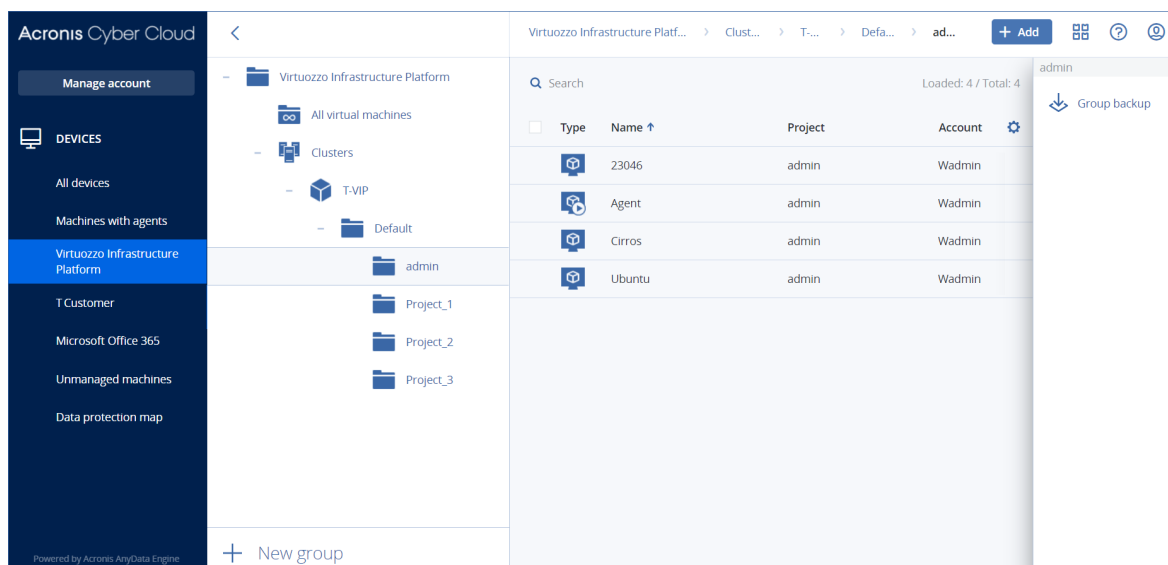
在 **/opt/acronis/etc/va-updater/config.yaml** 檔案中，將下列一行加入至檔案底部，並輸入您環境專用的值：

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

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

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

3. 選擇所需的電腦，並為其套用保護計劃。



7.13 正在部署 oVirt 用代理程式 (虛擬裝置)

7.13.1 在您開始之前

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

代理程式的系統需求

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

裝置虛擬磁碟的大小為 8 GiB。

我需要多少個代理程式？

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

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

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

不會發生這種情況。只有在您從 Cyber Protection 服務主控台移除這種代理程式後，才會開始重新分配。

檢查哪個代理程式管理特定的機器

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

限制

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

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

7.13.2 部署 OVA 範本

1. 請登入您的 Cyber Protection 帳戶。
2. 按一下 **[裝置]** > **[所有裝置]** > **[新增]** > **[Red Hat Virtualization (oVirt)]**。
.zip 封存將會下載到您的電腦中。
3. 解壓縮 .zip 封存。其中包含一個 .ova 檔案。
4. 將 .ova 檔案上傳到 Red Hat Virtualization/oVirt 資料中心中您要保護的主機。
5. 以系統管理員身分，登入 Red Hat Virtualization/oVirt 系統管理入口網站。如需有關操作虛擬機器所需角色的詳細資訊，請參閱 "oVirt 用代理程式 - 所需角色和連接埠" (第 104 頁)。
6. 從導覽功能表中，選擇 **[電腦]** > **[虛擬機器]**。
7. 按一下主要表格上方的垂直省略符號圖示 ，然後按一下 **[匯入]**。
8. 在 **[匯入虛擬機器]** 視窗中，執行下列作業：
 - a. 在 **[資料中心]** 中，選擇您要保護的資料中心。
 - b. 在 **[來源]** 中，選擇 **[虛擬裝置 (OVA)]**。
 - c. 在 **[主機]** 中，選擇您要上傳 .ova 檔案所在的主機。
 - d. 在 **[檔案路徑]** 中，指定包含 .ova 檔案的目錄的路徑。
 - e. 按一下 **[載入]**。
.ova 檔案中的 oVirt 虛擬裝置範本隨即出現在 **[來源上的虛擬機器]** 面板中。
如果範本沒有出現在此面板中，請確認您已經指定該檔案的正確路徑、檔案未損毀，而且可以聯繫主機。
 - f. 在 **[來源上的虛擬機器]** 中，選擇 oVirt 虛擬裝置範本，然後按一下向右箭頭。
範本隨即出現在 **[要匯入的虛擬機器]** 面板中。
 - g. 按 **[下一步]**。
9. 在新視窗中，按一下裝置名稱，然後設定下列設定：

- 在 **[網路介面]** 索引標籤上，設定網路介面。
- **[選用]** 在 **[一般]** 索引標籤上，變更裝有代理程式之虛擬機器的預設名稱。

部署現在已完成。接著，您必須設定虛擬裝置。如需有關設定方式的詳細資訊，請參閱 "設定虛擬裝置" (第 102 頁)。

注意事項

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

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

7.13.3 設定虛擬裝置

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

若要設定虛擬設備

1. 登入 Red Hat Virtualization/oVirt 系統管理入口網站。
2. 選擇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]** 圖示。
3. 在 **[eth0]** 欄位中，設定裝置的網路介面。
請確認自動指派的 DHCP 位址 (如果有的話) 在您虛擬機器所使用的網路內有效，或手動指派這些位址。可能有一或多個介面需要設定，端視裝置所使用的網路數量而定。
4. 在 **[oVirt]** 欄位中，按一下 **[變更]** 以指定 oVirt 引擎位址以及存取該位址所使用的認證：
 - a. 在 **[伺服器名稱/IP]** 欄位中，輸入引擎的 DNS 名稱或 IP 位址。
 - b. 在 **[使用者名稱]** 和 **[密碼]** 欄位中，輸入此引擎的系統管理員認證。
請確認此系統管理員帳戶具備操作 Red Hat Virtualization/oVirt 虛擬機器所需的角色。如需有關這些角色的詳細資訊，請參閱 "oVirt 用代理程式 - 所需角色和連接埠" (第 104 頁)。
 - c. **[選用]** 按一下 **[檢查連線]** 以確保提供的認證正確無誤。
 - d. 按一下 **[確定]**。
5. 在 **[Management Server]** 欄位中，按一下 **[變更]** 以指定 Cyber Protection 服務位址以及存取該位址所使用的認證。
 - a. 在 **[伺服器名稱/IP]** 欄位中，選擇 **[雲端]**，然後指定 Cyber Protection 服務位址。
 - b. 在 **[使用者名稱]** 和 **[密碼]** 欄位中，輸入您的帳戶在 Cyber Protection 服務中的認證。
 - c. 按一下 **[確定]**。
6. **[選用]** 在 **[名稱]** 欄位中，按一下 **[變更]** 以變更虛擬裝置的預設名稱，亦即 **localhost**。此名稱會顯示在 Cyber Protection 服務主控台中。
7. **[選擇性]** 在 **[時間]** 欄位中，按一下 **[變更]**，然後選擇您所在位置的時區，以確保排程作業在適當時間執行。
8. **[選用]** [如果您的網路中已啟用 Proxy 伺服器] 設定 Proxy 伺服器。
 - a. 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。

注意事項

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

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

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

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

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

7.13.4 oVirt 用代理程式 – 所需角色和連接埠

所需角色

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

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

- DiskCreator
- UserVmManager
- TagManager
- UserVmRunTimeManager
- VmCreator

oVirt/Red Hat Virtualization 4.4

- SuperUser

所需連接埠

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

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

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

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

7.14 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。

7.14.1 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。
- 您已下載所有 **Windows 用代理程式** 安裝程式。您可以在服務主控台其中的 **[新增裝置]** 頁面上取得下載連結。

7.14.2 步驟 1: 產生註冊權杖

註冊權杖會將使用者的身分識別傳遞至代理程式安裝程式，但不會儲存用於服務主控台的使用者認證。這可讓使用者以自己的帳戶註冊任意數目的電腦，而不必登入。基於安全性，權杖的存留時間受到限制，但您可以調整。預設期間為 3 天。

若要為您的帳戶產生註冊權杖

1. 登入服務主控台。
2. 按一下 **[裝置]** > **[所有裝置]** > **[新增]**。
3. 向下捲動至 **[註冊權杖]**，然後按一下 **[產生]**。
4. 指定權杖存留時間。
5. [選擇性] 若要讓權杖的使用者在新增的電腦上套用和撤銷保護計劃，請從下拉式清單中選擇該計劃。
6. 按一下 **[產生權杖]**。
7. 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]** 來檢視與刪除為您帳戶產生的權杖。

注意事項

基於安全性，[使用中的權杖] 表格不會顯示完整的權杖值。

若要代表您所管理租用戶中的使用者產生註冊權杖

1. 以合作夥伴或客戶系統管理員的身分，登入服務主控台。
如果您已登入管理主控台，請在 **[網路保護]** 索引標籤上，按一下 **[管理服務]** 以瀏覽至服務主控台。
2. 從左上方的下拉式清單中，選擇包含您要代表其建立權杖的使用者的租用戶。
3. 在 **[裝置]** 底下，按一下 **[所有裝置]** > **[新增]**。
[新增裝置] 對話方塊隨即在右側開啟。
4. 向下捲動至 **[註冊權杖]**，然後按一下 **[產生]**。
5. 指定權杖存留時間。
6. 選擇您要為其產生權杖的使用者。

注意事項

使用權杖註冊的代理程式將以您在此處選擇的使用者帳戶註冊。

7. [選擇性] 若要讓權杖的使用者在新增的電腦上套用和撤銷保護計劃，請從下拉式清單中選擇該計劃。

8. 按一下 **[產生權杖]**。

9. 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]** 來檢視與刪除為您可以管理的使用者產生的權杖。

注意事項

基於安全性，**[使用中的權杖]** 表格不會顯示完整的權杖值。

7.14.3 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. 按一下 **[註冊設定]** 旁的 **[指定]**，然後輸入您產生的權杖。

您可以將在 Cyber Protection 服務中註冊電腦的方法從 **[使用註冊權杖]** (預設) 變更為 **[使用認證]** 或 **[略過註冊]**。**[略過註冊]** 選項是假設您之後將會註冊電腦。

6. 檢閱或修改將新增到 .mst 檔案中的安裝設定，然後按一下 **[繼續]**。

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。

7.14.4 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。

7.15 更新代理程式

您可以手動更新所有代理程式。

您可以針對下列代理程式設定自動更新：

- Windows 用代理程式
- Linux 用代理程式
- Mac 用代理程式

注意事項

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

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

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

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

7.15.1 手動更新代理程式

您可以使用服務主控台，或下載並執行安裝檔案，以更新代理程式。

具有下列版本的虛擬裝置僅能使用服務主控台更新：

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

具有下列版本的代理程式也可以使用服務主控台更新：

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

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

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

必要條件

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

若要使用服務主控台更新代理程式

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

注意事項

在更新期間，進行中的所有備份都將失敗。

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

1. 按一下 **[設定]** > **[代理程式]** > 您要更新的代理程式 > **[詳細資料]**，然後檢查 **[已指派的虛擬機器]** 區段。更新後，您將需要重新輸入這些設定。
 - a. 記下 **[自動指派]** 開關的位置。
 - b. 若要尋找手動指派給代理程式的虛擬機器，請按一下 **[已指派:]** 連結。軟體會顯示已指派之虛擬機器的清單。請記下 **[代理程式]** 欄中的代理程式名稱後面有 (M) 的電腦。
2. 移除 VMware 用代理程式 (虛擬裝置)，如「**解除安裝代理程式**」中所述。在步驟 5 中，即使您打算再次安裝代理程式，還是要從 **[設定]** > **[代理程式]** 中刪除該代理程式。
3. 部署 VMware 用代理程式 (虛擬裝置)，如「**部署 OVF 範本**」中所述。
4. 設定 VMware 用代理程式 (虛擬裝置)，如「**設定虛擬裝置**」中所述。
如果您要重新架構本機連接的存放區，請在步驟 7 中執行下列操作：
 - a. 將含有本機存放區的磁碟新增至虛擬裝置。
 - b. 按一下 **[重新整理]** > **[建立存放區]** > **[掛載]**。
 - c. 此軟體會顯示磁碟的原始代號和標籤。請不要變更它們。
 - d. 按一下 **[確定]**。
5. 按一下 **[設定]** > **[代理程式]** > 您要更新的代理程式 > **[詳細資料]**，然後重新建構您在步驟 1 中記下的設定。如果部分虛擬機器已手動指派給代理程式，請再次指派它們，如「**虛擬機器繫結**」中所述。
一旦完成代理程式設定之後，套用至舊代理程式的保護計劃就會自動重新套用至新代理程式。
6. 啟用應用程式感知備份的計劃需要重新輸入客體作業系統認證。編輯這些計劃，然後重新輸入認證。
7. 備份 ESXi 設定的計劃需要重新輸入 "root" 密碼。編輯這些計劃，然後重新輸入密碼。

在電腦上更新網路保護定義

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

將**[更新者]**角色指派給代理程式

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

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]**。

7.15.2 自動更新代理程式

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

在執行下列任何作業系統的電腦上支援自動更新：

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

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

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

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

啟用自動更新之後，您可以設定下列選項：

- **更新通道**

更新通道可定義將使用的代理程式版本：最新版本還是先前版本的最新版本。

- **維護時段**

維護時段可定義安裝更新的時間。如果已停用維護時段，則可以隨時執行更新。

即使是在已啟用的維護時段內，當代理程式正在執行下列任何作業時，也不會安裝更新：

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

若要自訂自動更新設定

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

若要移除自訂自動更新設定

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

若要檢查自動更新狀態

1. 在服務主控台中, 移至 **[設定]>[代理程式]**。
2. 按一下表格右上角的齒輪圖示, 然後確認已選擇 **[自動更新]** 核取方塊。
3. 檢查 **[自動更新]** 欄中顯示的狀態。

7.16 防止未經授權者解除安裝或修改代理程式

您可以在保護計劃中啟用 **[密碼保護]** 設定, 以保護 Windows 用代理程式, 免於未經授權者解除安裝或修改。此設定僅適用於啟用 **[自我保護]** 設定時。

若要啟用密碼保護

1. 在保護計劃中, 展開 **[防毒和反惡意程式碼保護]** 模組 (適用於 Cyber Backup 版本的 **Active Protection** 模組)。
2. 按一下 **[自我保護]** 並確認已啟用 **[自我保護]** 開關。

3. 啟用 **[密碼保護]** 開關。
4. 在開啟的視窗中，複製您需要解除安裝或修改受保護之 Windows 用代理程式元件的密碼。
此密碼是唯一的，而且您關閉此視窗之後，將無法復原該密碼。如果您遺失或忘記此密碼，可以編輯保護計劃並建立新的密碼。
5. 按一下**[關閉]**。
6. 在 **[自我保護]** 窗格中，按一下 **[完成]**。
7. 儲存保護計劃。

系統將會為套用此保護計劃的電腦啟用密碼保護。密碼保護僅適用於 Windows 用代理程式 15.0.25851 版或更新版本。電腦必須在線上。

您可以將已啟用 [密碼保護] 的保護計劃套用到執行 macOS 的電腦，但不會提供任何保護。您無法將這種計劃套用到執行 Linux 的電腦。

此外，您無法將已啟用 [密碼保護] 的多個保護計劃套用到相同的 Windows 電腦。若要瞭解如何解決可能的衝突，請參閱[解決計劃衝突](#)。

若要在現有的保護計劃中變更密碼

1. 在保護計劃中，展開 **[防毒和反惡意程式碼保護]** 模組 (適用於 Cyber Backup 版本的 **Active Protection** 模組)。
2. 按一下 **[自我保護]**。
3. 按一下 **[建立新密碼]**。
4. 在開啟的視窗中，複製您需要解除安裝或修改受保護之 Windows 用代理程式元件的密碼。
此密碼是唯一的，而且您關閉此視窗之後，將無法復原該密碼。如果您遺失或忘記此密碼，可以編輯保護計劃並建立新的密碼。
5. 按一下**[關閉]**。
6. 在 **[自我保護]** 窗格中，按一下 **[完成]**。
7. 儲存保護計劃。

7.17 解除安裝代理程式

7.17.1 在 Windows 中

如果您要移除個別產品元件 (例如，其中一個代理程式或網路保護監視器)，請執行 **[所用 Windows 用代理程式]** 安裝程式、選擇修改產品，然後清除您要移除的元件選項。安裝程式的連結會在 **[下載]** 頁面中出現 (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。

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 Protection Agent]** > **[解除安裝]**。
3. **[適用於受密碼保護的代理程式]** 指定您解除安裝代理程式所需的密碼，然後按一下 **[下一步]**。
4. **[選用]** 選擇 **[移除記錄和組態設定]** 核取方塊。

如果您計劃再次安裝代理程式，請清除此核取方塊。如果您選取該核取方塊，電腦可能會在服務主控台中複製，且舊電腦的備份可能無法與新電腦產生關聯。

5. 按一下 **[解除安裝]**。

7.17.2 在 Linux 中

1. 以 root 使用者身分執行 `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall`。
2. [選用] 選擇 **[清理所有產品蹤跡 (移除產品記錄、工作、儲藏庫和組態設定)]** 核取方塊。
如果您計劃再次安裝代理程式，請清除此核取方塊。如果您選取該核取方塊，電腦可能會在服務主控台中複製，且舊電腦的備份可能無法與新電腦產生關聯。
3. 確認選項無誤。

7.17.3 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。

7.17.4 移除 VMware 用代理程式 (虛擬裝置)

1. 啟動 vSphere Client 並登入 vCenter Server。
2. 若虛擬裝置 (VA) 已開啟，請用滑鼠右鍵按一下，然後按一下 **[電源] > [關閉]**。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。
5. [選用] 若您計劃將再次安裝此代理程式，請略過此步驟。否則，在服務主控台中，按一下 **[備份儲存] > [位置]**，然後刪除對應本機連接的存放區的位置。

7.17.5 從服務主控台移除電腦

解除安裝代理程式之後，將會從 Cyber Protection 服務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服務主控台移除。

但是，如果在此作業期間失去與服務的連線 (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服務主控台中。在此情況下，您需要從服務主控台手動移除該電腦。

從服務主控台手動移除電腦

1. 以系統管理員身分登入 Cyber Protection 服務。
2. 在服務主控台中, 移至 **[設定]** > **[代理程式]**。
3. 選擇安裝代理程式所在的電腦。
4. 請按一下 **[刪除]**。

7.18 保護設定

若要設定 Cyber Protection 的一般保護設定, 移至服務主控台其中的 **[設定]** > **[保護]**。

7.18.1 元件自動更新

根據預設, 所有代理程式都可以連線至網際網路, 並下載更新。

系統管理員可以在環境中選擇一或數個代理程式, 並為其指派 **[更新者]** 角色, 以便將網路頻寬流量降至最低。因此, 專用的代理程式將會連線至網際網路, 並下載更新。其他所有代理程式將會使用對等技術連線至專用的更新程式代理程式, 然後從中下載更新。

如果環境中沒有專用的更新程式代理程式, 或者無法在大約五分鐘內建立與專用更新程式代理程式的連線, 則沒有 **[更新者]** 角色的代理程式將會連限制網際網路。

將 **[更新者]** 角色指派給代理程式之前, 請確認執行代理程式所在電腦的功能夠強大, 而且具備穩定的高速網際網路連線以及足夠的磁碟空間。

準備 **[更新者]** 角色的電腦

1. 在您打算啟用 **[更新者]** 角色的代理程式電腦上, 套用下列防火牆規則:
 - 輸入 (傳入) "updater_incoming_tcp_ports": 允許連線到所有防火牆設定檔 (公用、私人和網域) 的 TCP 連接埠 18018 和 6888。
 - 輸入 (傳入) "updater_incoming_udp_ports": 允許連線到所有防火牆設定檔 (公用、私人和網域) 的 UDP 連接埠 6888。
2. 重新啟動 Acronis Agent Core 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]** 角色指派給保護代理程式

1. 在服務主控台中, 移至 **[設定]** > **[代理程式]**。
2. 選擇您要將 **[更新者]** 角色指派給裝有代理程式的哪部電腦。
3. 按一下 **[詳細資料]**, 然後啟用 **[使用此代理程式下載並散佈修補程式和更新]** 開關。

對等更新運作方式如下。

1. 擁有 **[更新者]** 角色的代理程式依排程, 檢查服務提供者所提供的索引檔, 以更新核心元件。
2. 擁有 **[更新者]** 角色的代理程式開始下載更新, 並將其散佈至所有代理程式。

您可以將 **[更新者]** 角色指派給環境中的多個代理程式。因此, 如果擁有 **[更新者]** 角色的代理程式離線, 擁有此角色的其他代理程式可以當作定義更新的來源。

7.18.2 依排程更新 Cyber Protection 定義

在 **[排程]** 索引標籤上，您可以設定排程，以自動更新下列每個元件的 Cyber Protection 定義：

- 反惡意程式碼
- 弱點評估
- 修補程式管理

若要變更定義更新設定，請瀏覽至 **[設定] > [保護] > [保護定義更新] > [排程]**。

排程類型：

- **每日** – 定義在一週的哪幾天更新定義。
開始時間 – 選擇在哪個時間更新定義。
- **每小時** – 定義更細微的每小時排程，以進行更新。
執行週期 – 定義更新的週期。
從 ...到 – 定義特定的時間範圍，以進行更新。

7.18.3 視需要更新 Cyber Protection 定義

若要視需要更新特定電腦的 Cyber Protection 定義

1. 在服務主控台中，移至 **[設定] > [代理程式]**。
2. 選擇您要更新保護定義所在的電腦，然後按一下 **[更新定義]**。

7.18.4 快取儲存空間

快取資料的位置如下：

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

若要變更快取儲存設定，請瀏覽至 **[設定] > [保護] > [保護定義更新] > [快取儲存]**。

在 **[過期的更新檔案和修補程式管理資料]** 中，指定在哪個期限後移除快取資料。

代理程式的最大快取儲存空間大小 (GB)：

- **更新者角色** – 定義快取在具有 [更新者] 角色的電腦上的儲存空間大小。
- **其他角色** – 定義快取在其他電腦上的儲存空間大小。

7.18.5 遠端連線

若要透過 RDP 或 HTML 用戶端啟用與電腦的遠端連線

1. 在服務主控台中，移至 **[設定] > [保護]**。
2. 按一下 **[遠端桌面連線]**，然後啟用 **[遠端桌面連線]** 開關。

如果此開關遭到停用，則在服務主控台中將會隱藏 **[透過 RDP 用戶端連線]** / **[透過 HTML5 用戶端連線]** 選項，而且使用者將無法從遠端連線到電腦。此選項或影響貴組織的所有使用者。

若要啟用共用遠端連線

1. 在服務主控台中，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]** 選項將會出現在右側功能表中的 **[Cyber Protection 桌面]** 底下。當您在 **[裝置]** 索引標籤中選擇電腦時，右側功能表隨即開啟。

您可以按一下 **[共用遠端連線]**，以產生能夠與其他使用者共用的連結。此連結允許從遠端存取所選電腦。

7.19 變更電腦的服務配額

保護計劃第一次套用到電腦時，便會自動指派服務配額。

系統會根據受保護電腦的類型、其作業系統、所需的保護層級，以及配額可用性，指派最適當的配額。如果貴組織無法使用最適當的配額，則會指派次佳配額。例如，如果最適當的配額為 **Web 託管伺服器** 但無法使用，則會指派 **伺服器** 配額。

配額指派的範例：

- 執行 Windows Server 或 Linux 作業系統的實體機器會獲指派 **伺服器** 配額。
- 執行桌面 Windows 作業系統的實體機器會獲指派 **工作站** 配額。
- 執行已啟用 Hyper-V 角色之 Windows 10 的實體機器會獲指派 **工作站** 配額。
- 在虛擬桌面基礎架構上執行且客體作業系統內部安裝其保護代理程式 (例如，Windows 用代理程式) 的桌上型電腦會獲指派 **虛擬機器** 配額。如果無法使用 **虛擬機器** 配額，此類型的電腦也可以使用 **工作站** 配額。
- 在虛擬桌面基礎架構上執行且在無代理程式模式 (例如，VMware 用代理程式或 Hyper-V 用代理程式) 下備份的桌上型電腦會獲指派 **虛擬機器** 配額。
- Hyper-V 或 vSphere 伺服器會獲指派 **伺服器** 配額。
- 具有 cPanel 或 Plesk 的伺服器會獲指派 **Web 託管伺服器** 配額。根據網頁伺服器執行所在電腦的類型，如果無法使用 **Web 託管伺服器** 配額，也可以使用 **虛擬機器** 或 **伺服器** 配額。
- 即使是針對工作站，應用程式感知備份也需要使用 **伺服器** 配額。

您之後可以手動變更原始指派。例如，若要將更進階的保護計劃套用到相同的電腦，您可能需要升級電腦的服務配額。如果目前指派的服務配額不支援此保護計劃所需的功能，保護計劃將會失敗。

或者，如果您在指派原始配額之後購買更多合適的配額，則可以變更服務配額。例如，**工作站** 配額會被指派給虛擬機器。在您購買 **虛擬機器** 配額之後，可以手動將其指派給此機器，而不是指派原始的工作站配額。

您也可以釋出目前指派的服務配額，然後將此配額指派給其他機器。

您可以變更個別機器的服務配額，或一組機器的服務配額。

若要變更個別機器的服務配額

1. 在 Cyber Protection 服務主控台中, 移至 **[裝置]**。
2. 選擇所需的電腦, 然後按一下 **[詳細資料]**。
3. 在 **[服務配額]** 區段中, 按一下 **[變更]**。
4. 在 **[變更授權]** 視窗中, 選擇所需的服務配額或 **[無配額]**, 然後按一下 **[變更]**。

若要變更一組機器的服務配額

1. 在 Cyber Protection 服務主控台中, 移至 **[裝置]**。
2. 選擇多部機器, 然後按一下 **[指派配額]**。
3. 在 **[變更授權]** 視窗中, 選擇所需的服務配額或 **[無配額]**, 然後按一下 **[變更]**。

7.20 安裝在您環境中的 Cyber Protection 服務

Cyber Protection 會安裝下列部分或所有服務, 端視您所使用的 Cyber Protection 選項而定。

7.20.1 安裝在 Windows 中的服務

服務名稱	目的
Acronis Managed Machine Service	提供備份、復原、複寫、保留、驗證功能
Acronis Scheduler2 Service	針對特定活動執行排程工作
Acronis Active Protection Service	防禦勒索軟體
Acronis Cyber Protection Service	提供反惡意程式碼保護

7.20.2 安裝在 macOS 中的服務

服務的名稱與位置	目的
/Library/LaunchDaemons/com.acronis.aakore.plist	用於代理程式和管理元件間通訊的伺服器
/Library/LaunchDaemons/com.acronis.cyber-protect-service.plist	偵測惡意程式碼
/Library/LaunchDaemons/com.acronis.mms.plist	提供備份與復原功能
/Library/LaunchDaemons/com.acronis.schedule.plist	執行排程工作

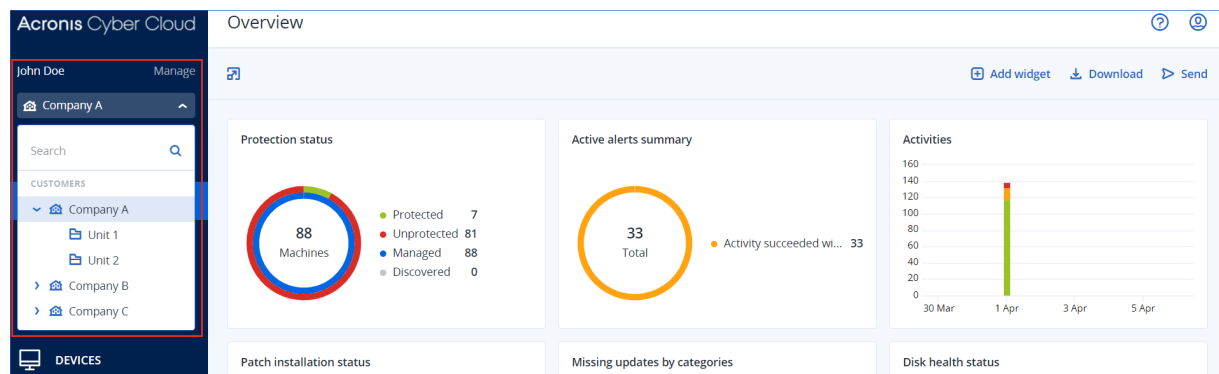
8 服務主控台

在服務主控台中，您可以管理裝置和保護計劃、變更保護設定、設定報告，或檢查備份儲存空間。

您可以在儀表板上找到有關保護的最重要資訊。

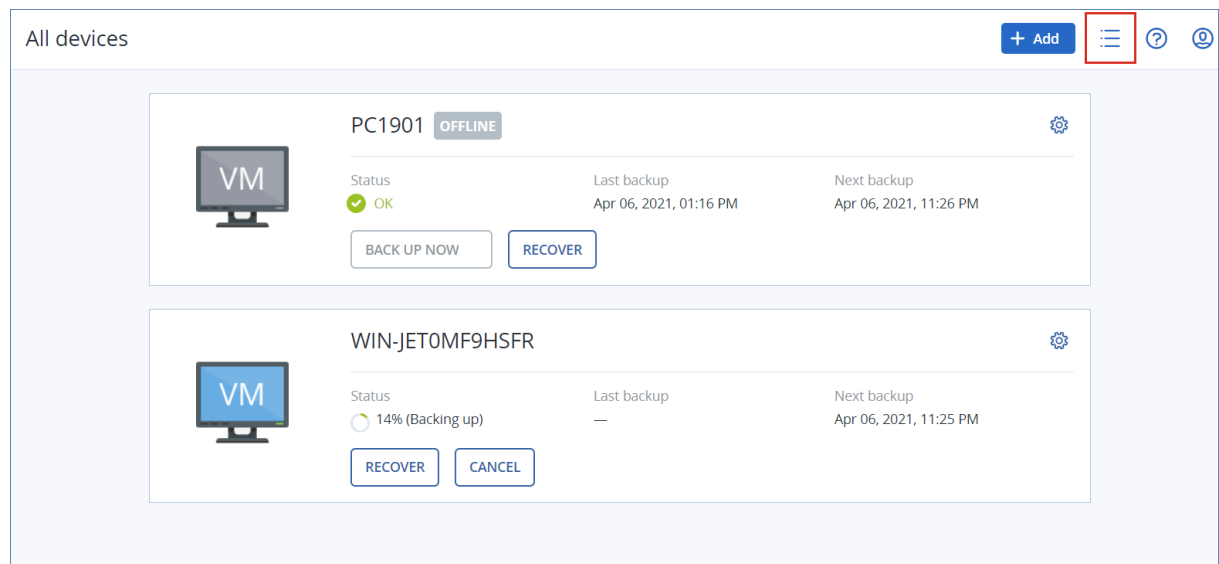
服務主控台可讓您存取其他 Cyber Protection 服務或功能，例如 File Sync & Share 或防毒和反惡意程式碼保護、修補程式管理、裝置控制和弱點評估。其類型與數量會隨著您的 Cyber Protection 授權而有所不同。

視您的存取權限而定，您可以為一個或多個客戶租用戶，或租用戶中的單位，管理保護。若要切換階層層級，請使用導覽功能表中的下拉式清單。系統僅會顯示您可以存取的層級。若要移至管理入口網站，請按一下 **[管理]**。



[裝置] 區段可在簡易檢視和表格檢視中使用。若要在這兩者之間切換，請按一下右上角對應的圖示。

簡易檢視畫面只會顯示少數電腦。



當電腦數目變多時，系統就會自動啟用表格檢視畫面。

All devices							
Search				Loaded: 2 / Total: 2 View: Standard			
☐	Type	Name ↑	Account	#CyberFit Score	Status	Last backup	Next backup
	VM	PC1901	CompanyA	625/850	OK	Apr 06 01:16:14 PM	Apr 06 11:26:28 PM
	VM	WIN-JET0MF9HSFR	CompanyA	625/850	14% (Backing up)	Never	Apr 06 11:25:23 PM

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，其在服務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。

從服務主控台中刪除電腦

1. 選擇所需電腦旁邊的核取方塊。
2. 按一下 **[刪除]**，然後確認您的選擇。

重要事項

從服務主控台中刪除電腦並不會解除安裝該電腦上的保護代理程式，而且不會刪除套用至此電腦的保護計劃。系統也將保留所刪除電腦的備份。

下列虛擬化平台上的 ESXi 主機和虛擬機器可以由未安裝在其上的代理程式備份，亦即在無代理程式模式下備份：

- Hyper-V
- VMware
- Virtuozzo Hybrid Infrastructure
- Scale Computing
- Red Hat Virtualization/oVirt

您無法個別刪除這類電腦。若要刪除它們，您必須尋找安裝個別代理程式 (Hyper-V 用代理程式、VMware 用代理程式、Virtuozzo Hybrid Infrastructure 用代理程式、Scale Computing 用代理程式或 oVirt 用代理程式) 所在的電腦，然後加以刪除。

刪除不含代理程式的虛擬機器或 ESXi 主機

1. 在 **[裝置]** 底下，選擇 **[所有裝置]**。
2. 按一下右上角的齒輪圖示，然後啟用 **[代理程式]** 欄。

All devices

+ Add

Search

Loaded: 2 / Total: 2 View: Last used

Type	Name ↑	Account	#CyberFit Score	Status	Last backup	Next backup	
VM	PC1901	CompanyA	625/850	OK	Apr 06 01:16:14		
VM	WIN-JETOMF9HSFR	CompanyA	625/850	16% (Backing up)	Never		

- General
- Hardware
- System
 - Motherboard
 - Motherboard serial num
 - BIOS version
 - Organization
 - Owner
 - Domain
 - Agent
 - Operating system
 - Operating system build
- Plans

3. 在 **[代理程式]** 欄中, 檢查安裝個別代理程式所在電腦的名稱。
4. 從服務主控台中刪除此電腦。這也將刪除其代理程式所備份的所有電腦。
5. 從已刪除的電腦中解除安裝代理程式, 如 "解除安裝代理程式" (第 111 頁) 中所述。

9 管理工作負載

本節描述如何在服務主控台中管理工作負載。

9.1 各 Device 群組

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

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。

9.1.1 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。

9.1.2 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。

9.1.3 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。

9.1.4 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]**。

9.1.5 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。

注意事項

您無法為 [所有裝置] 群組建立動態群組。

2. 透過使用搜尋欄位來搜尋裝置。您可以使用下述多個搜尋條件和運算子。
3. 按一下搜尋欄位旁邊的 **[另存新檔]**。

注意事項

部分搜尋條件不支援建立群組。請參閱以下「搜尋條件」一節中的表格。

4. 指定群組名稱, 然後按一下 **[確定]**。

搜尋條件

下表摘述可用的搜尋條件。

準則	含義	搜尋查詢範例	支援建立群組
name	- 實體機器的主機名稱 - 虛擬機器名稱 - 資料庫名稱 - 信箱的電子郵件地址	name = 'en-00'	是
comment	裝置的註解。您可以自動或手動指定註解。 預設值： - 若是執行 Windows 的實體電腦，則會自動複製 Windows 中的電腦描述作為註解。系統每 15 分鐘會同步一次這個值。 - 其他裝置留空。 注意事項 在註解欄位中有手動新增的文字時，便會停用與 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： <pre>net stop mms</pre> <pre>net start mms</pre> 若要檢視裝置註解，在 [裝置] 底下選取裝置、按一下 [詳細資料]，然後找出 [註解] 區段。 若要手動新增或變更註解，按一下 [新增] 或 [編輯]。 若是已安裝保護代理程式的裝置，則有兩個不同的註解欄位： - 代理程式註解 - 若是執行 Windows 的實體電	comment = 'important machine' comment = '' (不含註解所有電腦)	是

	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。 • 裝置註解 ◦ 如果代理程式註解是自動指定的，則系統會將其複製為裝置註解。系統不會將手動新增的代理程式註解複製為裝置註解。 ◦ 系統不會將裝置註解複製為代理程式註解。 裝置可以指定其中一個或兩個註解，或者將兩個註解都留空。如果指定兩個註解，則裝置註解優先。 若要檢視代理程式註解，在 [裝置] > [代理程式] 底下選取已安裝代理程式的裝置、按一下 [詳細資料]，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]。 注意事項 在註解欄位中有手動新增的文字時，便會停用與 Windows 描述自動同步。若要再次啟用，請清除您已經新增的註解。		
ip	IP 位址 (僅適用於實體機器)。	ip RANGE ('10.250.176.1', '10.250.176.50')	是
memorySize	RAM 的大小，以 MB 為單位。	memorySize < 1024	是
diskSize	硬碟大小，以 GB 或 MB 為單位 (僅適用於實體機器)。	diskSize < 300GB diskSize >= 3000000MB	否
insideVm	內部具有代理程式的虛擬機器。 可能的值： • true • false	insideVm = true	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。 注意 在 Windows 伺服器上指派網域控制站角色時, osProductType 會從 "server" 變更為 "dc"。這類電腦將不會包含在 filter "osProductType='server' 的搜尋結果中。 'server' 'workstation'	osProductType = 'server'	是
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
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。	state = 'backup'	否

	可能的值： • 'idle' • 'interactionRequired' • 'canceling' • 'backup' • 'recover' • 'install' • 'reboot' • 'failback' • 'testReplica' • 'run_from_image' • 'finalize' • 'failover' • 'replicate' • 'createAsz' • 'deleteAsz' • 'resizeAsz'		
protectedByPlan	由保護計劃保護的裝置具有給定 ID。 若要查看計劃 ID, 請在 [管理] > [保護計劃] 中選擇一個計劃, 按一下 [狀態] 欄中的列, 然後按一下狀態名稱。將建立具有計劃 ID 的新搜尋。	protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否
okByPlan	由保護計劃保護的裝置具有給定 ID, 且具有 [正常] 狀態。	okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否
errorByPlan	由保護計劃保護的裝置具有給定 ID, 且具有 [錯誤] 狀態。	errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否
warningByPlan	由保護計劃保護的裝置具有給定 ID, 且具有 [警告] 狀態。	warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否
runningByPlan	由保護計劃保護的裝置具有給定 ID, 且具有 [執行中] 狀態。	runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否
interactionByPlan	由保護計劃保護的裝置具有給定 ID, 且具有 [需要互動] 狀態。	interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否
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 > '2020-03-11' lastBackupTime <= '2019-03-11 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 >= '2020-03-11'	否
nextBackupTime*	下次備份的時間。 格式為 'YYYY-MM-DD HH:MM'。	nextBackupTime >= '2021-03-11'	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
resourceType	資源類型。 可能的值: 'machine' 'virtual_machine.vmwesx' 'virtual_machine.mshyperv' 'virtual_machine.scale' 'virtual_machine.hci' 'virtual_machine.ovirt' - virtual_machine.pcs	resourceType = 'machine' resourceType in ('mssql_aag_database', 'mssql_database')	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'
OR	邏輯分離運算子。	state = 'backup' OR state =

		'interactionRequired'
NOT	邏輯否定運算子。	NOT(osProductType = 'workstation')
LIKE 'wildcard pattern'	此運算子用來測試表示式是否符合萬用字元模式。此運算子不區分大小寫。 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_'
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。此運算子區分大小寫。	osType IN ('windows', 'linux')
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')
<	小於運算子。	memorySize < 1024
>	大於運算子。	diskSize > 300GB
<=	小於或等於運算子。	lastBackupTime <= '2019-03-11 00:15'
>=	大於或等於運算子。	nextBackupTime >= '2021-03-11'
= or ==	等於運算子。	osProductType = 'server'
!= or <>	不等於運算子。	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'

9.1.6 將保護計劃套用到群組

- 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。
- 選擇您要套用保護計劃的群組。
- 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。
- 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「[保護計劃](#)」中所述。

10 多租用戶支援

Cyber Protection 支援多租用戶。也就是說，租用戶系統管理員/使用者可以管理與其租用戶或其子租用戶(單位)相關的物件。單位的系統管理員/使用者無法管理父租用戶的物件。

例如，客戶系統管理員已建立一個保護計劃，並將其套用到電腦。客戶系統管理員也可以管理單位系統管理員所建立的保護計劃。不過，單位系統管理員無法管理客戶系統管理員所建立的保護計劃。單位系統管理員可以建立不會與客戶系統管理員計劃發生衝突的私有保護計劃。

多租用戶也意味著租用戶系統管理員/使用者可以看到與此租用戶或其子租用戶(單位)相關的所有物件。單位的系統管理員/使用者無法看到父租用戶的物件。

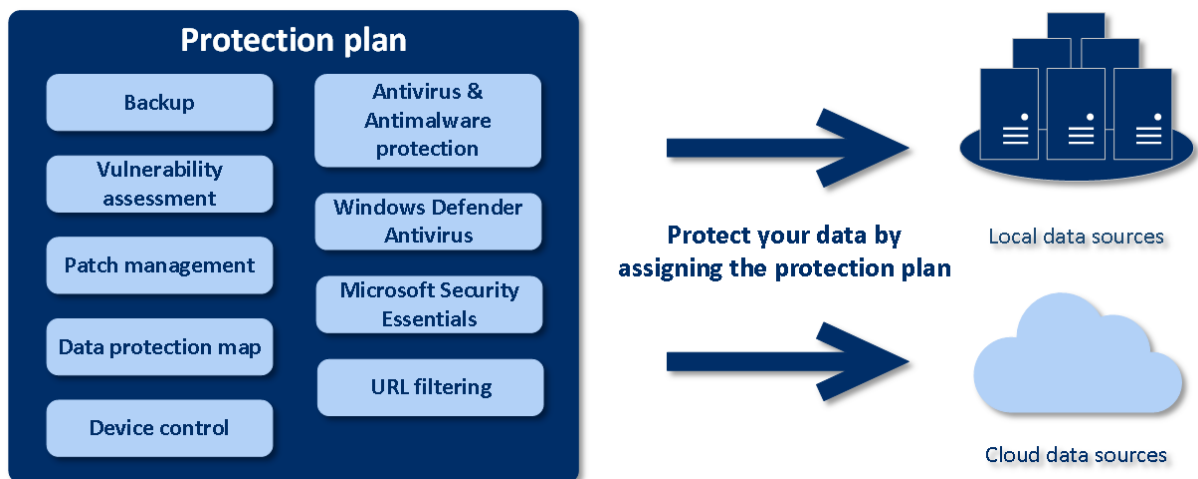
例如，修補程式清單、隔離區、威脅摘要、警示和活動中所顯示的資料僅會針對目前的租用戶及其子租用戶顯示。與父租用戶相關的資料則不會顯示。

11 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。
- **"災難復原"** (第 341 頁) – 可讓您在雲端站台上啟動確切的電腦複本，並將工作負載從損毀的原始電腦切換到雲端的復原伺服器。
- **防毒和反惡意程式碼保護** – 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、Linux、macOS、Microsoft 協力廠商產品和 macOS 協力廠商產品中的弱點，並對您發送通知。
- **修補程式管理** – 可讓您安裝電腦上 Microsoft、Linux、macOS、Microsoft 協力廠商產品和 macOS 協力廠商產品的修補程式和更新，以終止探索到的弱點。
- **資料保護圖** – 可讓您探索資料以監視重要檔案的保護狀態。
- **裝置控制** – 可讓您指定允許或限制使用者在電腦上使用的裝置。
- **進階版資料洩漏防禦** – 根據資料流程原則，可防止透過週邊裝置 (例如印表機或卸除式儲存裝置) 或內部和外部網路傳輸，洩漏敏感資料。

使用保護計劃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。



11.1 建立保護計劃

保護計劃可在其建立時 (或之後) 套用至多個工作負載。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。

保護計劃可以透過下列方式建立。

- 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 **[管理]** 區段中 – 當您建立計劃，然後選擇要套用的電腦時。

在 **[裝置]** 區段中建立第一個保護計劃

1. 在服務主控台中，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]**。
保護計劃預設設定隨即開啟。
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]**。

若要視需要執行模組 (例如 **[備份]**、**[防毒和反惡意程式碼保護]**、**[弱點評估]**、**[修補程式管理]** 或 **[資料保護圖]**) 時，按一下 **[立即執行]**。

觀看 [建立第一個保護計劃](#) 操作說明影片。

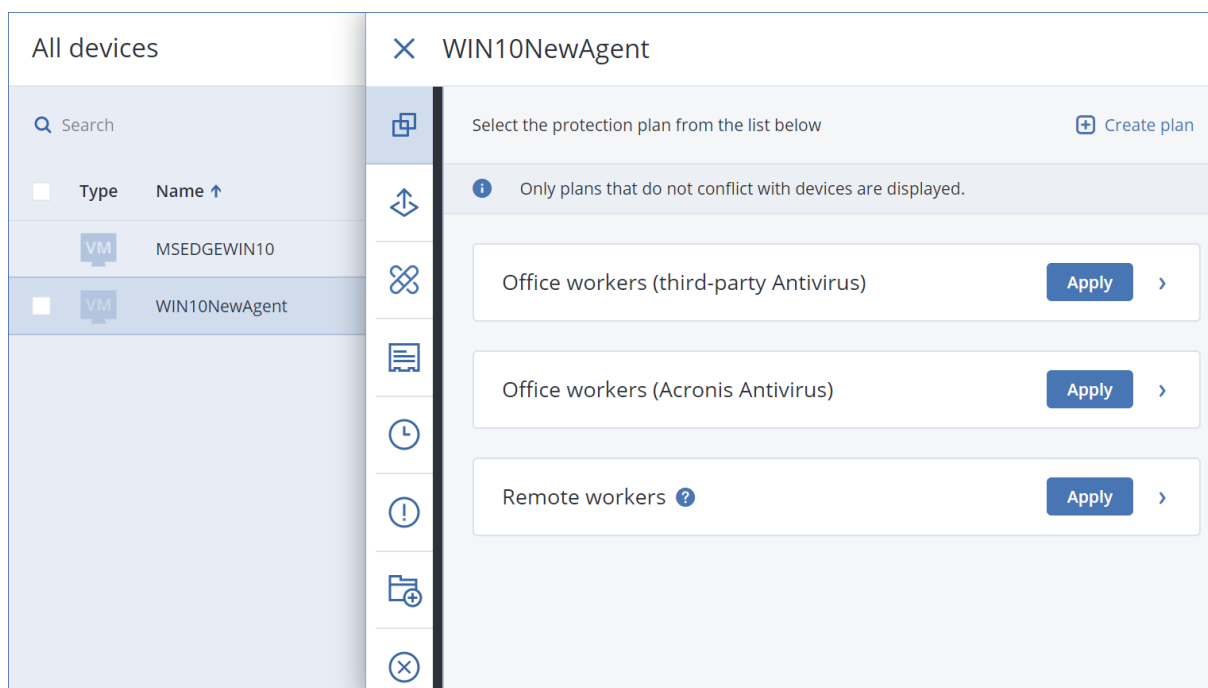
如需有關災難復原模組的詳細資訊，請參閱 "建立災難復原保護計劃" (第 345 頁)。

如需有關裝置控制模組的詳細資訊，請參閱 "裝置控制" (第 489 頁)。

11.2 預設保護計劃

預設提供的三個預先設定的計劃，可確保快速保護特定工作負載：

- 辦公室工作者 (Acronis Antivirus)
此計劃已針對在辦公室工作，且慣用 Acronis 防毒軟體的使用者進行最佳化。
- 辦公室工作者 (第三方防毒軟體)
此計劃已針對在辦公室工作，且慣用第三方防毒軟體的使用者進行最佳化。主要差異在於此計劃已停用 **[防毒和反惡意程式碼保護]** 模組以及 **[Active Protection]**。
- 遠端工作者
此計劃專門針對從遠端工作的使用者進行最佳化。其擁有更頻繁的工作 (例如，備份、反惡意程式碼保護、弱點評估)、更嚴格的保護動作，以及最佳化的效能與電源選項。
- 資料洩漏防禦
此計劃包含可在受保護的工作站上分析資料傳輸的內容和脈絡的模組。根據資料流程原則，模組可防止透過週邊裝置 (例如印表機或卸除式儲存裝置) 或內部和外部網路傳輸，洩漏敏感資料。資料流程原則規則可以由公司系統管理員手動定義，也可以由進階版資料洩漏防禦計劃的自我學習功能自動定義。



套用預設保護計劃

1. 在服務主控台中，移至 **[裝置]** > **[所有裝置]**。
2. 選擇您要保護的電腦。
3. 按一下 **[保護]**。
4. 選擇其中一個預設計劃，然後按一下 **[套用]**。

注意事項

您也可以按一下 **[建立計劃]**，設定您自己的保護計劃。

修改已套用的預設保護計劃

1. 在服務主控台中，移至 **[管理]** > **[保護計劃]**。
2. 選擇您要修改的計劃，然後按一下 **[編輯]**。
3. 修改包含在此計劃中的模組或其選項，然後按一下 **[儲存]**。

重要事項

您無法變更現有保護計劃的部分設定。

11.2.1 預設計劃選項

預先設定的計劃為每個模組*使用預設選項，但進行下列修改：

模組和選項/計劃	辦公室工作者 (Acronis Antivirus)	辦公室工作者 (第三方防毒軟體)	遠端工作者
"備份" (第 142 頁)			

要備份的內容	整部電腦	整部電腦	整部電腦
連續資料保護 (CDP)	停用	停用	Enabled
備份目標位置	雲端儲存	雲端儲存	雲端儲存
備份配置	一律增量備份 (單一檔案)	一律增量備份 (單一檔案)	一律增量備份 (單一檔案)
排程	預設每日排程	預設每日排程	每日:每週一到週五中午 12:00 另外啟用的選項和開始條件: • 如果電腦關閉,則在電腦啟動時執行遺漏的工作 • 從睡眠或休眠模式中喚醒,開始進行排程的備份 • 節省電池電力:不要在使用電池電力時開始 • 不要在使用計量付費連線時開始
保留備份的時間長度	每月:12 個月 每週:4 週 每日:7 天	每月:12 個月 每週:4 週 每日:7 天	每月:12 個月 每週:4 週 每日:7 天
備份選項	預設選項	預設選項	預設選項,加上: 效能和備份視窗(綠色組): • CPU 優先順序:低 • 輸出速度:50%
"防毒和反惡意程式碼保護"(第 400 頁)			
排程掃描	掃描類型:快速	不適用	掃描類型:完整 另外啟用的選項和開始條件: • 如果電腦關閉,則在電腦啟動時執行遺漏的工作 • 從睡眠或休眠模式中喚醒,開始進行排程的備份 • 節省電池電力:不要在使用電池電力時開始
"URL 篩選"(第 415 頁)			
惡意網站存取	一律詢問使用者	一律詢問使用者	封鎖
"弱點評估"(第 449 頁)			

	預設	預設	預設
"修補程式管理" (第 455 頁)			
排程	預設	預設	每日:每週一到週五下午 02:20
預先更新備份	關閉	關閉	開啟
"資料保護圖" (第 482 頁)			
擴展名	預設選項	預設選項	預設選項, 加上: 影像: • .bmp • .png • .ico • .wbmp • .gif • .bmp • .xcf • .psd • .tiff • .jpeg, .jpg • .dwg 音訊: • .wav • .aif, .aifc, .aiff • .au, .snd • .mid, .midi • .mid • .mpga, .mp3 • .oga • .flac • .oga • .oga • .opus • .oga • .spx • .oga • .ogg • .ogx • .ogx • .mp4
"裝置控制" (第 489 頁)			

裝置控制	停用	停用	停用
"進階版資料洩漏防禦" (第 429 頁)			
作業模式	觀察 (全部允許)	觀察 (全部允許)	觀察 (全部允許)
進階設定	安全性層級:基本 允許名單中的通道:無 允許名單中的遠端主機:無 允許名單中的應用程式:無	安全性層級:基本 允許名單中的通道:無 允許名單中的遠端主機:無 允許名單中的應用程式:無	安全性層級:基本 允許名單中的通道:無 允許名單中的遠端主機:無 允許名單中的應用程式:無

* 預設保護計劃中的模組數目在不同的 Cyber Protection 服務版本之間可能有所不同。

11.3 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。

11.3.1 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，您可以套用僅在計劃中啟用 [防毒和反惡意程式碼保護] 模組的計劃，以及僅包含 [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。如果在已套用的保護計劃中有類似的已啟用模組，您必須解決這類模組之間的衝突。

11.3.2 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] > <particular_device> > [詳細資料] > [服務配額]**，然後撤銷現有的配額並指派一個新配額。

11.4 具有保護計劃的作業

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，您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，您必須知道此計劃的名稱、從可用計劃清單中選擇該計劃，然後將其重新套用至所需的裝置。

- 停止計劃。

此動作將會停止套用計劃所在所有工作負載上的所有執行中備份作業。備份將會根據在計劃中設定的排程，再次開始。

反惡意程式碼掃描不會受到影響，而且將會根據在計劃中設定的排程繼續進行。

- 匯入/匯出計劃。

注意事項

您可以匯入使用 Cyber Protection 9.0 (2020 年 3 月發行) 和更新版本建立的保護計劃。在舊版產品中建立的計劃與 9.0 版和更新版本不相容。

- 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. 選擇要套用的保護計劃，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。

12 電腦的 #CyberFit 分數

#CyberFit 分數為您提供一個安全評估和評分機制，可評估電腦的安全態勢。此分數可識別 IT 環境中的安全漏洞以及向端點開放的攻擊媒介，並以報告的形式提供改進的建議動作。所有 Cyber Protect 版本都提供這項功能。

下列系統支援 #CyberFit 分數功能：

- Windows 7 (第一版) 和更新版本
- Windows Server 2008 R2 和更新版本

12.1 運作原理

電腦上安裝的保護代理程式會執行安全評估，並計算電腦的 #CyberFit 分數。系統會定期自動重新計算電腦的 #CyberFit 分數。

12.1.1 #CyberFit 評分機制

系統會根據下列指標，計算電腦的 #CyberFit 分數：

- 反惡意程式碼保護 0-275
- 備份保護 0-175
- 防火牆 0-175
- 虛擬私人網路 (VPN) 0-75
- 完整磁碟加密 0-125
- 網路安全 0-25

電腦的 #CyberFit 分數上限為 850。

公制	評估的內容為何？	對使用者的建議	評分
反惡意程式碼	代理程式會檢查電腦上是否安裝反惡意程式碼軟體。	發現： • 您已啟用反惡意程式碼保護 (+275 分) • 您沒有反惡意程式碼保護，您的系統可能有風險 (0 分) #CyberFit 分數提供的建議： 您應該在電腦上安裝並啟用反惡意程式碼解決方案，才能持續防禦安全風險。 如需建議的反惡意程式碼解決方案清單，請參閱 AV-Test 或 AV-Comparatives 等網站。	275 - 電腦上已安裝反惡意程式碼軟體 0 - 電腦上未安裝反惡意程式碼軟體
備份	代理程式會檢查電腦上是否安裝備份解決方案。	發現： • 您有可保護您資料的備份解決方案 (+175 分) • 找不到備份解決方案，您的資料可能有風險 (0 分)	175 - 電腦上已安裝備份解決方案 0 - 電腦上未安

		#CyberFit 分數提供的建議： 建議您定期備份資料以防止資料遺失或勒索軟體攻擊。以下是您應該考慮使用的一些備份解決方案： • Acronis Cyber Protect / Cyber Backup / True Image • Windows Server Backup (Windows Server 2008 R2 和更新版本)	裝備份解決方案
防火牆	代理程式會檢查環境中是否有防火牆並已啟用。 代理程式會執行下列操作： 1.檢查 Windows 防火牆和網路保護是否已開啟公用防火牆。 2. 檢查 Windows 防火牆和網路保護是否已開啟私人防火牆。 3.檢查協力廠商防火牆解決方案/代理程式是否已停用 Windows 公用和私人防火牆。	發現： • 您已針對公用網路和私人網路啟用防火牆，或找到協力廠商防火牆解決方案 (+175 分) • 您僅針對公用網路啟用防火牆 (+100 分) • 您僅針對私人網路啟用防火牆 (+75 分) • 您未啟用防火牆，您的網路連線不安全 (0 分) #CyberFit 分數提供的建議： 建議為您的公用和私人網路啟用防火牆，以提高對系統上惡意攻擊的安全保護。以下是根據您的安全性需求和網路架構，提供有關設定 Windows 防火牆的詳細指南： 適用於使用者/員工的指南： 如何在 PC 上設定 Windows Defender 防火牆 如何在 PC 上設定 Windows 防火牆 適用於系統管理員和工程師的指南： 如何使用進階安全性部署 Window Defender 防火牆 如何在 Windows 防火牆中建立進階規則	100 - Windows 公用防火牆已啟用 75 - Windows 私人防火牆已啟用 175 - Windows 公用和私人防火牆已啟用或者第三方防火牆解決方案已啟用 0 - 未啟用 Windows 防火牆，也未啟用協力廠商防火牆解決方案
虛擬私人網路 (VPN)	代理程式會檢查電腦上是否已安裝 VPN 解決方案，且是否已啟用 VPN 並在執行中。	發現： • 您有 VPN 解決方案，因此可以在公用網路和共用網路上安全地接收和傳送資料 (+75 分) • 找不到 VPN 解決方案，您與公用網路和共用網路的連線不安全 (0 分) #CyberFit 分數提供的建議： 建議使用 VPN 存取您的公司網路和機密資料。使用 VPN 確保您的通訊安全並維持私密性至關重要，尤其是當您使用咖啡店、圖書館、機場等地方的免費網路存取時。以下是您應該考慮使用的一些 VPN 解決方案： • Acronis Business VPN • OpenVPN • Cisco AnyConnect • NordVPN	75 - 已啟用 VPN 並在執行中 0 - 未啟用 VPN

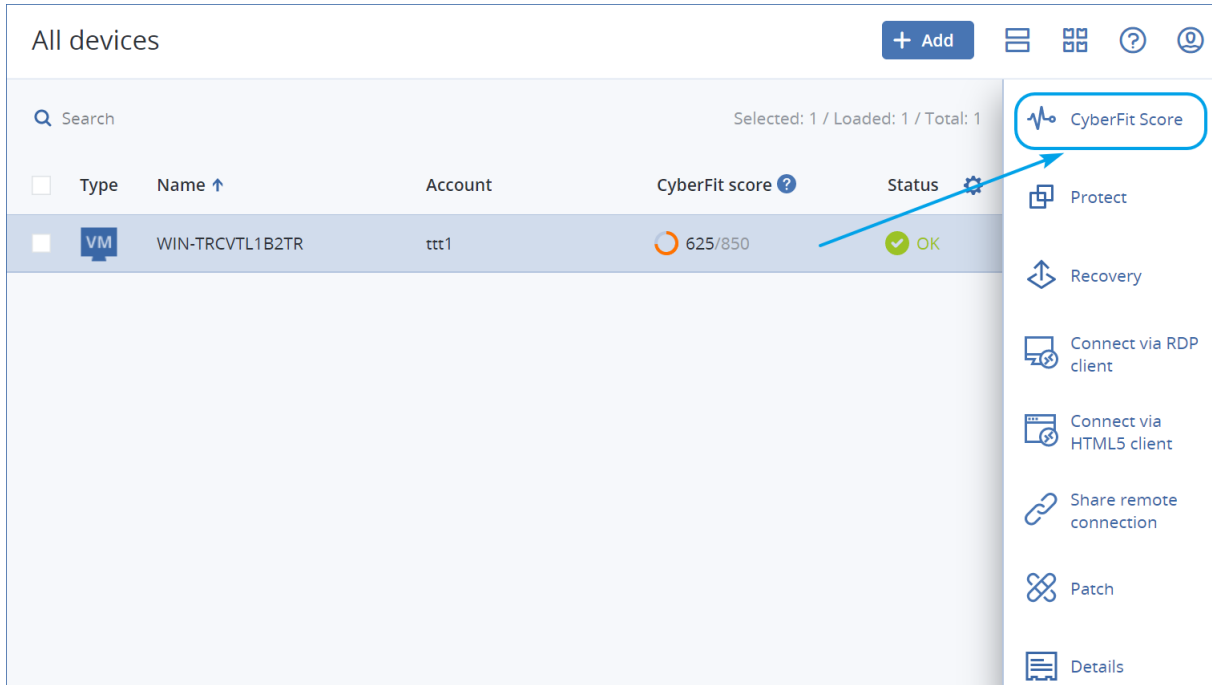
		• TunnelBear • ExpressVPN • PureVPN • CyberGhost VPN • Perimeter 81 • VyprVPN • IPVanish VPN • Hotspot Shield VPN • Fortigate VPN • ZYXEL VPN • SonicWall GVPN • LANCOM VPN	
磁碟加密	代理程式會檢查電腦是否已啟用磁碟加密。 代理程式會檢查是否已開啟 Windows BitLocker。	發現： • 您已啟用完整磁碟加密，您的電腦受到保護，免受實體竄改影響 (+125 分) • 只有部分硬碟機經過加密，您的電腦可能面臨實體竄改的風險 (+75 分) • 找不到磁碟加密，您的電腦面臨實體竄改的風險 (0 分) #CyberFit 分數提供的建議： 建議開啟 Windows BitLocker 以提高資料和檔案的保護。 指南：如何在 Windows 上開啟裝置加密	125 - 所有磁碟都經過加密 75 - 您的磁碟中至少有一個磁碟經過加密，但也有未加密的磁碟 0 - 未加密任何磁碟
網路安全 (遠端伺服器的輸出 NTLM 流量)	代理程式會檢查電腦對遠端伺服器是否有限制輸出 NTLM 流量。	發現： • 遠端伺服器的輸出 NTLM 流量遭到拒絕，您的認證受到保護 (+25 分) • 遠端伺服器的輸出 NTLM 流量未遭到拒絕，您的認證可能容易暴露 (0 分) #CyberFit 分數提供的建議： 建議拒絕遠端伺服器的所有輸出 NTLM 流量，以獲得更好的安全防護。您可以依照下列連結，找到如何變更 NTLM 設定以及新增例外的相關資訊。 指南：限制遠端伺服器的輸出 NTLM 流量	25 - 輸出 NTLM 流量設為 [全部拒絕] 0 - 輸出 NTLM 流量設為另一個值

根據授予每個指標的加總分數，電腦的 #CyberFit 總分可以滿足以下反映端點保護層級的其中一個評分：

- 0 - 579 - 差
- 580 - 669 - 尚可
- 670 - 739 - 好

- 740 - 799 - 非常好
- 800 - 850 - 非常出色

您可以在服務主控台中看到電腦的 #CyberFit 分數:移至 **[裝置]** > **[所有裝置]**。在裝置清單中, 您可以看到 **[#CyberFit 分數]** 欄。您也可以為電腦執行 #CyberFit 分數掃描以檢查其安全態勢。

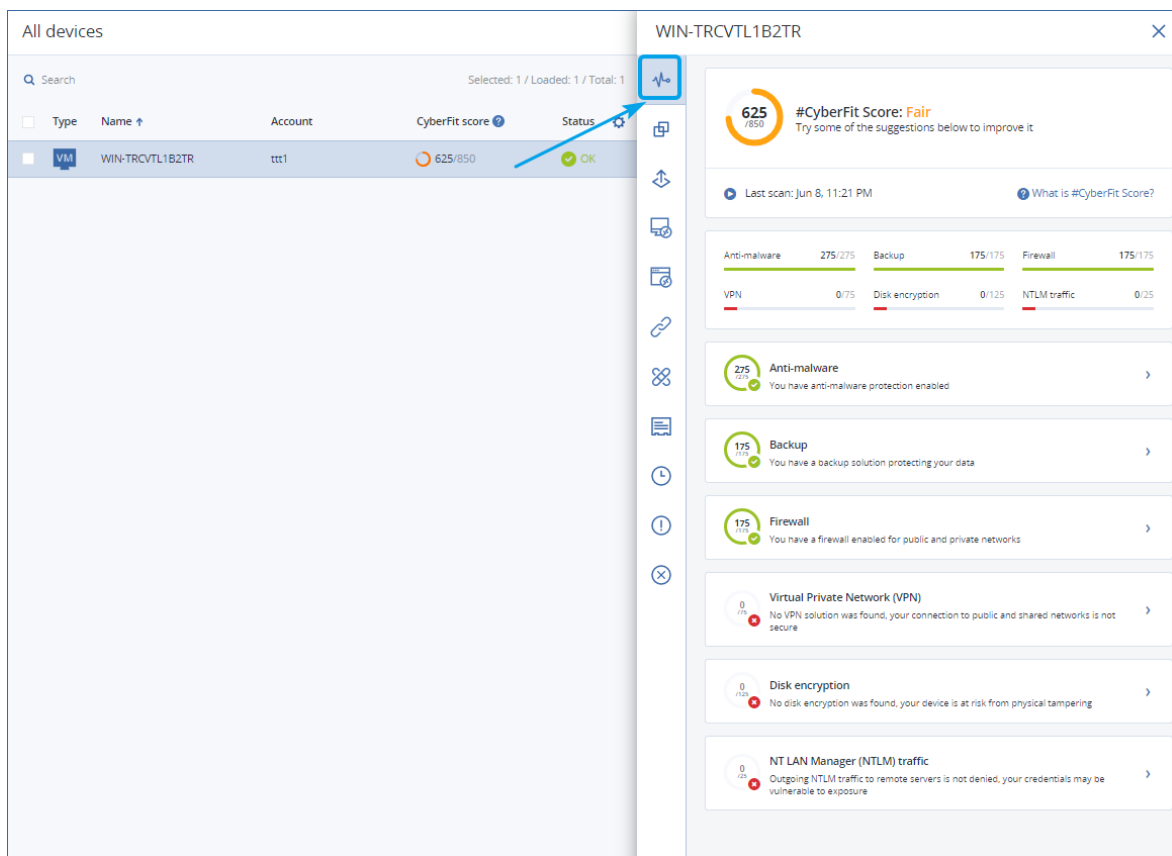


您也可以在對應的桌面小工具和報告頁面中, 取得 #CyberFit 分數的相關資訊。

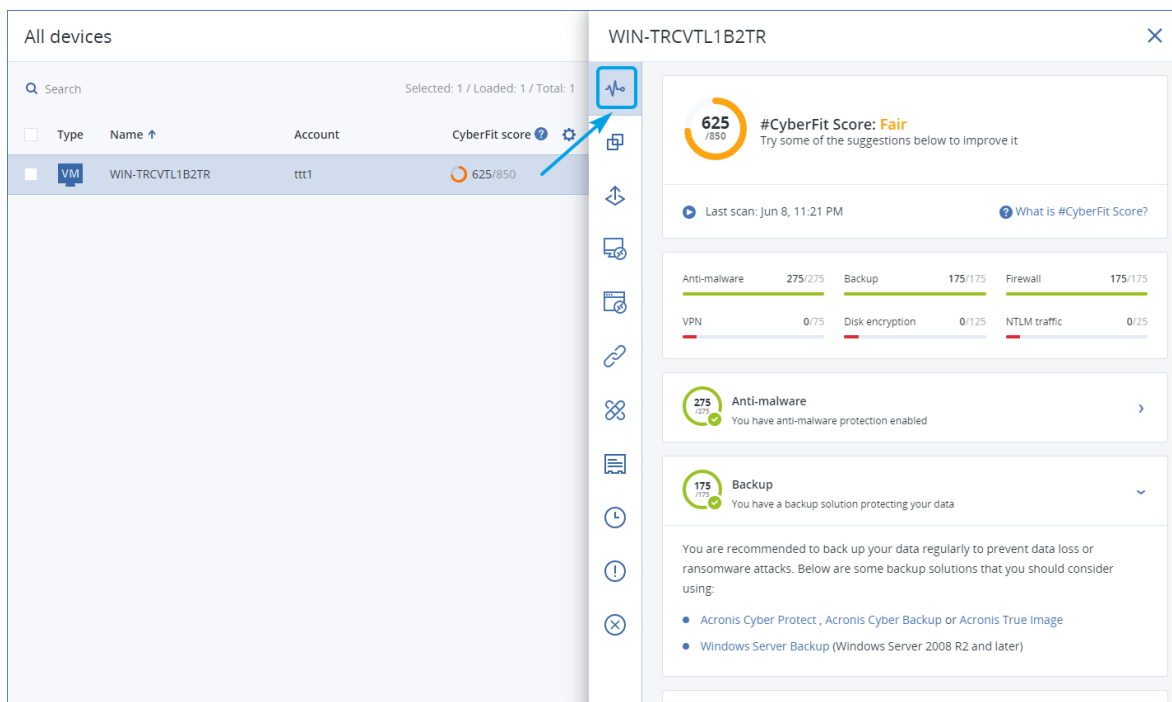
12.2 執行 #CyberFit 分數掃描

若要執行 #CyberFit 分數掃描

1. 在服務主控台中, 移至 **[裝置]**。
2. 選擇電腦, 然後按一下 **[#CyberFit 分數]**。
3. 如果之前從未掃描過電腦, 則按一下 **[執行第一次掃描]**。
4. 掃描完成後, 您將看到電腦的 #CyberFit 總分, 以及六個評估指標分別的分數: 反惡意程式碼、備份、防火牆、虛擬私人網路 (VPN)、磁碟加密, 以及 NT LAN Manager (NTLM) 流量。



5. 若要檢查如何針對可以改善安全設定的各個指標提高其分數，請展開對應的章節並閱讀建議。



6. 因應建議之後，您一律可以按一下 #CyberFit 總分正下方的箭頭按鈕，重新計算電腦的 #CyberFit 分數。

13 備份與復原

備份模組可啟用實體與虛擬機器、檔案與資料庫的備份與復原到本機或雲端儲存空間。

13.1 備份

已啟用 [備份] 模組的保護計劃是一組規則，用於指定將在指定電腦上保護指定資料的方式。

保護計劃可在其建立時 (或之後) 套用至多部電腦。

在啟用 [備份] 模組的情況下，建立第一個保護計劃

1. 選擇您要備份的電腦。
2. 按一下 [保護]。

顯示套用於機器的保護計劃。如果機器尚未指派任何計劃，則您將看到可套用的預設保護計劃。您可以視需要調整設定，並套用此計劃或建立新的計劃。

3. 若要建立新的計劃，按一下 [建立計劃]。啟用 [備份] 模組，並展開設定。

New protection plan (2)

Cancel

Create

Backup

Entire machine to Cloud storage, Monday to Friday at 05:45 PM

What to back up

Entire machine

Continuous data protection (CDP)

Where to back up

Cloud storage

Schedule

Monday to Friday at 05:45 PM

i

How long to keep

Monthly: 6 months
Weekly: 4 weeks
Daily: 7 days

Encryption

i

Application backup

Disabled

i

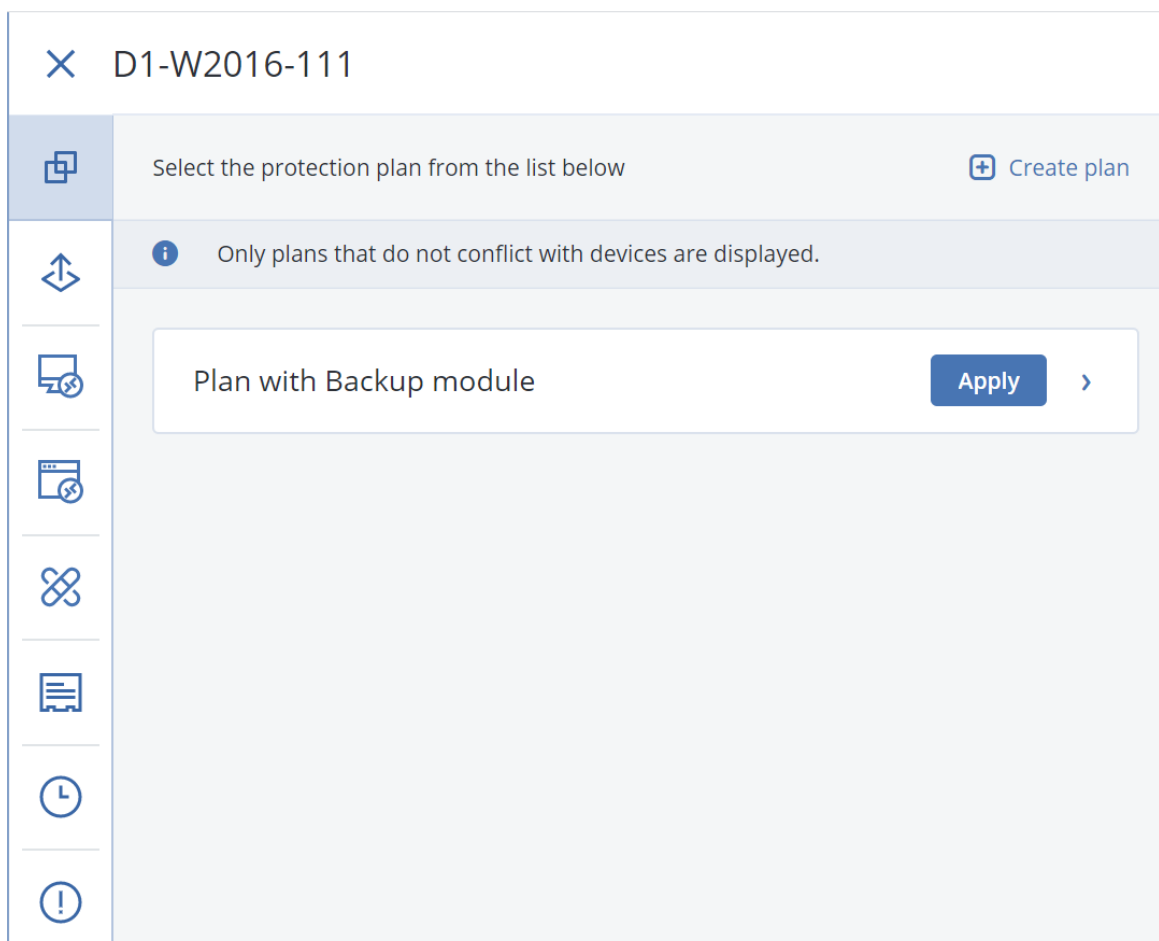
Backup options

Change

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設定。
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]**。

13.2 保護計劃速查表

下表摘述可用的保護計劃參數。使用本表格建立最符合您需求的保護計劃。

要備份的內容	要備份的項目	備份目標位置	排程 備份配置	保留多長時間

	選擇方法			
磁碟/磁碟區 (實體機器 ¹)	直接選擇 原則規則 檔案篩選器	雲端 本機資料夾 網路資料夾 NFS* Secure Zone**	一律增量備份 (單一檔案) 一律完整備份 每週完整備份, 每日增量備份 每月完整備份、每週差異備份和每日增量備份 (GFS) 自訂 (F-D-I)	按照備份存留期 (單一規則/每一組備份) 按照備份數目 依備份大小總計*** 永久保留
磁碟/磁碟區 (虛擬機器 ²)	原則規則 檔案篩選器	雲端 本機資料夾 網路資料夾 NFS*		
檔案 (僅限實體機器 ³)	直接選擇 原則規則 檔案篩選器	雲端 本機資料夾 網路資料夾 NFS* Secure Zone**	一律增量備份 (單一檔案) 一律完整備份 每週完整備份, 每日增量備份 每月完整備份、每週差異備份和每日增量備份 (GFS) 自訂 (F-D-I)	
ESXi 設定	直接選擇	本機資料夾 網路資料夾 NFS*		
網站 (檔案和 MySQL 資料庫)	直接選擇	雲端	—	

¹作業系統中所安裝之代理程式備份的電腦。

²外部代理程式 (例如 VMware 用代理程式或 Hyper-V 用代理程式) 在 Hypervisor 層級備份的虛擬機器。從備份觀點來看, 內部具有代理程式的虛擬機器會被視為實體機器。

³作業系統中所安裝之代理程式備份的電腦。

系統狀態		直接選擇	雲端	一律完整備份	
SQL 資料庫			本機資料夾	每週完整備份, 每日增量備份	
Exchange 資料庫			網路資料夾	自訂 (F-I)	
Microsoft 365	信箱 (本機 Microsoft 365 用代理程式)	直接選擇	本機資料夾 網路資料夾	一律增量備份 (單一檔案) - 僅是用於 SQL 資料庫 ~~一律增量備份 (單一檔案)~~	
	信箱 (雲端 Microsoft 365 用代理程式)	直接選擇	雲端	—	
	公用資料夾				
	Teams				
	OneDrive 檔案	直接選擇	雲端	—	
	SharePoint Online 資料	原則規則			
	Google Workspace	Gmail 信箱	直接選擇	雲端	—
Google 雲端硬碟檔案		直接選擇			
共用磁碟機檔案		原則規則			

* 在 Windows 中無法使用備份至 NFS 共用。

** 在 Mac 上無法建立 Secure Zone。

*** 依備份大小總計保留規則不適用於**一律增量備份 (單一檔案)** 備份配置或備份到雲端儲存空間時。

13.3 選擇要備份的資料

13.3.1 選擇整部機器

整部電腦的備份就是其所有非卸除式磁碟的備份。有關磁碟備份的更多資訊, 請參閱 "選擇磁碟/磁碟區" (第 146 頁)。

注意事項

遭到鎖定的加密 APFS 磁碟區不支援磁碟/磁碟區備份。

在整部電腦備份期間，將會略過這類磁碟區。

13.3.2 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。

注意事項

遭到鎖定的加密 APFS 磁碟區不支援磁碟/磁碟區備份。

在整部電腦備份期間，將會略過這類磁碟區。

透過 iSCSI 通訊協定連線至實體電腦的磁碟也可以備份，但是如果您使用 VMware 用代理程式或 Hyper-V 用代理程式備份與 iSCSI 連線的磁碟，則會有一些限制。

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。

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] 會選擇系統與開機磁碟區。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。
- [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_1-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, 採用 Windows Vista 開始的作業系統, 均未對 Windows 還原點進行備份。
 - 如果磁碟區陰影複製服務 (VSS) 備份選項已啟用, 檔案和資料夾指定於 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** 登錄機碼中。

Linux

磁碟區備份會儲存所選磁碟區的所有檔案和目錄 (不論其屬性為何)、開機記錄及檔案系統超級區塊。

磁碟備份儲存所有磁碟磁碟區以及包含主開機記錄的第零軌。

Mac

磁碟或磁碟區備份儲存所選磁碟或磁碟區的所有檔案和目錄, 以及磁碟區版面配置說明。

排除下列項目:

- 系統中繼資料, 如檔案系統日誌和 Spotlight 索引
- 垃圾桶
- Time Machine 備份

實際, 備份 Mac 上檔案層級的磁碟和磁碟區。可從磁碟區進行裸機復原, 並可進行磁碟區備份, 但逐一磁區備份模式不可用。

13.3.3 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。透過 iSCSI 通訊協定連線至實體電腦的磁碟上的檔案和資料夾也可以備份, 但是如果您使用 VMware 用代理程式或 Hyper-V 用代理程式備份與 iSCSI 連線的磁碟上的資料, 則會有一些限制。

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。

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. 指定 **[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. 指定 **[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。
原則規則將會套用到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**。

13.3.4 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

13.3.5 選擇 ESXi 設定

ESXi 主機設定備份可將 ESXi 主機復原至裸機。此復原會以可開機媒體執行。

在主機上執行的虛擬機器並未包含在備份中。這些虛擬機器可以另行單獨備份和復原。

ESXi 主機設定備份包含下列幾項：

- 主機的開機載入器和開機程式組磁碟分割。
- 主機狀態(虛擬網路和存放區設定、SSL 金鑰、伺服器網路設定, 和本機使用者資訊)。
- 已安裝或儲存在主機上的副檔名和修補。
- 記錄檔。

必要條件

- 必須在 ESXi 主機設定的 **安全設定檔** 中啟用 SSH。
- 您必須知道 ESXi 主機上「根」帳戶的密碼。

限制

- 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 **[保護]**。
3. 在 **要備份的內容** 中, 選擇 **ESXi 配置**。
4. 在 **ESXi「根」密碼** 中, 為每個所選擇的主機指定「根」帳戶的密碼, 或是讓所有主機適用同一個密碼。

13.4 連續資料保護 (CDP)

連續資料保護 (CDP) 是進階備份套件的一部分。它會在變更此資料後立即備份關鍵資料, 確保如果系統在兩次排程備份之間出現故障, 不會遺失任何變更。您可以為以下資料設定連續資料保護：

- 特定位置的檔案或資料夾
- 特定應用程式修改的檔案

僅 NTFS 檔案系統和以下作業系統支援連續資料保護：

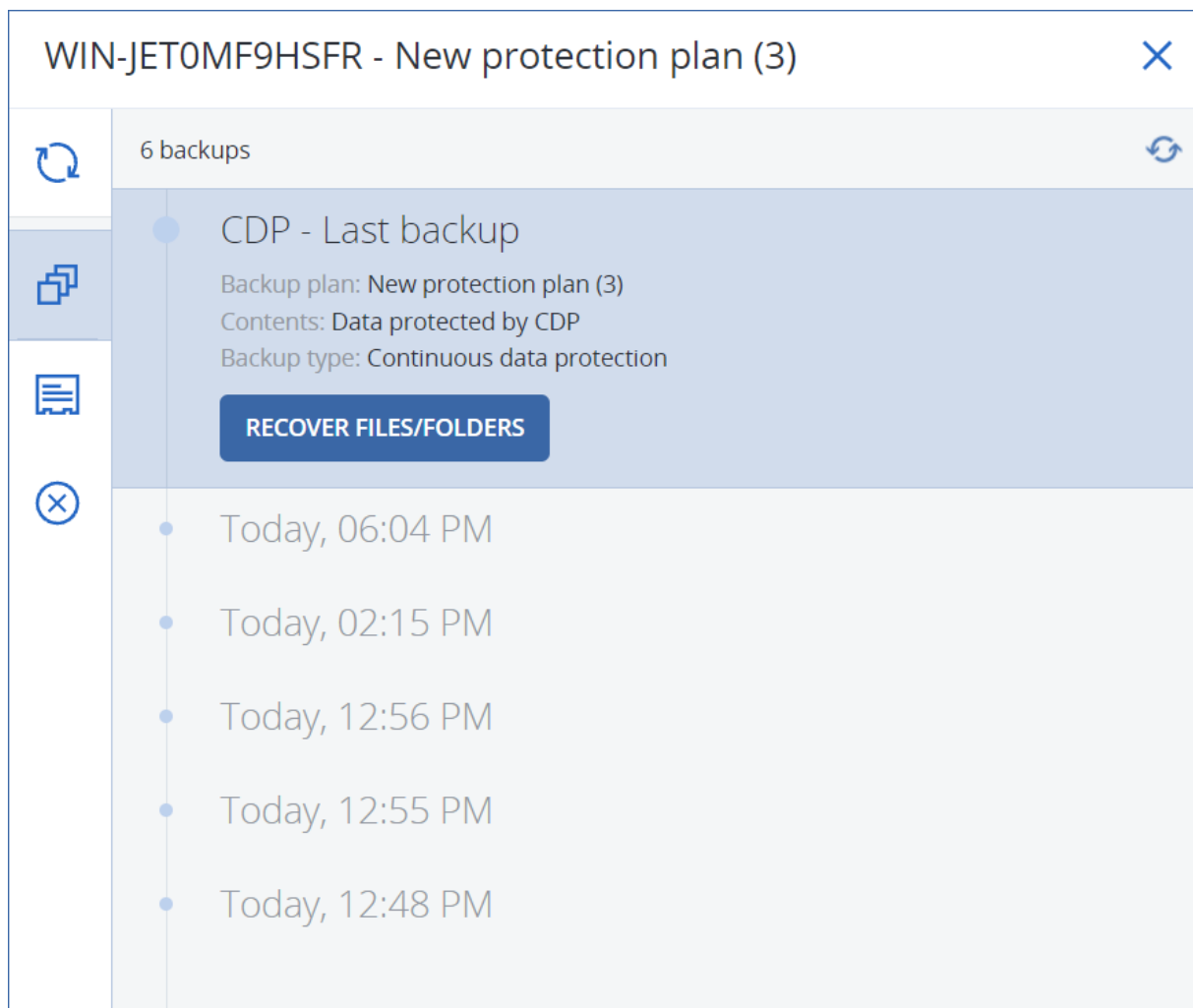
- 桌面: Windows 7 和更新版本
- 伺服器: Windows Server 2008 R2 和更新版本

僅支援本機資料夾。無法選擇網路資料夾進行連續資料保護。

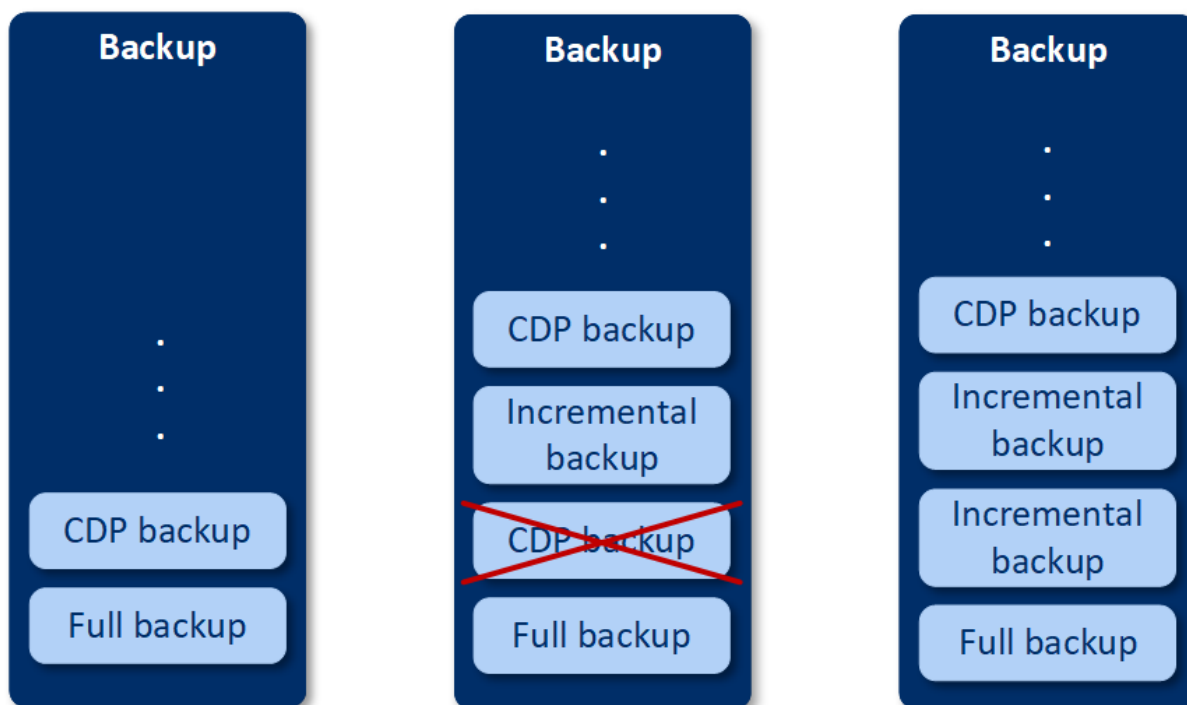
連續資料保護與 **[應用程式備份]** 選項不相容。

13.4.1 運作原理

透過連續資料保護追蹤的檔案和資料夾, 其中的變更會立即保存到特殊 CDP 備份中。一個備份組中只有一個 CDP 備份, 始終是最新備份。



當排程備份啟動時，連續資料保護將被置於暫停狀態，因為最新資料將包含在排程備份中。當計劃完成備份後，連續資料保護將會繼續，將刪除舊 CDP 備份，建立新的 CDP 備份。因此，CDP 備份始終保留備份組的最新備份，並且僅儲存追蹤檔案或資料夾的最新狀態。



如果機器在定期備份期間當機，連續資料保護會在機器重新啟動後自動復原，並在上次成功的排程備份之上建立 CDP 備份。

繼續資料保護要求在 CDP 備份之前至少建立一個定期備份。這就是為什麼，當您首次執行包含連續資料保護的保護計劃時，會建立完整備份，並立即在備份之上加入 CDP 備份。如果為現有保護計劃啟用 **[連續資料保護]** 選項，則 CDP 備份將加入現有備份組。

注意事項

如果系統為您啟用進階備份功能，而且您未將其他進階備份功能用於所選電腦，則預設會針對您從 **[裝置]** 索引標籤建立的保護計劃，啟用連續資料保護。如果您已經為所選電腦制定了具有連續資料保護的計劃，則預設不會在新建立的計劃中，為該電腦啟用連續資料保護。

系統預設不會針對為裝置群組建立的計劃，啟用連續資料保護。

13.4.2 支援的資料來源

您可以使用以下資料來源設定連續資料保護：

- 整部電腦
- 磁碟/磁碟區
- 檔案/資料夾

在保護計劃的 **[備份內容]** 部分選擇資料來源後，在 **[要連續保護的項目]** 部分中，選擇用於連續資料保護的檔案、資料夾或應用程式。有關如何設定連續資料保護的詳細資訊，請參閱 "設定 CDP 備份" (第 154 頁)。

13.4.3 支援的目的地

您可以使用以下目的地設定連續資料保護：

- 本機資料夾
- 網路資料夾
- 雲端儲存
- Acronis Cyber Infrastructure
- 指令碼所定義的位置

注意事項

您只能透過指令碼定義上面列出的位置。

13.4.4 設定 CDP 備份

您可以在保護計劃的 **[備份]** 模組中設定連續資料保護。有關如何建立保護計劃的詳細資訊，請參閱 "建立保護計劃" (第 129 頁)。

編輯連續資料保護設定

1. 在保護計劃的 **[備份]** 模組中，啟用 **[連續資料保護 (CDP)]** 開關。
此開關僅適用於以下資料來源：
 - 整部電腦
 - 磁碟 / 磁碟區
 - 檔案/資料夾
2. 在 **[要連續保護的項目]** 中，為 **[應用程式]** 或 **[檔案/資料夾]** 或兩者設定連續資料保護。
 - 按一下 **[應用程式]** 為特定應用程式修改的檔案設定 CDP 備份。
您可以從預先定義的類別中選擇應用程式，或透過指定可執行檔的路徑來加入其他應用程式，例如：
 - C:\Program Files\Microsoft Office\Office16\WINWORD.EXE
 - *:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
 - 按一下 **[檔案/資料夾]** 為特定位置的檔案設定 CDP 備份。
您可以使用選擇規則或直接選擇檔案和資料夾來定義這些位置。
 - **[對於所有機器]** 要建立選擇規則，請使用文字方塊。
您可以使用檔案的完整路徑或具有萬用字元 (* 和 ?) 的路徑。星號代表零個或多個字元。問號代表單一字元。

重要事項

要為資料夾建立 CDP 備份，必須使用星號萬用字元指定其內容：

正確的路徑：D:\Data*

不正確的路徑：D:\Data\

- **[對於連線機器]** 要直接選擇檔案和資料夾：
 - 在 **[要瀏覽的機器]** 中，選擇檔案或資料夾所在的機器。
 - 按一下 **[選擇檔案和資料夾]** 以瀏覽選定的機器。
直接選擇將建立選擇規則。如果將保護計劃套用於多台機器，並且某個選擇規則對某台機器無效，則在此機器上將跳過該保護計劃。

3. 在保護計劃窗格中，按一下 **[建立]**。

因此，您指定的資料將在排程備份之間進行連續備份。

13.5 選擇目的地

請按一下 **[備份目標位置]**，然後選擇下列其中一項：

- **雲端儲存**

備份將儲存在雲端資料中心。

- **本機資料夾**

如果選擇單一電腦，請瀏覽所選擇電腦上的資料夾，或是輸入資料夾路徑。

如果選擇多部機器，請輸入資料夾路徑。備份將儲存在所選擇的每部實體機器裡的這個資料夾中，或是儲存在已安裝虛擬機器用代理程式的電腦上。如果資料夾不存在，則會建立資料夾。

- **網路資料夾**

這是透過 SMB/CIFS/DFS 共用的資料夾。

瀏覽所需的共用資料夾或按下列格式輸入路徑：

- SMB/CIFS 共用：\\<主機名稱>\<路徑>\ 或 smb://<主機名稱>/<路徑>/
- DFS 共用：\\<完整 DNS 網域名稱>\<DFS 根>\<路徑>

例如 \\example.company.com\shared\files

然後按一下箭頭按鈕。如果看到提示，請指定共用資料夾的使用者名稱和密碼。您可以隨時按一下資料夾名稱旁邊的鑰匙圖示來變更這些認證。

不支援備份至具有匿名存取權的資料夾。

- **NFS 資料夾**(可用於執行 Linux 或 Mac OS 的電腦)

請確認安裝 Linux 用代理程式所在的 Linux 伺服器上已安裝 nfs-utils 套件。

瀏覽所需的 NFS 資料夾，或在下列格式中輸入路徑：

nfs://<主機名稱>/<匯出的資料夾>:/<子資料夾>

然後按一下箭頭按鈕。

注意事項

無法備份至受密碼保護的 NFS 資料夾。

- **Secure Zone** (若存在每個所選擇的電腦中，則可以使用)

Secure Zone 是指位於備份電腦磁碟上的安全磁碟分割。此磁碟分割必須在設定備份之前手動建立。如需有關如何建立 Secure Zone 及其優點和限制的資訊，請參閱 "關於 Secure Zone" (第 156 頁)。

13.5.1 進階儲存選項

注意事項

此功能僅適用於 Cyber Protection 服務的 Advanced 版本。

由指令碼定義 (適用於執行 Windows 的電腦)

您可以將每台電腦的備份儲存在指令碼定義的資料夾中。此軟體支援以 JScript、VBScript 或 Python 3.5 撰寫的指令碼。部署保護計劃時，此軟體會在每部電腦上執行指令碼。每台電腦的指令碼輸出應該是本機或網路資料夾路徑。如果資料夾不存在，系統會建立一個資料夾 (限制：以 Python 撰寫的指令碼無法在網路共用上建立資料夾)。在 **【備份儲存】** 索引標籤上，每個資料夾都會顯示為個別的備份位置。

在 **【指令碼類型】** 中，選擇指令碼類型 (**JScript**、**VBScript** 或 **Python**)，然後匯入或複製並貼上指令碼。對於網路資料夾，請使用讀取/寫入權限指定存取認證。

範例：

- 下列 JScript 指令碼會以 \\bkpsrv\<電腦名稱> 格式，輸出電腦的備份位置：

```
WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject("WScript.Network").ComputerName);
```

因此，每台電腦的備份將會儲存在伺服器 **bkpsrv** 上的同名資料夾中。

- 以下 JScript 指令碼將輸出備份位置到位於執行指令碼的機器上的資料夾：

```
WScript.Echo("C:\\Backup");
```

因此，此機器的備份將保存在同一台機器上的 C:\Backup 資料夾中。

注意事項

這些指令碼中的位置路徑區分大小寫。因此，C:\Backup 和 C:\backup 在服務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。

13.5.2 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。

✕ Create Secure Zone

Secure Zone disk

 Disk 1, 60.0 GB

Maximum possible size of Secure Zone: 35.9 GB

Secure Zone size:

 - 20 + GB ▾

There is not enough unallocated space. Free space will be taken from all volumes where it is present.

[Select volumes](#)

Password protection

☐ Off

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。

13.6 排程

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。

13.6.1 備份配置

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 **[單一檔案備份格式]**¹。

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。

如果備份位置為雲端儲存, 則強烈建議使用此配置。其他備份配置可能包括多個耗用許多時間和網路流量的完整備份。

- **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。

¹備份格式, 會將初始完整備份及後續增量備份儲存為單一的 .tibx 檔案。此格式可以善用了增量備份方法的速度, 同時避免其主要的缺點 - 不容易刪除過期備份。軟體會將過期備份所使用的區塊標示為「可用」, 並在區塊中寫入新備份。結果會以耗費最少資源的方式, 產生極快速的清理。備份至不支援隨機存取讀寫的位置時, 無法使用單一檔案備份格式。

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」。

注意事項

建立保護計劃之後，就無法在備份配置的單一檔案格式與多檔案格式之間切換。一律增量是單一檔案格式，其餘配置皆為多檔案格式。如果要在格式之間切換，請建立新的保護計劃。

13.6.2 其他排程選項

有了任何目的地，您可以執行下列作業：

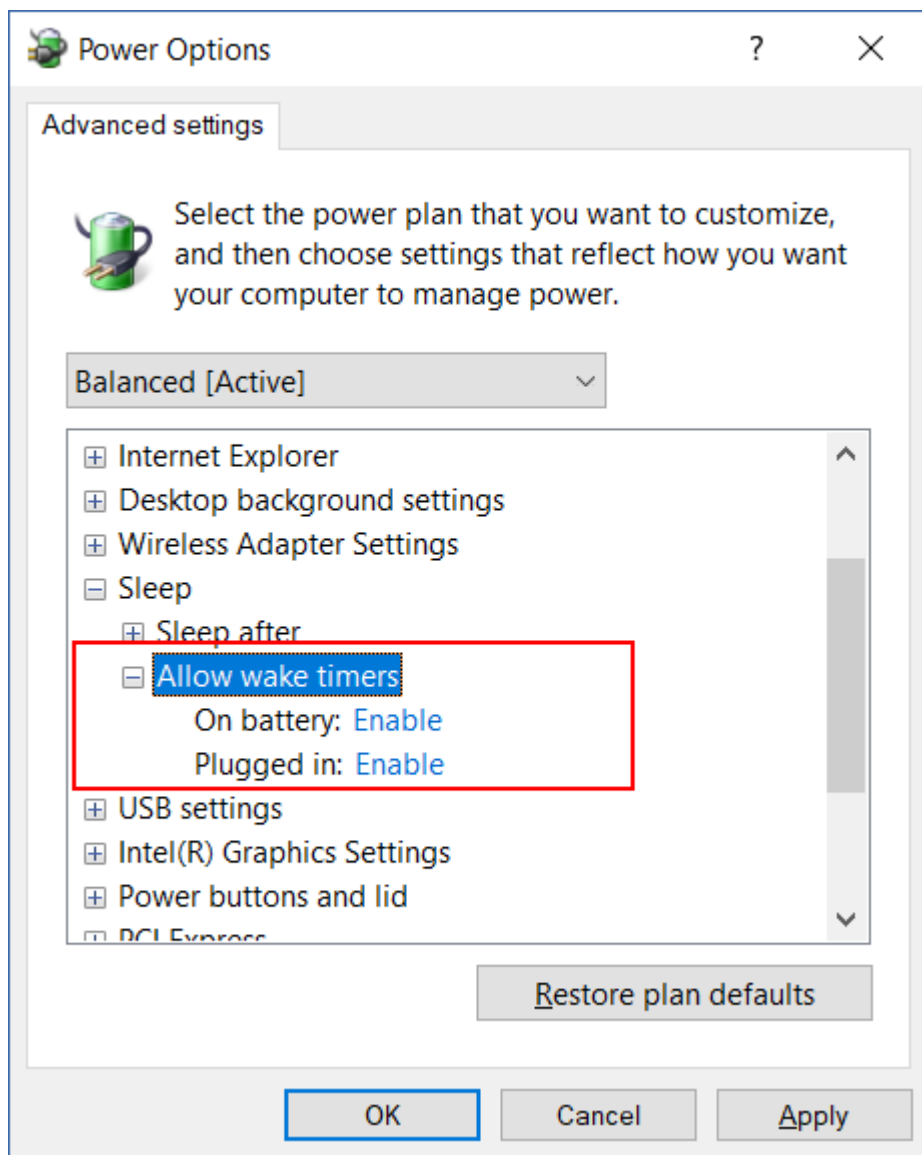
- 指定備份開始條件，以便在符合條件時才執行已排程的備份。如需詳細資訊，請參閱「開始條件」。
- 設定排程啟用時間的日期範圍。選擇 **[在日期範圍內執行計劃]** 核取方塊，然後指定日期範圍。
- 停用排程。排程停用後，除非手動啟動一項備份，否則不適用保留規則。
- 從排定的時間導入延遲。每台機器的延誤的時間是隨機選定的，範圍從 0 到您指定的最大時間值。您可以想在將多台電腦備份到網路位置時使用此設定，以避免網路負載過大。

在保護計劃的 [備份] 模組設定中，移至 **[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

此選項預設為啟用，且最大延遲設為 30 分鐘。

- 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，且其電源計劃已啟用 **[允許喚醒計時器]** 設定的電腦有效。



當電腦關機時，此選項無效，即該選項不會使用 LAN 喚醒功能。

13.6.3 依據事件排程

設定保護計劃的備份模組排程時，可以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。

13.6.4 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 時	Windows、 Linux、macOS	Windows、 Linux	-	-	-	-
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。

此條件對於網路資料夾、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。

不要在使用計量付費連線時開始

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，筆記型電腦在網路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。

13.7 保留規則

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**

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]) 選擇的那一天所建立的第一個備份。如果每週備份指的是每月一開始所建立的第一個備份, 則此備份會被視為每月備份。在此情況下, 每週備份將會在下一週選擇的那天建立。除非此備份落在每月或每週備份的定義範圍內, 否則每日備份指的是每日一開始所建立的第一個備份。除非此備份落在每月、每週或每日備份的定義範圍內, 否則每小時備份指的是每小時一開始所建立的第一個備份。

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)** 備份配置或備份到雲端儲存空間時。

- **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。

13.7.1 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。

- 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 Cyber Protection 服務中刪除之後，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。

13.8 複寫

您可以啟用備份複寫，以便在主要備份目的地建立備份後，立即將每個備份複寫到另一個位置。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。如果在備份複寫在過程中遭到中斷，則在下次開始複寫時，已經複寫的資料將不會再次複寫，如此可減少時間損失。

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。

13.8.1 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。

13.8.2 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

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

啟用備份的複寫。

1. 在保護計劃面板的 **[備份]** 區段中，按一下 **[新增位置]**。

注意事項

[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. 從可用位置的清單，選擇將複寫備份的位置。

根據您針對複寫新增的位置數目，此位置在保護計劃中會顯示為 **[第 2 個位置]**、**[第 3 個位置]**、**[第 4 個位置]** 或 **[第 5 個位置]**。

3. **[選用]** 按一下齒輪圖示可查看該位置可用的複寫選項。

- **[效能及備份視窗]** - 設定所選位置的備份視窗，如 "效能和備份時窗" (第 198 頁) 中所述。這些設定將會定義複寫效能。
- **[移除位置]** - 刪除目前選定的複寫位置。
- **[僅適用於雲端儲存空間位置] 實體資料傳送** - 將初始備份保存在抽取式存放裝置上，然後將其上傳到雲端，而非透過 Internet 複寫。此選項適合網路連線慢的位置，或是您想要透過網路節省大檔案傳輸頻寬的情況。啟用此選項並不需要進階 Cyber Protect 服務配額，但是您需要有實體資料運送服務配額，才能建立裝貨單並進行追蹤。請參閱 "實體資料運送" (第 200 頁)。

注意事項

Cyber Protect 代理程式 C21.06 版或更新版本支援此選項。

4. **[選用]** 在位置行 **[保留的時間長度]** 中，設定所選位置的保留規則，如 "保留規則" (第 168 頁) 中所述。
5. **[選用]** 重複步驟 1 - 4 以加入要複寫備份的位置。只要先前選定的備份或複寫位置支援複寫功能，您最多可以設定四個複寫位置。

重要事項

如果在同一個保護計劃中啟用備份和複寫，請確認在下一計劃備份之前完成複寫。如果複寫仍在進行中，排程的備份將無法開始；例如，如果複寫需要 26 小時完成，則每 24 小時執行一次的排程備份將不會開始。

為了避免這樣的相依性，請使用單獨的備份複寫計劃。如需有關此特定計劃的詳細資訊，請參閱 "備份複寫" (第 512 頁)。

13.9 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。

警告！

若是遺失或忘記密碼，則無法復原加密的備份。

13.9.1 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。

若是加強安全性模式下的帳戶，則您無法在保護計劃中設定加密密碼。您必須在受保護的裝置本機上設定此密碼。

在保護計劃中指定加密設定

1. 在保護計劃面板上的 [備份] 模組設定中，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]**。

13.9.2 以電腦屬性加密

無論電腦的保護計劃中的設定為何，您都可以為其強制加密備份或設定一個唯一的加密密碼。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 [備份] 模組設定中停用加密，所有備份仍會經過加密。

此選項也可用於執行 VMware 用代理程式的電腦。不過，如果有多個 VMware 用代理程式連線至相同的 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。

重要事項

您只能在電腦的保護計劃建立任何備份之前，變更其加密設定。如果您之後變更加密設定，保護計劃將會失敗，而且您將需要新的保護計劃，才能繼續備份此電腦。

儲存加密設定後，也可以依以下所述方式變更或重設。

儲存電腦上的加密設定

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。其預設為 **%ProgramFiles%\BackupClient**。
 - Linux 系統：`/usr/sbin/acropsh -m manage_creds --set-password <加密密碼>`
 - 在虛擬裝置中：`./sbin/acropsh -m manage_creds --set-password <encryption_password>`

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。其預設為 **%ProgramFiles%\BackupClient**。
 - Linux 系統：`/usr/sbin/acropsh -m manage_creds --reset`
 - 在虛擬裝置中：`./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 監視器] 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]**。

13.9.3 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。

13.10 公證

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

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

13.10.1 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 [\[驗證檔案真實性\]](#)。

13.10.2 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。

13.11 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 **[保護]**。
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。

13.12 預設備份選項

備份選項的預設值存在於公司、單位和使用者層級。在公司或單位內建立單位或使用者帳戶時，它會繼承針對公司或針對單位設定的預設值。

公司系統管理員、單位系統管理員，以及沒有系統管理員權限的每個使用者，都可以針對預先定義的選項，變更預設選項值。依預設，新值將用於變更生效後在個別層級建立的所有保護計劃中。

建立保護計劃時，使用者可以使用僅專用於此計劃的自訂值，來覆寫預設值。

若要變更預設選項值

1. 執行下列其中一項操作：
 - 若要變更公司的預設值，請以公司系統管理員身分登入服務主控台。
 - 若要變更單位的預設值，請以單位系統管理員身分登入服務主控台。
 - 若要變更您自己的預設值，請使用沒有系統管理員權限的帳戶登入服務主控台。
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]**。

13.13 備份選項

若要修改備份選項，請在保護計劃的**[備份]**模組中，按一下 **[備份選項]** 旁邊的 **[變更]**。

13.13.1 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
	Window	Linux	macO	Window	Linux	macO	ESXi	Hype	Virtuozz	Window

	s		S	s		S		r-V	o	s
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	+	+	+	+	+	+	+	+	+	+
錯誤處理										
發生錯誤時重新嘗試	+	+	+	+	+	+	+	+	+	+
處理時不顯示訊息和對話方塊 (無訊息模式)	+	+	+	+	+	+	+	+	+	+
忽略損壞的磁區	+	+	+	+	+	+	+	+	+	-
若建立 VM 快照期間發生錯誤，會重新嘗試	-	-	-	-	-	-	+	+	+	-
快速增	+	+	+	-	-	-	-	-	-	-

量/差異 備份										
檔案層 級備份 快照	-	-	-	+	+	+	-	-	-	-
檔案篩 選器	+	+	+	+	+	+	+	+	+	-
鑑識資 料	+	-	-	-	-	-	-	-	-	-
記錄截 斷	-	-	-	-	-	-	+	+	-	僅 SQL
LVM 快 照	-	+	-	-	-	-	-	-	-	-
掛載點	-	-	-	+	-	-	-	-	-	-
多重分 割檔快 照	+	+	-	+	+	-	-	-	-	-
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	+	+	+	+	+	+	-	-	-	+
排程										
在時間 視窗內 分配開 始時間	+	+	+	+	+	+	+	+	+	+
限制同 時執行 備份的 數目	-	-	-	-	-	-	+	+	+	-
逐一磁	+	+	-	-	-	-	+	+	+	-

區 備 份										
分割	+	+	+	+	+	+	+	+	+	+
工作失敗處理	+	+	+	+	+	+	+	+	+	+
工作開始條件	+	+	-	+	+	-	+	+	+	+
磁碟區陰影複製服務 (VSS)	+	-	-	+	-	-	-	+	-	+
虛擬機器的磁碟區陰影複製服務 (VSS)	-	-	-	-	-	-	+	+	-	-
每週備份	+	+	+	+	+	+	+	+	+	+
Windows 事件日誌	+	-	-	+	-	-	+	+	-	+

13.13.2 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。

13.13.3 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。

13.13.4 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？

根據所使用的備份配置以及**備份格式**而定，每個保護計劃都會在備份位置上建立一或多個檔案。以下表格會列出可依機器或信箱建立的檔案的清單。

	一律增量備份 (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
12 版 備份格式	每個備份鏈一個 TIBX 檔案 (完整或差異備份，以及所有相依的增量備份)。如果本機或網路 (SMB) 資料夾中儲存之檔案的大小超過 200 GB，則預設會將檔案分割為 200 GB 的檔案。	

所有檔案都有相同的名稱，可包含或不含時間戳記或序號。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)。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

整個實體和虛擬機器、磁碟/磁碟區、檔案/資料夾、Microsoft SQL Server 資料庫、Microsoft Exchange Server 資料庫，以及 ESXi 設定之備份的預設備份檔案名為 [Machine Name]-[Plan ID]-[Unique ID]A。

本機 Microsoft 365 用代理程式所建立之 Exchange 信箱備份和 Microsoft 365 信箱備份的預設名為 [Mailbox ID]_mailbox_[Plan ID]A。

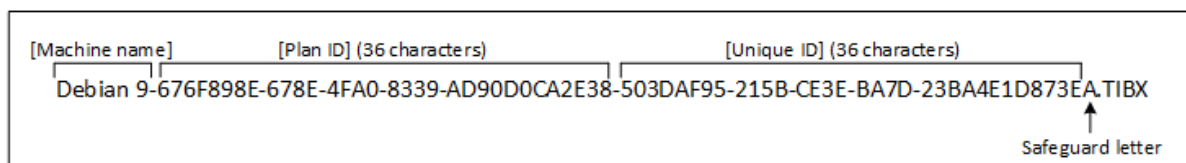
雲端代理程式所建立之雲端應用程式備份的預設名為 [Resource Name]_[Resource Type]_[Resource ID]_[Plan ID]A。

預設名稱包含下列變數：

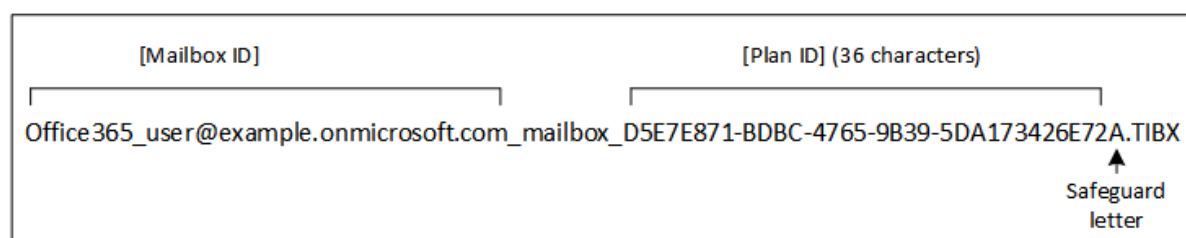
- [Machine Name] 此變數會取代為電腦的名稱 (與服務主控台中顯示的名稱相同)。
- [Plan ID]、[Plan Id] 這些變數會取代為保護計劃的唯一識別碼。重新命名計劃時，此值不會變更。
- [Unique ID] 此變數會取代為所選電腦的唯一識別碼。重新命名電腦時，此值不會變更。
- [Mailbox ID] 此變數會取代為信箱使用者的主要名稱 (UPN)。
- [Resource Name] 此變數會取代為雲端資料來源名稱，例如使用者的主要名稱 (UPN)、SharePoint 網站 URL 或共用磁碟機名稱。
- [Resource Type] 此變數會取代為雲端資料來源類型，例如 mailbox、0365Mailbox、0365PublicFolder、OneDrive、SharePoint、GDrive。

- [Resource ID] 此變數會取代為雲端資料來源的唯一識別碼。重新命名雲端資料來源時，此值不會變更。
- "A" 是保護字母，附加該字母可避免名稱結尾是數字。

下圖顯示預設備份檔案名稱。



下圖顯示本機代理程式所執行之 Microsoft 365 信箱備份的預設備份檔案名稱。



沒有變數的名稱

如果您將備份檔案名稱變更為 MyBackup，則備份檔案將類似於以下範例。這些範例假設每日增量備份排程於 14:40，並且從 2016 年 9 月 13 日開始。

對於具有 **[一律增量 (單一檔案)]** 備份配置的 12 版格式：

```
MyBackup.tibx
```

對於具有其他備份配置的 12 版格式：

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

使用變數

除了預設使用的變數之外，您還可以使用下列變數：

- [Plan name] 變數，這會取代為保護計劃的名稱。
- [Virtualization Server Type] 變數，這會取代為 "vmwesx" (如果虛擬機器透過 VMware 用代理程式備份) 或 "mshyperv" (如果虛擬機器透過 Hyper-V 用代理程式備份)。

如果選擇多個電腦或信箱進行備份，則備份檔案名稱必須包含 [Machine Name]、[Unique ID]、[Mailbox ID]、[Resource Name] 或 [Resource Id] 變數。

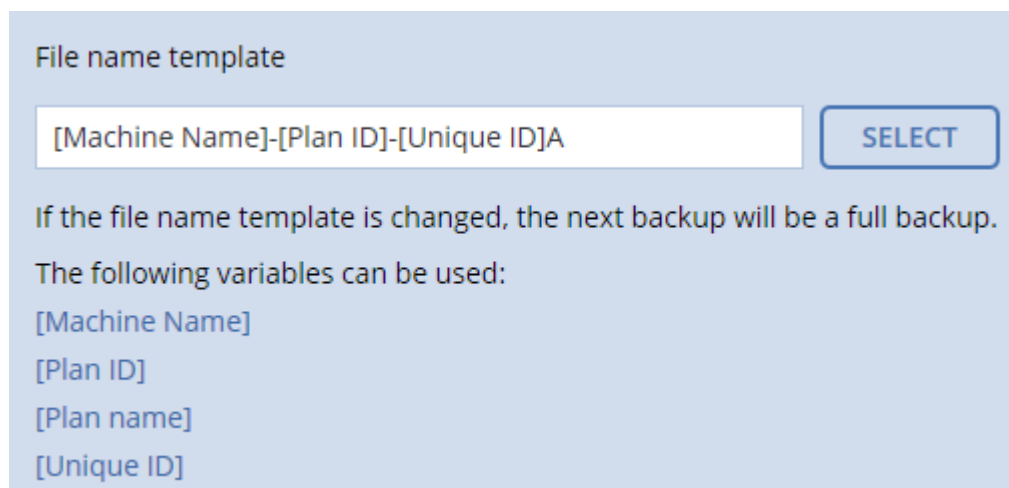
使用範例

- **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，而且您必須從服務主控台中移除此電腦，或者必須解除安裝代理程式以及其組態設定。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。



File name template

[Machine Name]-[Plan ID]-[Unique ID]A **SELECT**

If the file name template is changed, the next backup will be a full backup.

The following variables can be used:

- [Machine Name]
- [Plan ID]
- [Plan name]
- [Unique ID]

[選擇] 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。

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。

13.13.5 備份格式

[備份格式] 選項會定義保護計劃所建立之備份的格式。此選項僅適用於已使用 11 版備份格式的保護計劃。若是如此，您可以將備份格式變更為 12 版。將備份格式切換到 12 版之後，選項將變成無法使用。

- **11 版**

為回溯相容性而保留的舊版格式。

注意事項

您無法使用 11 版的備份格式，備份資料庫可用性群組 (DAG)。只有 12 版格式支援備份 DAG。

- **12 版**

Acronis Backup 12 中推出的備份格式，備份和復原速度更快。每一個備份鏈 (完整或差異備份，以及與之相依的所有增量備份) 都會儲存至單一 TIBX 檔案。

備份格式和備份檔案

對於可以使用檔案管理員瀏覽的備份位置 (例如本機或網路資料夾), 備份格式會判定檔案數目及其副檔名。以下表格會列出可依機器或信箱建立的檔案的清單。

	一律增量備份 (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
12 版備份格式	每個備份鏈一個 TIBX 檔案 (完整或差異備份, 以及所有相依的增量備份)。如果本機或網路 (SMB) 資料夾中儲存之檔案的大小超過 200 GB, 則預設會將檔案分割為 200 GB 的檔案。	

將備份格式變更為 12 版 (TIBX)

如果您將備份格式從 11 版 (TIB 格式) 變更為 12 版 (TIBX 格式):

- 下一次備份將為完整備份。
- 在可以使用檔案管理員瀏覽的備份位置 (例如本機或網路資料夾), 將會建立一個新的 TIBX 檔案。新檔案將會以原始檔案命名, 但附加 **_v12A** 尾碼。
- 保留規則和複寫只會套用到新的備份。
- 舊的備份將不會遭到刪除, 而且仍然保留在 **[備份儲存]** 索引標籤上。您可以手動刪除這些備份。
- 舊的雲端備份將不會耗用**雲端儲存空間**配額。
- 舊的本機備份將會耗用**本機備份**配額, 直到您手動刪除這些備份為止。

存檔內重複資料刪除

12 版的 TIBX 備份格式支援存檔內重複資料刪除, 其中包含下列優點:

- 透過內建的區塊層級重複資料刪除功能, 大幅減少任何類型資料的備份大小
- 有效處理硬式連結可確保沒有儲存重複
- 雜湊型區塊

注意事項

系統預設會針對 TIBX 格式的所有備份, 啟用存檔內重複資料刪除。您不必在備份選項中啟用該選項, 也無法加以停用。

13.13.6 備份驗證

驗證是檢視從備份中復原資料的可能性的作業。啟用此選項時, 保護計劃建立的每個備份都會在建立後立即進行驗證。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](#)。

注意事項

視您的服務提供者所選擇的設定而定，可能無法在備份到雲端儲存空間時進行驗證。

13.13.7 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。

13.13.8 叢集備份模式

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

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。

13.13.9 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。

13.13.10 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，如果網路上的備份目的地在執行備份期間變得無法使用或無法連線，此軟體會每隔 30 秒嘗試連線目的地一次，但不會超過 30 次。一旦連線繼續或執行指定次數的嘗試後（以先發生者為準），程式將立即停止嘗試。

不過，如果在備份開始時無法使用備份目的地，則只會嘗試 10 次。

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： $(300 \text{ 秒} + \text{嘗試間隔}) * (\text{嘗試次數} + 1)$ 。

範例：

- 使用預設值，備份將在 $(300 \text{ 秒} + 30 \text{ 秒}) * (300 + 1) = 99330 \text{ 秒}$ ，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 $(300 \text{ 秒} + 1 \text{ 秒}) * (1 + 1) = 602 \text{ 秒}$ ，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。

注意事項

Linux 不支援略過損毀的磁區。您可以在離線模式下，使用 Cyber Protect 內部部署版本中的 Bootable Media Builder，備份包含損毀磁區的 Linux 系統。使用內部部署 Bootable Media Builder 時，需要單獨的授權。如需協助，請聯絡支援部門。

若建立 VM 快照期間發生錯誤，會重新嘗試

預設為：**啟用**。**嘗試次數**:3。**嘗試間隔**:5 分鐘。

如果無法取得虛擬機器快照，程式會重新嘗試執行未成功的作業。您可以設定時間間隔和嘗試次數。一旦作業成功「或是」已執行指定次數的嘗試後（以先發生者為準），軟體將停止嘗試。

13.13.11 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。

13.13.12 檔案篩選器

檔案篩選器會定義備份程序中需要略過的檔案與資料夾。

除非另有說明，否則檔案篩選適用於磁碟層級備份、整部電腦備份以及檔案層級備份。

啟用檔案篩選器

1. 選擇要備份的資料。
2. 按一下 **[備份選項]** 旁邊的 **[變更]**。
3. 選取 **[檔案篩選器]**。
4. 使用下面敘述的任一選項。

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**)。

- **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 **Doc.txt** 或 **Doc11.txt** 檔案。

13.13.13 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。

13.13.14 鑑識資料

病毒、惡意程式碼和勒索軟體可能會執行惡意活動，例如竊取或變更資料。這些活動可能需要進行調查，這只有在提供數位證據時才可行。不過，數位證據片段（例如，檔案或活動蹤跡）可能會遭到刪除，或者進行惡意活動所在電腦可能會變成無法使用。

包含鑑識資料的備份允許調查人員分析通常不包含在定期磁碟備份中的磁碟區域。**[鑑識資料]** 備份選項可讓您收集下列能夠用於鑑識調查的數位證據片段：未使用磁碟空間的快照、記憶體傾印，以及執行中程序的快照。

系統會自動勾選含鑑識資料的備份。

[鑑識資料] 選項僅適用於執行下列作業系統的 Windows 電腦整部電腦備份：

- Windows 8.1、Windows 10
- Windows Server 2012 R2 – Windows Server 2019

包含鑑識資料的備份不適用於下列電腦：

- 透過 VPN 連線到網路，且無法直接存取網際網路的電腦
- 包含使用 BitLocker 加密的磁碟的電腦

注意事項

您無法在將已啟用 **[備份]** 模組的保護計劃套用到電腦後，修改鑑識資料設定。若要使用不同的鑑識資料設定，請建立新的保護計劃。

您可以將包含鑑識資料的備份儲存在下列位置中：

- 雲端儲存
- 本機資料夾

注意事項

只有透過 USB 連線的外接式硬碟才支援本機資料夾位置。
不支援本機動態磁碟作為包含鑑識資料的備份的位置。

- 網路資料夾

鑑識備份程序

系統會在鑑識備份程序期間執行下列動作：

1. 收集原始記憶體傾印以及執行中處理程序的清單。
2. 自動讓電腦重新開機進入可開機媒體。
3. 建立同時包含已佔用空間和未配置空間的備份。
4. 公證備份的磁碟。
5. 重新開機進入即時作業系統並繼續執行計劃 (例如, 複寫、保留、驗證等等)。

設定鑑識資料集合

1. 在服務主控台中, 移至 **[裝置]** > **[所有裝置]**。或者, 您可以從 **[管理]** 索引標籤建立保護計劃。
2. 選擇裝置, 然後按一下 **[保護]**。
3. 在保護計劃中, 啟用 **[備份]** 模組。
4. 在 **[要備份的內容]** 中選擇 **[整部電腦]**。
5. 在 **[備份選項]** 中, 按一下 **[變更]**。
6. 尋找 **[鑑識資料]** 選項。
7. 啟用 **[收集鑑識資料]**。系統將會自動收集記憶體傾印, 並建立執行中處理程序的快照。

注意事項

完整記憶體傾印可能包含密碼之類的敏感資料。

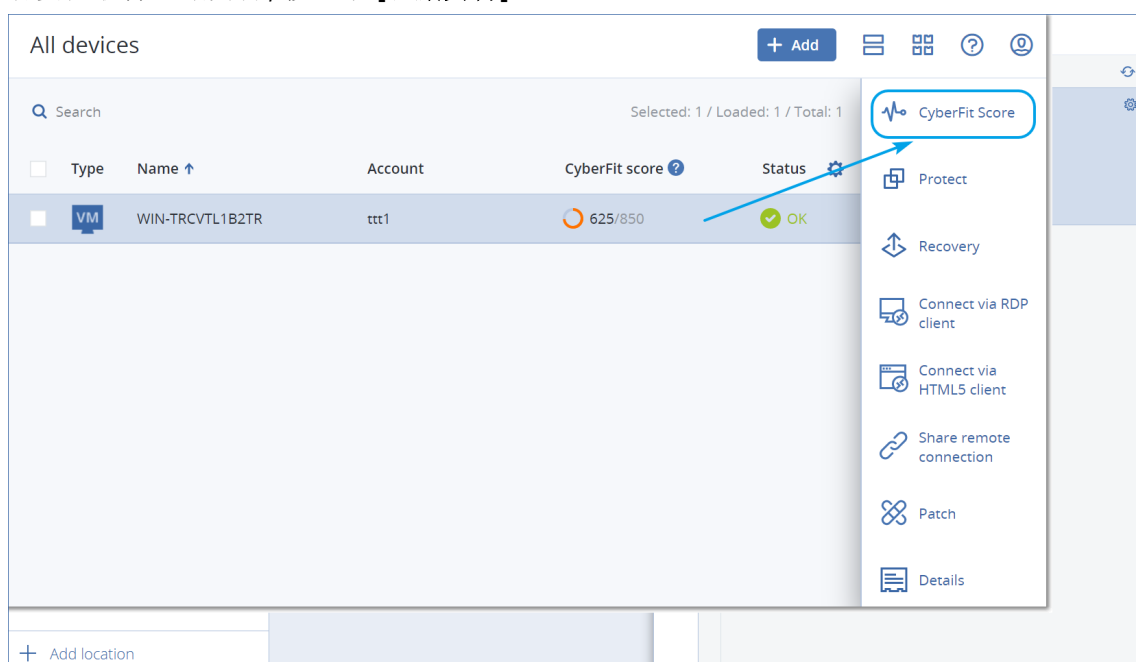
8. 指定位置。
9. 按一下 **[立即執行]** 可立即執行含鑑識資料的備份, 或根據排程, 等到建立備份為止。
10. 移至 **[監控]** > **[活動]**, 並確認已成功建立含鑑識資料的備份。

因此, 備份將包含鑑識資料, 而且您將能夠取得這些備份進行分析。含鑑識資料的備份會經過標示, 而且可以使用 **[僅搭配鑑識資料]** 選項, 在 **[備份儲存]** > **[位置]** 的其他備份中篩選出來。

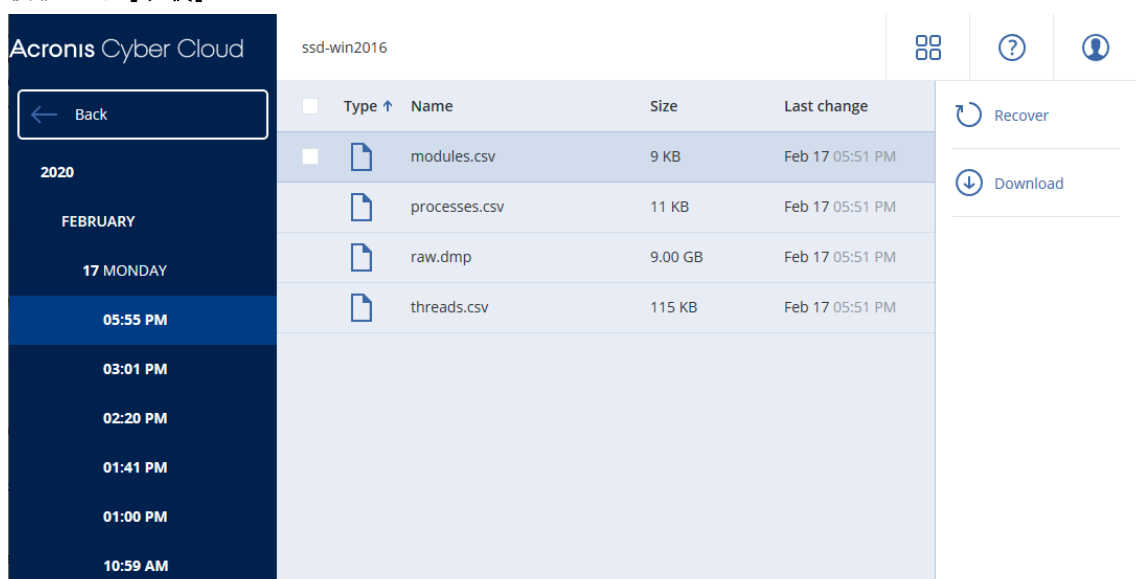
如何從備份取得鑑識資料?

1. 在服務主控台中, 移至 **[備份儲存]**, 然後選擇具有內含鑑識資料之備份的位置。
2. 選擇含鑑識資料的備份, 然後按一下 **[顯示備份]**。
3. 針對含鑑識資料的備份, 按一下 **[復原]**。

- 若要僅取得鑑識資料，按一下 **[鑑識資料]**。



系統將會顯示一個含鑑識資料的資料夾。選擇一個記憶體傾印檔案或其他任何鑑識檔案，然後按一下 **[下載]**。



- 若要復原完整鑑識備份，按一下 **[整部電腦]**。系統將會復原不含開機模式的備份。因此，可以檢查磁碟未經過變更。

您可以使用提供的記憶體傾印搭配數個協力廠商鑑識軟體，例如，使用 <https://www.volatilityfoundation.org/> 上的 Volatility Framework 進行進一步的記憶體分析。

公證含鑑識資料的備份

為確保含鑑識資料的備份就是所採用的映像而且未遭到損壞，備份模組可公證含鑑識資料的備份。

運作原理

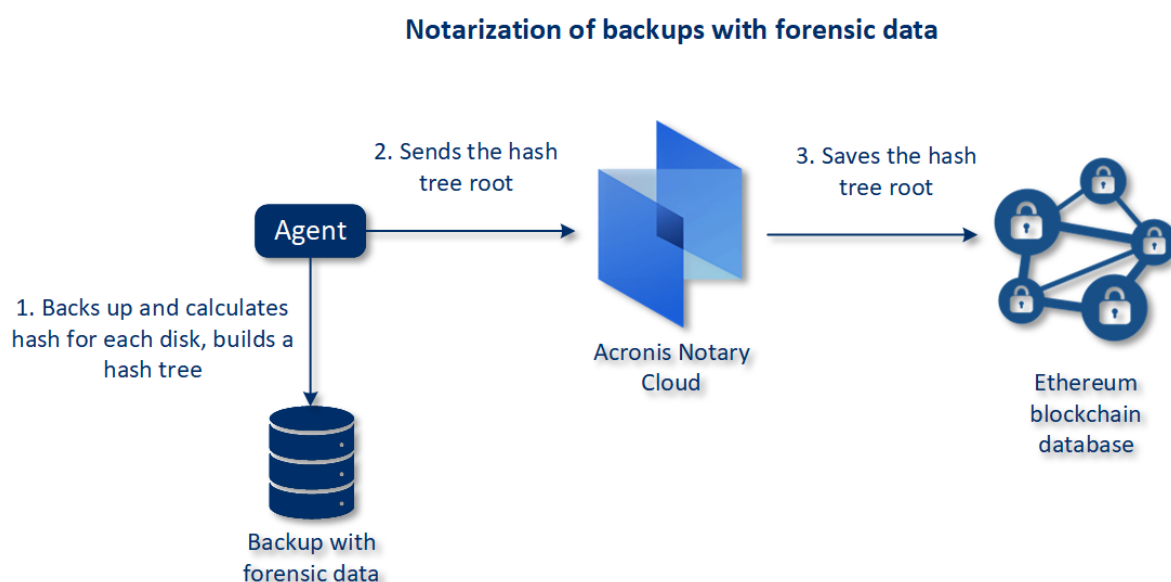
公證可讓您證明含鑑識資料的磁碟在備份後即是真實且未變更的。

在備份過程中，代理程式會計算已備份檔案的雜湊代碼、建置雜湊樹狀結構、儲存備份中的樹狀結構，然後將雜湊樹狀結構根部傳送到公證服務。公證服務將雜湊樹狀結構根部儲存在 Ethereum 區塊鏈資料庫中，以確保此值不會變更。

在驗證含鑑識資料之磁碟的真實性時，代理程式會計算磁碟雜湊，然後將其與儲存在備份內雜湊樹狀結構中的雜湊相比較。如果這些雜湊不相符，則磁碟會被視為不真實。否則，由雜湊樹狀結構保證磁碟的真實性。

若要驗證雜湊樹狀結構自身未受損，代理程式會將雜湊樹狀結構根部發送給公證服務。公證服務將其與儲存在區塊鏈資料庫中的雜湊相比較。如果雜湊相符，則所選磁碟保證為真實的。否則，軟體會顯示一則訊息，指示磁碟不真實。

以下的配置簡要地顯示含鑑識資料之備份的公證程序。



若要手動驗證公證的磁碟備份，您可以取得其憑證，並使用 **tibxread** 工具，依照與憑證一起顯示的驗證程序進行。

取得含鑑識資料之備份的憑證

若要從主控台取得含鑑識資料之備份的憑證，請執行下列動作：

1. 移至 **[備份儲存]**，然後選擇含鑑識資料的備份。
2. 復原整部電腦
3. 系統會開啟 **[磁碟對應]** 檢視畫面。
4. 按一下磁碟的 **[取得憑證]** 圖示。
5. 系統將會產生憑證，並使用憑證，在瀏覽器中開啟一個新視窗。在憑證下方，您將會看到手動驗證已公證磁碟備份的指示。

取得已備份資料的 "tibxread" 工具

Cyber Protection 提供稱為 **tibxread** 的工具，可手動檢查已備份磁碟的完整性。此工具可讓您從備份取得資料，並計算指定之磁碟的雜湊。此工具會自動與下列元件一起安裝：**Windows** 用代理程式、**Linux** 用代理程式和 **Mac** 用代理程式。

安裝路徑：與代理程式擁有的資料夾相同 (例如，C:\Program Files\BackupClient\BackupAndRecovery)。

支援的位置為：

- 本機磁碟
- 不需認證即可存取的網路資料夾 (CIFS/SMB)。

若是受密碼保護的網路資料夾，您可以使用作業系統工具，將網路資料夾掛載到本機資料夾，然後再掛載本機資料夾作為此工具的來源。

- 雲端儲存

您應該提供 URL、連接埠和憑證。URL 和連接埠可以從 Windows 登錄機碼或 Linux/Mac 電腦上的組態檔取得。

對於 Windows：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default<tenant_login>\FesUri
```

對於 Linux：

```
/etc/Acronis/BackupAndRecovery.config
```

對於 macOS：

```
/Library/Application Support/Acronis/Registry/BackupAndRecovery.config
```

憑證可以在下列位置找到：

對於 Windows：

```
%allusersprofile%\Acronis\BackupAndRecovery\OnlineBackup\Default
```

對於 Linux：

```
/var/lib/Acronis/BackupAndRecovery/OnlineBackup/Default
```

對於 macOS：

```
/Library/Application Support/Acronis/BackupAndRecovery/OnlineBackup/Default
```

此工具包含下列命令：

- list backups
- list content
- get content
- calculate hash

list backups

列出備份中的復原點。

SYNOPSIS:

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

選項

```
--loc=URI
--arc=BACKUP_NAME
--raw
--utc
--log=PATH
```

輸出範本:

```
GUID    日期    日期時間戳記
-----
<guid> <date> <timestamp>
```

<guid> – 備份 GUID。

<date> – 備份的建立日期。格式為 “DD.MM.YYYY HH24:MM:SS”。預設為當地時區 (可以使用 --utc 選項變更)。

輸出範例:

```
GUID    日期    日期時間戳記
-----
516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865
516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925
```

list content

列出復原點中的內容。

SYNOPSIS:

```
tibxread list content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID
--raw --log=PATH
```

選項

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--raw
--log=PATH
```

輸出範本：

```
磁碟      大小      公證狀態
-----
<number> <size> <notarization_status>
```

<number> – 磁碟的識別碼。

<size> – 以位元組為單位的大小。

<notarization_status> – 可能是下列狀態：未公證、已公證、下次備份。

輸出範例：

```
磁碟      大小      Notary 狀態
-----
1          123123465798 Notarized
2          123123465798 Notarized
```

get content

將復原點中指定之磁碟的內容寫入標準輸出 (stdout)。

SYNOPSIS:

```
tibxread get content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID -
-disk=DISK_NUMBER --raw --log=PATH --progress
```

選項

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
--progress
```

calculate hash

使用 SHA-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 主控台內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	您備份的加密密碼。如果備份未加密，請將此值留空。

碼	
--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： <pre> GUID 日期 日期時間戳記 ----- - 516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865 516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925 </pre> 含 "--raw" 的輸出： <pre> 516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865 516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925 </pre>
--utc	顯示 UTC 日期
--progress	顯示作業的進度。 例如： <pre> 1% 2% 3% 4% ... 100% </pre>

13.13.15 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。

13.13.16 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。

13.13.17 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。

13.13.18 多重磁碟區快照(M)

此選項適用於執行 Windows 或 Linux 之實體機器的備份。

此選項適用於磁碟層級備份。當檔案層級備份是藉由擷取快照的方式執行時，此選項也適用於檔案層級備份。(**[檔案層級備份快照]** 選項會決定是否要在檔案層級備份期間擷取快照)。

此選項會決定要同時或逐一擷取多個磁碟區的快照。

預設為：

- 如果選擇至少一部執行 Windows 的電腦進行備份：**[啟用]**。
- 其他情況：**[已停用]**。

啟用此選項時，系統會同時建立要備份之所有磁碟區的快照。此選項可用來為分佈在多個磁碟區的資料建立時間一致的備份，例如 Oracle 資料庫。

停用此選項時，系統會逐一擷取磁碟區的快照。因此，如果資料分佈在多個磁碟區，所產生的備份可能會有不一致的情形。

13.13.19 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（例如驗證）中包含的備份後命令和其他作業將會執行，而不受此選項影響。

預設為：**[已停用]**。

停用此選項時，可以利用下列參數，隨時執行備份（無論這些參數是否會針對預設值變更）：

- CPU 優先順序：**[低]**（在 Windows 中，會對應至 **[低於一般]**）。
- 輸出速度：**無限制**。

啟用此選項時，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。

Performance and backup window settings

No

Yes

AM

00

03

06

09

12

PM

03

06

09

AM

00

Sun

Mon

Tue

Wed

Thu

Fri

Sat

CPU priority

Low

Output speed

-

100

+

%

▼

CPU priority

Low

Output speed

-

25

+

%

▼

No backing up

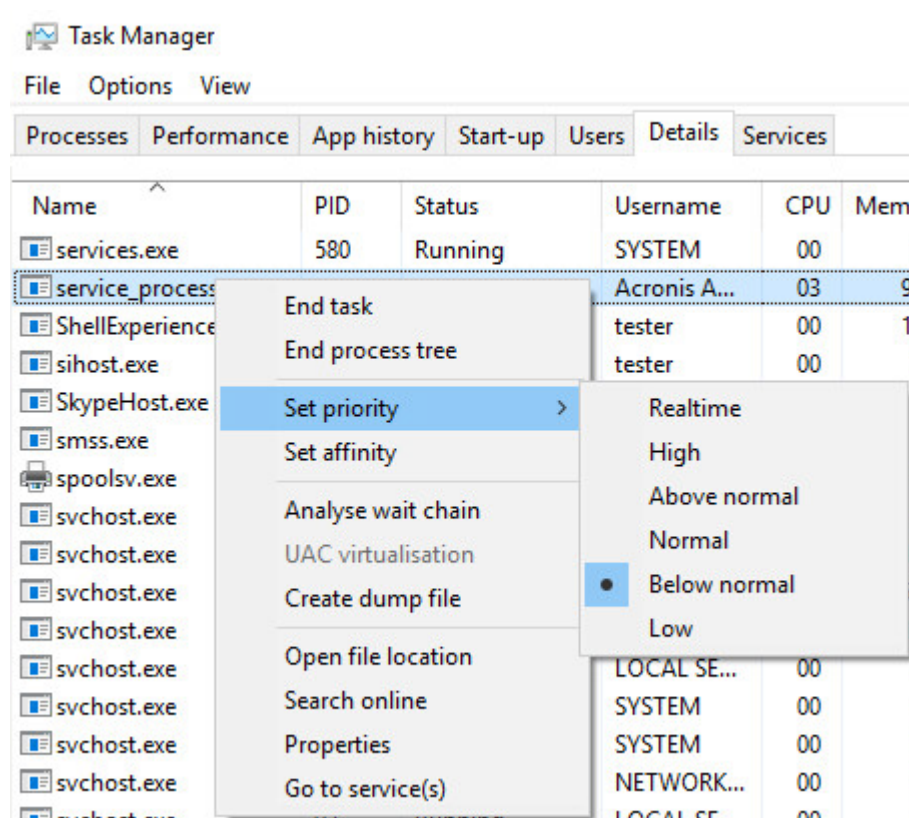
CPU 優先順序

此參數會定義作業系統內備份程序的優先順序。

可用設定包括：**[低]**、**[一般]**、**[高]**。

系統中執行程序的優先順序會決定分配給該程序的 CPU 和系統資源多寡。降低備份優先順序會釋放更多資源給其他應用程式。提高備份優先順序會要求作業系統配置更多資源 (例如 CPU) 給備份應用程式, 進而可加快備份程序。但是, 實際效果將取決於整體的 CPU 使用量和其他因素 (如磁碟輸入/輸出速度或網路流量)。

此選項可設定 Windows 中備份程序的優先順序 (**service_process.exe**), 以及 Linux 與 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)。

13.13.20 實體資料運送

如果備份或復原目的地為雲端儲存空間, 且備份格式設定為 **12 版**, 則可使用此選項。

此選項對於 Windows 用代理程式、Linux 用代理程式、Mac 用代理程式、VMware 用代理程式、Hyper-V 用代理程式, 以及 Virtuozzo 用代理程式所建立的磁碟層級備份和檔案備份有效。

使用此選項可透過「實體資料運送」服務，將保護計劃所建立的第一個完整備份傳送至硬碟機上的雲端儲存空間。後續的增量備份則是透過網路執行。

對於複寫至雲端的本機備份，增量備份則會繼續進行，並儲存在本機，直到初始備份上傳到雲端儲存空間為止。接著，所有增量變更都會複寫到雲端，並根據備份排程繼續複寫。

預設為：**[已停用]**。

關於「實體資料運送」服務

「實體資料運送」服務 Web 介面僅適用於系統管理員。

如需有關使用「實體資料運送」服務以及訂單建立工具的詳細指示，請參閱[實體資料運送系統管理員指南](#)。若要存取此文件，請在「實體資料運送」服務 Web 介面中，按一下問號圖示。

實體資料運送程序概觀

1. [運送將雲端儲存空間當作主要備份位置的備份]

- 建立備份到雲端的新保護計劃。
- 在 **[備份選項]** 列中，按一下 **[變更]**。
- 在可用選項的清單中，按一下 **[實體資料運送]**。

您可以直接備份到卸除式磁碟機，或者備份到本機或網路資料夾，然後將備份複製/移動到磁碟機。

2. [運送複寫到雲端的本機備份]

注意事項

Cyber Protect 代理程式 C21.06 版或更新版本支援此選項。

- 建立備份到本機或網路儲存空間的新保護計劃。
 - 按一下 **[新增位置]**，然後選擇 **[雲端儲存空間]**。
 - 在 **[雲端儲存空間]** 位置列中，按一下齒輪，然後選擇 **[實體資料運送]**。
- 在 **[使用實體資料運送]** 底下，按一下 **[是]**，然後按一下 **[完成]**。
在保護計劃中，會自動啟用 [加密] 選項，因為運送的所有備份都必須經過加密。
 - 在 **[加密]** 列中，按一下 **[指定密碼]**，然後輸入用於加密的密碼。
 - 在 **[實體資料運送]** 列中，選擇將儲存初始備份的卸除式磁碟機。
 - 按一下 **[建立]** 以儲存保護計劃。
 - 第一個備份完成後，請使用「實體資料運送」服務 Web 介面下載訂單建立工具，然後建立訂單。
若要存取此 Web 介面，請登入管理入口網站，按一下 **[概觀]** > **[使用量]**，然後按一下 **[實體資料運送]** 底下的 **[管理服務]**。

重要事項

一旦初始完整備份完成後，後續的備份必須由相同的保護計劃執行。另一個保護計劃即使是使用相同的參數且供相同的電腦使用，仍將需要另一個「實體資料運送」週期。

8. 封裝磁碟機並將其運送至資料中心。

重要事項

請確認您依照 [實體資料運送系統管理員指南](#) 中提供的封裝指示進行。

9. 使用「實體資料運送」服務 Web 介面追蹤訂單狀態。請注意，後續的備份將會失敗，直到初始備份上傳到雲端儲存為止。

13.13.21 事前/事後命令

此選項可以讓您定義在執行備份程序之前和之後要自動執行的命令。

以下配置說明事前/事後命令的執行時間。

備份事前命令	備份	備份事後命令

事前/事後命令使用方式的範例：

- 在開始備份之前，從磁碟中刪除部分暫存檔案。
- 設定在每次開始備份之前要啟動的第三方防毒產品。
- 選取備份，將其複製至其他位置。因為保護計劃中設定的複寫作業會將每個備份均複製至之後的位置，所以此選項可能相當實用。

執行完備份後命令之後，代理程式才會執行複寫。

程式不支援互動式命令，即需要使用者輸入的命令 (例如 [pause])。

備份事前命令

指定要在備份程序開始之前執行的命令/批次檔案

1. 啟用 **【備份之前執行命令】** 開關。
2. 在 **【命令...】** 欄位中輸入命令，或瀏覽至批次檔案。本程式不支援互動式命令，即需要使用者輸入的命令 (例如「pause」)。
3. 在 **【工作目錄】** 欄位中，指定將執行命令/批次檔案所在目錄的路徑。
4. 如有需要，請在 **【引數】** 欄位中指定該命令的執行引數。
5. 依據您要獲得的結果，選擇下表所述的相應選項。
6. 按一下 **【完成】**。

核取方塊	選擇			
若命令執行失敗，則放棄備份*	已選擇	已清除	已選擇	已清除
命令執行完成後再備份	已選擇	已選擇	已清除	已清除
結果				

	預設 僅在成功執行命令後執行備份。若命令執行失敗，則放棄備份。	執行命令後執行備份，無論命令執行是否成功。	不適用	執行命令的同時執行備份，無論命令執行的結果如何。

* 命令的結束碼如果不等於零便視為失敗。

注意事項

如果指令碼因為在 Linux 中發生與所需程式庫版本相關的衝突而失敗，請在指令碼中加入以下幾行，以排除 LD_LIBRARY_PATH 和 LD_PRELOAD 環境變數：

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

備份事後命令

指定備份完成後要執行的命令/可執行檔

1. 啟用 **【備份之後執行命令】** 開關。
2. 在 **【命令...】** 欄位中輸入命令，或瀏覽至批次檔案。
3. 在 **【工作目錄】** 欄位中，指定將執行命令/批次檔案所在目錄的路徑。
4. 在 **【引數】** 欄位中指定命令執行引數 (如有需要)。
5. 如果命令成功執行與否很重要，請選取 **【若命令執行失敗，則放棄備份】** 核取方塊。命令的結束碼如果不等於零，命令就視為失敗。如果命令執行失敗，則備份狀態將設為 **【錯誤】**。
如果未選擇核取方塊，則命令執行結果不會影響備份執行失敗或成功。您可以瀏覽 **【活動】** 標籤，以追蹤命令的執行結果。
6. 按一下 **【完成】**。

13.13.22 資料擷取前/後命令

透過選項，您可以定義要在資料擷取之前和之後自動執行的命令 (即拍攝資料快照)。資料擷取將於備份程序一開始的時候執行。

以下配置說明瞭何時在資料擷取前/後執行命令。

	<----- 備份 ----->				
備份事前命令	資料擷取事前命令	資料擷取	資料擷取事後命令	將資料寫入備份組	備份事後命令

與其他備份選項互動

其他備份選項可以修改資料擷取前/後執行的命令。

如果啟用了 **[多磁碟區快照]** 選項，則資料擷取前/後的命令將僅執行一次，因為將同時建立所有磁碟區快照。如果停用了 **[多磁碟區快照]** 選項，則將為每個要備份的磁碟區執行資料擷取前/後命令，因為快照是按照順序建立，而且是一個接著一個建立。

如果啟用 **[磁碟區陰影複寫服務 (VSS)]** 選項，則資料擷取前/後命令和 Microsoft VSS 作業將依照如下方式執行：

資料擷取前命令 > VSS 暫止 > 資料擷取 > VSS 繼續 > 資料擷取後命令

使用資料擷取事前/事後命令，您可以暫停和繼續與 VSS 不相容的資料庫或應用程式。由於資料擷取所需時間很短，因此資料庫或應用程式的閒置時間也會縮到最短。

資料擷取事前命令

指定要在資料擷取之前執行的命令/批次檔案

1. 啟用 **[資料擷取之前執行命令]** 開關。
2. 在 **[命令...]** 欄位中輸入命令，或瀏覽至批次檔案。本程式不支援互動式命令，即需要使用者輸入的命令 (例如「pause」)。
3. 在 **[工作目錄]** 欄位中，指定將執行命令/批次檔案所在目錄的路徑。
4. 如有需要，請在 **[引數]** 欄位中指定該命令的執行引數。
5. 依據您要獲得的結果，選擇下表所述的相應選項。
6. 按一下 **[完成]**。

核取方塊	選擇			
若命令執行失敗，則放棄備份*	已選擇	已清除	已選擇	已清除
命令執行完成後再執行資料擷取	已選擇	已選擇	已清除	已清除
結果				
	預設 僅在成功執行命令後執行資料擷取。若命令執行失敗，則放棄備份。	執行命令後執行資料擷取，無論命令執行是否成功。	不適用	執行命令的同時執行資料擷取，無論命令執行的結果如何。

* 命令的結束碼如果不等於零便視為失敗。

注意事項

如果指令碼因為在 Linux 中發生與所需程式庫版本相關的衝突而失敗，請在指令碼中加入以下幾行，以排除 LD_LIBRARY_PATH 和 LD_PRELOAD 環境變數：

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

資料擷取事後命令

指定要在資料擷取之後執行的命令/批次檔案

1. 啟用 **[資料擷取之後執行命令]** 開關。
2. 在 **[命令...]** 欄位中輸入命令，或瀏覽至批次檔案。本程式不支援互動式命令，即需要使用者輸入的命令 (例如「pause」)。
3. 在 **[工作目錄]** 欄位中，指定將執行命令/批次檔案所在目錄的路徑。
4. 如有需要，請在 **[引數]** 欄位中指定該命令的執行引數。
5. 依據您要獲得的結果，選擇下表所述的相應選項。
6. 按一下**[完成]**。

核取方塊	選擇			
若命令執行失敗，則放棄備份*	已選擇	已清除	已選擇	已清除
命令執行完成後再備份	已選擇	已選擇	已清除	已清除
結果				
	預設 僅在成功執行命令後繼續備份。	執行命令後繼續備份，無論命令執行是否成功。	不適用	執行命令的同時繼續備份，無論命令執行的結果如何。

* 命令的結束碼如果不等於零便視為失敗。

13.13.23 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：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。

13.13.24 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。

13.13.25 分割

此選項可讓您選取將較大備份分割成數個較小檔案的方法。

預設為：

- 如果備份位置為本機或網路 (SMB) 資料夾，而且備份格式為 12 版：**固定大小 - 200 GB**
此設定允許軟體在 NTFS 檔案系統上使用大量資料，而不會因為檔案分散程度造成負面影響。
- 其他情況：**自動**

以下是可用的設定：

- **自動**
若超過檔案系統可支援的檔案大小上限，就會切割備份。

- **固定大小**

輸入所需的檔案大小或從下拉式清單中選擇。

13.13.26 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]**。

13.13.27 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。

13.13.28 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。

13.13.29 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，備份軟體會分別使用 VMWare Tools、Hyper-V 整合服務、Virtuozzo Guest Tools、Red Hat Virtualization Guest Tools 或 QEMU Guest Tools，將 VSS 套用到虛擬機器內。

注意事項

對於 Red Hat Virtualization (oVirt) 虛擬機器，建議您安裝 QEMU Guest Tools 而非 Red Hat Virtualization Guest Tools。有些 Red Hat Virtualization Guest Tools 版本不支援應用程式一致的快照。

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。

啟用 **[虛擬機器的磁碟區陰影複製服務 (VSS)]** 選項也會在備份的虛擬機器上，觸發您可能擁有的凍結前和解除凍結後指令碼。如需有關這些指令碼的詳細資訊，請參閱 "自動執行凍結前和解除凍結後指令碼" (第 332 頁)。

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。

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 Tools 是否安裝在虛擬機器上。

13.13.30 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]**。

13.13.31 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]**。

13.14 復原

13.14.1 復原快速鍵清單

下表摘述可用的復原方法。使用此表格來選擇最適合您需求的復原方法。

注意事項

在「加強安全性」模式下，透過 Web 介面復原不適用於租用戶。

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、Red Hat Virtualization (oVirt) 或 Scale Computing HC3)	使用 Web 介面 使用可開機媒體
虛擬機器或容器 (Virtuozzo、Virtuozzo Hybrid Server 或 Virtuozzo Hybrid Infrastructure)	使用 Web 介面
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
網站	使用 Web 介面
Microsoft 365	
信箱 (本機 Microsoft 365 用代理程式)	使用 Web 介面
信箱 (雲端 Microsoft 365 用代理程式)	使用 Web 介面
公用資料夾	使用 Web 介面
OneDrive 檔案	使用 Web 介面
SharePoint Online 資料	使用 Web 介面
Google Workspace	
信箱	使用 Web 介面
Google 雲端硬碟檔案	使用 Web 介面
共用磁碟機檔案	使用 Web 介面

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。

13.14.2 安全復原

備份的 OS 映像中可能有復原後重新感染電腦的惡意程式碼。

安全復原功能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。

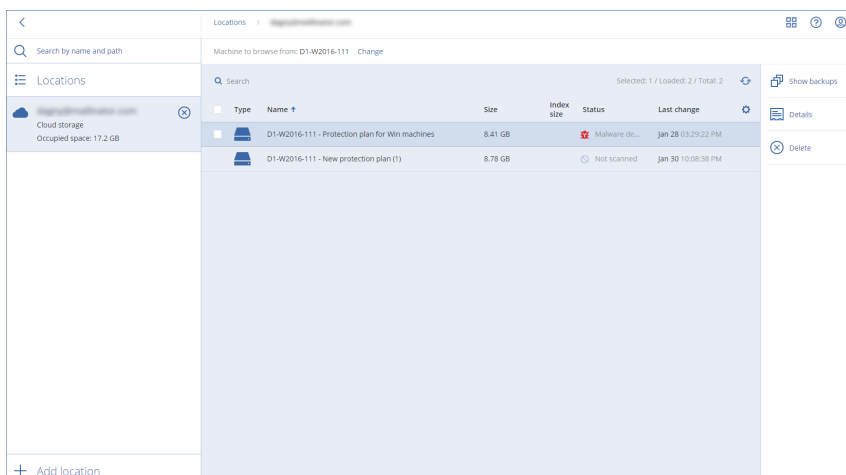
限制：

- 只有電腦內已安裝 Windows 用代理程式的實體或虛擬 Windows 電腦支援安全復原。
- 支援的備份類型為「整部電腦」或「磁碟/磁碟區」備份。
- 只有具有 NTFS 檔案系統的磁碟區才支援安全復原。非 NTFS 磁碟分割將會在不經過防惡意程式碼掃描的情況下復原。
- [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，請啟動 **[檔案/資料夾]** 復原。

運作原理

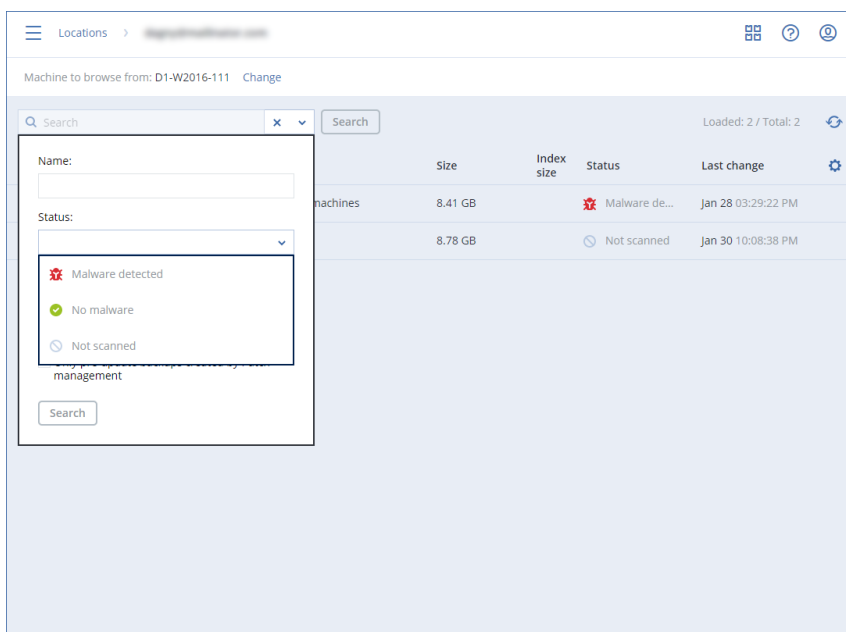
如果您在復原過程中啟用 [安全復原] 選項，則系統將會執行下列操作：

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。



1. 將備份復原至選定的電腦。
2. 刪除偵測到的惡意程式碼。

您可以使用 **[狀態]** 參數篩選備份。



13.14.3 復原電腦

復原實體電腦

本節說明使用 **Web** 介面來復原實體機器。

如果您要復原下列項目, 請使用可開機媒體, 而不要使用 **Web** 介面:

- 執行 **macOS** 的電腦
- 在「加強安全性」模式下租用戶中的電腦
- 裸機或離線電腦上的任何作業系統

- 邏輯磁碟區 (Linux 中邏輯磁碟區管理器所建立的磁碟區) 的結構。媒體可讓您自動重新建立邏輯磁碟區結構。

使用重新啟動復原

復原作業系統以及復原使用 BitLocker 加密的磁碟機都必須重新啟動。您可選擇要自動重新啟動電腦, 或指派電腦**需要互動**狀態。復原的作業系統即會自動上線。

重要事項

已備份的加密磁碟區會被當作未加密復原。

復原使用 BitLocker 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。如果未符合其中一個條件, 則復原會失敗。

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。

注意事項

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] 錯誤, 請嘗試停用 [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](#)。

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。

× Recover machine
?

RECOVER TO
Physical machine ▼

TARGET MACHINE
ssd-win2016

DISK MAPPING
Disk 1 → Disk 1
Disk 2 → Disk 2
Disk 3 → Disk 3

SAFE RECOVERY
☐ Off ⓘ

START RECOVERY
RECOVERY OPTIONS

- 如果您不滿意對應結果，或磁碟對應失敗，可以按一下 **【磁碟區對應】** 手動重新對應磁碟。該對應區段使您還可以選擇要復原的個別磁碟或磁碟區。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。

× Disk mapping
Switch to volume mapping

Backup

Target machine

☒ Disk 1

System Reserved 350 MB

NTFS (C:) 59.7 GB

☒ Disk 2

New Volume (E:) 39.9 GB

Disk 1

System Reserved 350 MB

C: 59.7 GB

Unallocated 1.00 MB

NT signature auto ▼

Disk 2

New Volume (E:) 39.9 GB

NT signature auto ▼

- [選擇性] 啟用 **【安全復原】** 以掃描備份中的惡意程式碼。如果偵測到惡意程式碼，將會在備份中標示初來，並在復原程序完成後立即刪除。
- 按一下 **【開始復原】**。

8. 確認您要以磁碟的備份版本來覆寫磁碟。選擇是否要自動重新啟動電腦。
復原進度會顯示在 **[活動]** 索引標籤上。

實體機器到虛擬

您可以在其中一個支援的 Hypervisor 上，將實體機器復原至虛擬機器。這也是將實體機器移轉至虛擬機器的機制。如需有關支援的 P2V 移轉路徑的詳細資訊，請參閱「[電腦移轉](#)」。

本節說明使用 Web 介面將實體機器復原至虛擬機器。至少在 Acronis Management Server 中為相關的 Hypervisor 安裝並註冊一個代理程式，才能執行此作業。例如，復原至 VMware ESXi 需要在環境中至少安裝並註冊一個 VMware 用代理程式；復原至 Hyper-V 則需要在環境中至少安裝並註冊一個 Hyper-V 用代理程式。

在「加強安全性」模式下，透過 Web 介面復原不適用於租用戶。

注意事項

您無法將 macOS 虛擬機器復原至 Hyper-V 主機，因為 Hyper-V 不支援 macOS。您可以將 macOS 虛擬機器復原至 Mac 硬體上安裝的 VMware 主機。

此外，您無法將 macOS 實體機器的備份當作虛擬機器復原。

如果要將實體機器復原為虛擬機器

1. 選擇已備份的電腦。
2. 按一下 **[復原]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。

如果電腦處於離線狀態，復原點就不會顯示。執行下列任何一項作業：

- 如果備份位置是雲端或共用儲存 (即可被其他代理程式存取)，按一下 **[選擇電腦]**，選擇在線上的電腦，然後選擇復原點。
- 在 **[備份儲存]** 索引標籤上選擇復原點。
- 如 [< 使用可開機媒體復原磁碟 >](#) 所述來復原電腦。

4. 按一下 **[復原] > [整部機器]**。
5. 在 **[復原至]** 中選擇 **[虛擬機器]**。
6. 按一下 **[目標電腦]**。
 - a. 選擇 Hypervisor。

注意事項

必須至少在 Acronis Management Server 中為該 Hypervisor 安裝並註冊一個代理程式。

- b. 選擇主機並指定新電腦名稱，或選擇現有目標電腦。最好選擇新電腦，這樣目標電腦的磁碟組態就不需完全符合備份中的磁碟組態。
 - c. 選擇主機並指定新電腦名稱，或選擇現有目標電腦。
 - d. 按一下 **[確定]**。
7. [若是 Virtuozzo Hybrid Infrastructure] 按一下 **[VM 設定]** 以選擇 **[類別]**。您可以選擇性地變更記憶體大小、處理器數量，以及虛擬機器的網路連線。

注意事項

選擇類別是 Virtuoizzo Hybrid Infrastructure 的必要步驟。

8. [選用] 設定其他復原選項：

- [不適用於 Virtuoizzo Hybrid Infrastructure] 按一下 **[資料存放區]** (ESXi), 或按一下 **[路徑]** (Hyper-V), 然後選擇虛擬機器的資料存放區 (儲存空間)。
- 按一下 **[磁碟對映]** 為每個虛擬磁碟選擇資料存放區 (儲存)、介面以及佈建模式。該對映區段使您還可以選擇要復原的個別磁碟。
若是 Virtuoizzo Hybrid Infrastructure, 您僅能選擇目標磁碟的儲存原則。方法是, 選擇所需的目標磁碟, 然後按一下 **[變更]**。在開啟的刀鋒視窗中, 按一下齒輪圖示、選擇儲存原則, 然後按一下 **[完成]**。
- [若是 VMware ESXi、Hyper-V 和 Red Hat Virtualization/oVirt] 按一下 **[VM 設定]** 以變更記憶體大小、處理器數量, 以及虛擬機器的網路連線。

RECOVER TO
Virtual machine

TARGET MACHINE
New machine on 10.250.22.17 New

DATASTORE
datastore1 (1)

DISK MAPPING
Disk 1 → datastore1 (1), 50.0 GB
Disk 2 → datastore1 (1), 50.0 GB

VM SETTINGS
Memory: 2.00 GB
Virtual processors: 2
Network adapters: 2

START RECOVERY ⚙️ RECOVERY OPTIONS

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

您可以從其備份復原虛擬機器。

注意事項

在「加強安全性」模式下，透過 Web 介面復原不適用於租用戶。

必要條件

- 復原至虛擬機器時，此虛擬機器必須為停止狀態。軟體預設不會顯示提示，即停止電腦。復原完成後，您必須手動啟動電腦。您可以使用 VM 電源管理復原選項來變更預設行為 (按一下 **[復原選項]** > **[VM 電源管理]**)。

程序

- 執行下列其中一項操作：
 - 選擇已備份的電腦，按一下 **復原**，然後選擇復原點。
 - 在 **[備份儲存]** 索引標籤上選擇復原點。
- 按一下 **[復原]** > **[整部機器]**。
- 如果您想要復原到實體機器，請在 **復原至** 中選擇 **實體機器**。否則，請跳過此步驟。

只有在目標電腦的磁碟組態完全符合備份中的磁碟組態時，才能復原至實體機器。

在此情況下，請繼續在「**實體機器**」中的步驟 4。否則，我們建議您使用 **可開機媒體** 來執行 V2P 移轉。
- [選擇性]** 軟體預設會自動選擇原始電腦做為目標電腦。若要復原到另一部虛擬機器，請按一下 **目標機器** 然後進行以下操作：
 - 選擇 Hypervisor (**[VMware ESXi]**、**[Hyper-V]**、**[Virtuozzo]**、**[Virtuozzo Hybrid Infrastructure]**、**[Scale Computing HC3]** 或 **[oVirt]**)。

只有 Virtuozzo 虛擬機器可復原至 Virtuozzo。如需 V2V 移轉的詳細資訊，請參閱「**電腦移轉**」。
 - 選擇主機並指定新電腦名稱，或選擇現有目標電腦。
 - 選擇主機並指定新電腦名稱，或選擇現有目標電腦。
 - 按一下 **[確定]**。
- 設定您需要的其他復原選項。
 - [選用]** **[不適用於 Virtuozzo Hybrid Infrastructure 和 Scale Computing HC3]** 若要選擇虛擬機器的資料存放區，按一下 **[資料存放區]** (ESXi)、**[路徑]** (Hyper-V 和 Virtuozzo)，或 **[儲存網域]** (Red Hat Virtualization (oVirt))，然後選擇虛擬機器的資料存放區 (儲存空間)。
 - [選用]** 若要檢視每個虛擬磁碟的資料存放區 (儲存空間)、介面以及佈建模式，按一下 **[磁碟對應]**。除非您要復原 Virtuozzo 容器或 Virtuozzo Hybrid Infrastructure 虛擬機器，否則您可以變更這些設定。

若是 Virtuozzo Hybrid Infrastructure，您僅能選擇目標磁碟的儲存原則。方法是，選擇所需的目標磁碟，然後按一下 **[變更]**。在開啟的刀鋒視窗中，按一下齒輪圖示、選擇儲存原則，然後按一下 **[完成]**。

該對映區段使您還可以選擇要復原的個別磁碟。

- [選用][適用於 VMware ESXi、Hyper-V 和 Virtuozzo] 若要變更記憶體大小、處理器數量，以及虛擬機器的網路連線，請按一下 **[VM 設定]**。
- [若是 Virtuozzo Hybrid Infrastructure] 若要變更虛擬機器的記憶體大小和處理器數量，請選擇 **[類別]**。

RECOVER TO
Virtual machine

TARGET MACHINE
New machine on 10.250.22.17 New

DATASTORE
datastore1 (1)

DISK MAPPING
Disk 1 → datastore1 (1), 50.0 GB
Disk 2 → datastore1 (1), 50.0 GB

VM SETTINGS
Memory: 2.00 GB
Virtual processors: 2
Network adapters: 2

START RECOVERY

 RECOVERY OPTIONS

6. 按一下 **[開始復原]**。
7. 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。

使用可開機媒體復原磁碟

如需有關如何建立可開機媒體的資訊，請參閱 "建立實體可開機媒體" (第 522 頁)。

使用可開機媒體復原磁碟

1. 使用可開機媒體將目標電腦開機。
2. [僅在復原 Mac 時] 若您要將 APFS 格式化的磁碟/磁碟區復原至非原始電腦或裸機，則會手動重新建立原始磁碟組態：
 - a. 按一下 **[磁碟公用程式]**。
 - b. 清除目標磁碟並將其格式化為 APFS。如需說明，請參閱 <https://support.apple.com/en-us/HT208496#erasedisk>。

- c. 重新建立原始磁碟組態。如需說明，請參閱 <https://support.apple.com/guide/disk-utility/add-erase-or-delete-apfs-volumes-dskua9e6a110/19.0/mac/10.15>。
- d. 按一下 **[磁碟公用程式]** > **[結束磁碟公用程式]**。
3. 按一下 **[在本機管理此電腦]** 或按兩次 **[救援可開機媒體]**，視您使用的媒體類型而定。
4. 如果您的網路中已啟用 Proxy 伺服器，請按一下 **[工具]** > **[Proxy 伺服器]**，然後指定 Proxy 伺服器主機名稱/IP 位址、連接埠和認證。否則，請跳過此步驟。
5. [選擇性] 復原 Windows 或 Linux 時，按一下 **[工具]** > **[在 Cyber Protection 服務中註冊媒體]**，然後指定您在下載媒體時取得的註冊權杖。如果您這麼做，您將不需要輸入認證或註冊碼，就可以存取雲端儲存空間，如步驟 8 所述。
6. 在歡迎畫面上，按一下 **[復原]**。
7. 按一下 **[選擇資料]**，然後按一下 **[瀏覽]**。
8. 指定備份位置：
 - 若要從雲端儲存進行復原，請選擇 **[雲端儲存]**。輸入已指派備份電腦之帳戶的認證。復原 Windows 或 Linux 時，您可以選擇要求註冊碼，並使用該註冊碼代替認證。按一下 **[使用註冊碼]** > **[要求代碼]**。軟體將會顯示註冊連結和註冊碼。您可以複製註冊連結和註冊碼，並在另一部電腦上執行註冊步驟。註冊碼的有效期限為一小時。
 - 若要從本機或網路資料夾進行復原，請瀏覽至 **[本機資料夾]** 或 **[網路資料夾]** 下的資料夾。按一下 **[確定]** 以確認您的選擇。
9. 選擇您要從中復原資料的備份。如果看到提示，請輸入備份的密碼。
10. 在 **[備份內容]** 中，選擇您要復原的磁碟。按一下 **[確定]** 以確認您的選擇。
11. 在 **[復原目標位置]** 下，軟體會自動將已選擇的磁碟對應至目標磁碟。如果對應不成功，或如果您不滿意對應結果，您可以手動重新對應磁碟。

注意事項

變更磁碟配置可能會影響作業系統的開機能力。除非您有十足的把握會成功，否則請使用原始電腦的磁碟配置。

12. [復原 Linux 時] 如果備份電腦有邏輯磁碟區 (LVM)，而您想要重現原始的 LVM 架構：
 - a. 請確保目標電腦磁碟數目和每個磁碟的容量等於或超過原始電腦，然後按一下 **[套用 RAID/LVM]**。
 - b. 檢閱磁碟區結構，然後按一下 **[套用 RAID/LVM]** 以建立磁碟區結構。
13. [選擇性步驟] 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. 如果電腦上有多个作業系統，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

13.14.4 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，您也可以每次使用 Universal Restore 時，直接指定存放庫路徑。

13.14.5 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

13.14.6 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。

13.14.7 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。

13.14.8 復原檔案

使用 Web 介面復原檔案

注意事項

在「加強安全性」模式下，透過 Web 介面復原不適用於租用戶。

1. 選擇原本存放所要復原之資料的電腦。
2. 按一下 **[復原]**。
3. 選擇復原點。請注意，復原點是依照位置進行篩選。

如果選擇實體且離線的電腦，則不會顯示復原點。執行下列任何一項作業：

- **[建議]** 如果備份位置是雲端或共用儲存 (即可被其他代理程式存取)，按一下 **[選擇電腦]**，選擇在線上的目標電腦，然後選擇復原點。
- 在 **[備份儲存]** 索引標籤上選擇復原點。
- [從雲端儲存下載檔案](#)。
- [使用可開機媒體](#)。

4. 按一下 **[復原]** > **[檔案/資料夾]**。
5. 瀏覽至所需的資料夾，或使用搜尋列以取得所需檔案和資料夾的清單。

搜尋與語言無關。

您可以使用一或多個萬用字元 (* 和 ?)。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。

如果您的選取項目含有資料夾，或者所選檔案的大小總計超過 100 MB，則無法下載。若要從雲端擷取更大量的資料，請使用程序 [「從雲端儲存下載檔案」](#) (第 223 頁)。

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、Virtuozzo 用代理程式、Scale Computing

HC3 用代理程式或 oVirt 用代理程式的電腦 (如果檔案源自於 ESXi、Hyper-V、Virtuozzo、Scale Computing HC3 或 Red Hat Virtualization/oVirt 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

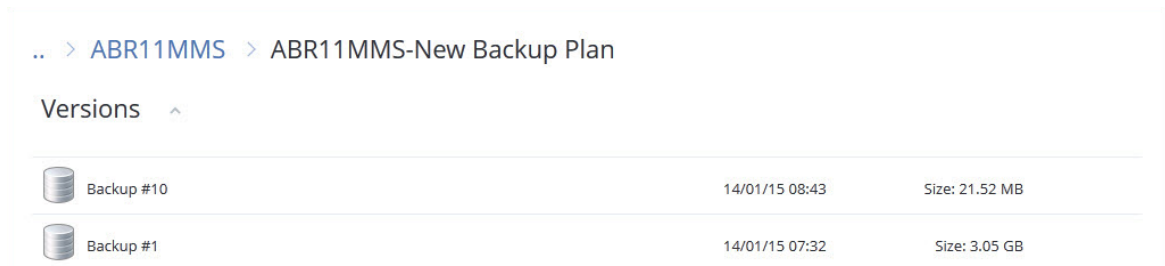
您可瀏覽雲端儲存、檢視備份內容, 然後下載您所需的檔案。

限制

- 無法瀏覽系統狀態、SQL 資料庫與 Exchange 資料庫的備份。

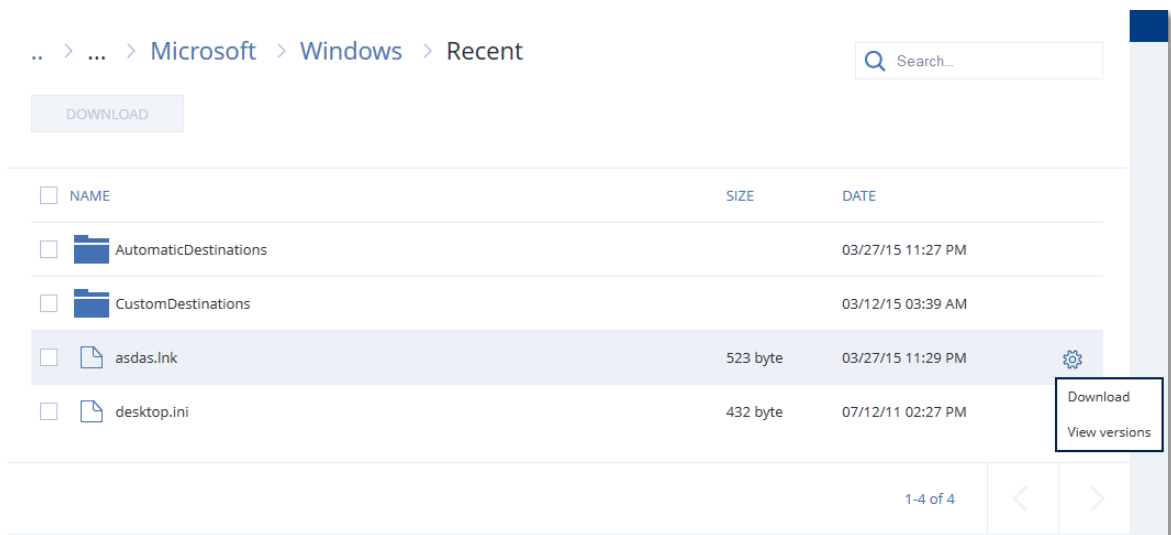
如果要從雲端儲存下載檔案

1. 選擇已經備份的電腦。
2. 按一下 **[復原]>[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, 或使用搜尋列以取得所需檔案的清單。
搜尋與語言無關。



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

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

ASign 是允許多人以電子方式簽署檔案的一項服務。此功能僅適用於儲存在雲端儲存中的檔案層級備份。

一次只能簽署一個檔案版本。如果多次備份檔案，則必須選擇要簽署的版本，而且只會簽署該版本。

例如，ASign 可用於以電子方式簽署如下檔案：

- 出租或租用協議
- 銷售合約
- 資產購買協議
- 貸款協議
- 權限名單
- 財務文件
- 保險文件
- 責任拋棄
- 醫療保健文件
- 調查報告
- 真品證明書
- 非公開協議
- 報價書
- 機密性協議
- 獨立承包商協議

要簽署檔案版本

1. 選擇檔案，如「[使用 Web 介面復原檔案](#)」一節步驟 1-6，或「[從雲端儲存空間下載檔案](#)」一節步驟 1-5 中所述。
2. 確認左面板上已選擇正確的日期與時間。
3. 按一下 **簽署此檔案版本**。
4. 指定要在其下儲存備份的雲端儲存帳戶的密碼。提示視窗中會顯示登入帳戶。
ASign 服務介面會在 Web 瀏覽器視窗中開啟。
5. 透過指定電子郵件地址新增其他簽署人。傳送邀請之後，就無法新增或移除簽署人，因此請確認清單中包含需要其簽章的所有人。
6. 按一下 **[邀請簽署]** 傳送邀請給簽署人。
各簽署人均收到帶有簽名請求的電子郵件訊息。所有已請求的簽署人簽署檔案後，表示該檔案已透過公證服務完成公證及簽署。
當每個簽署人簽署檔案且整個流程完成時，您將收到通知。您可以透過按一下所收到的任一電子郵件訊息中的 **[檢視詳細資料]** 來存取 ASign 網頁。
7. 當程序完成時，請前往 ASign 網頁並按一下 **[獲取文件]** 下載 .pdf 文件，其中包含：
 - 收集簽章的簽署憑證頁。
 - 具有活動歷程記錄的「審計存底」頁面：將邀請傳送至簽署人的時間，各簽署人簽署檔案的時間等。

使用可開機媒體復原檔案

如需有關如何建立可開機媒體的資訊，請參閱 [< 建立可開機媒體 >](#)。

如果要使用可開機媒體復原檔案

1. 使用可開機媒體將目標電腦開機。
2. 按一下 **[在本機管理此電腦]** 或按兩次 **[救援可開機媒體]**，視您使用的媒體類型而定。
3. 如果您的網路中已啟用 Proxy 伺服器，請按一下 **[工具] > [Proxy 伺服器]**，然後指定 Proxy 伺服器主機名稱/IP 位址、連接埠和認證。否則，請跳過此步驟。
4. [選擇性] 復原 Windows 或 Linux 時，按一下 **[工具] > [在 Cyber Protection 服務中註冊媒體]**，然後指定您在下載媒體時取得的註冊權杖。如果您這麼做，您將不需要輸入認證或註冊碼，就可以存取雲端儲存空間，如步驟 7 所述。
5. 在歡迎畫面上，按一下 **[復原]**。
6. 按一下 **[選擇資料]**，然後按一下 **[瀏覽]**。
7. 指定備份位置：
 - 若要從雲端儲存進行復原，請選擇 **[雲端儲存]**。輸入已指派備份電腦之帳戶的認證。
復原 Windows 或 Linux 時，您可以選擇要求註冊碼，並使用該註冊碼代替認證。按一下 **[使用註冊碼] > [要求代碼]**。軟體將會顯示註冊連結和註冊碼。您可以複製註冊連結和註冊碼，並在另一部電腦上執行註冊步驟。註冊碼的有效期限為一小時。
 - 若要從本機或網路資料夾進行復原，請瀏覽至 **[本機資料夾]** 或 **[網路資料夾]** 下的資料夾。
按一下 **[確定]** 以確認您的選擇。
8. 選擇您要從中復原資料的備份。如果看到提示，請輸入備份的密碼。
9. 在 **[備份內容]** 中選擇 **[資料夾/檔案]**。
10. 選擇您要復原的資料。按一下 **[確定]** 以確認您的選擇。
11. 在 **[復原目的地]** 下指定資料夾。或者，您也可禁止覆寫較新版本的檔案或將某些檔案排除在復原之外。
12. [選擇性步驟] 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。

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。

13.14.9 復原系統狀態

注意事項

在「加強安全性」模式下，透過 Web 介面復原不適用於租用戶。

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。

13.14.10 復原 ESXi 設定

若要復原 ESXi 設定，您需要 Linux 型的可開機媒體。如需有關如何建立可開機媒體的資訊，請參閱 "建立實體可開機媒體" (第 522 頁)。

如果您正在將 ESXi 設定復原至非原始主機，而原始 ESXi 主機仍連線至 vCenter Server，請中斷這部主機與 vCenter Server 的連線並從中移除，以避免復原期間發生意外問題。若要同時保留原始主機與復原主機，您可以在完成復原後將其再次加入。

在主機上執行的虛擬機器未包含在 ESXi 設定備份中。這些虛擬機器可以另行單獨備份和復原。

復原 ESXi 設定

1. 使用可開機媒體將目標電腦開機。
2. 按一下 **[在本機管理這部電腦]**。
3. 在歡迎畫面上，按一下 **[復原]**。
4. 按一下 **[選擇資料]**，然後按一下 **[瀏覽]**。
5. 指定備份位置：
 - 瀏覽至 **[本機資料夾]** 或 **[網路資料夾]** 下的資料夾。按一下 **[確定]** 以確認您的選擇。
6. 在 **[顯示]** 中，選擇 **[ESXi 設定]**。
7. 選擇您要從中復原資料的備份。如果看到提示，請輸入備份的密碼。
8. 按一下 **[確定]**。
9. 在 **[要用於新資料存放區的磁碟]** 中，執行以下動作：
 - 在 **[將 ESXi 復原至]** 下，選擇將復原主機設定的磁碟。如果您正在將設定復原至原始主機，則會依據預設選擇原始磁碟。

- [選擇性步驟] 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。

13.14.11 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 與 Virtuozzo	Windows
備份驗證	+	+	+	+	+	+	+	+	+
開機模式	+	-	-	-	-	-	-	+	-
檔案日期與時間	-	-	-	+	+	+	+	-	-
錯誤處理	+	+	+	+	+	+	+	+	+
檔案排除	-	-	-	+	+	+	+	-	-
檔案層級安全性	-	-	-	+	-	-	-	-	-
Flashback	+	+	+	-	-	-	-	+	-
復原完整路徑	-	-	-	+	+	+	+	-	-

掛載點	-	-	-	+	-	-	-	-	-
效能	+	+	-	+	+	+	-	+	+
事前/事後命令	+	+	-	+	+	+	-	+	+
SID 變更	+	-	-	-	-	-	-	-	-
VM 電源管理	-	-	-	-	-	-	-	+	-
Windows 事件日誌	+	-	-	+	-	-	-	僅 Hyper-V	+

備份驗證

此選項定義從備份復原資料前，是否驗證備份以確保備份未損毀。此作業是由保護代理程式所執行。

預設為：**[已停用]**。

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

視您的服務提供者所選擇的設定而定，可能無法在備份到雲端儲存空間時進行驗證。

開機模式

此選項適用於從含有 Windows 作業系統之磁碟層級備份復原實體機器或虛擬機器。。

此選項可讓您選擇 Windows 在復原後將使用的開機模式 (BIOS 或 UEFI)。如果原始電腦的開機模式與所選開機模式不同，則軟體會：

- 根據所選擇的開機模式 (BIOS 的 MBR、UEFI 的 GPT)，初始化您要復原系統磁碟區的目的地磁碟。
- 調整 Windows 作業系統，讓系統可使用所選開機模式啟動。

預設為：**如同在目標電腦上。**

可選擇以下一個選項：

- **如同在目標電腦上**
目標電腦上執行的代理程式會偵測 Windows 目前使用的開機模式，並根據偵測到的開機模式進行調整。

除非下列限制適用，否則這是自動導致可開機系統的最安全值。由於可開機媒體下沒有 **[開機模式]** 選項，因此媒體上的代理程式會一律執行如同選擇此值時的行為。

- **如同在已備份的電腦上**

目標電腦上執行的代理程式會從備份讀取開機模式，並根據此開機模式進行調整。這有助於在不同電腦上復原系統，即使此電腦使用其他開機模式也行，然後取代已備份電腦中的磁碟。

- **BIOS**

目標電腦上執行的代理程式會進行調整，以使用 BIOS。

- **UEFI**

目標電腦上執行的代理程式會進行調整，以使用 UEFI。

一旦設定變更之後，將會重複磁碟對應程序。這需要花費一些時間。

建議

如果您需要在 UEFI 和 BIOS 之間轉換 Windows：

- 復原系統磁碟區所在位置的整個磁碟。如果在現有磁碟區上僅復原系統磁碟區，代理程式將無法正確初始化目標磁碟。
- 請記得，BIOS 不允許使用 2 TB 以上的磁碟空間。

限制

- 下列系統支援在 UEFI 和 BIOS 之間的轉換：
 - 從 Windows 7 開始的 64 位元作業系統
 - 自 Windows Server 2008 SP1 之後的 64 位元 Windows Server 作業系統
- 如果備份儲存在磁帶裝置上，則不支援 UEFI 和 BIOS 之間的轉換。

如果不支援在 UEFI 和 BIOS 之間轉換系統，則代理程式會執行如同已選擇 **[如同在已備份的電腦上]** 設定時的行為。如果目標電腦同時支援 UEFI 與 BIOS 系統，您必須手動啟用與原始電腦對應的開機模式，否則系統將無法啟動。

檔案日期與時間

此選項僅在復原檔案時有效。

此選項定義是從備份復原檔案的日期與時間，還是將目前的日期與時間指派給檔案。

若啟用此選項，會將目前的日期與時間指派給檔案。

預設為：**[啟用]**。

錯誤處理

這些選項可讓您指定如何處理復原期間可能發生的錯誤。

發生錯誤時重新嘗試

預設為：**啟用**。**嘗試次數:30**。**嘗試間隔:30 秒**。

如果發生可復原的錯誤，程式將重新嘗試執行未成功的作業。您可以設定時間間隔和嘗試次數。一旦作業成功「或是」已執行指定次數的嘗試後 (以先發生者為準)，軟體將停止嘗試。

處理時不顯示訊息和對話方塊 (無訊息模式)

預設為：**[已停用]**。

啟用無訊息模式後，程式將自動處理需要使用者互動的情形 (如有可能)。如果需要使用者互動方可繼續，則作業將失敗。可在作業記錄中找到作業的詳細記錄，包括錯誤 (若有)。

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，則 MyFile.tmp 檔案將不會復原。

檔案層級安全性

此選項在從 NTFS 格式化磁碟區的磁碟層級和檔案層級備份復原檔案時有效。

此選項定義是否將檔案的 NTFS 權限連同檔案一併復原。

預設為：**[啟用]**。

您可選擇是復原權限，還是讓檔案繼承復原目標資料夾的 NTFS 權限。

Flashback

除 Mac 之外，在實體和虛擬機器上復原磁碟和磁碟區時，此選項會生效。

此選項只有在復原的磁碟的磁碟區配置完全符合目標磁碟的磁碟區配置時才會運作。

若啟用此選項，則只會復原備份中的資料與目標磁碟資料之間的差異部分。這可加速實體和虛擬機器的復原。資料會在資料區塊層級進行比較。

在復原實體機器時，其預設為：**[已停用]**。

在復原虛擬機器時，其預設為：**[啟用]**。

復原完整路徑

只有從檔案層級備份資料時，此選項才能發揮作用。

若啟用此選項，系統會在目標位置中重新建立至檔案的完整路徑。

預設為：**[已停用]**。

掛載點

只有在 Windows 中復原檔案層級備份的資料時，此選項才能發揮作用。

啟用此選項可復原存放在已掛載磁碟區，且於啟用 **[掛載點]** 選項時進行備份的檔案與資料夾。

預設為：**[已停用]**。

當您選擇資料夾進行復原時，資料夾的階層必須高於掛載點，此選項才能發揮作用。如果您選擇進行復原的資料夾位在掛載點內，或是掛載點本身，則無論 **[掛載點]** 選項的值為何，都會復原選擇的項目。

注意事項

請切記，如果復原時未掛載磁碟區，資料會直接復原至備份時已經是掛載點的資料夾。

效能

此選項會定義作業系統內復原程序的優先順序。

可用設定包括：**[低]**、**[一般]**、**[高]**。

預設為：**[一般]**。

系統中執行程序的優先順序會決定分配給該程序的 CPU 和系統資源多寡。降低復原優先順序，將會釋放更多資源給其他應用程式。提高復原的優先順序，將要求作業系統分配更多資源給執行復原的應用程式，從而可能加快復原程序的速度。但是，實際效果將取決於 CPU 使用總量和其他因素（如磁碟 I/O 速度或網路流量）。

事前/事後命令

此選項可讓您定義資料復原之前和之後要自動執行的命令。

事前/事後命令使用方式的範例：

- 啟動 **Checkdisk** 命令，以尋找並修正邏輯檔案系統錯誤、實體錯誤或損壞的磁區，以在復原開始前和復原結束後啟動。

本程式不支援互動式命令，即需要使用者輸入的命令（例如「pause」）。

如果復原過程將會重新啟動，則復原後命令將不被執行。

復原前命令

指定要在復原程序開始前執行的命令/批次檔案

1. 啟用 **[復原之前執行命令]** 開關。
2. 在 **[命令...]** 欄位中輸入命令, 或瀏覽至批次檔案。本程式不支援互動式命令, 即需要使用者輸入的命令 (例如「pause」)。
3. 在 **[工作目錄]** 欄位中, 指定將執行命令/批次檔案所在目錄的路徑。
4. 如有需要, 請在 **[引數]** 欄位中指定該命令的執行引數。
5. 依據您要獲得的結果, 選擇下表所述的相應選項。
6. 按一下**[完成]**。

核取方塊	選擇			
若命令執行失敗, 則放棄復原*	已選擇	已清除	已選擇	已清除
命令執行完成後再復原	已選擇	已選擇	已清除	已清除
結果				
	預設 僅在成功執行命令後執行復原。若命令執行失敗, 則放棄復原。	執行命令後執行復原, 無論命令執行是否成功。	不適用	執行命令的同時執行復原, 無論命令執行的結果如何。

* 命令的結束碼如果不等於零便視為失敗。

復原後命令

指定復原完成後要執行的命令/可執行檔

1. 啟用 **[復原之後執行命令]** 開關。
2. 在 **[命令...]** 欄位中輸入命令, 或瀏覽至批次檔案。
3. 在 **[工作目錄]** 欄位中, 指定將執行命令/批次檔案所在目錄的路徑。
4. 在 **[引數]** 欄位中指定命令執行引數 (如有需要)。
5. 如果命令成功執行與否很重要, 請選取 **[若命令執行失敗, 則放棄復原]** 核取方塊。命令的結束碼如果不等於零, 命令就視為失敗。如果命令執行失敗, 則復原狀態將設為 **[錯誤]**。
如果未選擇核取方塊, 則命令執行結果不會影響復原執行失敗或成功。您可以瀏覽 **[活動]** 標籤, 以追蹤命令的執行結果。
6. 按一下**[完成]**。

注意事項

如果復原過程將會重新啟動, 則復原後命令將不被執行。

SID 變更

此選項只有在復原 Windows 8.1/Windows Server 2012 R2 或舊版時有效。

VMware 用代理程式、Hyper-V 用代理程式、Scale Computing HC3 用代理程式或 oVirt 用代理程式執行復原至虛擬機器時，此選項不適用。

預設為：**[已停用]**。

軟體可為復原的作業系統產生唯一安全性識別碼 (電腦 SID)。只需要此選項，即可確保第三方軟體可依「電腦 SID」執行作業。

Microsoft 並未正式支援在部署或復原的系統上變更 SID，因此若使用此選項，請自行承擔風險。

VM 電源管理

VMware 用代理程式、Hyper-V 用代理程式、Virtuozzo 用代理程式、Scale Computing HC3 用代理程式或 oVirt 用代理程式執行復原至虛擬機器時，這些選項均有效。

開始復原時關閉目標虛擬機器

預設為：**[啟用]**。

若現有虛擬機器為連線狀態，即無法復原至該虛擬機器，因此復原一開始，就會自動關閉虛擬機器。使用者會與虛擬機器中斷連線，而任何未儲存的資料會流失。

若您偏好於復原前手動關閉虛擬機器，請清除此選項的核取方塊。

復原完成時開啟目標虛擬機器

預設為：**[已停用]**。

電腦從備份復原至另一台電腦後，網路上可能會顯示現有電腦的複本。基於安全考量，請在採取必要的預防措施後，再手動開啟復原的虛擬機器。

Windows 事件日誌

此選項僅在 Windows 作業系統下有效。

此選項定義代理程式是否必須在 Windows 的應用程式事件記錄檔中記錄復原作業事件 (若要查看此記錄，請執行 eventvwr.exe 或選擇 **[控制台] > [系統管理工具] > [事件檢視器]**)。您可以篩選要記錄的事件。

預設為：**[已停用]**。

13.15 備份的相關作業

13.15.1 備份儲存索引標籤

[備份儲存] 索引標籤可讓您存取所有備份，包括離線電腦的備份、不再登錄在 Cyber Protection 服務中之電腦的備份，以及孤立備份¹。

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。

¹孤立備份是與保護計劃不再有關聯的備份。

在 Windows 中，備份檔案會繼承其父資料夾的存取權限。因此，建議您限制此資料夾的讀取權限。

在雲端儲存中，使用者僅能存取他們自己的備份。

系統管理員能夠代表屬於特定單位或公司及其子群組的任何帳戶，透過選擇帳戶的雲端儲存空間，檢視雲端的備份。若要選擇您要用於取得雲端資料的裝置，按一下 **[要瀏覽的電腦]** 列中的 **[變更]**。

[備份儲存] 索引標籤會顯示曾以所選帳戶登錄之所有電腦的備份。

雲端 Microsoft 365 用代理程式所建立的備份以及 Google Workspace 資料的備份不會顯示在 **雲端儲存空間** 位置，而是顯示在名為 **[雲端應用程式備份]** 的另一個區段。

用於保護計劃的備份位置會自動新增至 **[備份儲存]** 索引標籤。欲新增自訂資料夾 (如卸離式 USB 裝置) 至備份位置清單，請按一下 **[瀏覽]** 然後指定資料夾路徑。

如果您使用檔案管理員新增或移除一些備份，按一下位置名稱旁的齒輪圖示，然後按一下 **[重新整理]**。

警告！

請勿嘗試手動編輯備份檔案，因為這可能會導致檔案損毀，並使備份無法使用。此外，建議您使用備份複寫，而非手動移動備份檔案。

如果曾經備份至該位置的所有電腦從服務中刪除，備份位置 (雲端儲存空間除外) 會從 **[備份儲存]** 索引標籤消失。如此可確保您不必支付此位置中儲存之備份的費用。只要備份至此位置，就會重新加入該位置以及儲存在其中的所有備份。

在 **[備份儲存]** 索引標籤上，您可以在清單中使用下列條件篩選備份：

- **僅搭配鑑識資料** – 只會顯示 [包含鑑識資料的備份](#)。
- **僅限修補程式管理所建立的預先更新的備份** – 只會顯示 [修補程式安裝之前，在修補程式管理執行期間所建立的備份](#)。

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。

13.15.2 從備份掛載磁碟區

掛載磁碟層級備份的磁碟區，可讓您如同存取實體磁碟般存取磁碟區。

在讀寫模式下掛載磁碟區可讓您修改備份內容，即儲存、移動、建立、刪除檔案或資料夾，並執行由一個檔案組成的執行檔。在此模式下，軟體會建立增量備份，其中包含您對備份內容所作的變更。請注意，後續的備份都不會包含這些變更。

需求

- 此功能僅限於 Windows 系統的「檔案總管」使用。
- 用來執行掛載作業的電腦必須已安裝 Windows 用代理程式。
- 電腦所執行的 Windows 版本必須支援備份的檔案系統。
- 備份檔案必須儲存在網路共用 (SMB/CIFS) 或 Secure Zone 的本機資料夾中。

使用情境

- 共用資料
您可以輕易透過網路共用已掛載磁碟區。
- "Band-aid" 資料庫復原解決方案
掛載一個包含 SQL 資料庫的磁碟區，而該資料庫來自最近發生故障的電腦。如此一來，將可讓您存取該資料庫，直到故障的電腦復原為止。此方法也可以透過 [SharePoint Explorer](#) 用於 Microsoft SharePoint 的細微復原。
- 離線病毒移除
如果電腦受到感染，請先掛載備份，並使用防毒軟體清理病毒 (或尋找最近一個未受到感染的備份)，然後再從該備份復原電腦。
- 錯誤檢查
如果重新調整大小的磁碟區復原失敗，則可能是備份檔案系統中發生的錯誤所致。請在讀寫模式下掛載備份。接著，使用 `chkdsk /r` 命令檢查已掛載磁碟區是否有錯誤。錯誤修正完成並建立新的增量備份之後，從此備份復原系統。

從備份掛載磁碟區

1. 使用檔案總管瀏覽至備份位置。
2. 按兩下備份檔案。檔案名稱是依據下列範本格式：
<電腦名稱> - <保護計劃 GUID>
3. 如果備份已加密，請輸入加密密碼。否則，請跳過此步驟。
檔案總管會顯示復原點。
4. 按兩下復原點。
檔案總管會顯示備份的磁碟區。

注意事項

按兩下磁碟區瀏覽內容。您可以從備份將檔案和資料夾複製到檔案系統上的任何資料夾。

5. 以滑鼠右鍵按一下要掛載的磁碟區，然後選擇下列其中一個選項：

- a. **安裝**

注意事項

您只能在讀寫模式下，掛載存檔中的最後一個備份 (備份鏈)。

- b. **掛載成唯讀模式。**

6. 如果備份儲存在網路共用，請提供存取認證。否則，請跳過此步驟。

軟體會掛載所選的磁碟區。系統會將第一個未使用的代號指派給磁碟區。

卸載磁碟區

1. 使用檔案總管瀏覽至 **[電腦]** (Windows 8.1 和更新版本會顯示為 **[本機]**)。
2. 用滑鼠右鍵按一下已掛載磁碟區。
3. 按一下 **[卸載]**。
4. **[選用]** 如果先前是在讀寫模式下掛載磁碟區，而其內容經過修改，則請選擇是否要建立包含變更的增量備份。否則，請跳過此步驟。

軟體會卸載所選的磁碟區。

13.15.3 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 513 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 234 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]**。

13.15.4 匯出備份

匯出作業會在您指定的位置建立備份的有效副本。原始備份保持不變。透過匯出備份，您可以從增量備份及差異備份鏈分離特定備份，以便快速復原、寫入抽取式或可拔除媒體或用於其他目的。

注意事項

此功能可在進階備份組取得，並為執行離線主機資料處理作業代理程式的機器要求伺服器配額。

匯出作業的結果一律是完整備份。如果要將整個備份鏈複製到其他位置並保留多個復原點，請使用備份複寫計劃。有關係此計劃的更多資訊，請參閱 "備份複寫" (第 512 頁)。

匯出備份的備份檔案名稱與原始備份的備份檔案名稱相同，序號除外。如果相同備份鏈中的多個備份匯出到相同的位置，則會將四位數序號附加到所有備份的檔案名稱，但第一個備份除外。

匯出的備份將繼承原始備份的加密設定和密碼。匯出加密備份時，您必須指定密碼。

若要匯出備份

1. 選擇備份的工作負載。
2. 按一下 **[復原]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。

如果工作負載處於離線狀態，則不會顯示復原點。執行下列任何一項作業：

- 如果備份位置是雲端或共用儲存空間(即其他代理程式可存取)，請按一下 **[選擇機器]**，選擇處於連線狀態的目標工作負載，然後選擇復原點。
- 在 **[備份儲存]** 索引標籤上選擇復原點。有關在該處備份的更多資訊，請參閱 "備份儲存索引標籤" (第 234 頁)。

4. 按一下齒輪圖示，然後按一下 **[匯出]**。
5. 選擇將執行匯出的代理程式。
6. 如果備份已經過加密，請提供加密密碼。否則，請跳過此步驟。
7. 指定匯出目的地。
8. 按一下 **[開始]**。

13.15.5 刪除備份

警告！

如果停用了固定儲存空間，將永久刪除備份資料，並且無法復原。

針對處於連線狀態且存在於服務主控台的工作負載，刪除其備份

1. 在 **[所有裝置]** 索引標籤上，選擇要刪除備份的工作負載。
2. 按一下 **[復原]**。
3. 選擇您要刪除的備份之位置。
4. 刪除所需的備份。您可以刪除整個備份鏈或其中的單一備份。

- 若要刪除整個備份鏈，按一下 **[全部刪除]**。
- 刪除所選備份鏈中的單一備份：
 - a. 選擇要刪除的備份，然後按一下齒輪圖示。
 - b. 請按一下 **[刪除]**。

5. 確認選項無誤。

要刪除任何工作負載的備份

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。備份將集合在備份組中。備份組根據以下範本命名：

- <workload name> - <protection plan name>
- <user name> 或 <drive name> - <cloud service> - <protection plan name> - 作為雲端到雲端的備份

2. 選擇備份組。

3. 刪除所需的備份。您可以刪除整個備份組或其中的單一備份。

- 要刪除整個備份組，請按一下 **[刪除]**。
- 要刪除所選備份組中的單一備份，請執行以下操作：
 - a. 按一下 **[顯示備份]**。
 - b. 選擇要刪除的備份，然後按一下齒輪圖示。
 - c. 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 "從雲端儲存下載檔案" (第 223 頁) 中所述。

2. 按一下想要刪除備份的工作負載名稱。

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。

如果您使用檔案管理員刪除本機備份，該怎麼辦

建議您使用服務主控台刪除備份 (如果可能)。如果您使用檔案管理員刪除本機備份，請執行下列操作：

1. 在 **[備份儲存]** 索引標籤上，按一下位置名稱旁的齒輪圖示。
2. 按一下 **[重新整理]**。

如此一來，您將通知 Cyber Protection 服務本機儲存空間使用量減少。

13.16 保護 Microsoft 應用程式

13.16.1 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**

這也是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。

13.16.2 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。

13.16.3 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。

13.16.4 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	整部電腦	整部電腦

	資料庫做為檔案	資料庫至即時 SQL Server 執行 個體 資料庫做為檔案	
Microsoft Exchange Server	資料庫至即時 Exchange 資料庫做為檔案 細微復原至即時 Exchange 或 Microsoft 365*	整部電腦 資料庫至即時 Exchange 資料庫做為檔案 細微復原至即時 Exchange 或 Microsoft 365*	整部電腦
Microsoft SharePoint 資料庫伺服器	資料庫至即時 SQL Server 執行 個體 資料庫做為檔案 使用 SharePoint Explorer 的細 微復原	整部電腦 資料庫至即時 SQL Server 執行 個體 資料庫做為檔案 使用 SharePoint Explorer 的細 微復原	整部電腦
Microsoft SharePoint 前端 Web 伺服器	-	-	整部電腦
Active Directory 網域服務	-	整部電腦	-

* 從信箱備份復原也提供細微復原。如果在本機安裝 Microsoft 365 用代理程式，則支援將 Exchange 資料項目復原至 Microsoft 365，反之亦然。

13.16.5 必要條件

在設定應用程式備份之前，請先確保符合以下列出的需求。

若要檢查 VSS 編寫器狀態，請使用 `vssadmin list writers` 命令。

一般需求

若是 **Microsoft SQL Server**，請確保：

- 至少已啟動一個 Microsoft SQL Server 執行個體。
- 已開啟 VSS 的 SQL 編寫器。

若是 **Microsoft Exchange Server**，請確保：

- 已啟動 Microsoft Exchange 資訊儲存庫服務。
- 已安裝 Windows PowerShell。若是 Exchange 2010 或更新版本，Windows PowerShell 版本至少必須是 2.0。
- 已安裝 Microsoft .NET Framework。
若是 Exchange 2007，Microsoft .NET Framework 版本至少必須是 2.0。

若是 Exchange 2010 或更新版本, Microsoft .NET Framework 版本至少必須是 3.5。

- VSS 的 Exchange 編寫器已開啟。

注意事項

Exchange 用代理程式需要臨時存放區才能運作。暫存檔預設位於 %ProgramData%\Acronis\Temp。請確定 %ProgramData% 資料夾所在磁碟區的可用空間應至少等於 Exchange 資料庫大小的 15%。或者,您可以先變更暫存檔的位置,再建立 Exchange 備份,如變更暫存檔和資料夾位置 (40040) 中所述。

在網域控制站上,請確保:

- 已開啟 VSS 的 Active Directory 編寫器。

建立保護計劃時,請確保:

- 若是實體電腦以及其中已安裝代理程式的電腦,啟用 [磁碟區陰影複製服務 (VSS)] 備份選項。
- 若是虛擬機器,請確保已啟用 [虛擬機器的磁碟區陰影複製服務 (VSS)] 備份選項。

應用程式感知備份的額外需求

建立保護計劃時,請確保已選擇 **[整部電腦]** 進行備份。保護計劃中必須停用 **[逐一磁區]** 備份選項,否則將無法從這類備份中復原應用程式資料。如果計劃是因為自動切換到 **[逐一磁區]** 模式而在此模式下執行的,也將無法復原應用程式資料。

ESXi 虛擬機器的需求

如果應用程式是在透過 VMware 用代理程式備份的虛擬機器上執行,請確保:

- 要備份的虛擬機器符合以下 VMware 文件的「Windows 備份實作」一文中列出之應用程式一致的備份和還原需求:<https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html>。
- 已在電腦上安裝 VMware Tools 且為最新版。
- 已在電腦上停用使用者帳戶控制 (UAC)。如果您不想要停用 UAC,您必須在啟用應用程式備份時提供內建網域系統管理員 (DOMAIN\Administrator) 的認證。

注意事項

使用建立網域時設定的內建網域系統管理員帳戶。不支援之後建立的帳戶。

Hyper-V 虛擬機器的需求

如果應用程式是在透過 Hyper-V 用代理程式備份的虛擬機器上執行,請確保:

- 客體作業系統為 Windows Server 2008 或更新版本。
- 若是 Hyper-V 2008 R2: 客體作業系統為 Windows Server 2008/2008 R2/2012。
- 虛擬機器沒有動態磁碟。
- 在 Hyper-V 主機和客體作業系統之間存在網路連線。若要在虛擬機器內部執行遠端 WMI 查詢,則這是必要的。

- 已在電腦上停用使用者帳戶控制 (UAC)。如果您不想要停用 UAC, 您必須在啟用應用程式備份時提供內建網域系統管理員 (DOMAIN\Administrator) 的認證。

注意事項

使用建立網域時設定的內建網域系統管理員帳戶。不支援之後建立的帳戶。

- 虛擬機器設定符合下列準則：
 - 已安裝 Hyper-V 整合服務且為最新版。重大更新為 <https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines>
 - 在虛擬機器設定中, [管理] > [整合服務] > [備份 (磁碟區檢查點)] 選項為啟用狀態。
 - 若是 Hyper-V 2012 和更新版本: 虛擬機器沒有檢查點。
 - 若是 Hyper-V 2012 R2 和更新版本: 虛擬機器有一個 SCSI 控制器 (核取 [設定] > [硬體])。

13.16.6 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)

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

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。如果使用主節點失敗, 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. 如「選擇 SQL 資料庫」所述, 選擇要備份的 AAG。

您必須選擇 AAG 本身, 才能備份 AAG 的所有資料庫。若要備份一組資料庫, 請在 AAG 的所有節點中定義這組資料庫。

警告!

在所有節點中的資料庫組必須完全相同。即使只有一組不同, 或未在所有節點上定義, 則叢集

備份將無法正確運作。

3. 設定「[叢集備份模式](#)」備份選項。

復原 AAG 中包含的資料庫

1. 選擇要復原的資料庫，然後選擇要從其復原資料庫的復原點。
在 **[裝置] > [Microsoft SQL] > [資料庫]**，下選擇叢集資料庫，然後按一下 **[復原]**後，軟體僅顯示與備份資料庫選定副本的時間相對應的復原點。
檢視叢集資料庫所有復原點的最簡單方法是在 **[備份儲存]** 索引標籤上選擇整個 AAG 的備份。
AAG 備份的名稱是以下列範本為基礎：**<AAG 名稱> - <保護計劃名稱>**，且有一個特殊圖示。
2. 若要設定復原，請遵循「[復原 SQL 資料庫](#)」中描述的步驟，從第 5 步開始。
軟體會自動定義資料復原目標叢集節點。該節點的名稱會顯示在 **[復原至]** 欄位中。您可以手動變更目標節點。

重要事項

包含在 Always On 可用性群組中的資料庫無法在復原期間遭到覆寫，因為 Microsoft SQL Server 禁止此作業。您需要在復原前從 AAG 排除目標資料庫。或者，您可逕將資料庫復原為新的非 AAG 資料庫。完成復原時，您可以在重建原始 AAG 設定。

保護資料庫可用性群組 (DAG)

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

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。

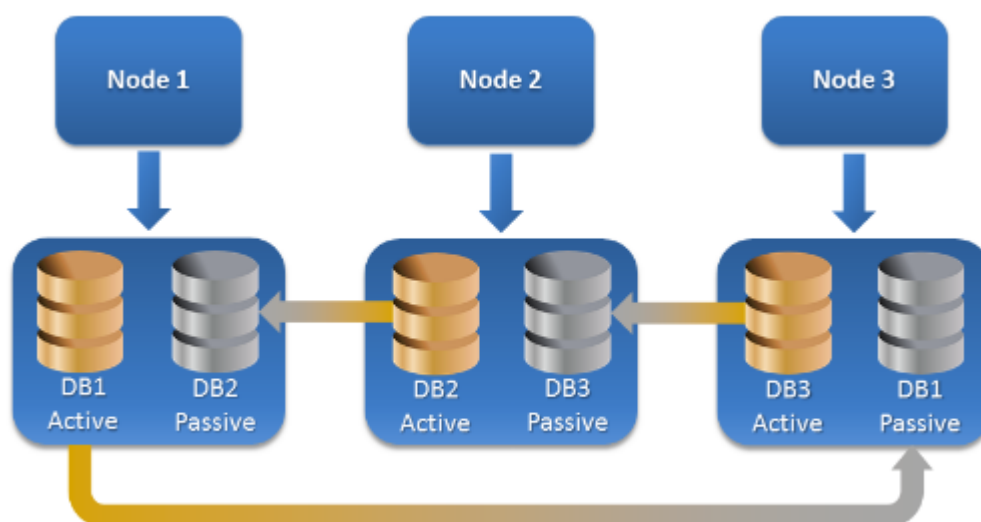
叢集感知備份

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, 服務主控台將在 **[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。

13.16.7 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) 可以建立應用程式感知備份, 但無法從那些備份復原應用程式資料。若要從此代理程式建立的備份復原應用程式資料, 在存取備份儲存位置的電腦上, 必須有 VMware 用代理程式 (Windows)、SQL 用代理程式或 Exchange 用代理程式。設定應用程式資料的復原時, 請在 **[備份儲存]** 索引標籤上選擇復原點, 然後在 **[要瀏覽的電腦]** 中選擇此電腦。

< 必要條件 > 和 < 需要的使用者權限 > 章節已列出其他需求。

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。

注意事項

使用建立網域時設定的內建網域系統管理員帳戶。不支援之後建立的帳戶。

13.16.8 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 **[保護]**。

所需的使用者權限

若要存取信箱，Exchange 用代理程式需要有適當權限的帳戶。系統會提示您在設定信箱的各種操作時，指定此帳戶。

在 **[組織管理]** 角色群組內的帳戶成員資格可存取任何信箱，包括未來將會建立的信箱。

所需的最低使用者權限如下：

- 帳戶必須是 **[伺服器管理]** 和 **[收件者管理]** 角色群組的成員。
- 針對代理程式將會存取其信箱之所有使用者或使用者群組，必須啟用帳戶的 **ApplicationImpersonation** 管理角色。

如需設定 **ApplicationImpersonation** 管理角色的資訊，請參閱下列 Microsoft 知識庫文章：<https://msdn.microsoft.com/en-us/library/office/dn722376.aspx>。

13.16.9 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主資料庫大致相同。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]**。

13.16.10 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**

- 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。
- 按一下 **[復原]**。
- 選擇復原點請注意，復原點是依照位置進行篩選。

如果電腦處於離線狀態，復原點就不會顯示。執行下列其中一項操作：

 - [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。
- 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]**。
- 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：
 - 按一下資料庫名稱。
 - 從 **[復原至]** 中選擇 **[新資料庫]**。
 - 指定新資料庫的名稱。
 - 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。
- 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](http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.80).aspx)

13.16.11 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 244 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

如果在本機安裝 Microsoft 365 用代理程式，則支援將 Exchange 資料項目復原至 Microsoft 365，反之亦然。

復原功能可在 Microsoft Exchange Server 2010 及更新版本的備份中執行。

將信箱復原至現有的 Microsoft 365 信箱時，現有項目會保持原樣，且復原的項目會放置在其旁邊。

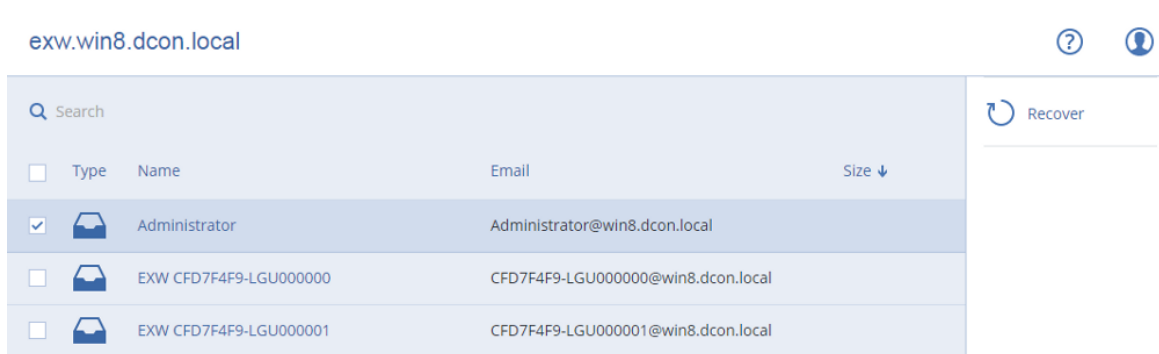
復原單一信箱時，您需要選擇目標 Microsoft 365 信箱。在一次復原作業過程中復原數個信箱時，軟體嘗試將每個信箱復原至相同名稱使用者的信箱。若找不到使用者，則會略過信箱。如果系統略過某些信箱，復原會成功，但會出現警告。如果系統略過所有信箱，復原將會失敗。

如需有關復原至 Microsoft 365 的詳細資訊，請參閱「[保護 Microsoft 365 信箱](#)」。

復原信箱

若要從應用程式感知備份或資料庫備份復原信箱

1. [僅在從資料庫備份復原至 Microsoft 365 時] 如果 Microsoft 365 用代理程式未安裝在已備份且執行 Exchange Server 的電腦上，請執行下列其中一項作業：
 - 如果組織中沒有 Microsoft 365 用代理程式，則在已備份的電腦 (或在具有相同 Microsoft Exchange Server 版本的另一部電腦) 上安裝 Microsoft 365 用代理程式。
 - 如果組織中已安裝 Microsoft 365 用代理程式，則從已備份的電腦 (或在具有相同 Microsoft Exchange Server 版本的另一部電腦) 上，將程式庫複製到裝有 Microsoft 365 用代理程式的電腦中，如「[複製 Microsoft Exchange 程式庫](#)」中所述。
2. 執行下列其中一項操作：
 - 從應用程式感知備份復原時：在 **[裝置]** 下，選擇原本存放所要復原之資料的電腦。
 - 從資料庫備份復原時，按一下 **[裝置] > [Microsoft Exchange] > [資料庫]**，然後選擇原本存放所要復原之資料的資料庫。
3. 按一下 **[復原]**。
4. 選擇復原點請注意，復原點是依照位置進行篩選。
如果電腦處於離線狀態，復原點就不會顯示。請使用其他復原方式：
 - [僅從應用程式感知備份復原時] 如果備份位置是雲端或共用儲存 (即可被其他代理程式存取)，按一下 **[選擇電腦]**，選擇有 Exchange 用代理程式或 VMware 用代理程式的線上電腦，然後選擇復原點。
 - 在 [\[備份儲存\] 索引標籤](#) 上選擇復原點。復原作業會由透過上述任一動作所選來瀏覽的電腦執行，而非由離線的原始電腦執行。
5. 依序按一下 **[復原] > [Exchange 信箱]**。
6. 選擇您要復原的信箱。
您可以按名稱搜尋信箱。不支援萬用字元。



7. 按一下 **[復原]**。
8. [僅在復原至 Microsoft 365 時]:

- a. 在 **[復原至]** 中, 選擇 **[Microsoft 365]**。
- b. [若只選擇步驟 6 中的一個信箱] 在 **目標信箱** 中, 指定目標信箱。
- c. 按一下 **[開始復原]**。

此程序無需執行更多步驟。

按一下 **[具有 Microsoft Exchange Server 的目標電腦]** 以選擇或變更目標電腦。此步驟可允許非執行 Exchange 用代理程式的電腦進行復原。

指定電腦的完整網域名稱 (FQDN), 其中已啟用 **[用戶端存取]** 角色 (在 Microsoft Exchange Server 2010/2013 中), 或 **[信箱角色]** (在 Microsoft Exchange Server 2016 或更新版本中)。電腦所屬的 Active Directory 樹系必須與執行復原之機器所屬的樹系相同。

9. 若顯示提示, 請指定將用於存取電腦的帳戶認證。此帳戶的需求會列在 **< 需要的使用者權限 >** 中。
10. [選擇性步驟] 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 Microsoft 365 用代理程式未安裝在已備份且執行 Exchange Server 的電腦上, 請執行下列其中一項作業：
 - 如果組織中沒有 Microsoft 365 用代理程式, 則在已備份的電腦 (或在具有相同 Microsoft Exchange Server 版本的另一部電腦) 上安裝 Microsoft 365 用代理程式。
 - 如果組織中已安裝 Microsoft 365 用代理程式, 則從已備份的電腦 (或在具有相同 Microsoft Exchange Server 版本的另一部電腦) 上, 將程式庫複製到裝有 Microsoft 365 用代理程式的電腦中, 如「**複製 Microsoft Exchange 程式庫**」中所述。
2. 執行下列其中一項操作：
 - 從應用程式感知備份復原時: 在 **[裝置]** 下, 選擇原本存放所要復原之資料的電腦。
 - 從資料庫備份復原時, 按一下 **[裝置] > [Microsoft Exchange] > [資料庫]**, 然後選擇原本存放所要復原之資料的資料庫。
3. 按一下 **[復原]**。
4. 選擇復原點請注意, 復原點是依照位置進行篩選。
如果電腦處於離線狀態, 復原點就不會顯示。請使用其他復原方式:

- [僅從應用程式感知備份復原時] 如果備份位置是雲端或共用儲存 (即可被其他代理程式存取), 按一下 **[選擇電腦]**, 選擇有 Exchange 用代理程式或 VMware 用代理程式的線上電腦, 然後選擇復原點。

- 在 **[備份儲存]** 索引標籤上選擇復原點。

復原作業會由透過上述任一動作所選來瀏覽的電腦執行, 而非由離線的原始電腦執行。

5. 依序按一下 **[復原]** > **[Exchange 信箱]**。

6. 按一下最初具有您想要復原之項目的信箱。

7. 選擇您要復原的項目。

您可以選取下列搜尋選項。不支援萬用字元。

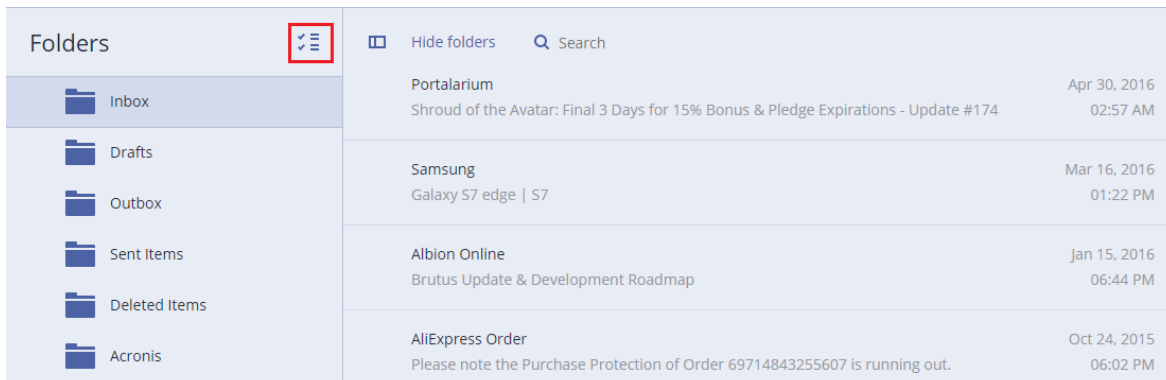
- 電子郵件訊息: 依主題、寄件者、收件者及日期搜尋。
- 事件: 依主題及日期搜尋。
- 工作: 依主題及日期搜尋。
- 連絡人: 依姓名、電子郵件地址和電話號碼搜尋。

選擇了電子郵件訊息後, 按一下 **[顯示內容]** 以檢視其內容和附件。

注意事項

要下載附加檔案, 請按一下名稱。

若要能夠選擇資料夾, 請按一下復原資料夾圖示。



8. 按一下 **[復原]**。

9. 若要復原至 Microsoft 365, 請在 **[復原至]** 中, 選擇 **[Microsoft 365]**。

若要復原至 Exchange Server, 保留 **復原至** 中的 **Microsoft Exchange** 預設值。

[僅在復原至 Exchange Server 時] 按一下 **[具有 Microsoft Exchange Server 的目標電腦]** 以選擇或變更目標電腦。此步驟可允許非執行 Exchange 用代理程式的電腦進行復原。

指定電腦的完整網域名稱 (FQDN), 其中已啟用 **[用戶端存取]** 角色 (在 Microsoft Exchange Server 2010/2013 中), 或 **[信箱角色]** (在 Microsoft Exchange Server 2016 或更新版本中)。電腦所屬的 Active Directory 樹系必須與執行復原之機器所屬的樹系相同。

10. 若顯示提示, 請指定將用於存取電腦的帳戶認證。此帳戶的需求會列在 **< 需要的使用者權限 >** 中。

11. **[目標信箱]** 可以檢視、變更或指定目標信箱。

原始信箱預設為選取狀態。如果此信箱不存在或選取了非原始目標電腦, 則必須指定目標信箱。

12. [僅恢復電子郵件訊息時] 在**目標資料夾**中, 查看或變更目標信箱中的目標資料夾。根據預設, 已選取 **[已復原項目]** 資料夾。由於 Microsoft Exchange 的限制, 無論指定任何不同的**目標資料夾**, 事件、工作、記事 and 聯絡人都會還原到其原始位置。

13. 按一下 **[開始復原]**。

復原進度會顯示在 **[活動]** 索引標籤上。

若要從信箱備份復原信箱項目

1. 按一下 **[裝置] > [Microsoft Exchange] > [信箱]**。

2. 按一下最初具有您想要復原之項目的信箱, 然後按一下**[復原]**。

您可以按名稱搜尋信箱。不支援萬用字元。

如果信箱遭到刪除, 在 **[備份儲存]** 索引標籤中選擇此信箱, 然後按一下 **[顯示備份]**。

3. 選擇復原點請注意, 復原點是依照位置進行篩選。

4. 按一下**[復原] > [電子郵件訊息]**。

5. 選擇您要復原的項目。

您可以選取下列搜尋選項。不支援萬用字元。

- 電子郵件訊息: 依主題、寄件者、收件者及日期搜尋。
- 事件: 依主題及日期搜尋。
- 工作: 依主題及日期搜尋。
- 連絡人: 依姓名、電子郵件地址和電話號碼搜尋。

選擇了電子郵件訊息後, 按一下 **[顯示內容]** 以檢視其內容和附件。

注意事項

要下載附加檔案, 請按一下名稱。

選擇電子郵件訊息後, 您可按一下**[以電子郵件傳送]**, 向電子郵件地址傳送訊息。訊息便會從您的管理員帳戶的電子郵件地址傳送。

若要能夠選擇資料夾, 請按一下 **[復原資料夾]** 圖示: 

6. 按一下 **[復原]**。

7. 執行以上程序的步驟 9-13。

複製 Microsoft Exchange Server 程式庫

將 **Exchange** 信箱或信箱項目復原至 **Microsoft 365** 時, 您可能需要從已備份的電腦 (或具有相同 Microsoft Exchange Server 版本的另一部電腦) 上, 將下列程式庫複製到已安裝 Microsoft 365 用代理程式的電腦中。

根據已備份的 Microsoft Exchange Server 版本, 複製下列檔案。

Microsoft Exchange Server 版本	程式庫	預設位置
Microsoft Exchange Server 2010	ese.dll esebcli2.dll store.exe	%ProgramFiles%\Microsoft\Exchange Server\V14\bin

Microsoft Exchange Server 2013	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll	%WINDIR%\system32
Microsoft Exchange Server 2016、2019	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll	%WINDIR%\system32
	msvcp110.dll	

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。

13.16.12 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]**。

13.17 保護行動裝置

Cyber Protect 應用程式可讓您將行動資料備份到雲端儲存空間，然後在遺失或損毀時將其復原。請注意，備份至雲端儲存空間需要有一個帳戶以及雲端訂購授權。

13.17.1 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 Cyber Protect 應用程式：

- iOS 12.0 和更新版本 (iPhone、iPod 和 iPad)
- Android 7.0 和更新版本

13.17.2 可備份的內容

- 連絡人
- 照片(保留照片的原始大小及格式)

- 影片
- 行事曆
- 提醒訊息 (僅適用於 iOS 裝置)

13.17.3 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。如果啟用此設定，Cyber Protect 應用程式會自動偵測新資料並將其上傳到雲端。
- **[僅使用 Wi-Fi]** 選項在應用程式設定中預設為啟用狀態。如果已開啟此設定，則只會在有 Wi-Fi 連線時，Cyber Protect 應用程式才會備份資料。如果失去 Wi-Fi 連線，備份程序將不會啟動。若要讓應用程式也使用行動數據連線，請將此選項關閉。
- 裝置上的電池最佳化功能可能會使 Cyber Protect 應用程式無法正常運作。若要準時執行備份，您應該停止應用程式的電池最佳化功能。
- 您有兩種節省能源的方法：
 - **[充電時備份]** 功能 (預設為停用狀態)。如果已開啟此設定，則只會在您的裝置連線到電源時，Cyber Protect 應用程式才會備份資料。當裝置在連續備份過程中與電源中斷連線，備份將會暫停。
 - **[省電模式]** (預設為啟用狀態)。如果已開啟此設定，則只會在您的裝置電池電力充足時，Cyber Protect 應用程式才會備份資料。當裝置電池電力不足時，將會暫停連續備份。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。您也可以使用服務主控台，將相片、影片或聯絡人下載到任何裝置。
- 從用您的帳戶登錄的行動裝置備份的資料僅可在此帳戶下使用。其他人無法檢視或復原您的資料。
- 在 Cyber Protect 應用程式中，您只能復原最新的資料版本。如果您需要從特定的備份版本復原，請在平板電腦或電腦上使用服務主控台。
- 保留規則不適用於行動裝置備份。
- **[僅適用於 Android 裝置]** 如果備份期間裝有 SD 卡，系統也會一併備份儲存在這張卡上的資料。資料將會復原到 SD 卡上；如果復原期間裝有 SD 卡，則會復原到 **[備份復原]** 資料夾；或者應用程式將會要求將資料復原到其他位置。

13.17.4 何處取得 Cyber Protect 應用程式

根據您的行動裝置而定，從 App Store 或 Google Play 安裝應用程式。

13.17.5 如何開始備份資料

1. 開啟應用程式。
2. 使用您的帳戶登入。
3. 點選 **[設定]** 可建立備份。請注意，只有在您沒有行動裝置備份時，才會出現此按鈕。

4. 選擇您要備份的資料類別。系統預設為全選所有類別。
5. [選擇性步驟] 啟用 **[加密備份]** 可透過加密保護備份。在這個案例中，您也將需要：
 - a. 輸入加密密碼兩次。

注意事項

請務必記住密碼，因為永遠無法還原或變更忘記的密碼。

- b. 點選 **[加密]**。
6. 點選**[備份]**。
7. 允許應用程式存取您的個人資料。如果您拒絕存取某些資料類別，便不會對它們進行備份。備份開始。

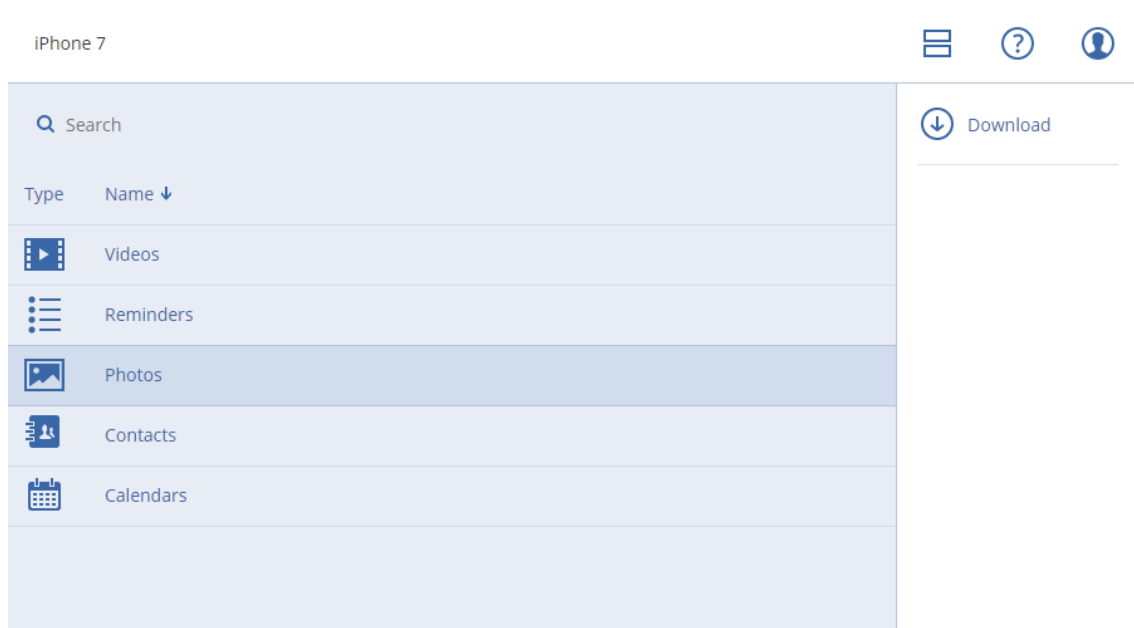
13.17.6 如何將資料復原至行動裝置

1. 開啟 Cyber Protect 應用程式。
2. 點選 **[瀏覽]**。
3. 點選裝置名稱。
4. 執行下列其中一項操作：
 - 若要復原所有備份的資料，點選 **[復原全部]**。您不需要再進行任何動作。
 - 若要復原一個或多個資料類別，點選 **[選擇]**，然後點選所需資料類別的核取方塊。點選 **[復原]**。您不需要再進行任何動作。
 - 若要復原屬於同一資料類別的一個或多個資料項目，點選資料類別。繼續進行後續步驟。
5. 執行下列其中一項操作：
 - 若要復原單一資料項目，請點選此項目。
 - 若要復原多個資料項目，點選 **[選擇]**，然後點選所需資料項目的核取方塊。
6. 點選 **[復原]**。

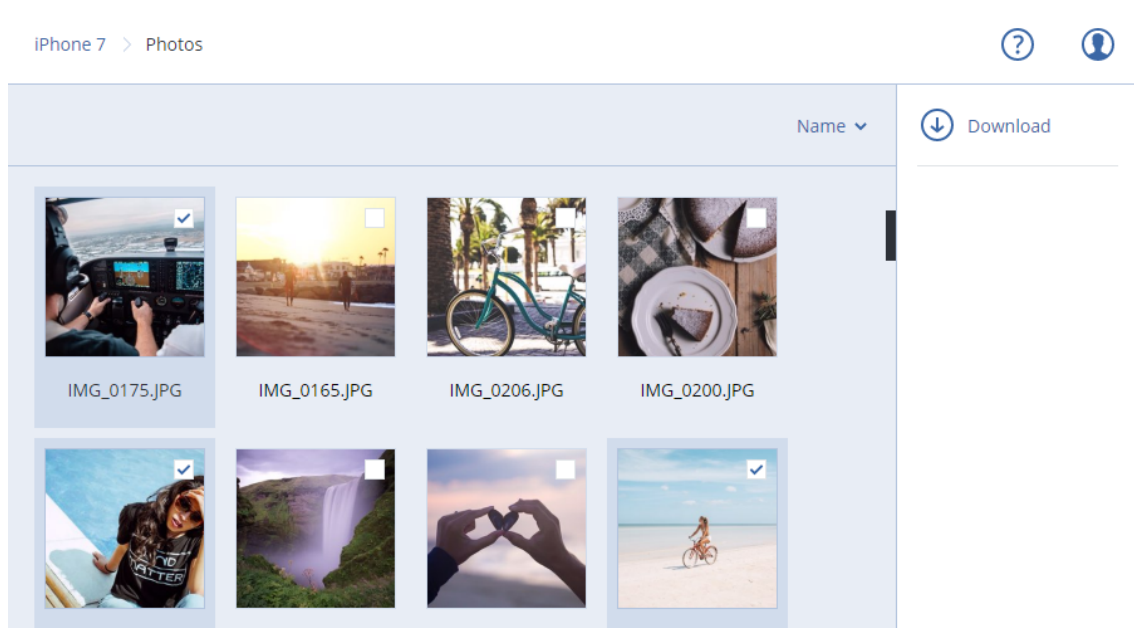
13.17.7 如何透過服務主控台檢閱資料

1. 在電腦上開啟瀏覽器，並輸入服務主控台 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。

13.18 保護託管的 Exchange 資料

13.18.1 哪些項目可以備份？

您可以備份使用者信箱、共用信箱和群組信箱。或者，您可以選擇備份所選信箱的封存信箱 (就地封存)。

13.18.2 可以復原哪些項目？

下列項目可以從信箱備份復原：

- 信箱
- 電子郵件資料夾
- 電子郵件訊息
- 行事曆事件
- 工作
- 連絡人
- 日誌項目
- 記事

您可以使用搜尋找出這些項目。

復原信箱、信箱項目、公用資料夾和公用資料夾項目時，您可以選擇是否要覆寫目標位置中的項目。

將信箱復原至現有的信箱時，系統會覆寫 ID 相符的現有項目。

信箱項目復原不會造成任何覆寫。而是會在目標資料夾中重新建立信箱項目的完整路徑。

13.18.3 選取信箱

如下所述選擇信箱，然後視需要指定保護計劃的其他設定。

若要選取 *Exchange Online* 信箱

1. 按一下 **[裝置] > [託管的 Exchange]**。
2. 如果多個託管的 Exchange 組織新增到 Cyber Protection 服務，請選擇您要備份其使用者資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
 - 若要備份所有使用者信箱和所有共用信箱 (包括之後建立的信箱)，展開 **[使用者]** 節點、選取 **[所有使用者]**，然後按一下 **[群組備份]**。
 - 若要備份個別的使用者信箱或共用信箱，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要備份其信箱的使用者，然後按一下 **[備份]**。
 - 若要備份所有群組的信箱 (包括之後建立之群組的信箱)，展開 **[群組]** 節點、選取 **[所有群組]**，然後按一下 **[群組備份]**。
 - 若要備份個別的群組信箱，展開 **[群組]** 節點、選取 **[所有群組]**、選取您要備份其信箱的群組，然後按一下 **[備份]**。

13.18.4 復原信箱和信箱項目

復原信箱

1. 按一下 **[裝置] > [託管的 Exchange]**。
2. 如果多個託管的 Exchange 組織新增到 Cyber Protection 服務, 請選擇您要復原其已備份資料的組織。否則, 請跳過此步驟。
3. 執行下列其中一項操作:
 - 若要復原使用者信箱, 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原其信箱的使用者, 然後按一下 **[復原]**。
 - 若要復原共用信箱, 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原的共用信箱, 然後按一下 **[復原]**。
 - 若要復原群組信箱, 展開 **[群組]** 節點、選取 **[所有群組]**、選取您要復原其信箱的群組, 然後按一下 **[復原]**。
 - 如果使用者、群組或共用信箱遭到刪除, 請在 **[備份儲存]** 索引標籤的 **[雲端應用程式備份]** 區段中選取該項目, 然後按一下 **[顯示備份]**。

您可以按名稱搜尋使用者和群組。不支援萬用字元。
4. 選擇復原點
5. 按一下 **[復原] > [整個信箱]**。
6. 如果多個託管的 Exchange 組織新增到 Cyber Protection 服務, 按一下 **[託管的 Exchange 組織]** 可檢視、變更或指定目標組織。

預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織, 您必須指定目標組織。
7. 在 **[復原至信箱]** 中, 檢視、變更或指定目標信箱。

原始信箱預設為選取狀態。如果此信箱不存在或選取了非原始組織, 則必須指定目標信箱。
8. 按一下 **[開始復原]**。
9. 選取其中一個覆寫選項:
 - **覆寫現有項目**
 - **不要覆寫現有項目**
10. 按一下 **[繼續]** 可確認您的決定。

復原信箱項目

1. 按一下 **[裝置] > [託管的 Exchange]**。
2. 如果多個託管的 Exchange 組織新增到 Cyber Protection 服務, 請選擇您要復原其已備份資料的組織。否則, 請跳過此步驟。
3. 執行下列其中一項操作:
 - 若要從使用者信箱復原項目, 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取其信箱原本包含您要復原之項目的使用者, 然後按一下 **[復原]**。
 - 若要復原共用信箱中的項目, 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取原本包含您要復原之項目的共用信箱, 然後按一下 **[復原]**。

- 若要從群組信箱復原項目，展開 **[群組]** 節點、選取 **[所有群組]**、選取其信箱原本包含您要復原之項目的群組，然後按一下 **[復原]**。
- 如果使用者、群組或共用信箱遭到刪除，請在 **[備份儲存]** 索引標籤的 **[雲端應用程式備份]** 區段中選取該項目，然後按一下 **[顯示備份]**。

您可以按名稱搜尋使用者和群組。不支援萬用字元。

4. 選擇復原點

5. 按一下 **[復原]** > **[電子郵件訊息]**。

6. 瀏覽到所需的資料夾，或使用搜尋以取得所需項目的清單。

您可以使用下列搜尋選項。不支援萬用字元。

- 電子郵件訊息：依主旨、寄件者、收件者、附件名稱及日期搜尋。
- 事件：依主題及日期搜尋。
- 工作：依主題及日期搜尋。
- 連絡人：依姓名、電子郵件地址和電話號碼搜尋。

7. 選擇您要復原的項目。若要能夠選擇資料夾，請按一下 **[復原資料夾]** 圖示：

此外，您可以執行下列任何一項作業：

- 選取項目後，按一下 **[顯示內容]** 可檢視其內容，包括附件。若要下載附加檔案，請按一下其名稱。
- 選取電子郵件訊息或行事曆項目後，按一下 **[以電子郵件傳送]**，可將該項目傳送到指定的電子郵件地址。您可以選取寄件者，並撰寫要加入至轉寄項目的文字。
- 只有在備份未經加密、使用搜尋，並在搜尋結果中選取單一項目時：按一下 **[顯示版本]** 來選取要復原的項目版本。您可以選取早於或晚於所選復原點的任何備份版本。

8. 按一下 **[復原]**。

9. 如果多個託管的 Exchange 組織新增到 Cyber Protection 服務，按一下 **[託管的 Exchange 組織]** 可檢視、變更或指定目標組織。

預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。

10. 在 **[復原至信箱]** 中，檢視、變更或指定目標信箱。

原始信箱預設為選取狀態。如果此信箱不存在或選取了非原始組織，則必須指定目標信箱。

11. [僅在復原至使用者信箱或共用信箱時] 在 **[路徑]** 中，檢視或變更目標信箱中的目標資料夾。根據預設，已選取 **[已復原項目]** 資料夾。

群組信箱項目一律復原至 **[收件匣]** 資料夾。

12. 按一下 **[開始復原]**。

13. 選取其中一個覆寫選項：

- 覆寫現有項目
- 不要覆寫現有項目

14. 按一下 **[繼續]** 可確認您的決定。

13.19 保護 Microsoft 365 資料

13.19.1 為什麼要備份 Microsoft 365 資料？

即使 Microsoft 365 是一組雲端服務，但定期備份可提供一層額外的保護，防止使用者出錯及故意的惡意操作。即使 Microsoft 365 的保留期過期後，您仍可從備份復原已刪除的項目。另外，如需遵守法規規定，您可以保留 Exchange Online 信箱的本機複本。

13.19.2 Microsoft 365 用代理程式

視所需的功能而定，您可以選擇在本機安裝 Microsoft 365 用代理程式、使用雲端上安裝的代理程式，或兩者。下表摘要說明本機和雲端代理程式的功能。

	本機 Microsoft 365 用代理程式	雲端 Microsoft 365 用代理程式
可以備份的資料項目	Exchange Online: 使用者信箱和共用信箱	• Exchange Online: 使用者信箱、共用信箱和群組信箱；公用資料夾 • OneDrive: 使用者檔案和資料夾 • SharePoint Online: 傳統網站集合、群組 (團隊) 網站、通訊網站、個別資料項目 • Microsoft 365 Teams: 整個小組、小組頻道、頻道檔案、小組信箱、檔案，以及小組信箱、會議和小組網站中的電子郵件訊息
封存信箱備份 (就地封存)	否	是
備份排程	使用者定義的	無法變更。每個保護計劃每天都會在相同的時間執行。*
備份位置	雲端儲存、本機資料夾、網路資料夾	僅限雲端儲存
自動保護新的 Microsoft 365 使用者、群組、網站和小組	否	是，透過將保護計劃套用至 [所有使用者] 、 [所有群組] 、 [所有網站] 、 [所有小組] 群組
保護多個 Microsoft 365 組織	否	是
精細復原	是	是
復原至一個組織內的另一位使用者	是	是
復原至另一個組織	否	是

復原至內部部署 Microsoft Exchange Server	否	否
可以備份但不會降低效能的項目數上限	備份到雲端儲存空間時:每個公司 5000 個信箱 備份到其他目的地時:每個保護計劃 2000 個信箱 (每個公司的信箱數量則沒有限制)	每個公司 10000 個受保護的項目 (信箱、OneDrives 或網站)**
可執行的手動備份數目上限	否	一小時內手動執行 10 次
同時復原作業數目上限	否	10 個作業, 包括 Google Workspace 復原作業

* 一個雲端代理程式服務多個客戶, 因此它會針對每個保護計劃, 自行決定開始時間, 以確保一天中的負載均衡, 且所有客戶都獲得同等的服務品質。

注意事項

保護排程可能會受到第三方服務作業的影響, 例如, Microsoft 365 伺服器的可存取性、Microsoft 伺服器的調節設定等等。另請參閱 <https://docs.microsoft.com/en-us/graph/throttling>。

** 建議您按以下順序, 逐步備份受保護的項目:

1. 信箱。
2. 所有信箱都備份之後, 請繼續進行 OneDrives。
3. OneDrive 備份完成後, 請繼續進行 SharePoint Online 網站。

初次完整備份可能需要數天的時間, 端視受保護項目的數目及其大小而定。

13.19.3 限制

- 只有擁有獲指派 Microsoft 365 授權的使用者, 以及擁有信箱或 OneDrive 的使用者會顯示在服務主控台中。
- 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。
- 無法在復原期間自動建立使用者、公用資料夾、群組或網站。例如, 如果您要復原已經刪除的 SharePoint Online 網站, 請先手動建立一個新網站, 然後將其指定為復原期間的目標網站。
- 即使您可以從搜尋結果中選擇這類項目, 也無法同時從不同的復原點復原這些項目。
- 在備份期間, 將會保留套用到內容的所有敏感度標籤。因此, 如果要將敏感內容復原到非原始位置, 且其使用者的存取權限不同, 則可能不會顯示該內容。

13.19.4 所需的使用者權限

在 Cyber Protection 服務中

本機 Microsoft 365 用代理程式必須以公司系統管理員帳戶的身分註冊，並在客戶租用戶層級使用。單位層級的公司系統管理員、單位系統管理員和使用者無法備份或復原 Microsoft 365 資料。

雲端 Microsoft 365 用代理程式可以同時在客戶租用戶層級和單位層級使用。如需有關這些層級及其個別系統管理員的詳細資訊，請參閱 "管理在不同層級新增的 Microsoft 365 組織" (第 274 頁)。

在 Microsoft 365 中

您的帳戶必須獲指派 Microsoft 365 中的全域系統管理員角色。

若要探索、備份和復原 Microsoft 365 公用資料夾，至少其中一個 Microsoft 365 系統管理員帳戶必須有一個信箱，而且必須有您要備份之公用資料夾的讀取/寫入權限。

- 本機代理程式會使用此帳戶登入 Microsoft 365。若要啟用代理程式存取所有信箱的內容，此帳戶便會被指派 **ApplicationImpersonation** 管理角色。如果您變更此帳戶密碼，請在服務主控台中更新密碼，如「變更 Microsoft 365 存取認證」中所述。
- 雲端代理程式無法登入 Microsoft 365。Microsoft 365 會直接為代理程式提供所需的權限。您只需要以全域系統管理員身分登入，以確認授予這些權限一次即可。代理程式不會儲存您的帳戶認證，也不用將這些帳戶認證用於執行備份和復原。在 Microsoft 365 中變更此帳戶密碼、停用此帳戶或刪除此帳戶不會影響代理程式作業。

13.19.5 Microsoft 365 授權報告

公司系統管理員可以下載受保護 Microsoft 365 授權的報告。此報告採用 CSV 格式，其中包含各授權的授權狀態以及使用授權的原因等資訊。此報告也包含受保護的授權名稱、相關聯的電子郵件、群組、Microsoft 365 組織、受保護工作負載的名稱和類型。

此報告僅適用於註冊 Microsoft 365 組織所在的租用戶。

若要下載 Microsoft 365 授權報告

1. 以公司系統管理員的身分，登入 Cyber Protection 服務主控台。
2. 按一下右上角的帳戶圖示。
3. 按一下 **[Microsoft 365 授權報告]**。

13.19.6 使用本機安裝的 Office 365 用代理程式

新增 Microsoft 365 組織

新增 Microsoft 365 組織

1. 以公司系統管理員的身分，登入服務主控台。
2. 按一下右上角的帳戶圖示，然後按一下 **[下載] > [Office 365 用代理程式]**。

3. 在已連線至網際網路的 Windows 電腦上下載及安裝代理程式。
4. 安裝完成後，按一下 **[裝置]** > **[Microsoft Office 365]**，然後輸入 Microsoft 365 全域系統管理員認證。

重要事項

組織 (公司群組) 內只能有一個本機安裝的 Microsoft 365 用代理程式。

因此，貴組織的資料項目會出現在服務主控台中的 **[Microsoft Office 365]** 頁面上。

保護 Exchange Online 信箱

哪些項目可以備份？

您可以備份使用者信箱和共用信箱。群組信箱和封存信箱 (**就地封存**) 無法進行備份。

可以復原哪些項目？

下列項目可以從信箱備份復原：

- 信箱
- 電子郵件資料夾
- 電子郵件訊息
- 行事曆事件
- 工作
- 連絡人
- 日誌項目
- 記事

您可以使用搜尋找出各項目。

將信箱復原至現有的信箱時，系統會覆寫 ID 相符的現有項目。

信箱項目復原不會造成任何覆寫。而是會在目標資料夾中重新建立信箱項目的完整路徑。

選取信箱

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. 按一下 **[Microsoft Office 365]**。
2. 如果出現提示，請以全域系統管理員身分登入 Microsoft 365。
3. 選擇您要備份的信箱。
4. 按一下 **[備份]**。

復原信箱和信箱項目

復原信箱

1. 按一下 **[Microsoft Office 365]**。
2. 選擇要復原的信箱，然後按一下**[復原]**。
您可以按名稱搜尋信箱。不支援萬用字元。
如果信箱遭到刪除，在 **[備份儲存]** 索引標籤中選擇此信箱，然後按一下 **[顯示備份]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。
4. 請按一下**[復原]>[信箱]**。
5. **[目標信箱]**可以檢視、變更或指定目標信箱。
原始信箱預設為選取狀態。如果此信箱不存在，則必須指定目標信箱。
6. 按一下 **[開始復原]**。

復原信箱項目

1. 按一下 **[Microsoft Office 365]**。
2. 按一下最初具有您想要復原之項目的信箱，然後按一下**[復原]**。
您可以按名稱搜尋信箱。不支援萬用字元。
如果信箱遭到刪除，在 **[備份儲存]** 索引標籤中選擇此信箱，然後按一下 **[顯示備份]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。
4. 按一下**[復原]>[電子郵件訊息]**。
5. 選擇您要復原的項目。
您可以選取下列搜尋選項。不支援萬用字元。
 - 電子郵件訊息：依主旨、寄件者、收件者、附件名稱及日期搜尋。
 - 事件：依主題及日期搜尋。
 - 工作：依主題及日期搜尋。
 - 連絡人：依姓名、電子郵件地址和電話號碼搜尋。選擇了電子郵件訊息後，按一下 **[顯示內容]** 以檢視其內容和附件。

注意事項

要下載附加檔案，請按一下名稱。

選擇電子郵件訊息後，您可按一下**[以電子郵件傳送]**，向電子郵件地址傳送訊息。訊息便會從您的管理員帳戶的電子郵件地址傳送。

若要能夠選擇資料夾，請按一下 **[復原資料夾]** 圖示：

6. 按一下 **[復原]**。
7. **[目標信箱]**可以檢視、變更或指定目標信箱。
原始信箱預設為選取狀態。如果此信箱不存在，則必須指定目標信箱。
8. 按一下 **[開始復原]**。
9. 確認選項無誤。

信箱項目必定復原至目標信箱中的 [已復原項目] 資料夾。

變更 Microsoft 365 存取認證

您可以變更 Microsoft 365 的存取認證，而無需重新安裝代理程式。

變更 Microsoft 365 存取認證

1. 按一下 [裝置] > **Microsoft Office 365**。
2. 按一下 [指定認證]。
3. 輸入 Microsoft 365 全域系統管理員認證，然後按一下 [確定]。

代理程式便會使用此帳戶登入 Microsoft 365。若要啟用代理程式存取所有信箱的內容，此帳戶便會被指派 **ApplicationImpersonation** 管理角色。

13.19.7 使用雲端 Microsoft 365 用代理程式

新增 Microsoft 365 組織

系統管理員可以將一或多個 Microsoft 365 組織新增到客戶租用戶或單位。

公司系統管理員可將組織新增至客戶租用戶。單位系統管理員和單位層級的客戶系統管理員可將組織新增至單位。

新增 Microsoft 365 組織

1. 根據您需要新增組織之處，以公司系統管理員或單位系統管理員的身分，登入服務主控台。
2. [適用於單位層級的公司系統管理員] 在管理入口網站中，瀏覽至所需的單位。
3. 按一下 [裝置] > [新增] > [Microsoft 365 商務版]。
此軟體會將您重新導向至 Microsoft 365 登入頁面。
4. 使用 Microsoft 365 全域系統管理員認證登入。
Microsoft 365 會顯示備份和復原貴組織資料所需權限的清單。
5. 確認您為 Cyber Protection 服務授予這些權限。

結果，您的 Microsoft 365 組織出現在服務主控台的 [裝置] 索引標籤底下。

有用的提示

- 雲端代理程式從組織新增至 Cyber Protection 服務開始，每 24 小時會與 Microsoft 365 同步一次。如果您新增或移除使用者、群組或網站，將不會在服務主控台中立即看到這個變更。若要立即同步變更，請在 [Microsoft 365] 頁面上選取組織，然後按一下 [重新整理]。
- 如果您已經將保護計劃套用到 [所有使用者]、[所有群組] 或 [所有網站] 群組，則只有在同步後，新增的項目才會包含在備份中。
- 根據 Microsoft 原則，當使用者、群組或網站從 Microsoft 365 圖形化使用者介面移除之後，仍然可以透過 API 使用幾天。在這段時間內，已移除的項目在服務主控台中為非作用中 (呈灰色) 狀態，而且將不會進行備份。當已移除的項目變成無法透過 API 使用時，就會從服務主控台中消失。其備份 (如果有的話) 可以在 [備份儲存] > [雲端應用程式備份] 中找到。

管理在不同層級新增的 Microsoft 365 組織

公司系統管理員對於新增至客戶租用戶層級的 Microsoft 365 組織，擁有完整的存取權。

公司系統管理員對於新增至單位的組織，擁有限制的存取權。在這些組織 (以括號中的單位名稱顯示) 中，公司系統管理員可以執行下列操作：

- 從備份中復原資料。
公司系統管理員可以將資料復原到租用戶中的所有組織 (無論在哪個層級新增這些組織)。
- 瀏覽備份中的備份與復原點。
- 刪除備份中的備份與復原點。
- 檢視警示與活動。

客戶租用戶層級的公司系統管理員無法執行下列操作：

- 將 Microsoft 365 組織新增至單位。
- 從單位刪除 Microsoft 365 組織。
- 同步新增至單位的 Microsoft 365 組織。
- 在新增至單位的 Microsoft 365 組織中，檢視、建立、編輯、刪除、套用、執行或撤銷資料項目的保護計劃。

單位系統管理員和單位層級的公司系統管理員對於新增至單位的組織，擁有完整的存取權。但是，他們無法存取父客戶租用戶中的任何資源，包括在其中建立的保護計劃。

刪除 Microsoft 365 組織

刪除 Microsoft 365 組織不會影響此組織資料的現有備份。如果您不再需要這些備份，請先刪除它們，然後再刪除 Microsoft 365 組織。否則，備份仍將使用可能會計費的雲端儲存空間。

如需有關如何刪除備份的詳細資訊，請參閱 "要刪除任何工作負載的備份" (第 239 頁)。

刪除 Microsoft 365 組織

1. 根據新增組織之處，以公司系統管理員或單位系統管理員的身分，登入服務主控台。
2. [適用於單位層級的公司系統管理員] 在管理入口網站中，瀏覽至所需的單位。
3. 前往 **[裝置] > [Microsoft 365]**。
4. 選擇組織，然後按一下 **[刪除群組]**。

結果，套用至此群組的備份計劃將會遭到撤銷。

但是，您還應該手動撤銷 Backup Service 應用程式對 Microsoft 365 組織資料的存取權限。

若要撤銷存取權限

1. 以全域系統管理員的身分登入 Microsoft 365。
2. 前往 **[系統管理中心] > [Azure Active Directory] > [企業應用程式] > [所有應用程式]**。
3. 選擇 **[Backup Service]** 應用程式並向下鑽研。
4. 前往 **[屬性]** 索引標籤，然後按一下動作面板上的 **[刪除]**。
5. 確認刪除作業。

結果, Microsoft 365 組織資料的存取權限將從 Backup Service 應用程式撤銷。

保護 Exchange Online 資料

哪些項目可以備份?

您可以備份使用者信箱、共用信箱和群組信箱。或者,您可以選擇備份所選信箱的封存信箱 (**就地封存**)。

從 Cyber Protection 服務 8.0 版開始,您可以備份公用資料夾。如果貴組織在 8.0 版發行前新增至 Cyber Protection 服務,您需要重新新增組織以取得此功能。請不要刪除組織,只要重複「[新增 Microsoft 365 組織](#)」中所述的步驟即可。因此, Cyber Protection 服務會取得使用對應 API 的權限。

可以復原哪些項目?

下列項目可以從信箱備份復原:

- 信箱
- 電子郵件資料夾
- 電子郵件訊息
- 行事曆事件
- 工作
- 連絡人
- 日誌項目
- 記事

下列項目可以從公用資料夾備份復原:

- 子資料夾
- 貼文
- 電子郵件訊息

您可以使用搜尋找出這些項目。

復原信箱、信箱項目、公用資料夾和公用資料夾項目時,您可以選擇是否要覆寫目標位置中的項目。

選取信箱

如下所述選擇信箱,然後[視需要](#)指定保護計劃的其他設定。

若要選取 Exchange Online 信箱

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務,請選取您要備份其使用者資料的組織。否則,請跳過此步驟。
3. 執行下列其中一項操作:

- 若要備份所有使用者信箱和所有共用信箱 (包括之後建立的信箱), 展開 **[使用者]** 節點、選取 **[所有使用者]**, 然後按一下 **[群組備份]**。
- 若要備份個別的使用者信箱或共用信箱, 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要備份其信箱的使用者, 然後按一下 **[備份]**。
- 若要備份所有群組的信箱 (包括之後建立之群組的信箱), 展開 **[群組]** 節點、選取 **[所有群組]**, 然後按一下 **[群組備份]**。
- 若要備份個別的群組信箱, 展開 **[群組]** 節點、選取 **[所有群組]**、選取您要備份其信箱的群組, 然後按一下 **[備份]**。

注意事項

雲端 Microsoft 365 用代理程式使用具有適當權限的帳戶存取群組信箱。因此, 若要備份群組信箱, 至少要有其中一個群組擁有者必須是擁有信箱的獲授權 Microsoft 365 使用者。如果是私有群組或擁有隱藏會員資格的群組, 則擁有者必須也是群組成員。

4. 在保護計劃面板上:

- 請確認在 **[要備份的內容]** 中已選擇 **[Microsoft 365 信箱]** 項目。
如果部分個別選擇的使用者沒有在其 Microsoft 365 計劃中包含 Exchange 服務, 您將無法選擇此選項。
如果部分針對群組備份選擇的使用者沒有在其 Microsoft 365 計劃中包含 Exchange 服務, 您將可以選擇此選項, 但是保護計劃將不會套用到這些使用者。
- 如果您不想要備份封存信箱, 停用 **[封存信箱]** 開關。

選擇公用資料夾

如下所述選擇公用資料夾, 然後視需要指定保護計劃的其他設定。

注意事項

公用資料夾會耗用 Microsoft 365 授權的備份配額中的授權。

若要選取 **Exchange Online** 公用資料夾

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務, 請展開您要備份其資料的組織。否則, 請跳過此步驟。
3. 展開 **[公用資料夾]** 節點, 然後選取 **[所有公用資料夾]**。
4. 執行下列其中一項操作:
 - 若要備份所有公用資料夾 (包括之後建立的公用資料夾), 請按一下 **[群組備份]**。
 - 若要備份個別的公用資料夾, 選取您要備份的公用資料夾, 然後按一下 **[備份]**。
5. 在保護計劃面板上, 請確認在 **[要備份的內容]** 中已選擇 **[Microsoft 365 信箱]** 項目。

復原信箱和信箱項目

復原信箱

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
 - 若要復原使用者信箱，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原其信箱的使用者，然後按一下 **[復原]**。
 - 若要復原共用信箱，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原的共用信箱，然後按一下 **[復原]**。
 - 若要復原群組信箱，展開 **[群組]** 節點、選取 **[所有群組]**、選取您要復原其信箱的群組，然後按一下 **[復原]**。
 - 如果使用者、群組或共用信箱遭到刪除，請在 **[備份儲存]** 索引標籤的 **[雲端應用程式備份]** 區段中選取該項目，然後按一下 **[顯示備份]**。您可以按名稱搜尋使用者和群組。不支援萬用字元。
4. 選擇復原點

注意事項

若只要查看含有信箱的復原點，請在 **[依內容篩選]** 中選取 **[信箱]**。

5. 按一下 **[復原] > [整個信箱]**。
6. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。
預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
7. 在 **[復原至信箱]** 中，檢視、變更或指定目標信箱。
原始信箱預設為選取狀態。如果此信箱不存在或選取了非原始組織，則必須指定目標信箱。
您無法在復原期間建立新的目標信箱。若要將某個信箱復原到新的信箱，首先您需要在所需的 Microsoft 365 組織中建立目標信箱，然後讓雲端代理程式同步變更。雲端代理程式每 24 小時會自動與 Microsoft 365 同步一次。若要立即同步變更，請在服務主控台的 **[Microsoft 365]** 頁面上選取組織，然後按一下 **[重新整理]**。
8. 按一下 **[開始復原]**。
9. 選取其中一個覆寫選項：
 - 覆寫現有項目
 - 不要覆寫現有項目
10. 按一下 **[繼續]** 可確認您的決定。

復原信箱項目

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
 - 若要從使用者信箱復原項目，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取其信箱原本包含您要復原之項目的使用者，然後按一下 **[復原]**。
 - 若要復原共用信箱中的項目，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取原本包含您要復原之項目的共用信箱，然後按一下 **[復原]**。
 - 若要從群組信箱復原項目，展開 **[群組]** 節點、選取 **[所有群組]**、選取其信箱原本包含您要復原之項目的群組，然後按一下 **[復原]**。
 - 如果使用者、群組或共用信箱遭到刪除，請在 **[備份儲存]** 索引標籤的 **[雲端應用程式備份]** 區段中選取該項目，然後按一下 **[顯示備份]**。您可以按名稱搜尋使用者和群組。不支援萬用字元。
4. 選擇復原點

注意事項

若只要查看含有信箱的復原點，請在 **[依內容篩選]** 中選取 **[信箱]**。

5. 按一下 **[復原] > [電子郵件訊息]**。
6. 瀏覽到所需的資料夾，或使用搜尋以取得所需項目的清單。

您可以使用下列搜尋選項。不支援萬用字元。

 - 電子郵件訊息：依主旨、寄件者、收件者、附件名稱及日期搜尋。
 - 事件：依主題及日期搜尋。
 - 工作：依主題及日期搜尋。
 - 連絡人：依姓名、電子郵件地址和電話號碼搜尋。
7. 選擇您要復原的項目。若要能夠選擇資料夾，請按一下 **[復原資料夾]** 圖示：

此外，您可以執行下列任何一項作業：

 - 選取項目後，按一下 **[顯示內容]** 可檢視其內容，包括附件。若要下載附加檔案，請按一下其名稱。
 - 選取電子郵件訊息或行事曆項目後，按一下 **[以電子郵件傳送]**，可將該項目傳送到指定的電子郵件地址。您可以選取寄件者，並撰寫要加入至轉寄項目的文字。
 - 只有在備份未經加密、使用搜尋，並在搜尋結果中選取單一項目時：按一下 **[顯示版本]** 來選取要復原的項目版本。您可以選取早於或晚於所選復原點的任何備份版本。
8. 按一下 **[復原]**。
9. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。

預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
10. 在 **[復原至信箱]** 中，檢視、變更或指定目標信箱。

原始信箱預設為選取狀態。如果此信箱不存在或選取了非原始組織，則必須指定目標信箱。

11. [僅在復原至使用者信箱或共用信箱時] 在 [路徑] 中，檢視或變更目標信箱中的目標資料夾。根據預設，已選取 [已復原項目] 資料夾。

群組信箱項目一律復原至 [收件匣] 資料夾。

12. 按一下 [開始復原]。
13. 選取其中一個覆寫選項：

- 覆寫現有項目
- 不要覆寫現有項目

14. 按一下 [繼續] 可確認您的決定。

復原公用資料夾和資料夾項目

若要復原公用資料夾或公用資料夾項目，目標 Microsoft 365 組織至少有一個系統管理員必須擁有目標公用資料夾的 [擁有者] 權限。如果復原失敗並出現拒絕存取的錯誤，請在目標資料夾內容中指派這些權限、在服務主控台中選取目標組織、按一下 [重新整理]，然後重複復原。

若要復原公用資料夾或資料夾項目

1. 按一下 [Microsoft 365]。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請展開您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
 - 展開 [公用資料夾] 節點、選取 [所有公用資料夾]、選取您要復原的公用資料夾或原本包含您要復原之項目的公用資料夾，然後按一下 [復原]。
 - 如果公用資料夾遭到刪除，請在 [備份儲存] 索引標籤的 [雲端應用程式備份] 區段中選取該公用資料夾，然後按一下 [顯示備份]。

您可以按名稱搜尋公用資料夾。不支援萬用字元。

4. 選擇復原點
5. 按一下 [復原資料]。
6. 瀏覽到所需的資料夾，或使用搜尋以取得所需項目的清單。

您可以依主旨、寄件者、收件者及日期搜尋電子郵件訊息和貼文。不支援萬用字元。

7. 選擇您要復原的項目。若要能夠選擇資料夾，請按一下 [復原資料夾] 圖示：

此外，您可以執行下列任何一項作業：

- 選取電子郵件訊息或貼文後，按一下 [顯示內容] 可檢視其內容，包括附件。若要下載附加檔案，請按一下其名稱。
- 選取電子郵件訊息或貼文後，按一下 [以電子郵件傳送]，可將該項目傳送到指定的電子郵件地址。您可以選取寄件者，並撰寫要加入至轉寄項目的文字。
- 只有在備份未經加密、使用搜尋，並在搜尋結果中選取單一項目時：按一下 [顯示版本] 來選取要復原的項目版本。您可以選取早於或晚於所選復原點的任何備份版本。

8. 按一下 [復原]。
9. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 [Microsoft 365 組織] 可檢視、變更或指定目標組織。

預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。

10. 在 **[復原至公用資料夾]** 中，檢視、變更或指定目標公用資料夾。

原始資料夾根據預設已經選取。如果此資料夾不存在或選取了非原始組織，則必須指定目標資料夾。

11. 在 **[路徑]** 中，檢視或變更目標公用資料夾中的目標子資料夾。預設將會重新建立原始路徑。
12. 按一下 **[開始復原]**。
13. 選取其中一個覆寫選項：

- **覆寫現有項目**
- **不要覆寫現有項目**

14. 按一下 **[繼續]** 可確認您的決定。

保護 OneDrive 檔案

哪些項目可以備份？

您可以備份整個 OneDrive 或個別的檔案和資料夾。

檔案會與其共用權限一起備份。進階權限層級 (**[設計]**、**[完整]**、**[提供]**) 不會進行備份。

有些檔案可能含有機密資訊，而且 Microsoft 365 中的資料洩漏防禦 (DLP) 規則可能會封鎖對它們的存取。這些檔案未備份，而且備份作業完成後也不會顯示任何警告。

可以復原哪些項目？

您可以復原整個 OneDrive 或已備份的任何檔案或資料夾。

您可以使用搜尋找出這些項目。

您可以選擇要復原共用權限，還是讓檔案繼承復原目標資料夾的權限。

檔案與資料夾的共用連結不會復原。

選取 OneDrive 檔案

如下所述選擇檔案，然後視需要指定保護計劃的其他設定。

若要選取 OneDrive 檔案

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選取您要備份其使用者資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
 - 若要備份所有使用者 (包括之後建立的使用者) 的檔案，展開 **[使用者]** 節點、選取 **[所有使用者]**，然後按一下 **[群組備份]**。
 - 若要備份個別使用者的檔案，展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要備份其檔案的使用者，然後按一下 **[備份]**。
4. 在保護計劃面板上：

- 確認在 **[要備份的內容]** 中，選擇 **[OneDrive]** 項目。
如果部分個別選擇的使用者沒有在其 Microsoft 365 計劃中包含 OneDrive 服務，您將無法選擇此選項。
如果部分針對群組備份選擇的使用者沒有在其 Microsoft 365 計劃中包含 OneDrive 服務，您可以選擇此選項，但是保護計劃將不會套用到這些使用者。
- 在 **[要備份的項目]** 中，執行下列其中一項操作：
 - 保留預設設定 **[全部]** (所有檔案)。
 - 新增檔案和資料夾的名稱或路徑來指定要備份的檔案和資料夾。
您可以使用萬用字元 (*、** 和 ?)。如需有關指定路徑和使用萬用字元的詳細資訊，請參閱 [「檔案篩選器」](#)。
 - 瀏覽來指定要備份的檔案和資料夾。
只有在建立單一使用者的保護計劃時，才可以使用 **[瀏覽]** 連結。
- [選擇性] 在 **[要備份的項目]** 中，按一下 **[顯示排除項目]** 來指定要在備份期間略過的檔案和資料夾。
檔案排除項目會覆寫檔案選項，亦即，如果您在兩個欄位中指定相同的檔案，將會在備份期間略過這個檔案。

復原 OneDrive 和 OneDrive 檔案

復原整個 OneDrive

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原其 OneDrive 的使用者，然後按一下 **[復原]**。
如果使用者遭到刪除，請在 **[備份儲存]** 索引標籤的 **[雲端應用程式備份]** 區段中選取該使用者，然後按一下 **[顯示備份]**。
您可以按名稱搜尋使用者。不支援萬用字元。
4. 選擇復原點

注意事項

若只要查看含有 OneDrive 檔案的復原點，請在 **[依內容篩選]** 中選取 **[OneDrive]**。

5. 按一下 **[復原] > [整個 OneDrive]**。
6. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。
預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
7. 在 **[復原至磁碟機]** 中，檢視、變更或指定目標使用者。
預設會選取原始使用者。如果此使用者不存在或選取了非原始組織，則必須指定目標使用者。
8. 選取是否要復原檔案的共用權限。
9. 按一下 **[開始復原]**。

10. 選取其中一個覆寫選項：
 - 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
11. 按一下 **[繼續]** 可確認您的決定。

復原 OneDrive 檔案

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原其 OneDrive 檔案的使用者，然後按一下 **[復原]**。

如果使用者遭到刪除，請在 **[備份儲存]** 索引標籤的 **[雲端應用程式備份]** 區段中選取該使用者，然後按一下 **[顯示備份]**。

您可以按名稱搜尋使用者。不支援萬用字元。

4. 選擇復原點

注意事項

若只要查看含有 OneDrive 檔案的復原點，請在 **[依內容篩選]** 中選取 **[OneDrive]**。

5. 按一下 **[復原] > [檔案/資料夾]**。
6. 瀏覽至所需的資料夾，或使用搜尋以取得所需檔案和資料夾的清單。

如果備份經過加密，則無法使用搜尋。
7. 選擇您要復原的檔案。

如果備份未經加密而且您選擇單一檔案，您可以按一下 **[顯示版本]** 來選取要復原的檔案版本。您可以選取早於或晚於所選復原點的任何備份版本。
8. 如果您要下載檔案，請選擇該檔案，按一下 **[下載]**，選擇儲存資料的位置，然後按一下 **[儲存]**。否則，請跳過此步驟。
9. 按一下 **[復原]**。
10. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。

預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
11. 在 **[復原至磁碟機]** 中，檢視、變更或指定目標使用者。

預設會選取原始使用者。如果此使用者不存在或選取了非原始組織，則必須指定目標使用者。
12. 在 **[路徑]** 中，檢視或變更目標使用者 OneDrive 中的目標資料夾。預設會選取原始位置。
13. 選取是否要復原檔案的共用權限。
14. 按一下 **[開始復原]**。
15. 選擇其中一個檔案覆寫選項：
 - 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

16. 按一下 **[繼續]** 可確認您的決定。

保護 SharePoint Online 網站

哪些項目可以備份？

您可以備份 SharePoint 傳統網站集合、群組 (新型團隊) 網站和通訊網站。此外，您也可以選擇個別的子網站、清單和程式庫以進行備份。

備份期間會略過下列項目：

- **[外觀與風格]** 網站設定 (但 **標題、描述和標誌** 除外)。
- 網站頁面註解與頁面註解設定 (註解 **開啟/關閉**)。
- **[網站功能]** 網站設定。
- Web 組件頁面和 wiki 頁面中內嵌的 Web 組件 (基於 SharePoint Online API 限制)。
- 已簽出的檔案—已手動簽出以供編輯的檔案以及已在程式庫中建立或上傳的所有檔案，其中已啟用 **[需要簽出]** 選項。若要備份這些檔案，請先簽入這些檔案。
- OneNote 檔案 (基於 SharePoint Online API 限制)。
- 外部資料和受管理中繼資料類型的欄。
- 預設網站集合 "domain-my.sharepoint.com"。這是所有組織使用者 OneDrive 檔案所在的集合。
- 資源回收筒的內容。

限制

- 如果標題/描述的大小超過 10000 個位元組，則在備份期間，網站/子網站/清單/欄的標題和描述會遭到截斷。
- 您無法備份在 SharePoint Online 中建立的舊版檔案。只有最新版的檔案受到保護。
- 您無法備份文件保留庫。
- 您無法備份使用 Microsoft 365 前置項 Business Productivity Online Suite (BPOS) 建立的網站。
- 您無法針對使用受管理路徑 /portals 的網站備份設定 (例如，<https://<tenant>.sharepoint.com/portals/...>)。
- 只有在目標 Microsoft 365 組織中啟用資訊版權管理 (IRM) 的情況下，才能復原清單或文件庫的 IRM 設定。

可以復原哪些項目？

下列項目可以從網站備份復原：

- 整個網站
- 子網站
- 清單
- 清單項目
- 文件庫
- 文件

- 清單項目附件
- 網站頁面和 wiki 頁面

您可以使用搜尋找出這些項目。

項目可以復原到原始或非原始的網站。已復原項目的路徑與原始項目路徑相同。如果路徑不存在，則會建立一個路徑。

您可以選擇要復原共用權限，還是讓項目在復原後繼承父物件的權限。

無法復原哪些項目？

- 以 **Visio 程序存放庫**範本為基礎的子網站。
- 以下類型的清單：**調查清單**、**工作清單**、**圖片庫**、**連結**、**行事曆**、**討論板**、**外部**和**匯入試算表**。
- 啟用多個內容類型的清單。

選擇 SharePoint Online 資料

如下所述選擇資料，然後視需要指定保護計劃的其他設定。

若要選擇 **SharePoint Online** 資料

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選取您要備份其使用者資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
 - 若要備份組織中的所有傳統 SharePoint 網站 (包括之後建立的網站)，展開 **[網站集合]** 節點、選擇 **[所有網站集合]**，然後按一下 **[群組備份]**。
 - 若要備份個別的傳統網站，展開 **[網站集合]** 節點、選取 **[所有網站集合]**、選取您要備份的網站，然後按一下 **[備份]**。
 - 若要備份所有群組 (新型團隊) 網站 (包括之後建立的網站)，展開 **[群組]** 節點、選擇 **[所有群組]**，然後按一下 **[群組備份]**。
 - 若要備份個別的群組 (新型團隊) 網站，展開 **[群組]** 節點、選擇 **[所有群組]**、選擇您要備份其網站的群組，然後按一下 **[備份]**。
4. 在保護計劃面板上：
 - 確認在 **[要備份的內容]** 中，選擇 **[SharePoint 網站]** 項目。
 - 在 **[要備份的項目]** 中，執行下列其中一項操作：
 - 保留預設設定 **[全部]** (所選網站的所有項目)。
 - 新增子網站、清單和程式庫的名稱或路徑來指定要備份的子網站、清單和程式庫。
若要備份子網站或最上層網站清單/程式庫，請使用下列格式指定其顯示名稱：`/display name/**`
若要備份子網站清單/程式庫，請使用下列格式指定其顯示名稱：`/subsite display name/list display name/**`
子網站、清單和程式庫的顯示名稱會顯示在 SharePoint 網站或子網站的 **[網站內容]** 頁面上。

- 瀏覽來指定要備份的子網站。
只有在建立單一網站的保護計劃時, 才可以使用 **[瀏覽]** 連結。
- [選擇性] 在 **[要備份的項目]** 中, 按一下 **[顯示排除項目]** 來指定要在備份期間略過的子網站、清單和程式庫。
項目排除項目會覆寫項目選項, 亦即, 如果您在兩個欄位中指定相同的子網站, 將會在備份期間略過這個子網站。

復原 SharePoint Online 資料

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務, 請選擇您要復原其已備份資料的組織。否則, 請跳過此步驟。
3. 執行下列其中一項操作:
 - 若要從群組 (新型團隊) 網站復原資料, 展開 **[群組]** 節點、選擇 **[所有群組]**、選擇其網站原本包含您要復原之項目的群組, 然後按一下 **[復原]**。
 - 若要從傳統網站復原資料, 展開 **[網站集合]** 節點、選取 **[所有網站集合]**、選取原本包含您要復原之項目的網站, 然後按一下 **[復原]**。
 - 如果網站遭到刪除, 請在 **[備份儲存]** 索引標籤的 **[雲端應用程式備份]** 區段中選取該網站, 然後按一下 **[顯示備份]**。

您可以按名稱搜尋群組和網站。不支援萬用字元。

4. 選擇復原點

注意事項

若只要查看含有 SharePoint 網站的復原點, 請在 **[依內容篩選]** 中選取 **[SharePoint 網站]**。

5. 按一下 **[復原 SharePoint 檔案]**。
6. 瀏覽到所需的資料夾, 或使用搜尋以取得所需資料項目的清單。
如果備份經過加密, 則無法使用搜尋。
7. 選擇您要復原的項目。
如果備份未經加密、使用搜尋, 並在搜尋結果中選取單一項目, 您可以按一下 **[顯示版本]** 來選取要復原的項目版本。您可以選取早於或晚於所選復原點的任何備份版本。
8. 如果您要下載項目, 請選擇該項目, 按一下 **[下載]**, 選擇儲存項目的位置, 然後按一下 **[儲存]**。
否則, 請跳過此步驟。
9. 按一下 **[復原]**。
10. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務, 按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。
預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織, 您必須指定目標組織。
11. 在 **[復原至網站]** 中, 檢視、變更或指定目標網站。
預設會選取原始網站。如果此網站不存在或選取了非原始組織, 則必須指定目標網站。
12. 選取是否要復原已復原項目的共用權限。
13. 按一下 **[開始復原]**。
14. 選取其中一個覆寫選項:

- 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

15. 按一下 **[繼續]** 可確認您的決定。

保護 Microsoft 365 Teams

哪些項目可以備份？

您可以備份整個小組。這包括小組名稱、小組成員清單、小組頻道及其內容、小組信箱和會議, 以及小組網站。

可以復原哪些項目？

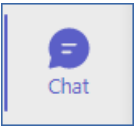
- 整個小組
- 小組頻道
- 頻道檔案
- 小組信箱
- 小組信箱中的電子郵件資料夾
- 小組信箱中的電子郵件訊息
- 會議
- 小組網站

您無法復原小組頻道中的對話, 但是您可以將這些對話下載為單一 html 檔案。

限制

系統不會備份下列項目：

- 一般頻道的設定 (仲裁喜好設定) – 由於 [Microsoft Teams 測試版 API](#) 的限制。
- 自訂頻道的設定 (仲裁喜好設定) – 由於 [Microsoft Teams 測試版 API](#) 的限制。
- 會議記錄。

聊天區段  中的訊息。這些是私人的一對一聊天或群組聊天。

•

- 貼圖和稱讚。

下列頻道索引標籤支援備份和復原：

- Word
- Excel
- PowerPoint
- PDF
- 文件庫

由於 API 的限制, 系統會備份私人頻道中共用的檔案, 但無法還原。

注意事項

這些檔案與公用頻道中共用的檔案分別儲存在特定位置。

選擇小組

如下所述選擇小組，然後視需要指定保護計劃的其他設定。

若要選擇小組

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要備份其小組的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
 - 若要備份組織中的所有小組 (包括之後建立的小組)，展開 **[小組]** 節點、選擇 **[所有小組]**，然後按一下 **[群組備份]**。
 - 若要備份個別的小組，展開 **[小組]** 節點、選擇 **[所有小組]**、選擇您要備份的小組，然後按一下 **[備份]**。

您可以按名稱搜尋小組。不支援萬用字元。
4. 在保護計劃面板上：
 - 請確認已在 **[要備份的內容]** 中，選擇 **[Microsoft Teams]** 項目。
 - [選擇性] 在 **[保留時間]** 中，設定清理選項。
 - [選擇性] 如果您要加密備份，請啟用 **[加密]** 開關，然後設定密碼並選擇加密演算法。

復原整個小組

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份小組的組織。否則，請跳過此步驟。
3. 展開 **[小組]** 節點、選擇 **[所有小組]**、選擇您要復原的小組，然後按一下 **[復原]**。

您可以按名稱搜尋小組。不支援萬用字元。
4. 選擇復原點
5. 按一下 **[復原] > [整個小組]**。

如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。

預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
6. 在 **[復原到團隊]** 中，查看目標團隊或選擇另一個目標團隊。

預設選取原始團隊。如果此團隊不存在 (例如，已刪除) 或您選擇的組織未包含原始團隊，則必須從下拉清單中選擇目標團隊。

您只能將團隊還原到現有團隊。您無法在復原作業期間建立團隊。
7. 按一下 **[開始復原]**。
8. 選取其中一個覆寫選項：

- 若現有內容較舊則加以覆寫
- 覆寫現有內容
- 不要覆寫現有內容

9. 按一下 **[繼續]** 可確認您的決定。

當您在 Microsoft Teams 的圖形介面中刪除頻道時，該頻道不會立即從系統移除。因此，當您復原整個小組時，無法使用此頻道的名稱，而且該名稱將會加上一個後置。

對話在頻道的 **[檔案]** 索引標籤中，會復原為單一 html 檔案。您可以在根據下列模式命名的資料夾中找到此檔案：<小組名稱>_<頻道名稱>_conversations_backup_<復原日期>T<復原時間>Z。

注意事項

復原小組或小組頻道之後，前往 Microsoft Teams，選擇所復原的頻道，然後按一下其 **[檔案]** 索引標籤。否則，這些頻道之後的備份將不會包含此索引標籤的內容 – 由於 [Microsoft Teams 測試版 API](#) 的限制。

復原小組頻道或小組頻道中的檔案

若要復原小組頻道

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份小組的組織。否則，請跳過此步驟。
3. 展開 **[小組]** 節點、選擇 **[所有小組]**、選擇您要復原其頻道的小組，然後按一下 **[復原]**。
4. 選擇復原點
5. 按一下 **[復原]>[頻道]**。
6. 選擇您要復原的頻道，然後按一下 **[復原]**。若要在主窗格中選擇頻道，請選擇其名稱前方的核取方塊。
下列搜尋選項可供使用：
 - 若是 **[對話]**：傳送者、主旨、內容、語言、附件名稱、日期或日期範圍。
 - 若是 **[檔案]**：檔案名稱或資料夾名稱、檔案類型、大小、上次變更的日期或日期範圍。
7. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。
預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
8. 在 **[復原至小組]** 中，檢視、變更或指定目標小組。
預設會選取原始小組。如果此小組不存在或選取了非原始組織，則必須指定目標小組。
9. 在 **[復原至頻道]** 中，檢視、變更或指定目標頻道。
10. 按一下 **[開始復原]**。
11. 選取其中一個覆寫選項：
 - 若現有內容較舊則加以覆寫
 - 覆寫現有內容
 - 不要覆寫現有內容
12. 按一下 **[繼續]** 可確認您的決定。

對話在頻道的 **[檔案]** 索引標籤中，會復原為單一 html 檔案。您可以在根據下列模式命名的資料夾中找到此檔案：<小組名稱>_<頻道名稱>_conversations_backup_<復原日期>T<復原時間>Z。

注意事項

復原小組或小組頻道之後，前往 Microsoft Teams，選擇所復原的頻道，然後按一下其 **[檔案]** 索引標籤。否則，這些頻道之後的備份將不會包含此索引標籤的內容 – 由於 [Microsoft Teams 測試版 API](#) 的限制。

若要復原小組頻道中的檔案

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份小組的組織。否則，請跳過此步驟。
3. 展開 **[小組]** 節點、選擇 **[所有小組]**、選擇您要復原其頻道的小組，然後按一下 **[復原]**。
4. 選擇復原點
5. 按一下 **[復原]>[頻道]**。
6. 選擇所需的頻道，然後開啟 **[檔案]** 資料夾。
瀏覽到所需的項目，或使用搜尋以取得所需項目的清單。下列搜尋選項可供使用：檔案名稱或資料夾名稱、檔案類型、大小、上次變更的日期或日期範圍。
7. 選擇您要復原的項目，然後按一下 **[復原]**
8. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。
預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
9. 在 **[復原至小組]** 中，檢視、變更或指定目標小組。
預設會選取原始小組。如果此小組不存在或選取了非原始組織，則必須指定目標小組。
10. 在 **[復原至頻道]** 中，檢視、變更或指定目標頻道。
11. 選取是否要復原已復原項目的共用權限。
12. 按一下 **[開始復原]**。
13. 選取其中一個覆寫選項：
 - 若現有內容較舊則加以覆寫
 - 覆寫現有內容
 - 不要覆寫現有內容
14. 按一下 **[繼續]** 可確認您的決定。

您無法復原個別的對話。在主窗格中，您僅能瀏覽 **[對話]** 資料夾或將其內容下載為單一 html 檔案。方法是，按一下 **[復原資料夾]** 圖示 、選擇所需的 **[對話]** 資料夾，然後按一下 **[下載]**。

您可以在 **[對話]** 資料夾中，按照下列條件，搜尋訊息：

- 寄件者
- 內容
- 附件名稱
- 日期

復原小組信箱

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份小組的組織。否則，請跳過此步驟。
3. 展開 **[小組]** 節點、選擇 **[所有小組]**、選擇您要復原其信箱的小組，然後按一下 **[復原]**。
您可以按名稱搜尋小組。不支援萬用字元。
4. 選擇復原點
5. 按一下 **[復原]>[電子郵件訊息]**。
6. 按一下 [復原資料夾] 圖示 、選擇根信箱資料夾，然後按一下 **[復原]**。

注意事項

您也可以從所選信箱復原個別的資料夾。

7. 按一下 **[復原]**。
8. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。
預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
9. 在 **[復原至信箱]** 中，檢視、變更或指定目標信箱。
原始信箱預設為選取狀態。如果此信箱不存在或選取了非原始組織，則必須指定目標信箱。
10. 按一下 **[開始復原]**。
11. 選取其中一個覆寫選項：
 - 覆寫現有項目
 - 不要覆寫現有項目
12. 按一下 **[繼續]** 可確認您的決定。

復原電子郵件訊息和會議

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份小組的組織。否則，請跳過此步驟。
3. 展開 **[小組]** 節點、選擇 **[所有小組]**、選擇您要復原其電子郵件訊息或會議的小組，然後按一下 **[復原]**。
您可以按名稱搜尋小組。不支援萬用字元。
4. 選擇復原點
5. 按一下 **[復原]>[電子郵件訊息]**。
6. 瀏覽到所需的項目，或使用搜尋以取得所需項目的清單。
下列搜尋選項可供使用：
 - 電子郵件訊息：依主題、寄件者、收件者及日期搜尋。
 - 若是會議：依事件名稱和日期搜尋。
7. 選擇您要復原的項目，然後按一下 **[復原]**。

注意事項

您可以在 **[行事曆]** 資料夾中找到會議。

此外，您可以執行下列任何一項作業：

- 選取項目後，按一下 **[顯示內容]** 可檢視其內容，包括附件。要下載附加檔案，請按一下名稱。
 - 選取電子郵件訊息或會議後，按一下 **[以電子郵件傳送]** 可將該項目傳送到指定的電子郵件地址。您可以選取寄件者，並撰寫要加入至轉寄項目的文字。
8. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。
預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
 9. 在 **[復原至信箱]** 中，檢視、變更或指定目標信箱。
原始信箱預設為選取狀態。如果此信箱不存在或選取了非原始組織，則必須指定目標信箱。
 10. 按一下 **[開始復原]**。
 11. 選取其中一個覆寫選項：
 - **覆寫現有項目**
 - **不要覆寫現有項目**
 12. 按一下 **[繼續]** 可確認您的決定。

復原小組網站或特定的網站項目

1. 按一下 **[Microsoft 365]**。
2. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，請選擇您要復原其已備份小組的組織。否則，請跳過此步驟。
3. 展開 **[小組]** 節點、選擇 **[所有小組]**、選擇您要復原其網站的小組，然後按一下 **[復原]**。
您可以按名稱搜尋小組。不支援萬用字元。
4. 選擇復原點
5. 按一下 **[復原] > [小組網站]**。
6. 瀏覽到所需的項目，或使用搜尋以取得所需項目的清單。
如果備份經過加密，則無法使用搜尋。
7. 選擇您要復原的項目，然後按一下 **[復原]**。
8. 如果多個 Microsoft 365 組織新增到 Cyber Protection 服務，按一下 **[Microsoft 365 組織]** 可檢視、變更或指定目標組織。
預設會選取原始組織和小組。如果 Cyber Protection 服務中不再登錄此組織，您必須指定目標組織。
9. 在 **[復原至小組]** 中，檢視、變更或指定目標小組。
預設會選取原始小組。如果此小組不存在或選取了非原始組織，則必須指定目標網站。
10. 選取是否要復原已復原項目的共用權限。
11. 按一下 **[開始復原]**。
12. 選取其中一個覆寫選項：

- 若現有內容較舊則加以覆寫
- 覆寫現有內容
- 不要覆寫現有內容

13. 按一下 **[繼續]** 可確認您的決定。

升級雲端代理程式

本節描述如何升級到最新版本的 Microsoft 365 備份解決方案。此版本支援 OneDrive 和 SharePoint Online 備份，並提升備份和復原效能。從 8.0 版 Cyber Protection 服務開始，舊版解決方案不再支援下列功能：編輯、刪除、套用以及撤銷保護計劃。

升級可用性取決於資料中心準備情況以及服務提供者所進行的設定。如果可以升級，服務主控台會在 **Microsoft Office 365 (v1)** 索引標籤的最上方顯示一則通知。

升級程序

在升級期間，您的 Microsoft 365 組織使用者會新增到新的備份解決方案。保護計劃會移轉並套用到適當的使用者。

稍早建立的備份會從雲端中的一個位置複製到另一個位置。在 **[備份儲存]** 索引標籤上，已複製的備份會顯示在不同於 **[雲端應用程式備份]** 的另一個區段，而原始備份則保留在 **[雲端儲存空間]** 位置。升級程序完成時，原始備份會從 **[雲端儲存空間]** 位置刪除。

根據組織中的使用者數目、備份數目，以及 Microsoft 365 存取速度，升級可能需要數小時甚至數天才會完成。在升級期間，可以從稍早建立的備份復原。不過，將會失去升級期間建立的備份和保護計劃。

在升級失敗少有的情況下，備份解決方案仍然可以完整運作，而且升級可以從失敗點重新開始。

若要開始升級程序

1. 按一下 **Microsoft Office 365 (v1)**。
2. 按一下畫面最上方通知中的 **[升級]**。
3. 確認您想要開始升級程序。
4. 選取貴組織使用的 Microsoft 資料中心。
此軟體會將您重新導向至 Microsoft 365 登入頁面。
5. 使用 Microsoft 365 全域系統管理員認證登入。
Microsoft 365 會顯示備份和復原貴組織資料所需權限的清單。
6. 確認您為 Cyber Protection 服務授予這些權限。
系統會將您重新導向至服務主控台，並開始升級程序。升級進度會顯示在 **[Microsoft 365] > [活動]** 面板上。

13.20 保護 Google Workspace 資料

13.20.1 Google Workspace 保護是什麼意思？

- Google Workspace 使用者資料 (Gmail 信箱、行事曆、聯絡人、Google 雲端硬碟) 與 Google Workspace 共用磁碟機的雲端對雲端備份和復原。
- 電子郵件、檔案、聯絡人和其他項目的細微復原。
- 對數個 Google Workspace 組織和跨組織復原的支援。
- 選擇性地透過 Ethereum 區塊鏈資料庫公證備份檔案。啟用時，您可以證明檔案在備份後即是真實和未變更的。
- 選擇性的全文檢索。啟用時，您可以依電子郵件內容來搜尋電子郵件。
- 每個公司最多有 5000 個項目 (信箱、Google 雲端硬碟和共用磁碟機) 可以受到保護，而不會降低效能。

13.20.2 所需的使用者權限

在 Cyber Protection 服務中

在 Cyber Protection 服務中，您必須是客戶租用戶層級的公司系統管理員。單位層級的公司系統管理員、單位系統管理員和使用者無法備份或復原 Google Workspace 資料。

在 Google Workspace 中

若要將 Google Workspace 組織新增到 Cyber Protection 服務，您必須使用已啟用 API 存取的 Super Admin 身分登入 (在 Google Admin 主控台中的 **[安全性]** > **[API 參照]** > **[啟用 API 存取]**)。

Super Admin 密碼不會儲存在任何地方，也不會用於執行備份和復原。在 Google Workspace 中變更此密碼不會影響 Cyber Protection 服務作業。

如果新增 Google Workspace 組織的 Super Admin 從 Google Workspace 刪除，或者獲指派權限較少的角色，則備份將會失敗，並出現「拒絕存取」之類的錯誤。在此情況下，重複「[新增 Google Workspace 組織](#)」程序，並指定有效的 Super Admin 認證。若要避免這個情形，建議您建立專用的 Super Admin 使用者，以供備份和復原之用。

13.20.3 關於備份排程

雲端代理程式可服務多個客戶，因此它會針對每個保護計劃，自行決定開始時間，以確保一天中的負載均衡，且所有客戶都獲得同等的服務品質。

每個保護計劃每天都會在相同的時間執行。

13.20.4 限制

- 主控台僅會顯示擁有獲指派 Google Workspace 授權和信箱或 Google 雲端硬碟的使用者。
- 不支援在加密的備份中進行搜尋。

- 原生 Google 格式的文件會備份為一般 Office 文件，並以不同的副檔名顯示在服務主控台中，例如 .docx 或 .pptx。在復原期間，這些文件會轉換為其原始格式。
- 一小時內手動執行備份不超過 10 次。
- 不超過 10 個同時復原作業 (此數目包括 Microsoft 365 和 Google Workspace 復原)。
- 即使您可以從搜尋結果中選擇這類項目，也無法同時從不同的復原點復原這些項目。

13.20.5 新增 Google Workspace 組織

若要將 Google Workspace 組織新增至 Cyber Protection 服務，您需要專用的個人 Google Cloud 專案。如需有關如何建立並設定這種專案的詳細資訊，請參閱 "建立個人 Google Cloud 專案" (第 294 頁)。

使用專用的個人 Google Cloud 專案新增 Google Workspace 組織

1. 以公司系統管理員的身分，登入服務主控台。
2. 按一下 **[裝置] > [新增] > [Google Workspace]**。
3. 輸入 Google Workspace 帳戶超級系統管理員的電子郵件地址。
對於此程序，無論是否針對超級系統管理員電子郵件帳戶啟用 2 步驟驗證，都無關緊要。
4. 瀏覽包含您在 Google Cloud 專案中建立之服務帳戶私密金鑰的 JSON 檔案。
您也可以將檔案內容當作文字貼上。
5. 按一下 **[確認]**。

結果，您的 Google Workspace 組織出現在服務主控台的 **[裝置]** 索引標籤底下。

有用的提示

- 新增 Google Workspace 組織之後，將會備份主要網域和所有次要網域 (如果有的話) 中的使用者資料與共用磁碟機。已備份的資源將會顯示在一個清單中，而且將不會依其網域分組。
- 雲端代理程式從組織新增至 Cyber Protection 服務開始，每 24 小時會與 Google Workspace 同步一次。如果您新增或移除使用者或共用磁碟機，將不會在服務主控台中立即看到這個變更。若要立即同步變更，請在 **[Google Workspace]** 頁面上選取組織，然後按一下 **[重新整理]**。
- 如果您已經將保護計劃套用到 **[所有使用者]** 或 **[所有共用磁碟機]** 群組，則只有在同步後，新增的項目才會包含在備份中。
- 根據 Google 原則，當使用者或共用磁碟機從 Google Workspace 圖形化使用者介面移除之後，仍然可以透過 API 使用幾天。在這段時間內，已移除的項目在服務主控台中為非作用中 (呈灰色) 狀態，而且將不會進行備份。當已移除的項目變成無法透過 API 使用時，就會從服務主控台中消失。其備份 (如果有的話) 可以在 **[備份儲存] > [雲端應用程式備份]** 中找到。

13.20.6 建立個人 Google Cloud 專案

若要使用專用的 Google Cloud 專案將 Google Workspace 組織新增至 Cyber Protection 服務，您需要執行下列操作：

1. 建立新的 Google Cloud 專案。
2. 啟用此專案所需的 API。

3. 設定此專案的認證：
 - a. 設定 OAuth 同意畫面。
 - b. 為 Cyber Protection 服務建立並設定服務帳戶。
4. 為您的 Google Workspace 帳戶授予新的專案存取權。

注意事項

本主題包含第三方使用者介面的描述，如有變更，恕不另行通知。

建立新的 Google Cloud 專案

1. 以超級系統管理員的身分，登入 Google Cloud Platform (console.cloud.google.com)。
2. 在 Google Cloud Platform 主控台中，按一下 **[選取專案] > [新增專案]**。
3. 為您的新專案指定一個名稱。
4. 按一下 **[建立]**。

結果，您的新 Google Cloud 專案隨即建立。

啟用此專案所需的 API

1. 在 Google Cloud Platform 主控台中，選取您的新專案。
2. 從導覽功能表中，選取 **[API 和服務] > [已啟用的 API 和服務]**。
3. 逐一停用在此專案中預設啟用的所有 API：
 - a. 向下捲動 **[已啟用的 API 和服務]** 頁面，然後按一下已啟用之 API 的名稱。
所選 API 的 **[API/服務詳細資料]** 頁面隨即開啟。
 - b. 按一下 **[停用 API]**，然後按一下 **[停用]**，確認您的選擇。
 - c. 返回 **[API 和服務] > [已啟用的 API 和服務]**，然後停用下一個 API。
4. 從導覽功能表中，選取 **[API 和服務] > [程式庫]**。
5. 在 API 程式庫中，逐一啟用下列 API：
 - Gmail API
 - Google Drive API
 - Admin SDK
 - Google Calendar API
 - Google People API

使用搜尋列尋找所需的 API。若要啟用 API，請按一下其名稱，然後按一下 **[啟用]**。若要搜尋下一個 API，從導覽功能表中，選取 **[API 和服務] > [程式庫]** 以返回 API 程式庫。

設定 OAuth 同意畫面

1. 從 Google Cloud Platform 的導覽功能表中，選取 **[API 和服務] > [OAuth 同意畫面]**。
2. 在開啟的視窗中，選取 **[內部]** 作為使用者類型，然後按一下 **[建立]**。
3. 在 **[應用程式名稱]** 欄位中，為您的應用程式指定一個名稱。
4. 在 **[使用者支援電子郵件]** 欄位中，輸入超級系統管理員電子郵件。
5. 在 **[開發人員聯絡資訊]** 欄位中，輸入超級系統管理員電子郵件。
6. 將其他所有欄位留空，然後按一下 **[儲存並繼續]**。

7. 在 **[範圍]** 頁面上, 按一下 **[儲存並繼續]**, 而不必變更任何內容。
8. 在 **[摘要]** 頁面上, 確認您的設定, 然後按一下 **[返回資訊主頁]**。

為 **Cyber Protection** 服務建立並設定服務帳戶

1. 從 Google Cloud Platform 的導覽功能表中, 選取 **[IAM 與管理]** > **[服務帳戶]**。
2. 按一下 **[建立服務帳戶]**。
3. 指定服務帳戶的名稱。
4. 指定服務帳戶的說明。
5. 按一下 **[建立並繼續]**。
6. 請勿變更 **[將專案存取權授予這個服務帳戶]** 和 **[將這個服務帳戶的存取權授予使用者]** 步驟中的任何內容。
7. 按一下 **[完成]**。
[服務帳戶] 頁面隨即開啟。
8. 在 **[服務帳戶]** 頁面上, 選取新的服務帳戶, 然後在 **[動作]** 底下, 按一下 **[管理金鑰]**。
9. 在 **[金鑰]** 底下, 按一下 **[新增金鑰]** > **[建立新的金鑰]**, 然後選取 **[JSON]** 金鑰類型。
10. 按一下 **[建立]**。
結果, 含有服務帳戶私密金鑰的 JSON 檔案會自動下載到您的電腦。安全地儲存此檔案, 因為在您將 Google Workspace 組織新增到 Cyber Protection 服務時, 將需要這個檔案。

為您的 **Google Workspace** 帳戶授予新的專案存取權

1. 從 Google Cloud Platform 的導覽功能表中, 選取 **[IAM 與管理]** > **[服務帳戶]**。
2. 在清單中, 找出您建立的服務帳戶, 然後複製顯示在 **[OAuth 2.0 用戶端 ID]** 欄中的用戶端 ID。
3. 以超級系統管理員的身分, 登入 Google Admin 主控台 (admin.google.com)。
4. 從導覽功能表中, 選取 **[安全性]** > **[存取和資料控制]** > **[API 控制項]**。
5. 向下捲動 **[API 控制項]** 頁面, 然後在 **[全網域委派]** 底下, 按一下 **[管理全網域委派]**。
[全網域委派] 頁面隨即開啟。
6. 在 **[全網域委派]** 頁面上, 按一下 **[新增]**。
[新增用戶端編號] 視窗隨即開啟。
7. 在 **[用戶端編號]** 欄位中, 輸入您服務帳戶用戶端的用戶端編號。
8. 在 **[OAuth 範圍]** 欄位中, 新增下列範圍:
 - <https://mail.google.com>
 - <https://www.googleapis.com/auth/contacts>
 - <https://www.googleapis.com/auth/calendar>
 - <https://www.googleapis.com/auth/admin.directory.user.readonly>
 - <https://www.googleapis.com/auth/admin.directory.domain.readonly>
 - <https://www.googleapis.com/auth/drive>
 - <https://www.googleapis.com/auth/gmail.modify>
9. 按一下 **[授權]**。

結果，您的新 Google Cloud 專案可以存取您 Google Workspace 帳戶中的資料。若要備份資料，您需要將此專案連結到 Cyber Protection 服務。如需有關操作方式的詳細資訊，請參閱 "使用專用的個人 Google Cloud 專案新增 Google Workspace 組織" (第 294 頁)。

如果您需要撤銷 Google Workspace 帳戶對 Google Cloud 專案的存取權，以及對 Cyber Protection 服務的存取權，請刪除您專案使用的 API 用戶端。

撤銷對 Google Workspace 帳戶的存取權

1. 在 Google Admin 主控台 (admin.google.com) 中，以超級系統管理員的身分登入。
2. 從導覽功能表中，選取 **[安全性] > [存取和資料控制] > [API 控制項]**。
3. 向下捲動 **[API 控制項]** 頁面，然後在 **[全網域委派]** 底下，按一下 **[管理全網域委派]**。
[全網域委派] 頁面隨即開啟。
4. 在 **[全網域委派]** 頁面上，選取您專案所使用的 API 用戶端，然後按一下 **[刪除]**。
結果，您的 Google Cloud 專案和 Cyber Protection 服務將無法存取您的 Google Workspace 帳戶並備份其中的資料。

13.20.7 保護 Gmail 資料

哪些項目可以備份？

您可以備份 Gmail 使用者的信箱。信箱備份也包括行事曆和聯絡人資料。或者，您可以選擇備份共用行事曆。

備份期間會略過下列項目：

- **[生日]**、**[提醒]**、**[任務]** 行事曆
- 連接至行事曆活動的資料夾
- **[聯絡人]** 中的 **[目錄]** 資料夾

系統會因為 Google Calendar API 的限制，而略過下列行事曆項目：

- 預約時段
- 活動的會議欄位
- 行事曆設定 **[全天活動通知]**
- 行事曆設定 **[自動接受邀請]** (在行事曆中，用於房間或共用空間)

系統會因為 Google People API 的限制，而略過下列聯絡人項目：

- **[其他聯絡人]** 資料夾
- 聯絡人的外部設定檔 (**目錄設定檔**、**Google 設定檔**)
- 聯絡人欄位 **[歸檔為]**

可以復原哪些項目？

下列項目可以從信箱備份復原：

- 信箱
- 電子郵件資料夾 (根據 Google 詞彙,「標籤」。標籤在備份軟體中會顯示為資料夾,以便與其他資料顯示保持一致)。
- 電子郵件訊息
- 行事曆事件
- 連絡人

除非備份經過加密,否則您可以使用搜尋找出備份中的項目。不支援在加密的備份中進行搜尋。

復原信箱和信箱項目時,您可以選擇是否要覆寫目標位置中的項目。

限制

- 無法復原聯絡人相片
- **[不在辦公室]** 行事曆項目會因為 Google Calendar API 的限制而復原為一般行事曆活動

選取信箱

如下所述選擇信箱,然後視需要指定保護計劃的其他設定。

若要選擇 Gmail 信箱

1. 按一下 **[Google Workspace]**。
2. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務,請選取您要備份其使用者資料的組織。否則,請跳過此步驟。
3. 執行下列其中一項操作:
 - 若要備份所有使用者的信箱 (包括之後建立的信箱),展開 **[使用者]** 節點、選取 **[所有使用者]**,然後按一下 **[群組備份]**。
 - 若要備份個別的使用者信箱,展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要備份其信箱的使用者,然後按一下 **[備份]**。
4. 在保護計劃面板上:
 - 確認在 **[要備份的內容]** 中,選擇 **[Gmail]** 項目。
 - 如果您要備份與所選使用者共用的行事曆,請啟用 **[包括共用行事曆]** 開關。
 - 決定您是否需要**全文檢索**已備份的電子郵件訊息。若要存取此選項,按一下齒輪圖示 > **[備份選項]** > **[全文檢索]**。

全文檢索

此選項可定義雲端代理程式是否會編製電子郵件訊息內容的索引。

預設為:**[啟用]**。

如果啟用此選項,則會編製訊息內容,而且您可以依其內容搜尋訊息。否則,只能使用依主旨、寄件者、收件者或日期搜尋。

注意事項

不支援在加密的備份中進行搜尋。

編製索引程序不會影響備份效能，因為備份是由不同的軟體元件執行。編製第一次 (完整) 備份的索引可能需要一些時間，因此在備份完成到內容出現在搜尋結果中可能會有出現延遲。

索引會佔用 10-30% 信箱備份佔用的儲存空間。若要瞭解確切的值，按一下 **[備份儲存]** > **[雲端應用程式備份]**，然後檢視 **[索引大小]** 欄。您可能想要停用全文檢索以節省此空間。**[索引大小]** 欄中的值在下次備份之後將會減少幾 MB。這個最少中繼資料量是依主旨、寄件者、收件者或日期執行搜尋所需。

當您重新啟用全文檢索時，軟體就會編製保護計劃先前建立之所有備份的索引。這也需要一些時間。

復原信箱和信箱項目

復原信箱

1. 按一下 **[Google Workspace]**。
2. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，請選取您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原其信箱的使用者，然後按一下 **[復原]**。
如果使用者遭到刪除，請在 **[備份儲存]** 索引標籤的 **[雲端應用程式備份]** 區段中選取該使用者，然後按一下 **[顯示備份]**。
您可以按名稱搜尋使用者和群組。不支援萬用字元。
4. 選擇復原點

注意事項

若只要查看含有信箱的復原點，請在 **[依內容篩選]** 中選取 **[Gmail]**。

5. 按一下 **[復原]** > **[整個信箱]**。
6. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，按一下 **[Google Workspace 組織]** 可檢視、變更或指定目標組織。
預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須從可用的已登錄組織中選擇一個新的目標組織。
7. 在 **[復原至信箱]** 中，檢視、變更或指定目標信箱。
原始信箱預設為選取狀態。如果此信箱不存在或選取了非原始組織，則必須指定目標信箱。
您無法在復原期間建立新的目標信箱。若要將某個信箱復原到新的信箱，首先您需要在所需的 Google Workspace 組織中建立目標信箱，然後讓雲端代理程式同步變更。雲端代理程式每 24 小時會自動與 Google Workspace 同步一次。若要立即同步變更，請在服務主控台的 **[Google Workspace]** 頁面上選取組織，然後按一下 **[重新整理]**。
8. 按一下 **[開始復原]**。
9. 選取其中一個覆寫選項：
 - 覆寫現有項目
 - 不要覆寫現有項目
10. 按一下 **[繼續]** 可確認您的決定。

復原信箱項目

1. 按一下 **[Google Workspace]**。
2. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，請選取您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取其信箱原本包含您要復原之項目的使用者，然後按一下 **[復原]**。

如果使用者遭到刪除，請在 **[備份儲存]** 索引標籤的 **[雲端應用程式備份]** 區段中選取該使用者，然後按一下 **[顯示備份]**。

您可以按名稱搜尋使用者和群組。不支援萬用字元。

4. 選擇復原點

注意事項

若只要查看含有信箱的復原點，請在 **[依內容篩選]** 中選取 **[Gmail]**。

5. 按一下 **[復原] > [電子郵件訊息]**。
6. 瀏覽至所需的資料夾。如果備份未經過加密，您可以使用搜尋以取得所需項目的清單。
您可以使用下列搜尋選項。不支援萬用字元。
 - 電子郵件訊息：依主旨、寄件者、收件者、日期、附件名稱和訊息內容搜尋。如果在備份期間啟用了 **[全文檢索]** 選項，則只有最後兩個選項會產生結果。要搜尋之訊息片段的語言可以指定為其他參數。
 - 事件：依主題及日期搜尋。
 - 連絡人：依姓名、電子郵件地址和電話號碼搜尋。
7. 選擇您要復原的項目。若要能夠選擇資料夾，請按一下 **[復原資料夾]** 圖示：
此外，您可以執行下列任何一項作業：
 - 選取項目後，按一下 **[顯示內容]** 可檢視其內容，包括附件。若要下載附加檔案，請按一下其名稱。
 - 只有在備份未經加密、使用搜尋，並在搜尋結果中選取單一項目時：按一下 **[顯示版本]** 來選取要復原的項目版本。您可以選取早於或晚於所選復原點的任何備份版本。
8. 按一下 **[復原]**。
9. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，按一下 **[Google Workspace 組織]** 可檢視、變更或指定目標組織。
預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須從可用的已登錄組織中選擇一個新的目標組織。
10. 在 **[復原至信箱]** 中，檢視、變更或指定目標信箱。
原始信箱預設為選取狀態。如果此信箱不存在或選取了非原始組織，則必須指定目標信箱。
11. 在 **[路徑]** 中，檢視或變更目標信箱中的目標資料夾。原始資料夾根據預設已經選取。
12. 按一下 **[開始復原]**。
13. 選取其中一個覆寫選項：

- 覆寫現有項目
- 不要覆寫現有項目

14. 按一下 **[繼續]** 可確認您的決定。

13.20.8 保護 Google 雲端硬碟檔案

哪些項目可以備份？

您可以備份整個 Google 雲端硬碟或個別的檔案和資料夾。或者，您可以選擇備份與 Google 雲端硬碟使用者共用的檔案。

檔案會與其共用權限一起備份。

備份期間會略過下列項目：

- 共用檔案 (如果使用者對檔案有註解者或檢視者的存取權，而且檔案擁有者為註解者和檢視者停用了下載、列印和複製的選項)。
- **[電腦]** 資料夾 (由備份和同步用戶端所建立)

限制

- 在 Google 專用的檔案格式中，僅備份 Google 文件、Google 試算表、Google 簡報，以及 Google 繪圖。

可以復原哪些項目？

您可以復原整個 Google 雲端硬碟或已備份的任何檔案或資料夾。

除非備份經過加密，否則您可以使用搜尋找出備份中的項目。不支援在加密的備份中進行搜尋。

您可以選擇要復原共用權限，還是讓檔案繼承復原目標資料夾的權限。

限制

- 系統不會復原檔案中的註解。
- 檔案與資料夾的共用連結不會復原。
- 復原期間，無法變更共用檔案的唯讀 **[擁有者設定]** (**[防止編輯者變更存取權並加入新的人員]** 以及 **[為註解者和檢視者停用下載、列印和複製的選項]**)。
- 如果為此資料夾啟用 **[防止編輯者變更存取權並加入新的人員]** 選項，則在復原期間，無法變更共用資料夾的所有權。此設定會防止 Google Drive API 列出資料夾權限。系統會正確地復原資料夾中檔案的所有權。

選擇 Google 雲端硬碟檔案

如下所述選擇檔案，然後視需要指定保護計劃的其他設定。

若要選擇 Google 雲端硬碟檔案

1. 按一下 **[Google Workspace]**。
2. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務, 請選取您要備份其使用者資料的組織。否則, 請跳過此步驟。
3. 執行下列其中一項操作:
 - 若要備份所有使用者 (包括之後建立的使用者) 的檔案, 展開 **[使用者]** 節點、選取 **[所有使用者]**, 然後按一下 **[群組備份]**。
 - 若要備份個別使用者的檔案, 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要備份其檔案的使用者, 然後按一下 **[備份]**。
4. 在保護計劃面板上:
 - 確認在 **[要備份的內容]** 中, 選擇 **[Google 雲端硬碟]** 項目。
 - 在 **[要備份的項目]** 中, 執行下列其中一項操作:
 - 保留預設設定 **[全部]** (所有檔案)。
 - 新增檔案和資料夾的名稱或路徑來指定要備份的檔案和資料夾。
您可以使用萬用字元 (*、** 和 ?)。如需有關指定路徑和使用萬用字元的詳細資訊, 請參閱「[檔案篩選器](#)」。
 - 瀏覽來指定要備份的檔案和資料夾。
只有在建立單一使用者的保護計劃時, 才可以使用 **[瀏覽]** 連結。
 - **[選擇性]** 在 **[要備份的項目]** 中, 按一下 **[顯示排除項目]** 來指定要在備份期間略過的檔案和資料夾。
檔案排除項目會覆寫檔案選項, 亦即, 如果您在兩個欄位中指定相同的檔案, 將會在備份期間略過這個檔案。
 - 如果您要備份與所選使用者共用的檔案, 請啟用 **[包括共用檔案]** 開關。
 - 如果您要對選定備份的所有檔案啟用公證, 請啟用 **[公證]** 開關。如需公證的詳細資訊, 請參閱「[公證](#)」。

復原 Google 雲端硬碟和 Google 雲端硬碟檔案

復原整個 Google 雲端硬碟

1. 按一下 **[Google Workspace]**。
2. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務, 請選取您要復原其已備份資料的組織。否則, 請跳過此步驟。
3. 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原其 Google 雲端硬碟的使用者, 然後按一下 **[復原]**。
如果使用者遭到刪除, 請在 **[備份儲存]** 索引標籤的 **[雲端應用程式備份]** 區段中選取該使用者, 然後按一下 **[顯示備份]**。
您可以按名稱搜尋使用者。不支援萬用字元。
4. 選擇復原點

注意事項

若只要查看含有 Google 雲端硬碟檔案的復原點，請在 **[依內容篩選]** 中選取 **[Google 雲端硬碟]**。

5. 按一下 **[復原]** > **[整個雲端硬碟]**。
6. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，按一下 **[Google Workspace 組織]** 可檢視、變更或指定目標組織。
預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須從可用的已登錄組織中選擇一個新的目標組織。
7. 在 **[復原至磁碟機]** 中，檢視、變更或指定目標使用者或目標共用磁碟機。
預設會選取原始使用者。如果此使用者不存在或選取了非原始組織，則必須指定目標使用者或目標共用磁碟機。
如果備份中含有共用檔案，則檔案將會復原到目標磁碟機的 root 資料夾。
8. 選取是否要復原檔案的共用權限。
9. 按一下 **[開始復原]**。
10. 選取其中一個覆寫選項：
 - 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
11. 按一下 **[繼續]** 可確認您的決定。

復原 Google 雲端硬碟檔案

1. 按一下 **[Google Workspace]**。
2. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，請選取您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 展開 **[使用者]** 節點、選取 **[所有使用者]**、選取您要復原其 Google 雲端硬碟檔案的使用者，然後按一下 **[復原]**。
如果使用者遭到刪除，請在 **[備份儲存]** 索引標籤的 **[雲端應用程式備份]** 區段中選取該使用者，然後按一下 **[顯示備份]**。
您可以按名稱搜尋使用者。不支援萬用字元。
4. 選擇復原點

注意事項

若只要查看含有 Google 雲端硬碟檔案的復原點，請在 **[依內容篩選]** 中選取 **[Google 雲端硬碟]**。

5. 按一下 **[復原]** > **[檔案/資料夾]**。
6. 瀏覽至所需的資料夾，或使用搜尋以取得所需檔案和資料夾的清單。
如果備份經過加密，則無法使用搜尋。
7. 選擇您要復原的檔案。

如果備份未經加密而且您選擇單一檔案，您可以按一下 **[顯示版本]** 來選取要復原的檔案版本。您可以選取早於或晚於所選復原點的任何備份版本。

8. 如果您要下載檔案，請選擇該檔案，按一下 **[下載]**，選擇儲存資料的位置，然後按一下 **[儲存]**。否則，請跳過此步驟。
9. 按一下 **[復原]**。
10. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，按一下 **[Google Workspace 組織]** 可檢視、變更或指定目標組織。
預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須從可用的已登錄組織中選擇一個新的目標組織。
11. 在 **[復原至磁碟機]** 中，檢視、變更或指定目標使用者或目標共用磁碟機。
預設會選取原始使用者。如果此使用者不存在或選取了非原始組織，則必須指定目標使用者或目標共用磁碟機。
12. 在 **[路徑]** 中，檢視或變更目標使用者 Google 雲端硬碟或目標共用磁碟機中的目標資料夾。預設會選取原始位置。
13. 選取是否要復原檔案的共用權限。
14. 按一下 **[開始復原]**。
15. 選擇其中一個檔案覆寫選項：
 - 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
16. 按一下 **[繼續]** 可確認您的決定。

13.20.9 保護共用磁碟機檔案

哪些項目可以備份？

您可以備份整個共用磁碟機或個別的檔案和資料夾。

檔案會與其共用權限一起備份。

限制

- 由於 Google Drive API 的限制，無法備份不含成員的共用磁碟機。
- 在 Google 專用的檔案格式中，僅備份 Google 文件、Google 試算表、Google 簡報，以及 Google 繪圖。

可以復原哪些項目？

您可以復原整個共用磁碟機或已備份的任何檔案或資料夾。

除非備份經過加密，否則您可以使用搜尋找出備份中的項目。不支援在加密的備份中進行搜尋。

您可以選擇要復原共用權限，還是讓檔案繼承復原目標資料夾的權限。

系統不會復原下列項目：

- 如果目標共用磁碟機中停用了在組織外部共用，則不會復原與組織外部使用者共用之檔案的共用權限。
- 如果目標共用磁碟機中停用了 **[與非成員共用]**，則不會復原與非目標共用磁碟機成員的使用者共用之檔案的共用權限。

限制

- 系統不會復原檔案中的註解。
- 檔案與資料夾的共用連結不會復原。

選擇共用磁碟機檔案

如下所述選擇檔案，然後[視需要](#)指定保護計劃的其他設定。

若要選擇共用磁碟機檔案

1. 按一下 **[Google Workspace]**。
2. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，請選取您要備份其使用者資料的組織。否則，請跳過此步驟。
3. 執行下列其中一項操作：
 - 若要備份所有共用磁碟機 (包括之後建立的共用磁碟機) 的檔案，展開 **[共用磁碟機]** 節點、選取 **[所有共用磁碟機]**，然後按一下 **[群組備份]**。
 - 若要備份個別共用磁碟機的檔案，展開 **[共用磁碟機]** 節點、選取 **[所有共用磁碟機]**、選取您要備份的共用磁碟機，然後按一下 **[備份]**。
4. 在保護計劃面板上：
 - 在 **[要備份的項目]** 中，執行下列其中一項操作：
 - 保留預設設定 **[全部]** (所有檔案)。
 - 新增檔案和資料夾的名稱或路徑來指定要備份的檔案和資料夾。
您可以使用萬用字元 (*、** 和 ?)。如需有關指定路徑和使用萬用字元的詳細資訊，請參閱 [「檔案篩選器」](#)。
 - 瀏覽來指定要備份的檔案和資料夾。
只有在建立單一共用磁碟機的保護計劃時，才可以使用 **[瀏覽]** 連結。
 - [選擇性] 在 **[要備份的項目]** 中，按一下 **[顯示排除項目]** 來指定要在備份期間略過的檔案和資料夾。
檔案排除項目會覆寫檔案選項，亦即，如果您在兩個欄位中指定相同的檔案，將會在備份期間略過這個檔案。
 - 如果您要對選定備份的所有檔案啟用公證，請啟用 **[公證]** 開關。如需公證的詳細資訊，請參閱 [「公證」](#)。

復原共用磁碟機和共用磁碟機檔案

復原整個共用磁碟機

1. 按一下 **[Google Workspace]**。
2. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，請選取您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 展開 **[共用磁碟機]** 節點、選取 **[所有共用磁碟機]**、選取您要復原的共用磁碟機，然後按一下 **[復原]**。
如果共用磁碟機遭到刪除，請在 **[備份儲存]** 索引標籤的 **[雲端應用程式備份]** 區段中選取該共用磁碟機，然後按一下 **[顯示備份]**。
您可以按名稱搜尋共用磁碟機。不支援萬用字元。
4. 選擇復原點
5. 按一下 **[復原]** > **[整個共用磁碟機]**。
6. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，按一下 **[Google Workspace 組織]** 可檢視、變更或指定目標組織。
預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須從可用的已登錄組織中選擇一個新的目標組織。
7. 在 **[復原至磁碟機]** 中，檢視、變更或指定目標共用磁碟機或目標使用者。如果您指定某個使用者，資料將會復原到此使用者的 Google 雲端硬碟。
預設會選取原始共用磁碟機。如果此共用磁碟機不存在或選取了非原始組織，則必須指定目標共用磁碟機或目標使用者。
8. 選取是否要復原檔案的共用權限。
9. 按一下 **[開始復原]**。
10. 選取其中一個覆寫選項：
 - 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
11. 按一下 **[繼續]** 可確認您的決定。

復原共用磁碟機檔案

1. 按一下 **[Google Workspace]**。
2. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，請選取您要復原其已備份資料的組織。否則，請跳過此步驟。
3. 展開 **[共用磁碟機]** 節點、選取 **[所有共用磁碟機]**、選取包含您要復原之檔案的共用磁碟機，然後按一下 **[復原]**。
如果共用磁碟機遭到刪除，請在 **[備份儲存]** 索引標籤的 **[雲端應用程式備份]** 區段中選取該共用磁碟機，然後按一下 **[顯示備份]**。
您可以按名稱搜尋共用磁碟機。不支援萬用字元。
4. 選擇復原點

5. 按一下 **[復原]** > **[檔案/資料夾]**。
6. 瀏覽至所需的資料夾，或使用搜尋以取得所需檔案和資料夾的清單。
如果備份經過加密，則無法使用搜尋。
7. 選擇您要復原的檔案。
如果備份未經加密而且您選擇單一檔案，您可以按一下 **[顯示版本]** 來選取要復原的檔案版本。
您可以選取早於或晚於所選復原點的任何備份版本。
8. 如果您要下載檔案，請選擇該檔案，按一下 **[下載]**，選擇儲存資料的位置，然後按一下 **[儲存]**。
否則，請跳過此步驟。
9. 按一下 **[復原]**。
10. 如果多個 Google Workspace 組織新增到 Cyber Protection 服務，按一下 **[Google Workspace 組織]** 可檢視、變更或指定目標組織。
預設會選取原始組織。如果 Cyber Protection 服務中不再登錄此組織，您必須從可用的已登錄組織中選擇一個新的目標組織。
11. 在 **[復原至磁碟機]** 中，檢視、變更或指定目標共用磁碟機或目標使用者。如果您指定某個使用者，資料將會復原到此使用者的 Google 雲端硬碟。
預設會選取原始共用磁碟機。如果此共用磁碟機不存在或選取了非原始組織，則必須指定目標共用磁碟機或目標使用者。
12. 在 **[路徑]** 中，檢視或變更目標共用磁碟機或目標使用者 Google 雲端硬碟中的目標資料夾。預設會選取原始位置。
13. 選取是否要復原檔案的共用權限。
14. 按一下 **[開始復原]**。
15. 選擇其中一個檔案覆寫選項：
 - 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
16. 按一下 **[繼續]** 可確認您的決定。

13.20.10 公證

公證讓您證明檔案在備份後即是真實和未變更的。建議您在備份法律檔案或需要證明真實性的任何其他檔案時啟用公證。

公證僅適用於 Google 雲端硬碟檔案和 Google Workspace 共用磁碟機檔案的備份。

如何使用公證

若要對選定備份的所有檔案啟用公證，建立保護計劃時，請啟用 **[公證]** 開關。

在設定復原時，公證檔將標記有特殊圖示，並且您可以 [\[驗證檔案真實性\]](#)。

運作原理

在備份過程中，代理程式會計算備份檔案的雜湊代碼，組建雜湊樹狀結構 (基於資料夾結構)，儲存備份中的樹狀結構，然後將雜湊樹狀結構根部發送給公證服務。公證服務將雜湊樹狀結構根部儲存

在 Ethereum 區塊鏈資料庫中，以確保此值不會變更。

在驗證檔案真實性時，代理程式會計算檔案雜湊，然後將其與儲存在備份內雜湊樹狀結構中的雜湊相比較。若這些雜湊不相符，則檔案被視為不真實。否則，由雜湊樹狀結構保證檔案的真實性。

若要驗證雜湊樹狀結構自身未受損，代理程式會將雜湊樹狀結構根部發送給公證服務。公證服務將其與儲存在區塊鏈資料庫中的雜湊相比較。若雜湊相符，則所選檔案保證為真實的。否則，軟體會顯示一則訊息，指示檔案不真實。

向 Notary Service 驗證檔案真實性

如果備份期間啟用公證，則可驗證備份檔案的真實性。

要驗證檔案的真實性

1. 執行下列其中一項操作：

- 若要驗證 Google 雲端硬碟檔案的真實性，請選擇檔案，如「[復原 Google 雲端硬碟檔案](#)」一節的步驟 1-7 所述。
- 若要驗證 Google Workspace 共用磁碟機檔案的真實性，請選擇檔案，如「[復原共用磁碟機檔案](#)」一節的步驟 1-7 所述。

2. 確保所選檔案標記有下列圖示：。這表示檔案已公證。

3. 執行下列其中一項操作：

- 按一下 **驗證**。
軟體會檢查檔案真實性並顯示結果。
- 按一下 **取得憑證**。
確認檔案公證的憑證會在 Web 瀏覽器視窗中開啟。該視窗還包含了容許您手動驗證檔案真實性的說明。

13.21 保護 Oracle 資料庫

在另一個文件中說明了對 Oracle 資料庫的保護：https://dl.managed-protection.com/u/pdf/OracleBackup_whitepaper.pdf

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

13.22 保護 SAP HANA

SAP HANA 的保護詳述於可在 https://dl.managed-protection.com/u/pdf/SAP%20HANA_backup_whitepaper.pdf 取得的另一份文件

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

13.23 保護 MySQL 和 MariaDB 資料

您可以使用應用程式感知備份來保護 MySQL 或 MariaDB 資料。它會收集應用程式中繼資料，並允許在執行個體、資料庫或資料表層級上的細微復原。

注意事項

MySQL 或 MariaDB 資料的應用程式感知備份可在進階備份套件取得。

若要使用應用程式感知備份來保護執行 MySQL 或 MariaDB 執行個體的實體或虛擬機器，您必須在此電腦上安裝 MySQL/MariaDB 用代理程式。MySQL/MariaDB 用代理程式是與 Linux 用代理程式 (64 位元) 一起搭售。

若要下載 Linux 用代理程式 (64 位元) 安裝檔案

1. 登入 Cyber Protection 服務主控台。
2. 按一下右上角的帳戶圖示，然後選擇 **[下載]**。
3. 按一下 **[Linux 用代理程式 (64 位元)]**。

安裝檔案會下載到您的電腦中。若要安裝代理程式，請依照 "在 Linux 中安裝 Cyber Protection 代理程式" (第 56 頁) 或 "Linux 中的自動安裝或解除安裝" (第 67 頁) 中的描述繼續進行。確認您選擇 MySQL/MariaDB 用代理程式，這是一個選擇性元件。

若要將資料庫和資料表復原至執行中的執行個體，則 MySQL/MariaDB 用代理程式需要臨時存放區才能運作。預設會使用 /tmp 目錄。您可以透過設定 ACRONIS_MYSQL_RESTORE_DIR 環境變數來變更此目錄。

限制

- 不支援 MySQL 或 MariaDB 叢集。
- 不支援 Docker 容器中執行的 MySQL 或 MariaDB 執行個體。
- 不支援在使用 BTRFS 檔案系統之作業系統上執行的 MySQL 或 MariaDB 執行個體。
- 系統資料庫 (sys、mysql、information-schema 和 performance_schema) 和不包含任何資料表的資料庫無法復原至執行中的執行個體。不過，當復原整個執行個體時，這些資料庫可以復原為檔案。
- 復原僅支援與備份執行個體相同版本或更新版本的目標執行個體，並有以下限制：
 - 不支援從 MySQL 5.x 執行個體復原至 MySQL 8.x 執行個體。
 - 只有透過將整個執行個體復原為檔案的方式，才支援復原至更新的 MySQL 5.x 版本 (包括次要版本)。在嘗試復原之前，參考官方 MySQL 升級指南以瞭解目標版本，例如 [MySQL 5.7 升級指南](#)。
- 不支援從儲存在 Secure Zone 上的備份復原。
- 在已安裝 AppArmor 的電腦上執行的 MySQL/MariaDB 用代理程式無法復原資料庫和資料表。您仍然可將執行個體復原為檔案，或整個電腦。
- 不支援復原至使用符號連結設定的目標資料庫。您可將備份資料庫復原為新資料庫，方法是變更其名稱。

已知問題

如果在從密碼保護的 Samba 共用復原資料時碰到問題，請登出服務主控台，然後再登入回去。選擇想要的復原點，然後按一下 **[MySQL/MariaDB 資料庫]**。請勿按下 **[整部電腦]** 或 **[檔案/資料夾]**。

13.23.1 設定應用程式感知備份

必要條件

- 所選電腦上至少必須執行一個 MySQL 或 MariaDB 執行個體。
- 在執行 MySQL 或 MariaDB 執行個體的電腦上，保護代理程式必須在 root 使用者下啟動。
- 只有在保護計劃選擇 **[整部電腦]** 作為備份來源時，才可使用應用程式感知備份。
- 保護計劃中務必停用 **[逐一磁區]** 備份選項。否則，無法復原應用程式資料。

若要設定應用程式感知備份

1. 在 Cyber Protection 服務主控台中，選擇一或多部執行 MySQL 或 MariaDB 執行個體的電腦。
每部電腦上可以有一或多個執行個體。
2. 在啟用備份模組的情況下，建立一個保護計劃。
3. 在 **[要備份的內容]** 中選擇 **[整部電腦]**。
4. 按一下 **[應用程式備份]**，然後啟用 **[MySQL/MariaDB Server]** 旁邊的開關。
5. 選擇如何指定 MySQL 或 MariaDB 執行個體：
 - **對於所有工作負載**
如果您在多部伺服器上執行具有相同設定的執行個體，請使用此選項。所有執行個體都將使用相同的連線參數和存取認證。
 - **針對特定工作負載**
使用此選項來指定每個執行個體的連線參數和存取認證。
6. 按一下 **[新增執行個體]** 以設定連線參數和存取認證。
 - a. 選擇連線類型，然後指定下列各項：
 - **[針對 TCP 通訊端]** IP 位址和連接埠。
 - **[針對 Unix 通訊端]** 通訊端路徑。
 - b. 指定具備下列執行個體權限的使用者帳戶認證：
 - FLUSH_TABLES 或 RELOAD，針對所有資料庫和資料表 (*.*)
 - SELECT for the information_schema.tables
 - c. 按一下 **[確定]**。
7. 按一下 **[完成]**。

13.23.2 從應用程式感知備份復原資料

您可以從應用程式感知備份復原 MySQL 或 MariaDB 執行個體、資料庫和資料表。您還可復原執行執行個體的整個伺服器，或從此伺服器復原檔案和資料夾。

下表摘要所有復原選項。

復原內容	復原為	復原至
MySQL Server MariaDB Server	整部電腦	已安裝 Linux 用代理程式的電腦*
MySQL Server MariaDB Server	檔案或資料夾	已安裝 Linux 用代理程式的電腦*
執行個體	檔案	已安裝 MySQL/MariaDB 用代理程式的電腦*
資料庫	相同資料庫 新資料庫	已安裝 MySQL/MariaDB 用代理程式的電腦* • 原始執行個體 • 其他執行個體 • 原始資料庫 • 新資料庫
Table	相同資料表 新資料表	已安裝 MySQL/MariaDB 用代理程式的電腦* • 原始執行個體 • 其他執行個體 • 原始資料庫 • 原始資料表 • 新資料表

* 從備份觀點來看，內部具有代理程式的虛擬機器會被視為實體機器。

復原整個伺服器

若要瞭解如何復原正在執行 MySQL 或 MariaDB 執行個體的整個伺服器，請參閱 "復原電腦" (第 212 頁)。

復原執行個體

您可以從應用程式感知備份，將 MySQL 或 MariaDB 執行個體復原為檔案。

若要復原執行個體

1. 在 Cyber Protection 服務主控台中，選擇原本存放所要復原之資料的電腦。
2. 按一下 **[復原]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。

如果電腦處於離線狀態，復原點就不會顯示。執行下列其中一項操作：

- 如果備份位置是雲端或共用儲存 (即可被其他代理程式存取)，按一下 **[選擇電腦]**，選擇有 MySQL/MariaDB 用代理程式的線上電腦，然後選擇復原點。
- 在 **[備份儲存]** 索引標籤上選擇復原點。

依照上述動作任一而選擇瀏覽的電腦，將成為復原的目標電腦。

4. 按一下 **[復原]** > **[MySQL/MariaDB 資料庫]**。
5. 選擇您要復原的執行個體，然後按一下 **[復原為檔案]**。
6. 在 **[路徑]** 底下，選擇將要復原檔案的目標目錄。
7. 按一下 **[開始復原]**。

復原資料庫

您可以從應用程式感知備份，將資料庫復原至執行中的 MySQL 或 MariaDB 執行個體。

1. 在 Cyber Protection 服務主控台中，選擇原本存放所要復原之資料的電腦。
2. 按一下 **[復原]**。
3. 選擇復原點請注意，復原點是依照位置進行篩選。
如果電腦處於離線狀態，復原點就不會顯示。執行下列其中一項操作：
 - 如果備份位置是雲端或共用儲存(即可被其他代理程式存取)，按一下 **[選擇電腦]**，選擇有 MySQL/MariaDB 用代理程式的線上電腦，然後選擇復原點。
 - 在 **[備份儲存]** 索引標籤上選擇復原點。依照上述動作任一而選擇瀏覽的電腦，將成為復原的目標電腦。
4. 按一下 **[復原]** > **[MySQL/MariaDB 資料庫]**。
5. 按一下所需的執行個體名稱，以向下鑽研至其資料庫。
6. 請選擇您要復原的一或多個資料庫。
7. 按一下 **[復原]**。
8. 按一下 **[目標 MySQL/MariaDB 執行個體]** 以指定目標執行個體的連線參數和存取認證。
 - 驗證您要復原資料的目標執行個體。預設會選擇原始執行個體。
 - 指定可存取目標執行個體的使用者帳戶認證。此使用者帳戶必須具備為所有資料庫和資料表 (*.*) 指派的下列權限：
 - INSERT
 - CREATE
 - DROP
 - LOCK_TABLES
 - ALTER
 - SELECT
 - 按一下 **[確定]**。
9. 驗證目標資料庫。
預設會選擇原始資料庫。
若要將資料庫復原為新資料庫，請按一下目標資料庫名稱，然後加以變更。此動作僅適用於復原單一資料庫時。
10. 在 **[覆寫現有的資料庫]** 底下，選擇覆寫模式。
依預設，會啟用覆寫，而且備份資料庫會取代名稱相同的目標資料庫。
如果停用覆寫，在復原作業期間會略過備份資料庫，而且不會取代名稱相同的目標資料庫。
11. 按一下 **[開始復原]**。

復原資料表

您可以從應用程式感知備份，將資料表復原至執行中的 MySQL 或 MariaDB 執行個體。

1. 在 Cyber Protection 服務主控台中，選擇原本存放所要復原之資料的電腦。

2. 按一下 **[復原]**。

3. 選擇復原點請注意，復原點是依照位置進行篩選。

如果電腦處於離線狀態，復原點就不會顯示。執行下列其中一項操作：

- 如果備份位置是雲端或共用儲存 (即可被其他代理程式存取)，按一下 **[選擇電腦]**，選擇有 MySQL/MariaDB 用代理程式的線上電腦，然後選擇復原點。
- 在 **[備份儲存]** 索引標籤上選擇復原點。

依照上述動作任一而選擇瀏覽的電腦，將成為復原的目標電腦。

4. 按一下 **[復原] > [MySQL/MariaDB 資料庫]**。

5. 按一下所需的執行個體名稱，以向下鑽研至其資料庫。

6. 按一下所需的資料庫名稱，以向下鑽研至其資料表。

7. 請選擇您要復原的一或多個資料表。

8. 按一下 **[復原]**。

9. 按一下 **[目標 MySQL/MariaDB 執行個體]** 以指定目標執行個體的連線參數和存取認證。

- 驗證您要復原資料的目標執行個體。預設會選擇原始執行個體。
- 指定可存取目標執行個體的使用者帳戶認證。此使用者帳戶必須具備為所有資料庫和資料表 (*.*) 指派的下列權限：
 - INSERT
 - CREATE
 - DROP
 - LOCK_TABLES
 - ALTER
 - SELECT
- 按一下 **[確定]**。

10. 驗證目標資料表。

預設會選擇原始資料表。

若要將資料表復原為新資料表，請按一下目標資料表名稱，然後加以變更。此動作僅適用於復原單一資料表時。

11. 在 **[覆寫現有的資料表]** 下方，選擇覆寫模式。

依預設，會啟用覆寫，而且備份資料表會取代名稱相同的目標資料表。

如果停用覆寫，在復原作業期間會略過備份資料表，而且不會取代名稱相同的目標資料表。

12. 按一下 **[開始復原]**。

13.24 保護網站和託管伺服器

13.24.1 保護網站

未經授權的存取或惡意程式碼攻擊，可能導致網站損毀。如果希望在發生損毀狀況時輕鬆還原其健康狀態，請備份您的網站。

備份網站需要什麼？

網站必須能透過 SFTP 或 SSH 通訊協定存取。您不需要安裝代理程式，只要按本節稍後所述新增網站即可。

哪些項目可以備份？

您可備份下列項目：

- **網站內容檔案**
您針對 SFTP 或 SSH 連線所指定的帳戶可存取的所有檔案。
- **MySQL 伺服器上已連結的資料庫 (如果有的話)。**
您指定的 MySQL 帳戶可存取的所有資料庫。

如果您的網站採用資料庫，我們建議您備份檔案和資料庫，以便將它們復原為一致的狀態。

限制

- 網站備份可用的唯一備份位置是雲端儲存空間。
- 您可以將數個保護計劃套用至一個網站，但其中只有一個保護計劃可以依排程執行。其他計劃必須手動啟動。
- 唯一可用的備份選項為 [\[備份檔案名稱\]](#)。
- 網站保護計劃不會顯示在 **[管理]>[保護計劃]** 索引標籤上。

備份網站

若要新增網站

1. 按一下 **[裝置]>[新增]**。
2. 按一下**[網站]**。
3. 為網站設定下列存取設定：
 - 在 **[網站名稱]** 中，建立及輸入網站名稱。此名稱將顯示在服務主控台中。
 - 在 **[主機]** 中，指定要用來透過 SFTP 或 SSH 存取網站的主機名稱或 IP 位址。例如，`my.server.com` 或 `10.250.100.100`。
 - 在 **[連接埠]**，指定連接埠號碼。
 - 在 **[使用者名稱]** 和 **[密碼]** 中，指定可用來透過 SFTP 或 SSH 存取網站的帳戶的認證。

重要事項

只會備份指定帳戶可存取的檔案。

除了密碼，也可以指定私密 SSH 金鑰。若要這麼做，請選擇 **[使用 SSH 私密金鑰而非密碼]** 核取方塊，然後指定金鑰。

4. 按 **[下一步]**。
5. 如果您的網站使用 MySQL 資料庫，請設定資料庫的存取設定。否則，請按一下 **[略過]**。
 - a. 在 **[連線類型]** 中，選則如何從雲端存取資料庫：
 - **[透過 SSH 來源主機]**— 將透過步驟 3 終止定的主機存取資料庫。
 - **[直接連線]**— 直接存取資料庫。僅當可從網際網路存取資料庫時，才選擇此設定。
 - b. 在 **[主機]** 中，指定執行 MySQL 伺服器的主機的名稱或 IP 位址。
 - c. 在 **[連接埠]** 中，指定與伺服器的 TCP/IP 連線的連接埠號碼。預設的連接埠號碼是 3306。
 - d. 在 **[使用者名稱]** 及 **[密碼]** 中指定 MySQL 帳戶認證。

重要事項

只會備份指定帳戶可存取的資料庫。

- e. 按一下 **[建立]**。

此網站將會出現在服務主控台的 **[裝置] > [網站]** 底下。

若要變更連線設定

1. 在 **[裝置] > [網站]** 下選擇網站。
2. 按一下 **[詳細資料]**。
3. 按一下網站或資料庫連線設定旁的鉛筆圖示。
4. 進行必要的變更，然後按一下 **[儲存]**。

建立網站的保護計劃

1. 在 **[裝置] > [網站]** 下選擇一個或數個網站。
2. 按一下 **[保護]**。
3. **[選擇性]** 啟用資料庫備份。

如果選擇數個網站，則預設會停用資料庫備份。
4. **[選擇性]** 變更 **保留規則**。
5. **[選擇性]** 啟用 **備份的加密**。
6. **[選擇性]** 按一下齒輪圖示以編輯 **[備份檔案名稱]** 選項。這在兩個情況下是可行的：
 - 如果您稍早備份此網站，而且想要繼續現有的備份順序
 - 如果您想要在 **[備份儲存]** 索引標籤上看到自訂名稱
7. 按一下 **[套用]**。

您可以按照與電腦相同的方式，編輯、撤消和刪除網站的保護計劃。這些作業將詳述於「保護計劃相關操作」中。

復原網站

若要復原網站

1. 執行下列其中一項操作：
 - 在 **[裝置]>[網站]** 下選擇您要復原的網站，然後按一下 **[復原]**。
您可以按名稱搜尋網站。不支援萬用字元。
 - 如果網站遭到刪除，請在 **[備份儲存]** 索引標籤的 **[雲端應用程式備份]** 區段中選取該網站，然後按一下 **[顯示備份]**。
若要復原已刪除的網站，您必須將目標網站當做裝置新增。
2. 選擇復原點。
3. 按一下 **[復原]**，然後選擇您要復原哪些內容：**[整個網站]**、**[資料庫]** (如果有的話)，或 **[檔案/資料夾]**。
為了確保您的網站處於一致狀態，我們建議復原檔案和資料庫，順序不限。
4. 視您的選擇而定，請遵照以下所述的其中一個程序。

若要復原整個網站

1. 在 **[復原到網站]** 中，檢視或變更目標網站。
預設會選取原始網站。如果原始網站不存在，您必須選取目標網站。
2. 選取是否要復原已復原項目的共用權限。
3. 按一下 **[開始復原]**，然後確認動作。

若要復原資料庫

1. 請選擇您要復原的資料庫。
2. 如果您要將資料庫當做檔案下載，請按一下 **[下載]**，選擇儲存檔案的位置，然後按一下 **[儲存]**。
否則，請跳過此步驟。
3. 按一下 **[復原]**。
4. 在 **[復原到網站]** 中，檢視或變更目標網站。
預設會選取原始網站。如果原始網站不存在，您必須選取目標網站。
5. 按一下 **[開始復原]**，然後確認動作。

若要復原網站檔案/資料夾

1. 選擇您要復原的檔案/資料夾。
2. 如果您要儲存檔案，請按一下 **[下載]**，選擇儲存檔案的位置，然後按一下 **[儲存]**。否則，請跳過此步驟。
3. 按一下 **[復原]**。
4. 在 **[復原到網站]** 中，檢視或變更目標網站。
預設會選取原始網站。如果原始網站不存在，您必須選取目標網站。
5. 選取是否要復原已復原項目的共用權限。
6. 按一下 **[開始復原]**，然後確認動作。

13.24.2 保護 Web 託管伺服器

您可以保護執行 Plesk、cPanel、DirectAdmin、VirtualMin 或 ISPManager 控制面板的 Linux 型 Web 託管伺服器。執行其他廠商的 Web 託管控制面板的伺服器會當作一般工作負載受到保護。

配額

執行 Plesk、cPanel、DirectAdmin、VirtualMin 或 ISPManager 控制面板的伺服器會被視為 Web 託管伺服器。每部備份的 Web 託管伺服器都會耗用 **Web 託管伺服器** 配額。如果此配額遭到停用，或超過此配額的超額，將會按如下方式指派配額，或者備份將會失敗：

- 如果是實體伺服器，將會使用 **伺服器** 配額。如果此配額遭到停用，或超過此配額的超額，備份將會失敗。
- 如果是虛擬伺服器，將會使用 **虛擬機器** 配額。如果此配額遭到停用，或超過此配額的超額，備份將會失敗。

Plesk 和 cPanel 的整合

使用 Plesk 或 cPanel 平台的 Web 託管系統管理員可以將這些平台與 Cyber Protection 服務整合在一起。

整合可讓系統管理員執行下列操作：

- 使用磁碟層級備份，將整部 Plesk 或 cPanel 伺服器備份到雲端儲存空間
- 復原整部伺服器，包括所有網站
- 若是 Plesk：針對網站、個別檔案、信箱或資料庫，執行細微復原
- 若是 cPanel：針對網站、個別檔案、信箱、郵件篩選器、郵件轉寄站、資料庫和帳戶，執行細微復原
- 為 Plesk 和 cPanel 客戶啟用自助復原

使用 Cyber Protection 服務擴充功能執行整合。如果您需要適用於 Plesk 或 cPanel 的擴充功能，請聯絡 Cyber Protection 服務提供者。

支援的 Plesk 和 cPanel 版本

- Plesk for Linux 17.0 和更新版本
- PHP 版本為 5.6 和更新版本的任何 cPanel 版本

13.25 虛擬機器的特殊作業

13.25.1 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

- 必須至少有一個 VMware 用代理程式或 Hyper-V 用代理程式在 Cyber Protection 服務中註冊。
- 備份可以儲存在網路資料夾或已安裝 VMware 用代理程式或 Hyper-V 用代理程式的電腦本機資料夾中。如果您選擇網路資料夾, 則必須可以從該電腦存取。虛擬機器亦可從儲存在雲端儲存的備份執行, 但速度較慢, 因為這項作業需要從備份進行密集隨機存取讀取。
- 備份必須包含足以讓作業系統啟動的整個電腦或是所有磁碟區。
- 實體機器和虛擬機器的備份均可以使用。Virtuozzo 容器的備份不可使用。
- 含有 Linux 邏輯磁碟區 (LVM) 的備份必須透過 VMware 用代理程式或 Hyper-V 用代理程式建立。虛擬機器與原始電腦 (ESXi 或 Hyper-V) 的類型必須相同。

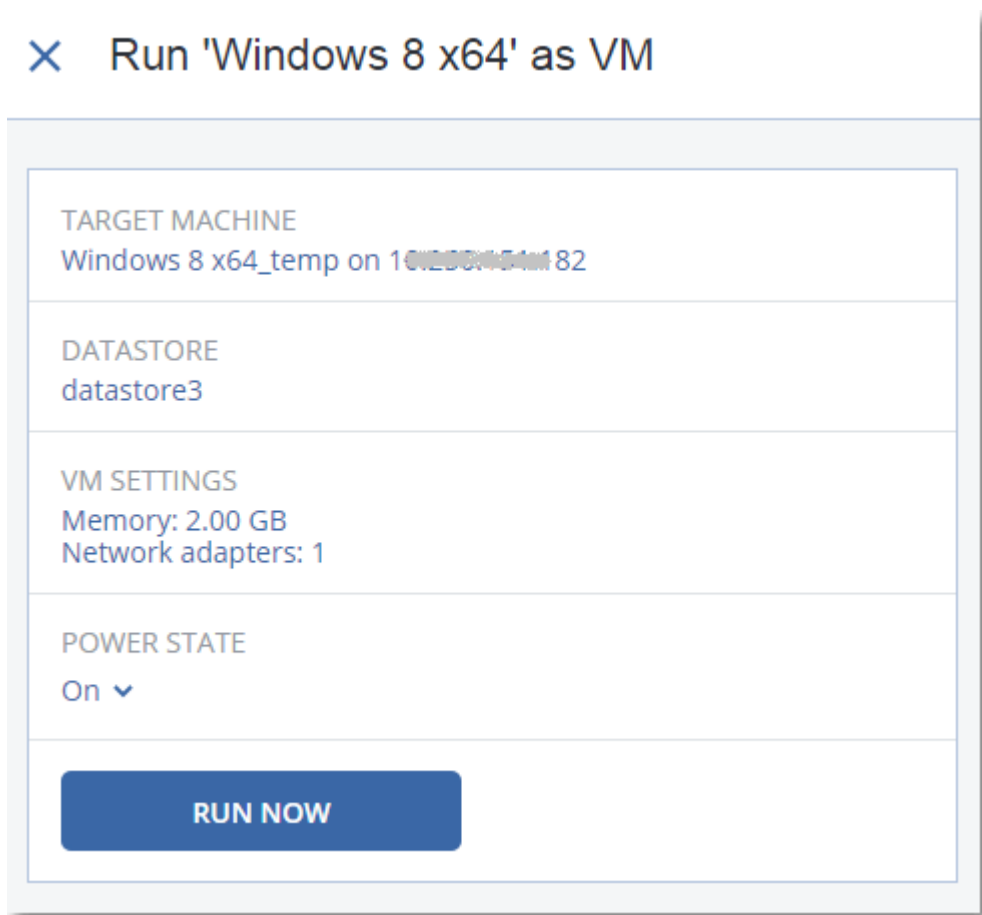
執行電腦

1. 執行下列其中一項操作:

- 選擇已備份的電腦, 按一下**復原**, 然後選擇復原點。
- 在 [\[備份儲存\] 索引標籤](#)上選擇復原點。

2. 按一下 **[以 VM 的身分執行]**。

軟體會自動選擇主機與其他所需的參數。



3. [選擇性] 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**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。

13.25.2 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

- 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。
- [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。
- 執行計劃一次。
複本已建立在原始的 ESXi 上。
- 匯出虛擬機器 (或複本) 檔案至外接硬碟。
 - 連結外接硬碟至執行 vSphere 用戶端的電腦。
 - 連結 vSphere 用戶端至原始的 vCenter\ESXi。
 - 選擇詳細目錄中最新建立的複本。

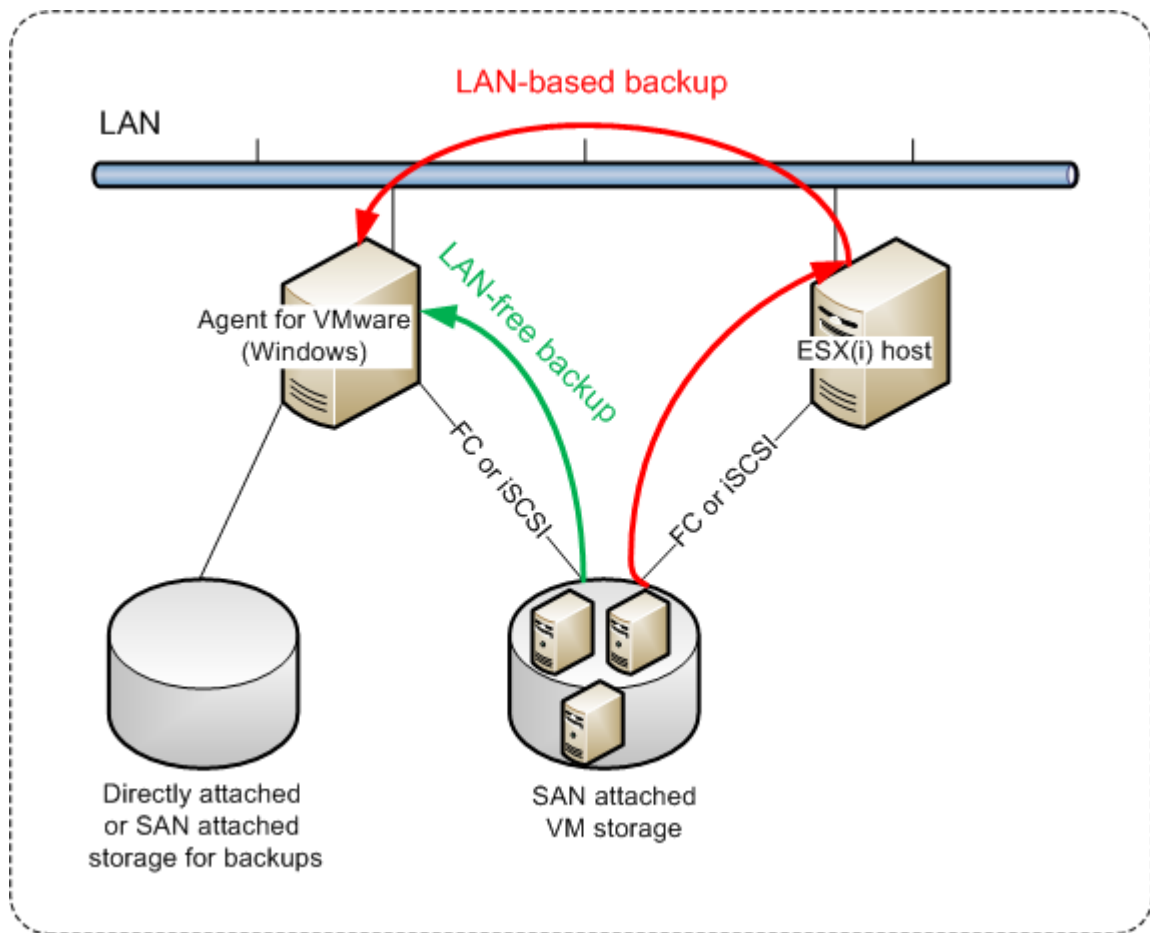
- d. 按一下 **[檔案] > [匯出] > [匯出 OVF 範本]**。
 - e. 在 **[目錄]** 中指定外接式硬碟上的資料夾。
 - f. 按一下 **[確定]**。
5. 移轉硬碟至遠端位置。
6. 匯入複本至目標 ESXi。
 - a. 連結外接硬碟至執行 vSphere 用戶端的電腦。
 - b. 連結 vSphere 用戶端至目標 vCenter\ESXi。
 - c. 按一下 **[檔案] > [部署 OVF 範本]**。
 - d. 在 **[從檔案或 URL 部署]** 中, 指定您在步驟 4 匯出的範本。
 - e. 完成匯入程序。
7. 編輯您在步驟 2 中建立的複寫計劃。在 **[目標電腦]** 中選擇 **[現有的複本]**, 然後選擇已匯入的複本。

如此一來, 軟體將會繼續更新複本。所有複寫將會增量。

VMware 用代理程式 - 不透過 LAN 備份

如果您的 ESXi 使用 SAN 連接儲存裝置, 請將代理程式安裝在連線至相同 SAN 的電腦上。代理程式將會直接從儲存裝置備份虛擬機器, 而不是透過 ESXi 主機和 LAN。此功能稱為「不透過 LAN 備份」。

下方圖表說明透過 LAN 與不透過 LAN 的備份方式。如果您有光纖通道 (FC) 或 iSCSI 儲存區域網路, 就可以不透過 LAN 存取虛擬機器。若要完全停用透過 LAN 傳送備份資料, 請將備份儲存在代理程式電腦的本機磁碟上, 或 SAN 附加存放區上。



啟用代理程式直接存取資料存放區

1. 在可經由網路存取 vCenter Server 的 Windows 電腦上安裝 VMware 用代理程式。
2. 將託管資料存放區的邏輯單元編號 (LUN) 連線至電腦。考慮以下情況：
 - 使用資料存放區連線至 ESXi 所用的相同協定 (即 iSCSI 或 FC)。
 - LUN 不得進行初始化, 但須在**[磁碟管理]**中顯示為「離線」磁碟。如果 Windows 對 LUN 進行初始化, 則其可能會損毀並且無法被 VMware vSphere 讀取。

因此, 代理程式會使用 SAN 傳輸模式存取虛擬磁碟, 即其會讀取 iSCSI/FC 上的原始 LUN 磁區, 而不識別 VMFS 檔案系統 (Windows 不會感知到這種行為)。

限制

- 在 vSphere 6.0 及更新版本中, 如果部分 VM 磁碟在 VMware 虛擬磁碟區 (VVol), 部分不在, 代理程式便無法使用 SAN 傳輸模式。此類虛擬機器的備份便會失敗。
- 即使您為代理程式設定了 SAN 傳輸模式, VMware vSphere 6.5 中提供的加密虛擬機器仍會透過 LAN 進行備份。由於 VMware 不支援採用 SAN 傳輸備份加密虛擬磁碟, 所以代理程式會回復至 NBD 傳輸。

範例

如果您使用 iSCSI SAN, 在執行 Windows 並安裝 VMware 用代理程式的電腦上設定 iSCSI 起始端。

設定 SAN 原則。

1. 以系統管理員身分登入、開啟命令提示字元、輸入 diskpart, 然後按 **Enter**。
2. 輸入 san, 然後按 **Enter**。確保 **SAN 原則:將顯示全部離線**。
3. 如果有設定 SAN 原則的另一個值:
 - a. 輸入 san policy=offlineall。
 - b. 按一下 **Enter**。
 - c. 要檢查是否有正確套用設定, 請執行步驟 2。
 - d. 重新啟動機器。

設定 iSCSI 起始端

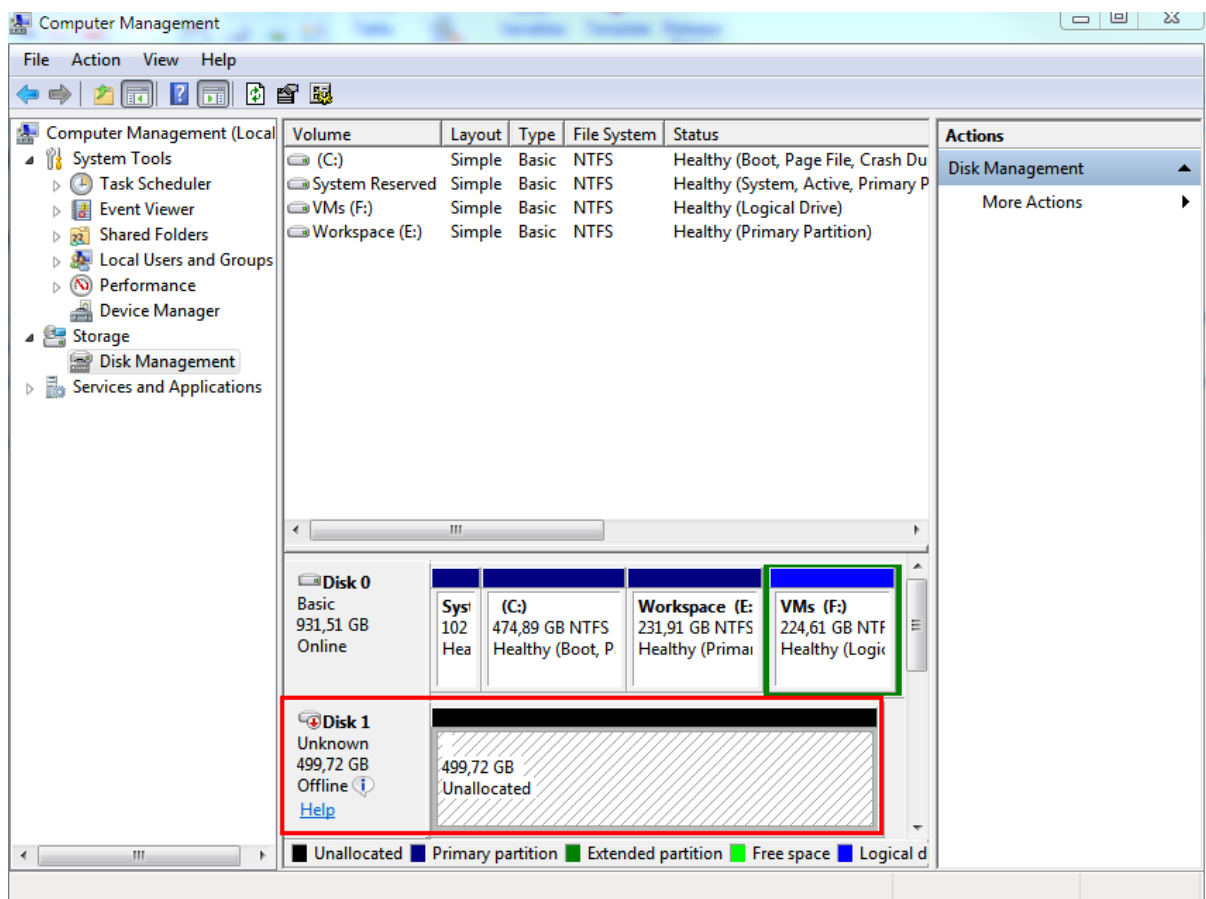
1. 移至 **[控制台]>[管理工具]>[iSCSI 起始端]**。

注意事項

若要尋找 **[管理工具]** 小程式, 您或需將 **[控制台]** 視圖變更為 **[首頁]** 或 **[類別]** 以外的項目, 或使用搜尋。

2. 如果這是第一次發佈 Microsoft iSCSI 起始端, 請確認您要啟動 Microsoft iSCSI 起始端服務。
3. 在**[目標]**索引標籤, 輸入目標 SAN 裝置的完整網域名稱 (FQDN) 或 IP 位址, 然後按一下**[快速連線]**。
4. 選擇託管資料存放區的 LUN, 然後按一下**[連線]**。
如果 LUN 未顯示, 請確保 iSCSI 目標的分區允許執行代理程式的電腦存取 LUN。電腦必須新增至此目標上已允許的 iSCSI 起始端清單。
5. 按一下 **[確定]**。

就緒的 SAN LUN 應顯示在下方螢幕擷取畫面所示的**[磁碟管理]**中。



使用本機附加的存放區

您可以將額外的磁碟附加到 VMware 用代理程式 (虛擬裝置)，讓代理程式可以備份到這個本機附加的存放區。這種方法減少了代理程式與備份位置之間的網路流量。

藉助備份虛擬機器執行於相同主機或叢集的虛擬裝置可以直接存取電腦所在的資料存放區。這意味著該裝置可以透過使用 HotAdd 傳輸來連接備份磁碟，因此，備份流量是由一個本端磁碟導向至另一個本端磁碟。若資料存放區是連線作為**磁碟/LUN**，而不是 **NFS**，則備份將完全不用 LAN。在 NFS 資料存放區的情況下，資料存放區與主機之間將會存在網路流量。

使用本機附加的存放區，即假設代理程式一律會備份相同的電腦。如果有多個代理程式於 vSphere 中運作，且其中一或多個代理程式使用本機附加的存放區，則您需要**手動**將每個代理程式繫結至所有其必須備份的電腦。否則，如果由管理伺服器重新分配電腦給代理程式，則可能發生一部電腦的備份分散到多個存放區的情形。

您可以將存放區新增到運作中的代理程式，亦可在從 **OVF 範本** 部署代理程式時新增存放區。

若要將存放區附加至運作中的代理程式

1. 在 VMware vSphere 詳細目錄中，用滑鼠右鍵按一下 [VMware 用代理程式 (虛擬裝置)]。
2. 編輯虛擬機器的設定，以新增磁碟。磁碟大小必須至少為 10 GB。

警告！

新增現有的磁碟時請務必小心。存放區一旦建立，此磁碟上所有先前含有的資料都將喪失。

3. 前往虛擬裝置主控台。您可以在畫面底部找到**建立存放區**連結。如果找不到此連結，請按一下**重新整理**。
4. 按一下**建立存放區**連結，選擇磁碟並為其指定標籤。由於檔案系統限制，標籤長度的限制為 16 個字元。

若要選擇本機附加的存放區作為備份目的地

建立保護計劃時，於**【備份目標位置】**中，選擇**【本機資料夾】**，然後輸入對應到本機連接存放區的代號，例如 **D:**。

虛擬機器繫結

本節概述 Cyber Protection 服務如何在 VMware vCenter 內組織多個代理程式的作業。

下列分配演算法適用於安裝在 Windows 的虛擬裝置和代理程式。

分配演算法

虛擬機器將自動平均分佈於 VMware 用代理程式之間。所謂的平均，是指每個代理程式會管理相同數量的虛擬機器。虛擬機器所佔用的儲存空間則不會納入計算。

然而，為虛擬機器選擇代理程式時，軟體會嘗試最佳化整體系統效能。軟體特別會考量代理程式與虛擬機器的位置。管理伺服器會優先選擇裝載於相同主機代理程式。如果相同的主機上沒有代理程式，則會優先選擇來自相同叢集的代理程式。

虛擬機器一旦指定給某個代理程式後，此虛擬機器的所有備份都會交由此代理程式負責進行。

重新分配

每當既定的平衡被破壞時 (更精確地說，當代理程式間負載不平衡的情況達到百分之 20 的程度時)，就會進行重新分配。當您新增或移除虛擬機器或代理程式、將虛擬機器移轉到不同的主機或叢集，或手動將虛擬機器繫結到代理程式時，就可能會發生這種情形。如果發生此情形，Cyber Protection 服務會使用相同的演算法重新分配電腦。

例如，您發現需要更多代理程式來增進處理能力，以及部署額外的虛擬裝置到叢集。Cyber Protection 服務會指派最適合的電腦給新的代理程式。舊代理程式的負載將會減少。

當您從 Cyber Protection 服務移除代理程式時，指派給代理程式的電腦會分配給剩餘的代理程式。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。
- 如果代理程式具有本機連接存放區, 則需將 VM 繫結到代理程式。

- 停用自動指派讓您能夠確保可根據您指定的排程對特定電腦進行預測備份。排程時間到來時，僅備份一台 VM 的代理程式無法正常備份其他 VM。
- 如果您有多台在地理上分離的 ESXi 主機，則停用自動指派非常有用。如果停用自動指派，然後將每台主機上的 VM 繫結到在同一主機上執行的代理程式，則可確保代理程式不會備份在遠端 ESXi 主機上執行的任何電腦，從而節省網路流量。

自動執行凍結前和解除凍結後指令碼

您可以透過 VMware Tools，在您使用無代理程式模式備份的虛擬機器上，自動執行自訂的凍結前和解除凍結後指令碼。因此，例如，您可以執行自訂的 quiescing 指令碼，並針對執行非 VSS 感知應用程式的虛擬機器，建立應用程式一致的備份。

必要條件

凍結前和解除凍結後指令碼必須位於虛擬機器上的特定資料夾。

- 若是 Windows 虛擬機器，此資料夾的位置取決於主機的 ESXi 版本。
例如，若是在 ESXi 6.5 主機上執行的虛擬機器，此資料夾為 C:\Program Files\VMware\VMware Tools\backupScripts.d\。您必須手動建立 backupScripts.d 資料夾。請不要在此資料夾中儲存其他類型的檔案，因為這可能會使 VMware Tools 變得不穩定。
如需有關其他 ESXi 版本的凍結前和解除凍結後指令碼位置的詳細資訊，請參閱 VMware 文件。
- 若是 Linux 虛擬機器，請將您的指令碼分別複製到 /usr/sbin/pre-freeze-script 和 /usr/sbin/post-thaw-script 目錄。當您建立快照時，會執行 /usr/sbin/pre-freeze-script 中的指令碼；當快照最終化時，會執行 /usr/sbin/post-thaw-script 中的指令碼。這些指令碼必須可由 VMware Tools 使用者執行。

若要自動執行凍結前和解除凍結後指令碼

1. 請確認 VMware Tools 已安裝在虛擬機器上。
2. 在虛擬機器上，將您的自訂指令碼放到所需的資料夾中。
3. 在此機器的保護計劃中，啟用 **[虛擬機器的磁碟區陰影複製服務 (VSS)]** 選項。
如此會在啟用 **[靜止客體檔案系統]** 選項時，建立 VMware 快照，然後觸發虛擬機器內的凍結前和解除凍結後指令碼。

您不需要在執行 VSS 感知應用程式 (例如 Microsoft SQL Server 或 Microsoft Exchange) 的虛擬機器上執行自訂的 quiescing 指令碼。若要針對這類機器建立應用程式一致的備份，請在保護計劃中啟用 **[虛擬機器的磁碟區陰影複製服務 (VSS)]** 選項。

支援虛擬機器移轉

本節包含虛擬機器在 vSphere 環境中移轉的相關資訊，包括 vSphere 叢集所屬 ESXi 主機之間的移轉。

vMotion 允許將虛擬機器的狀態和組態移至其他主機，而電腦磁碟則保持在共用儲存空間的相同位置。Storage vMotion 允許將虛擬機器磁碟從一個資料存放區移至另一個資料存放區。

- 執行 VMware 用代理程式的虛擬機器 (虛擬裝置) 不支援使用 vMotion (包括 Storage vMotion) 進行移轉，且已自動遭到停用。此虛擬機器會新增至 vSphere 叢集設定的 **[VM 覆寫]** 清單中。

- 開始備份虛擬機器時，會自動停用使用 vMotion (包括 Storage vMotion) 進行移轉。此虛擬機器會暫時新增至 vSphere 叢集設定的 **[VM 覆寫]** 清單中。備份完成後，系統會將 **[VM 覆寫]** 設定自動還原至其先前的狀態。
- 正在使用 vMotion (包括 Storage vMotion) 進行虛擬機器移轉時，無法開始該虛擬機器的備份。當此虛擬機器的移轉完成後，就會開始該機器的備份。

管理虛擬化環境

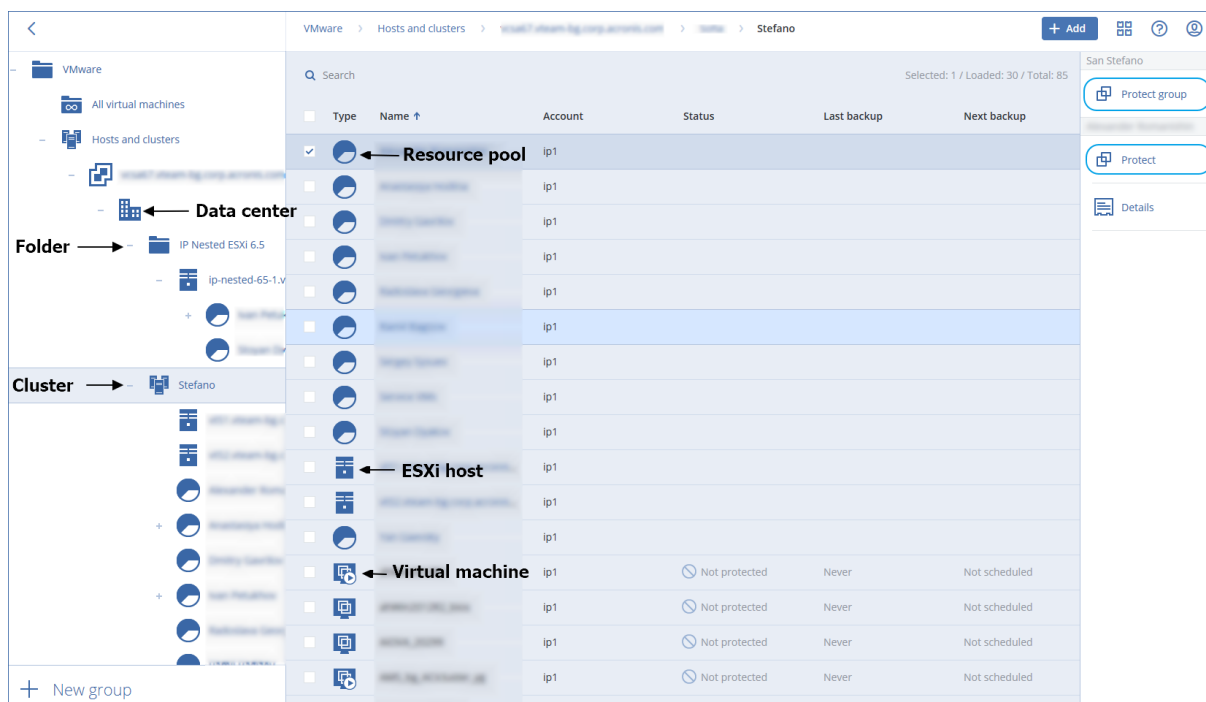
您可以使用原生的呈現方式檢視 vSphere、Hyper-V 及 Virtuozzo 環境。一旦已安裝並登錄對應的代理程式之後，**[VMware]**、**[Hyper-V]** 或 **[Virtuozzo]** 索引標籤就會出現在 **[裝置]** 底下。

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 **[保護]** 來備份所選群組電腦，或按一下 **[保護群組]** 來保護所選群組所屬的父群組電腦。

例如，您已經選擇 Stefano 叢集，然後選擇其中的資源集區。如果您按一下 **[保護]**，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 **[保護群組]**，則會備份 Stefano 叢集中包含的所有虛擬機器。



[VMware] 索引標籤可讓您變更 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]**

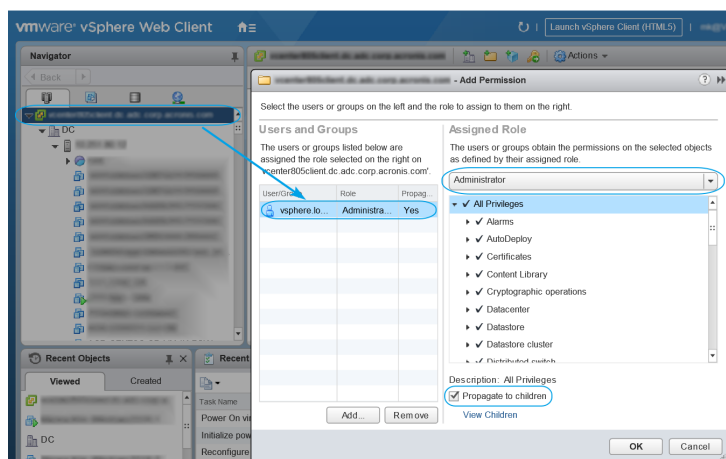
VMware 用代理程式 - 必要權限

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。如果您稍後需要變更帳戶，請參閱 "管理虛擬化環境" (第 333 頁)。

若要將權限指派給 vCenter 層級的 vSphere 使用者

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
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	儲存磁碟分割組態				+
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		+	+	+
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		+	+	
	由 VIX API 執行客體作業系統管理 (適用於 vSphere 5.1 及更新版本)				+
	關閉電源			+	+
	開啟電源		+	+	+
虛擬機器 > 清查	建立自現有		+	+	+
	新建		+	+	+
	登錄				+
	移除		+	+	+
	取消登錄				+
虛擬機器 > 佈建	允許磁碟存取		+	+	+

	允許唯讀磁碟存取	+		+	
	允許虛擬機器下載	+	+	+	+
虛擬機器 > 狀態 虛擬機器 > 快照管理 (vSphere 6.5 和更新版本)	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。

13.25.3 備份叢集 Hyper-V 虛擬機器

在 Hyper-V 叢集中，虛擬機器可以在不同的叢集節點之間移轉。請依照以下建議，設定正確的叢集 Hyper-V 虛擬機器備份：

1. 無論虛擬機器移轉的目的地節點為何，都必須可供備份。為了確保 Hyper-V 用代理程式可以存取任何節點上的電腦，代理程式服務必須以在各叢集節點上具有系統管理權限的網域使用者帳戶身分執行。
建議您在 Hyper-V 用代理程式安裝期間，為代理程式服務指定上述帳戶。
2. 在叢集的每個節點上安裝 Hyper-V 用代理程式。
3. 在 Cyber Protection 服務中註冊所有代理程式。

已復原虛擬機器的高可用性

當您將備份的磁碟復原至現有的 Hyper-V 虛擬機器時，虛擬機器的 [高可用性] 屬性將保持原樣。

當您將備份的磁碟復原至新的 Hyper-V 虛擬機器時，所產生的虛擬機器將不具有高可用性。它會視為備用虛擬機器，而且電源通常會關閉。如果您需要在實際執行環境中使用該虛擬機器，可以從容錯移轉叢集管理嵌入式管理單元中，將其設定為具有 [高可用性]。

13.25.4 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 登錄編輯程式 5.00 版

```
[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
```

限制 VMware 用代理程式 (虛擬裝置) 可以備份的虛擬機器總數

1. 若要啟動命令殼層, 在虛擬裝置 UI 中時, 按下 CTRL+SHIFT+F2。
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="Tdwor">"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. 執行 **reboot** 命令以重新啟動代理程式。

13.25.5 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	ESX i 虛 擬 機 器	Hype r-V 虛 擬 機 器	Virtuoz zo 虛 擬 機 器	Virtuoz zo 容 器	Virtuozzo Hybrid Infrastruc ture 虛擬機器	Scale Computi ng HC3 虛擬機 器	RHV/oV irt 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	+	+	+	-	-	+	+	+

注意事項

您無法將 macOS 虛擬機器復原至 Hyper-V 主機，因為 Hyper-V 不支援 macOS。您可以將 macOS 虛擬機器復原至 Mac 硬體上安裝的 VMware 主機。

如需執行移轉的指示，請參閱下列章節：

- 實體到虛擬 (P2V) -「[實體機器到虛擬](#)」
- 虛擬到虛擬 (V2V) -「[虛擬機器](#)」
- 虛擬到實體 (V2P) -「[虛擬機器](#)」或「[使用可開機媒體復原磁碟](#)」

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，從 Virtuozzo 執行 P2V 移轉、V2P 移轉或 V2V 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。

13.25.6 Microsoft Azure 和 Amazon EC2 虛擬機器

若要備份 Microsoft Azure 或 Amazon EC2 虛擬機器，請在電腦上安裝保護代理程式。對於實體電腦，備份和復原作業是相同的。不過，您設定機器的數量配額時，系統會將該電腦視為虛擬機器。

這和實體機器的差異之處在於 Microsoft Azure 和 Amazon EC2 虛擬機器無法從可開機媒體開機。若您需要復原至新的 Microsoft Azure 或 Amazon EC2 虛擬機器，請依照以下程序執行。

若要將電腦復原為 *Microsoft Azure* 或 *Amazon EC2* 虛擬機器

1. 從 Microsoft Azure 或 Amazon EC2 中的影像/範本建立新的虛擬機器。新電腦的磁碟組態必須與您要復原的電腦組態相同。
2. 在新電腦上安裝 Windows 用代理程式或 Linux 用代理程式。
3. 按照「[實體機器](#)」一節中所述的程序復原備份電腦。設定復原時，選擇新電腦做為目標電腦。

14 災難復原

注意事項

此功能僅能搭配 Cyber Protection 服務的 Disaster Recovery 附加元件使用。

14.1 關於 Cyber Disaster Recovery Cloud

Cyber Disaster Recovery Cloud (DR) – Cyber Protection 的一部分，可提供災難復原即服務 (DRaaS)。Cyber Disaster Recovery Cloud 可為您提供一個快速且穩定的解決方案，以便在雲端站台上啟動確切的電腦複本，並在發生人為或自然災害時，將工作負載從損毀的原始電腦切換到雲端的復原伺服器。

您可以透過下列方式安裝並設定災難復原：

- 建立包含災難復原模組的保護計劃，並將其套用至您的裝置。這將會自動設定預設災難復原基礎架構。請參閱[建立災難復原保護計劃](#)。
- 手動設定災難復原雲端基礎架構並控制每個步驟。請參閱 "設定復原伺服器" (第 377 頁)。

14.1.1 主要功能

注意事項

部分功能可能需要額外的授權，端視適用的授權模型而定。

- 從單一主控台管理 Cyber Disaster Recovery Cloud 服務
- 使用安全的 VPN 通道，將最多 23 個區域網路延伸至雲端
- 建立與雲端站台的連線，而不需要部署任何 VPN 設備¹ (僅雲端模式)
- 建立本機站台和雲端站台的點對站台連線
- 使用雲端的復原伺服器保護您的電腦
- 使用雲端的主要伺服器保護應用程式和設備
- 為加密的備份執行自動災難復原作業
- 在隔離的網路中執行測試容錯移轉
- 使用 Runbook 在雲端啟動實際執行環境

14.2 軟體需求

14.2.1 支援的作業系統

使用復原伺服器的保護，已針對下列作業系統進行測試：

¹[災難復原] 特殊的虛擬機器，可透過安全的 VPN 通道，在區域網路和雲端站台之間連線。VPN 設備是在本機站台上部署的。

- CentOS 6.6, 7.x, 8.x
- Debian 9
- Ubuntu 16.04、18.04
- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – 所有安裝選項, Nano Server 除外
- Windows Server 2019 – 所有安裝選項, Nano Server 除外

由於 Microsoft 產品條款的緣故, 不支援 Windows 桌面作業系統。

軟體可能可搭配其他 Windows 作業系統或 Linux 版本使用, 但不提供保證。

14.2.2 支援的虛擬化平台

使用復原伺服器的虛擬機器保護, 已針對下列虛擬化平台進行測試:

- VMware ESXi 5.1、5.5、6.0、6.5、6.7
- 帶 Hyper-V 的 Windows Server 2008 R2
- 帶 Hyper-V 的 Windows Server 2012/2012 R2
- Windows Server 2016 with Hyper-V – 所有安裝選項, Nano Server 除外
- Windows Server 2019 與 Hyper-V – 所有安裝選項, Nano Server 除外
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- 核心虛擬機器 (KVM)
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5、7.0、7.1、7.2

VPN 設備已針對下列虛擬化平台進行測試:

- VMware ESXi 5.1、5.5、6.0、6.5、6.7
- 帶 Hyper-V 的 Windows Server 2008 R2
- 帶 Hyper-V 的 Windows Server 2012/2012 R2
- Windows Server 2016 with Hyper-V – 所有安裝選項, Nano Server 除外
- Windows Server 2019 與 Hyper-V – 所有安裝選項, Nano Server 除外
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

軟體可能可搭配其他虛擬化平台或版本使用, 但不提供保證。

14.2.3 限制

在 Cyber Disaster Recovery Cloud 中不支援下列平台和設定:

1. 不支援的平台：

- Virtuozzo 用代理程式
- macOS

2. 不支援的設定：

Microsoft Windows

- 不支援動態磁碟
- 不支援 Windows 桌面作業系統 (由於 Microsoft 產品條款的緣故)
- 不支援具有 FRS 複寫的 Active Directory 服務
- 不支援不採用 GPT 或 MBR 格式 (所謂的「超級軟碟」) 的卸除式媒體

Linux

- 不含磁碟分割表的檔案系統
- 使用客體 OS 的代理程式備份，而且擁有包含下列進階邏輯磁碟區管理員 (LVM) 設定之磁碟區的 Linux 工作負載：等量磁碟區、鏡像磁碟區、RAID 0、RAID 4、RAID 5、RAID 6 或 RAID 10 磁碟區。

3. 不支援的備份類型：

- 連續資料保護 (CDP) 復原點不相容。

重要事項

如果您從擁有 CDP 復原點的備份建立復原伺服器，則在容錯回復或建立復原伺服器備份期間，您將失去 CDP 復原點中所包含的資料。

- 鑑識備份無法用於建立復原伺服器。

復原伺服器擁有一個網路介面。如果原始電腦有數個網路介面，則只模擬一個。

雲端伺服器未加密。

14.3 Cyber Disaster Recovery Cloud 試用版產品

您可以使用 Acronis Cyber Disaster Recovery Cloud 的試用版產品 30 天。在此情況下，災難復原具備下列限制：

- 您僅能使用 1 TB 的 Acronis 災難復原即時儲存空間。
- 您僅能使用 100 個計算點。如需有關計算點的詳細資訊，請參閱 [Compute-points.htm](https://www.acronis.com/en/Products/Cloud/Compute-points.htm)。
- 您僅能使用 1 TB 的 Acronis 離線雲端儲存空間來儲存備份。
- 復原伺服器和主要伺服器無法存取公用網際網路。您無法將公共 IP 位址指派給伺服器。
- IPsec 多站台 VPN 無法使用。

14.4 計算點

在 [災難復原] 中，計算點在測試容錯移轉和實際執行容錯移轉期間用於主要伺服器及復原伺服器。計算點會反映在雲端執行伺服器 (虛擬機器) 所使用的計算資源。

計算點在災難復原期間的耗用量取決於伺服器的參數，以及伺服器處於容錯移轉狀態期間的持續時間。伺服器越強大且時間越長，耗用的計算點越多。此外，耗用的計算點越多，您要支付的價格就越高。

在下表中，您可以看到雲端伺服器的八種不同類別。您可以在 **[詳細資料]** 索引標籤中變更伺服器的類別。

類型	CPU	RAM	計算點
F1	1 個 vCPU	2 GB	1
F2	1 個 vCPU	4 GB	2
F3	2 個 vCPU	8 GB	4
F4	4 個 vCPU	16 GB	8
F5	8 個 vCPU	32 GB	16
F6	16 個 vCPU	64 GB	32
F7	16 個 vCPU	128 GB	64
F8	16 個 vCPU	256 GB	128

您可以使用表格中的資訊，輕鬆地估計一部伺服器 (虛擬機器) 將耗用的計算點數量。

例如，如果您要使用 [災難復原] 保護一部擁有 4 個 vCPU* 16 GB RAM 的虛擬機器，以及一部擁有 2 個 vCPU 8 GB RAM 的虛擬機器，則第一部虛擬機器每小時將耗用 8 個計算點，第二部虛擬機器每小時將耗用 4 個計算點。如果兩部虛擬機器都處於容錯移轉狀態，則總耗用量將為每小時 12 個計算點，或整天 288 個計算點 (12 個計算點 x 24 小時 = 288 個計算點)。

*vCPU 指的是指派給虛擬機器的實體中央處理器 (CPU)，而且是與時間相關的實體。

14.5 設定災難復原功能

注意事項

部分功能可能需要額外的授權，端視適用的授權模型而定。

若要設定災難復原功能

- 設定雲端站台的連線類型：
 - 點對站台連線
 - 站台對站台 OpenVPN 連線
 - 多站台 IPsec VPN 連線
 - 僅雲端模式
- 在啟用備份模組的情況下建立保護計劃，並選擇整部電腦或系統以及開機磁碟區以進行備份。建立復原伺服器時，至少需要有一個保護計劃。
- 將保護計劃套用至要保護的本機伺服器。

4. 針對您要保護的每部本機伺服器, [建立復原伺服器](#)。
5. [執行測試容錯移轉](#)以確認其運作方式。
6. [選擇性] [建立主要伺服器](#)以進行應用程式複寫。

因此, 您已經設定災難復原功能來保護您的本機伺服器免於災難。

如果發生災難, 您可以[容錯移轉工作負載](#)到雲端的復原伺服器。容錯移轉至復原伺服器之前, 必須至少建立一個復原點。當您的本機站台從災難復原時, 您可以執行容錯回復, 將工作負載切換回本機站台。如需有關容錯回復程序的詳細資訊, 請參閱 "對虛擬機器執行容錯回復" (第 385 頁) 和 "對實體機器執行容錯回復" (第 387 頁)。

14.6 建立災難復原保護計劃

建立包含災難復原模組的保護計劃, 並將其套用至您的裝置。

根據預設, 建立新的保護計劃時, 會停用災難復原模組。啟用災難復原功能並將計劃套用到您的電腦之後, 系統會針對每部受保護的電腦, 建立雲端網路基礎架構, 包括復原伺服器。復原伺服器是雲端中所選裝置複本的虛擬機器。系統會針對每個選取的裝置, 在待命狀態 (虛擬機器未執行) 下使用預設設定建立一部復原伺服器。復原伺服器會根據受保護電腦的 CPU 和 RAM, 自動調整大小。系統也會自動建立預設的雲端網路基礎架構: 連線復原伺服器所在雲端站台上的 VPN 閘道和網路。

如果您撤銷、刪除或關閉保護計劃的災難復原模組, 就不會自動刪除復原伺服器和雲端網路。如有需要, 您可以手動移除災難復原基礎架構。

注意事項

- 建議您事先設定災難復原。您將能夠從為裝置建立復原伺服器後產生的任何復原點, 執行測試或實際執行容錯移轉。未使用災難復原保護裝置 (例如, 未建立復原伺服器) 時產生的復原點無法用於容錯移轉。
 - 如果無法偵測到裝置的 IP 位址 (例如, 當虛擬機器以無代理程式備份且未獲指派 IP 位址時), 則無法啟用災難復原保護計劃。
 - 當您套用保護計劃時, 系統會在雲端站台中指派相同的網路和 IP 位址。IPsec VPN 連線要求雲端站台和本機站台的網路區段不要重疊。如果已設定多站台 IPsec VPN 連線, 且您之後將保護計劃套用至一或數個裝置, 則您必須另外更新雲端網路, 並重新指派雲端伺服器的 IP 位址。如需詳細資訊, 請參閱 "重新指派 IP 位址" (第 370 頁)。
-

建立災難復原保護計劃

1. 在服務主控台中, 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]**。
保護計劃預設設定隨即開啟。
4. 設定備份選項。
若要使用災難復原功能, 此計劃必須在雲端儲存空間備份整部電腦, 或僅備份開機及提供必要服務所需的磁碟。
5. 按一下模組名稱旁邊的開關, 以啟用災難復原模組。

6. 按一下 **[建立]**。

系統隨即建立計劃，並將其套用至選取的電腦。

後續步驟

- 您可以編輯復原伺服器的預設設定。如需詳細資訊，請參閱 "設定復原伺服器" (第 377 頁)。
- 您可以編輯預設網路設定。如需詳細資訊，請參閱 "設定連線" (第 347 頁)。
- 您可以深入瞭解復原伺服器預設參數和雲端網路基礎架構。如需詳細資訊，請參閱 "編輯復原伺服器預設參數" (第 346 頁) 和 "雲端網路基礎架構" (第 347 頁)。

14.6.1 編輯復原伺服器預設參數

當您建立並套用災難復原保護計劃時，會使用預設參數建立復原伺服器。您之後可以編輯這些預設參數。

注意事項

復原伺服器只有在不存在時才會建立。系統不會變更或重新建立現有的復原伺服器。

編輯復原伺服器預設參數

1. 移至 **[裝置] > [所有裝置]**。
2. 選擇一個裝置，然後按一下 **[災難復原]**。
3. 編輯復原伺服器預設參數。

復原伺服器參數如下表所述。

復原伺服器參數	預設價值	描述
CPU 和 RAM	自動	復原伺服器的虛擬 CPU 數量和 RAM 數量。系統將會根據原始裝置的 CPU 和 RAM 設定，自訂決定預設設定。
雲端網路	自動	將與伺服器連線的雲端網路。如需有關如何設定雲端網路的詳細資訊，請參閱雲端網路基礎架構。
實際執行網路中的 IP 位址	自動	伺服器將在實際執行網路中具備的 IP 位址。依預設，會設定原始電腦的 IP 位址。
測試 IP 位址	已停用	測試 IP 位址可讓您有能力在隔離的測試網路中測試容錯移轉，並在測試容錯移轉期間，透過 RDP 或 SSH 連線到復原伺服器。在測試容錯移轉模式中，VPN 閘道將會使用 NAT 通訊協定，將測試 IP 位址取代為實際執行 IP 位址。如果未指定測試 IP 位址，則在測試容錯移轉期間只能使用主控台存取伺服器。
網際網路存取	已啟用	可讓復原伺服器在實際或測試容錯移轉期間存取網際網路。預設拒絕 TCP 連接埠 25，以供輸出連

		線使用。
使用公共位址	已停用	具有公共 IP 位址可在容錯移轉或測試容錯移轉期間，讓復原伺服器從網際網路使用。如果您沒有使用公共 IP 位址，則只能在您的實際執行網路中使用該伺服器。若要使用公共 IP 位址，您必須啟用網際網路存取。公共 IP 位址將在您完成設定之後顯示。預設開放 TCP 連接埠 443，以供輸入連線使用。
設定 RPO 閾值	已停用	RPO 閾值會定義上次復原點和目前時間之間的最大可允許時間間隔。此值可以設定在 15 – 60 分鐘、1 – 24 小時、1 – 14 天內。

14.6.2 雲端網路基礎架構

雲端網路基礎架構是由連線復原伺服器所在雲端站台和雲端網路上的 VPN 閘道所組成。

注意事項

套用災難復原保護計劃只有在復原雲端網路基礎架構不存在時才會加以建立。系統不會變更或重新建立現有的雲端網路。

系統會檢查裝置 IP 位址，如果沒有 IP 位址適用的現有雲端網路，就會自動建立適合的雲端網路。如果您已經有復原伺服器 IP 位址適用的現有雲端網路，將不會變更或重新建立現有的雲端網路。

- 如果您沒有現有的雲端網路或者您是第一次設定災難復原設定，將會根據您裝置的 IP 位址範圍，使用 IANA 建議的最大範圍建立私人用途的雲端網路 (10.0.0.0/8、172.16.0.0/12、192.168.0.0/16)。您可以透過編輯網路遮罩來縮小網路的範圍。
- 如果在多個區域網路上都有您的裝置，則雲端站台上的網路將會變成區域網路的超集。您可以在 **[連線]** 區段中重新設定網路。請參閱 "管理網路" (第 364 頁)。
- 如果您需要設定站台對站台的 OpenVPN 連線，請下載並安裝 VPN 設備。請參閱 "設定站台對站台 OpenVPN" (第 357 頁)。請確認您的雲端網路範圍符合連線到 VPN 設備的區域網路範圍。
- 若要變更預設網路設定，按一下保護計劃的「災難復原」模組上的 **移至連線** 連結，或瀏覽至 **[災難復原] > [連線]**。

14.7 設定連線

本節說明您要瞭解網路在 Cyber Disaster Recovery Cloud 中的運作方式所需的網路概念。您將瞭解如何根據您的需求，設定不同類型的雲端站台連線。最後，您將瞭解如何在雲端管理您的網路，以及管理 VPN 設備和 VPN 閘道的設定。

14.7.1 網路概念

注意事項

部分功能可能需要額外的授權，端視適用的授權模型而定。

您可以透過 Cyber Disaster Recovery Cloud, 定義下列雲端站台的連線類型：

- **僅雲端模式**

這種類型的連線不需要在本機站台上部署 VPN 設備。

區域網路和雲端網路是兩個獨立的網路。這種類型的連線意味著容錯移轉所有本機站台受保護的伺服器, 或部分容錯移轉不需要與本機站台通訊的獨立伺服器。

雲端站台上的雲端伺服器可以透過點對站台 VPN, 以及公共 IP 位址 (如果已指派) 存取。

- **站台對站台 OpenVPN 連線**

這種類型的連線必須在本機站台上部署 VPN 設備。

站台對站台 OpenVPN 連線允許將您的網路延伸至雲端, 並保留 IP 位址。

您的區域網路會透過安全的 VPN 通道連線至雲端站台。如果您在本機站台上擁有緊密相依的伺服器 (例如, 網頁伺服器和資料庫伺服器), 則適合這種類型的連線。如果發生部分容錯移轉, 當您在雲端重建這些伺服器中的其中一部伺服器, 而其他伺服器則保留在本機站台上時, 它們將仍然能夠透過 VPN 通道, 與彼此通訊。

雲端站台上的雲端伺服器可以透過區域網路、點對站台 VPN, 以及公共 IP 位址 (如果已指派) 存取。

- **多站台 IPsec VPN 連線**

此類型的連線需要有支援 IPsec IKE v2 的本機 VPN 裝置。

當您開始設定多站台 IPsec VPN 連線時, Cyber Disaster Recovery Cloud 會使用公共 IP 位址, 自動建立一個雲端 VPN 閘道。

使用多站台 IPsec VPN 時, 您的本機站台會透過安全的 IPsec VPN 通道連線至雲端站台。

當您有一或數個本機站台主控重要工作負載或緊密相依的服務時, 此類型的連線適用於災難復原情境。

如果其中一部伺服器發生部分容錯移轉, 系統會在雲端站台上重新建立該伺服器, 而其他伺服器則保留在本機站台上, 而且這些伺服器仍然能夠透過 IPsec VPN 通道, 與彼此通訊。

如果其中一個本機站台發生部分容錯移轉, 其餘的本機站台則維持運作, 而且將仍然能夠透過 IPsec VPN 通道, 與彼此通訊。

- **點對站台遠端 VPN 存取**

使用端點裝置, 從外部進行雲端和本機站台工作負載的安全點對站台遠端 VPN 存取。

對於本機站台存取, 這種類型的連線必須在本機站台上部署 VPN 設備。

注意事項

您可以透過 Cyber Disaster Recovery Cloud, 將區域網路延伸至雲端。

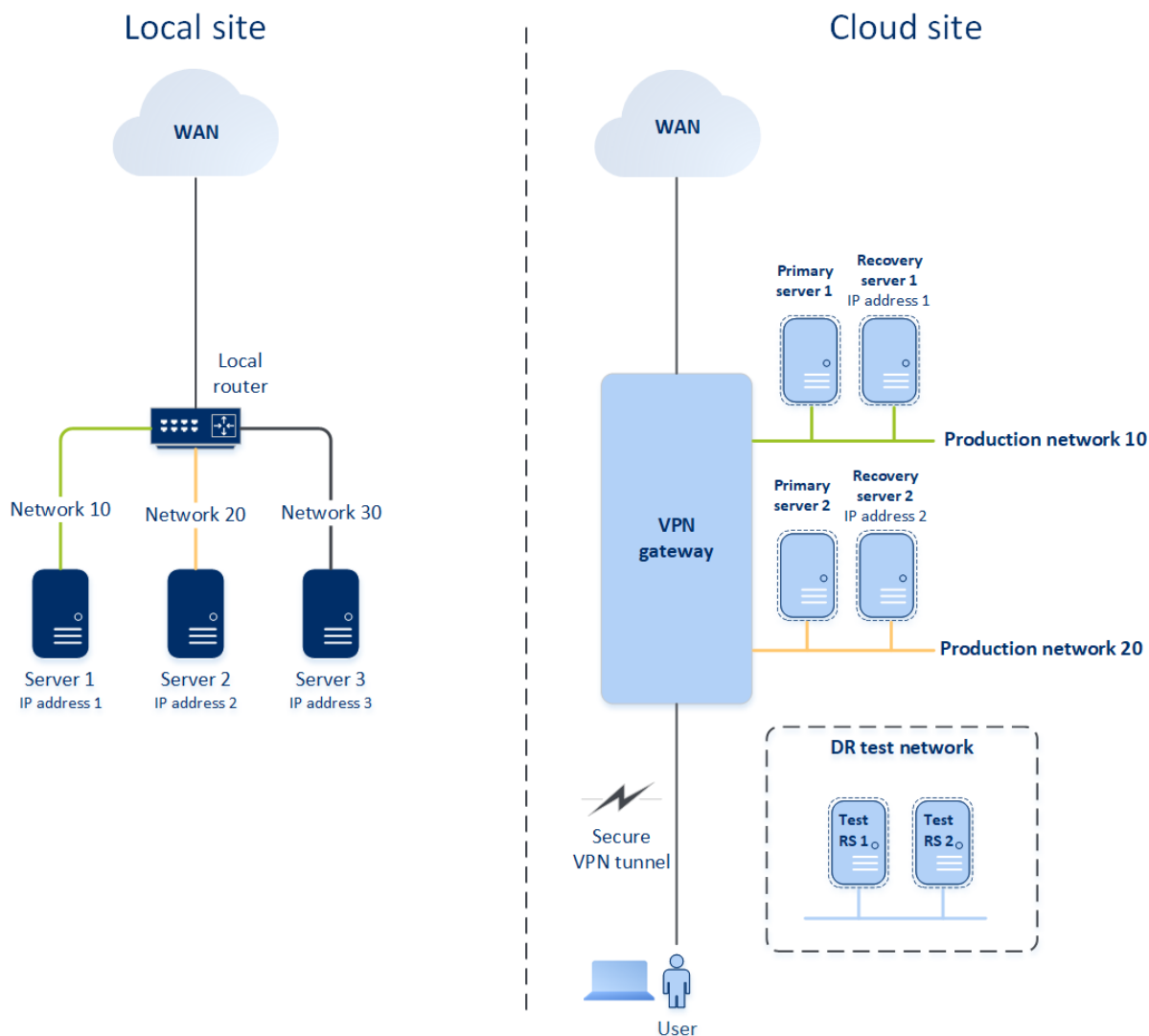
- 如果您的雲端站台使用的是 US2 或 US5 資料中心, 則最多可以延伸至 5 個區域網路。
 - 如果您的雲端站台使用的是其他任何資料中心, 則最多可以延伸至 23 個區域網路。
-

僅雲端模式

僅雲端模式不需要在本機站台上部署 VPN 設備。這意味著您有兩個獨立網路: 一個在本機站台上, 另一個在雲端站台上。路由是使用路由器, 在雲端站台上執行的。

路由的運作方式

如果已建立僅雲端模式，則會使用雲端站台上的路由器執行路由，讓不同雲端網路的伺服器可以彼此通訊。



站台對站台 OpenVPN 連線

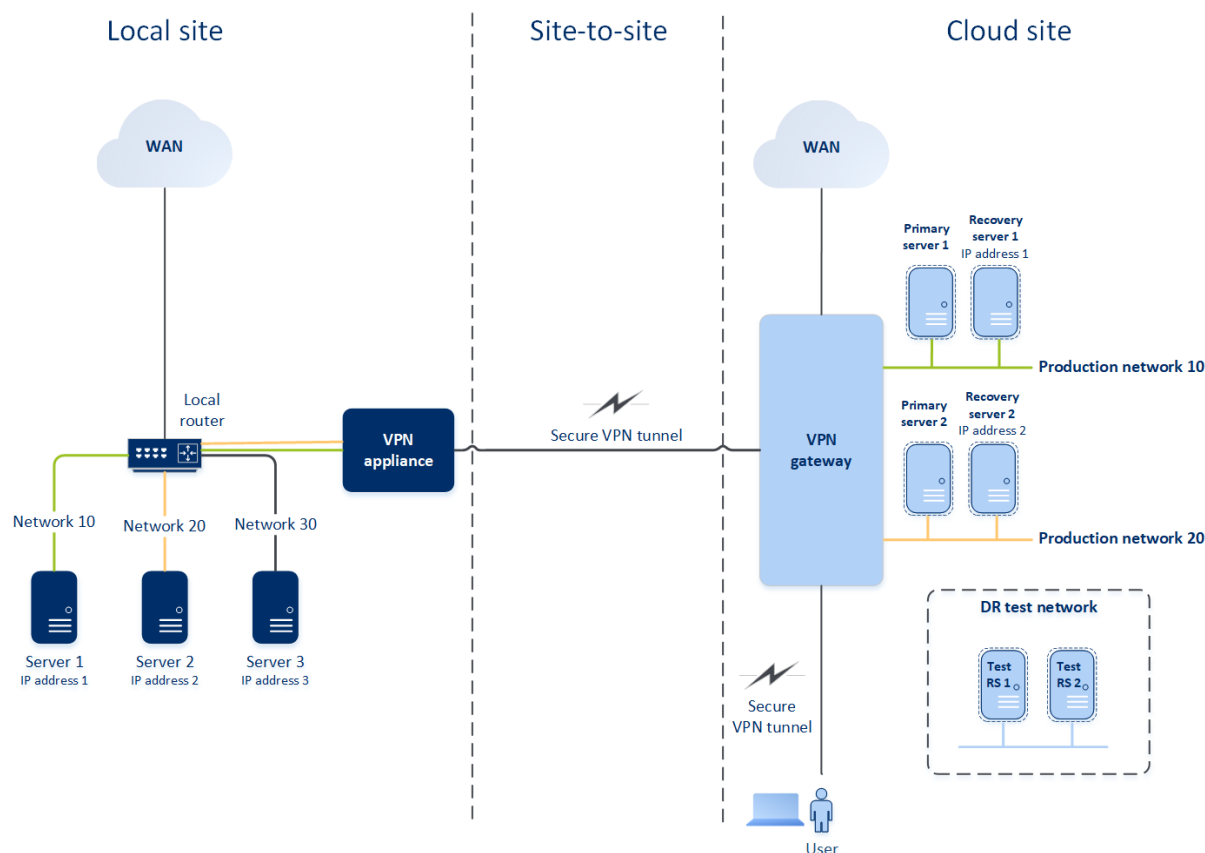
注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

為瞭解網路在 Cyber Disaster Recovery Cloud 中運作的方式，我們將考慮當您有三個網路時，每個本機站台都有一部電腦的情況。您將為下列兩個網站設定災難防護：網路 10 和網路 20。

在以下的圖表中，您可以看到託管電腦所在的本機站台，以及發生災難時啟動雲端伺服器所在的雲端站台。

您可以使用 Cyber Disaster Recovery Cloud 解決方案，將所有工作負載從本機站台中損毀的電腦容錯移轉至雲端中的雲端伺服器。使用 Cyber Disaster Recovery Cloud 最多可以保護 23 個網路。



若要在本機站台和雲端站台之間建立站台對站台 OpenVPN 通訊，會使用 **VPN 設備**和 **VPN 閘道**。當您開始在服務主控台中設定站台對站台 OpenVPN 連線時，會在雲端站台中自動部署 VPN 閘道。接著，您必須在本機站台上部署 VPN 設備、新增要保護的網路，然後在雲端登錄設備。Cyber Disaster Recovery Cloud 會在雲端建立您區域網路的複本。系統會在 VPN 設備和 VPN 閘道之間建立一個安全的 VPN 通道。它可讓您的區域網路延伸到雲端。雲端中的實際執行網路會與您的區域網路橋接。本機伺服器和雲端伺服器可以透過此 VPN 通道通訊，如同它們全都位於相同的乙太網路區段。路由是使用您的本機路由器執行的。

對於要保護的每部來源電腦，您必須在雲端站台上建立一部復原伺服器。它會維持在 **[待命]** 狀態，直到發生生容錯移轉事件為止。如果發生災難，而且您開始容錯移轉程序 (在 **實際執行模式**下)，會在雲端啟動代表您受保護電腦確切複本的復原伺服器。它可能會獲指派與來源電腦相同的 IP 位址，而且它可以在相同的乙太網路區段中啟動。您的用戶端可以繼續使用伺服器，而不會注意到任何背景變更。

您也可以在 **測試模式**下啟動容錯移轉程序。也就是說，來源電腦仍在運作中，同時，擁有相同 IP 位址的個別復原伺服器會在雲端啟動。若要防止 IP 位址發生衝突，要在雲端建立一個特殊的虛擬網路 - **測試網路**。測試網路會加以隔離，以防某個乙太網路區段中的來源電腦 IP 位址重複。若要在測試容錯移轉模式下存取復原伺服器，當您建立復原伺服器時，必須將 **[測試 IP 位址]** 指派給該復原伺服器。復原伺服器有可以指定的其他參數，在以下相應的章節中將會考慮使用這些參數。

路由的運作方式

如果已建立站台對站台連線，則會使用您的本機路由器執行雲端網路之間的路由。**VPN 伺服器**不會執行不同雲端網路中的雲端伺服器間的路由。如果某個網路的雲端伺服器想要與另一個雲端網路的伺服器通訊，流量會通過 **VPN 通道**到達本機站台上的本機路由器，接著本機路由器會將其路由傳送到另一個網路，然後再通過通道到達雲端站台上的目的地伺服器。

VPN 閘道

允許在本機站台和雲端站台間通訊的主要元件為 **VPN 閘道**。這是雲端中安裝特殊軟體，並專門設定網路所在的虛擬機器。**VPN 閘道**具備下列功能：

- 在 L2 模式下，連線雲端中區域網路和實際執行網路的乙太網路區段。
- 提供 iptables 和 ebtables 規則。
- 當做預設路由器和 NAT 使用，以供測試和實際執行網路中的電腦使用。
- 當做 DHCP 伺服器使用。實際執行與測試網路中的所有電腦都會透過 DHCP 取得網路設定 (IP 位址、DNS 設定)。每次雲端伺服器都將從 DHCP 伺服器取得相同的 IP 位址。如果您需要設定自訂 DNS 設定，應該連絡支援小組。
- 當做快取 DNS 使用。

VPN 閘道網路設定

VPN 閘道有數個網路介面：

- 外部介面，連線至網際網路
- 實際執行介面，連線至實際執行網路
- 測試介面，連線至測試網路

此外，系統會新增兩個虛擬介面，分別供點對站台連線和站台對站台連線使用。

部署並初始化 **VPN 閘道**時，系統會建立橋接 (一個供外部介面使用，一個供用戶端和實際執行介面使用)。雖然用戶端實際執行橋接和測試介面使用相同的 IP 位址，但是 **VPN 閘道**可以使用特定技術，正確路由傳送套件。

VPN 設備

VPN 設備是本機站台上已安裝 Linux 的一部虛擬機器，其中安裝了特殊軟體，而且具有特殊網路設定。此設備允許在本機和雲端站台之間進行通訊。

復原伺服器

復原伺服器：原始電腦的一個複本，以儲存在雲端的受保護伺服器備份為基礎。復原伺服器在發生災難時，用於從原始伺服器切換工作負載。

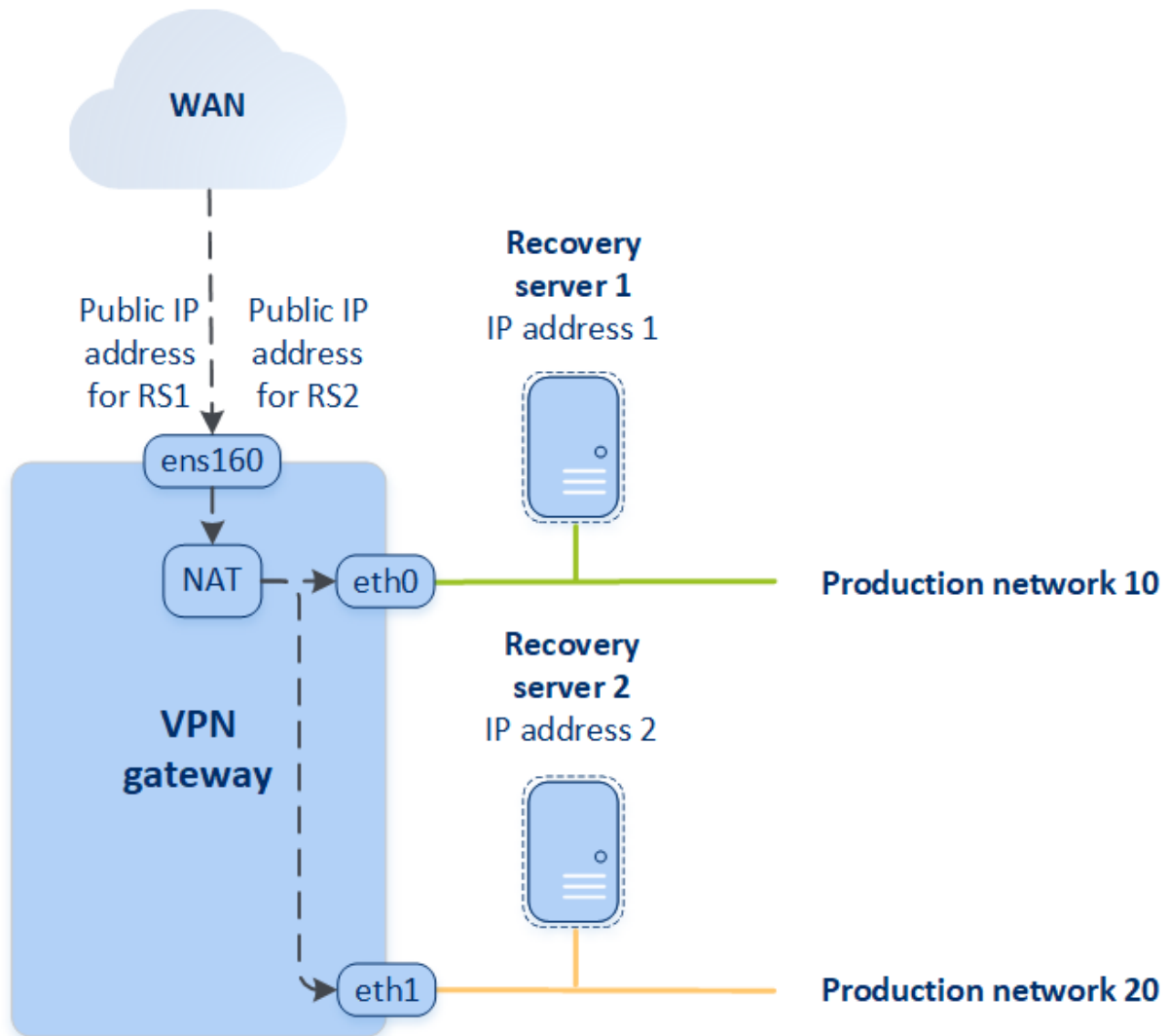
建立復原伺服器時，您必須指定下列網路參數：

- **雲端網路 (必填):**將與復原伺服器連線的雲端網路。
- **實際執行網路中的 IP 位址 (必填):**將啟動復原伺服器之虛擬機器所使用的 IP 位址。此位址同時用於實際執行網路和測試網路。啟動前,系統會設定虛擬機器以透過 DHCP 取得 IP 位址。
- **測試 IP 位址 (選擇性):**在測試容錯移轉期間,從用戶端實際執行網路存取復原伺服器所使用的 IP 位址,以防實際執行 IP 位址在相同網路中重複。此 IP 位址不同於實際執行網路中的 IP 位址。本機站台中的伺服器可以在測試容錯移轉期間,透過測試 IP 位址聯繫復原伺服器,但是無法反向進行存取。如果在復原伺服器建立期間選取 **[網際網路存取]** 選項,則可以在測試網路中從復原伺服器進行網際網路存取。
- **公共 IP 位址 (選擇性):**從網際網路存取復原伺服器所使用的 IP 位址。如果伺服器沒有公共 IP 位址,則僅能從區域網路聯繫該伺服器。
- **網際網路存取 (選擇性):**它可讓復原伺服器存取網際網路 (在實際執行和測試容錯移轉的情況下)。

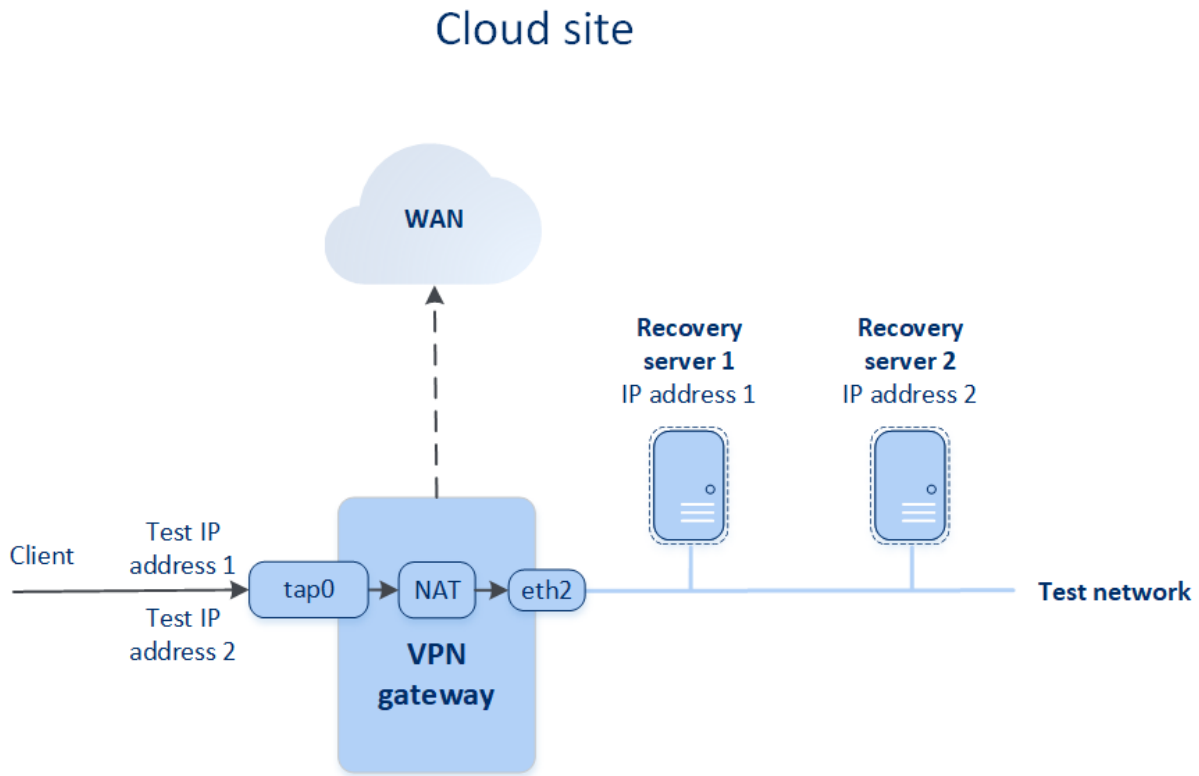
公共和測試 IP 位址

如果您在建立復原伺服器時指派公共 IP 位址,則復原伺服器會變成可以透過此 IP 位址,從網際網路使用。當具有目的地公共 IP 位址的封包來自網際網路時,VPN 閘道會使用 NAT,將其重新對應到個別的實際執行 IP 位址,然後將其傳送至對應的復原伺服器。

Cloud site



如果您在建立復原伺服器時指派測試 IP 位址，則復原伺服器會變成可以透過此 IP 位址，在測試網路中使用。如果您執行測試容錯移轉，當具有相同 IP 位址的復原伺服器在雲端的測試網路中啟動的同時，原始電腦仍在執行中。IP 位址不會發生衝突，因為測試網路遭到隔離。測試網路中的復原伺服器可透過其測試 IP 位址聯繫，這些 IP 位址會透過 NAT，重新對應到實際執行 IP 位址。



如需有關站台對站台 OpenVPN 的詳細資訊，請參閱 "附錄 A. 站台對站台 OpenVPN - 其他資訊" (第 562 頁)。

主要伺服器

主要伺服器 – 相較於復原伺服器，在本機站台上沒有連結電腦的虛擬機器。主要伺服器用於透過複寫保護應用程式，或執行各種輔助服務 (例如，網頁伺服器)。

一般而言，主要伺服器用於執行重要應用程式之伺服器之間的即時資料複寫。您應使用應用程式的原生工具，自行設定複寫。例如：可以在本機伺服器和主要伺服器之間設定 Active Directory 複寫或 SQL 複寫。

或者，主要伺服器可以包含在 AlwaysOn 可用性群組 (AAG) 或資料庫可用性群組 (DAG) 中。

這兩種方法都需要深入瞭解應用程式和系統管理員權限。主要伺服器會持續消耗快速災難復原儲存空間上的計算資源與空間。它需要您那一端的維護：監控複寫、安裝軟體更新以及備份。其優點是最小的 RPO 和 RTO，以及實際執行環境的最小負載 (相較於將整個伺服器備份到雲端而言)。

主要伺服器一律僅在實際執行網路中啟動，而且有下列網路參數：

- **雲端網路 (必填)**: 將與主要伺服器連線的雲端網路。
- **實際執行網路中的 IP 位址 (必填)**: 主要伺服器將在實際執行網路中具備的 IP 位址。根據預設，會設定您實際執行網路中的第一個可用 IP 位址。
- **公共 IP 位址 (選擇性)**: 從網際網路存取主要伺服器所使用的 IP 位址。如果伺服器沒有公共 IP 位址，則僅能從區域網路 (而無法透過網際網路) 聯繫該伺服器。
- **網際網路存取 (選擇性)**: 可讓主要伺服器存取網際網路。

多站台 IPsec VPN 連線

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以使用多站台 IPsec VPN 連線來連線單一本機站台，或透過安全的 L3 IPsec VPN 連線，將多個本機站台連線到 Cyber Disaster Recovery Cloud。

如果您有下列其中一個使用案例，此連線類型適用於災難復原情境：

- 您有一個本機站台主控重要工作負載。
- 您有多個本機站台主控重要工作負載，例如不同地點的辦公室。
- 您使用第三方軟體站台或受管理服務供應商站台，並透過 IPsec VPN 通道，連線到這些站台。

若要在本機站台和雲端站台之間建立多站台 IPsec VPN 通訊，會使用 **VPN 閘道**。當您開始在服務主控台中設定多站台 IPsec VPN 連線時，會在雲端站台中自動部署 VPN 閘道。您應該設定雲端網路區段，並確認這些區段沒有與區域網路區段重疊。系統會在本機站台和雲端站台之間建立一個安全的 VPN 通道。本機伺服器 and 雲端伺服器可以透過此 VPN 通道通訊，如同它們全都位於相同的乙太網路區段。

對於要保護的每部來源電腦，您必須在雲端站台上建立一部復原伺服器。它會維持在 **[待命]** 狀態，直到發生生容錯移轉事件為止。如果發生災難，而且您開始容錯移轉程序（在 **實際執行模式** 下），會在雲端啟動代表您受保護電腦確切複本的復原伺服器。您的用戶端可以繼續使用伺服器，而不會注意到任何背景變更。

您也可以 **在測試模式下** 啟動容錯移轉程序。也就是說，來源電腦仍在運作中，同時，個別復原伺服器會在雲端中建立之特殊虛擬網路中的雲端啟動 - **測試網路**。測試網路會加以隔離，以防其他雲端網路區段中的 IP 位址重複。

VPN 閘道

允許在本機站台和雲端站台間通訊的主要元件為 **VPN 閘道**。這是雲端中安裝特殊軟體，並專門設定網路所在的虛擬機器。VPN 閘道提供下列功能：

- 在 L3 IPsec 模式下，連線雲端中區域網路和實際執行網路的乙太網路區段。
- 當做預設路由器和 NAT 使用，以供測試和實際執行網路中的電腦使用。
- 當做 DHCP 伺服器使用。實際執行與測試網路中的所有電腦都會透過 DHCP 取得網路設定 (IP 位址、DNS 設定)。每次雲端伺服器都將從 DHCP 伺服器取得相同的 IP 位址。

如果您希望，可以設定自訂 DNS 設定。如需詳細資訊，請參閱 "設定自訂 DNS 伺服器" (第 371 頁)。

- 當做快取 DNS 使用。

路由的運作方式

使用雲端站台上的路由器執行雲端網路之間的路由，讓不同雲端網路的伺服器可以彼此通訊。

點對站台遠端 VPN 存取

注意事項

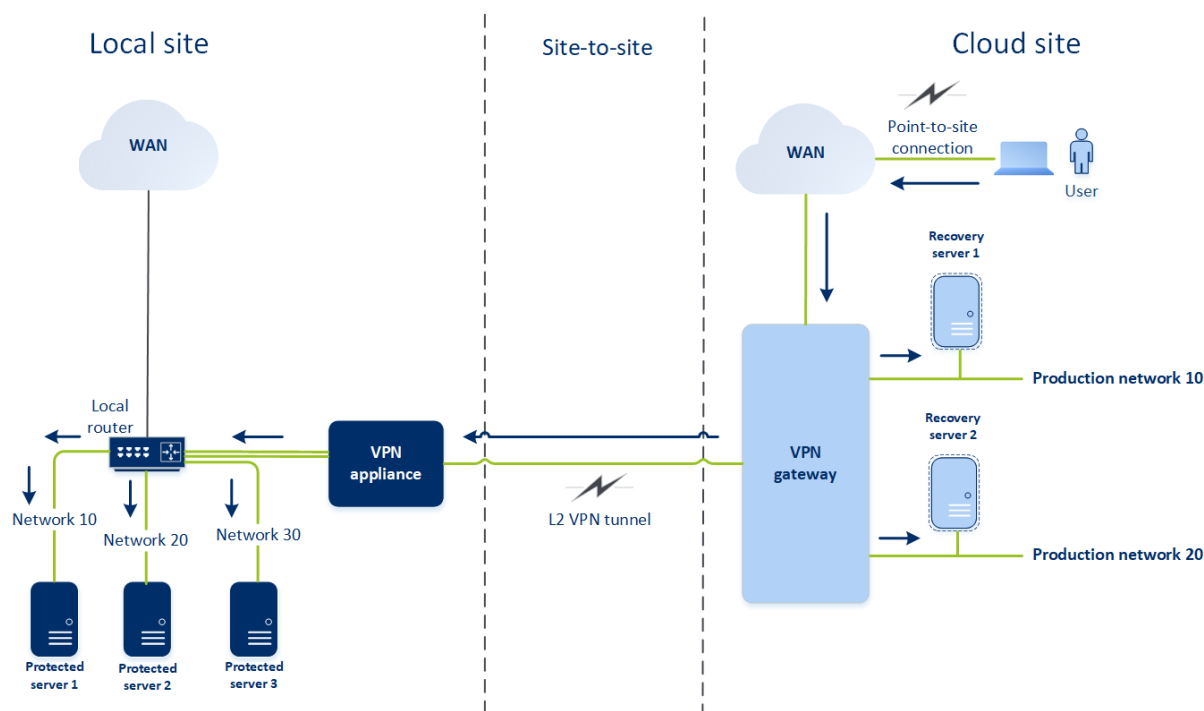
是否能夠使用此功能視您帳戶啟用的服務配額而定。

點對站台連線是一種使用端點裝置 (例如電腦或筆記型電腦), 從外部透過 VPN 對雲端站台和本機站台進行的安全連線。在您建立與 Cyber Disaster Recovery Cloud 站台的站台對站台 OpenVPN 連線之後, 即可供使用。此類型的連線在下列情況中非常有用:

- 在許多公司中, 僅能從公司網路取得公司服務和 Web 資源。您可以使用點對站台連線, 安全地連線到本機站台。
- 如果發生災難, 當工作負載切換到雲端站台, 且您的區域網路斷線時, 您可能需要直接存取雲端伺服器。這可以透過雲端站台的點對站台連線完成。

對於本機站台的點對站台連線, 您需要在本地機台上安裝 VPN 設備、設定站台對站台連線, 然後設定本地機台的點對站台連線。因此, 您的遠端員工將透過 L2 VPN 存取公司網路。

以下配置顯示本地機台、雲端站台, 以及以綠色醒目提示的伺服器間的通訊。L2 VPN 通道可連線本地機台和雲端站台。當使用者建立點對站台連線時, 會透過雲端站台對本地機台執行通訊。



點對站台設定會使用憑證向 VPN 用戶端進行驗證。此外, 使用者認證用於驗證。請注意有關本地機站台的點對站台連線的下列資訊:

- 使用者應該使用其 Cyber Cloud 認證, 在 VPN 用戶端中進行驗證。他們必須具備「公司系統管理員」或「網路保護」使用者角色。
- 如果您重新產生 OpenVPN 設定, 則您必須將更新的設定提供給使用點對站連線與雲端站台連線的所有使用者。

自動刪除雲端站台上未使用的客戶環境

災難復原服務會追蹤針對災難復原用途而建立之客戶環境的使用狀況，並在未使用時自動刪除。

下列準則用於定義客戶租用戶是否作用中：

- 目前至少有一部雲端伺服器，或者在過去七天有雲端伺服器。
或者
- 已啟用 **[本機站台的 VPN 存取]** 選項，且已建立站台對站台 OpenVPN 通道，或在過去 7 天有從 VPN 設備回報的資料。

其餘所有的租用戶都會被視為非使用中租用戶。系統會針對這類租用戶執行下列操作：

- 刪除 VPN 閘道以及與租用戶相關的所有雲端資源。
- 取消登錄 VPN 設備。

非作用中的租用戶會回復到其連線設定前的狀態。

14.7.2 初始連線設定

本節描述連線設定案例。

設定僅雲端模式

在僅雲端模式下設定連線

1. 在服務主控台中，移至 **[災難復原] > [連線]**。
2. 選擇 **[僅雲端]**，然後按一下 **[設定]**。

因此，將會在雲端站台上部署具有已定義之位址和遮罩的 VPN 閘道與雲端網路。

若要瞭解如何在雲端管理網路並設定 VPN 閘道設定，請參閱「[管理雲端網路](#)」。

設定站台對站台 OpenVPN

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

VPN 裝置的需求

系統需求

- 1 顆 CPU
- 1 GB RAM
- 8 GB 磁碟空間

連接埠

- TCP 443 (輸出) - 用於 VPN 連線
- TCP 80 (輸出) - 用於自動[更新設備](#)

請確認您的防火牆以及您網路安全性系統的其他元件允許透過這些連接埠連線到任何 IP 位址。

設定站台對站台 OpenVPN 連線

VPN 設備會將您的區域網路透過安全的 VPN 通道延伸至雲端。此類連線通常稱為「站台對站台」(S2S) 連線。您可以依照下方的程序或觀看[影片教學](#)。

透過 VPN 設備設定連線

1. 在服務主控台中，移至 **[災難復原] > [連線]**。
2. 選擇 **[站台對站台 OpenVPN 連線]**，然後按一下 **[設定]**。
系統會開始在雲端部署 VPN 閘道。這需要花費一些時間。此時，您可以繼續進行下一個步驟。

注意事項

VPN 閘道不會另外收費。如果未使用災難復原功能，則會將它刪除，也就是說，雲端會有七天沒有主要伺服器或復原伺服器。

3. 在 **[VPN 設備]** 區塊中，按一下 **[下載並部署]**。根據您所使用的虛擬化平台，下載使用，下載適用於 VMware vSphere 或 Microsoft Hyper-V 的 VPN 設備。
4. 部署設備，並將其連線至實際執行網路。
在 vSphere 中，確認已啟用 **[混合模式]** 和 **[偽造傳輸]**，並針對將 VPN 設備連線到實際執行網路的所有虛擬交換器，設定為 **[接受]**。若要存取這些設定，請在 vSphere Client 中選取主機 > **[摘要] > [網路]**，然後選取交換器 > **[編輯設定...] > [安全性]**。
在 Hyper-V 中，建立具有 1024 MB 記憶體的第 1 代虛擬機器。我們也建議為該電腦啟用**動態記憶體**。建立電腦之後，前往 **[設定] > [硬體] > [網路卡] > [進階功能]** 並選取 **[啟用 MAC 位址詐騙]** 核取方塊。
5. 開啟設備電源。
6. 開啟設備主控台，並以 "admin"/"admin" 使用者名稱和密碼登入。
7. **[選擇性步驟]** 變更密碼。
8. **[選擇性]** 如有需要，變更網路設定。定義將當做網際網路連線的 WAN 介面使用的介面。
9. 使用公司系統管理員的認證，在 Cyber Protection 服務中登錄設備。
這些認證僅能用於擷取憑證一次。資料中心 URL 是預先定義的。

注意事項

如果為您的帳戶設定雙重驗證機制，系統也將提示您輸入 TOTP 代碼。如左已啟用雙重驗證機制，但尚未為您的帳戶是定，則您無法登錄 VPN 設備。首先，您必須移至服務主控台登入頁面，並為您的帳戶完成雙重驗證機制設定。如需有關雙重驗證機制的更多詳細資訊，請參閱《[管理入口網站系統管理員指南](#)》。

設定完成之後，該設備將顯示 **[線上]** 狀態。此設備會連線到 VPN 閘道，並開始將網路相關資訊從所有作用中介面回報到 Cyber Disaster Recovery Cloud 服務。服務主控台會根據來自 VPN 設備的資訊，顯示介面。

設定多站台 IPsec VPN

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以透過下列兩種方式，設定多站台 IPsec VPN 連線：

- 從 **[災難復原] > [連線]** 索引標籤。
- 在一或數個裝置上套用保護計劃，然後從自動建立的站台對站台 OpenVPN 連線，自動切換到多站台 IPsec VPN 連線、設定多站台 IPsec VPN 設定，並重新指派 IP 位址。

從 **[連線]** 標籤設定多站台 IPsec VPN 連線

1. 在服務主控台中，移至 **[災難復原] > [連線]**。
2. 在 **[多站台 VPN 連線]** 區段中，按一下 **[設定]**。
VPN 閘道是在雲端站台上部署的。
3. [設定多站台 IPsec VPN 設定](#)。

從保護計劃設定多站台 IPsec VPN 連線

1. 在服務主控台中，移至 **[裝置]**。
2. 將保護計劃套用到清單中的一或多個裝置。
系統會針對站台對站台的 OpenVPN 連線，自動設定復原伺服器 and 雲端基礎架構設定。
3. 移至 **[災難復原] > [連線]**。
4. 按一下 **[顯示屬性]**。
5. 按一下 **[切換到多站台 IPsec VPN]**。
6. [設定多站台 IPsec VPN 設定](#)。
7. 針對雲端網路和雲端伺服器，[重新指派 IP 位址](#)。

設定多站台 IPsec VPN 設定

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

設定多站台 IPsec VPN 之後，您必須在 **[災難復原] > [連線]** 索引標籤上設定雲端站台和本機站台設定。

14.7.3 必要條件

- 已設定多站台 IPsec VPN 連線。如需有關設定多站台 IPsec VPN 連線的詳細資訊，請參閱 "設定多站台 IPsec VPN" (第 359 頁)。
- 每個本機 IPsec VPN 閘道的公共 IP 位址。

- 將雲端網路規劃成具備足夠的 IP 位址，以供作為受保護電腦複本的雲端伺服器 (在實際執行網路中) 以及復原伺服器 (根據您的需求，擁有一或兩個 IP 位址) 使用。
- 如果您在本機站台和雲端站台之間使用防火牆，則必須在本機站台上允許下列 IP 通訊協定和 UDP 連接埠：IP 通訊協定 ID 50 (ESP)、UDP 連接埠 500 (IKE) 和 UDP 連接埠 4500。

設定多站台 IPsec VPN 連線

1. 將一或多個網路新增到雲端站台。

- a. 按一下 **[新增網路]**。

注意事項

新增雲端網路時，系統將會自動新增擁有相同網路位址和遮罩的對應測試網路，以執行測試容錯移轉。測試網路中的雲端伺服器與雲端實際執行網路中的雲端伺服器擁有相同的 IP 位址。如果您需要在測試容錯移轉期間，從實際執行網路存取雲端伺服器，請在建立復原伺服器時，為其指派另一個測試 IP 位址。

- b. 在 **[網路位址]** 欄位中，輸入網路的 IP 位址。
 - c. 在 **[網路遮罩]** 欄位中，輸入網路的遮罩。
 - d. 按一下 **[新增]**。
2. 依照適用於本機站台的建議，為您希望連線到雲端站台的每個本機站台進行設定。如需有關這些建議的詳細資訊，請參閱 "對於本機站台的一般建議" (第 361 頁)。
 - a. 按一下 **[新增連線]**。
 - b. 輸入本機 VPN 閘道的名稱。
 - c. 輸入本機 VPN 閘道的公共 IP 位址。
 - d. **[選用]** 輸入本機 VPN 閘道的描述。
 - e. 按 **[下一步]**。
 - f. 在 **[預先共用金鑰]** 欄位中，輸入預先共用金鑰，或按一下 **[產生新的預先共用金鑰]**，使用自動產生的值。

注意事項

您必須為本機和雲端 VPN 閘道使用相同的預先共用金鑰。

- g. 按一下 **[IPsec/IKE 安全性設定]** 以進行設定。如需有關您可以進行之設定的詳細資訊，請參閱 "IPsec/IKE 安全性設定" (第 361 頁)。

注意事項

您可以使用自動填入的預設設定，或使用自訂值。僅支援 IKEv2 通訊協定連線。建立 VPN 時的預設 **[啟動動作]** 為 **[新增]** (您的本機 VPN 閘道會起始連線)，但是您可以將其變更為 **[啟動]** (雲端 VPN 閘道會起始連線) 或 **[路由]** (適用於支援路由選項的防火牆)。

- h. 設定 **[網路政策]**。
網路政策會指定 IPsec VPN 所連線的網路。使用 CIDR 格式，輸入網路的 IP 位址和遮罩。區域網路區段和雲端網路區段不應重疊。
- i. 按一下 **[儲存]**。

對於本機站台的一般建議

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

當您為多站台 IPsec VPN 連線設定本機站台時，請考慮下列建議：

- 針對每個 IKE 階段，請為下列參數設定至少一個在雲端站台中設定的值：加密演算法、雜湊演算法以及 Diffie-Hellman 群組號碼。
- 針對為 IKE 階段 2 在雲端站台中設定的 Diffie-Hellman 群組號碼，使用至少其中一個值，啟用 [完整轉寄密碼]。
- 針對 IKE 階段 1 和 IKE 階段 2，為 [存留時間] 設定與雲端站台中相同的值。
- 請注意，[啟動動作] 設定可定義哪一端起始連線。預設值 **[新增]** 意指本機站台起始連線，而雲端站台正在等待連線起始。如果您希望雲端站台起始連線，請將值變更為 **[啟動]**；如果您希望兩端都能夠起始連線（適用於支援路由選項的防火牆），則將該值變更為 **[路由]**。

如需詳細資訊以及不同解決方案的設定範例，請參閱：

- [本系列的知識庫文章](#)
- [本影片範例](#)

IPsec/IKE 安全性設定

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

下表提供有關 IPsec/IKE 安全性參數的詳細資訊。

參數	描述
加密演算法	將用於確保在傳輸中無法檢視資料的加密演算法。預設會選擇所有演算法。您必須在本機閘道裝置上，針對每個 IKE 階段設定至少其中一個所選演算法。
雜湊演算法	將用於驗證資料完整性和真實性的雜湊演算法。預設會選擇所有演算法。您必須在本機閘道裝置上，針對每個 IKE 階段設定至少其中一個所選演算法。
Diffie-Hellman 群組號碼	Diffie-Hellman 群組號碼可定義網際網路金鑰交換 (IKE) 程序中使用之金鑰的強度。 群組號碼越高越安全，但是需要額外的時間讓金鑰運算。 預設會選擇所有群組。您必須在本機閘道裝置上，針對每個 IKE 階段設定至少其中一個所選群組。

參數	描述
存留時間 (秒)	存留時間值可透過使用者封包的一組加密/驗證金鑰，決定從成功交涉到過期的連線執行個體持續時間。 階段 1 的範圍：900-28800 秒，預設為 28800。 階段 2 的範圍：900-3600 秒，預設為 3600。 階段 2 的存留時間必須小於階段 1 的存留時間。 連線會在過期之前，透過金鑰處理通道進行重新交涉，請參閱重設金鑰寬限時間。如果本機和遠端的存留時間不一致，則存留時間較長的那一端將會發生替換連線的混亂情況。另請參閱重設金鑰寬限時間和重設金鑰模糊資料。
重設金鑰寬限時間 (秒)	連線過期或金鑰處理通道過期之前的寬限時間，在此期間內，VPN 連線的本機端會嘗試交涉替換。系統會根據重設金鑰模糊資料的值，隨機選擇重設金鑰的確切時間。僅在本機相關，遠端無需對此達成共識。範圍：900-3600 秒。預設值為 3600。
重新執行視窗大小 (封包)	此連線的 IPsec 重新執行視窗大小。 預設值 -1 使用在 strongswan.conf 檔案中，以 charon.replay_window 設定的值。 只有在使用 Netlink 後端時，才支援大於 32 的值。 值為 0 時，會停用 IPsec 重新執行保護。
重設金鑰模糊資料 (%)	隨機增加寬限位元組、寬限封包和寬限時間的百分比上限以隨機選擇重設金鑰間隔 (對於具有許多連線的主機很重要)。 重設金鑰模糊資料值可以超過 100%。marginTYPE 的值在隨機增加之後，不得超過 lifeTYPE，其中 TYPE 是其中一個位元組 (封包或時間)。 值為 0% 時，會停用隨機選擇。僅在本機相關，遠端無需對此達成共識。
DPD 逾時 (秒)	發生無作用對等偵測 (DPD) 逾時前等待的時間。您可以將值指定為 30 或更高。預設值為 30。
無作用對等偵測 (DPD) 逾時動作	無作用對等偵測 (DPD) 逾時發生後採取的動作。 重新啟動 - DPD 逾時發生時，重新啟動工作階段。 清除 - DPD 逾時發生時，結束工作階段。 無 - DPD 逾時發生時，不採取任何動作。
啟動動作	決定哪一端起始連線，並為 VPN 連線建立通道。

參數	描述
	新增 - 您的本機 VPN 閘道會起始連線。 啟動 - 雲端 VPN 閘道會起始連線。 路由 - 適用於支援路由選項的 VPN 閘道。只有在存在從本機 VPN 閘道或雲端 VPN 閘道起始的流量時，通道才會啟動。

對於 Active Directory 網域服務可用性的建議

如果受保護的工作負載需要在網域控制站中進行驗證，建議您在災難復原站台擁有 Active Directory 網域控制站 (AD DC) 執行個體。

適用於 L2 OpenVPN 連線的 Active Directory 網域控制站

使用 L2 OpenVPN 連線時，受保護工作負載的 IP 位址在測試容錯移轉或實際執行容錯移轉期間，會保留在雲端站台中。因此，測試容錯移轉或實際執行容錯移轉期間的 AD DC 與本機站台的 AD DC 具有相同的 IP 位址。

您可以透過自訂 DNS，為所有雲端伺服器設定您自己的自訂 DNS 伺服器。如需詳細資訊，請參閱 "設定自訂 DNS 伺服器" (第 371 頁)。

適用於 L3 IPsec VPN 連線的 Active Directory 網域控制站

使用 L3 IPsec VPN 連線時，受保護工作負載的 IP 位址不會保留在雲端站台中。因此，建議您在執行實際執行容錯移轉之前，先具備其他專用的 AD DC 執行個體，作為雲端站台中的主要伺服器。

對於設定為雲端站台中主要伺服器的專用 AD DC 執行個體，其建議如下：

- 關閉 Windows 防火牆。
- 將主要伺服器加入至 Active Directory 服務。
- 確認主要伺服器可存取網際網路。
- 新增 Active Directory 功能。

您可以透過自訂 DNS，為所有雲端伺服器設定您自己的自訂 DNS 伺服器。如需詳細資訊，請參閱 "設定自訂 DNS 伺服器" (第 371 頁)。

設定點對站台遠端 VPN 存取

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

如果您需要從遠端連線到本機站台，可以設定本機站台的點對站台連線。您可以依照下方的程序或觀看影片教學。

必要條件

- 已設定站台對站台 OpenVPN 連線。
- 已在本機站台上安裝 VPN 設備。

設定本機站台的點對站台連線

1. 在服務主控台中，移至 **[災難復原] > [連線]**。
2. 按一下 **[顯示屬性]**。
3. 啟用 **[本機站台的 VPN 存取]** 選項。
4. 確認需要建立本機站台的點對站台連線的使用者：
 - 在 Cyber Cloud 中擁有使用者帳戶。這些認證在 VPN 用戶端中用於驗證。否則，請在 [Cyber Cloud](#) 中建立使用者帳戶。
 - 具備「公司系統管理員」或「網路保護」使用者角色。
5. 設定 OpenVPN 用戶端：
 - a. 從下列位置下載 OpenVPN 用戶端 2.4.0 版或更新版本：<https://openvpn.net/community-downloads/>。
 - b. 將 OpenVPN 用戶端安裝在您要連線到本機站台的來源電腦上。
 - c. 按一下 **[下載 OpenVPN 的設定]**。設定檔適用於貴組織中擁有「公司系統管理員」或「網路保護」使用者角色的使用者。
 - d. 將已下載的設定匯入 OpenVPN。
 - e. 使用 Cyber Cloud 使用者認證，登入 OpenVPN 用戶端 (請參閱上述的步驟 4)。
 - f. [選擇性] 如果針對貴組織啟用雙重驗證機制，則您應該提供產生的一次性 TOTP 代碼。

重要事項

如果為您的帳戶啟用雙重驗證機制，您需要重新產生設定檔，並為您現有的 OpenVPN 用戶端更新設定檔。使用者必須重新登入 Cyber Cloud，才能為其帳戶設定雙重驗證機制。

因此，您的使用者將可以連線到本機站台上的電腦。

14.7.4 網路管理

本節描述網路管理案例。

管理網路

注意事項

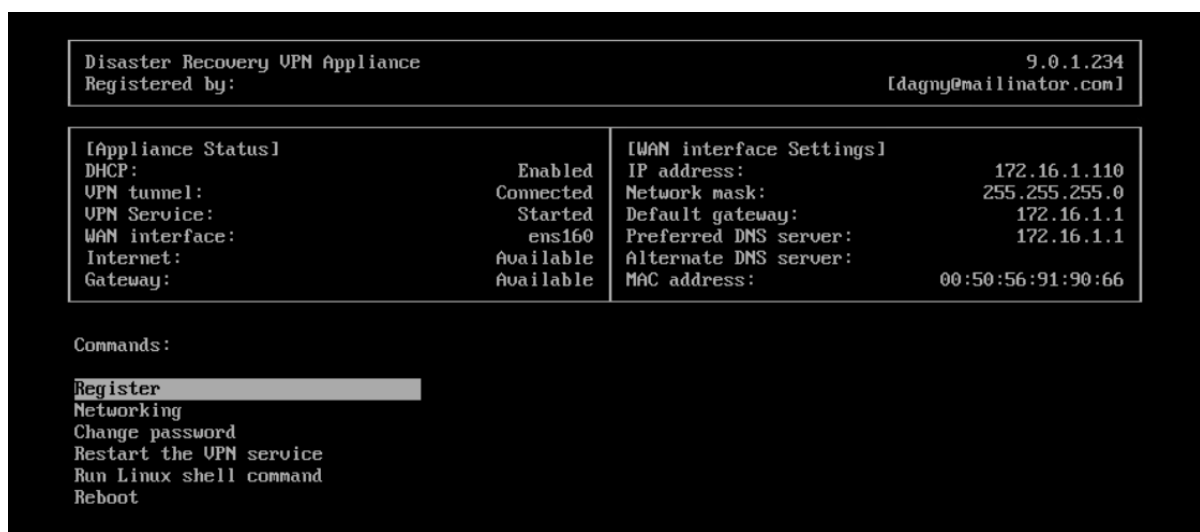
部分功能可能需要額外的授權，端視適用的授權模型而定。

站台對站台 OpenVPN 連線

若要在本機站台上新增網路，並將其延伸到雲端

1. 在 VPN 設備上，使用您要在雲端延伸的區域網路，設定新的網路介面。
2. 登入 VPN 設備主控台。

3. 在 **[網路]** 區段中，設定新介面的網路設定。



VPN 設備會開始將網路相關資訊從所有作用中介面回報到 Cyber Disaster Recovery Cloud。服務主控台會根據來自 VPN 設備的資訊，顯示介面。

若要刪除延伸至雲端的網路

1. 登入 VPN 設備主控台。
2. 在 **[網路]** 區段中，選取您要刪除的介面，然後按一下 **[清除網路設定]**。
3. 確認作業。

因此，透過安全的 VPN 通道延伸至雲端的區域網路將會遭到停止。此網路將會當做獨立的雲端區段運作。如果使用此介面從雲端站台傳遞流量或將流量傳遞到雲端站台，將會中斷與雲端站台的網路連線。

若要變更網路參數

1. 登入 VPN 設備主控台。
2. 在 **[網路]** 區段中，選取您要編輯的介面。
3. 按一下 **[編輯網路設定]**。
4. 選取下列其中一個可能的選項：
 - 若要透過 DHCP 自動設定網路，按一下 **[使用 DHCP]**。確認作業。
 - 若要手動設定網路，按一下 **[設定靜態 IP 位址]**。以下是可用於編輯的設定：
 - **IP 位址**：區域網路中介面的 IP 位址。
 - **VPN 閘道 IP 位址**：為網路的雲端區段保留的特殊 IP 位址，以便讓 Cyber Disaster Recovery Cloud 服務正常運作。
 - **網路遮罩**：區域網路的網路遮罩。
 - **預設閘道**：本機站台的預設閘道。
 - **慣用的 DNS 伺服器**：本機站台上的主要 DNS 伺服器。
 - **替代的 DNS 伺服器**：本機站台上的次要 DNS 伺服器。

```
Disaster Recovery VPN Appliance
Registered by:
9.0.1.234
[ldagny@mailinator.com]

Command: Networking \ configure ens160

Usage:
<Up>, <Down> - to select parameter
<Esc> - to cancel the command

IP address:
VPN gateway IP address:
Network mask:
Default gateway:
Preferred DNS server:
Alternate DNS server:
```

- 請進行必要的變更，然後按 Enter 鍵確認。

僅雲端模式

您在雲端最多可以擁有 23 個網路。

若要新增雲端網路

1. 移至 **[災難復原] > [連線]**。
2. 在 **[雲端站台]** 上，按一下 **[新增雲端網路]**。
3. 定義雲端網路參數：網路位址和遮罩。準備就緒後，按一下 **[完成]**。

因此，將會在雲端站台上建立具有已定義之位址和遮罩的其他雲端網路。

若要刪除雲端網路

注意事項

如果雲端網路中至少有一部雲端伺服器，則無法刪除該網路。首先，刪除雲端伺服器，然後再刪除網路。

1. 移至 **[災難復原] > [連線]**。
2. 在 **[雲端站台]** 上，按一下您要刪除的網路位址。
3. 按一下 **[刪除]** 以確認作業。

若要變更雲端網路參數

1. 移至 **[災難復原] > [連線]**。
2. 在 **[雲端站台]** 上，按一下您要編輯的網路位址。
3. 按一下 **[編輯]**。
4. 定義網路位址和遮罩，然後按一下 **[完成]**。

IP 位址重新設定

為獲得適當的災難復原效能，指派給本機伺服器和雲端伺服器的 IP 位址必須一致。如果 IP 位址有任何不一致或不相符，您將會在 **[災難復原] > [連線]** 中對應網路的旁邊看到一個驚嘆號。

IP 位址不一致的部分常見原因列在下方：

1. 復原伺服器從一個網路移轉到另一個網路，或者雲端網路的網路遮罩遭到變更。因此，雲端伺服器的 IP 位址來自未連線的網路。
2. 連線類型從沒有站台對站台連線切換到站台對站台連線。因此，本機伺服器置於不同於針對雲端站台上的復原伺服器而建立的網路。
3. 連線類型從站台對站台 OpenVPN 切換到多站台 IPsec VPN，或從多站台 IPsec VPN 切換到站台對站台 OpenVPN。如需有關此案例的詳細資訊，請參閱[切換連線](#)和[重新指派 IP 位址](#)。
4. 在 VPN 設備站台上編輯下列網路參數：
 - 透過網路設定新增介面
 - 透過介面設定手動編輯網路遮罩
 - 透過 DHCP 編輯網路遮罩
 - 透過介面設定手動編輯網位址和路遮罩
 - 透過 DHCP 編輯網路遮罩和位址

上列動作的結果是，雲端站台上的網路可能會變成區域網路的子集或超集，或者 VPN 設備介面可能會針對不同的介面回報相同的網路設定。

若要解決網路設定的問題

1. 按一下需要 IP 位址重新設定的網路。

您將會一份所選網路中伺服器、其狀態以及 IP 位址的清單。其網路設定不一致的伺服器會以驚嘆號標示。
2. 若要變更伺服器的網路設定，按一下 **[前往伺服器]**。若要一次變更所有伺服器的網路設定，按一下通知區塊中的 **[變更]**。
3. 如有需要，請在 **[新 IP]** 和 **[新的測試 IP]** 欄位中進行變更，以變更 IP 位址。
4. 準備就緒後，按一下 **[確認]**。

將伺服器移至合適的網路

當您建立災難復原保護計劃，並將其套用到選取的裝置時，系統會檢查裝置 IP 位址，如果沒有 IP 位址適用的現有雲端網路，就會自動建立雲端網路。預設將會使用 IANA 建議的最大範圍，設定私人用途的雲端網路 (10.0.0.0/8、172.16.0.0/12、192.168.0.0/16)。您可以透過編輯網路遮罩來縮小網路的範圍。

如果選取的裝置位於多個區域網路上，則雲端站台上的網路將會變成區域網路的超集。在此情況下，若要重新設定雲端網路：

1. 按一下需要重新設定網路大小的雲端網路，然後按一下 **[編輯]**。
2. 使用正確的設定，重新設定網路大小。
3. 建立其他所需的網路。
4. 按一下連線到網路的裝置數量旁邊的通知圖示。
5. 按一下 **[移至合適的網路]**。
6. 選擇您想要移至合適網路的伺服器，然後按一下 **[移動]**。

管理 VPN 設備設定

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

在服務主控台 ([**災難復原**] > [**連線**]) 中，您可以：

- 下載記錄檔。
- 取消登錄設備 (如果您需要重設 VPN 設備設定或切換到僅雲端模式)。

若要存取這些設定，請按一下 [**VPN 設備**] 區塊中的 **i** 圖示。

在 VPN 設備主控台中，您可以：

- 變更設備的密碼。
- 檢視/變更網路設定，並定義將當做網際網路連線的 WAN 使用的介面。
- 註冊/變更註冊帳戶 (透過重複註冊)。
- 重新啟動 VPN 服務。
- 重新啟動 VPN 設備。
- 執行 Linux 殼層命令 (僅適用於進階疑難排解情況)。

重新安裝 VPN 閘道

如果有您無法解決的 VPN 閘道問題，您可能需要重新安裝 VPN 閘道。可能的問題包括：

- VPN 閘道處於 [**錯誤**] 狀態。
- VPN 閘道長時間處於 [**等候中**] 狀態。
- VPN 閘道狀態長時間未確定。

重新安裝 VPN 閘道程序包括下列自動動作：完全刪除現有的 VPN 閘道虛擬機器、從範本安裝新的虛擬機器，然後在新的虛擬機器上套用先前 VPN 閘道的設定。

必要條件：

必須設定雲端站台的其中一個連線類型。

若要重新安裝 VPN 閘道

1. 在 Cyber Protection 服務主控台中，移至 [**災難復原**] > [**連線**]。
2. 按一下 VPN 閘道的齒輪圖示，然後選擇 [**重新安裝 VPN 閘道**]。
3. 在 [**重新安裝 VPN 閘道**] 對話方塊中，輸入您的登入資料。
4. 按一下 [**重新安裝**]。

啟用和停用站台對站台連線

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

在下列情況下，您可以啟用站台對站台連線：

- 如果您需要雲端站台上的雲端伺服器與本機站台上的伺服器通訊。
- 容錯移轉至雲端之後，會復原本機基礎架構，而且您會想要將伺服器容錯回復至本機站台。

若要啟用站台對站台連線

1. 移至 **[災難復原] > [連線]**。
2. 按一下 **[顯示屬性]**，然後啟用 **[站台對站台連線]** 選項。

因此會在本機站台和雲端站台之間啟用站台對站台 VPN 連線。Cyber Disaster Recovery Cloud 服務會從 VPN 設備取得網路設定，並將區域網路延伸至雲端站台。

如果您不需要雲端站台上的雲端伺服器與本機站台上的伺服器通訊，您可以停用站台對站台連線。

若要停用站台對站台連線

1. 移至 **[災難復原] > [連線]**。
2. 按一下 **[顯示屬性]**，然後停用 **[站台對站台連線]** 選項。

因此，本機站台將與雲端站台中斷連線。

切換站台對站台連線類型

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以輕鬆地從站台對站台 OpenVPN 連線切換到多站台 IPsec VPN 連線，也可以輕鬆地從多站台 IPsec VPN 連線切換到站台對站台 OpenVPN 連線。

當您切換連線類型時，作用中的 VPN 連線會遭到刪除，但是會保留雲端伺服器和網路設定。但是，您仍然需要重新指派雲端網路和伺服器的 IP 位址。

下表比交站台對站台 OpenVPN 連線與多站台 IPsec VPN 連線的基本特性。

	站台對站台 OpenVPN	多站台 IPsec VPN
本機站台支援	單一	單一、多個
VPN 開道模式	L2 Open VPN	L3 IPsec VPN
網路區段	將區域網路延伸到雲端網路	區域網路區段和雲端網路區段不應重疊
支援本機站台的點對站台存取	是	否
支援雲端站台的點對站台存取	是	是
需要公共 IP 產品項目	否	是

從站台對站台 OpenVPN 連線切換到多站台 IPsec VPN 連線

1. 在服務主控台中, 移至 **[災難復原] > [連線]**。
2. 按一下 **[顯示屬性]**。
3. 按一下 **[切換到多站台 IPsec VPN]**。
4. 按一下 **[重新設定]**。
5. 針對雲端網路和雲端伺服器, **重新指派 IP 位址**。
6. **設定多站台 IPsec 連線設定**。

從多站台 IPsec VPN 連線切換到站台對站台 OpenVPN 連線

1. 在服務主控台中, 移至 **[災難復原] > [連線]**。
2. 按一下 **[顯示屬性]**。
3. 按一下 **[切換到站台對站台 OpenVPN]**。
4. 按一下 **[重新設定]**。
5. 針對雲端網路和雲端伺服器, **重新指派 IP 位址**。
6. **設定切換站台對站台連線設定**。

重新指派 IP 位址

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

在下列情況下, 您必須重新指派雲端網路和雲端伺服器的 IP 位址以完成設定:

- 從站台對站台 OpenVPN 切換到多站台 IPsec VPN, 或從多站台 IPsec VPN 切換到站台對站台 OpenVPN 之後。
- 套用保護計劃之後 (如果已設定多站台 IPsec VPN 連線)。

重新指派雲端網路的 IP 位址

1. 在 **[連線]** 索引標籤中, 按一下雲端網路的 IP 位址。
2. 在 **[網路]** 快顯視窗中, 按一下 **[編輯]**。
3. 輸入新的網路位址和網路遮罩。
4. 按一下**[完成]**。

重新指派雲端網路的 IP 位址之後, 您必須重新指派屬於重新指派之雲端網路的雲端伺服器。

重新指派伺服器的 IP 位址

1. 在 **[連線]** 索引標籤中, 按一下伺服器在雲端網路中的 IP 位址。
2. 在 **[伺服器]** 快顯視窗中, 按一下 **[變更 IP 位址]**。
3. 在 **[變更 IP 位址]** 快顯視窗中, 輸入伺服器的新 IP 位址, 或使用自動產生的 IP 位址 (重新指派的雲端網路一部分)。

注意事項

Cyber Disaster Recovery Cloud 會將雲端網路中的 IP 位址自動指派給雲端網路所屬的所有雲端伺服器，然後再重新指派網路 IP 位址。您可以使用建議的 IP 位址，一次重新指派所有雲端伺服器的 IP 位址。

4. 按一下 **[確認]**。

設定自訂 DNS 伺服器

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

當您設定連線時，Cyber Disaster Recovery Cloud 會建立雲端網路基礎架構。雲端 DHCP 伺服器會將預設 DNS 伺服器自動指派給復原伺服器和主要伺服器，但是您可以變更預設設定，並設定自訂 DNS 伺服器。新的 DNS 設定將在下次對 DHCP 伺服器提出要求時套用。

必要條件：

必須設定雲端站台的其中一個連線類型。

設定自訂 DNS 伺服器

1. 在服務主控台中，移至 **[災難復原] > [連線]**。
2. 按一下 **[顯示屬性]**。
3. 按一下 **[預設 (雲端站台所提供)]**。
4. 選擇 **[自訂伺服器]**。
5. 輸入 DNS 伺服器的 IP 位址。
6. [選擇性] 如果您想要新增其他 DNS 伺服器，按一下 **[新增]**，然後輸入 DNS 伺服器 IP 位址。

注意事項

新增自訂 DNS 伺服器之後，您也可以新增預設 DNS 伺服器。如此一來，如果自訂 DNS 伺服器無法使用，Cyber Disaster Recovery Cloud 將使用預設 DNS 伺服器。

7. 按一下 **[完成]**。

刪除自訂 DNS 伺服器

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以從自訂 DNS 清單刪除 DNS 伺服器。

必要條件：

已設定自訂 DNS 伺服器。

刪除自訂 DNS 伺服器

1. 在服務主控台中，移至 **[災難復原] > [連線]**。
2. 按一下 **[顯示屬性]**。
3. 按一下 **[自訂伺服器]**。
4. 按一下 DNS 伺服器旁的刪除圖示。

注意事項

只有一個自訂 DNS 伺服器可用時，才會停用刪除作業。如果您要刪除所有自訂 DNS 伺服器，選擇 **[預設 (雲端站台所提供)]**。

5. 按一下 **[完成]**。

設定本機路由

除了透過 VPN 設備延伸到雲端的區域網路之外，您可以擁有未在 VPN 設備中登錄，但其中的伺服器必須與雲端伺服器通訊的其他區域網路。若要建立這類本機伺服器和雲端伺服器間的連線，您需要設定本機路由設定。

若要設定本機路由

1. 移至 **[災難復原] > [連線]**。
2. 按一下 **[顯示屬性]**，然後按一下 **[本機路由]**。
3. 以 CIDR 標記法指定區域網路。
4. 按一下 **[儲存]**。

因此，來自指定之區域網路的伺服器可以與雲端伺服器通訊。

允許透過 L2 VPN 的 DHCP 流量

如果本機站台上的裝置是從 DHCP 伺服器取得其 IP 位址，您可以使用災難復原保護 DHCP 伺服器，將其容錯移轉至雲端，然後允許 DHCP 流量透過 L2 VPN 執行。因此，您的 DHCP 伺服器將在雲端上執行，但會繼續將 IP 位址指派給本機裝置。

必要條件：

必須設定雲端的站台對站台 L2 VPN 連線類型。

若要允許透過 L2 VPN 連線的 DHCP 流量

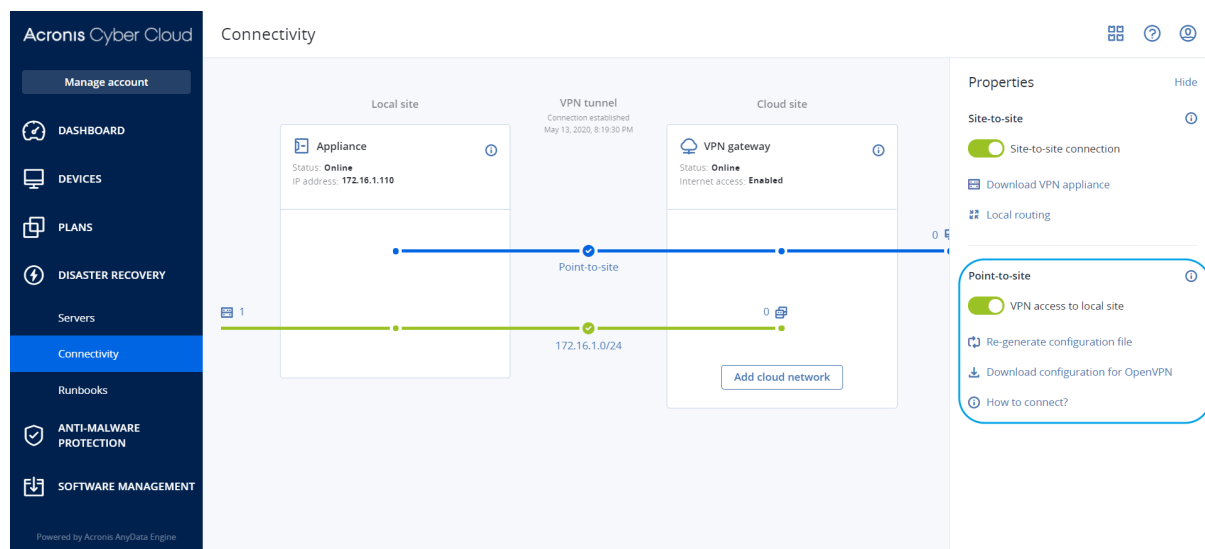
1. 移至 **[災難復原] > [連線]** 索引標籤。
2. 按一下 **[顯示屬性]**。
3. 啟用 **[允許透過 L2 VPN 的 DHCP 流量]** 開關。

管理點對站台連線設定

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

在服務主控台中，移至 **[災難復原] > [連線]**，然後按一下右上角的 **[顯示屬性]**。



本機站台的 VPN 存取

此選項用於管理對本機站台的 VPN 存取。預設為啟用狀態。如果遭到停用，將不允許對本機站台的點對站台存取。

下載 OpenVPN 的設定

這會下載 OpenVPN 用戶端的設定檔。若要建立與雲端站台的點對站台連線，需要這個檔案。

重新產生設定

您可以重新產生 OpenVPN 用戶端的設定檔。

在下列情況下，這是必要的：

- 如果您懷疑設定檔已損壞。
- 如果您的帳戶已啟用雙重驗證機制。

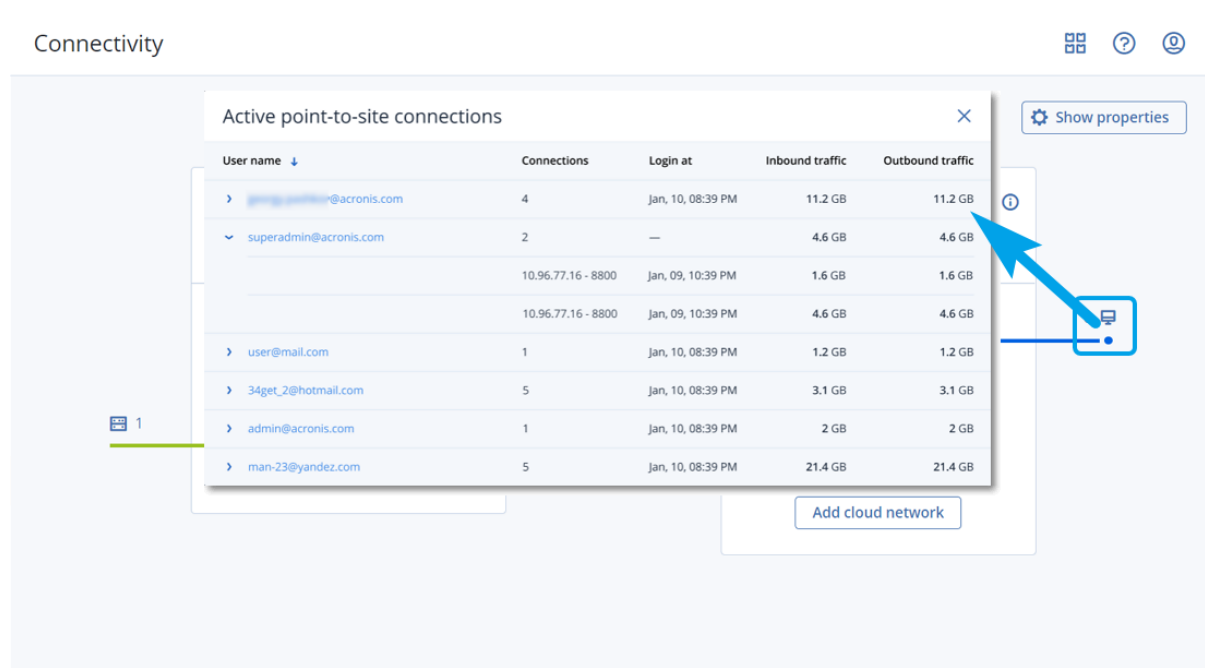
當設定檔更新之後，將無法透過舊的設定檔連線。確認將新檔案散發給獲允許使用點對站台連線的使用者。

作用中的點對站台連線

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以在 **[災難復原] > [連線]** 中檢視所有作用中的點對站台連線。按一下 **點對站台** 藍線上的電腦圖示，您將會看到依使用者名稱分組的作用中點對站台連線的詳細資訊。



疑難排解 IPsec VPN 設定

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

當您設定或使用 IPsec VPN 連線時，可能會遇到問題。

您可以在 IPsec 記錄檔中深入瞭解您所遇到的問題，並查閱「疑難排解 IPsec VPN 設定問題」主題，以找出部分可能會發生的常見問題的可能解決方案。

疑難排解 IPsec VPN 設定問題

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

下表描述最常發生的 IPsec VPN 設定問題，並說明其疑難排解方式。

問題	可能的解決方案
我看到下列錯誤訊息： IKE 第 1 階段交涉錯誤。請檢查雲端和本機站台上的 IPsec IKE 設定。	按一下 [重試] ，然後確認是否出現更具體的錯誤訊息。例如，更具體的錯誤訊息可能是關於演算法不相符或預先共用金鑰不正確的錯誤訊息。

問題	可能的解決方案
	注意事項 基於安全性，下列限制適用於 IPsec VPN 連線： - 在 RFC8247 中需要取代 IKEv1，而且因為安全性風險的緣故而不受支援。僅支援 IKEv2 通訊協定連線。 - 下列加密演算法不被視為安全，因此不受支援：DES 與 3DES。 - 下列雜湊演算法不被視為安全，因此不受支援：SHA1 與 MD5。 - Diffie-Hellman 群組號碼 2 不被視為安全，因此不受支援。
我的本機站台和雲端站台之間的連線維持在 [正在連線] 狀態。	檢查： - 是否已開放 UDP 連接埠 500 (當您使用防火牆時)。 - 本機站台和雲端站台之間的連線。 - 本機站台的 IP 位址是否正確。
我的本機站台和雲端站台之間的連線維持在 [正在等候連線] 狀態。	當雲端站台的 [啟動動作] 設定為 [新增] (亦即，雲端站台正在等候本機站台起始連線) 時，您會看到這個狀態。 從本機站台起始連線。
我的本機站台和雲端站台之間的連線維持在 [正在等候流量] 狀態。	當雲端站台的 [啟動動作] 設定為 [路由] 時，您會看到這個狀態。 如果您希望從本機站台起始連線，請執行下列操作： - 嘗試從本機站台 Ping 雲端站台中的虛擬機器。這是為某些裝置建立通道所需的標準行為，例如 Cisco ASA。(路由模式) - 請確認本機站台已透過將本機站台的 [啟動動作] 設定為 [啟動] 來建立通道。
我的本機站台和雲端站台之間的連線已建立，但是我可以看到其中一或多個網路政策已關閉。	此問題可能是由於下列原因所造成： - 雲端 IPsec 站台的網路對應與本機站台的網路對應不同。 請確認本機站台和雲端站台的網路對應和網路政策順序完全相符。 - 當本機站台和/或雲端站台的 [啟動動作] 設定為 [路由] (例如，在 Cisco ASA 裝置上)，而且目前沒有流量時，此狀態是正確的。您可以嘗試 Ping 以確認是否已建立通道。如果 Ping 沒有作用，請檢查本機站台和雲端站台的網路對應。

問題	可能的解決方案
我想要重新啟動特定的 IPsec 連線。	重新啟動特定的 IPsec 連線： 1. 在 [災難復原] > [連線] 畫面中，按一下 IPsec 連線。 2. 按一下 [停用連線]。 3. 再按一下 IPsec 連線。 4. 按一下 [啟用連線]。

下載 IPsec VPN 記錄檔

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以在 VPN 伺服器上的記錄檔中，找到 IPsec 連線的其他資訊。記錄檔會壓縮成您可以下載並解壓縮的 .zip 存檔。

14.7.5 必要條件

已設定多站台 IPsec VPN 連線。

下載包含記錄檔的 .zip 存檔

1. 在服務主控台中，移至 **[災難復原] > [連線]**。
2. 按一下雲端站台 VPN 閘道旁的齒輪圖示。
3. 按一下 **[下載記錄檔]**。

多站台 IPsec VPN 記錄檔

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

以下清單提供 zip 存檔中 IPsec VPN 記錄檔的詳細資訊以及這些記錄檔所含的資訊。

- ip.txt - 此檔案包含網路介面設定中的記錄。您必須看到兩個 IP 位址：公共 IP 位址和本機 IP 位址。如果您在記錄中看不到這些 IP 位址，則表示有問題。請聯絡支援小組。

注意事項

公共 IP 位址的遮罩必須是 32。

- swanctl-list-loaded-config.txt - 此檔案包含所有 IPsec 站台的相關資訊。
如果您在檔案中看不到站台，則表示未套用 IPsec 設定。請嘗試更新設定並加以儲存，或聯絡支援小組。
- swanctl-list-active-sas.txt - 此檔案包含處於作用中或正在連線狀態的連線和政策。

14.8 設定復原伺服器

本節描述容錯移轉和容錯回復、建立復原伺服器，以及災難復原作業的概念。

14.8.1 建立復原伺服器

您可以依照下方的指示或觀看[影片教學](#)。

必要條件

- 保護計劃必須套用到您要保護的原始電腦。此計劃必須在雲端儲存空間備份整部電腦，或僅備份開機及提供必要服務所需的磁碟。
- 必須設定雲端站台的其中一個連線類型。

建立復原伺服器

- 在 **[所有裝置]** 索引標籤上，選取您要保護的電腦。
- 按一下 **[災難復原]**，然後按一下 **[建立復原伺服器]**。
- 選取虛擬核心數量和 RAM 大小。

注意事項

您可以查看每個選項的計算點。計算點的數量會反應復原伺服器每小時的執行成本。如需詳細資訊，請參閱 "計算點" (第 343 頁)。

- 指定將與伺服器連線的雲端網路。
- 選擇 **[DHCP]** 選項。

DHCP 選項	描述
雲端站台所提供	預設設定。伺服器的 IP 地址將由雲端中自動設定的 DHCP 伺服器提供。
自訂	伺服器的 IP 地址將由雲端中您自己的 DHCP 伺服器提供。

- [選用] 指定 **[MAC 位址]**。

MAC 位址是指派給伺服器網路介面卡的唯一識別碼。如果使用自訂 DHCP，您可將它設定為一律指派特定的 IP 位址給特定的 MAC 位址。透過這個方式，您可確保復原伺服器一定會獲得相同的 IP 位址。您可以執行具有以 MAC 位址註冊之授權的應用程式。

- 指定伺服器將在實際執行網路中具備的 IP 位址。依預設，會設定原始電腦的 IP 位址。

注意事項

如果您使用 DHCP 伺服器，請將此 IP 位址新增至伺服器排除清單，以避免 IP 位址發生衝突。

如果使用自訂 DHCP 伺服器，您必須在 **[實際執行網路中的 IP 位址]** 中指定與 DHCP 伺服器中設定的 IP 位址相同的 IP 位址。否則，測試容錯移轉將無法正常運作，而且無法透過公用 IP 位址存取伺服器。

- [選擇性步驟] 選取 **[測試 IP 位址]** 核取方塊，然後指定 IP 位址。

這可讓您有能力在隔離的測試網路中測試容錯移轉，並在測試容錯移轉期間，透過 RDP 或 SSH 連線到復原伺服器。在測試容錯移轉模式中，VPN 閘道將會使用 NAT 通訊協定，將測試 IP 位址取代為實際執行 IP 位址。

如果您未選取該核取方塊，則在測試容錯移轉期間只能使用主控台存取伺服器。

注意事項

如果您使用 DHCP 伺服器，請將此 IP 位址新增至伺服器排除清單，以避免 IP 位址發生衝突。

您可以選擇建議的 IP 位址其中之一或輸入不同的位址。

9. [選擇性步驟] 選取 **[網際網路存取]** 核取方塊。

這將可讓復原伺服器在實際或測試容錯移轉期間存取網際網路。預設開放 TCP 連接埠 25，以供與公用 IP 位址的輸出連線使用。

10. [選擇性] 設定 **[RPO 閾值]**。

RPO 閾值會定義上次適合容錯移轉的復原點和目前時間之間允許的最大時間間隔。此值可以設定在 15 – 60 分鐘、1 – 24 小時、1 – 14 天內。

11. [選擇性] 選取 **[使用公用 IP 位址]** 核取方塊。

具有公共 IP 位址可在容錯移轉或測試容錯移轉期間，讓復原伺服器從網際網路使用。如果您未選取該核取方塊，則只能在您的實際執行網路中使用該伺服器。

[使用公用 IP 位址] 選項需要啟用 **[網際網路存取]** 選項。

公共 IP 位址將在您完成設定之後顯示。預設開放 TCP 連接埠 443，以供與公用 IP 位址的輸入連線使用。

注意事項

如果您清除 **[使用公用 IP 位址]** 核取方塊，或刪除復原伺服器，將不會保留其公用 IP 位址。

12. [選擇性] 如果所選電腦的備份經過加密，您可以指定從加密備份建立用於復原伺服器的虛擬機器時將會自動使用的密碼。按一下 **[指定]**，然後定義認證名稱和密碼。根據預設，您將會在清單中看到最新的備份。若要檢視所有備份，選取 **[顯示所有備份]**。

13. [選擇性步驟] 變更復原伺服器名稱。

14. [選擇性步驟] 輸入復原伺服器的描述。

15. [選擇性] 按一下 **[雲端防火牆規則]** 索引標籤以編輯預設防火牆規則。如需詳細資訊，請參閱 "設定雲端伺服器的防火牆規則" (第 393 頁)。

16. 按一下 **[建立]**。

復原伺服器將會出現在服務主控台的 **[災難復原] > [伺服器] > [復原伺服器]** 索引標籤中。您也可以透過選取原始電腦並按一下 **[災難復原]** 來檢視其設定。

Acronis Cyber Cloud Manage account DISASTER RECOVERY Servers Connectivity Runbooks ANTI-MALWARE PROTECTION SOFTWARE MANAGEMENT BACKUP STORAGE REPORTS SETTINGS Powered by Acronis AnyData Engine	Servers ? 🔒					
	RECOVERY SERVERS PRIMARY SERVERS					
	Search					
	☐ Name ↓ Status ↓ State ↓ RPO compliance ↓ VM state ↓ ⚙️					
	Win16 OK Standby — — ⋮					
	cen7-sg7 OK Standby — — ⋮					
	Cen_vg-1 OK Failover Not set On ⋮					
	Cen_mb-3 OK Testing failover Not set On ⋮					
	Cen_mb-2 OK Failback Not set Off ⋮					
	Cen_mb-1 OK Failback Not set Off ⋮					

14.8.2 容錯移轉的運作方式

實際執行容錯移轉

注意事項

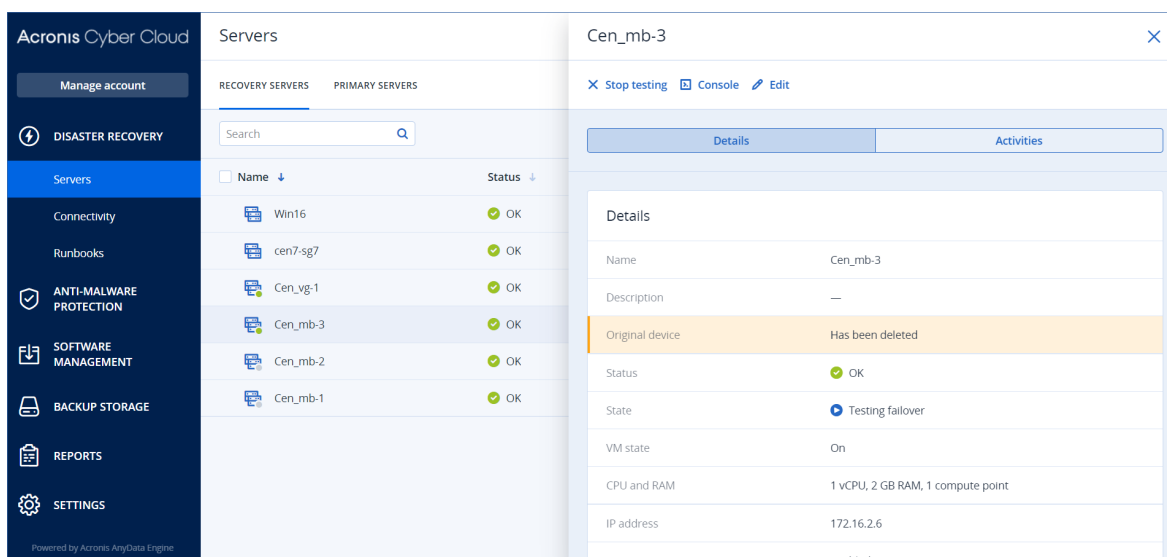
是否能夠使用此功能視您帳戶啟用的服務配額而定。

復原伺服器建立時，它會維持在 **【待命】** 狀態。在起始容錯移轉之前，對應的虛擬機器不存在。開始容錯移轉程序之前，您必須為原始電腦建立至少一個磁碟影像備份 (含可開機的磁碟區)。

開始容錯移轉程序時，您要選取原始電腦的復原點，您可以從該復原點使用預先定義的參數建立虛擬機器。容錯移轉作業會使用「從備份執行 VM」功能。復原伺服器的過渡狀態為 **【最終化】**。此程序意味著將伺服器的虛擬磁碟從備份儲存空間 (「冷」儲存) 傳送到災難復原儲存空間 (「熱」儲存)。在最終化期間，雖然效能低於正常狀態，但仍然可以存取和操作。當最終化完成時，伺服器效能就會達到其正常值。伺服器狀態會變更為 **【容錯移轉】**。工作負載現在會從原始電腦切換到雲端站台中的復原伺服器。

如果復原伺服器內部有保護代理程式，則會停止代理程式服務，以避免干擾 (例如開始備份或將過期的狀態報告至備份元件)。

在以下的圖表中，您可以同時看到容錯移轉和容錯回復程序。



6. 使用下列任何一個方法測試復原伺服器：

- 在 **[災難復原]>[伺服器]** 中，選取復原伺服器，然後按一下 **[主控台]**。
- 使用 RDP 或 SSH，以及您在建立復原伺服器時指定的測試 IP，連線到復原伺服器。在實際執行網路內部和外部皆嘗試連線 (如「點對站連線」中所述)。
- 在復原伺服器內執行指令碼。
指令碼可檢查登入畫面、應用程式是否啟動、網際網路連線，以及其他電腦連線到復原伺服器的能力。
- 如果復原伺服器具備網際網路存取權和公共 IP 位址，您可能會想使用 TeamViewer。

7. 當測試完成時，按一下 **[停止測試]**。

復原伺服器隨即停止。在測試容錯移轉期間針對復原伺服器所做的變更都不會保留。

注意事項

在 Runbook 中，或在手動啟動測試容錯移轉時，**[啟動伺服器]** 和 **[停止伺服器]** 動作都不適用於測試容錯移轉作業。如果您嘗試執行此種動作，將會失敗，並出現下列錯誤訊息：

失敗：此動作不適用於目前的伺服器狀態。

執行容錯移轉

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

容錯移轉是從您本機將工作負載移到雲端的程序，也是工作負載保留在雲端的狀態。

當您啟動容錯移轉時，復原伺服器會在實際執行網路中啟動。所有保護計劃都會從原始電腦撤銷。新的保護計劃會自動建立並套用至復原伺服器。

容錯移轉至復原伺服器之前，必須至少建立一個復原點。

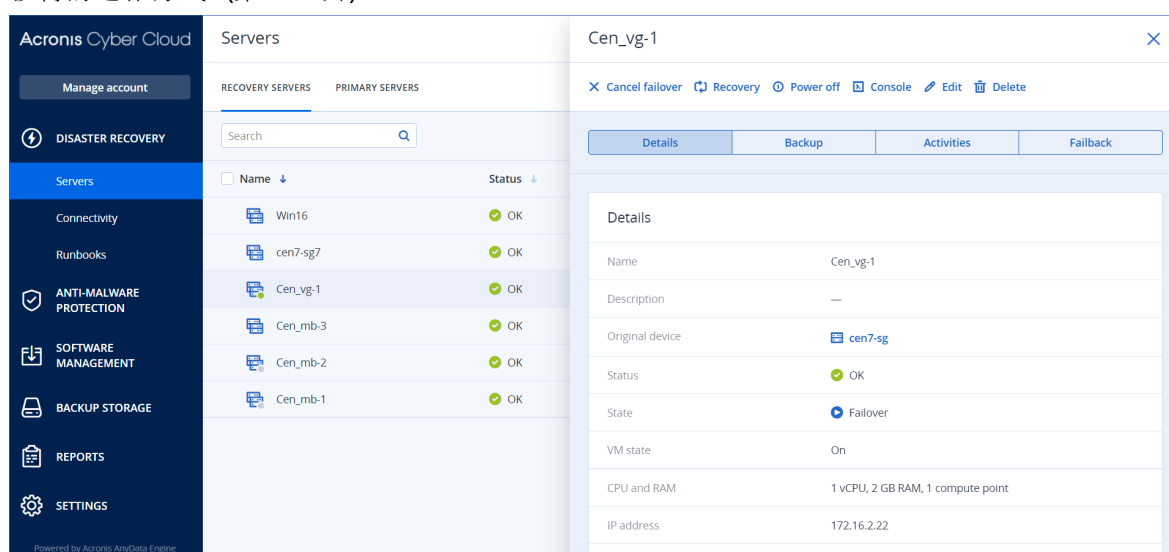
您必須事先 [建立復原伺服器](#) 以保護您的裝置免受災難影響。您將能夠從為裝置建立復原伺服器後產生的任何復原點，執行實際執行容錯移轉。

您可以依照下方的指示或觀看 [影片教學](#)。

執行容錯移轉

1. 確認原始電腦在網路上無法使用。
2. 在服務主控台中，移至 **[災難復原] > [伺服器] > [復原伺服器]**，然後選取復原伺服器。
3. 按一下 **[容錯移轉]**。
4. 選取容錯移轉類型 **[實際執行容錯移轉]**。
5. 選擇復原點，然後按一下 **[啟動實際執行容錯移轉]**。

當復原伺服器啟動時，其狀態會變更為 **[最終化]**，一段時間後則會變更為 **[容錯移轉]**。儘管有運轉進度指示器，但瞭解伺服器在兩種狀態下都可以使用至關重要。如需詳細資訊，請參閱 "容錯移轉的運作方式" (第 379 頁)。



6. 透過檢視其主控台，確認復原伺服器已啟動。按一下 **[災難復原] > [伺服器]**，選取復原伺服器，然後按一下 **[主控台]**。
7. 確認可使用您在建立復原伺服器時指定的實際執行 IP 位址存取復原伺服器。

復原伺服器最終化之後，會自動建立新的保護計劃並套用至復原伺服器。此保護計劃是以用來建立復原伺服器的保護計劃為基礎，其有特定限制。在此計劃中，您可以變更的只有排程和保留規則。如需詳細資訊，請參閱 [< 備份雲端伺服器 >](#)。

如果您要取消容錯移轉，請選取復原伺服器，然後按一下 **[取消容錯移轉]**。除了復原伺服器備份之外，從容錯移轉那一刻開始的所有變更都將遺失。復原伺服器將會返回 **[待命]** 狀態。

如果您要執行容錯回復，請選取復原伺服器，然後按一下 **[容錯回復]**。

如何使用本機 DNS 執行伺服器的容錯移轉

如果您使用本機站台上的 DNS 伺服器解析電腦名稱，則在容錯移轉對應依賴 DNS 之電腦的復原伺服器之後，將因為雲端中使用的 DNS 伺服器不同而無法通訊。根據預設，雲端站台的 DNS 伺服器用於新建立的雲端伺服器。如果您需要套用自訂 DNS 設定，請連絡支援小組。

如何執行 DHCP 伺服器的容錯移轉

您本機基礎架構的 DHCP 伺服器可能位於 Windows 或 Linux 主機。當這種主機容錯移轉至雲端站台時，會發生 DHCP 伺服器重複問題，因為雲端中的 VPN 閘道也會執行 DHCP 角色。若要解決這個

問題, 請執行下列其中一項操作:

- 如果只有 DHCP 主機容錯移轉至雲端, 雖然其餘的雲端伺服器仍在本機站台, 但您還是必須登入雲端的 DHCP 主機, 並關閉其上的 DHCP 伺服器。因此, 將不會發生衝突, 而且只有 VPN 閘道將會當做 DHCP 伺服器。
- 如果您的雲端伺服器已經從 DHCP 主機取得 IP 位址, 則您必須登入雲端的 DHCP 主機, 並關閉其上的 DHCP 伺服器。您也必須登入雲端伺服器並更新 DHCP 租賃, 以指派從正確的 DHCP 伺服器 (在 VPN 閘道上託管) 配置的新 IP 位址。

注意事項

當您的雲端 DHCP 伺服器設定為 **[自訂 DHCP]** 選項時, 這些指示無效, 而且某些復原或主要伺服器會從此 DHCP 伺服器獲得其 IP 位址。

14.8.3 容錯回復的運作方式

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

容錯回復是從雲端將工作負載移回您本機站台上的實體或虛擬機器的程序。您可以在**容錯移轉**狀態下的復原伺服器上執行容錯回復, 並在本機站台上繼續使用伺服器。

在容錯回復至目標虛擬機器的過程中, 您可以在雲端的虛擬機器繼續執行時, 將備份資料傳輸到本機站台。此技術有助於達到非常短的停機期間, 且此停機期間可以估算並顯示在服務主控台中。您可以檢視此停機期間, 並使用這項資訊規劃您的活動, 並在必要時, 對您的用戶端提出停機期間即將到來的警告。

容錯回復至目標虛擬機器的程序與容錯回復至目標實體機器的程序不同。如需有關容錯回復程序階段的詳細資訊, 請參閱 "容錯回復至目標虛擬機器" (第 383 頁) 和 "容錯回復至目標實體機器" (第 387 頁)。

注意事項

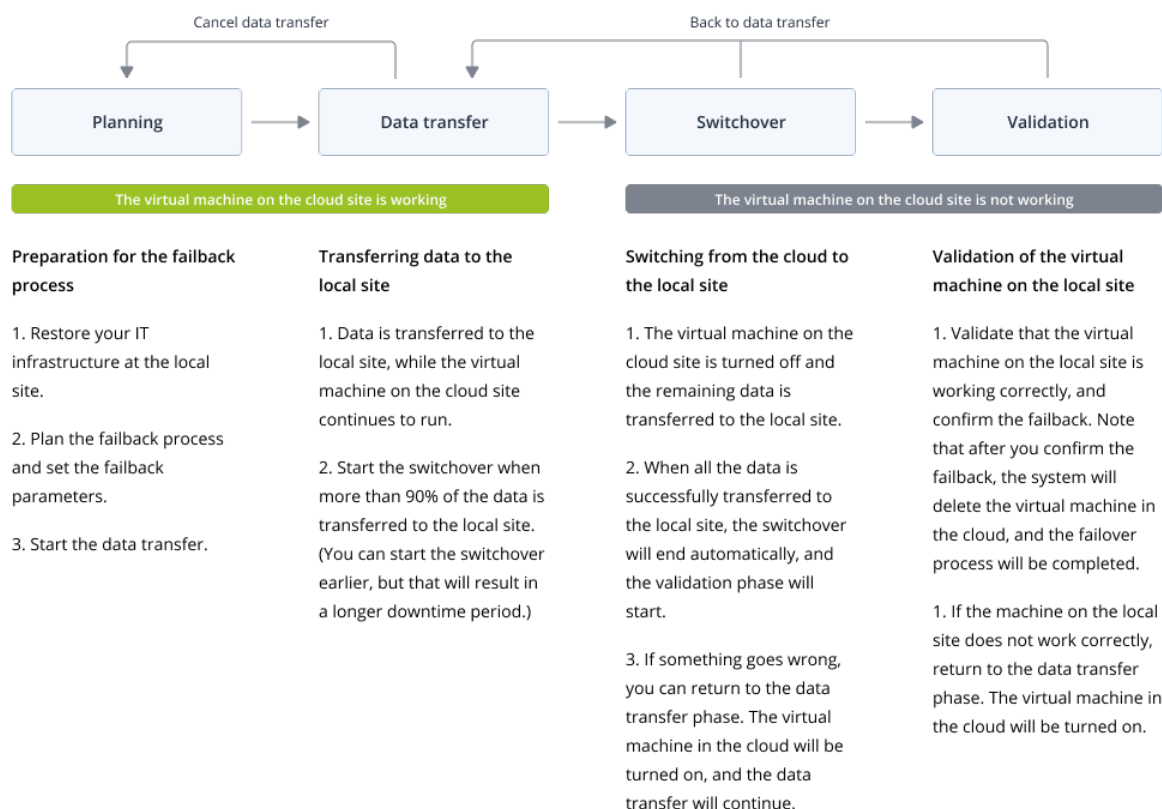
Runbook 作業僅支援容錯回復至實體機器。也就是說, 如果您透過執行包含**容錯回復伺服器**步驟的 Runbook 來開始容錯回復程序, 此程序將需要手動互動。您必須手動復原機器, 並從 **[災難復原] > [伺服器]** 索引標籤確認或取消容錯回復程序。

容錯回復至目標虛擬機器

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

容錯回復至目標虛擬機器的程序包含四個階段。



1. **規劃**。在此階段期間，您要在本機站台還原 IT 基礎架構 (例如，主機和網路設定)、設定容錯回復參數，以及規劃開始資料傳輸的時間。

注意事項

為將容錯回復程序的全部時間減至最少，建議您在設定本機伺服器後立即開始**資料傳輸**階段，然後在**資料傳輸**階段期間，繼續設定網路以及其餘的本機基礎架構。

2. **資料傳輸**。在此階段期間，資料會在雲端的虛擬機器繼續執行時，從雲端站台傳輸到本機站台。您可以在**資料傳輸**階段期間，隨時開始下一個階段 (**轉換**)，但是您應該考慮下列關係：

您維持在**資料傳輸**階段的時間越長，

- 雲端的虛擬機器繼續執行的時間越長
- 傳輸到本機站台的資料越大量
- 您將支付的費用越高 (您花費的計算點越多)
- 您在**轉換**階段經歷的停機期間越短。

如果您要將停機時間減至最少，請在超過 90% 的資料傳輸到本機站台之後，就開始**轉換**階段。

如果您可以承受經歷較長的停機期間，而且不想要花費更多的計算點執行雲端的虛擬機器，您可以更早開始**轉換**階段。

如果您在**資料傳輸**階段期間取消容錯回復程序，已傳輸的資料將不會從本機站台刪除。為避免可能的問題，請先手動刪除已傳輸的資料，然後再開始新的容錯回復程序。下列資料傳輸程序將從頭開始。

3. **轉換**。此階段期間會關閉雲端的虛擬機器，而且包括上次備份增量在內的剩餘資料會傳輸到本機站台。請注意，當**轉換**階段完成後，所有資料都會傳輸到本機站台。不會失去任何資料，而且本機站台上的虛擬機器為雲端虛擬機器的確切複本。您可以在服務主控台中，檢視完成此階段的估計時間(停機期間)。當所有資料都傳輸到本機站台之後，就會復原本機站台上的虛擬機器，而且會自動開始**驗證**階段。
4. **驗證**。在此階段期間，本機站台上的虛擬機器已準備就緒，您可以將其開啟。您可以確認虛擬機器正確運作，而且：
 - 如果一切如預期般運作，請確認容錯回復。容錯回復確認之後，雲端的虛擬機器就會遭到刪除，且復原伺服器會回復到**待命**狀態。這是容錯回復程序的結尾。
 - 如果發生問題，您可以取消轉換，並返回**資料傳輸**階段。

對虛擬機器執行容錯回復

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以對本機站台上的目標虛擬機器執行容錯回復。

必要條件

- 您將用於執行容錯回復的代理程式已連線，且目前未用於其他容錯回復作業。
- 您的網際網路連線穩定。

對虛擬機器執行容錯回復

1. 在服務主控台中，移至 **[災難復原]>[伺服器]**。
2. 選擇處於**[容錯移轉]**狀態的復原伺服器。
3. 按一下 **[容錯回復]** 索引標籤。
4. 在 **[容錯回復參數]** 區段中，選擇 **[虛擬機器]** 作為 **[目標]**，並設定其他參數。
請注意，部分 **[容錯回復參數]** 預設會自動填入建議的值，但是您可以加以變更。
下表提供有關 **[容錯回復參數]** 的詳細資訊。

參數	描述
備份大小	在容錯回復程序期間傳輸到本機站台的資料量。 在您開始容錯回復到目標虛擬機器的程序之後，[備份大小] 將會在 [資料傳輸] 階段增加，因為雲端的虛擬機器將繼續執行並產生新資料。 若要計算容錯回復至目標虛擬機器程序期間的預估停機期間，請使用 10% 的 [備份大小] 值 (因為我們建議您在 90% 的資料傳輸到本機站台之後再開始 [轉換] 階段)，並將其除以您網際網路速度的值。 注意事項 當您同時執行數個容錯回復程序時，網際網路速度的值將會減少。
目標	您要將雲端伺服器復原到的本機站台的工作負載類型： [虛擬機器] 或 [實體機器] 。

參數	描述
目標電腦位置	容錯回復位置:VMware ESXi 主機或 Microsoft Hyper-V 主機。 您可以從裝有已向網路保護服務註冊之代理程式的所有主機選擇。
代理程式	將執行容錯回復作業的代理程式。 您可以同時使用一個代理程式執行一個容錯回復作業。 您可以選擇已連線且目前未用於其他容錯回復程序、具備支援容錯回復功能的版本,以及擁有存取備份權限的代理程式。 請注意,您可以在 VMware ESXi 主機上安裝數個代理程式,並使用每一個代理程式開始一個個別的容錯回復程序。這些容錯回復程序可以同時執行。
目標電腦設定	虛擬機器設定: • 虛擬處理器。選擇虛擬裝置的數量。 • 記憶體。選擇虛擬機器將具備的記憶體數量。 • 單位。選擇記憶體的單位。 • [選用]網路介面卡。若要新增網路介面卡,按一下 [新增],然後在 [網路] 欄位中選擇一個網路。 當您準備好進行變更時,按一下 [完成] 。
路徑	(適用於 Microsoft Hyper-V 主機)將存放您電腦所在主機上的資料夾。 請確認電腦的主機上有足夠的可用記憶體空間。
資料存放區	(適用於 VMware ESXi 主機)將存放您電腦所在主機上的資料存放區。 請確認電腦的主機上有足夠的可用記憶體空間。
佈建模式	虛擬磁碟配置的方法。 若是 Microsoft Hyper-V 主機: • 動態擴充 (預設值)。 • 固定大小。 若是 Microsoft Hyper-V 主機: • 精簡 (預設值)。 • 密集。
目標電腦名稱	目標電腦的名稱。根據預設,目標電腦名稱與復原伺服器名稱相同。 目標電腦名稱在所選 目標電腦位置 上必須是唯一的。

5. 按一下 **[開始資料傳輸]**, 然後在確認視窗中, 按一下 **[開始]**。

資料傳輸階段隨即開始。主控台會顯示以下資訊:

- **進度**。此參數會顯示已經傳輸到本機站台的資料量以及必須傳輸的總資料量。請注意, 總資料量包括資料傳輸階段開始前最後備份的資料, 以及新產生資料的備份 (備份增量), 因為虛擬機器在**資料傳輸**階段期間會繼續執行。因此, **[進度]** 參數的這兩個值會隨著時間而增加。
- **停機時間預估**。此參數會顯示如果您現在開始**轉換**階段, 將無法使用虛擬機器的時間。這個值是根據 **[進度]** 的值計算得來, 而且會隨著時間而減少。

6. 按一下 **[轉換]**，然後在確認視窗中，再按一下 **[轉換]**。

轉換階段隨即開始。主控台會顯示以下資訊：

- **進度**。此參數會顯示在本機站台上還原虛擬機器的進度。
- **估計的完成時間**。此參數會顯示將完成**轉換**階段，而且您將能夠開啟本機站台上的虛擬機器的大約時間。

7. **轉換**階段完成後，驗證本機站台上的虛擬機器是否如預期般運作。

8. 按一下 **[確認容錯回復]**，然後在確認視窗中，按一下 **[確認]** 以結束程序。

雲端的虛擬機器會遭到刪除，且復原伺服器會回復到**待命**狀態。

注意事項

在復原的伺服器上套用保護計劃不是容錯回復程序的一部分。在容錯回復程序完成之後，在復原的伺服器上套用保護計劃以確保其再次受到保護。您可以套用在原始伺服器上套用的相同保護計劃，也可以套用已啟用災難復原模組的新保護計劃。

容錯回復至目標實體機器

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

容錯回復至目標實體機器的程序與容錯回復至目標虛擬機器的程序不同。將資料從雲端的備份傳輸到本機站台不是自動化工作流程的一部分，而且可以在雲端中的虛擬機器關閉之後手動完成。因此，容錯回復至實體機器時，預計需要的停機期間較長。

容錯回復至目標實體機器的程序包括下列階段：

1. **規劃**。在此階段期間，您要在本機站台還原 IT 基礎架構 (例如，主機和網路設定)、設定容錯回復參數，以及規劃開始資料傳輸的時間。
2. **轉換**。此階段期間會關閉雲端的虛擬機器，並備份新產生的資料。備份完成後，您要手動將電腦復原到本機站台。您可以使用可開機媒體復原磁碟，或從雲端備份儲存空間復原整部電腦。
3. **驗證**。在此階段期間，您要確認實體機器正確運作並確認容錯回復。確認之後，雲端站台的虛擬機器會遭到刪除，且復原伺服器會回復到**待命**狀態。

對實體機器執行容錯回復

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以對本機站台上的目標實體機器執行容錯回復。

對實體機器執行容錯回復

1. 在服務主控台中，移至 **[災難復原] > [伺服器]**。
2. 選擇處於**[容錯移轉]**狀態的復原伺服器。
3. 按一下 **[容錯回復]** 索引標籤。
4. 在 **[選擇目標]** 欄位中，選擇 **[實體機器]**。

5. [選擇性] 將 **[備份大小]** 值除以您網際網路速度的值，以計算容錯回復程序期間的預估停機期間。

注意事項

當您同時執行數個容錯回復程序時，網際網路速度的值將會減少。

6. 按一下 **[轉換]**，然後在確認視窗中，再按一下 **[轉換]**。
雲端站台上的虛擬機器隨即關閉。
7. 將伺服器從備份復原到本機站台上的實體機器。
 - 如果您要使用可開機媒體，請如 [網路保護使用指南](#) 中的「使用可開機媒體復原磁碟」所述進行。請確認您使用登錄伺服器的帳戶登入雲端，而且您選取最近的備份。
 - 如果目標電腦已連線，您可以使用服務主控台。在 **[備份儲存]** 索引標籤上，選取雲端儲存。在 **[要瀏覽的電腦]** 中，選擇目標實體機器。所選電腦必須登錄登錄伺服器所使用的相同帳戶。尋找最近的伺服器備份、按一下 **[復原整部電腦]**，然後設定其他復原參數。如需詳細指示，請參閱 [網路保護使用指南](#) 中的「復原電腦」。
8. 確認復原已完成且復原的電腦正常運作，然後按一下 **[電腦已還原]**。
9. 如果一切如預期般運作，按一下 **[確認容錯回復]**，然後在確認視窗中，再按一下 **[確認]**。
復原伺服器和復原點會變成準備就緒供下次容錯移轉之用。若要建立新的復原點，請將保護計劃套用到新的本機伺服器。

注意事項

在復原的伺服器上套用保護計劃不是容錯回復程序的一部分。在容錯回復程序完成之後，在復原的伺服器上套用保護計劃以確保其再次受到保護。您可以套用在原始伺服器上套用的相同保護計劃，也可以套用已啟用災難復原模組的新保護計劃。

14.8.4 使用加密備份

您可以從加密備份建立復原伺服器。您可以在容錯移轉至復原伺服器期間，對加密備份設定自動套用密碼，以供您方便之用。

建立復原伺服器時，您可以指定要用於自動災難復原作業的密碼。此密碼將會儲存到認證儲存區，這是一個安全的認證儲存區，可以在 **[設定] > [認證]** 區段中找到。

一個認證可以連結到數個備份。

若要在認證儲存區中管理已儲存的密碼

1. 移至 **[設定] > [認證]**。
2. 若要管理特定的認證，請按一下最後一欄中的圖示。您可以檢視連結至此認證的項目。
 - 若要從所選認證取消連結備份，請按一下備份附近的 **[資源回收筒]** 圖示。因此，您必須在容錯移轉至復原伺服器期間，手動指定密碼。
 - 若要編輯認證，按一下 **[編輯]**，然後指定名稱或密碼。
 - 若要刪除認證，按一下 **[刪除]**。請注意，您必須在容錯移轉至復原伺服器期間，手動指定密碼。

14.8.5 使用 Microsoft Azure 虛擬機器進行操作

注意事項

部分功能可能需要額外的授權，端視適用的授權模型而定。

您可以將 Microsoft Azure 虛擬機器容錯移轉至 Acronis Cyber Protect Cloud。如需詳細資訊，請參閱 "執行容錯移轉" (第 381 頁)。

之後，您可以從 Acronis Cyber Protect Cloud 容錯回復到 Azure 虛擬機器。容錯回復程序與容錯回復至實體機器的程序相同。如需詳細資訊，請參閱 "對實體機器執行容錯回復" (第 387 頁)。

注意事項

若要登錄新的 Azure 虛擬機器進行容錯回復，您可以使用 Azure 中提供的 Acronis Backup VM 擴充功能。

您可以在 Acronis Cyber Protect Cloud 和 Azure VPN 閘道之間設定多站台 IPsec VPN 連線。如需詳細資訊，請參閱 "設定多站台 IPsec VPN" (第 359 頁)。

14.9 設定主要伺服器

本節描述如何建立和管理主要伺服器。

14.9.1 建立主要伺服器

必要條件

- 必須設定雲端站台的其中一個連線類型。

建立主要伺服器

1. 移至 **[災難復原] > [伺服器] > [主要伺服器]** 索引標籤。
2. 按一下 **[建立]**。
3. 為新的虛擬機器選取範本。
4. 選取虛擬核心數量和 RAM 大小。

注意事項

您可以查看每個選項的計算點。計算點的數量會反應主要伺服器每小時的執行成本。如需詳細資訊，請參閱 "計算點" (第 343 頁)。

5. [選擇性步驟] 變更虛擬磁碟大小。如果您需要一個以上的硬碟，請按一下 **[新增磁碟]**，然後指定新的磁碟大小。目前您可以針對主要伺服器新增不超過 10 個磁碟。
6. 指定主要伺服器將包含在內的雲端網路。
7. 選擇 **[DHCP]** 選項。

DHCP 選項	描述
雲端站台所提供	預設設定。伺服器的 IP 地址將由雲端中自動設定的 DHCP 伺服器提供。
自訂	伺服器的 IP 地址將由雲端中您自己的 DHCP 伺服器提供。

8. [選用] 指定 **[MAC 位址]**。

MAC 位址是指派給伺服器網路介面卡的唯一識別碼。如果使用自訂 DHCP, 您可將它設定為一律指派特定的 IP 位址給特定的 MAC 位址。如此可確保主要伺服器一定會獲得相同的 IP 位址。您可以執行具有以 MAC 位址註冊之授權的應用程式。

9. 指定伺服器將在實際執行網路中具備的 IP 位址。根據預設, 會設定您實際執行網路中的第一個可用 IP 位址。

注意事項

如果您使用 DHCP 伺服器, 請將此 IP 位址新增至伺服器排除清單, 以避免 IP 位址發生衝突。

如果使用自訂 DHCP 伺服器, 您必須在 **[實際執行網路中的 IP 位址]** 中指定與 DHCP 伺服器中設定的 IP 位址相同的 IP 位址。否則, 測試容錯移轉將無法正常運作, 而且無法透過公用 IP 位址存取伺服器。

10. [選擇性步驟] 選取 **[網際網路存取]** 核取方塊。

這將可讓主要伺服器存取網際網路。預設開放 TCP 連接埠 25, 以供與公用 IP 位址的輸出連線使用。

11. [選擇性] 選取 **[使用公共 IP 位址]** 核取方塊。

具有公共 IP 位址可讓主要伺服器從網際網路使用。如果您未選取該核取方塊, 則只能在您的實際執行網路中使用該伺服器。

公共 IP 位址將在您完成設定之後顯示。預設開放 TCP 連接埠 443, 以供與公用 IP 位址的輸入連線使用。

注意事項

如果您清除 **[使用公用 IP 位址]** 核取方塊, 或刪除復原伺服器, 將不會保留其公用 IP 位址。

12. [選擇性] 選擇 **[設定 RPO 閾值]**。

RPO 閾值會定義上次復原點和目前時間之間的最大可允許時間間隔。此值可以設定在 15 – 60 分鐘、1 – 24 小時、1 – 14 天內。

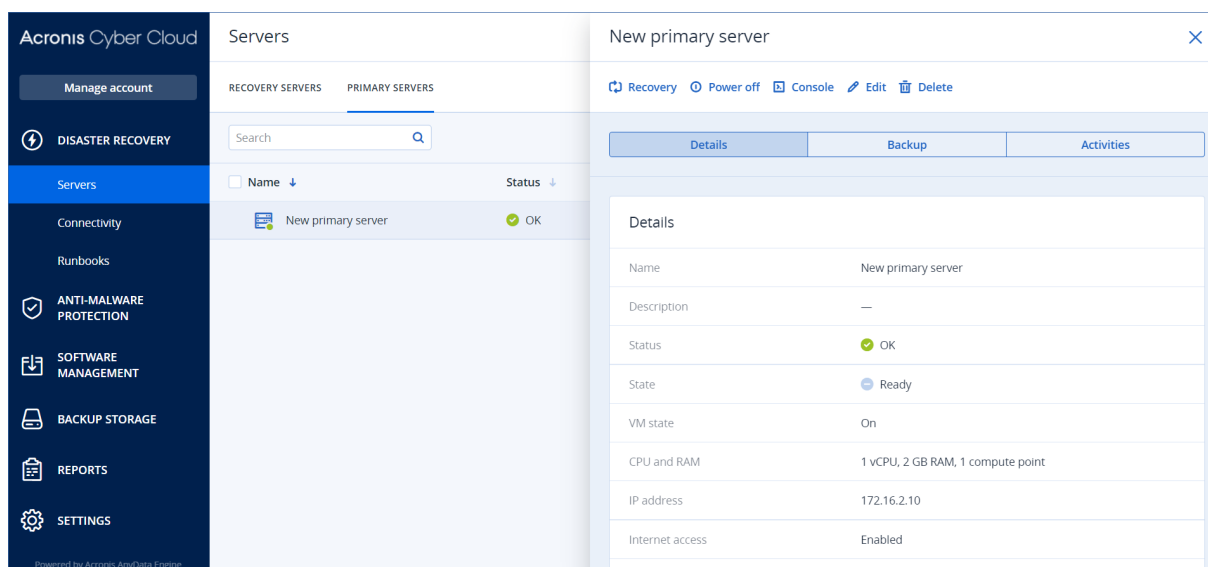
13. 定義主要伺服器名稱。

14. [選擇性] 指定主要伺服器的描述。

15. [選擇性] 按一下 **[雲端防火牆規則]** 索引標籤以編輯預設防火牆規則。如需詳細資訊, 請參閱 "設定雲端伺服器的防火牆規則" (第 393 頁)。

16. 按一下 **[建立]**。

主要伺服器便可在實際執行網路中使用。您可以使用伺服器的主控台、RDP、SSH 或 TeamViewer 來管理伺服器。



14.9.2 主要伺服器的操作

主要伺服器將會出現在服務主控台的 **[災難復原] > [伺服器] > [主要伺服器]** 索引標籤中。

若要啟動或停止伺服器，在主要伺服器面板上按一下 **[開機]** 或 **[關機]**。

若要編輯主要伺服器設定，停止該伺服器，然後按一下 **[編輯]**。

若要將保護計劃套用到主要伺服器，選取該伺服器，然後在 **[計劃]** 索引標籤上，按一下 **[建立]**。您將會看到一個預先定義的保護計劃，其中，您僅能變更排程和保留規則。如需詳細資訊，請參閱 [< 備份雲端伺服器 >](#)。

14.10 管理雲端伺服器

若要管理雲端伺服器，請移至 **[災難復原] > [伺服器]**。該處有兩個索引標籤：**[復原伺服器]** 和 **[主要伺服器]**。若要顯示表格中的所有選用欄，請按一下齒輪圖示。

您可以透過選取每部雲端伺服器，找到該伺服器的下列相關資訊。

欄名稱	描述
名稱	您定義的雲端伺服器名稱
狀態	反映雲端伺服器最嚴重問題的狀態 (根據作用中警示)
狀態	雲端伺服器狀態
VM 狀態	與雲端伺服器相關之虛擬機器的電源狀態
使用中的位置	託管雲端伺服器所在的位置。例如，雲端。
RPO 閾值	上次適合容錯移轉的復原點和目前時間之間允許的最大時間間隔。此值可以設定在 15-60 分鐘、1-24 小時、1-14 天內。

RPO 合規	RPO 合規是實際 RPO 和 RPO 閾值之間的比率。如果 RPO 閾值已經過定義，則會顯示 RPO 合規。 其計算方式如下： RPO 合規 = 實際 RPO/RPO 閾值 其中： 實際 RPO = 目前時間 - 上次復原點時間 RPO 合規狀態 根據實際 RPO 和 RPO 閾值間比率的值，會使用下列狀態： • 合規。RPO 合規 < 1x。伺服器符合 RPO 閾值。 • 超過。RPO 合規 <= 2x。伺服器違反 RPO 閾值。 • 嚴重超過。RPO 合規 <= 4x。伺服器違反 RPO 閾值超過 2x 次。 • 極度超過。RPO 合規 > 4x。伺服器違反 RPO 閾值超過 4x 次。 • 擱置中 (無備份)。伺服器受到保護計劃保護，但備份正在建立，而且還未完成。
實際 RPO	自上次建立復原點後經過的時間
上次復原點	建立上次復原點的日期與時間

14.11 雲端伺服器的防火牆規則

您可以將防火牆規則設定為控制雲端站台上，主要伺服器和復原伺服器的輸入及輸出流量。

您可以在佈建雲端伺服器的公用 IP 位址後設定輸入規則。預設允許 TCP 連接埠 443，並拒絕其他所有輸入連線。您可以變更預設防火牆規則，並新增或移除輸入例外。如果未佈建公用 IP，您僅能檢視輸入規則，但無法進行設定。

您可以在佈建雲端伺服器的網際網路存取後設定輸出規則。預設拒絕 TCP 連接埠 25，並允許其他所有輸出連線。您可以變更預設防火牆規則，並新增或移除輸出例外。如果未佈建網際網路存取，您僅能檢視輸出規則，但無法進行設定。

注意事項

基於安全性原因，有一些預先定義且您無法變更的防火牆規則。

針對輸入和輸出連線：

- 允許 Ping: ICMP echo-request (type 8, code 0) and ICMP echo-reply (type 0, code 0)
- Permit ICMP need-to-frag (type 3, code 4)
- Permit TTL exceeded (type 11, code 0)

僅針對輸入連線：

- 無法設定的部分：全部拒絕

僅針對輸出連線：

- 無法設定的部分：全部拒絕
-

14.11.1 設定雲端伺服器的防火牆規則

您可以針對雲端的主要伺服器和復原伺服器編輯預設防火牆規則。

若要編輯雲端站台上伺服器的防火牆規則

1. 在服務主控台中，移至 **[災難復原] > [伺服器]**。
2. 如果您要編輯復原伺服器的防火牆規則，按一下 **[復原伺服器]** 索引標籤。或者，如果您要編輯主要伺服器的防火牆規則，按一下 **[主要伺服器]** 索引標籤。
3. 按一下伺服器，然後按一下 **[編輯]**。
4. 按一下 **[雲端防火牆規則]** 索引標籤。
5. 如果您要變更輸入連線的預設動作：
 - a. 在 **[輸入]** 下拉式欄位中，選擇預設動作。

動作	描述
全部拒絕	拒絕任何輸入流量。 您可以新增例外，並允許來自特定 IP 位址、通訊協定和連接埠的流量。
全部允許	允許所有輸入 TCP 和 UDP 流量。 您可以新增例外，並拒絕來自特定 IP 位址、通訊協定和連接埠的流量。

注意事項

變更預設動作會使現有輸入規則的設定失效並加以移除。

- b. [選用] 如果您要儲存現有的例外，請在確認視窗中，選擇 **[儲存填入的例外]**。
 - c. 按一下 **[確認]**。
6. 如果您要新增例外：
 - a. 按一下 **[新增例外]**。
 - b. 指定防火牆參數。

防火牆參數	描述
通訊協定	選擇用於連線的通訊協定。支援下列選項： • TCP • UDP • TCP+UDP
伺服器連接埠	選擇要套用規則的連接埠。您可以指定： • 特定連接埠號碼 (例如, 2298) • 連接埠號碼範圍 (例如, 6000-6700) • 任何連接埠號碼。如果您希望將規則套用到任何連接埠號碼, 請使用 *。
用戶端 IP 位址	選擇要套用規則的 IP 位址。您可以指定： • 特定 IP 位址 (例如, 192.168.0.0) • 使用 CIDR 標記法的 IP 位址範圍 (例如, 192.168.0.0/24) • 任何 IP 位址。如果您希望將規則套用到任何 IP 位址, 請使用 *。

7. 如果您要移除現有的輸入例外, 按一下旁邊的垃圾桶圖示。

8. 如果您要變更輸出連線的預設動作：

a. 在 **[輸出]** 下拉式欄位中, 選擇預設動作。

動作	描述
全部拒絕	拒絕任何輸出流量。 您可以新增例外, 並允許前往特定 IP 位址、通訊協定和連接埠的流量。
全部允許	允許所有輸出流量。 您可以新增例外, 並拒絕來自特定 IP 位址、通訊協定和連接埠的流量。

注意事項

變更預設動作會使現有輸出規則的設定失效並加以移除。

b. [選用] 如果您要儲存現有的例外, 請在確認視窗中, 選擇 **[儲存填入的例外]**。

c. 按一下 **[確認]**。

9. 如果您要新增例外：

a. 按一下 **[新增例外]**。

b. 指定防火牆參數。

防火牆參數	描述
通訊協定	選擇用於連線的通訊協定。支援下列選項： • TCP • UDP • TCP+UDP
伺服器連接埠	選擇要套用規則的連接埠。您可以指定：

防火牆參數	描述
	• 特定連接埠號碼 (例如, 2298) • 連接埠號碼範圍 (例如, 6000-6700) • 任何連接埠號碼。如果您希望將規則套用到任何連接埠號碼, 請使用 *。
用戶端 IP 位址	選擇要套用規則的 IP 位址。您可以指定: • 特定 IP 位址 (例如, 192.168.0.0) • 使用 CIDR 標記法的 IP 位址範圍 (例如, 192.168.0.0/24) • 任何 IP 位址。如果您希望將規則套用到任何 IP 位址, 請使用 *。

10. 如果您要移除現有的輸出例外, 按一下旁邊的垃圾桶圖示。

11. 按一下 **[儲存]**。

14.11.2 檢查雲端防火牆活動

雲端伺服器防火牆規則設定更新後, 更新活動記錄會出現在服務主控台中。您可以檢視記錄並檢查下列資訊:

- 更新設定之使用者的使用者名稱
- 更新的日期和時間
- 輸入和輸出連線的防火牆設定
- 輸入和輸出連線的預設動作
- 輸入和輸出連線例外的通訊協定、連接埠和 IP 位址

若要檢視有關雲端防火牆規則設定變更的詳細資訊

1. 在服務主控台中, 按一下 **[監控] > [活動]**。
2. 按一下對應的活動, 然後按一下 **[所有屬性]**。
活動的描述應該是 **[正在更新雲端伺服器設定]**。
3. 在 **[內容]** 欄位中, 檢查您感興趣的資訊。

14.12 備份雲端伺服器

主要伺服器和復原伺服器是由 VMware 用代理程式備份, 此代理程式安裝在雲端站台上。在初始版本中, 與本機代理程式執行的備份相比, 此備份在功能上有所限制。這些限制都是暫時的, 且將在日後版本中移除。

- 唯一的備份位置是雲端儲存。
- 一個保護計劃無法套用到多部伺服器。每部伺服器都必須有自己的保護計劃, 即使所有保護計劃的設定都相同也一樣。
- 一部伺服器僅能套用一个保護計劃。

- 不支援應用程式感知備份。
- 加密不可使用。
- 備份選項不可使用。

當您刪除主要伺服器時，也同時刪除其備份。

復原伺服器僅在容錯移轉狀態中才會備份。其備份會繼續原始伺服器的備份順序。執行容錯回復時，原始伺服器會繼續此備份順序。因此，復原伺服器的備份只能以手動方式刪除，或當做套用保留規則的結果。當刪除復原伺服器時，其備份一律會保留。

注意事項

雲端伺服器的保護計劃是根據 UTC 時間執行的。

14.13 編排 (Runbook)

注意事項

部分功能可能需要額外的授權，端視適用的授權模型而定。

Runbook 是一組說明如何在雲端啟動實際執行環境的指示。您可以在服務主控台中建立 Runbook。若要存取 **[Runbook]** 索引標籤，選取 **[災難復原] > [Runbook]**。

14.13.1 為什麼使用 Runbook?

Runbook 可讓您：

- 自動容錯移轉一或多部伺服器
- Ping 伺服器 IP 位址並檢查您指定之連接埠的連線，以便自動檢查容錯移轉結果
- 針對執行分散式應用程式的伺服器，設定操作順序
- 在工作流程中包含手動作業
- 在測試模式下執行 Runbook，以確認災難復原解決方案的完整性。

14.13.2 建立 Runbook

您可以依照下方的指示或觀看 [影片教學](#)。

若要開始建立 Runbook，按一下 **[建立 Runbook] > [新增步驟] > [新增動作]**。您可以使用拖放方式移動動作和步驟。請記得為 Runbook 提供一個獨特的名稱。建立冗長的 Runbook 時，請不時按一下 **[儲存]**。完成後，按一下 **[關閉]**。

步驟和動作

Runbook 包含連續執行的步驟。步驟則包含同時開始的動作。動作可包含：

- 透過雲端伺服器執行的作業 (容錯移轉伺服器、啟動伺服器、停止伺服器、容錯回復伺服器)。若要定義此作業，您必須選擇作業、雲端伺服器，以及作業參數。
- 您需要口頭描述的手動作業。作業完成後，使用者必須按一下 [確認] 按鈕，才能讓 Runbook 繼續。
- 執行另一個 Runbook。若要定義此作業，您必須選擇 Runbook。
一個 Runbook 僅能包含一個指定 Runbook 的執行。例如，如果您新增「執行 Runbook A」動作，您可以新增「執行 Runbook B」動作，但無法新增另一個「執行 Runbook A」動作。

注意事項

在此產品版本中，使用者必須手動執行容錯回復。Runbook 會在需要時顯示提示。

動作參數

雲端伺服器的所有作業都具備下列參數：

- **完成時繼續** (預設為啟用)
此參數會定義所需作業已經完成時的 Runbook 行為 (例如，已經執行容錯移轉或伺服器已經在執行)。啟用時，Runbook 會發出警告並繼續。停用時，作業和 Runbook 都將失敗。
- **失敗時繼續** (預設為停用)
此參數會定義所需作業失敗時的 Runbook 行為。啟用時，Runbook 會發出警告並繼續。停用時，作業和 Runbook 都將失敗。

完成檢查

您可以將完成檢查新增至 **[容錯移轉伺服器]** 和 **[啟動伺服器]** 動作，以確保伺服器可用並提供所需的服務。如果任何檢查失敗，則會將動作視為失敗。

- **Ping IP 位址**

此軟體將會 Ping 雲端伺服器的實際運作 IP 位址，直到伺服器回覆或逾時到期為止 (以先到者為準)。

- **連線到連接埠** (預設為 443)

此軟體將會嘗試使用其實際運作 IP 位址和您指定的連接埠，連線至雲端伺服器，直到建立連線或逾時到期為止 (以先到者為準)。如此一來，您就可以確認接聽指定之連接埠的應用程式是否正在執行。

預設逾時為 10 分鐘。如有需要，您可以加以變更。

14.13.3 Runbook 的相關作業

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

若要存取作業清單，請將滑鼠暫留在 Runbook 上，然後按一下省略符號圖示。當 Runbook 沒有在執行時，可以使用下列作業：

- 執行
- 編輯
- 複製
- 刪除

執行 Runbook

每次按一下 **[執行]** 時，都會收到執行參數的提示。這些參數適用於 Runbook 中包含的所有容錯移轉和容錯回復作業。在 **[執行 Runbook]** 作業中指定的 Runbook 會從主要 Runbook 繼承這些參數。

- **容錯移轉和容錯回復模式**

選擇您要執行測試容錯移轉 (預設) 還是實際 (實際運作) 容錯移轉。容錯回復模式將對應到選擇的容錯移轉模式。

- **容錯移轉復原點**

選擇最近的復原點 (預設) 或選取過去的時間點。如果是後者，將會為每部伺服器選取最接近指定之日期和時間前的復原點。

停止 Runbook 執行

在 Runbook 執行期間，您可以選取作業清單中的 **[停止]**。此軟體將會完成所有已經開始的動作，但需要使用者互動的動作除外。

檢視執行歷程記錄

在 **[Runbook]** 索引標籤上選取 Runbook 時，此軟體會顯示 Runbook 詳細資料以及執行歷程記錄。按一下對應到特定執行的行可檢視執行記錄。

Runbooks

Name ↑

Failback 3-2

Rb0 000

Runbook with ConfirmManualOperation

Runbook with ConfirmManualOperation

jk one server with checking port

New runbook (10)

Failover/Failback (centos-1) (Clone)

New runbook (9)

Runbook #009.

Runbook #010.

Rb0 000

Execute

Edit

Clone

Delete

Details

NameRb0 000

Description-

Execution history

Start and end time	Result	Mode
Aug 14, 5:30 PM - Aug 14, 10:27 PM	Failed	Production
Aug 14, 5:23 PM - Aug 14, 5:25 PM	Failed	Production
Aug 4, 2:45 AM - Aug 4, 2:46 AM	Completed	Test
Jul 30, 4:18 PM - Jul 30, 4:18 PM	Completed	Test
Jul 30, 4:16 PM - Jul 30, 4:16 PM	Completed	Test

15 反惡意程式碼和 Web 保護

注意事項

在 Windows 電腦上，反惡意程式碼保護和 URL 篩選功能需要安裝反惡意程式碼保護和 URL 篩選用代理程式。如果在其保護計劃中啟用 **[防毒和反惡意程式碼保護]** 或 **[URL 篩選]** 模組，則會為受保護的工作負載自動安裝該代理程式。

Cyber Protection 中的反惡意程式碼保護可為您提供下列優點：

- 所有階段的頂級保護：預防性、主動性和反應性。
- 內部的四種不同反惡意程式碼技術可提供同類最佳的多層保護。
- Microsoft Security Essentials 和 Microsoft Defender 防毒軟體的管理。

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

重要事項

只有在保護計劃中啟用 **[進階反惡意程式碼]** 選項時，才會偵測到 EICAR 測試檔案。但是，偵測不到 EICAR 檔案也不會影響 Cyber Protection 的反惡意程式碼功能。

15.1 防毒和反惡意程式碼保護

注意事項

部分功能可能需要額外的授權，端視適用的授權模型而定。

[防毒和反惡意程式碼保護] 模組可保護您的 Windows、Linux 和 macOS 電腦，免受所有最近的惡意程式碼威脅的影響。查看支援的反惡意程式碼功能完整清單：[作業系統支援的功能](#)。

Windows Security Center 支援並登錄防毒和反惡意程式碼保護。

15.1.1 反惡意程式碼功能

Windows Security Center 支援並登錄防毒和反惡意程式碼保護。

15.1.2 反惡意程式碼功能

- 在即時保護和按需模式下偵測檔案中的惡意程式碼
- 偵測處理程序中的惡意行為 (適用於 Windows)
- 封鎖對惡意 URL 的存取 (適用於 Windows)
- 將危險的檔案置入隔離區
- 將受信任的公司應用程式新增到允許名單中

15.1.3 掃描類型

您可以將防毒和反惡意程式碼保護設定為持續在背景執行或視需要執行。

即時保護

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

即時保護會檢查正在電腦上執行或開啟的所有檔案，以防止惡意程式碼威脅。

為防止潛在的相容性和效能問題，即時保護無法與也使用即時保護功能的其他防毒解決方案同時執行。其他已安裝的防毒解決方案的狀態是透過 Windows Security Center 判斷的。如果 Windows 電腦已受到其他防毒解決方案的保護，就會自動關閉即時保護。

若要啟用即時保護，請停用或解除安裝其他防毒解決方案。即時保護可以自動取代 Microsoft Defender 即時保護。

注意事項

在執行 Windows Server 作業系統的電腦上啟用即時保護時，將不會自動關閉 Microsoft Defender。系統管理員必須手動關閉 Microsoft Defender 以避免潛在的相容性問題。

您可以選擇以下其中一個掃描模式：

- **智慧型主動即時掃描** 偵測是指反惡意程式碼程式在背景執行，並在系統開機的整個持續時間內，主動且不斷地掃描電腦系統中是否有病毒和其他惡意威脅。當檔案正在執行時，以及檔案的各種操作 (例如，開啟檔案以供讀取或編輯) 期間，系統將會偵測惡意程式碼。
- **執行時偵測** 是指只有在可執行檔執行時才會進行掃描，以確保可執行檔未受感染，而且將不會對電腦或資料造成任何損害。複製受感染的檔案將不會引起注意。

排程掃描

反惡意程式碼掃描是根據排程執行的。

您可以選擇以下其中一個掃描模式。

- **快速掃描**—僅檢查工作負載系統檔案。
- **完整掃描**—檢查工作負載上的所有檔案。
- **自訂掃描**—檢查系統管理員新增至保護計劃的檔案/資料夾。

防惡意程式碼掃描完成之後，您可以在 **[監控] > [概觀] > [最近受影響]** 桌面小工具中查看受威脅影響的工作負載的詳細資料。

15.1.4 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]** 模組設定下列功能。

注意事項

本節包含所有支援的作業系統可用設定的描述。如需有關適用於您工作負載之功能的參考資料，請查看作業系統支援之 Cyber Protect 功能的表格："作業系統支援的 Cyber Protect 功能。" (第 19 頁)。

部分功能可能需要額外的授權，端視適用的授權模型而定。

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。

預設設定：**[啟用]**。

若是 Windows，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)。
對於代理程式 21.07 版和更新版本，請確認已安裝下列適用於 Windows 7 的 KB 更新：
 - 適用於 Windows Server 2008 R2、Windows 7 和 Windows Server 2008 的 SHA-2 程式碼簽署支援更新 (KB4474419)
 - 適用於 Windows 7 SP1 和 Windows Server 2008 R2 SP1 的服務堆疊更新 (KB4490628)
- 伺服器作業系統：Windows Server 2008 R2 和更新版本

必須在受保護的電腦上安裝 Windows 用代理程式。代理程式版本必須是 12.0.4290 (2017 年 10 月發行) 或更新版本。如需有關如何更新代理程式的詳細資訊，請參閱 "更新代理程式" (第 107 頁)。

若是 Linux，Active Protection 適用於執行下列作業系統的電腦：

- CentOS 6.10、7.8 和更新的次要版本
- CloudLinux 6.10、7.8 和更新的次要版本
- Ubuntu 16.04.7 和更新的次要版本

必須在受保護的電腦上安裝 Linux 用代理程式。代理程式版本必須是 15.0.26077 (2020 年 12 月發行) 或更新版本。如需支援的 Linux 核心版本清單，請參閱 Linux 用 Active Protection: 支援的核心版本 (67747)。

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**。

先進的反惡意軟體

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

[進階反惡意程式碼] 開關可啟用本機特徵比對引擎。此引擎使用增強的病毒特徵資料庫提高快速掃描和完整掃描的反惡意程式碼偵測效率。

即時保護只能搭配本機特徵比對引擎使用。

macOS 與 Linux 用防毒和反惡意程式碼保護也需要使用本機特徵比對引擎。對於 Windows，防毒和反惡意程式碼保護則不一定要搭配此引擎使用。

網路資料夾保護

[保護對應為本機磁碟機的網路資料夾] 設定會定義 Active Protection 是否會保護對應為本機磁碟機的網路資料夾免受本機惡意程序攻擊。

此設定適用於透過 SMB 或 NFS 通訊協定共用的資料夾。

如果檔案原本位於對應的磁碟機，則當 **[使用快取還原]** 動作從快取擷取該檔案時，無法儲存到原始位置。但是會儲存到此設定中指定的資料夾。Windows 的預設資料夾是

C:\ProgramData\Acronis\Restored Network Files，以及 macOS 的 Library/Application

Support/Acronis/Restored Network Files/。如果此資料夾不存在，將建立此資料夾。如果您要變更此路徑，請指定本機資料夾。不支援網路資料夾，包括對應磁碟機的資料夾。

預設設定：**[啟用]**。

伺服器端保護

此設定會定義 Active Protection 是否會保護您從外部傳入連線共用的網路資料夾，免受網路中可能帶來威脅的其他伺服器的攻擊。

預設設定：**[已停用]**。

注意事項

Linux 不支援伺服器端保護。

設定受信任和已封鎖連線

若要設定受信任或已封鎖的連線：

1. 在伺服器端保護對話方塊中，選擇一個索引標籤：
 - 若要指定能夠修改任何資料的連線，選擇 **[受信任]** 索引標籤上。
 - 若要指定無法修改任何資料的連線，選擇 **[已封鎖]** 索引標籤上。

2. 輸入下列資料：
 - 安裝保護代理程式所在電腦的電腦名稱和帳戶。
例如, MyComputer\TestUser。
 - 可以使用代理程式連線至電腦的電腦主機名稱。
3. 按一下右側的核取標記以儲存連線定義。
4. 若要新增其他連線, 按一下 **[新增]** 按鈕。

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, 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。

系統管理員可以在不啟用 **[Active Protection]** 的情況下啟用 **[自我保護]**。預設設定:**[啟用]**。

注意事項

Linux 不支援自我保護。

密碼保護

密碼保護可防止未經授權的使用者或軟體解除安裝 Windows 用代理程式或修改其元件。只有使用系統管理員可以提供的密碼才能執行這些動作。

下列動作永遠不需要密碼：

- 在本機執行安裝程式以更新安裝
- 使用 Cyber Protection Web 主控台更新安裝
- 修復安裝

預設設定:**已停用**

如需有關如何啟用密碼保護的詳細資訊, 請參閱[防止未經授權者解除安裝或修改代理程式](#)。

加密採礦程序偵測

此設定會定義 Active Protection 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。為保護您的工作負載, 建議您將加密採礦惡意程式碼加入至 **[有害的程序]** 清單。

系統管理員可以在不啟用 **[Active Protection]** 的情況下啟用 **[加密採礦程序偵測]**。預設設定:**[啟用]**。

注意事項

Linux 不支援加密採礦程序偵測。

加密採礦程序偵測設定

在 **[偵測到時採取的動作]** 中，選擇偵測到加密採礦程序時，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持隔離狀態。

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**。

如需有關此功能的詳細資訊，請參閱[隔離](#)。

行為引擎

AcronisCyber Protection 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]**。

注意事項

Linux 不支援行為引擎。

對於 macOS，在 ARM 型 Apple Silicon 處理器 (例如 Apple M1) 上不支援行為引擎。

行為引擎設定

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**。

預防利用

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

漏洞利用防禦可偵測受感染的程序並防止其散播並利用 Windows 系統上的軟體弱點。偵測到漏洞利用時，此軟體可以產生警示並停止懷疑有漏洞利用活動的程序。

漏洞利用防禦僅適用於代理程式 12.5.23130 (21.08, 2020 年 8 月發行) 版或更新版本。

預設設定：**啟用**新建立的保護計劃，並**停用**使用舊版代理程式建立的現有保護計劃。

注意事項

Linux 不支援漏洞攻擊防護。

漏洞利用防禦設定

您可以選擇偵測到漏洞利用時，程式要採取的動作，以及程式要套用的漏洞利用防禦方法。

在 **[已啟用偵測到時採取的動作]** 底下，選擇偵測到漏洞利用時要採取的動作，然後按一下 **[完成]**。

- **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。

預設設定：**停止程序**

在 **[啟用漏洞利用防禦技術]** 底下，啟用或停用您想要套用的方法，然後按一下 **[完成]**。

您可以選擇下列其中一項：

- **記憶體保護**

偵測並防止記憶體頁面執行權限的可疑修改。惡意程序會套用對頁面屬性的這類修改，以便從非可執行記憶體區域 (例如堆疊和堆積) 執行 shell 程式碼。

- **傳回導向程式設計 (ROP) 保護**

偵測並防止可讓攻擊者在存在安全性防禦 (例如，可執行空間保護和程式碼簽署) 的情況下執行程式碼的 ROP 漏洞利用技術。攻擊者會獲得呼叫堆疊的控制權，然後劫持程式控制流程，並執行惡意程式碼。

- **權限提升保護**

偵測並防止未經授權的程式碼或應用程式所進行的權限提升嘗試。惡意程式碼會使用權限提升獲得受攻擊電腦的完整存取權，然後執行重要和敏感的工作。未經授權的程式碼無法存取重要的系統資源或修改系統設定。

- **程式碼插入保護**

偵測並防止惡意程式碼插入遠端程序。程式碼插入用於將應用程式的惡意意圖隱藏在未受感染或良性的程序後面，以逃避反惡意程式碼產品的偵測。

預設設定：**已啟用所有方法**。

注意事項

系統將不會掃描 [排除] 清單中列為受信任程序的程序中是否有漏洞利用。

允許程序修改備份

只有在啟用 **[自我保護]** 設定時，才能使用 **[允許特定程序修改備份]** 設定。

此選項適用於副檔名為 .tibx、.tib、.tia，且位於本機資料夾中的檔案。

此設定可讓您指定修改備份檔案的程序，即使這些檔案受到自我保護的保護，也是如此。這很實用，例如，當您使用指令碼移除備份檔案，或將其移至其他位置時。

如果停用此設定，則只有備份軟體廠商簽署的程序可以修改備份檔案。如此可讓軟體套用保留規則，並在使用者從 Web 介面提出要求時，移除備份。其他程序 (無論是否可疑) 都無法修改備份。

如果啟用此設定，您可以允許其他程序修改備份。指定程序執行檔的完整路徑，並以磁碟機代號開頭。

預設設定：**[已停用]**。

即時保護

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

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]**。

重要事項

即時保護只能在本機特徵比對引擎開啟時使用。針對即時保護，您需要同時啟用 **[即時保護]** 開關和 **[進階反惡意程式碼]** 開關。

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**。

掃描模式：

- **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在 **保護** 計劃中選擇的檔案/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]**。

預設設定：已排程 **[快速]** 和 **[完整]** 掃描。

預設：**[自訂掃描]** 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。

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](#)」中。您可以定義下列額外的開始條件：

- **在時間視窗中分配工作開始時間** – 此選項可讓您設定工作的時間範圍，以避免網路瓶頸。您可以以小時或分鐘，指定延遲時間。例如，如果預設開始時間為上午 10:00，且延遲為 60 分鐘，則工作將會在上午 10:00 到上午 11:00 之間開始。
- **如果電腦關閉，則在電腦啟動時執行遺漏的工作**
- **防止在工作執行期間進入睡眠或休眠模式** – 此選項僅適用於執行 Windows 的電腦。
- **如果未符合開始條件，請無論如何在此時間後執行工作** – 指定無論開始條件為何，將會在其後執行工作的時段。

注意事項

Linux 不支援開始條件。

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, 隨身碟和外接式硬碟)
- **CD/DVD**

注意事項

Linux 不支援掃描卸除式磁碟機。

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或其他惡意程式碼時, 您可以定義以下的設定:

在 **[受信任]** 索引標籤上, 您可以指定:

- 絕不會被視為勒索軟體或受到監視的雜湊。
- 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:

- 一律遭到封鎖的雜湊。
- 將一律遭封鎖的程序。只要在電腦上啟用 Active Protection 或反惡意程式碼保護, 這些程序就無法啟動。

預設設定: 預設沒有定義任何排除項目。

您可以使用萬用字元 (*), 將項目新增到排除清單。

您也可以使用變數, 將項目新增到排除清單。請注意下列限制:

- 若是 Windows, 僅支援 SYSTEM 變數。不支援使用者專用的變數 (例如 %USERNAME%、%APPDATA%)。不支援包含 {username} 的變數。如需詳細資訊, 請參閱 <https://ss64.com/nt/syntax-variables.html>。
- 若是 macOS, 不支援環境變數。
- 若是 Linux, 不支援環境變數。

支援的格式的範例:

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\ *

15.2 Cyber Backup Standard 版本中的 Active Protection

在 Cyber Backup Standard 版本中，Active Protection 是保護計劃中的獨立模組。因此其可以單獨設定，並套用至不同的裝置或裝置群組。

在其他所有版本的網路保護服務中，Active Protection 是「防毒和反惡意程式碼保護」模組的一部分。

預設設定：**[啟用]**。

若是 Windows，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 \(KB2533623\)](#)。
對於代理程式 21.07 版和更新版本，請確認已安裝下列適用於 Windows 7 的 KB 更新：
 - 適用於 [Windows Server 2008 R2、Windows 7 和 Windows Server 2008 的 SHA-2 程式碼簽署支援更新 \(KB4474419\)](#)
 - 適用於 [Windows 7 SP1 和 Windows Server 2008 R2 SP1 的服務堆疊更新 \(KB4490628\)](#)
- 伺服器作業系統：Windows Server 2008 R2 和更新版本

必須在受保護的電腦上安裝 Windows 用代理程式。代理程式版本必須是 12.0.4290 (2017 年 10 月發行) 或更新版本。如需有關如何更新代理程式的詳細資訊，請參閱 "更新代理程式" (第 107 頁)。

若是 Linux，Active Protection 適用於執行下列作業系統的電腦：

- CentOS 6.10、7.8 和更新的次要版本
- CloudLinux 6.10、7.8 和更新的次要版本
- Ubuntu 16.04.7 和更新的次要版本

必須在受保護的電腦上安裝 Linux 用代理程式。代理程式版本必須是 15.0.26077 (2020 年 12 月發行) 或更新版本。如需支援的 Linux 核心版本清單，請參閱 [Linux 用 Active Protection: 支援的核心版本 \(67747\)](#)。

運作原理

Active Protection 會在受保護的機器上監控所執行的程式。當第三方程序嘗試加密檔案或進行加密貨幣採礦時，Active Protection 會產生警示，並執行額外的動作，如保護計劃中所指定。

此外，Active Protection 可避免對備份軟體自身的程式、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。

15.2.1 Cyber Backup Standard 中的 Active Protection 設定

在 Cyber Backup Standard 版本中，您可以設定下列 Active Protection 功能：

- 偵測到時採取的動作
- 自我保護
- 網路資料夾保護
- 伺服器端保護
- 加密採礦程序偵測
- 排除

注意事項

Linux 用 Active Protection 支援以下設定：偵測到時採取的動作、網路資料夾保護，以及排除項目。網路資料夾保護一律處於開啟狀態，而且無法設定。

偵測到時採取的動作

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**。

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，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。

系統管理員可以在不啟用 **[Active Protection]** 的情況下啟用 **[自我保護]**。預設設定：**[啟用]**。

注意事項

Linux 不支援自我保護。

密碼保護

密碼保護可防止未經授權的使用者或軟體解除安裝 Windows 用代理程式或修改其元件。只有使用系統管理員可以提供的密碼才能執行這些動作。

下列動作永遠不需要密碼：

- 在本機執行安裝程式以更新安裝
- 使用 Cyber Protection Web 主控台更新安裝
- 修復安裝

預設設定：**已停用**

如需有關如何啟用密碼保護的詳細資訊，請參閱[防止未經授權者解除安裝或修改代理程式](#)。

網路資料夾保護

[保護對應為本機磁碟機的網路資料夾] 設定會定義 Active Protection 是否會保護對應為本機磁碟機的網路資料夾免受本機惡意程序攻擊。

此設定適用於透過 SMB 或 NFS 通訊協定共用的資料夾。

如果檔案原本位於對應的磁碟機，則當 **[使用快取還原]** 動作從快取擷取該檔案時，無法儲存到原始位置。但是會儲存到此設定中指定的資料夾。Windows 的預設資料夾是

C:\ProgramData\Acronis\Restored Network Files，以及 macOS 的 Library/Application

Support/Acronis/Restored Network Files/。如果此資料夾不存在，將建立此資料夾。如果您要變更此路徑，請指定本機資料夾。不支援網路資料夾，包括對應磁碟機的資料夾。

預設設定：**[啟用]**。

伺服器端保護

此設定會定義 Active Protection 是否會保護您從外部傳入連線共用的網路資料夾，免受網路中可能帶來威脅的其他伺服器的攻擊。

預設設定：**[已停用]**。

注意事項

Linux 不支援伺服器端保護。

設定受信任和已封鎖連線

若要設定受信任或已封鎖的連線：

1. 在伺服器端保護對話方塊中，選擇一個索引標籤：
 - 若要指定能夠修改任何資料的連線，選擇 **[受信任]** 索引標籤上。
 - 若要指定無法修改任何資料的連線，選擇 **[已封鎖]** 索引標籤上。
2. 輸入下列資料：
 - 安裝保護代理程式所在電腦的電腦名稱和帳戶。
例如，MyComputer\TestUser。
 - 可以使用代理程式連線至電腦的電腦主機名稱。
3. 按一下右側的核取標記以儲存連線定義。
4. 若要新增其他連線，按一下 **[新增]** 按鈕。

加密採礦程序偵測

此設定會定義 Active Protection 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。為保護您的工作負載，建議您將加密採礦惡意程式碼加入至 **[有害的程序]** 清單。

系統管理員可以在不啟用 **[Active Protection]** 的情況下啟用 **[加密採礦程序偵測]**。預設設定：**[啟用]**。

注意事項

Linux 不支援加密採礦程序偵測。

加密採礦程序偵測設定

在 **[偵測到時採取的動作]** 中，選擇偵測到加密採礦程序時，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**。

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或其他惡意程式碼時，您可以定義以下的設定：

在 **[受信任]** 索引標籤上，您可以指定：

- 絕不會被視為勒索軟體或受到監視的雜湊。
- 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：

- 一律遭到封鎖的雜湊。
- 將一律遭封鎖的程序。只要在電腦上啟用 Active Protection 或反惡意程式碼保護，這些程序就無法啟動。

預設設定：預設沒有定義任何排除項目。

您可以使用萬用字元 (*)，將項目新增到排除清單。

您也可以使用變數，將項目新增到排除清單。請注意下列限制：

- 若是 Windows，僅支援 SYSTEM 變數。不支援使用者專用的變數 (例如 %USERNAME%、%APPDATA%)。不支援包含 {username} 的變數。如需詳細資訊，請參閱

<https://ss64.com/nt/syntax-variables.html>。

- 若是 macOS, 不支援環境變數。
- 若是 Linux, 不支援環境變數。

支援的格式的範例：

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\ *

15.3 URL 篩選

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

惡意程式碼通常是由惡意網站或受感染的網站散佈, 並使用所謂的**路過式下載**感染方法。

「URL 篩選」功能可讓您保護電腦, 免受來自網際網路的惡意程式碼和網路釣魚等威脅。您可以透過封鎖對可能含有惡意內容之網站的使用者存取, 以保護貴組織。URL 篩選資料庫也包含網站的相關資料, 這些網站對 COVID-19、詐欺和網路釣魚 URL 的資訊存在爭議。因此, 當使用者嘗試開啟這類網站時, 系統將會自動加以封鎖。

URL 篩選也可讓您控制網路使用量以符合外部法規和公司內部政策。您可以根據網站的相關類別, 設定其存取權。URL 篩選目前支援 44 個網站類別, 並允許管理其存取權。

目前, 保護代理程式將會檢查 Windows 電腦上的 HTTP/HTTPS 連線。

URL 篩選功能需要有網際網路連線才能運作。

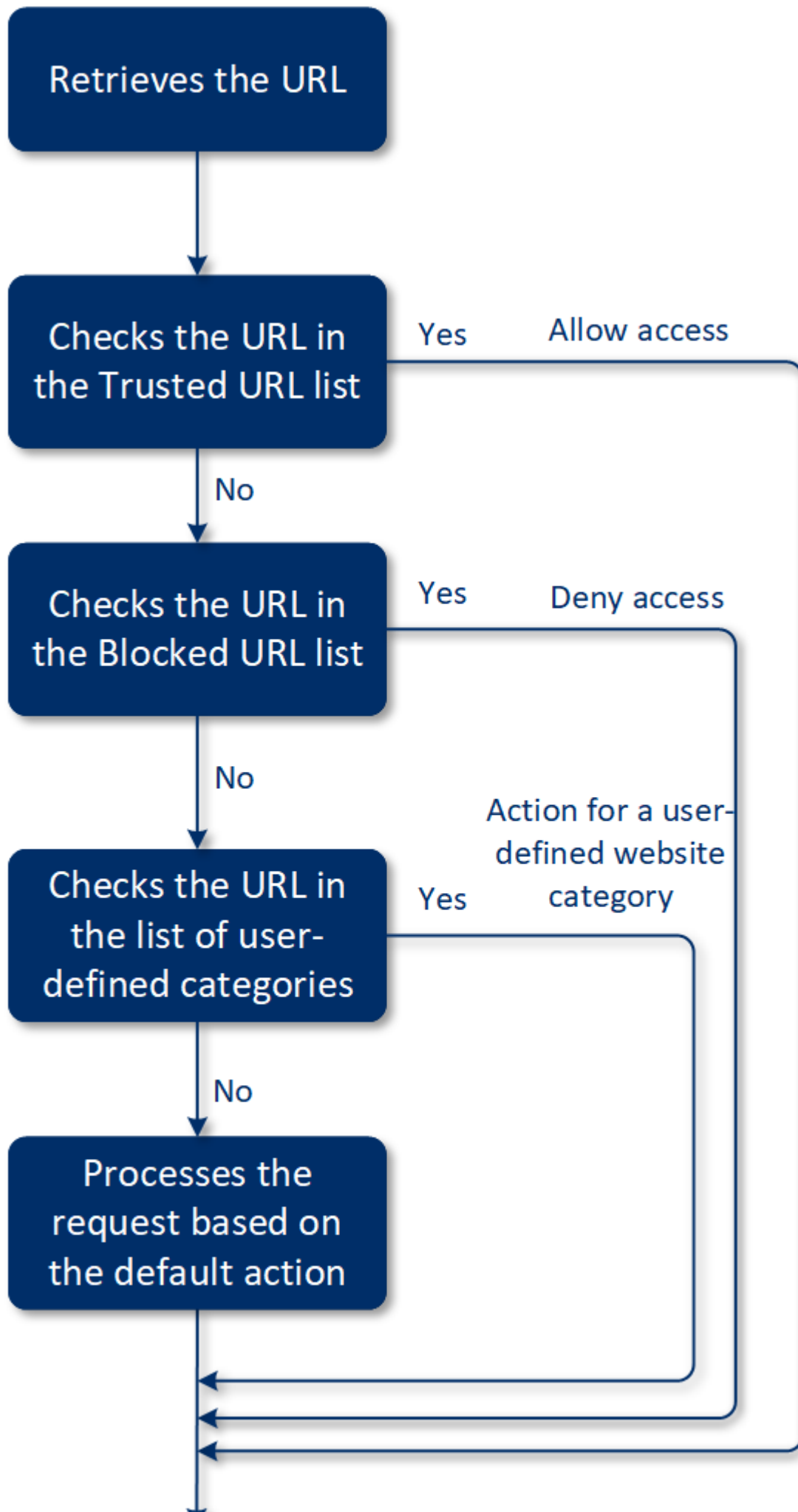
注意事項

為防止可能發生的網路保護代理程式組建 15.0.26692 (版本 C21.03 HF1) 和更舊版本相容性問題, 如果偵測到其他防毒解決方案, 或者如果系統上沒有 Windows 資訊安全中心服務, 則會自動停用 URL 篩選功能。

在之後的網路保護代理程式中, 相容性問題會獲得解決, 因此根據原則, 一律啟用 URL 篩選。

15.3.1 運作原理

使用者在瀏覽器中輸入一個 URL 連結。攔截器取得連結, 並傳送到保護代理程式中。代理程式取得 URL、進行剖析, 然後檢查結果。攔截器將使用者重新導向至含有訊息的頁面, 此訊息中含有手動前往所要求頁面的可用動作。

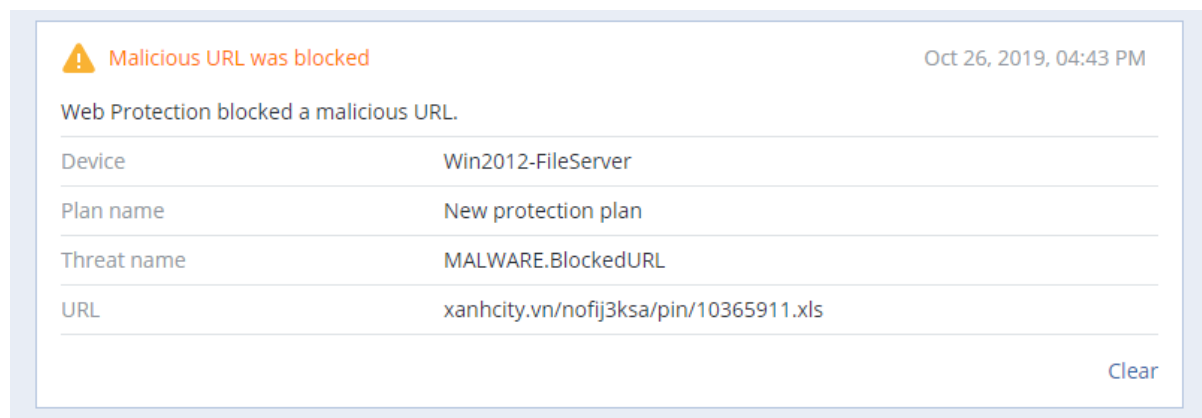


15.3.2 URL 篩選設定工作流程

一般而言，URL 篩選設定包含下列步驟：

1. 在啟用 **[URL 篩選]** 模組的情況下，[建立一個保護計劃](#)。
2. 指定 URL 篩選設定 (請參閱以下內容)。
3. 將保護計劃指派給電腦。

若要檢查已遭到封鎖的 URL，請移至 **[監控] > [警示]**。



15.3.3 URL 篩選設定

您可以針對 **[URL 篩選]** 模組指定下列設定。

惡意網站存取

指定當使用者開啟惡意網站時將執行的動作：

- **封鎖** – 封鎖對惡意網站的存取。使用者將無法存取網站，而且系統將會產生一個警告警示。
- **一律詢問使用者** – 詢問使用者仍要繼續前往網站還是要返回。

要篩選的類別

您可以設定其存取權的網站有 44 個：

- **允許** – 允許存取與所選類別相關的網站。
- **拒絕** – 拒絕存取與所選類別相關的網站。

系統預設允許所有類別。

顯示依類別封鎖之 URL 的所有通知 – 如果啟用，您將收到系統匣中顯示的所有通知 (依類別封鎖的 URL)。如果某個網站有數個子網域，則系統也會為其產生通知，因此通知數量可能很大。

在下表中，您可以找到類別描述：

	網站類別	描述

1	廣告	此類別涵蓋其主要用途為提供廣告服務的網域。
2	留言板	此類別涵蓋論壇、討論區和問答型網站。此類別未涵蓋公司網站上客戶提出問題的特定部分。
3	個人網站	此類別涵蓋個人網站以及所有類型的部落格：個人、團體甚至公司部落格。部落格是在全球資訊網上發佈的一種日誌。其由條目（「貼文」）所組成，通常以相反的時間順序顯示，因此最新的貼文最先顯示。
4	公司/商業網站	這是一個廣泛的類別，其中涵蓋通常不屬於其他任何類別的公司網站。
5	電腦軟體	此類別涵蓋提供電腦軟體的網站，通常是開放原始碼、免費軟體或共享軟體。其可能也涵蓋線上軟體商店。
6	醫療藥品	此類別涵蓋與藥品/酒精/煙草相關的網站，其中討論（合法）醫療藥品或器材、酒精或煙草產品的使用或銷售。 請注意，非法藥物涵蓋在「毒品」類別中。
7	教育	此類別涵蓋屬於正式教育機構的網站，包括 .edu 網域之外的網站。其也包含教育網站，例如 Encyclopedia。
8	娛樂	此類別涵蓋提供與藝術活動和博物館相關資訊的網站，以及評論或評價電影、音樂或藝術等內容的網站。
9	檔案共用	此類別涵蓋使用者可以在其中上傳檔案並與他人共用的檔案共用網站。其也涵蓋 torrent 共享網站和 torrent 追蹤器。
10	財務	此類別涵蓋屬於全球所有提供線上存取的銀行的網站。部分信用合作社和其他金融機構也涵蓋在內。但是，可能不包括部分本地銀行。
11	賭博	此類別涵蓋賭博網站。這些是「線上賭場」或「線上樂透彩」類型網站，通常需要先付款，使用者才能在線上輪盤、撲克牌、21 點或類似遊戲中賭博。其中有一些是合法的，也就是有贏的機會；有一些則是欺詐性的，也就是沒有贏的機會。它還會偵測「密技和作弊」網站，其中描述在賭博和線上樂透彩網站上賺錢的方式。
12	遊戲	此類別涵蓋提供線上遊戲的網站，這些網站通常是以 Adobe Flash 或 Java Applet。偵測遊戲是免費的還是需要訂購授權並不重要，但是，在「賭博」類別中會偵測賭場形式的網站。 以下類別不涵蓋在內： • 開發電玩遊戲的公司的官方網站（除非他們製作線上遊戲） • 討論遊戲的討論網站 • 可以下載非線上遊戲的網站（其中部分屬於「非法」類別） • 要求使用者下載並執行可執行檔的遊戲，例如《魔獸世界》；可以透過不同方式（例如，防火牆）防禦的遊戲
13	政府機構	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	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

	侵	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	浪費時間	此類別涵蓋個人傾向於花費大量時間的網站。這可能包括其他類別的網站，例如，社交網路或娛樂。
39	旅遊	此類別涵蓋顯示旅遊優惠和旅遊裝備以及旅遊目的地評論和評等的網站。
40	影片	此類別涵蓋裝載各種影片或相片的網站，這些內容是由使用者上傳或由各種內容提供者所提供。這包括 YouTube、Metacafe、Google Video 之類的網站，以及 Picasa 或 Flickr 之類的相片網站。其也會偵測到其他網站或部落格中內嵌的影片。
41	暴力卡通	此類別涵蓋討論、分享和提供暴力卡通或漫畫的網站，這些內容可能會因為暴力、露骨的語言或色情內容而不適合未成年人。 此類別未涵蓋提供《湯姆貓與傑利鼠》等主流卡通的網站。
42	武器	此類別涵蓋提供武器出售或交換、製造或使用的網站。其也涵蓋打獵資源與空氣槍和 BB 槍的使用，以及格鬥武器。
43	電子郵件	此類別涵蓋以 Web 應用程式提供電子郵件功能的網站。
44	Web Proxy	此類別涵蓋提供 Web Proxy 服務的網站。這是一個當使用者開啟網頁、在表單中輸入所要求的 URL，然後按一下[提交]時的「瀏覽器內的瀏覽器」類型網站。Web Proxy 網站會下載實際的網頁，並將其顯示在使用者瀏覽器內。

	偵測到 (而且可能需要封鎖) 這個類型的原因如下： • 用於匿名瀏覽。由於對目的地網頁伺服器的要求是從 Proxy 網頁伺服器發出的，因此只能看到其 IP 位址，而且如果伺服器系統管理員追蹤使用者，則追蹤將在 Web Proxy 上結束，這不一定會保留找出原始使用者所需的記錄。 • 用於位置詐騙。使用者 IP 位址通常用於依來源位置分析服務 (部分國家政府網站可能只能從本機 IP 位址存取)，而且這些服務可協助使用者欺騙其真實位置。 • 用於存取禁止的內容。如果使用簡單的 URL 篩選，將只會看到 Web Proxy URL，而不會看到使用者所造訪的實際伺服器。 • 用於避免公司監視。公司政策可能會要求監視員工的網際網路使用情況。透過 Web Proxy 存取所有內容時，使用者可能會逃避將不會提供正確資訊的監視。 SDK 不僅會分析 HTML 網頁 (若有提供)，還會分析 URL，因此對於某些類別而言，SDK 將仍然能夠偵測到內容。但是，僅使用 SDK 無法避免其他原因。

排除

URL

已知為安全的網域名稱或 IP 位址可以新增到受信任 URL 的清單中。代表威脅的網域名稱或 IP 位址可以新增到已封鎖 URL 的清單中。

若要將主機新增到受信任的 URL，按一下 **[受信任]** 索引標籤上的 **[新增]**，然後指定特定的網域名稱或 IP 位址。

若要將主機新增到已封鎖的 URL，按一下 **[已封鎖]** 索引標籤上的 **[新增]**，然後指定特定的網域名稱或 IP 位址。

注意事項

您輸入的網域中的所有位址都將被視為受信任或已封鎖。例如，如果您輸入 **xyz.com** 作為受信任的網域，**xyz.com** 底下的所有路徑或子網域都會被視為受信任。

輸入網域名稱時，請不要包含 **"www."** 首碼。

程序

絕不會被視為惡意程式碼的程序可以新增至受信任程序的清單。由 **Microsoft** 簽署的程序一律受到信任。

URL 篩選支援僅排除受信任的程序。您無法將程序新增至封鎖清單。

預設設定：預設沒有定義任何排除項目。

您可以使用萬用字元 (*****)，將項目新增至受信任程序的清單。請注意，路徑開頭不支援萬用字元，但僅在結尾支援。

您也可以使用變數，將項目新增至程序排除清單。請注意下列限制：

- 若是 Windows，僅支援 **SYSTEM** 變數。不支援使用者專用的變數，例如 **%USERNAME%** 或 **%APPDATA%**。不支援包含 {username} 的變數。如需詳細資訊，請參閱

<https://ss64.com/nt/syntax-variables.html>。

- 不支援網路路徑。
- 若是 macOS, 不支援環境變數。
- 若是 Linux, 不支援環境變數。

支援的格式的範例：

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\ *

15.4 Microsoft Defender 防毒軟體與 Microsoft Security Essentials

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

Microsoft Defender 防毒軟體

Microsoft Defender 防毒軟體是 Microsoft Windows 從 Windows 8 開始提供的一種內建反惡意程式碼元件。

Microsoft Defender 防毒軟體 (WDA) 模組可讓您透過 Cyber Protection 服務主控台, 設定 Microsoft Defender 防毒軟體安全性原則並追蹤其狀態。

此模組適用於已安裝 Microsoft Defender 防毒軟體的電腦。

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 Protection 服務主控台, 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 的設定與 Microsoft Defender 防毒軟體的設定類似, 但是您無法設定即時保護, 而且無法透過 Cyber Protection 服務主控台定義排除項目。

15.4.1 排程掃描

指定排程掃描的排程。

掃描模式：

- **完整** – 除了在快速掃描中掃描的項目之外, 完整檢查所有檔案和資料夾。相較於快速掃描, 完整掃描需要更多用於執行的電腦資源。

- **快速** – 快速檢查通常會找到惡意程式碼的記憶體內程序和資料夾。快速掃描需要用於執行的電腦資源較少。

定義執行掃描的時間和星期幾。

每日快速掃描 – 定義每日快速掃描的時間。

您可以根據您的需求，設定以下選項：

當電腦開啟但未使用中時，啟動排程掃描

執行排程掃描之前，檢查最新的病毒和間諜軟體定義

進行下列掃描期間，限制 CPU 使用量

如需有關 Microsoft Defender 防毒軟體設定的詳細資訊，請參閱 <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings>

15.4.2 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 Microsoft Defender 防毒軟體預設動作設定的詳細資訊，請參閱 <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings>

15.4.3 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 Microsoft Defender 防毒軟體即時保護設定的詳細資訊，請參閱 <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings>

15.4.4 進階

指定進階掃描設定：

- **掃描存檔檔案** – 將存檔檔案 (例如 .zip 或 .rar 檔案) 包含在掃描中。
- **掃描卸除式磁碟機** – 在完整掃描期間掃描卸除式磁碟機。
- **建立系統還原點** – 在某些情況下，重要檔案或登錄項目可能會被當作「誤報」遭到移除，則您將能夠從還原點復原。
- **在下列時間後移除隔離的檔案** – 定義將移除隔離檔案的期限。
- **需要進一步分析時，自動傳送檔案範例：**
 - **一律提示** – 檔案傳送之前，將會要求您確認。
 - **自動傳送安全範例** – 大多數範例將會自動傳送，但可能包含個人資訊的檔案除外。這類檔案將需要另外確認。
 - **自動傳送所有範例** – 系統將自動傳送所有範例。
- **停用 Windows Defender 防毒軟體 GUI** – 如果已選擇，使用者將無法使用 WDA 使用者介面。您可以透過 Cyber Protection 服務主控台管理 WDA 原則。
- **MAPS (Microsoft Active Protection Service)** – 可協助您選擇如何回應潛在威脅的線上社群。
 - **我不要加入 MAPS** – 對於偵測到的軟體，將不會傳送任何資訊給 Microsoft。
 - **基本成員資格** – 對於偵測到的軟體，將會傳送基本資訊給 Microsoft。
 - **進階成員資格** – 對於偵測到的軟體，將會傳送更詳細的資訊給 Microsoft。

如需詳細資訊，請參閱 <https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise/>

如需有關 Microsoft Defender 防毒軟體進階設定的詳細資訊，請參閱

<https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings>

15.4.5 排除

您可以定義下列要從掃描排除的檔案和資料夾：

- **程序** – 將會從掃描中排除已定義之程序讀取或寫入的任何檔案。您需要定義程序可執行檔的完整路徑。
- **檔案和資料夾** – 指定的檔案和資料夾將從掃描排除。您需要定義資料夾或檔案的完整路徑，或定義副檔名。

如需有關 Microsoft Defender 防毒軟體排除設定的詳細資訊，請參閱

<https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings>

15.5 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。

15.5.1 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。

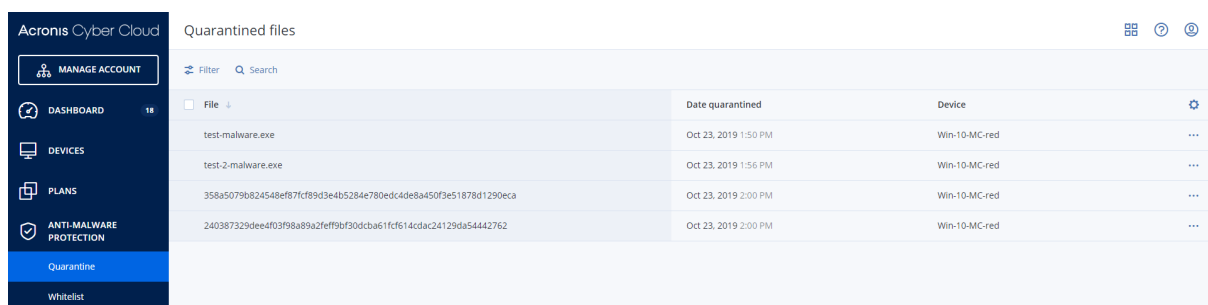
15.5.2 管理隔離的檔案

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。您可以使用相同的檔案雜湊，刪除所有檔案。您可以使用相同的檔案雜湊，還原所有檔案。依雜湊為檔案分組、選擇需要的檔案，然後刪除這些檔案。
- **還原** – 在不進行任何修改的情況下，將隔離的檔案還原到原始位置。如果目前在原始位置中有名稱相同的檔案，則該檔案將會以還原的檔案覆寫。請注意，系統會將已還原的檔案加入至白名單中，並在進一步的反惡意程式碼掃描期間略過該檔案。



Quarantined files		
File	Date quarantined	Device
test-malware.exe	Oct 23, 2019 1:50 PM	Win-10-MC-red
test-2-malware.exe	Oct 23, 2019 1:56 PM	Win-10-MC-red
358a5079b824548ef87cf89d3e4b5284e780edc4de8a450f3e51878d1290eca	Oct 23, 2019 2:00 PM	Win-10-MC-red
240387329dee4f03f98a89a2feff9bf30dcba61fcf614cdac24129da54442762	Oct 23, 2019 2:00 PM	Win-10-MC-red

15.5.3 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 電腦：/Library/Application Support/Acronis/Quarantine
- 若是 Linux 電腦：/opt/acronis/Quarantine

隔離儲存空間受到服務提供者的自我防衛保護。

15.6 隨選自助服務自訂資料夾

您可以在工作負載上選擇自訂資料夾，然後直接從內容功能表掃描這些資料夾。

若要在內容功能表中存取使用 **Cyber Protect** 選項進行掃描

對於已在保護計劃中啟用防毒和反惡意程式碼的工作負載，以滑鼠右鍵按一下您要掃描的檔案/資料夾。

注意事項

此選項僅適用於工作負載的系統管理員。

15.7 公司白名單

防毒解決方案可能會將合法的公司專用應用程式視為可疑的應用程式。為防止這些誤報偵測，必須將信任的應用程式手動新增到白名單，這非常耗時。

Cyber Protection 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。

系統會針對每個客戶，而且僅基於此客戶的資料，建立白名單。

您可以啟用和停用白名單。停用白名單時，會暫時隱藏其中新增的檔案。

注意事項

只有擁有系統管理員角色的帳戶 (例如，Cyber Protection 系統管理員；公司系統管理員；代表公司系統管理員行事的合作夥伴系統管理員；單位系統管理員) 才可以設定和管理白名單。此功能不適用於唯讀系統管理員帳戶或使用者帳戶。

15.7.1 自動新增至白名單

1. 在至少兩部電腦上對備份執行雲端掃描。您可以使用 [備份掃描計劃](#) 達到這個目的。
2. 在白名單設定中，啟用 **[自動產生白名單]** 開關。

15.7.2 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. 在服務主控台中，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]**。

15.7.3 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. 在服務主控台中，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]**。

15.7.4 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。

15.7.5 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。

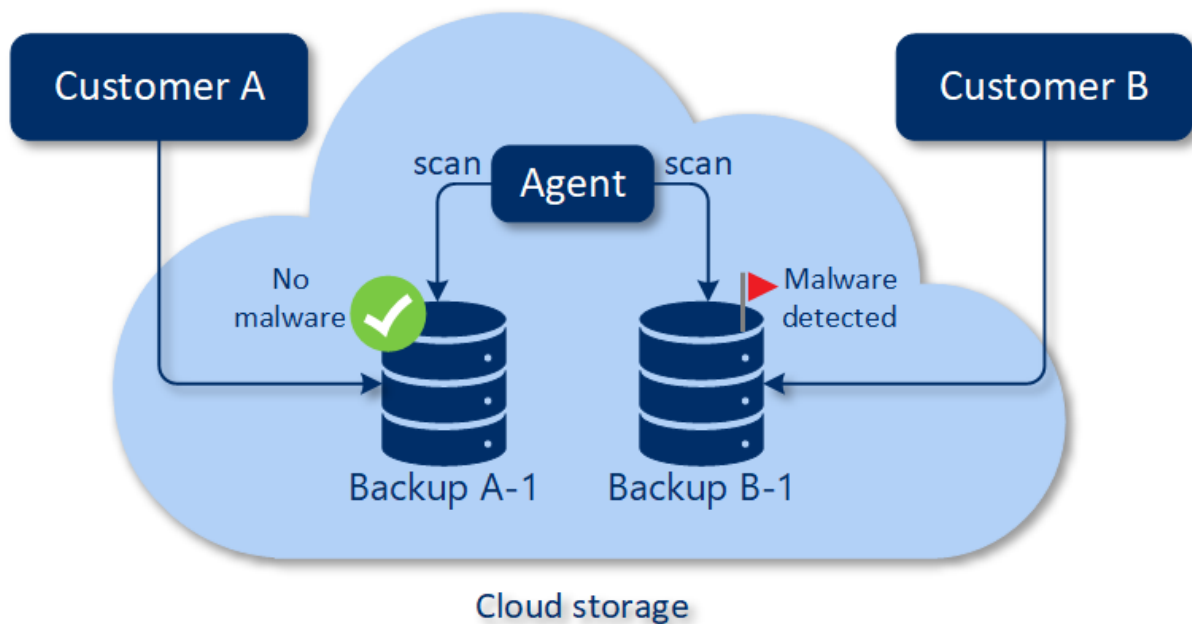
15.8 備份的反惡意程式碼掃描

備份掃描功能可讓您防止從備份還原受感染的檔案。您可以使用此功能檢查備份是否未受感染 (未受惡意程式碼感染)。只有 Windows 作業系統支援備份掃描功能。

備份掃描是雲端代理程式在使用者電腦之外的環境中執行的，也就是在 Acronis 雲端。每個新的備份掃描計劃都會建立一個新的掃描工作，該工作會放入目前資料中心的共同佇列中，並根據佇列中的順序，進行處理。掃描所需的時間取決於備份大小，因此在建立備份掃描計劃並執行後，可能會經歷一些延遲。

如果未執行備份掃描，則備份會留在 **[未掃描]** 狀態。執行備份掃描之後，備份將變成下列其中一種狀態：

- **無惡意程式碼**
- **偵測到惡意程式碼**



備份掃描可以透過使用備份掃描計劃來設定。

15.8.1 如何在雲端設定備份掃描

請注意下列情況：

- 支援的備份類型為「整部電腦」或「磁碟/磁碟區」備份。
- 僅掃描具有 GPT 和 MBR 磁碟分割之 NTFS 檔案系統的磁碟區。
- 支援的備份位置為雲端儲存空間 (目前僅託管 Acronis)。
- 您可以選擇包含 [CDP 復原點](#) 的備份進行掃描, 但僅能掃描一般復原點 (不包括 CDP 復原點)。
- 選擇 CDP 備份對整部機器進行安全復原時, 將會在沒有 CDP 復原點中資料的情況下, 安全地復原電腦。若要還原 CDP 資料, 請啟動 [檔案/資料夾] 復原活動。

若要在雲端設定備份掃描, 請建立一個[備份掃描計劃](#)。

備份掃描的結果可以在「[備份掃描詳細資料](#)」桌面小工具中的監控儀表板上找到。

16 進階保護

根據預設，Cyber Protect 包含涵蓋大多數網路安全威脅的功能。不需要額外的費用，您就可以使用這些功能。此外，您也可以啟用進階功能增強對工作負載的保護。

如果啟用進階保護功能供您使用，則該功能會出現在以進階功能圖示  標示的保護計劃中。當您嘗試啟用此功能時，系統會提示您將收取額外費用。

如果未啟用進階保護功能供您使用，則下列圖示會出現在保護計劃  中的功能名稱旁邊。此時會出現一個訊息，提示您聯絡系統管理員，以便為您啟用所需的進階套件。

16.1 進階版資料洩漏防禦

重要事項

這是優先體驗版本的進階版資料洩漏防禦文件。部分功能和描述可能不完整。

進階版資料洩漏防禦模組會分析受保護工作負載上資料傳輸的內容和環境，並根據資料流程原則，防止透過週邊裝置或公司網路內外的網路傳輸，洩漏敏感資料。

如果為此客戶啟用保護服務和進階版資料洩漏防禦套件，則可以將進階版資料洩漏防禦功能包含在客戶租用戶的任何保護計劃中。

開始使用 [進階版資料洩漏防禦] 模組之前，請確認您閱讀並瞭解[基礎指南](#)中所述之進階版 DLP 管理的基本概念和邏輯。

16.1.1 建立資料流程原則和原則規則

重要事項

這是優先體驗版本的進階版資料洩漏防禦文件。部分功能和描述可能不完整。

資料洩漏防禦的主要原則要求應該允許公司 IT 系統的使用者僅在執行其工作職責所需的範圍內，處理敏感資料。其他任何敏感資料傳輸 (與業務流程不相關) 應該遭到封鎖。因此，區分與業務相關的資料傳輸和欺詐資料傳輸或流程至關重要。

資料流程原則包含指定允許哪些資料流程以及禁止哪些資料流程的規則，從而在保護計劃中啟用 [資料洩漏防禦] 模組並在 [執行] 模式下執行時，防止未經授權傳輸機密資訊。

原則中的每個敏感度類別都包含一個預設規則 (以星號 (*) 標示) 以及一個或多個明確 (非預設) 規則 (用於定義特定使用者或群組的資料流程)。在[基礎指南](#)中閱讀更多關於原則規則類型的資訊。

在觀察模式下執行進階版資料洩漏防禦時，通常會自動建立資料流程原則。建立代表性資料流程原則所需的時間大約是一個月，但根據您組織的業務流程，可能有所不同。資料流程原則也可以由公司或單位系統管理員手動建立、設定或編輯。

若要開始自動建立資料流程原則

1. 以系統管理員身分登入 Cyber Protect 服務主控台。
2. 導覽至 **[管理]** > **[保護計劃]**。
3. 按一下 **[建立計劃]**。
4. 展開 **[資料洩漏防禦]** 區段，然後按一下 **[模式]** 列。
5. 在 **[模式]** 對話方塊中，選擇 **[觀察模式]**，然後選擇處理資料傳輸的方式：

選 項	描述
全 部 允 許	從使用者工作負載進行的所有敏感資料傳輸都會被視為業務流程所需，而且安全無虞。系統會針對不符合原則中已定義規則的每個偵測到的資料流程，建立一個新規則。
全 部 證 明	從使用者工作負載進行的所有敏感資料傳輸都會被視為業務流程所需，但是有風險。因此，每次將敏感資料傳輸至不符合先前所建立資料流程的任何收件者或目的地（組織內部和外部）遭到攔截時，使用者都必須提供一次性的業務理由。提交理由後，就會在資料流程原則中建立一個新的資料流程規則。
混 合	系統會針對所有內部敏感資料流程套用 [允許所有邏輯] ，並針對所有外部資料流程套用 [證明所有邏輯] 。

6. 儲存保護計劃並將其套用至您要從中收集資料的工作負載以建立原則。

注意事項

在觀察模式期間無法防止資料洩漏。

若要手動設定資料流程原則

1. 在 Cyber Protect 服務主控台中，導覽至 **[保護]** > **[資料流程原則]**。
2. 按一下 **[新增資料流程規則]**。
[新增資料流程規則] 窗格隨即在右側展開。
3. 選擇敏感度類別、新增寄件者和收件者，然後針對所選類別、寄件者和收件者，定義資料傳輸的權限。

選 項	描述
允 許	允許此寄件者將這個敏感度類別的資料傳輸給此收件者。
例 外	不允許此寄件者將這個敏感度類別的資料傳輸給此收件者，但允許寄件者針對特定傳輸提交規則的例外。 當此寄件者嘗試將這個敏感度類別的資料傳輸給此收件者時，封鎖傳輸，並要求寄件者提交例外以允許此次傳輸。提交例外之後，就允許繼續進行資料傳輸。 重要事項 提交例外之後，將允許此寄件者與這個敏感度類別的收件者之間所有後續的資料傳輸。

選項	描述
拒絕	不允許此寄件者將這個敏感度類別的資料傳輸給此收件者，而且不允許寄件者要求規則的例外。

4. (選擇性) 選擇在觸發規則時應該執行的動作。

動作	描述
在記錄中寫入	觸發規則時，在事件檢視中儲存事件記錄。建議針對具有 [例外] 權限的規則選擇此動作。
產生警示	觸發規則時，在 Cyber Protect [警示] 索引標籤中產生警示。如果針對系統管理員啟用通知，也將傳送電子郵件通知。
資料傳輸遭到拒絕時通知終端使用者	當使用者觸發規則時，以畫面上的警告即時通知他們。

5. 按一下 **[儲存]**。

6. 重複步驟 2 到 5 以便為不同敏感度類別和選項建立多個規則，並確認所產生的規則對應到您選擇的選項。

資料流程原則結構

重要事項

這是優先體驗版本的進階版資料洩漏防禦文件。部分功能和描述可能不完整。

在 **[資料流程原則]** 檢視中，原則規則會根據其所控制的敏感資料類別分組。敏感度類別識別碼會顯示在原則規則群組的正上方。

- 敏感
 - 受保護的健康資訊 (PHI)
 - 個人識別資訊 (PII)
 - 支付卡產業資料安全標準 (PCI DSS),
 - 已標示為機密
- 非敏感

如需有關資料流程原則概念和功能的詳細資訊，請參閱[基礎指南](#)。

規則結構

每個原則規則都包含下列元素。

- 敏感度類別
 - 受保護的健康資訊 (PHI)
 - 個人識別資訊 (PII)
 - 支付卡產業資料安全標準 (PCI DSS)

- 已標示為機密
請參閱 "敏感資料定義" (第 440 頁)
- **寄件者** - 指定受此規則控制之資料傳輸的起始端。它可能是單一使用者、使用者清單或使用者群組。
 - **任何內部** - 包含組織所有內部使用者的使用者群組。
 - **聯絡人/寄件者組織** - 組織中的 Windows 帳戶, 由進階版資料洩漏防禦識別。
 - **聯絡人/自訂身分識別** - 以下列其中一種格式指定的內部使用者識別碼: 電子郵件、Skype ID、ICQ 識別碼、IRC 識別碼、Jabber 電子郵件、Mail.ru Agent 電子郵件、Viber 電話號碼、Zoom 電子郵件。
下列萬用字元可以用於指定一組聯絡人:
 - * - 任意數目的符號
 - ? - 任何單一符號
- **收件者** - 指定受此規則控制之資料傳輸的目的地。它可能是單一使用者、使用者清單或使用者群組, 以及以下所指定的其他類型目的地。
 - **任何** - 進階版 DLP 支援的任何收件者類型。
 - **聯絡人/任何聯絡人** - 任何內部或外部聯絡人。
 - **聯絡人/任何內部聯絡人** - 任何內部使用者的聯絡人。
 - **聯絡人/任何外部聯絡人** - 任何外部人員或實體的聯絡人。
 - **聯絡人/寄件者組織** - 與 [寄件者] 欄位中描述的原則相同。
 - **聯絡人/自訂身分識別** - 與 [寄件者] 欄位中描述的原則相同。
 - **檔案共用服務** - 受控制的檔案共用服務識別碼。
 - **社群網路** - 受控制的社群網路識別碼。
 - **主機/任何主機** - 進階版 DLP 視為內部或外部的任何電腦。
 - **主機/任何內部主機** - 進階版 DLP 視為內部的任何電腦。
 - **主機/任何外部主機** - 進階版 DLP 視為外部的任何電腦。
 - **主機/特定主機** - 指定為主機名稱的電腦識別碼 (例如 FQDN) 或 IP 位址 (IPv4 或 IPv6)。
 - **裝置/任何裝置** - 連線到工作負載的任何週邊裝置。
 - **裝置/外部裝置** - 連線到工作負載的卸除式儲存裝置或重新導向的對應磁碟機。
 - **裝置/重新導向的剪貼簿** - 連線到工作負載的重新導向的剪貼簿。
 - **印表機** - 連線到工作負載的任何本機或網路印表機。
- **權限** - 透過此規則控制的資料傳輸執行的預防性控制。詳述於主題 [資料流程原則規則中的權限](#)。
- **動作** - 觸發此規則時執行的非預防性動作。根據預設, 此欄位設定為 [無動作]。這些選項包括:
 - **在記錄中寫入** - 觸發規則時, 在稽核記錄中儲存事件記錄。
 - **資料傳輸遭到拒絕時通知終端使用者** - 觸發規則時, 以畫面上的即時警告通知使用者。
 - **產生警示** - 觸發規則時, 警示系統管理員。

什麼會觸發原則規則?

如果下列所有條件都成立, 則表示資料傳輸符合資料流程原則規則:

- 此資料傳輸的所有寄件者都有列出或屬於規則的 **[寄件者]** 欄位中指定的使用者群組。
- 此資料傳輸的所有收件者都有列出或屬於規則的 **[收件者]** 欄位中指定的使用者群組。

- 要傳輸的資料符合規則的**敏感度類別**。

調整資料流程原則規則中的權限

進階版資料洩漏防禦支援資料流程原則規則中的三種權限。這些權限是在每個原則規則中個別設定的。

允許 (許可) 允許符合在規則中定義之敏感度類別、寄件者和收件者組合的資料傳輸。

例外 (禁止) 不允許符合在規則中定義之敏感度類別、寄件者和收件者組合的資料傳輸，但是寄件者可以提交規則的例外以允許特定傳輸。

重要事項

提交例外之後，將允許此寄件者與這個敏感度類別的收件者之間所有後續的資料傳輸。

拒絕 (禁止) 不允許符合在規則中定義之敏感度類別、寄件者和收件者組合的資料傳輸，而且寄件者無法選擇提交例外。

此外，還可以將優先順序旗標指派給 **[允許]** 和 **[例外]** 權限，以提高原則管理的靈活性。您可以透過這個設定，在原則的其他資料流程規則中，覆寫針對特定群組設定的權限。您可以使用該權限，將群組資料流程規則僅套用到其部分成員。為達到此目的，您必須針對您要從群組規則中排除的特定使用者，建立資料流程規則，然後將其權限的優先順序設定為高於在規則中，針對這些使用者所屬群組設定的資料流程限制。如需結合規則時權限優先順序的相關資訊，請參閱 "結合資料流程原則規則" (第 434 頁)。

重要事項

將公司或單位原則從 **[觀察]** 模式切換到 **[執行]** 模式之前，將每個敏感資料類別的預設規則從許可狀態調整為禁止狀態。在 **[資料流程原則]** 檢視中，預設規則會以星號 (*) 標示。在 [基礎指南](#) 中閱讀更多關於原則規則類型的資訊。

若要編輯原則規則中的權限

1. 以系統管理員身分登入 Cyber Protect 服務主控台。
2. 導覽至 **[保護]** > **[資料流程原則]**。
3. 選擇您想要編輯的原則規則，然後按一下規則清單上方的 **[編輯]**。
[編輯資料流程規則] 視窗隨即開啟。
4. 在 **[權限]** 區段中，選擇 **[允許]**、**[例外]** 或 **[拒絕]**。
5. (選擇性) 若要將此規則的 **[允許]** 或 **[例外]** 權限優先順序設定為高於其他規則中的權限，請選擇 **[優先]** 核取方塊。
您不需要使用此核取方塊，將資料流程規則的優先順序設定為高於預設的 **[任何]** > **[其他規則]**，因為其在原則中的優先順序預設為最低。
如需結合規則時權限優先順序的相關資訊，請參閱 "結合資料流程原則規則" (第 434 頁)。

6. (選擇性) 選擇要在觸發規則時執行的動作。
7. 將變更儲存至原則規則。

結合資料流程原則規則

重要事項

這是優先體驗版本的進階版資料洩漏防禦文件。部分功能和描述可能不完整。

當資料傳輸符合多個規則時，會結合並套用針對所有規則設定的權限和動作，如下所示。

權限

如果資料傳輸符合多個規則，而且這些規則對於相同資料類別的權限不同，則根據下列權限優先順序清單 (以遞減順序排序)，覆寫規則是優先順序較高的權限：

1. 具有 **[優先]** 旗標的例外
2. 具有 **[優先]** 旗標的允許
3. 拒絕
4. 例外
5. 允許

如果資料傳輸符合多個規則，而且這些規則對於不同資料類別的權限不同，則會套用下列邏輯以進行覆寫：

1. 系統會針對資料傳輸符合的每個敏感度類別，定義最嚴格的規則權限。
2. 系統會強制執行在第 1 點定義的最嚴格規則權限。

範例

檔案傳輸符合不同敏感度類別中的三個規則，如下所示：

敏感度類別	權限
PII	允許 - 優先
PHI	例外 - 優先
PCI	拒絕

將套用的權限為 **[拒絕]**。

動作

如果資料傳輸符合多個規則，而且這些規則已在 **[動作]** 欄位中設定不同的選項，則會執行所有觸發的規則中所有已設定的動作。

原則檢閱與管理

重要事項

這是優先體驗版本的進階版資料洩漏防禦文件。部分功能和描述可能不完整。

在執行自動建立的基準資料流程原則之前，該原則必須經過客戶的檢閱、驗證和核准，因為客戶本身才知道其業務流程的所有特點，而且可以評估這些流程在基準原則中，是否以一致的方式解譯。此外，客戶可以識別不準確之處，然後由合作夥伴系統管理員修正。

在原則檢閱期間，合作夥伴系統管理員會將基準資料流程原則呈現給客戶，讓客戶檢閱原則中的每個資料流程，並驗證與其業務流程的一致性。驗證不需要任何技術上的技能，因為保護服務主控台中顯示的原則規則非常直覺式：每個規則都會描述敏感資料流程的寄件者和收件者是誰。

根據客戶的指示，合作夥伴系統管理員會透過編輯、刪除和建立資料流程原則規則，手動調整基準原則。客戶核准後，就會將已套用到這些工作負載的保護計劃切換到【執行】模式，以便對受保護的工作負載執行經過檢閱的原則。

執行經過檢閱的原則之前，請務必在所有針對敏感資料類別自動建立的預設原則規則中，將【允許】權限變更為【拒絕】或【例外】。使用者無法覆寫【拒絕】權限，而【例外】權限則會封鎖符合規則的所有傳輸，但允許使用者在緊急情況下，透過提交業務相關例外來覆寫封鎖。

資料流程原則更新

重要事項

這是優先體驗版本的進階版資料洩漏防禦文件。部分功能和描述可能不完整。

當公司或其單位的業務流程發生重大變更時，必須更新其 DLP 原則，使其與所更新業務流程敏感資料流程中的變更保持一致。如果員工的工作角色變更，也需要更新原則。在此案例中，也必須更新用於保護員工工作負載的單位原則部分。

進階版 DLP 原則管理工作流程可讓系統管理員針對整個公司、單位、使用者或單位中的部分使用者，自動更新原則。

更新公司或單位的原則

【觀察】模式的所有選項都可以用來更新整個公司或整個單位的原則，以及單位中一或多個使用者的部分單位原則。

若要更新公司或單位的原則

更新程序包含下列步驟，公司系統管理員或管理公司工作負載的合作夥伴都必須完成這些步驟。

1. 刪除強制執行原則中的所有非預設規則。
2. 若要開始更新，請根據最適合此特定公司或單位的選項，將已將進階版 DLP 套用到公司或單位的保護計劃切換到其中一個觀察模式選項，然後將該計劃套用到該公司或單位中的所有工作流程。
3. 當更新期間結束後，與客戶一起檢閱新的公司或單位原則、必要時進行調整，然後獲得客戶核准。
4. 將已套用到公司或單位工作負載的保護計劃切換到適當的執行模式選項，客戶會將此選項視為最適合防止資料從單位的工作負載洩漏。

更新公司或單位中一或多個使用者的原則

您可以使用【觀察】模式的任何選項以及調適型執行模式，更新使用者層級的原則。

使用觀察模式來更新使用者原則

使用觀察模式來更新公司 (或單位) 中某個使用者或部分使用者的原則具備下列特點: 在更新期間, 不會透過使用者的資料傳輸, 執行對整個公司 (或單位) 執行的資料流程原則。因此, 可以在更新期間為使用者建立個別的規則, 這些規則可能會公司 (或單位) 執行政策中的現有群組規則互相矛盾或相符。完成更新並透過使用者的資料傳輸重新執行原則之後, 這些為使用者建立的新個別規則實際上是否會套用至使用者的資料傳輸, 取決於其與這些資料傳輸相符之原則中其他規則相比的優先順序。

若要透過觀察模式更新使用者的原則

更新程序包含下列步驟, 公司系統管理員或管理公司工作負載的合作夥伴都必須完成這些步驟。

1. 在針對將使用者當作其單一寄件者的公司 (或單位) 執行的原則中, 刪除所有非預設規則。
2. 從已執行的原則中所有非預設資料流程規則的寄件者清單移除使用者。
3. 在觀察模式下, 使用進階版 DLP 建立新的保護計劃, 並將其套用至使用者的工作負載, 以開始更新 (觀察) 期間。
更新期間的持續時間取決於使用者完成全部或 90-95% 從工作負載傳輸敏感資料相關定期業務活動可能需要的時間。
4. 當更新期間結束後, 檢閱與已新增至強制原則的這個使用者相關的新規則、必要時進行調整, 然後獲得客戶核准。
5. 將已套用到使用者工作負載的保護計劃切換到 **[嚴格執行]** 模式或 **[調適型執行]** 模式, 端視客戶將哪個選項視為最適合防止資料從使用者的工作負載洩漏而定。
或者, 您可以將已套用到公司 (或單位) 的保護計劃重新套用到使用者的工作負載。

使用調適型執行模式來更新使用者原則

在進階版 DLP 已套用至使用者工作負載的情況下, 使用保護計劃的 **[調適型執行]** 模式可以對公司 (或單位) 中的單一使用者或部分使用者執行原則更新。

注意事項

此原則更新方法具備下列特點: 對於具有使用者成員資格 (亦即, 任何內部) 的寄件者群組, 已執行的公司 (單位) 原則在更新期間, 也會透過從此使用者進行資料傳輸來執行。因此, 更新將不會為使用者建立與這些寄件者群組現有原則互相矛盾或相符的新個別規則。在這兩個方法中, 哪個方法對於特定客戶的使用者原則更新更有效率, 取決於其具體的 IT 安全性需求

若要透過調適型執行模式更新使用者的原則

更新程序包含下列步驟, 公司系統管理員或管理公司工作負載的合作夥伴都必須完成這些步驟。

1. 在針對將使用者當作其單一寄件者的公司 (單位) 執行的原則中, 刪除所有非預設規則。
2. 從已執行的原則中所有非預設資料流程規則的寄件者清單移除使用者。
3. 針對為公司 (或單位) 執行的原則中的所有預設規則, 將其權限設定為 **[例外]**, 然後在 **[動作]** 欄位中, 選擇 **[在記錄中寫入]** 動作。
4. 如果目前已套用到使用者工作負載的保護計劃設定為 **[嚴格執行]** 模式, 請使用進階版 DLP 建立新的保護計劃, 並在 **[調適型執行]** 模式下, 將其套用到使用者的工作負載, 以開始更新期間。

更新期間的持續時間取決於使用者完成全部或 90-95% 從工作負載傳輸敏感資料相關定期業務活動可能需要的時間。

5. 當更新期間結束後，檢閱與已新增至強制原則的這個使用者相關的新規則、必要時進行調整，然後獲得客戶核准。
6. 將已套用到使用者工作負載的保護計劃切換到 **【嚴格執行】** 模式或留在 **【調適型執行】** 模式，端視客戶將哪個選項視為最適合防止資料從使用者的工作負載洩漏而定。
或者，您可以將已套用到公司 (或單位) 的保護計劃重新套用到使用者的工作負載。

16.1.2 在保護計劃中啟用進階版資料洩漏防禦

重要事項

這是優先體驗版本的進階版資料洩漏防禦文件。部分功能和描述可能不完整。

如果為此客戶啟用保護服務和進階版資料洩漏防禦套件，則可以將進階版資料洩漏防禦功能包含在客戶租用戶的任何保護計劃中。

進階版 DLP 是資料洩漏防禦功能群組的進階模組。進階版 DLP 功能和裝置控制可以單獨使用或一起使用，在該情況下，其功能會加以協調，如下所示。

- 裝置控制會停止控制使用者存取進階版 DLP 檢查已傳輸資料內容所在的這些本機通道。
- 裝置控制會執行使用者對允許名單中下列邏輯通道和週邊裝置的存取：
 - 光碟機
 - 軟碟機
 - 連線 MTP 的行動裝置
 - 藍牙介面卡
 - Windows 剪貼簿
 - 螢幕擷取畫面擷取
 - USB 裝置和裝置類型

若要使用進階版 DLP 建立保護計劃

1. 導覽至 **【管理】** > **【保護計劃】**。
2. 按一下 **【建立計劃】**。
3. 展開 **【資料洩漏防禦】** 區段，然後按一下 **【模式】** 列。
【模式】 對話方塊隨即開啟。

- 若要開始建立或更新資料流程原則，請選擇 **[觀察模式]**，然後選擇處理資料傳輸的方式：

選項	描述
全部允許	從使用者工作負載進行的所有敏感資料傳輸都會被視為業務流程所需，而且安全無虞。系統會針對不符合原則中已定義規則的每個偵測到的資料流程，建立一個新規則。
全部證明	從使用者工作負載進行的所有敏感資料傳輸都會被視為業務流程所需，但是有風險。因此，每次將敏感資料傳輸至不符合先前所建立資料流程的任何收件者或目的地（組織內部和外部）遭到攔截時，使用者都必須提供一次性的業務理由。提交理由後，就會在資料流程原則中建立一個新的資料流程規則。
混合	系統會針對所有內部敏感資料傳輸套用 [允許所有邏輯]，並針對所有外部敏感資料傳輸套用 [證明所有邏輯]。 如需內部目的地的定義，請參閱 "自動偵測目的地" (第 440 頁)

警告！

- 只有在您之前未建立資料流程原則或您要更新原則時，才選擇 **[觀察模式]**。在您開始更新原則之前，請參閱 "資料流程原則更新" (第 435 頁)。
 - 在觀察模式下無法防止資料洩漏。請參閱 [《基礎指南》中的觀察模式](#)。
- 若要執行現有的資料流程原則，請選擇 **[執行模式]**，然後選擇執行資料流程原則規則的嚴格程度：

選項	描述
嚴格執行	資料流程原則以原樣執行，而且在偵測到之前未觀察到的敏感資料流程時，不會使用新的權限原則規則進行擴展。請參閱 《基礎指南》中的嚴格執行 。
調適型執行 (透過學習來執行)	已執行的原則會繼續自動適應在觀察期間未執行的業務作業或業務流程的變化。此模式可讓已執行的資料流程原則根據在工作負載上偵測到新學到的資料流程，進行擴充。請參閱 《基礎指南》中的調適型執行 。

重要事項

將公司或單位原則從 [觀察] 模式切換到 [執行] 模式之前，將每個敏感資料類別的預設規則從許可狀態調整為禁止狀態。在 **[資料流程原則]** 檢視中，預設規則會以星號 (*) 標示。在 [基礎指南](#) 中閱讀更多關於原則規則類型的資訊。

- 按一下 **[完成]**，關閉 [模式] 對話方塊。
- (選擇性) 若要設定光學字元辨識、允許名單以及其他保護選項，按一下 **[進階設定]**。
如需可用選項的相關資訊，請參閱 "進階設定" (第 439 頁)。
- 儲存保護計劃並將其套用至您要保護的工作負載。

進階設定

重要事項

這是優先體驗版本的進階版資料洩漏防禦文件。部分功能和描述可能不完整。

您可以使用保護計劃中的進階設定搭配進階版資料洩漏防禦，以提高進階版資料洩漏防禦所控制之通道中資料內容檢查的品質，並從任何預防性控制中，排除對允許名單中的週邊裝置類型、網路通訊類別、目的地主機起始的資料傳輸，以及由允許名單中應用程式起始的資料傳輸。您可以設定下列進階設定：

- **光學字元辨識**

此設定可開啟或關閉光學字元辨識 (OCR)，以便從文件、訊息、掃描、螢幕擷取畫面與其他物件中的圖形檔案和影像擷取 31 種語言的片段文字，以進行進一步的內容檢查。

- **傳輸受密碼保護的資料**

無法檢查受密碼保護之存檔和文件的內容。透過此設定，進階版 DLP 可讓系統管理員選擇允許還是封鎖受密碼保護資料的傳出傳輸。

- **防止發生錯誤時傳輸資料**

有時候正在傳送的內容分析可能會失敗，或者在 DLP 代理程式操作時可能會發生其他控制錯誤。若啟用此選項，將會封鎖傳輸。若停用此選項，即使發生錯誤，也會允許傳輸。

- **裝置類型和網路通訊的允許名單**

無論資料的敏感度和強制執行的資料流程原則為何，都允許將資料傳輸到此清單中勾選的週邊裝置類型和網路內通訊類型。

警告！

如果發生特定裝置類型或通訊協定問題，會使用此選項。除非支援代表建議，否則請不要啟用該選項。

- **遠端主機的允許名單**

無論資料的敏感度和強制執行的資料流程原則為何，都允許將資料傳輸到此清單中指定的目的地主機。

- **應用程式的允許名單**

無論資料的敏感度和強制執行的資料流程原則為何，都允許此清單中指定的應用程式執行資料傳輸。

在 **[建立保護計劃]** 檢視以及保護計劃 **[詳細資料]** 檢視中顯示之 **[進階]** 設定的 **[安全性層級]** 指標具備下列層級跡象的邏輯：

- **[基本]** 表示未開啟或已開啟其中一個進階設定。
- **[中度]** 表示已開啟多個設定，但未啟用 **[OCR]**、**[傳輸受密碼保護的資料]** 和 **[防止發生錯誤時傳輸資料]** 的組合。
- **[嚴格]** 表示至少已啟用 **[OCR]**、**[傳輸受密碼保護的資料]** 和 **[防止發生錯誤時傳輸資料]** 的組合。

16.1.3 自動偵測目的地

重要事項

這是優先體驗版本的進階版資料洩漏防禦文件。部分功能和描述可能不完整。

在 [混合觀察] 模式下，進階版資料洩漏防禦會根據偵測到的資料傳輸目的地 (內部或外部) 而套用不同的規則。判斷目的地為內部的邏輯如下所述。其他所有目的地都被視為外部。

針對每個攔截的資料傳輸，進階版資料洩漏防禦會透過執行 DNS 要求，並比較執行資料洩漏防禦代理程式所在電腦和遠端伺服器的 FQDN 名稱，以自動偵測目的地 HTTP、FTP 或 SMB 伺服器是否為內部。如果 DNS 要求失敗，其也會檢查受保護的工作負載和遠端伺服器是否在相同的網路中。網域名稱與執行資料洩漏防禦代理程式所在電腦相同 (或位於相同子網路) 的伺服器會被視為內部。

對於電子郵件通訊，如果收件者電子郵件與寄件者電子郵件位於相同的網域，且收件者郵件伺服器名稱相同，則進階版資料洩漏防禦會將使用公司郵件伺服器，從公司電子郵件地址傳送的所有電子郵件視為內部傳輸。

除非已知收件者帳戶，否則透過即時訊息進行的通訊會被視為外部通訊。當資料洩漏防禦監視網路上的使用者活動，並在後端將資料庫更新為與使用者相關聯之帳戶的資料時，會更新已知帳戶。

16.1.4 敏感資料定義

重要事項

這是優先體驗版本的進階版資料洩漏防禦文件。部分功能和描述可能不完整。

本主題描述在內容分析期間用於識別敏感資料的邏輯。

若要減少誤報的數目，針對所描述邏輯運算式的所有群組，相同的符合項目會計為一個符合項目。

重要事項

用於內容識別的邏輯運算式僅供參考，不會詳細描述解決方案。

受保護的健康資訊 (PHI)

支援語言

- 美國、英國、英文 (國際)
- Finnish
- Italian
- French
- Polish
- Russian
- Hungarian

- Norwegian
- Spanish

被視為受保護的健康資訊的資料

下列資料被視為受保護的健康資訊。

- 名字和姓氏
- 地址 (街道、縣/市、區域、郵遞區號及其對等的地理代碼)
- 電話號碼
- 電子郵件地址
- 社會安全號碼
- 健康計劃受益人編號
- 銀行帳號
- URL
- IP 位址編號
- ICD-10-CM 代碼
- ICD-10-PCS-and-GEMs
- HIPAA
- 其他健康醫療相關
- 信用卡號碼

用於內容偵測的邏輯運算式

邏輯運算式包含以邏輯運算子 OR 加入的下列字串。如果未明確指定 AND 運算子, 則 OR 運算子用於加入上方清單中的不同資料群組。括號中的數字表示偵測到且將傳回正面偵測結果的執行個體數目。

- 社會安全號碼 (5)
- (名字和姓氏 (3) OR 地址 (3) OR 電話號碼 (3) OR 電子郵件地址 (3)) AND (社會安全號碼 (3) OR 健康計劃受益人編號 (3) OR 銀行帳號 (3) OR 信用卡號碼 (3) OR ICD-10-CM 代碼 (3) OR ICD-10-PCS-and-GEMs (3) OR HIPAA (3) OR 其他健康醫療相關 (3))
- (名字和姓氏 (30) OR 地址 (30) OR 電話號碼 (30) OR 電子郵件地址 (30)) AND (URL (30) OR IP 位址號碼 (30))
- 名字和姓氏 (30) AND 地址 (30) AND 電話號碼 (30) AND 電子郵件地址 (30)
- 健康計劃受益人編號 (5) AND (信用卡號碼 (5) OR 銀行帳號 (5))
- 其他健康醫療相關 (5) AND (信用卡號碼 (5) OR 銀行帳號 (5))

個人識別資訊 (PII)

支援語言

- 美國、英國、英文 (國際)
- Bulgarian

- 繁體中文
- 捷克文
- Danish
- Dutch
- Finnish
- French
- German
- Hungarian
- Indonesian
- Italian
- Korean
- Malay
- Norwegian
- Polish
- 葡萄牙文 (巴西)
- 葡萄牙文 (葡萄牙)
- Russian
- Serbian
- Spanish
- Swedish
- Turkish
- Japanese

被視為個人識別資訊 (PII) 的資料

- 名字和姓氏
- 地址 (街道、縣/市、郵遞區號)
- 銀行帳號
- 個人身分證號碼和財政 ID 號碼
- 護照號碼
- 社會安全號碼
- 電話號碼
- 車牌號碼
- 駕駛執照號碼
- 識別碼和序號
- IP 位址
- 電子郵件地址
- 信用卡號碼

用於內容偵測的邏輯運算式

用於日文之外所有支援的語言的邏輯運算式

邏輯運算式包含以邏輯運算子 OR 或 AND 加入的下列字串。括號中的數字表示偵測到且將傳回正面偵測結果的執行個體數目。

- 信用卡號碼 (5) OR 社會安全號碼 (5) OR 個人身分證號碼和財政 ID 號碼 (5)
- 名字和姓氏 (3) AND (信用卡號碼 (3) OR 社會安全號碼 (3) OR 銀行帳號 (3) OR 個人身分證號碼和財政 ID 號碼 (3) OR 駕駛執照號碼 (3) OR 護照號碼 (3) OR 社會安全號碼 (3) OR IP 位址 (3) OR 車牌號碼 (3) OR 識別碼和序號)
- 電話號碼 (3) AND (信用卡號碼 (3) OR 社會安全號碼 (3) OR 銀行帳號 (3) OR 地址 (3) OR 個人身分證號碼和財政 ID 號碼 (3) OR 駕駛執照號碼 (3) OR 護照號碼 (3) OR 社會安全號碼 (3) OR 車牌號碼 (3) OR 識別碼和序號 (3))
- 名字和姓氏 (30) AND (電子郵件地址 (30) OR 電話號碼 (30) OR IP 位址 (30) OR 地址 (30))
- 電子郵件地址 (3) AND (信用卡號碼 (3) OR 社會安全號碼 (3) OR 銀行帳號 (3) OR 個人身分證號碼和財政 ID 號碼 (3) OR 駕駛執照號碼 (3) OR 護照號碼 (3) OR 社會安全號碼 (3) OR 車牌號碼 (3) OR 識別碼和序號 (3))
- 電子郵件地址 (30) AND (地址 (30) OR 電話號碼 (30))
- 名字和姓氏 (30) AND 地址 (30)
- 電話號碼 (30) AND 地址 (30)
- 名字和姓氏 (3) AND 銀行帳號 (3)
- 電話號碼 (3) AND (信用卡號碼 (3) OR 銀行帳號 (3) OR 社會安全號碼 (3) OR 個人身分證號碼和財政 ID 號碼 (3) OR 駕駛執照號碼 (3) OR 護照號碼 (3))

用於日文的邏輯運算式

注意事項

內容偵測只會計算獨特的相符項目。

邏輯運算式包含以邏輯運算子 OR 加入的下列字串。如果未明確指定邏輯運算子 AND, 則運算子 OR 用於加入不同的群組。

- 信用卡號碼 (5) OR 社會安全號碼 (5)
- 名字和姓氏 (3) AND (信用卡號碼 (3) OR 銀行帳號 (3) OR 駕駛執照號碼 (3) OR 護照號碼 (3) OR 社會安全號碼 (3))
- 名字和姓氏 (30) AND (電子郵件地址 (30) OR 電話號碼 (30) OR IP 位址 (30) OR 地址 (30))
- 地址 (3) AND (信用卡號碼 (3) OR 銀行帳號 (3) OR 駕駛執照號碼 (3) OR 護照號碼 (3) OR 社會安全號碼 (3))
- 電子郵件地址 (3) AND (信用卡號碼 (3) OR 銀行帳號 (3) OR 社會安全號碼 (3) OR 駕駛執照號碼 (3))
- 地址 (5) AND (電子郵件地址 (5) OR 名字和姓氏 (5) OR 電話號碼 (5) OR IP 位址 (5))
- 名字和姓氏 (3) AND 銀行帳號 (3)

- 電話號碼 (3) AND (信用卡號碼 (3) OR 銀行帳號 (3) OR 地址 (3) OR 社會安全號碼 (3) OR 駕駛執照號碼 (3))

支付卡產業資料安全標準 (PCI DSS)

支援語言

此敏感度群組與語言無關。所有國家/地區的 PCI DSS 資料都採用英文。

被視為 PCI DSS 的資料

- 持卡人資料
 - 主要帳號 (PAN)
 - 持卡人姓名
 - 到期日
 - 服務代碼
- 敏感驗證資料
 - 完整追蹤資料 (磁條資料或晶片上的同等資料)
 - CAV2/CVC2/CVV2/CID
 - PIN/PIN 區塊

用於內容偵測的邏輯運算式

邏輯運算式包含以邏輯運算子 OR 加入的下列字串。括號中的數字表示偵測到且將傳回正面偵測結果的執行個體數目。

- 信用卡號碼 (3)
- 信用卡號碼 (3) AND (美國名字 (Ex) (3) OR 美國名字 (3) OR PCI DSS 關鍵字 (3) OR 日期 (月/年) (3))
- 信用卡傾印 (3)

已標示為機密

標示為機密的資料是透過關鍵字群組偵測的。

Match 條件是以權重為基礎, 每個字的權重 == 1。當 Match if 權重 > 3 時, 內容偵測會被視為正面的。

支援語言

- English
- Bulgarian
- 簡體中文
- 繁體中文
- 捷克文
- Danish
- Dutch

- Finnish
- French
- German
- Hungarian
- Indonesian
- Italian
- Japanese
- Korean
- Malay
- Norwegian
- Polish
- 葡萄牙文 - 巴西
- 葡萄牙文 - 葡萄牙
- Russian
- Serbian
- Spanish
- Swedish
- Turkish

關鍵字群組

每個語言的關鍵字群組都包含以下用於英語的國家/地區專用的相等關鍵字 (不區分大小寫)。

- confidential
- internal distribution
- not for distribution
- do not distribute
- not for public
- not for external distribution
- for internal use only
- highly qualified documentation
- private
- privileged information
- for internal use only
- for official use only

16.1.5 資料洩漏防禦事件

重要事項

這是優先體驗版本的進階版資料洩漏防禦文件。部分功能和描述可能不完整。

進階版資料洩漏防禦會在事件檢視器中產生事件，如下所示。

- 在觀察模式期間，系統會針對所有已證明的資料傳輸產生事件。
- 在執行模式期間，系統會根據針對所觸發的每個原則規則設定的 **[在記錄中寫入]** 動作產生事件。

若要檢視資料流程原則中規則的事件

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 導覽至 **[保護]** > **[資料流程原則]**。
3. 找出您要檢視其事件的規則，然後按一下規則行結尾的省略符號。
4. 選擇 **[檢視事件]**。

若要在 DLP 事件清單中檢視某個事件的詳細資料

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 導覽至 **[保護]** > **[DLP 事件]**。
3. 按一下清單中的某個事件，以檢視其詳細資料。
[事件詳細資料] 窗格隨即在右側展開。
4. 在 [事件詳細資料] 窗格中上下捲動可檢視可用的資訊。
顯示在窗格中的詳細資料取決於觸發事件的規則類型以及規則設定。

若要在 DLP 事件清單中篩選事件

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 導覽至 **[保護]** > **[DLP 事件]**。
3. 按一下右上方的 **[篩選]**。
4. 從下拉式功能表中選擇敏感度類別、工作負載、動作類型、使用者以及通道。
您可以在下拉式功能表中選擇多個項目。篩選會在相同的功能表中的項目之間套用邏輯運算子 OR，但是在不同功能表中的項目之間使用邏輯運算子 AND。
例如，如果您選擇 **PHI** 和 **PII** 敏感度類別，結果將傳回包含 PHI 或 PII 或兩者的所有事件。如果您選擇 **PHI** 敏感度類別以及 **[寫入存取]** 動作，則只有符合兩個類別的事件才會出現在篩選的結果中。
5. 按一下 **[套用]**。
6. 若要再次檢視所有事件，依序按一下 **[篩選]** 和 **[重設為預設值]**，最後再按一下 **[套用]**。

若要在 DLP 事件清單中搜尋事件

1. 重複以上程序中的步驟 1-2。
2. 從 [篩選] 右側的下拉式清單中，選擇您要搜尋的類別：**[寄件者]**、**[目的地]**、**[程序]**、**[訊息主旨]** 或 **[原因]**。
3. 在文字方塊中，輸入您感興趣的字詞，然後按下鍵盤上的 Enter 鍵來確認。
只有符合您所輸入之字詞的事件才會出現在清單中。
4. 若要重設事件清單，按一下 [搜尋] 文字方塊中的 **X** 符號，然後按下 Enter 鍵。

若要檢視資料流程原則中與特定規則相關事件的清單

1. 以系統管理員身分登入 Cyber Protect 主控台。
2. 導覽至 **[保護]** > **[資料流程原則]**。
3. 選擇您感興趣的原則規則名稱前方的核取方塊。
如果需要, 您可以選擇多個原則規則。
4. 按一下 **[檢視事件]**。
此檢視畫面會切換到 **[保護]** > **[DLP 事件]**, 與您所選原則規則相關的事件就會出現在清單中。

16.1.6 概觀儀表板上的進階版資料洩漏防禦桌面小工具

重要事項

這是優先體驗版本的進階版資料洩漏防禦文件。部分功能和描述可能不完整。

[概觀] 儀表板提供許多可自訂的桌面小工具, 可概覽與 Cyber Protection 服務相關的作業, 包括進階版資料洩漏防禦。您可以在 **[概觀]** 儀表板上的 **[監控]** 底下, 找到下列進階版資料洩漏防禦桌面小工具。

- **敏感資料傳輸** - 顯示傳送給內部和外部收件者的敏感資料傳輸作業總數。此圖表按權限類型劃分: 已允許、已證明或已封鎖。您可以選擇所需的時間範圍 (1 天、7 天、30 天或當月) 來自訂此桌面小工具。
- **輸出敏感資料類別** - 顯示傳送給外部收件者的敏感資料傳輸總數。此圖表按權限類型劃分: 已允許、已證明或已封鎖。您可以選擇所需的時間範圍 (1 天、7 天、30 天或當月) 來自訂此桌面小工具。
- **輸出敏感資料的常見寄件者** - 顯示從組織傳給外部收件者的敏感資料傳輸總數和傳輸數量最大的前五個使用者的清單 (以及這些傳輸的數量)。此統計資料包括允許的和證明的傳輸。您可以選擇所需的時間範圍 (1 天、7 天、30 天或當月) 來自訂此桌面小工具。
- **敏感資料傳輸遭封鎖的常見寄件者** - 顯示封鎖的敏感資料傳輸總數和嘗試傳輸次數最多的前五個使用者的清單 (以及這些傳輸的數量)。您可以選擇所需的時間範圍 (1 天、7 天、30 天或當月) 來自訂此桌面小工具。
- **最近的 DLP 事件** - 針對所選時間範圍顯示最近資料洩漏防禦事件的詳細資料。您可以使用下列選項自訂此桌面小工具:
 - **範圍 (張貼日期)** (1 天、7 天、30 天或當月)。
 - **工作負載** 的名稱
 - **作業狀態** (已允許、已證明或已封鎖)
 - **敏感度** (PHI、PII、機密、PCI DSS)
 - **目的地類型** (外部、內部)
 - **分組** (工作負載、使用者、通道、目的地類型)

系統會每五分鐘更新一次桌面小工具。動態小工具帶有可按一下的元素, 可讓您調查問題並進行疑難排解。您可以透過 .pdf 和/或 .xlsx 格式下載最新狀態的儀表板或透過電子郵件進行傳送。

17 協同作業和通訊應用程式的保護

Zoom、Cisco Webex Meetings、Citrix Workspace 和 Microsoft Teams 現在廣泛用於視訊/網路會議和通訊。Cyber Protection 服務可讓您保護協同作業工具。

Zoom、Cisco Webex Meetings、Citrix Workspace 和 Microsoft Teams 的保護設定都類似。在以下的範例中，我們將考慮 Zoom 的設定。

設定 Zoom 保護

1. 在安裝協同作業應用程式所在的電腦上 [安裝保護代理程式](#)。
2. 登入服務主控台，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

18 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。在 [弱點評估] 模組中，您可以掃描電腦中的弱點，並檢查作業系統和已安裝的應用程式皆處於最新狀態且運作正常。

具有下列作業系統的電腦支援弱點評估掃描：

- Windows。如需詳細資訊，請參閱 "支援的 Microsoft 和第三方產品" (第 449 頁)。
- macOS。如需詳細資訊，請參閱 "支援的 Apple 和協力廠商產品" (第 451 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 451 頁)。

使用 **修補程式管理 (PM)** 功能，為電腦上所安裝的應用程式和作業系統，管理修補程式 (更新)，並將您的系統維持在最新狀態。在 [修補程式管理] 模組中，您可以自動或手動核准電腦上的更新安裝。

具有 Windows 作業系統的電腦支援修補程式管理。如需詳細資訊，請參閱 "支援的 Microsoft 和第三方產品" (第 449 頁)。

18.1 弱點評估

弱點評估程序包含下列步驟：

1. 您在已啟用 [弱點評估] 模組的情況下，[建立保護計劃](#)、指定 [弱點評估設定](#)，然後將計劃指派給電腦。
2. 系統會依排程或視需要，將執行弱點評估掃描的命令傳送到電腦上安裝的保護代理程式。
3. 代理程式會取得命令、開始掃描電腦中的弱點，然後產生掃描活動。
4. 弱點評估掃描完成之後，代理程式會產生結果，並將其傳送到監控服務。
5. 監控服務會處理來自代理程式的資料，並將結果顯示在 [弱點評估桌面小工具](#) 和已找到弱點的清單中。
6. 當您取得 [已找到弱點的清單](#) 時，可以處理該清單並決定必須修正哪些找到的弱點。

您可以在 [監控] > [概觀] > [\[弱點/現有的弱點\]](#) 桌面小工具中，監視弱點評估掃描的結果。

18.1.1 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

Windows OS

- Windows 7 (企業版、專業版、旗艦版)
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Windows Server OS

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Microsoft Office 和相關元件

- Microsoft Office 2019 (x64, x86)
- Microsoft Office 2016 (x64, x86)
- Microsoft Office 2013 (x64, x86)
- Microsoft Office 2010 (x64, x86)

Windows OS 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 Exchange Server 2016
- Microsoft Exchange Server 2019
- Microsoft Sharepoint Server 2016
- Microsoft Sharepoint Server 2016

Windows OS 支援的第三方產品

遠端工作在全球變得越來越廣泛, 因此, 協同作業和通訊工具、VPN 用戶端現在對於永遠維持最新狀態並檢查可能的漏洞非常重要。Cyber Protection 服務支援這類應用程式的弱點評估和修補程式管理。

協同作業和通訊工具、VPN 用戶端

- Microsoft Teams
- Zoom
- Skype
- Slack
- Webex
- NordVPN
- TeamViewer

如需有關 Windows OS 支援的第三方產品的詳細資訊，請參閱[修補程式管理支援的第三方產品清單 \(62853\)](#)。

18.1.2 支援的 Apple 和協力廠商產品

下列 Apple 產品和適用於 macOS 的協力廠商產品支援弱點評估：

支援的 Apple 產品

macOS

- macOS 10.14.x 及更新版本

macOS 內建應用程式

- Safari、iTunes 等等。

支援的適用於 macOS 的協力廠商產品

- Microsoft Office (Word、Excel、PowerPoint、Outlook、OneNote)
- Adobe Acrobat Reader
- Google Chrome
- Firefox
- Opera
- Zoom
- Skype
- Thunderbird
- VLC 媒體播放程式

18.1.3 支援的 Linux 產品

支援適用於 VA 的下列 Linux 發行版和版本：

- 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

18.1.4 弱點評估設定

若要瞭解如何使用 [弱點評估] 模組建立保護計劃, 請參閱「[建立保護計劃](#)」。您可以依排程或視需要執行 VA 掃描 (透過使用保護計劃中的 **[立即執行]** 動作)。

您可以在 [弱點評估] 模組中指定下列設定。

掃描內容

定義您要掃描弱點的軟體產品：

- Windows 電腦：
 - **Microsoft 產品**
 - **Windows 第三方產品** (如需有關 Windows OS 支援的第三方產品的詳細資訊, 請參閱[修補程式管理支援的第三方產品清單 \(62853\)](#))
- macOS 電腦：
 - **Apple 產品**
 - **macOS 協力廠商產品**
- Linux 電腦：
 - 掃描 **Linux 套件**

排程

根據將在所選電腦上執行的弱點評估掃描, 定義排程：

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。

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](#)」中。您可以定義下列額外的開始條件：

- **在時間視窗中分配工作開始時間** – 此選項可讓您設定工作的時間範圍，以避免網路瓶頸。您可以以小時或分鐘，指定延遲時間。例如，如果預設開始時間為上午 10:00，且延遲為 60 分鐘，則工作將會在上午 10:00 到上午 11:00 之間開始。
- **如果電腦關閉，則在電腦啟動時執行遺漏的工作**
- **防止在工作執行期間進入睡眠或休眠模式** – 此選項僅適用於執行 Windows 的電腦。
- **如果未符合開始條件，請無論如何在此時間後執行工作** – 指定無論開始條件為何，將會在其後執行工作的時段。

注意事項

Linux 不支援開始條件。

18.1.5 適用於 Windows 電腦的弱點評估

您可以掃描 Windows 電腦和適用於 Windows 的協力廠商產品的弱點。

若要設定適用於 **Windows** 電腦的弱點評估

1. 在服務主控台中，[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 452 頁)。
3. [將計劃指派給 Windows 電腦](#)。

弱點評估掃描之後，您可以查看 [已找到弱點的清單](#)。您可以處理這項資訊並決定必須修正哪些找到的弱點。

若要監視弱點評估的結果，請查看 **[監視]** > **[概觀]** > **[弱點/現有的弱點]** 桌面小工具。

18.1.6 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. 在服務主控台中, [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 452 頁)。

3. [將計劃指派給 Linux 電腦](#)。

弱點評估掃描之後, 您可以查看 [已找到弱點的清單](#)。您可以處理這項資訊並決定必須修正哪些找到的弱點。

若要監視弱點評估的結果, 請查看 **【監視】** > **【概觀】** > **【弱點/現有的弱點】** 桌面小工具。

18.1.7 適用於 macOS 裝置的弱點評估

您可以掃描 macOS 裝置中的作業系統層級和應用程式層級弱點。

若要設定適用於 macOS 裝置的弱點評估

1. 在服務主控台中, [建立保護計劃](#), 然後啟用 **【弱點評估】** 模組。

2. 指定弱點評估設定:

- **掃描內容** – 選擇 **【Apple 產品】**、**【macOS 協力廠商產品】**, 或兩者。
- **排程** – 定義執行弱點評估的排程。

如需有關 **【排程】** 選項的詳細資訊, 請參閱 "弱點評估設定" (第 452 頁)。

3. [將計劃指派給 macOS 裝置](#)。

弱點評估掃描之後, 您可以查看 [已找到弱點的清單](#)。您可以處理這項資訊並決定必須修正哪些找到的弱點。

若要監視弱點評估的結果, 請查看 **【監視】** > **【概觀】** > **【弱點/現有的弱點】** 桌面小工具。

18.1.8 管理找到的弱點

如果至少執行過弱點評估一次, 且找到一些弱點, 您可以在 **【軟體管理】** > **【弱點】** 中看到這些弱點。

弱點清單會同時顯示具有要安裝之修補程式的弱點, 以及沒有建議之修補程式的弱點。您可以使用篩選功能, 僅顯示具有修補程式的弱點。

名稱	描述
名稱	弱點的名稱。
受影響的產品	找到其中有弱點的軟體產品。
電腦	受影響電腦的數量。
嚴重性	找到之弱點的嚴重性。根據通用弱點評分系統 (CVSS), 可以指派下列層級: • 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。

Acronis Cyber Cloud		Vulnerabilities			
Manage account		Filter	Search	Loaded: 30 / Total: 82	
☐	Name ↓	Affected products ↓	Machines ↓	Severity ↓	Patches ↓
	CVE-2015-16723	Microsoft Windows 8.1	1	CRITICAL	2
	CVE-2015-0016	Microsoft Windows 8.1	1	CRITICAL	1
	CVE-2014-4073	Microsoft Windows 8.1	1	CRITICAL	1
☐	CVE-2010-3190	Microsoft Visual Studio 2008	1	CRITICAL	1
	CVE-2015-1756	Microsoft Windows 8.1	1	CRITICAL	1
	CVE-2014-4121	Microsoft Windows 8.1	1	CRITICAL	1
	CVE-2016-3236	Microsoft Windows 8.1	1	CRITICAL	1
	CVE-2014-6324	Microsoft Windows 8.1	1	CRITICAL	1

開始弱點修復程序

1. 在服務主控台中，移至 **[軟體管理]** > **[弱點]**。
2. 在清單中選擇弱點，然後按一下 **[安裝修補程式]**。弱點修復精靈將會開啟。
3. 選擇要安裝在所選電腦上的修補程式。按 **[下一步]**。
4. 選擇您要為其安裝修補程式的電腦。
5. 選擇在安裝修補程式之後是否必須對電腦執行重新開機：

- 否 – 更新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，才會進行重新開機。
- 是 – 更新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。

準備就緒後，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。

18.2 修補程式管理

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

如需有關 Windows OS 支援的第三方產品的詳細資訊，請參閱[修補程式管理支援的第三方產品清單 \(62853\)](#)。

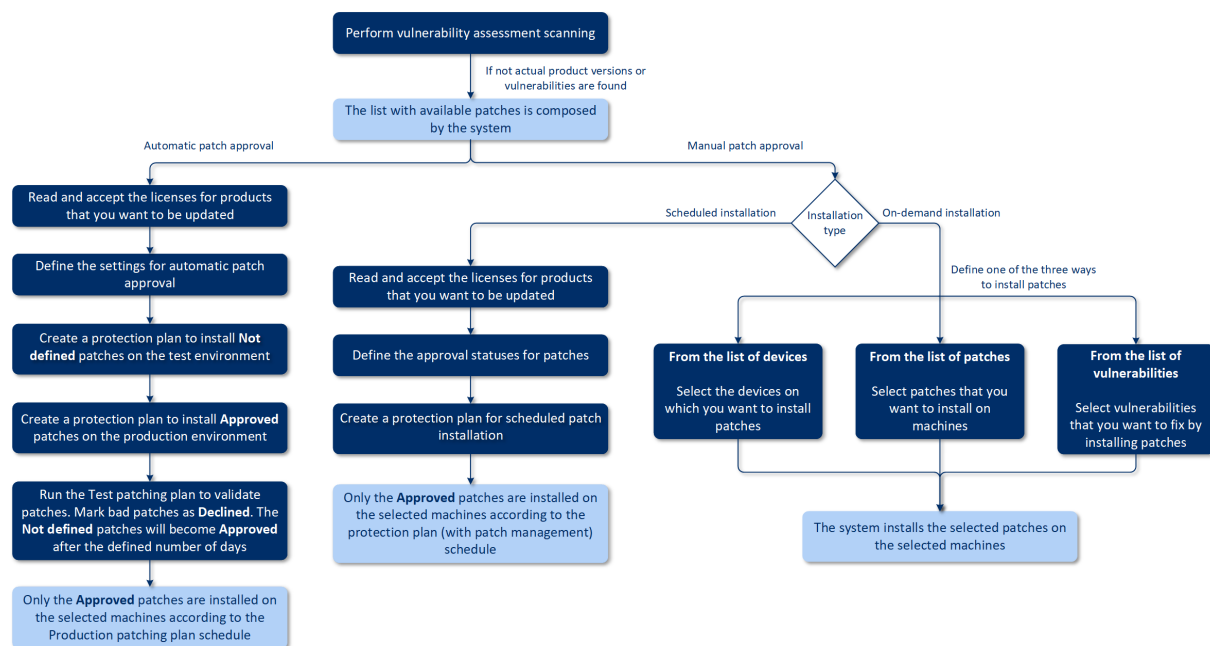
使用修補程式管理功能可：

- 安裝 OS 層級與應用程式層級的更新
- 手動或自動核准修補程式
- 視需要或根據排程，安裝修補程式
- 依下列不同的條件，精確地定義要安裝的修補程式：嚴重性、類別和核准狀態
- 執行更新前備份以防止可能不成功的更新
- 定義修補程式安裝後的重新開機動作

Cyber Protection 推出對等技術，可將網路頻寬流量減至最少。您可以選擇一或多個專用代理程式，這些代理程式將從網際網路下載更新，並在網路中的其他代理程式之間散佈。所有代理程式也會當作對等代理程式，彼此共用更新。

18.2.1 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。有三種替代方式可視需要安裝修補程式：
 - 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 **[監控]** > **[概觀]** > **[修補程式安裝歷史記錄]** 桌面小工具中，監控修補程式安裝的結果。

18.2.2 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。

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以針對 [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。

Updates of specific products ✕

	Products ↓	Category	Severity	Approval status
☐	Windows Server 2012 R2 L...	Custom	Custom	Custom
☒	Windows Server 2012 R2	ServicePacks, Upd...	Critical, High, Medi...	Approved
☒	Windows Server 2012	CriticalUpdates	Critical, High	Approved
☐	Windows Server 2016 and ...	—	—	—
☒	Windows Server 2016	SecurityUpdates	Critical	Approved

[Reset to default](#) [Cancel](#) [Save](#)

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：

- [僅限最近的主要更新] 可讓您安裝最新可用的更新版本。
- [僅限最近的次要更新] 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。

Updates of specific products ✕

	Products	Category	Severity	Approval status
☐	Adobe Reader	Custom	Custom	Approved
☐	Adobe Flash Player for Chr...	—	—	—
☐	Adobe Flash Player for Fire...	—	—	—
☒	Oracle Java Runtime Envir...	Major updates	Critical	Approved
☒	Mozilla Firefox	Minor updates	All	Approved
☐	Google Chrome	—	—	—

Reset to default Cancel Save

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。

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](#)」中。您可以定義下列額外的開始條件：

- **在時間視窗中分配工作開始時間** – 此選項可讓您設定工作的時間範圍，以避免網路瓶頸。您可以以小時或分鐘，指定延遲時間。例如，如果預設開始時間為上午 10:00，且延遲為 60 分鐘，則工作將會在上午 10:00 到上午 11:00 之間開始。
- **如果電腦關閉，則在電腦啟動時執行遺漏的工作**
- **防止在工作執行期間進入睡眠或休眠模式** – 此選項僅適用於執行 Windows 的電腦。
- **如果未符合開始條件，請無論如何在此時間後執行工作** – 指定無論開始條件為何，將會在其後執行工作的時段。

注意事項

Linux 不支援開始條件。

更新之後重新開機 – 定義在安裝更新之後，是否起始重新開機：

- **永不** – 更新後絕不會起始重新開機。
- **如有需要** – 只有在需要套用更新時，才會進行重新開機。
- **一律** – 更新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。

預先更新備份

安裝軟體更新前執行備份 – 系統將會在電腦上安裝任何更新之前，先建立電腦的增量備份。如果沒有稍早建立的備份，將會建立電腦的完整備份。它可以防止更新安裝失敗而且需要恢復到之前狀態的情況。若要讓 **[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。

18.2.3 管理修補程式清單

弱點評估掃描完成之後，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

18.2.4 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。讓我們考慮運作方式的範例。

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. 在服務主控台中，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. 在服務主控台中，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]**。經過 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. 在服務主控台中，移至 **[管理] > [保護計劃]**。
2. 按一下 **[建立計劃]**。
3. 啟用 **[修補程式管理]** 模組。
4. 定義要為 Microsoft 和第三方產品安裝的更新、排程，以及更新前備份。如需有關這些設定的詳細資訊，請參閱「[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。

Updates of specific products ✕

☒	Products ↓	Category	Severity	Approval status
☒	Products ↓	Custom ↓	Custom ↓	Not defined ↓
☒	Active Directory Rights Ma...	CriticalUpdates, Se... ↓	Critical ↓	Not defined ↓
☒	Antigen for Exchange/SMTP	None ↓	All ↓	Not defined ↓
☒	ASP.NET Web Frameworks	Updates ↓	Critical, High, Medi... ↓	Not defined ↓
☒	Azure File Sync agent upda...	None ↓	All ↓	Not defined ↓
☒	Azure File Sync agent upda...	None ↓	All ↓	Not defined ↓

[Reset to default](#) Cancel Save

步驟 4. 準備實際運作修補保護計劃

1. 在服務主控台中，移至 **[管理] > [保護計劃]**。
2. 按一下 **[建立計劃]**。
3. 啟用 **[修補程式管理]** 模組。
4. 定義要為 Microsoft 和第三方產品安裝的更新、排程，以及更新前備份。如需有關這些設定的詳細資訊，請參閱「[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。

Updates of specific products ✕

☒	Products ↓	Category	Severity	Approval status
☒	Active Directory Rights Ma...	Custom	Custom	Approved
☒	Antigen for Exchange/SMTP	CriticalUpdates, Se...	Critical	Approved
☒	ASP.NET Web Frameworks	All	All	Approved
☒	Azure File Sync agent upda...	Updates	Critical, High, Medi...	Approved
☒	Azure File Sync agent upda...	All	All	Approved
☒	Azure File Sync agent upda...	All	All	Approved

Reset to default Cancel Save

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]**。

18.2.5 手動核准修補程式

手動核准修補程式程序如下：

1. 在服務主控台中, 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, 透過按一下 **[立即執行]**, 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。

18.2.6 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. 在服務主控台中, 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。

18.2.7 清單中的修補程式存留時間

若要將修補程式清單維持在最新狀態，移至 **[軟體管理] > [修補程式] > [設定]**，然後指定 **[清單中的存留時間]** 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** – 如果首次安裝後經過 7 天，則會移除該修補程式。

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** – 如果首次安裝後經過 30 天，則會移除該修補程式。

19 軟體清查

軟體清查功能可讓您使用 Cyber Protect (Essentials、Standard 或 Advanced) 授權，檢視適用於所有 Windows 和 macOS 裝置的所有軟體應用程式。

若要取得軟體清查資料，您可以在裝置上執行自動或手動掃描。

您可以使用軟體清查資料來：

- 瀏覽並比較安裝在公司裝置上的所有應用程式的相關資訊
- 判斷應用程式是否需要更新
- 判斷未使用的應用程式是否需要移除
- 確定多個公司裝置上的軟體版本相同
- 監視連續掃描之間軟體狀態的變更。

19.1 啟用軟體清查掃描

使用獲指派的 Cyber Protect 授權和服務配額，在裝置上啟用軟體清查掃描時，系統會每 12 小時自動收集軟體資料一次。

預設會啟用軟體清查掃描功能，但必要時，您可以變更設定。

注意事項

客戶租用戶可以啟用或停用軟體清查掃描。單位租用戶僅能檢視軟體清查掃描設定，但無法變更設定。

若要啟用軟體清查掃描

1. 在服務主控台中，移至 **[設定]**。
2. 按一下 **[保護]**。
3. 按一下 **[清查掃描]**。
4. 按一下模組名稱旁邊的開關，以啟用 **[軟體清查掃描]** 模組。

若要停用軟體清查掃描

1. 在服務主控台中，移至 **[設定]**。
2. 按一下 **[保護]**。
3. 按一下 **[清查掃描]**。
4. 按一下模組名稱旁邊的開關，以停用 **[軟體清查掃描]** 模組。

19.2 手動執行軟體清查掃描

您可以從 **[軟體清查]** 畫面，或從 **[清查]** 畫面中的 **[軟體]** 索引標籤，手動執行軟體清查掃描。

必要條件

- 此裝置可使用 Windows 或 macOS 作業系統。
- 此裝置有一個 Cyber Protect 授權。

若要從 [軟體清查] 畫面執行軟體清查掃描

1. 在服務主控台中，移至 [軟體管理]。
2. 按一下 [軟體清查]。
3. 在 [分組依據:] 下拉式欄位中，選擇 [裝置]。
4. 尋找您要掃描的裝置，然後按一下 [立即掃描]。

若要從 [清查] 畫面中的 [軟體] 索引標籤執行軟體清查掃描

1. 在服務主控台中，移至 [裝置]。
2. 按一下您要掃描的裝置，然後按一下 [清查]。
3. 在 [軟體] 索引標籤中，按一下 [立即掃描]。

19.3 瀏覽軟體清查

您可以檢視並瀏覽資料中可用於所有公司裝置的所有軟體應用程式。

必要條件

- 這些裝置可使用 Windows 或 macOS 作業系統。
- 這些裝置有一個 Cyber Protect 授權。
- 裝置上的軟體清查掃描已成功完成。

若要檢視適用於所有 **Windows** 和 **macOS** 公司裝置的所有軟體應用程式

1. 在服務主控台中，移至 [軟體管理]。
2. 按一下 [軟體清查]。

根據預設，資料會依裝置分組。下表描述 [軟體清查] 畫面中顯示的資料。

欄	描述
名稱	應用程式的名稱。
版本	應用程式的版本。
狀態	應用程式的狀態。 • 新增。 • 已更新。 • 已移除。 • 無變更。
廠商	應用程式的廠商。

欄	描述
安裝日期	安裝應用程式的日期及時間。
上次執行時間	僅限 macOS 裝置。應用程式上次作用中的日期及時間。
位置	安裝應用程式所在的目錄。
使用者	安裝應用程式的使用者。
系統類型	僅限 Windows 裝置。應用程式的位元類型。 • X86 (適用於 32 位元應用程式)。 • X64 (適用於 64 位元應用程式)。

3. 若要將資料依應用程式分組，請在 **[分組依據:]** 下拉式欄位中，選擇 **[應用程式]**。

4. 若要縮小畫面上顯示的資訊範圍，請使用一個篩選條件或多個篩選條件的組合。

a. 按一下 **[篩選]**。

b. 選擇一個篩選條件或數個篩選條件的組合。

下表描述 **[軟體清查]** 畫面中的篩選條件。

篩選器	描述
裝置名稱	裝置名稱。可以複選。如果您要比較特定裝置上的軟體，請使用此篩選條件。
應用程式	應用程式名稱。可以複選。如果您要比較特定裝置或所有裝置上特定應用程式的資料，請使用此篩選條件。
廠商	應用程式的廠商。可以複選。如果您要在特定裝置或所有裝置上，檢視特定廠商的所有應用程式，請使用此篩選條件。
狀態	應用程式狀態。可以複選。如果您要在特定裝置或所有裝置上，檢視所選狀態的所有應用程式，請使用此篩選條件。
安裝日期	安裝應用程式的日期。如果您要在特定裝置或所有裝置上，檢視特定日期安裝的所有應用程式，請使用此篩選條件。
掃描日期	軟體清查掃描的日期。如果您要在該日期掃描的特定裝置或所有裝置上，檢視軟體的相關資訊，請使用此篩選條件。

c. 按一下 **[套用]**。

5. 若要瀏覽整個軟體清查清單，請使用畫面下半部的分頁。

- 按一下您要開啟的頁面的號碼。
- 在下拉式欄位中，選擇您要開啟的頁面的頁碼。

19.4 檢視單一裝置的軟體清查

您可以檢視安裝在單一裝置上的所有軟體應用程式的清單，以及應用程式的相關詳細資訊，例如，狀態、版本、廠商、安裝日期、上次執行時間和位置。

必要條件

- 此裝置可使用 Windows 或 macOS 作業系統。
- 此裝置有一個 Cyber Protect 授權。
- 裝置上的軟體清查掃描已成功完成。

若要從 **[軟體清查]** 畫面檢視單一裝置的軟體清查

1. 在服務主控台中，移至 **[軟體管理]**。
2. 按一下 **[軟體清查]**。
3. 在 **[分組依據:]** 下拉式欄位中，選擇 **[裝置]**。
4. 使用下列其中一個選項，尋找您要檢查的裝置。
 - 使用 **[篩選]** 尋找裝置：
 - a. 按一下 **[篩選]**。
 - b. 在 **[裝置名稱]** 欄位上，選擇您要檢視的裝置的名稱。
 - c. 按一下**[套用]**。
 - 使用動態 **[搜尋]** 尋找裝置：
 - a. 按一下 **[搜尋]**。
 - b. 輸入裝置的完整或部分名稱。

若要從 **[裝置]** 畫面檢視單一裝置的軟體清查

1. 在服務主控台中，移至 **[裝置]**。
2. 按一下您要檢視的裝置，然後按一下 **[清查]**。
3. 按一下 **[軟體]** 索引標籤。

20 硬體清查

硬體清查功能可讓您檢視適用於下列裝置的所有硬體元件：

- 實體 Windows 和 macOS 裝置，其中包含支援硬體清查功能的授權。
- 在下列虛擬化平台上執行的須你 Windows 和 macOS 電腦：VMware、Hyper-V、Citrix、Parallels、Oracle、Nutanix、Virtuozzo 和 Virtuozzo Hybrid Infrastructure。如需有關支援的虛擬化平台版本的詳細資訊，請參閱 "支援的虛擬化平台" (第 31 頁)。

注意事項

Cyber Protect 舊版不支援虛擬機器的硬體清查功能。

只有已安裝保護代理程式的裝置支援硬體清查功能。

若要取得硬體清查資料，您可以在裝置上執行自動或手動掃描。

您可以使用硬體清查資料來：

- 探索組織的所有硬體資產
- 瀏覽組織中所有裝置的硬體清查
- 比較多個公司裝置上的硬體元件
- 檢視硬體元件的詳細資訊。

20.1 啟用硬體清查掃描

在實體裝置和虛擬機器上啟用硬體清查掃描時，系統會每 12 小時自動收集硬體資料一次。

預設會啟用硬體清查掃描功能，但必要時，您可以變更設定。

注意事項

客戶租用戶可以啟用或停用硬體清查掃描。單位租用戶僅能檢視硬體清查掃描設定，但無法變更設定。

若要啟用硬體清查掃描

1. 在服務主控台中，移至 **[設定]**。
2. 按一下 **[保護]**。
3. 按一下 **[清查掃描]**。
4. 按一下模組名稱旁邊的開關，以啟用 **[硬體清查掃描]** 模組。

若要停用硬體清查掃描

1. 在服務主控台中，移至 **[設定]**。
2. 按一下 **[保護]**。
3. 按一下 **[清查掃描]**。
4. 按一下模組名稱旁邊的開關，以停用 **[硬體清查掃描]** 模組。

20.2 手動執行硬體清查掃描

您可以對單一裝置手動執行硬體清查掃描，並檢視裝置硬體元件的目前資料。

注意事項

只有在虛擬機器的目前日期和時間對應到 UTC 的目前日期和時間時，才支援虛擬機器的硬體清查掃描。為確保虛擬機器使用正確的時間設定，請停用虛擬機器的 **[時間同步]** 選項，設定目前的日期、時間和時區，然後重新啟動 **[Acronis Agent Core Service]** 和 **[Acronis Managed Machine Service]**。

必要條件

- (適用於所有裝置) 這些裝置可使用 Windows 或 macOS 作業系統。
- (適用於所有裝置) 這些裝置的授權支援硬體清查功能。請注意，Cyber Protect 舊版不支援虛擬機器的硬體清查功能。
- (適用於所有裝置) 裝置上已安裝保護代理程式。
- (適用於虛擬機器) 電腦可在其中一個支援的虛擬化平台上運作。如需詳細資訊，請參閱 "硬體清查" (第 469 頁)。

若要在單一裝置上執行硬體清查掃描

1. 在服務主控台中，移至 **[裝置]**。
2. 按一下您要掃描的裝置，然後按一下 **[清查]**。
3. 在 **[硬體]** 索引標籤中，按一下 **[立即掃描]**。

20.3 瀏覽硬體清查

您可以檢視並瀏覽資料中可用於所有公司裝置的所有硬體元件。

必要條件

- (適用於所有裝置) 這些裝置可使用 Windows 或 macOS 作業系統。
- (適用於所有裝置) 這些裝置的授權支援硬體清查功能。請注意，Cyber Protect 舊版不支援虛擬機器的硬體清查功能。
- (適用於所有裝置) 裝置上已安裝保護代理程式。
- (適用於所有裝置) 裝置上的硬體清查掃描已成功完成。
- (適用於虛擬機器) 電腦可在其中一個支援的虛擬化平台上運作。如需詳細資訊，請參閱 "硬體清查" (第 469 頁)。

若要檢視適用於 Windows 和 macOS 公司裝置的所有硬體元件

1. 在服務主控台中，移至 **[裝置]**。
2. 在 **[檢視:]** 下拉式欄位中，選擇 **[硬體]**。

注意事項

此檢視是一組欄位，可決定在畫面中顯示的資料。預先定義的檢視為 **[標準]** 和 **[硬體]**。您可以建立並儲存包含不同組欄位，且更方便滿足您需求的自訂檢視。

下表描述 **[硬體]** 檢視中顯示的資料。

欄	描述
名稱	裝置名稱。
硬體掃描狀態	硬體掃描的狀態。 • [已完成]。 • [未開始]。 • 系統會針對不支援硬體清查功能的工作負載，顯示 [不支援] 狀態，亦即，虛擬機器、行動裝置、Linux 裝置。 • 如果在裝置上安裝過期版本的代理程式，則會顯示 [更新代理程式]。按一下此動作將會重新導向至 [設定] > [代理程式] 頁面，系統管理員可以在該頁面上執行代理程式更新。 • 升級配額。按一下此選項將開啟一個對話方塊，系統管理員可以在該對話方塊中，將目前的授權切換到其他可用於租用戶授權的其中一個授權
處理器	裝置所有處理器的型號。
處理器核心	裝置所有處理器的型號。
磁碟儲存空間	以使用的儲存空間，以及裝置所有磁碟的總儲存空間。
記憶體	裝置的 RAM 容量總計。
掃描日期	上次硬體清查掃描的日期和時間。
主機板	裝置的主機板。
主機板序號	主機板的序號。
BIOS 版本	系統 BIOS 的版本。
組織	裝置所屬的組織。
擁有者	裝置的擁有者。
網域	裝置的網域。
作業系統	裝置的作業系統。
作業系統組建	裝置作業系統的組建。

3. 若要在表格中新增欄，按一下欄選項圖示，然後選擇您要在表格中顯示的欄。
4. 若要縮小畫面上顯示的資訊範圍，請使用一或多個篩選條件。
 - a. 按一下 **[搜尋]**。
 - b. 按一下箭頭，然後按一下 **[硬體]**。
 - c. 選擇一個篩選條件或數個篩選條件的組合。

下表描述 **[硬體]** 篩選條件。

篩選器	描述
處理器型號	可以複選。如果您要檢視具備指定處理器型號之裝置的硬體資料，請使用此篩選條件。
處理器核心	如果您要檢視具備指定處理器核心數目之裝置的硬體資料，請使用此篩選條件。
磁碟大小總計	如果您要檢視具備指定儲存空間大小總計之裝置的硬體資料，請使用此篩選條件。
記憶體容量	如果您要檢視具備指定 RAM 容量之裝置的硬體資料，請使用此篩選條件。

- d. 按一下**[套用]**。
5. 若要以遞增順序排序資料，按一下欄名稱。

20.4 檢視單一裝置的硬體

您可以檢視特定裝置的主機板、處理器、記憶體、圖形卡、儲存磁碟機、網路和系統的詳細資訊。

必要條件

- (適用於所有裝置) 這些裝置可使用 Windows 或 macOS 作業系統。
- (適用於所有裝置) 這些裝置的授權支援硬體清查功能。請注意，Cyber Protect 舊版不支援虛擬機器的硬體清查功能。
- (適用於所有裝置) 裝置上已安裝保護代理程式。
- (適用於所有裝置) 裝置上的硬體清查掃描已成功完成。
- (適用於虛擬機器) 電腦可在其中一個支援的虛擬化平台上運作。如需詳細資訊，請參閱 "硬體清查" (第 469 頁)。

若要檢視特定裝置硬體的詳細資訊

1. 在服務主控台中，移至 **[裝置]** > **[所有裝置]**。
2. 在 **[檢視:]** 下拉式欄位中，選擇 **[硬體]**。
3. 使用以下所述的其中一個方法，尋找您要檢查的裝置。
 - 使用 **[篩選]** 尋找裝置：
 - a. 按一下 **[篩選]**。
 - b. 選擇一個篩選參數或數個篩選參數的組合以尋找裝置。
 - c. 按一下**[套用]**。

- 使用 **[搜尋]** 尋找裝置：
 - a. 按一下 **[搜尋]**。
 - b. 輸入裝置的完整或部分名稱，然後按一下 **Enter**。
- 4. 按一下列出裝置的那一行，然後按一下 **[清查]**。
- 5. 按一下 **[硬體]** 索引標籤。

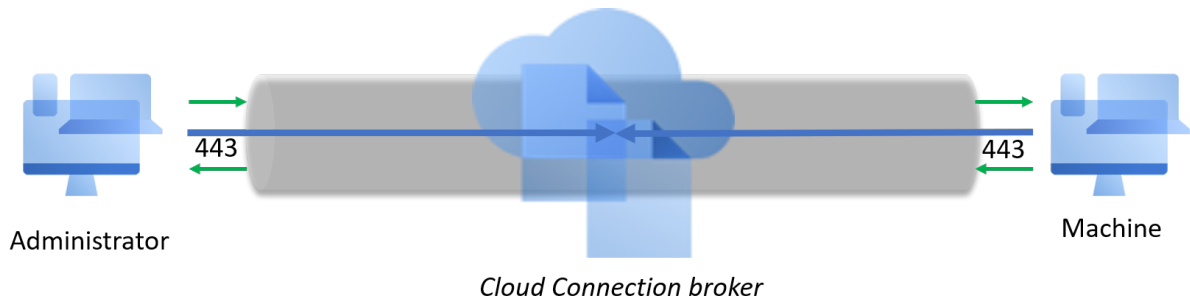
隨即提供下列硬體資料。

硬體元件	顯示的資訊
主機板	裝置主機板的名稱、製造商、型號和序號。
處理器	裝置各個處理器的製造商、型號、最大時脈速度和核心數目。
記憶體	裝置記憶體的容量、製造商和序號。
圖形卡	裝置 GPU 的製造商和型號。
儲存磁碟機	裝置儲存磁碟機的型號、媒體類型、可用空間和大小。
網路	裝置網路介面卡的 Mac 位址、IP 位址和類型。
系統	系統的產品識別碼、原始安裝日期、系統開機時間、系統製造商、系統型號、BIOS 版本、開機裝置、系統地區設定和時區。

21 遠端桌面存取

21.1 遠端存取 (RDP 和 HTML5 用戶端)

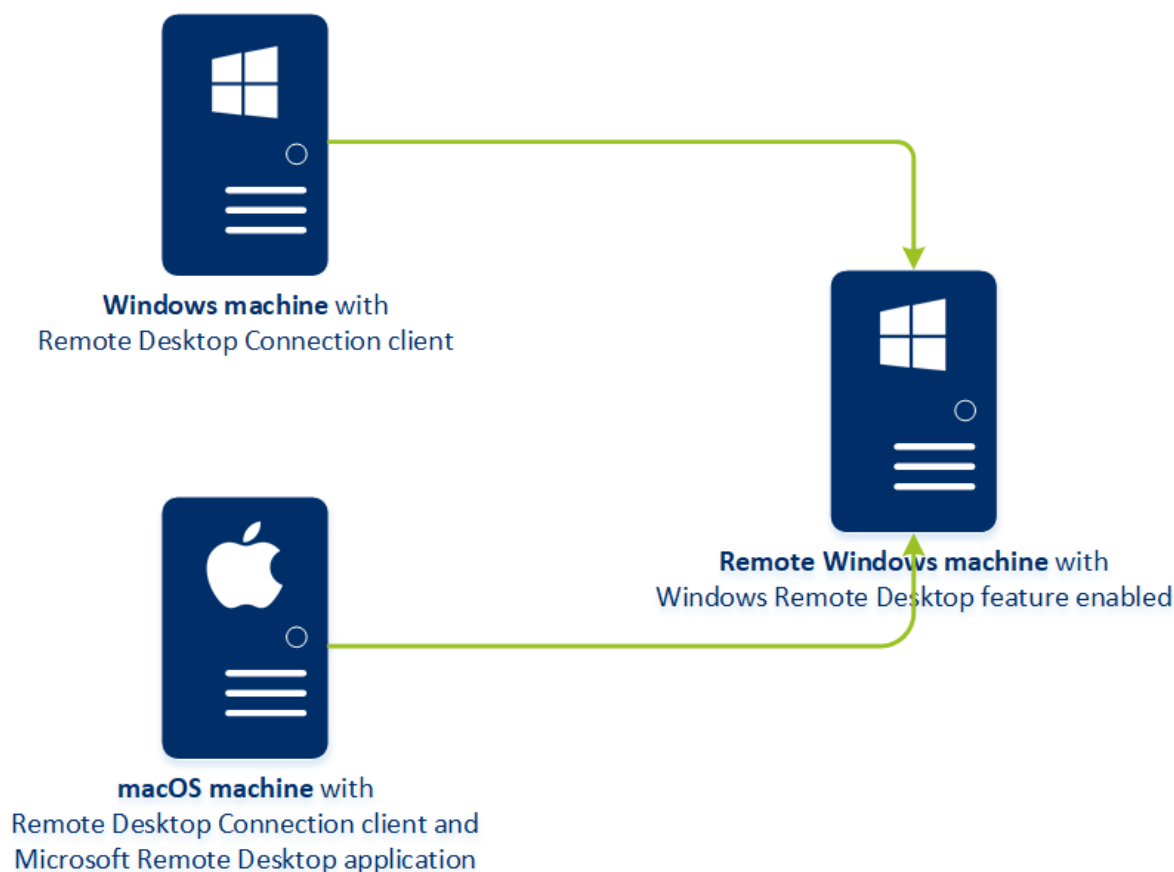
Cyber Protection 為您提供遠端存取功能。您可以透過遠端連線，連線並管理使用者電腦。您可以使用 HTML5 用戶端，將文字複製並貼到遠端電腦中，或從遠端電腦複製並貼上文字。您可以使用 RDP 用戶端，複製並貼上文字以及檔案。如此可讓您輕鬆地協助使用者解決其電腦上的問題。



必要條件：

- 遠端電腦會在 Cyber Protection 中登錄，並安裝保護代理程式。
- Cyber Protect 配額已存在或已為電腦取得。
- 若是 RDP 連線，Remote Desktop Connection Client 已安裝在啟動連線所在的電腦上。

RDP 工作階段可以從 Windows 和 macOS 電腦建立。HTML5 遠端連線工作階段可以從支援 HTML5 的任何瀏覽器建立。



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。因此，遠端存取無法用於連線至 Windows 10 家用版和 macOS 系統。

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

21.1.1 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 配額。如果客戶租用戶存在遠端 RDP 功能所需的服務配額，但是此電腦未取得該配額，則系統會提示您手動取得此服務配額。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，您輸入認證，如果其驗證成功，則可存取電腦。

21.1.2 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. 在服務主控台中，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] / [透過 HTML5 用戶端連線]**。

系統會檢查此電腦是否有 Cyber Protect 配額。如果客戶租用戶存在遠端 RDP 功能所需的服務配額，但是此電腦未取得該配額，則系統會提示您手動取得此服務配額。

3. 如果出現提示，請選擇其中一個建議的服務配額，然後按一下 **[變更並連線]**。
4. [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。
5. 指定用來存取電腦的登入和密碼，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。

21.1.3 如何執行遠端協助工作階段

遠端協助允許並行存取相同的遠端桌面工作階段。例如，當您需要修正遠端使用者電腦上的問題時，可以使用遠端協助連線至該電腦。使用者和遠端系統管理員會共用一個工作階段，而且使用者可以分享並重現問題。

1. 在服務主控台中，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]>[執行遠端協助]**。
系統會檢查此電腦是否有 Cyber Protect 配額。如果客戶租用戶存在遠端 RDP 功能所需的服務配額，但是此電腦未取得該配額，則系統會提示您手動取得此服務配額。
3. 如果出現提示，請選擇其中一個建議的服務配額，然後按一下 **[變更並連線]**。
4. 複製遠端協助工作階段密碼，然後按一下 **[連線]**。如果工作階段未啟動，請在電腦上下載並安裝連線代理程式，然後重試連線。
5. 如果有持續的互動式工作階段，按一下 **[連線至工作階段]**。
6. 輸入遠端協助工作階段密碼。

結果，您擁有遠端電腦的遠端桌面存取權，而且可以協助使用者。

21.2 與使用者共用遠端連線

從遠端工作且需要存取遠端電腦的使用者可以在沒有為遠端連線設定的 VPN 或其他工具的情況下存取電腦。

Cyber Protection 服務可讓您能夠與使用者共用 RDP 連結，從而使他們可以從遠端存取其電腦。

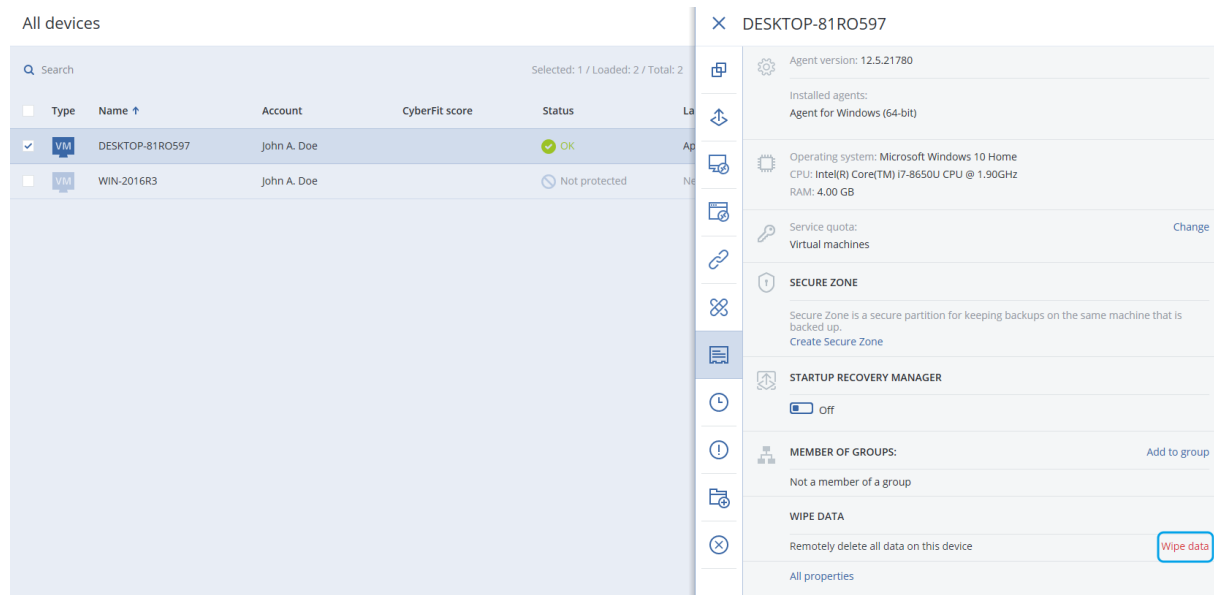
1. 啟用遠端連線功能
 - a. 在服務主控台中，移至 **[設定]>[保護]>[遠端連線]**。
 - b. 啟用 **[共用遠端桌面連線]**。
當您選擇裝置時，**[共用遠端連線]** 選項將會出現在右側功能表中。
2. 產生共用遠端連線的連結。
 - a. 在服務主控台中，移至 **[裝置]>[所有裝置]**，然後選擇您要為其提供遠端連線的裝置。
 - b. 按一下 **[網路保護桌面]>[共用遠端連線]**。
 - c. 按一下 **[取得連結]**。在開啟的視窗中，複製所產生的連結。
此連結的有效期限為 10 小時。
3. 與使用者共用連結。
此連結會將使用者重新導向至必須選擇連線類型所在的頁面：

- 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 RDP 用戶端。系統會將使用者重新導向至必須輸入使用者對遠端電腦的認證所在的登入畫面。

22 遠端抹除

遠端抹除可讓 Cyber Protection 服務系統管理員和電腦擁有者刪除受管理電腦上的資料，例如，當資料遺失或遭竊時。因此，將會防止任何未經授權者存取機密資訊。

遠端抹除僅適用於執行 Windows 10 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. 在服務主控台中，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 **[監控] > [活動]** 中檢查抹除程序以及啟動者的詳細資料。

23 智慧型保護

23.1 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下列一組特定動作，解決部分安全性警示。其他安全性警示只是用於通知您即將來臨的威脅，但是沒有可用的建議動作。

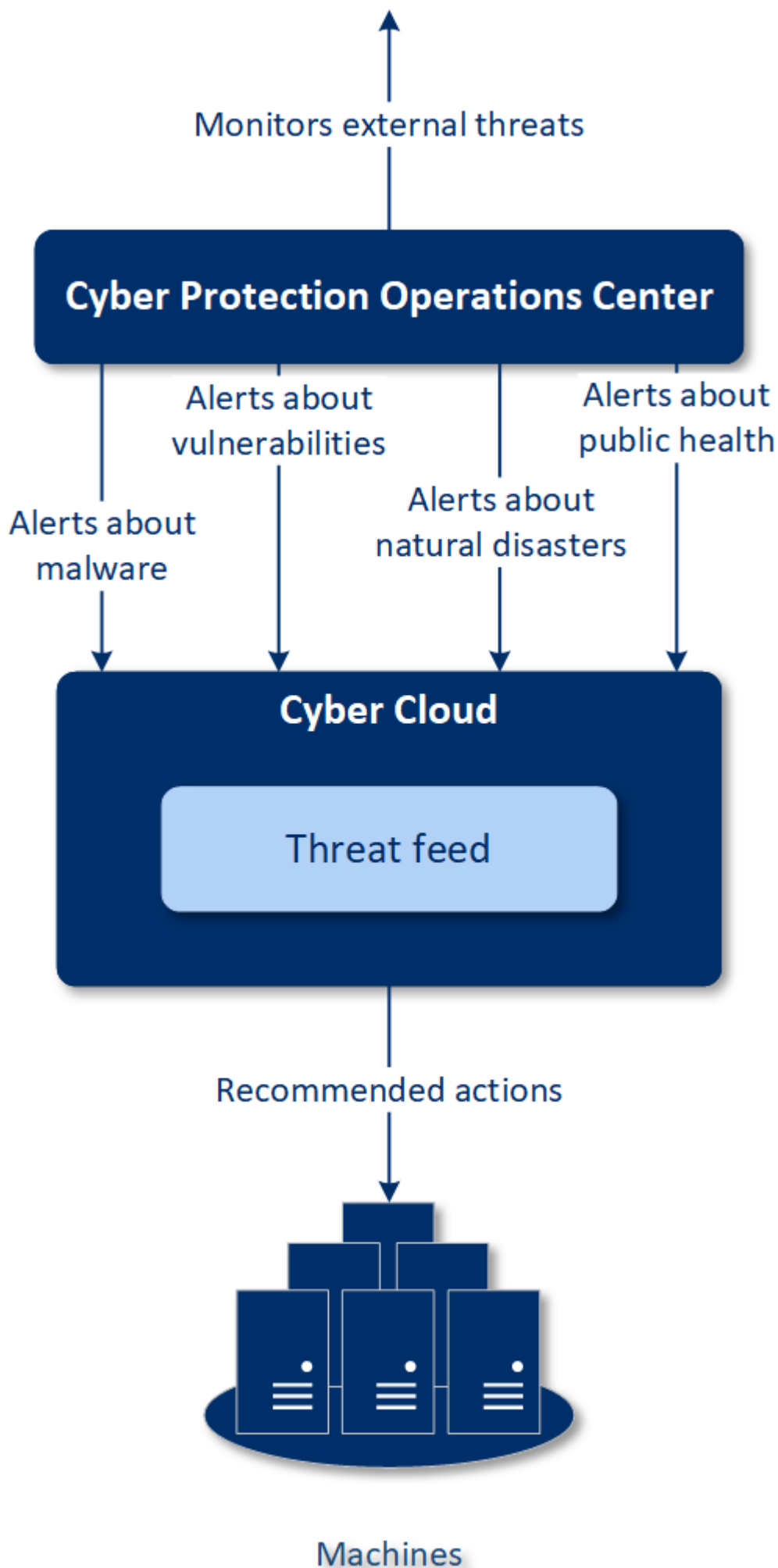
注意事項

系統僅會針對已安裝反惡意程式碼保護用代理程式的電腦，產生惡意程式碼警示。

23.1.1 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。您將能夠在服務主控台的 **[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. 在服務主控台中，移至 **[監控]** > **[威脅摘要]** 以檢閱是否有任何現有的安全性警示。
2. 在清單中選擇一個警示，然後檢閱所提供的詳細資料。
3. 按一下 **[開始]** 以啟動精靈。
4. 啟用您想要執行的動作，以及必須套用這些動作的電腦。可以建議下列動作：
 - **弱點評估** – 掃描電腦中的弱點
 - **修補程式管理** – 將修補程式安裝在所選電腦上
 - **反惡意程式碼保護** – 對所選電腦執行完整掃描

注意事項

此動作僅是用於已安裝反惡意程式碼保護用代理程式的電腦。

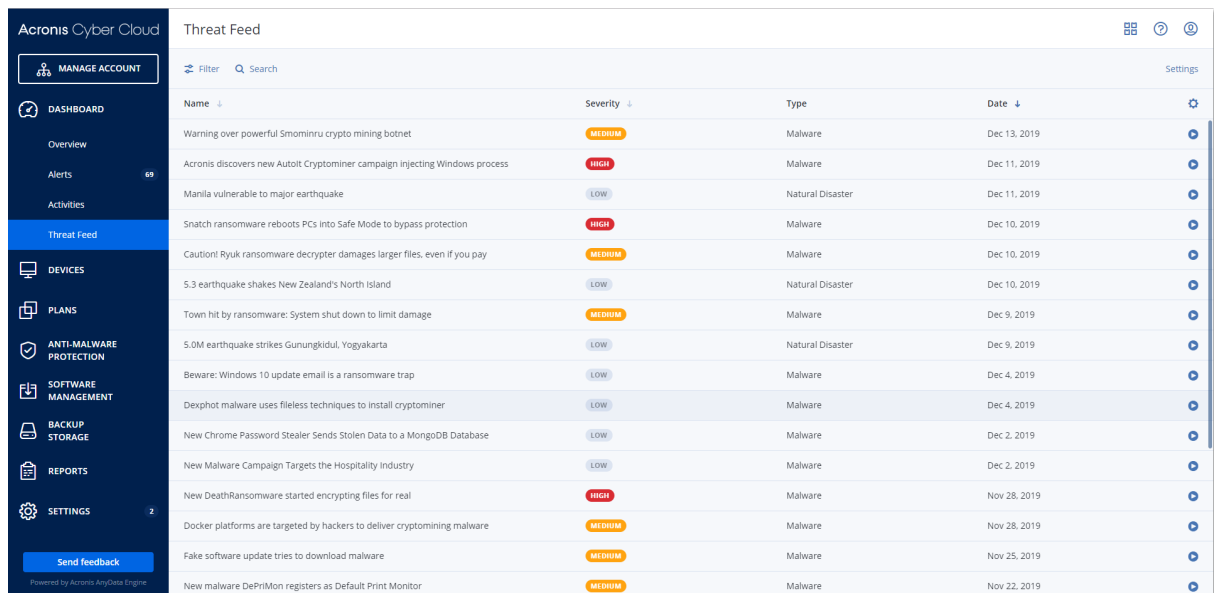
- **備份受保護或未受保護的電腦** – 備份受保護和未受保護的工作負載。
如果還沒有適用於工作負載 (在所有可存取的位置、雲端和本機) 的備份，或現有備份經過加密，則系統會使用下列名稱格式，建立一個完整備份：

%workload_name%-Remediation

根據預設，備份的目的地是 **Cyber Cloud** 儲存空間，但是您可以在開始作業之前，設定其他位置。

如果未加密的備份已存在，系統將會在現有的存檔中，建立一個增量備份。

5. 按一下 **[開始]**。
6. 在 **[活動]** 頁面上，確認已成功執行活動。



Name	Severity	Type	Date
Warning over powerful Smominru crypto mining botnet	MEDIUM	Malware	Dec 13, 2019
Acronis discovers new Autoit Cryptominer campaign injecting Windows process	HIGH	Malware	Dec 11, 2019
Manila vulnerable to major earthquake	LOW	Natural Disaster	Dec 11, 2019
Snatch ransomware reboots PCs into Safe Mode to bypass protection	HIGH	Malware	Dec 10, 2019
Caution! Ryuk ransomware decrypter damages larger files, even if you pay	MEDIUM	Malware	Dec 10, 2019
5.3 earthquake shakes New Zealand's North Island	LOW	Natural Disaster	Dec 10, 2019
Town hit by ransomware: System shut down to limit damage	MEDIUM	Malware	Dec 9, 2019
5.0M earthquake strikes Gunungkidul, Yogyakarta	LOW	Natural Disaster	Dec 9, 2019
Beware: Windows 10 update email is a ransomware trap	LOW	Malware	Dec 4, 2019
Dexphot malware uses fileless techniques to install cryptominer	LOW	Malware	Dec 4, 2019
New Chrome Password Stealer Sends Stolen Data to a MongoDB Database	LOW	Malware	Dec 2, 2019
New Malware Campaign Targets the Hospitality Industry	LOW	Malware	Dec 2, 2019
New DeathRansomware started encrypting files for real	HIGH	Malware	Nov 28, 2019
Docker platforms are targeted by hackers to deliver cryptominer malware	MEDIUM	Malware	Nov 28, 2019
Fake software update tries to download malware	MEDIUM	Malware	Nov 25, 2019
New malware DePrimon registers as Default Print Monitor	MEDIUM	Malware	Nov 22, 2019

23.1.2 刪除所有警示

在下列期限之後，從威脅摘要進行自動清理：

- 自然災害 – 1 週
- 弱點 – 1 個月

- 惡意程式碼 - 1 個月
- 公共衛生 - 1 週

23.2 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。

23.2.1 運作原理

1. 首先, 您在啟用 [資料保護圖模組](#) 的情況下, 建立一個保護計劃。
2. 接著, 在執行計劃並發現和分析資料之後, 您將在 [\[資料保護圖\]](#) 桌面小工具上, 取得資料保護的視覺表示。
3. 您也可以移至 **[裝置] > [資料保護圖]**, 並在該處尋找每個裝置上未受保護檔案的相關資訊。
4. 您可以採取動作以保護裝置上偵測到的未受保護檔案。

23.2.2 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. 在服務主控台中, 移至 **[裝置] > [資料保護圖]**。
在裝置的清單中, 您可以找到未受保護檔案數目、每個裝置這類檔案大小, 以及上次資料探索的相關資訊。
若要保護特定電腦上的檔案, 按一下省略符號圖示, 然後按一下 **[保護所有檔案]**。系統會將您重新導向到計劃清單, 您可以在已啟用 [備份] 模組的情況下, 在其中建立一個保護計劃。
若要從清單中刪除具有未受保護檔案的特定裝置, 按一下 **[在下次資料探索之前隱藏]**。
2. 若要檢視特定裝置上未受保護檔案的更詳細資訊, 請按一下該裝置的名稱。
您將根據副檔名和位置, 看到未受保護檔案的數目。在搜尋欄位中, 定義您要取得其未受保護檔案相關資訊的副檔名。
3. 若要保護所有未受保護的檔案, 按一下 **[保護所有檔案]**。系統會將您重新導向到計劃清單, 您可以在已啟用 [備份] 模組的情況下, 在其中建立一個保護計劃。

若要以報告形式取得未受保護檔案的相關資訊, 按一下 **[下載 CSV 格式的詳細報告]**。

23.2.3 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。

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](#)」中。您可以定義下列額外的開始條件:

- **在時間視窗中分配工作開始時間** - 此選項可讓您設定工作的時間範圍, 以避免網路瓶頸。您可以以小時或分鐘, 指定延遲時間。例如, 如果預設開始時間為上午 10:00, 且延遲為 60 分鐘, 則工作將會在上午 10:00 到上午 11:00 之間開始。
- **如果電腦關閉, 則在電腦啟動時執行遺漏的工作**
- **防止在工作執行期間進入睡眠或休眠模式** - 此選項僅適用於執行 Windows 的電腦。
- **如果未符合開始條件, 請無論如何在此時間後執行工作** - 指定無論開始條件為何, 將會在其後執行工作的時段。

注意事項

Linux 不支援開始條件。

副檔名和例外規則

在 **[副檔名]** 索引標籤上, 您可以定義在資料復原期間將被視為重要並檢查其是否受到保護之副檔名的清單。使用下列格式定義副檔名:

.html、.7z、.docx、.zip、.pptx、.xml

在 **[例外規則]** 索引標籤上, 您可以定義在資料復原期間, 不檢查保護狀態的檔案和資料夾。

- **隱藏的檔案和資料夾** - 如果已選擇, 在資料檢查期間, 將會略過隱藏的檔案和資料夾。
- **系統檔案和資料夾** - 如果已選擇, 在資料檢查期間, 將會略過系統檔案和資料夾。

24 加強安全性模式

加強安全性模式為具有更高安全性需求的用戶端，提供特殊設定。此模式要求強制加密所有備份，而且僅允許在本機設定加密密碼。

使用加強安全性模式時，在客戶租用戶及其單位中建立的所有備份都會自動使用 AES 演算法和 256 位元金鑰加密。使用者僅能在受保護的裝置上設定其加密密碼，而且無法在保護計劃中設定加密密碼。

雲端服務無法存取加密密碼。基於此限制，下列功能在加強安全性模式下無法用於租用戶：

- 透過服務主控台復原
- 透過服務主控台瀏覽檔案層級的備份
- 雲端對雲端備份
- 網站備份
- 應用程式備份
- 備份行動裝置
- 備份的反惡意程式碼掃描
- 安全復原
- 自動建立公司白名單
- 資料保護圖
- 災難復原
- 與無法使用之功能相關的報告和儀表板

24.1 限制

- 加強安全性模式僅與其版本為 15.0.26390 或更新版本的代理程式相容。
- 加強安全性模式不適用於執行 Red Hat Enterprise Linux 4.x 或 5.x 及其衍生產品的裝置。

24.2 設定加密密碼

您必須在受保護的裝置本機上設定加密密碼。您無法在保護計劃中設定加密密碼。如果沒有密碼，建立備份將會失敗。

您可以利用下列方式，設定加密密碼：

1. 在安裝保護計劃期間 (適用於 Windows、macOS 和 Linux)。
2. 使用命令列 (適用於 Windows 和 Linux)。

這是在虛擬裝置上設定加密密碼的唯一方式。

如需有關如何使用 **Acropsh** 工具設定加密密碼的詳細資訊，請參閱 "儲存電腦上的加密設定" (第 172 頁)。

3. 在 Cyber Protect 監視器中 (適用於 Windows 和 macOS)。

警告！

若是遺失或忘記密碼，則無法復原加密的備份。

在 **Cyber Protect** 監視器中設定加密密碼

1. 在受保護的裝置上，以系統管理員身分登入。
2. 按一下通知區域 (Windows) 或功能表列 (macOS) 中的 [Cyber Protect 監視器] 圖示。
3. 按一下齒輪圖示。
4. 按一下**加密**。
5. 設定加密密碼。
6. 按一下 **[確定]**。

24.3 變更加密密碼

您可以在保護計劃建立任何備份之前，變更加密密碼。

不建議在建立備份之後變更加密密碼，因為後續的備份將會失敗。若要繼續保護相同的電腦，您必須為其建立新的保護計劃。同時變更加密密碼和保護計劃將會導致建立使用變更後的密碼加密的新備份。在這些變更之前建立的備份將不會受到影響。

或者，您可以保留已套用的保護計劃，僅變更其中的備份檔案名稱。這也將導致建立使用變更後的密碼加密的新備份。若要深入瞭解備份檔案名稱，請參閱 "備份檔案名稱" (第 178 頁)。

您可以利用下列方式，變更加密密碼：

1. 在 Cyber Protect 監視器中 (適用於 Windows 和 macOS)。
2. 使用命令列 (適用於 Windows 和 Linux)。

如需有關如何使用 **Acropsh** 工具設定加密密碼的詳細資訊，請參閱 "儲存電腦上的加密設定" (第 172 頁)。

24.4 復原備份

您無法使用加強安全性模式，透過服務主控台復原備份。

您可以選取下列選項：

- 使用可開機媒體復原整部電腦、其磁碟或檔案。
- 使用 [Windows 檔案總管]，透過已安裝的代理程式，從 Windows 電腦本機備份解擷取檔案。

25 不可變動儲存空間

固定儲存空間允許您在指定的保留期間內存取已刪除的備份。您可從這些備份中復原內容，但無法變更、移動或刪除。當保留期限結束後，固定儲存空間內的已刪除備份將會永久抹除。

固定儲存空間中已刪除的備份仍然會使用儲存空間，並據以收費。

25.1 限制

- 固定儲存空間需要保護代理程式版本 21.12 (組建 15.0.28532) 或更高版本。
- 僅支援 TIBX(版本 12) 備份。

25.2 啟用和停用固定儲存空間

公司管理員可以啟用或停用固定儲存空間，或變更其保留期間。

在子租用戶中未套用任何自訂設定時，子租用戶會繼承父租用戶的設定。

只有在針對系統管理員帳戶所屬的租用戶啟用雙重驗證機制時，您才可以設定固定儲存空間設定。

您可以在 Cyber Protection 服務主控台或管理入口網站中設定固定儲存空間設定。兩者都可以存取相同的設定。

若要在服務主控台中啟用固定儲存空間

1. 以公司系統管理員的身分，登入 Cyber Protection 服務主控台。
2. 在導覽功能表中，按一下 **[設定]>[系統設定]**。
3. 捲動預設備份選項清單，然後按一下 **[固定儲存空間]**。
4. 啟用 **[固定儲存空間]** 開關。
5. **[選用]** 在 1 到 999 天範圍內指定所需保留期間。
預設保留期間為 14 天。較長保留期間可能會導致儲存空間使用量增加。
6. 要讓現有備份支援固定儲存空間，請執行其保護計劃來更新備份。
備份作業完成之後，當您刪除備份時，它在固定儲存空間的保留期間內仍可存取，而非永久抹除。

警告！

如果在啟用固定儲存空間之後刪除備份而不進行更新，將會永久抹除該備份。

因此，您將能夠從指定保留期間內的已刪除備份中復原資料。

若要在服務主控台中停用固定儲存空間

1. 以公司系統管理員的身分，登入 Cyber Protection 服務主控台。
2. 在導覽功能表中，按一下 **[設定]>[系統設定]**。
3. 捲動預設備份選項清單，然後按一下 **[固定儲存空間]**。
4. 停用 **[固定儲存空間]** 開關。

警告！

如果停用固定儲存空間，將永久抹除所有已刪除的備份。刪除新備份也屬於永久性。

若要了解如何在管理入口網站中設定固定儲存空間設定，請參閱系統管理員指南中的[設定固定儲存空間](#)。

25.3 存取固定儲存空間中已刪除的備份

當啟用固定儲存空間時，您可以存取已刪除的備份並在指定的保留期間內從這些備份復原資料。

存取已刪除的備份並從中復原資料

1. 在 **[備份儲存空間]**索引標籤上，選擇包含已刪除備份的雲端儲存空間。
2. [僅適用於已刪除的備份組] 要查看已刪除的備份組，請按一下 **[顯示已刪除]** 的備份組。
3. 選擇想要的備份組。
4. 按一下 **[顯示備份]**，然後按一下 **[顯示已刪除]** 的備份組。
5. 選擇已刪除的備份並從中復原資料。
6. 繼續執行復原作業，如 "復原" (第 209 頁) 中所述。

26 裝置控制

裝置控制模組¹運用每個受保護電腦上的資料洩漏防禦用代理程式²功能子集，偵測並防止本機電腦通道上未經授權的資料存取和傳輸，作為 Cyber Protection 服務保護計劃的一部分。其對各式各樣的資料洩漏途徑提供細微的控制，包括使用卸除式媒體、印表機、虛擬和重新導向的裝置，以及 Windows 剪貼簿交換資料。

此模組適用於按工作負載授權的 Cyber Protect Essentials、Cyber Protect Standard 以及 Cyber Protect Advanced 版本。

注意事項

在 Windows 電腦上，裝置控制功能需要安裝資料洩漏防禦用代理程式。如果在其保護計劃中啟用 **[裝置控制]** 模組，則會為受保護的工作負載自動安裝該代理程式。

裝置控制模組依賴代理程式的資料洩漏防禦³功能，強制對受保護電腦上的資料存取和傳輸作業，執行情境控制。這些包括使用者對週邊裝置和連接埠的存取、文件列印、剪貼簿複製/貼上作業、媒體格式化和退出作業，以及與本機連線行動裝置的同步。資料洩漏防禦用代理程式包含裝置控制模組所有中央管理和系統管理元件的架構，因此其必須安裝在要使用裝置控制模組保護的每部電腦上。此代理程式會根據其接收自受保護電腦所套用之保護計劃的裝置控制設定，允許、限制或拒絕使用者動作。

無論是直接在受保護電腦上使用，還是在受保護電腦上託管的虛擬化環境中重新導向，裝置控制模組都可以控制對各種週邊裝置的存取。此模組可辨識在 Microsoft Remote Desktop Server、Citrix XenDesktop / XenApp / XenServer，以及 VMware Horizon 中重新導向的裝置。它也可以控制在 VMware Workstation / Player、Oracle VM VirtualBox 或 Windows Virtual PC 上執行之客體作業系統的剪貼簿，以及在受保護電腦上執行之主機作業系統的剪貼簿之間的資料複製作業。

裝置控制模組可以保護執行下列作業系統的電腦：

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

¹裝置控制模組運用每個受保護電腦上的資料洩漏防禦代理程式功能子集，偵測並防止本機電腦通道上未經授權的資料存取和傳輸，作為保護計劃的一部分。這些包括使用者對週邊裝置和連接埠的存取、文件列印、剪貼簿複製/貼上作業、媒體格式化和退出作業，以及與本機連線行動裝置的同步。裝置控制模組對允許使用者在受保護的電腦上存取的裝置和連接埠的類型，以及使用者可以在這些裝置上執行的動作，提供精細的情境控制。

²資料洩漏防禦系統的用戶端元件，可透過套用環境和內容分析技術的組合，並強制執行集中管理的資料洩漏防禦政策，保護其主機電腦，免於未經授權者使用、傳輸和儲存機密、受保護或敏感的資料。網路保護提供一個功能全面的資料洩漏防禦代理程式。但是，代理程式在受保護電腦上的功能受限於網路保護授權使用的一組資料洩漏防禦功能，並取決於套用至該電腦的保護計劃。

³一種整合式技術和組織措施的系統，旨在偵測和防止組織內外部未經授權的實體有意和無意地洩露/存取機密、受保護或敏感的資料，或將此類資料傳輸到不受信任的環境。

注意事項

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

注意事項

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

26.0.1 使用資料洩漏防禦用代理程式搭配 Hyper-V 的限制

請勿將資料洩漏防禦用代理程式安裝在 Hyper-V 叢集中的 Hyper-V 主機上, 因為這可能會造成 BSOD 問題, 主要是在具有叢集式共用磁碟區 (CSV) 的 Hyper-V 叢集中。

如果您使用下列任何版本的 Hyper-V 用代理程式, 您需要手動移除資料洩漏防禦用代理程式:

- 15.0.26473 (C21.02)
- 15.0.26570 (C21.02 HF1)
- 15.0.26653 (C21.03)
- 15.0.26692 (C21.03 HF1)
- 15.0.26822 (C21.04)

若要移除資料洩漏防禦用代理程式, 請在 Hyper-V 主機上, 手動執行安裝程式, 然後清除 [資料洩漏防禦用代理程式] 核取方塊, 或執行下列命令:

```
<installer_name> --remove-components=agentForDlp -quiet
```

您可以在服務主控台中保護計劃的 **[裝置控制]** 區段內啟用並設定裝置控制模組。如需指示, 請參閱 [啟用或停用裝置控制的步驟](#)。

[裝置控制] 區段會顯示模組設定的摘要:

Device control Access to 7 device types is limited. Allowlists are configured			
Access settings	Restricted: USB, Removable, Printers and 4 more		
Device types allowlist	1 allowed		
USB devices allowlist	1 allowed		
Exclusions	2 excluded		

- **存取設定** - 顯示具有受限 (拒絕或唯讀) 存取權之裝置類型和連接埠的摘要 (如果有的話)。否則, 指明允許所有裝置類型。按一下此摘要可檢視或變更存取設定 (請參閱[檢視或變更存取設定的步驟](#))。
- **裝置類型允許名單** - 透過從裝置存取控制排除, 顯示允許的裝置子類別數量 (如果有的話)。否則, 指明允許名單是空的。按一下此摘要可檢視或變更允許的裝置子類別選項 (請參閱[從存取控制排除裝置子類別的步驟](#))。
- **USB 裝置允許名單** - 透過從裝置存取控制排除, 顯示允許的 USB 裝置/型號數量 (如果有的話)。否則, 指明允許名單是空的。按一下此摘要可檢視或變更允許的 USB 裝置/型號清單 (請參閱[從存取控制排除各個 USB 裝置的步驟](#))。
- **排除** - 顯示針對 Windows 剪貼簿、螢幕擷取畫面擷取、印表機和行動裝置設定的存取控制排除數目。

26.1 使用裝置控制

本節涵蓋使用裝置控制模組時基本工作的逐步指示。

26.1.1 啟用或停用裝置控制

您可以在 [建立保護計劃](#) 時啟用裝置控制。您可以將現有的保護計劃變更為啟用或停用裝置控制。

啟用或停用裝置控制

1. 在服務主控台中, 移至 **[裝置] > [所有裝置]**。
2. 執行下列其中一項操作以開啟保護計劃面板:
 - 如果您要建立新的保護計劃, 選擇要保護的電腦, 按一下 **[保護]**, 然後按一下 **[建立計劃]**。
 - 如果您要變更現有的保護計劃, 選擇受保護的電腦, 按一下 **[保護]**, 按一下保護計劃名稱旁的省略符號 (...), 然後按一下 **[編輯]**。
3. 在保護計劃面板中, 瀏覽至 **[裝置控制]** 區域, 然後按一下滑鼠, 以開啟或關閉 **[裝置控制]** 開關。
4. 執行下列其中一項操作以套用您的變更:
 - 若要建立保護計劃, 按一下 **[建立]**。
 - 若要編輯保護計劃, 按一下 **[儲存]**。

您也可以從 [\[管理\]](#) 索引標籤存取保護計劃面板。但是, 此功能無法用於 Cyber Protection 服務的所有版本。

26.1.2 在 macOS 上啟用裝置控制模組

保護計劃的裝置控制設定僅會在受保護的工作負載上載入裝置控制驅動程式之後生效。本節描述如何載入裝置控制驅動程式, 以便在 macOS 上啟用裝置控制模組。這是需要端點電腦系統管理員權限的一次性作業。

支援的 macOS 版本:

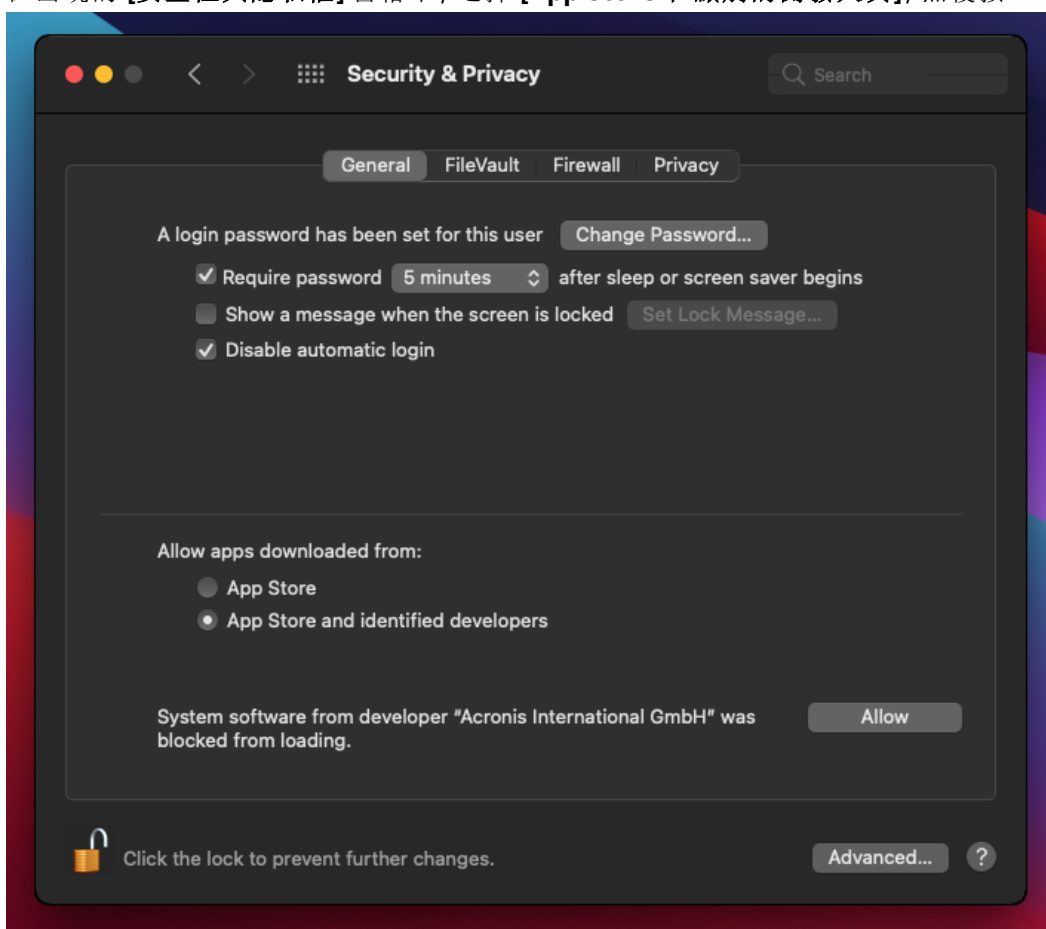
- macOS 10.15 (Catalina) 和更新版本
- macOS 11.2.3 (Big Sur) 和更新版本

若要在 macOS 上啟用裝置控制模組

1. 在您要保護的電腦上, 安裝 Mac 用代理程式。
2. 在保護計劃中, 啟用裝置控制設定。
3. 套用保護計劃。
4. 「系統擴充功能已封鎖」警告將會出現在受保護的工作負載上。按一下 **[開啟安全性喜好設定]**。



5. 在出現的 **[安全性與隱私權]** 窗格中, 選擇 **[App Store 和識別的開發人員]**, 然後按一下 **[允許]**。



6. 在出現的對話方塊中, 按一下 **[重新啟動]** 以重新啟動工作負載, 並啟用裝置控制設定。

注意事項

如果停用裝置控制設定後再次啟用, 您就不必重複這些步驟。

26.1.3 檢視或變更存取設定

從保護計劃面板中, 您可以管理裝置控制模組的存取設定。如此一來, 您可以允許或拒絕存取特定類型的裝置, 以及啟用或停用通知和警示。

檢視或變更存取設定

1. 開啟保護計劃的保護計劃面板, 然後在該計劃中啟用裝置控制 (請參閱[啟用或停用裝置控制的步驟](#))。
2. 按一下 **[裝置控制]** 開關旁的箭頭圖示以展開設定, 然後按一下 **[存取設定]** 旁的連結。
3. 在出現的[管理存取設定](#)頁面上, 視需要檢視或變更存取設定。

啟用或停用作業系統通知和服務警示

管理存取設定時, 您可以啟用或停用 **[作業系統通知和服務警示]**, 告知使用者嘗試執行不允許的動作。

啟用或停用作業系統通知

1. 依照[檢視或變更存取設定的步驟](#)進行。
2. 在[管理存取設定的頁面上](#)，選取或清除 **[當終端使用者嘗試使用封鎖的裝置類型或連接埠時，向其顯示作業系統通知]** 核取方塊。

啟用或停用服務警示

1. 依照[檢視或變更存取設定的步驟](#)進行。
2. 在[管理存取設定的頁面上](#)，為所需的裝置類型選取或清除 **[顯示警示]** 核取方塊。

[顯示警示] 核取方塊僅適用於存取權有限 (唯讀或拒絕存取) 的裝置類型，但螢幕擷取畫面擷取除外。

26.1.4 從存取控制排除裝置子類別

您可以從保護計劃面板選擇要從存取控制排除的裝置子類別。結果，無論裝置控制存取設定為何，都允許存取這些裝置。

從存取控制排除裝置子類別

1. 開啟保護計劃的保護計劃面板，然後在該計劃中啟用裝置控制 (請參閱[啟用或停用裝置控制的步驟](#))。
2. 按一下 **[裝置控制]** 開關旁的箭頭圖示以展開設定，然後按一下 **[裝置類型允許名單]** 旁的連結。
3. 在出現的[管理允許名單頁面上](#)，檢視或變更要從存取控制排除的裝置子類別選項。

26.1.5 從存取控制排除個別 USB 裝置

在保護計劃面板上，您可以指定要從存取控制排除的個別 USB 裝置或 USB 裝置型號。結果，無論裝置控制存取設定為何，都允許存取這些裝置。

從存取控制排除 USB 裝置

1. 開啟保護計劃的保護計劃面板，然後在該計劃中啟用裝置控制 (請參閱[啟用或停用裝置控制的步驟](#))。
2. 按一下 **[裝置控制]** 開關旁的箭頭圖示以展開設定，然後按一下 **[USB 裝置允許名單]** 旁的連結。
3. 在出現的[管理允許名單頁面上](#)，按一下 **[從資料庫新增]**。
4. 在出現的[選取 USB 裝置頁面上](#)，從透過 [USB 裝置資料庫](#) 登錄的裝置，選擇所需的裝置。
5. 按一下 **[新增至允許名單]** 按鈕。

停止從存取控制排除 USB 裝置

1. 開啟保護計劃的保護計劃面板，然後在該計劃中啟用裝置控制 (請參閱[啟用或停用裝置控制的步驟](#))。
2. 按一下 **[裝置控制]** 開關旁的箭頭圖示以展開設定，然後按一下 **[USB 裝置允許名單]** 旁的連結。
3. 在出現的[管理允許名單頁面上](#)，按一下代表所需 USB 裝置的清單項目尾端的刪除圖示。

從資料庫新增或移除 USB 裝置

若要從存取控制排除特定 USB 裝置，您需要將其新增至 [USB 裝置資料庫](#)。接著，您可以透過從該資料庫中選擇，將裝置新增至允許名單。

下列程序適用於已啟用裝置控制功能的保護計劃。

將 USB 裝置新增至資料庫

1. 開啟裝置的保護計劃進行編輯：
按一下保護計劃名稱旁的省略符號 (...), 然後選擇 **[編輯]**。

注意事項

計劃中必須啟用裝置控制, 您才可以存取裝置控制設定。

2. 按一下 **[裝置控制]** 開關旁的箭頭圖示以展開設定, 然後按一下 **[USB 裝置允許名單]** 旁的連結。
3. 在出現的 **[USB 裝置允許名單]** 頁面上, 按一下 **[從資料庫新增]**。
4. 在出現的 USB 裝置資料庫管理頁面上, 按一下 **[新增至資料庫]**。
5. 在出現的 **[新增 USB 裝置]** 對話方塊中, 按一下連接 USB 裝置的電腦。
只有連線的電腦會顯示在電腦清單中。
系統僅會針對已安裝資料洩漏防禦用代理程式的電腦, 顯示 USB 裝置的清單。
USB 裝置列在樹狀目錄檢視中。樹狀目錄的第一層表示裝置型號。第二層則表示該行號的特定裝置。
裝置描述旁的藍色圖示表示裝置目前連接至電腦。如果裝置未連接至該電腦, 圖示會呈現灰色。
6. 選擇要新增至資料庫的 USB 裝置的核取方塊, 然後按一下 **[新增至資料庫]**。
選擇的 USB 裝置隨即新增至資料庫。
7. 關閉或儲存保護計劃。

將 USB 裝置從電腦詳細資料面板新增至資料庫

注意事項

此程序僅適用於已連線且其上已安裝資料洩漏防禦用代理程式的裝置。您無法針對離線或未安裝資料洩漏防禦代理程式的電腦, 檢視 USB 裝置的清單。

1. 在服務主控台中, 移至 **[裝置] > [所有裝置]**。
2. 選擇已連接所需 USB 裝置的電腦, 然後在右側的功能表中, 按一下 **[清查]**。
電腦詳細資料面板隨即開啟。
3. 在電腦詳細資料面板上, 按一下 **[USB 裝置]** 索引標籤。
所選電腦上已知 USB 裝置的清單隨即開啟。
USB 裝置列在樹狀目錄檢視中。樹狀目錄的第一層表示裝置型號。第二層則表示該行號的特定裝置。
裝置描述旁的藍色圖示表示裝置目前連接至電腦。如果裝置未連接至該電腦, 圖示會呈現灰色。
4. 選擇要新增至資料庫的 USB 裝置的核取方塊, 然後按一下 **[新增至資料庫]**。

將 USB 裝置從服務警示新增至資料庫

1. 在服務主控台中, 移至 **[監控] > [警示]**。
2. 找出裝置控制警示, 其會告知拒絕存取 USB 裝置。

3. 在警示的簡易檢視中, 按一下 **[允許此 USB 裝置]**。

如此會從存取控制排除 USB 裝置, 並將其新增至資料庫, 以供進一步參考。

透過將裝置清單匯入至資料庫來新增 USB 裝置

您可以將包含 USB 裝置清單的 JSON 檔案匯入至資料庫。請參閱 "將 USB 裝置的清單匯入至資料庫" (第 504 頁)。

從資料庫移除 USB 裝置

1. 開啟裝置的保護計劃進行編輯：

按一下保護計劃名稱旁的省略符號 (...), 然後選擇 **[編輯]**。

注意事項

計劃中必須啟用裝置控制, 您才可以存取裝置控制設定。

2. 按一下 **[裝置控制]** 開關旁的箭頭以展開設定, 然後按一下 **[USB 裝置允許名單]** 列。
3. 在出現的**管理允許名單**頁面上, 按一下 **[從資料庫新增]**。
4. 在**從資料庫選取 USB 裝置**的頁面上, 按一下代表裝置之清單項目尾端的省略符號 (...), 按一下 **[刪除]**, 然後確認刪除。
USB 裝置隨即從資料庫刪除。
5. 關閉或儲存保護計劃。

26.1.6 檢視裝置控制警示

裝置控制模組可以設定為引發警示, 告知拒絕使用者嘗試使用特定裝置類型 (請參閱**啟用或停用作業系統通知和服務警示**)。使用下列步驟, 檢視這些警示。

檢視裝置控制警示

1. 在服務主控台中, 移至 **[監控] > [警示]**。
2. 尋找具有下列狀態的警示:「週邊裝置存取遭到封鎖」。

如需進一步的詳細資料, 請參閱**裝置控制警示**。

26.2 存取設定

在 **[存取設定]** 頁面上, 您可以允許或拒絕存取特定類型的裝置, 以及啟用或停用作業系統通知和裝置控制警示。

存取設定可讓您限制使用者對下列裝置類型和連接埠的存取：

- **卸除式** (依裝置類型的存取控制) - 具有任何介面的裝置, 這些介面可連接至作業系統視為卸除式儲存裝置 (例如, USB 隨身碟、讀卡機、電磁光碟機等) 的電腦 (USB、FireWire、PCMCIA、IDE、SATA、SCSI 等)。裝置控制可將透過 USB、FireWire 和 PCMCIA 連接的所有硬碟機分類為卸除式裝置。如果某些硬碟機 (通常具有 SATA 和 SCSI) 支援熱插拔功能, 而且其上未安裝執行中的作業系統, 則裝置控制也會將這些硬碟機分類為卸除式裝置。

您可以對卸除式裝置允許完整存取、唯讀存取，或拒絕存取，從而控制將資料複製到受保護電腦上的任何卸除式裝置，或從受保護電腦上的任何卸除式裝置複製資料的作業。存取權限不會影響使用 BitLocker 或 FileVault 加密的裝置 (僅限 HFS+ 檔案系統)。

Windows 和 macOS 都支援此裝置類型。

- **加密的卸除式裝置** (依裝置類型的存取控制) - 使用 BitLocker (在 Windows 上) 或 FileVault (在 macOS 上) 磁碟機加密來加密的卸除式裝置。

在 macOS 上，僅支援使用 HFS+ (亦稱為 HFS Plus 或 Mac OS Extended, 或 HFS Extended) 檔案系統的已加密卸除式磁碟機。使用 APFS 檔案系統的已加密卸除式裝置會被視為卸除式磁碟機。

您可以對加密的卸除式裝置允許完整存取、唯讀存取，或拒絕存取，從而控制將資料複製到受保護電腦上的任何加密的卸除式裝置，或從受保護電腦上的任何加密的卸除式裝置複製資料的作業。存取權限僅會影響使用 BitLocker 或 FileVault 加密的裝置 (僅限 HFS+ 檔案系統)。

Windows 和 macOS 都支援此裝置類型。

- **印表機** (依裝置類型的存取控制) - 具有可連接至電腦 (USB、LPT、藍牙等) 之任何介面的實體印表機，以及從網路上的電腦存取的印表機。

您可以允許或拒絕存取印表機，從而控制在受保護電腦的任何印表機上列印文件。

注意事項

當您將印表機的存取設定變更為 **[拒絕]** 時，必須重新啟動存取印表機的應用程式和程序，才能強制執行新設定的存取設定。為確保已正確強制執行存取設定，請重新啟動受保護的工作負載。

僅 Windows 支援此裝置類型。

- **剪貼簿** (依裝置類型的存取控制) - Windows 剪貼簿。

您可以允許或拒絕存取剪貼簿，從而控制透過受保護電腦上 Windows 剪貼簿的複製和貼上作業。

注意事項

當您將剪貼簿的存取設定變更為 **[拒絕]** 時，必須重新啟動存取剪貼簿的應用程式和程序，才能強制執行新設定的存取設定。為確保已正確強制執行存取設定，請重新啟動受保護的工作負載。

僅 Windows 支援此裝置類型。

- **螢幕擷取畫面擷取** (依裝置類型的存取控制) - 可擷取整個畫面、作用中視窗或畫面所選部分的螢幕擷取畫面。

您可以允許或拒絕存取螢幕擷取畫面擷取，從而控制受保護電腦上的螢幕擷取畫面擷取。

注意事項

當您將螢幕擷取畫面擷取的存取設定變更為 **[拒絕]** 時，必須重新啟動存取螢幕擷取畫面擷取的應用程式和程序，才能強制執行新設定的存取設定。為確保已正確強制執行存取設定，請重新啟動受保護的工作負載。

僅 Windows 支援此裝置類型。

- **行動裝置** (依裝置類型的存取控制) - 透過媒體傳輸通訊協定 (MTP) 通訊，且具有用於連接至電腦 (USB、IP、藍牙) 的任何介面的裝置 (例如，Android 智慧手機等)。

您可以對行動裝置允許完整存取、允許唯讀存取，或拒絕存取，從而控制將資料複製到受保護電腦上的任何 MTP 型行動裝置，或從受保護電腦上的任何 MTP 型行動裝置複製資料的作業。

注意事項

當您將行動裝置的存取設定變更為 **[唯讀]** 或 **[拒絕]** 時，必須重新啟動存取行動裝置的應用程式和程序，才能強制執行新設定的存取設定。為確保已正確強制執行存取設定，請重新啟動受保護的工作負載。

僅 Windows 支援此裝置類型。

- **藍牙** (依裝置類型的存取控制) - 具有連接至電腦 (USB、PCMCIA 等) 的任何介面的外接式和內建式藍牙裝置。這個設定可控制此類型裝置的使用，而不是控制使用這類裝置交換資料。

您可以允許或拒絕存取藍牙，從而控制在受保護的電腦上使用任何藍牙裝置。

注意事項

在 macOS 上，藍牙的存取權限不會影響藍牙 HID 裝置。系統一律允許對這些裝置的存取，以防在 iMac 和 Mac Pro 硬體上停用無線 HID 裝置 (滑鼠和鍵盤)。

Windows 和 macOS 都支援此裝置類型。

- **光碟機** (依裝置類型的存取控制) - 具有連接至電腦 (IDE、SATA、USB、FireWire、PCMCIA 等) 的任何介面的外接式和內建式 CD/DVD/BD 光碟機 (包括編寫器)。

您可以對光碟機允許完整存取、允許唯讀存取，或拒絕存取，從而控制將資料複製到受保護電腦上的任何光碟機，或從受保護電腦上的任何光碟機複製資料的作業。

Windows 和 macOS 都支援此裝置類型。

- **軟碟機** (依裝置類型的存取控制) - 具有連接至電腦 (IDE、USB、PCMCIA 等) 的任何介面的外接式和內建式軟碟機。作業系統會將某些軟碟機型號視為卸除式磁碟機，在此情況下，裝置控制也會將這些磁碟機視為卸除式裝置。

您可以對軟碟機允許完整存取、允許唯讀存取，或拒絕存取，從而控制將資料複製到受保護電腦上的任何軟碟機，或從受保護電腦上的任何軟碟機複製資料的作業。

僅 Windows 支援此裝置類型。

- **USB** (依裝置介面的存取控制) - 連接至 USB 連接埠的任何裝置，但集線器除外。

您可以對 USB 連接埠允許完整存取、允許唯讀存取，或拒絕存取，從而控制將資料複製到受保護電腦上連接到任何 USB 連接埠的裝置，或從受保護電腦上連接到任何 USB 連接埠的裝置複製資料的作業。

Windows 和 macOS 都支援此裝置類型。

- **FireWire** (依裝置介面的存取控制) - 連接至 FireWire (IEEE 1394) 連接埠的任何裝置，但集線器除外。

您可以對 FireWire 連接埠允許完整存取、允許唯讀存取，或拒絕存取，從而控制將資料複製到受保護電腦上連接到任何 FireWire 連接埠的裝置，或從受保護電腦上連接到任何 FireWire 連接埠的裝置複製資料的作業。

Windows 和 macOS 都支援此裝置類型。

- **重新導向的裝置** (依裝置介面的存取控制) - 重新導向至虛擬應用程式/桌面工作階段的對應磁碟機 (硬碟機、卸除式磁碟機、光碟機)、USB 裝置以及剪貼簿。

裝置控制在受保護 Windows 電腦上託管的 Microsoft RDS、Citrix XenDesktop、Citrix XenApp、Citrix XenServer 和 VMware Horizon 虛擬化環境中，可識別透過 Microsoft RDP、Citrix ICA、VMware PCoIP 和 HTML5/WebSocket 遠端通訊協定重新導向的裝置。它也可以控制在 VMware Workstation、VMware Player、Oracle VM VirtualBox 或 Windows Virtual PC 上執行之客體作業系統的 Windows 剪貼簿，以及在受保護 Windows 電腦上執行之主機作業系統的剪貼簿之間的資料複製作業。

僅 Windows 支援此裝置類型。

您可以設定對重新導向裝置的存取，如下所示：

- **對應磁碟機** - 允許完整存取、允許唯讀存取或拒絕存取，從而控制將資料複製到重新導向至受保護電腦上託管之工作階段的任何硬碟機、卸除式磁碟機或光碟機，或從重新導向至受保護電腦上託管之工作階段的任何硬碟機、卸除式磁碟機或光碟機複製資料的作業。
- **剪貼簿傳入** - 允許或拒絕存取，從而控制透過剪貼簿，將資料複製到受保護電腦上託管的工作階段的作業。

注意事項

當您將剪貼簿傳入的存取設定變更為 **[拒絕]** 時，必須重新啟動存取剪貼簿的應用程式和程序，才能強制執行新設定的存取設定。為確保已正確強制執行存取設定，請重新啟動受保護的工作負載。

- **剪貼簿傳出** - 允許或拒絕存取，從而控制透過剪貼簿，從受保護電腦上託管的工作階段複製資料的作業。

注意事項

當您將剪貼簿傳出的存取設定變更為 **[拒絕]** 時，必須重新啟動存取剪貼簿的應用程式和程序，才能強制執行新設定的存取設定。為確保已正確強制執行存取設定，請重新啟動受保護的工作負載。

- **USB 連接埠** - 允許或拒絕存取，從而控制將資料複製到連接至任何 USB 連接埠 (重新導向至受保護電腦上託管的工作階段) 的裝置，或從連接至任何 USB 連接埠 (重新導向至受保護電腦上託管的工作階段) 的裝置複製資料的作業。

裝置控制設定會同樣地影響所有使用者。例如，如果您拒絕存取卸除式裝置，您會防止任何使用者將資料複製到受保護電腦上的這類裝置，以及從受保護電腦上的這類裝置複製資料。您可以從存取控制排除個別的 USB 裝置，以選擇性地允許存取個別的 USB 裝置 (請參閱[裝置類型允許名單](#)和[USB 裝置允許名單](#))。

對裝置的存取同時受到其類型和介面的控制時，在介面層級拒絕存取優先。例如，如果拒絕存取 USB 連接埠 (裝置介面)，則無論允許還是拒絕存取行動裝置 (裝置類型)，都會拒絕存取連接至 USB 連接埠的行動裝置。若要允許存取這種裝置，您必須同時允許其介面和類型。

注意事項

如果在 macOS 上使用的保護計劃的設定適用於僅在 Windows 上受支援的裝置類型，則在 macOS 上將忽略這些裝置類型的設定。

重要事項

當卸除式裝置、加密的卸除式裝置、印表機或藍牙裝置連接至 USB 連接埠時，允許存取該裝置將優先於在 USB 介面層級設定的拒絕存取。如果您允許這種裝置類型，則無論是否拒絕存取 USB 連接埠，都允許存取裝置。

26.2.1 作業系統通知和服務警示

您可以設定裝置控制在終端使用者嘗試在受保護的電腦上使用封鎖的裝置類型時，向其顯示作業系統通知。如果在存取設定中選取 **【當終端使用者嘗試使用封鎖的裝置類型或連接埠時，向其顯示作業系統通知】** 核取方塊，代理程式會在發生下列任何事件時，在受保護電腦的通知區域中顯示快顯訊息：

- 拒絕嘗試使用 USB 或 FireWire 連接埠上的裝置。每當使用者插入在介面層級 (例如，拒絕存取 USB 連接埠時) 或在類型層級 (例如，拒絕使用卸除式裝置時) 拒絕的 USB 或 FireWire 裝置時，就會出現這個通知。此通知會告知不允許使用者存取指定的裝置/磁碟機。
- 拒絕嘗試從特定裝置複製資料物件 (例如檔案)。拒絕對下列裝置進行讀取存取時，將會出現這個通知：軟碟機、光碟機、卸除式裝置、加密的卸除式裝置、行動裝置、重新導向的對應磁碟機，以及重新導向的剪貼簿傳入資料。此通知會告知不允許使用者從指定的裝置取得指定的資料物件。

拒絕對藍牙、FireWire 連接埠、USB 連接埠以及重新導向的 USB 連接埠進行讀取/寫入存取時，也會顯示拒絕讀取通知。

- 拒絕嘗試將資料物件 (例如檔案) 複製到特定裝置。拒絕對下列裝置進行寫入存取時，將會出現這個通知：軟碟機、光碟機、卸除式裝置、加密的卸除式裝置、行動裝置、本機剪貼簿、螢幕擷取畫面擷取、印表機、重新導向的對應磁碟機，以及重新導向的剪貼簿傳出資料。此通知會告知不允許使用者將指定的資料物件傳送到指定的裝置。

使用者嘗試在受保護的電腦上存取封鎖的裝置類型可能會引發在服務主控台中記錄的警示。在存取設定中選取 **【顯示警示】** 核取方塊可以分別為每個裝置類型 (螢幕擷取畫面擷取除外) 或連接埠啟用警示。例如，如果對卸除式裝置的存取限制為唯讀，且已針對該裝置類型選取 **【顯示警示】** 核取方塊，則每次使用者在受保護的電腦上嘗試將資料複製到卸除式裝置時，就會記錄一個警示。如需進一步的詳細資料，請參閱[裝置控制警示](#)。

另請參閱[啟用或停用作業系統通知和服務警示的步驟](#)。

26.3 裝置類型允許名單

在 **【裝置類型允許名單】** 頁面上，您可以選擇要從裝置存取控制排除的裝置子類別。結果，無論裝置控制模組中的存取設定為何，都允許存取這些裝置。

裝置控制模組可以讓您選擇允許存取拒絕的裝置類型中某些子類別的裝置。此選項可讓您拒絕某個特定類型的所有裝置，但此類型裝置的某些子類別除外。這可能非常實用，例如，當您需要拒絕存取所有 USB 連接埠，同時允許使用 USB 鍵盤和滑鼠時。

設定裝置控制模組時，您可以指定要從裝置存取控制排除的裝置子類別。當某個裝置屬於排除的子類別時，無論是否拒絕該裝置類型或連接埠，都允許存取該裝置。您可以從裝置存取控制，選擇性地排除下列裝置子類別：

- **USB HID (滑鼠、鍵盤等)** - 選取時，即使拒絕 USB 連接埠，也允許存取連接到 USB 連接埠的人性化介面裝置 (滑鼠、鍵盤等等)。預設會選取此項目，因此，拒絕存取 USB 連接埠並不會停用鍵盤或滑鼠。
支援 Windows 和 macOS。
- **USB 和 FireWire 網路卡** - 選取時，即使拒絕 USB 連接埠和/或 FireWire 連接埠，也允許存取連接到 USB 或 FireWire (IEEE 1394) 連接埠的網路卡。
支援 Windows 和 macOS。
- **USB 掃描器和靜止影像裝置** - 選取時，即使拒絕 USB 連接埠，也允許存取連接到 USB 連接埠的掃描器和靜止影像裝置。
僅支援 Windows。
- **USB 音訊裝置** - 選取時，即使拒絕 USB 連接埠，也允許存取連接到 USB 連接埠的音訊裝置，例如耳機和麥克風。
僅支援 Windows。
- **USB 攝影機** - 選取時，即使拒絕 USB 連接埠，也允許存取連接到 USB 連接埠的網路攝影機。
僅支援 Windows。
- **藍牙 HID (滑鼠、鍵盤等)** - 選取時，即使拒絕藍牙，也允許存取透過藍牙連接的人性化介面裝置 (滑鼠、鍵盤等等)。
僅支援 Windows。
- **應用程式內的剪貼簿複製/貼上** - 選取時，即使拒絕剪貼簿，也允許透過相同應用程式中的剪貼簿複製/貼上資料。
僅支援 Windows。

注意事項

如果在已套用的保護計劃中設定這些設定，就會忽略不支援裝置子類別的設定。

將裝置類型加入允許名單時，請考慮以下情況：

- 您僅能透過裝置類型允許名單，允許整個裝置子類別。您無法在允許某個特定裝置型號的同時，拒絕其他所有相同子類別的裝置。例如，您可以透過從裝置存取控制排除 USB 攝影機，允許使用任何型號和廠商的 USB 攝影機。關於如何允許個別的裝置/型號，請參閱 [USB 裝置允許名單](#)。
- 您只能從裝置子類別的封閉式清單中選擇裝置類型。如果允許的裝置屬於不同的子類別，則無法透過使用裝置類型允許名單來允許該裝置。例如，USB 智慧卡讀取機之類的子類別無法新增到允許名單。若要在拒絕 USB 連接埠時允許 USB 智慧卡讀取機，請依照 [USB 裝置允許名單](#) 中的指示進行。
- 裝置類型允許名單僅適用於使用標準 Windows 驅動程式的裝置。裝置控制可能無法辨識部分具有專屬驅動程式之 USB 裝置的子類別。因此，您無法使用裝置類型允許名單，允許對此類 USB 裝置的存取。在此情況下，您可以根據裝置/型號，允許存取 (請參閱 [USB 裝置允許名單](#))。

26.4 USB 裝置允許名單

允許名單旨在允許使用特定 USB 裝置，而與其他任何裝置控制設定無關。您可以將個別的裝置或裝置型號新增至允許名單，以停用這些裝置的存取控制。例如，如果您將擁有唯一 ID 的行動裝置新增至允許名單，表示即使拒絕其他任何 USB 裝置，您也允許使用該特定裝置。

在 **[USB 裝置允許名單]** 頁面上，您可以指定要從裝置存取控制排除的個別 USB 裝置或 USB 裝置型號。結果，無論裝置控制模組中的存取設定為何，都允許存取這些裝置。

識別允許名單中的裝置有兩種方法：

- **裝置型號** - 共同識別特定型號的所有裝置。每個裝置型號都以廠商 ID (VID) 和產品 ID (PID) 識別，例如 USB\VID_0FCE&PID_E19E。

這個 VID 和 PID 組合無法識別特定裝置，但是可以識別整個裝置型號。您可以透過將裝置型號新增到允許名單，允許對該型號任何裝置的存取。例如，如此一來，您可以允許使用特定型號的 USB 印表機。

- **唯一的裝置** - 識別特定的裝置。每個唯一的裝置都以廠商 ID (VID)、產品 ID (PID) 以及序號識別，例如 USB\VID_0FCE&PID_E19E\D55E7FCA。

並非所有 USB 裝置都有獲指派序號。您只有裝置有在生產期間獲指派序號時，才可以將裝置以序號新增至允許名單。例如，擁有唯一序號的 USB 隨身碟。

若要將裝置新增至允許名單，您必須先將其新增至 [USB 裝置資料庫](#)。接著，您可以透過從該資料庫中選擇，將裝置新增至允許名單。

允許名單是在稱為 **USB 裝置允許名單** 的個別設定頁面上管理的。清單中的每個項目都代表一個裝置或裝置型號，而且包含下列欄位：

- **描述** - 作業系統會在連接 USB 裝置時，指定特定的描述。您可以在 USB 裝置資料庫中修改裝置的描述 (請參閱 [USB 資料庫管理頁面](#))。
- **裝置類型** - 如果清單項目代表唯一的裝置，請顯示 [唯一]；如果代表裝置型號，則顯示 [型號]。
- **唯讀** - 選取時，僅允許從裝置接收資料。如果裝置不支援唯讀存取，則對裝置的存取會遭到封鎖。清除此核取方塊可允許對裝置的完整存取。
- **重新初始化** - 選取時，會使裝置模擬在新使用者登入時中斷連接/重新連接。部分 USB 裝置 (滑鼠、鍵盤等等) 需要重新初始化才能運作，因此建議為這類裝置選取此核取方塊。同時建議為資料儲存裝置 (USB 隨身碟、光碟機、外接式硬碟機等等) 清除此核取方塊。
裝置控制可能無法重新初始化部分具有專屬驅動程式的 USB 裝置。如果無法存取此種裝置，您必須從 USB 連接埠移除 USB 裝置，然後再將其插回。

注意事項

[重新初始化] 欄位預設為隱藏狀態。若要在表格中顯示此欄，按一下表格右上角的齒輪圖示，然後選擇 **[重新初始化]** 核取方塊。

注意事項

在 macOS 上，不支援 **[唯讀]** 和 **[重新初始化]** 欄位。如果在已套用的保護計劃中設定這些欄位，將會遭到忽略。

您可以從允許名單中新增或移除裝置/型號，如下所示：

- 按一下清單上方的 **[從資料庫新增]**，然後從透過 [USB 裝置資料庫](#) 登錄的裝置，選擇所需的裝置。所選裝置會新增至清單，您可以在其中進行設定並確認變更。
- 按一下警示中的 **[允許此 USB 裝置]**，告知拒絕存取 USB 裝置 (請參閱[裝置控制警示](#))。如此會將裝置新增至允許名單以及 USB 裝置資料庫。
- 按一下清單項目尾端的刪除圖示。如此會從允許名單中移除個別的裝置/型號。

26.4.1 USB 裝置資料庫

裝置控制模組會維護 USB 裝置的資料庫，您可以從該資料庫中，將裝置新增到排除清單 (請參閱[USB 裝置允許名單](#))。使用下列任何一種方式，都可以向資料庫登錄 USB 裝置：

- 在將裝置新增至排除清單時出現的頁面上新增裝置 (請參閱[USB 裝置資料庫管理頁面](#))。
- 在服務主控台中，從電腦 [清查] 窗格的 [USB 裝置] 索引標籤新增裝置 (請參閱[電腦上的 USB 裝置清單](#))。
- 從拒絕存取 USB 裝置的警示允許裝置 (請參閱[裝置控制警示](#))。

另請參閱[從資料庫新增或移除 USB 裝置的步驟](#)。

USB 裝置資料庫管理頁面

設定 USB 裝置的允許名單時，您可以選擇從資料庫新增裝置。如果您選擇此選項，將會出現管理頁面以及裝置清單。在此頁面上，您可以檢視向資料庫登錄的所有裝置的清單、您可以選擇要新增到允許名單的裝置，並執行下列作業：

向資料庫登錄裝置

1. 按一下頁面頂端的 **[新增至資料庫]**。
2. 在出現的 **[新增 USB 裝置]** 對話方塊中，選擇連接 USB 裝置的電腦。
只有連線的電腦會顯示在電腦清單中。
系統僅會針對已安裝資料洩漏防禦用代理程式的電腦，顯示 USB 裝置的清單。
USB 裝置列在樹狀目錄檢視中。樹狀目錄的第一層表示裝置型號。第二層則表示該行號的特定裝置。
裝置描述旁的藍色圖示表示裝置目前連接至電腦。如果裝置未連接至該電腦，圖示會呈現灰色。
3. 選擇要登錄的 USB 裝置的核取方塊，然後按一下 **[新增至資料庫]**。

變更裝置的描述

1. 在 **[USB 裝置資料庫]** 頁面上，按一下代表裝置之清單項目尾端的省略符號 (...), 然後按一下 **[編輯]**。
2. 在出現的對話方塊中，對描述進行變更。

從資料庫移除裝置

1. 按一下代表裝置之清單項目尾端的省略符號 (...).
2. 按一下 **[刪除]**，並確認刪除。

針對每個裝置，頁面上的清單都會提供下列資訊：

- **描述** - 裝置可讀取的識別碼。您可以視需要變更描述。
- **裝置類型** - 如果清單項目代表唯一的裝置，請顯示 [唯一]；如果代表裝置型號，則顯示 [型號]。唯一的裝置必須具備序號以及廠商 ID (VID) 和產品 ID (PID)，其中裝置型號是以 VID 和 PID 的組合識別。
- **廠商 ID、產品 ID、序號** - 這些值共同組成裝置 ID，其格式為 USB\VID_<廠商 ID>&PID_<產品 ID>\<序號>。
- **帳戶** - 指出此裝置所屬的租用戶。此租用戶包含向資料庫登錄裝置所使用的使用者帳戶。

注意事項

此欄預設為隱藏狀態。若要在表格中顯示此欄，按一下表格右上角的齒輪圖示，然後選擇 **[帳戶]**。

最左側的欄用於選擇要新增至允許名單的裝置：選擇要新增的每個裝置的核取方塊，然後按一下 **[新增至允許名單]** 按鈕。若要選擇或清除所有核取方塊，按一下欄標頭中的核取方塊。

您可以搜尋或篩選裝置清單：

- 按一下頁面頂端的 **[搜尋]**，然後輸入一個搜尋字串。此清單會顯示其描述符合所輸入字串的裝置。
- 按一下 **[篩選]**，然後在出現的對話方塊中，設定並套用篩選。此清單限制為包含您在設定篩選時所選擇之類型、廠商 ID、產品 ID 和帳戶的裝置。若要取消篩選並列出所有裝置，按一下 **[重設為預設值]**。

匯出資料庫中的 USB 裝置清單

您可以匯出新增至資料庫的 USB 裝置的清單。

1. 開啟裝置的保護計劃進行編輯。
2. 按一下 **[裝置控制]** 開關旁的箭頭圖示以展開設定，然後按一下 **[USB 裝置允許名單]** 列。
3. 在 [USB 裝置允許名單] 頁面上，按一下 **[從資料庫新增]**。
4. 在出現的 USB 裝置資料庫管理頁面上，按一下 **[匯出]**。
標準的 [瀏覽] 對話方塊隨即開啟。
5. 選擇您要儲存檔案的位置、輸入新的檔案名稱 (如有需要)，然後按一下 **[儲存]**。

USB 裝置的清單隨即匯出至 JSON 檔案。

您可以編輯所產生的 JSON 檔案，以便從中新增或移除裝置，並對裝置描述進行大量變更。

將 USB 裝置的清單匯入至資料庫

您可以匯入 USB 裝置的清單，而不必從服務主控台使用者介面新增 USB 裝置。此清單是一個 JSON 格式的檔案。

注意事項

您可以將 JSON 檔案匯入至不包含檔案中所述之裝置的資料庫。若要將修改過的檔案匯入至從中匯出該檔案的資料庫，您必須先清理資料庫，因為您無法匯入重複的項目。如果您匯出 USB 裝置的清單並加以修改，然後嘗試在不清理的情況下匯入至相同的資料庫，匯入將會失敗。

1. 開啟裝置的保護計劃進行編輯。
2. 按一下 **[裝置控制]** 開關旁的箭頭圖示以展開設定，然後按一下 **[USB 裝置允許名單]** 列。
3. 在 **[USB 裝置允許名單]** 頁面上，按一下 **[從資料庫新增]**。
4. 在出現的 USB 裝置資料庫管理頁面上，按一下 **[匯入]**。
[從檔案匯入 USB 裝置] 對話方塊隨即開啟。
5. 使用拖放方式或瀏覽您要匯入的檔案。

服務主控台會檢查清單中是否包含已存在於資料庫的重複項目，並略過這些項目。在資料庫中找不到的 USB 裝置則會附加到該資料庫中。

電腦上的 USB 裝置清單

在服務主控台中，電腦的 **[清查]** 面板包含 **[USB 裝置]** 索引標籤。如果電腦已連線且其上已安裝資料洩漏防禦用代理程式，則 **[USB 裝置]** 索引標籤會顯示曾經連接至該電腦的所有 USB 裝置的清單。

USB 裝置列在樹狀目錄檢視中。樹狀目錄的第一層表示裝置型號。第二層則表示該行號的特定裝置。

針對每個裝置，清單都會提供下列資訊：

- **描述** - 作業系統會在連接 USB 裝置時指派描述。此描述可以作為裝置可讀取的識別碼。
裝置描述旁的藍色圖示表示裝置目前連接至電腦。如果裝置未連接至該電腦，圖示會呈現灰色。
- **裝置 ID** - 作業系統指派給裝置的識別碼。此識別碼的格式如下：有下列格式：USB\VID_<廠商 ID>&PID_<產品 ID>\<序號>，其中 <序號> 是選擇性的。範例：USB\VID_0FCE&PID_ADDE\D55E7FCA (含序號的裝置)；USB\VID_0FCE&PID_ADDE (不含序號的裝置)。

若要將裝置新增至 USB 裝置資料庫，請選擇所需裝置的核取方塊，然後按一下 **[新增至資料庫]** 按鈕。

26.5 從存取控制排除程序

您可以透過插入程序的勾點，控制對 Windows 剪貼簿、螢幕擷取畫面擷取、印表機和行動裝置的存取。如果程序未遭到攔截，對這些裝置的存取將不會受到控制。

注意事項

在 macOS 上不支援從存取控制排除程序。如果在已套用的保護計劃中設定排除程序的清單，將會遭到忽略。

在 **[排除]** 頁面上，您可以指定將不會遭到攔截的程序的清單。也就是說，剪貼簿 (本機和重新導向的)、螢幕擷取畫面擷取、印表機和行動裝置存取控制將不會套用到這類程序。

例如，您套用拒絕存取印表機的保護計劃，然後啟動 Microsoft Word 應用程式。嘗試從此應用程式列印將會遭到封鎖。但是如果您將 Microsoft Word 程序新增至排除清單，則應用程式將不會遭到封鎖。因此，從 Microsoft Word 列印將不會遭到封鎖，但是從其他應用程式列印仍將遭到封鎖。

將程序新增至排除

1. 開啟裝置的保護計劃進行編輯：

按一下保護計劃名稱旁的省略符號 (...), 然後選擇 **[編輯]**。

注意事項

計劃中必須啟用裝置控制，您才可以存取裝置控制設定。

2. 按一下 **[裝置控制]** 開關旁的箭頭以展開設定，然後按一下 **[排除]** 列。
3. 在 **[排除]** 頁面上的 **[程序和資料夾]** 列中，按一下 **[+新增]**。
4. 新增您要從存取控制排除的程序。

例如，C:\Folder\subfolder\process.exe。

您可以使用萬用字元：

- * 可取代任意數目的字元。
- ? 可取代一個字元。

例如：

C:\Folder*

\Folder\SubFolder?

*\process.exe

5. 按一下核取標記，然後按一下 **[完成]**。
6. 在保護計劃中，按一下 **[儲存]**。
7. 重新啟動您排除的程序，以確保已正確移除勾點。

無論剪貼簿、螢幕擷取畫面擷取、印表機和行動裝置的存取設定為何，已排除的程序都可以存取這些裝置。

從排除移除程序

開啟裝置的保護計劃進行編輯：

按一下保護計劃名稱旁的省略符號 (...), 然後選擇 **[編輯]**。

注意事項

計劃中必須啟用裝置控制，您才可以存取裝置控制設定。

1. 按一下 **[裝置控制]** 開關旁的箭頭以展開設定，然後按一下 **[排除]** 列。
2. 在 **[排除]** 頁面上，按一下您要從排除移除的程序旁的垃圾桶圖示。
3. 按一下 **[完成]**。
4. 在保護計劃中，按一下 **[儲存]**。
5. 重新啟動程序，以確保已正確插入勾點。

保護計劃中的存取設定將會套用到您從排除移除的程序。

編輯排除中的程序

1. 開啟裝置的保護計劃進行編輯：

按一下保護計劃名稱旁的省略符號 (...), 然後選擇 **[編輯]**。

注意事項

計劃中必須啟用裝置控制, 您才可以存取裝置控制設定。

2. 按一下 **[裝置控制]** 開關旁的箭頭以展開設定, 然後按一下 **[排除]** 列。
3. 在 **[排除]** 頁面上, 按一下您要編輯的程序旁的 **[編輯]** 圖示。
4. 套用變更, 然後按一下核取標記確認。
5. 按一下**[完成]**。
6. 在保護計劃中, 按一下 **[儲存]**。
7. 重新啟動受影響的程序以確保正確套用您的變更。

26.6 裝置控制警示

裝置控制透過追蹤使用者對存取控制的裝置類型、連接埠或介面的嘗試, 維護事件記錄。部分事件可能會引發在服務主控台中記錄的警示。例如, 裝置控制模組可以設定為透過每次使用者嘗試將資料複製到此種裝置或從此種裝置複製資料時記錄的警示, 防止使用卸除式裝置。

設定裝置控制模組時, 您可以為列在裝置類型 (螢幕擷取畫面擷取除外) 或連接埠底下的大多數項目啟用警示。如果啟用警示, 每個使用者對執行不允許的作業的嘗試都會產生一個警示。例如, 如果對卸除式裝置的存取限制為唯讀, 且已針對該裝置類型選取 **[顯示警示]** 選項, 則每次使用者在受保護的電腦上嘗試將資料複製到卸除式裝置時, 就會產生一個警示。

若要檢視服務主控台中的警示, 請移至 **[監控] > [警示]**。在每個裝置控制警示中, 主控台都會針對個別事件提供下列資訊：

- **類型** - 警告。
- **狀態** - 顯示「週邊裝置存取遭到封鎖」。
- **訊息** - 顯示「存取『<電腦名稱>』上的『<裝置類型或連接埠>』遭到封鎖」。例如, 「存取 'accountant-pc' 上的 'Removable' 遭到封鎖」。
- **日期和時間** - 事件發生的日期和時間。
- **裝置** - 事件發生所在電腦的名稱。
- **計劃名稱** - 導致事件發生的保護計劃的名稱。
- **來源** - 事件涉及的裝置類型或連接埠。例如, 如果拒絕使用者嘗試存取卸除式裝置, 此欄位會顯示「卸除式裝置」。
- **動作** - 導致事件發生的操作。例如, 如果拒絕使用者嘗試將資料複製到裝置, 此欄位會顯示「寫入」。如需詳細資訊, 請參閱[動作欄位值](#)。
- **名稱** - 事件目標物件的名稱, 例如, 使用者嘗試複製的檔案, 或使用者嘗試使用的裝置。如果無法識別目標物件, 則不會顯示。
- **資訊** - 關於事件目標裝置的其他資訊, 例如 USB 裝置的裝置 ID。如果沒有關於目標裝置的其他資訊可用, 則不會顯示。

- **使用者** - 導致事件發生之使用者的名稱。
- **程序** - 導致事件發生之應用程式的可執行檔完整路徑。在某些情況下，可能會顯示程序名稱而非路徑。如果沒有可用的程序資訊，則不會顯示。

如果某個警示適用於 USB 裝置 (包括卸除式裝置和加密的卸除式裝置)，則系統管理員可以直接從警示中，將裝置新增到允許名單，如此可防止裝置控制模組限制對該特定裝置的存取。按一下 **[允許此 USB 裝置]** 可將其新增至裝置控制模組設定中的 USB 裝置允許名單，也會將其新增至 [\[USB 裝置資料庫\]](#) 以供進一步參考。

另請參閱[檢視裝置控制警示的步驟](#)。

26.6.1 動作欄位值

[警示動作] 欄位可以包含下列值：

- **讀取** - 從裝置或連接埠取得資料。
- **寫入** - 將資料傳送至裝置或連接埠。
- **格式化** - 直接存取 (格式化、檢查磁碟等) 裝置。若是連接埠，則適用於連接至該連接埠的裝置。
- **退出** - 從系統移除裝置，或從裝置退出媒體。若是連接埠，則適用於連接至該連接埠的裝置。
- **列印** - 將文件傳送到印表機。
- **複製音訊** - 透過本機剪貼簿複製/貼上音訊資料。
- **複製檔案** - 透過本機剪貼簿複製/貼上檔案。
- **複製影像** - 透過本機剪貼簿複製/貼上影像。
- **複製文字** - 透過本機剪貼簿複製/貼上文字。
- **複製未識別的內容** - 透過本機剪貼簿複製/貼上其他資料。
- **複製 RTF 資料 (影像)** - 使用 RTF 格式，透過本機剪貼簿複製/貼上影像。
- **複製 RTF 資料 (檔案)** - 使用 RTF 格式，透過本機剪貼簿複製/貼上檔案。
- **複製 RTF 資料 (文字、影像)** - 使用 RTF 格式，透過本機剪貼簿複製/貼上文字以及影像。
- **複製 RTF 資料 (文字、檔案)** - 使用 RTF 格式，透過本機剪貼簿複製/貼上文字以及檔案。
- **複製 RTF 資料 (影像、檔案)** - 使用 RTF 格式，透過本機剪貼簿複製/貼上影像以及檔案。
- **複製 RTF 資料 (文字、影像、檔案)** - 使用 RTF 格式，透過本機剪貼簿複製/貼上文字以及影像和檔案。
- **刪除** - 從裝置 (例如，卸除式裝置、行動裝置等等) 刪除資料。
- **裝置存取** - 存取特定裝置或連接埠 (例如，藍牙裝置、USB 連接埠等等)。
- **傳入音訊** - 透過重新導向的剪貼簿，將音訊資料從用戶端電腦複製/貼上到裝載的工作階段。
- **傳入檔案** - 透過重新導向的剪貼簿，將檔案從用戶端電腦複製/貼上到裝載的工作階段。
- **傳入影像** - 透過重新導向的剪貼簿，將影像從用戶端電腦複製/貼上到裝載的工作階段。
- **傳入文字** - 透過重新導向的剪貼簿，將文字從用戶端電腦複製/貼上到裝載的工作階段。
- **傳入未識別的內容** - 透過重新導向的剪貼簿，將其他資料從用戶端電腦複製/貼上到裝載的工作階段。
- **傳入 RTF 資料 (影像)** - 使用 RTF 格式，透過重新導向的剪貼簿，將影像從用戶端電腦複製/貼上到裝載的工作階段。

- **傳入 RTF 資料 (檔案)** - 使用 RTF 格式, 透過重新導向的剪貼簿, 將檔案從用戶端電腦複製/貼上到裝載的工作階段。
- **傳入 RTF 資料 (文字、影像)** - 使用 RTF 格式, 透過重新導向的剪貼簿, 將文字以及影像從用戶端電腦複製/貼上到裝載的工作階段。
- **傳入 RTF 資料 (文字、檔案)** - 使用 RTF 格式, 透過重新導向的剪貼簿, 將文字以及檔案從用戶端電腦複製/貼上到裝載的工作階段。
- **傳入 RTF 資料 (影像、檔案)** - 使用 RTF 格式, 透過重新導向的剪貼簿, 將影像以及檔案從用戶端電腦複製/貼上到裝載的工作階段。
- **傳入 RTF 資料 (文字、影像、檔案)** - 使用 RTF 格式, 透過重新導向的剪貼簿, 將文字以及影像和檔案從用戶端電腦複製/貼上到裝載的工作階段。
- **插入** - 連接 USB 裝置或 FireWire 裝置。
- **傳出音訊** - 透過重新導向的剪貼簿, 將音訊資料從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出檔案** - 透過重新導向的剪貼簿, 將檔案從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出影像** - 透過重新導向的剪貼簿, 將影像從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出文字** - 透過重新導向的剪貼簿, 將文字從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出未識別的內容** - 透過重新導向的剪貼簿, 將其他資料從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出 RTF 資料 (影像)** - 使用 RTF 格式, 透過重新導向的剪貼簿, 將影像從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出 RTF 資料 (檔案)** - 使用 RTF 格式, 透過重新導向的剪貼簿, 將檔案從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出 RTF 資料 (文字、影像)** - 使用 RTF 格式, 透過重新導向的剪貼簿, 將文字以及影像從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出 RTF 資料 (文字、檔案)** - 使用 RTF 格式, 透過重新導向的剪貼簿, 將文字以及檔案從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出 RTF 資料 (影像、檔案)** - 使用 RTF 格式, 透過重新導向的剪貼簿, 將影像以及檔案從裝載的工作階段複製/貼上到用戶端電腦。
- **傳出 RTF 資料 (文字、影像、檔案)** - 使用 RTF 格式, 透過重新導向的剪貼簿, 將文字以及影像和檔案從裝載的工作階段複製/貼上到用戶端電腦。
- **重新命名** - 將裝置 (例如, 卸除式裝置、行動裝置等等) 上的檔案重新命名。

27 [管理] 索引標籤

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以使用 **[管理]** 索引標籤來管理保護計劃和其他計劃。

[管理] 索引標籤的每個區段都包含特定類型的所有計劃。以下區段可用：

- 保護計劃
- 備份掃描
- 雲端應用程式備份
- 備份複寫
- 驗證
- 清理
- 轉換成 VM
- VM 複寫

若是保護計劃和 VM 複寫計劃，可以使用可點選的狀態列。它會顯示下列以顏色區分的狀態：

- OK (綠燈)
- 警告 (橘色)
- 錯誤 (紅色)
- 計劃執行中 (藍色)
- 計劃已停用 (灰色)

您可以按一下狀態列，查看計劃處於何種狀態以及在多少部電腦上。此清單中的每個狀態也可以點選。

27.1 保護計劃

若要建立保護計劃

1. 在服務主控台中，移至 **[管理] > [保護計劃]**。
2. 按一下 **[建立計劃]**。
3. 選擇您要保護的電腦。
4. 按一下 **[保護]**。您將會看到具有預設設定的保護計劃。
5. [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。
6. [選擇性] 若要啟用或停用計劃模組，按一下模組名稱旁邊的開關。
7. [選擇性] 若要設定模組參數，按一下保護計劃的對應區段。
8. 按一下 **[新增裝置]** 以選擇您要套用計劃的電腦。
9. 準備就緒後，按一下 **[建立]**。

結果，所選裝置將會使用保護計劃受到保護。

您可以使用保護計劃執行下列作業：

- 建立、檢視、編輯、複製、停用、啟用，以及刪除保護計劃
- 檢視與每個保護計劃相關的活動
- 檢視與每個保護計劃相關的警示
- 將計劃匯出至檔案
- 匯入先前匯出的計劃

27.2 雲端應用程式的備份計劃

[管理]>[雲端應用程式備份] 索引標千會顯示雲端對雲端備份計劃。這些計劃會透過在雲端執行的代理程式，備份在雲端執行的應用程式，並使用雲端儲存空間做為備份位置。

在本節中，您可以執行下列作業：

- 建立、檢視、執行、停止、編輯，以及刪除備份計劃
- 檢視與每個備份計劃相關的活動
- 檢視與每個備份計劃相關的警示

如需雲端應用程式備份的詳細資訊，請參閱：

- [保護 Microsoft 365 資料](#)
- [保護 Google Workspace 資料](#)

手動執行雲端對雲端備份

為防止中斷 Cyber Protection 服務，手動雲端對雲端備份執行的次數限制為每個 Microsoft 365 或 Google Workspace 組織每小時執行 10 次。達到此次數之後，會將允許的執行次數重設為每小時一次，然後每小時之後可以再額外執行一次 (例如，第 1 個小時，執行 10 次；第 2 個小時，執行 1 次；第 3 個小時，執行 2 次)，直到達到每小時總共執行 10 次為止。

無法手動執行套用至裝置 (信箱、磁碟機、網站) 群組或包含超過 10 個裝置的備份計劃。

27.3 備份掃描計劃

若要掃描備份中的惡意程式碼 (包括勒索軟體)，請建立備份掃描計劃。

27.3.1 限制

- 當您選擇要掃描的備份時，可以選擇包含連續資料保護 (CDP) 備份的備份集。但是，系統只會掃描這些備份集中的非 CDP 備份。如需有關 CDP 備份的詳細資訊，請參閱 "連續資料保護 (CDP)" (第 151 頁)。
- 當您對整部電腦執行安全復原時，您可以選擇包含 CDP 備份的備份集。但是，復原將不會使用 CDP 備份資料。若要復原此資料，請另外執行 **[檔案/資料夾]** 復原。

建立備份掃描計劃

1. 在服務主控台中，移至 **[管理]>[備份掃描]**。
2. 按一下 **[建立計劃]**。

3. 指定計劃的名稱以及下列參數：

- **掃描類型：**
 - **雲端** – 無法變更此選項。自動選擇的雲端代理程式將執行備份掃描。
- **要掃描的備份：**
 - **位置** – 選擇含有您要掃描之備份集的位置。
 - **備份** – 選擇您要掃描的備份集。
- **掃描：**
 - **惡意程式碼** – 無法變更此選項。此掃描會檢查選擇的備份集中是否有惡意程式碼 (包括勒索軟體)。
- **加密** – 若要掃描加密的備份集，請指定加密密碼。如果您選擇一個位置或多個備份集，而且指定的密碼與備份集不符，則會建立警示。
- **排程** – 無法變更此選項。在雲端儲存空間，掃描會自動開始。

4. 按一下 **[建立]**。

因此，您要建立備份掃描計劃，雲端代理程式就會掃描您指定的位置或備份集中是否有惡意程式碼。

27.4 脫離主機資料處理

複寫、驗證及套用保留規則通常同時由執行備份的代理程式負責。這會使執行此代理程式的機器產生額外負載，即使在備份過程完成後也是如此。

然而，您可以利用離線主機資料處理，為虛擬機器的複寫、驗證、清理及轉換建立單獨的計劃。這些單獨的計劃允許您：

- 選擇執行這些作業的其他代理程式
- 將這些作業安排在離峰時段，盡可能減少網路頻寬
- 如果您的計劃中沒有設定專用代理程式，則將這些作業移到工作時間以外

注意事項

此功能可在進階備份組取得，並為執行離線主機資料處理作業代理程式的機器要求伺服器配額。

離線主機的資料處理計劃根據安裝代理程式的作業系統時間設定 (包括時區) 執行。虛擬裝置的時區 (例如，VMware 代理程式或 Scale Computing HC3 代理程式) 也可以在其界面中進行設定。

27.4.1 備份複寫

注意事項

此功能可在進階備份組取得，並為執行離線主機資料處理作業代理程式的機器要求伺服器配額。

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	-	-

若要建立備份複寫計劃

1. 按一下 **[管理]>[備份複寫]**。
2. 按一下 **[建立計劃]**。
此時將打開新保護計劃的範本。
3. **[選用]** 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. **[選用]** 在 **[複寫方式]** 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. **[選用]** 按一下 **[排程]**，然後變更排程。
9. **[選用]** 按一下 **[保留規則]**，然後指定目標位置的保留規則，如 "保留規則" (第 168 頁) 中所述。
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. **[選用]** 要修改計劃選項，請按一下齒輪圖示。
12. 按一下 **[建立]**。

27.4.2 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。

注意事項

此功能可在進階備份組取得，並為執行離線主機資料處理作業代理程式的機器要求伺服器配額。

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

有關透過計算總和檢查碼進行驗證的詳細資訊，請參閱 "備份驗證" (第 182 頁)。

- 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	-	-

若要建立新的驗證計劃

1. 按一下 **[管理]** > **[驗證]**。

2. 按一下 **[建立計劃]**。

軟體會顯示新的計劃範本。

3. **[選用]** 要修改計劃名稱，請按一下預設名稱。

4. 按一下 **代理程式**，然後選擇將執行驗證的代理程式。

如果要從備份執行虛擬機器進行驗證，請選擇 VMware 代理程式或 Hyper-V 代理程式。否則，請選擇有權存取備份位置的任何代理程式。

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. [選用] 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. [選用] 按一下 **[驗證方式]**, 然後選擇以下任一方法:
 - **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. [選擇性步驟] 請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. 若您需要正確的驗證結果, 請勿停用 **[VM 活動訊號]** 開關。此開關專為將來版本而設計。
 - e. [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。
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]**。

27.4.3 清理

清理作業會根據保留規則刪除過期的備份。

注意事項

此功能可在進階備份組取得, 並為執行離線主機資料處理作業代理程式的機器要求伺服器配額。

支援的位置

清理計劃支援除 NFS 資料夾和 Secure Zone 之外的所有備份位置。

若要建立新的清理計劃

1. 按一下 **[管理]>[清理]**。
2. 按一下 **[建立計劃]**。
軟體會顯示新的計劃範本。
3. [選用] 要修改計劃名稱, 請按一下預設名稱。
4. 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. [選用] 按一下 **[排程]**, 然後變更排程。
7. [選用] 按一下 **[保留規則]**, 然後指定保留規則, 如 "保留規則" (第 168 頁) 中所述。
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. [選用] 要修改計劃選項, 請按一下齒輪圖示。
10. 按一下 **[建立]**。

27.4.4 轉換為虛擬機器

轉換為虛擬機器僅可用於磁碟層級備份。若備份包含系統磁碟區以及啟動作業系統的所有必要資訊, 則產生的虛擬機器可以自行啟動。否則, 您可將其虛擬磁碟新增至其他虛擬機器。

您可以為轉換為虛擬機器建立單獨的計劃, 然後手動或按計劃執行此計劃。

有關先決條件及限制的資訊, 請參閱 "關於轉換, 您需要知道的内容" (第 517 頁)。

注意事項

此功能可在進階備份組取得, 並為執行離線主機資料處理作業代理程式的機器要求伺服器配額。

若要建立轉換至虛擬機器的計劃

1. 按一下 **[管理]>[轉換為 VM]**。
2. 按一下 **[建立計劃]**。
軟體會顯示新的計劃範本。
3. [選用] 要修改計劃名稱, 請按一下預設名稱。
4. 在 **轉換為** 中, 選擇目標虛擬機器的類型。您可以選擇以下其中之一:
 - **VMware ESXi**
 - **Microsoft Hyper-V**
 - **Scale Computing HC3**
 - **VMware Workstation**
 - **VHDX 檔案**

注意事項

為了節省儲存空間, 每次轉換到 VHDX 檔案或 VMware 工作站都會覆寫在上一次轉換過程中在目標位置建立的 VHDX/VMDK 檔案。

5. 執行下列其中一項操作:
 - [VMware ESXi、Hyper-V 和 Scale Computing HC3]: 按一下 **[主機]**, 選擇目標主機, 然後指定新的電腦名稱範本。
 - [其他虛擬機器類型]: 在 **[路徑]** 中, 指定儲存虛擬機器檔案和檔案名稱範本的位置。

預設名稱為 **[電腦名稱]_converted**。

6. 按一下 **[代理程式]**，然後選擇將執行轉換的代理程式。
7. 按一下 **[要轉換的項目]**，然後選擇此計劃將轉換為虛擬機器的備份。
可以使用右上角的 **[位置]/[備份]** 開關，在選擇備份和選擇整個位置之間切換。
如果選定備份已加密，則所有備份必須使用相同的加密密碼。對於使用不同加密密碼的備份，請建立單獨的計劃。
8. [僅適用於 VMware ESXi 和 Hyper-V] 按一下 **[資料存放區]** (ESXi)，或按一下 **[路徑]** (Hyper-V)，然後選擇虛擬機器的資料存放區 (儲存)。
9. [僅適用於 VMware ESXi 和 Hyper-V]：選擇磁碟佈建模式。預設設定為：**[精簡]** (適用於 VMware ESXi) 和 **[動態延伸]** (適用於 Hyper-V)。
10. [選用] [VMware ESXi、Hyper-V 和 Scale Computing HC3]：按一下 **[VM 設定]** 以修改記憶體大小、處理器數量或虛擬機器的網路連線。
11. [選用] 按一下 **[排程]**，然後變更排程。
12. 如果 **[要轉換的項目]** 中選擇的備份已加密，請啟用 **[備份密碼]** 開關，然後提供加密密碼。否則，請跳過此步驟。
13. [選用] 要修改計劃選項，請按一下齒輪圖示。
14. 按一下 **[建立]**。

關於轉換，您需要知道的内容

支援的虛擬機器類型

將備份轉換至虛擬機器可以由建立備份的相同代理程式或其他代理程式完成。

若要轉換至 VMware ESXi、Hyper-V 或 Scale Computing HC3，您分別需要 ESXi、Hyper-V 或 Scale Computing HC3 主機以及用於管理此主機的保護代理程式 (VMware 用代理程式、Hyper-V 用代理程式或 Scale Computing HC3 用代理程式)。

轉換至 VHDx 檔案時，會假設檔案將當做虛擬磁碟連線至 Hyper-V 虛擬機器。

下表總結可以透過 **[轉換為 VM]** 作業建立虛擬機器的類型。表中的行顯示轉換後的虛擬機器類型。這些欄顯示執行轉換的代理程式。

VM 類型	VMware 用代理程式	Hyper-V 用代理程式	Windows 用代理程式	Linux 用代理程式	Mac 用代理程式	Scale Computing HC3 用代理程式	oVirt (KVM) 代理程式	Virtuozzo Hybrid Infrastructure 用代理程式	Virtuozzo 用代理程式
VMware ESXi	+	-	-	-	-	-	-	-	-
Micros	-	+	-	-	-	-	-	-	-

oft Hyper-V									
VMwar e 工作 站	+	+	+	+	-	-	-	-	-
VHDX 檔案	+	+	+	+	-	-	-	-	-
Scale Compu ting HC3	-	-	-	-	-	+	-	-	-

限制

- 無法轉換儲存空間在 NFS 上的備份。
- 儲存空間在安全區域中的備份只能由在同一台機器上執行的代理程式進行轉換。
- 只有在含有 Linux 邏輯磁碟區 (LVM) 的備份由 VMware 用代理程式、Hyper-V 用代理程式或 Scale Computing HC3 用代理程式建立，並導向至相同的 Hypervisor 時，才能加以轉換。不支援跨 Hypervisor 轉換。
- 當 Windows 電腦的備份轉換至 VMware Workstation 或 VHDX 檔案時，產生的虛擬機器會繼承執行轉換所在電腦中的 CPU 類型。因此，對應的 CPU 驅動程式會安裝在客體作業系統中。如果在具有不同 CPU 類型的主機上啟動，客體系統會顯示驅動程式錯誤。請手動更新此驅動程式。

定期轉換為虛擬機器和從備份執行虛擬機器

若原始電腦出現故障，則這兩種作業均會向您提供可在幾秒內啟動的虛擬機器。

定期轉換為虛擬機器佔用 CPU 和記憶體資源。虛擬機器的檔案會不斷佔用資料存放區 (儲存) 上的空間。若生產主機用於轉換，則定期轉換可能不實際。然而，虛擬機器效能僅受主機資源限制。

從備份執行虛擬機器僅在虛擬機器執行時佔用資源。資料存放區 (儲存) 空間僅需要保留虛擬磁碟的變更。然而，由於主機不直接存取虛擬磁碟，但是會與從備份中讀取資料的代理程式通訊，因此虛擬機器可能執行較慢。此外，此虛擬機器為臨時機器。

虛擬機器如何定期轉換

定期轉換的工作方式取決於您選擇建立虛擬機器的位置。

- **如果您選擇將虛擬機器儲存為一組檔案：**每次轉換都會從頭開始重新建立虛擬機器。
- **如果您選擇在虛擬化伺服器上建立虛擬機器：**轉換增量或差異備份時，軟體會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。如果操作成功，將會刪除舊機器。如果此作業失敗，則會刪除新的機器，並給予舊機器其先前名稱。如此一來，轉換程序結束後一律只會剩下一部虛擬機器。但是，在轉換期間需要額外的儲存空間來存放舊的機器。

如果您選擇在虛擬化伺服器建立虛擬機器

第一次轉換會建立一部新的虛擬機器。後續每次轉換的程序如下：

- 如果自上次轉換以來進行 [完整備份]，則將從頭開始重新建立虛擬機器，如本節前面所述。
- 否則，系統會更新現有的虛擬機器，反映上次轉換以來的變更。如果無法更新 (例如，如果您刪除下述的中間快照)，系統便會重新建立虛擬機器。

中間快照

為了能夠安全更新轉換後的虛擬機器，軟體會儲存此機器的中間 Hypervisor 快照。快照命名為 **Replica...** 並且必須保留。

Replica... 快照對應到最新轉換的結果。如果要將機器復原到該狀態，可前往此快照；例如，如果您在機器進行操作，現在要放棄對其所做的變更。

對於轉換後的 Scale Computing HC3 虛擬機器，將建立附帶的 **工具快照**。僅供 Cyber Protection 服務使用。

28 Cyber Protect 監視器

Cyber Protect 監視器提供 Windows 用代理程式、Mac 用代理程式和 File Sync & Share 用代理程式的圖形化使用者介面。其會顯示安裝 Windows 用代理程式或 Mac 用代理程式所在電腦保護狀態的相關資訊，並可讓其使用者設定備份加密和 Proxy 伺服器設定。它可以透過 File Sync & Share 用代理程式存取 File Sync & Share 服務。

這些代理程式是使用安裝它們的使用者帳戶註冊的。但是，在使用者登入自己的 File Sync & Share 帳戶並選擇個人同步資料夾強制上限之後，就可以存取 File Sync & Share 功能。如需有關 File Sync & Share 用代理程式的詳細資訊，請參閱 [Cyber Files Cloud 使用指南](#)。

Cyber Protect 監視器可供對 Cyber Protection 或 File Sync & Share 服務可能沒有系統管理權限的使用者存取。

沒有系統管理權限的 Cyber Protection 使用者可以執行下列工作：

- 將預設保護計劃套用至其電腦
- 檢查其電腦的保護狀態
- 暫時暫停備份其電腦

他們無法套用自訂保護計劃，也無法管理已經套用的保護計劃。

沒有系統管理權限的 File Sync & Share 使用者可以執行下列工作：

- 同步本機同步資料夾及其 File Sync & Share 帳戶之間的內容
- 暫停其同步作業
- 變更其同步資料夾
- 檢查其同步受到限制的檔案類型

所有 Cyber Protect 監視器使用者都可以變更備份加密設定或設定 Proxy 伺服器設定。

警告！

變更 Cyber Protect 監視器中的加密設定會覆寫保護計劃中的設定，並影響電腦的所有備份。此作業可能會使部分保護計劃失敗。如需詳細資訊，請參閱 "加密" (第 171 頁)。

若是遺失或忘記密碼，則無法復原加密的備份。

變更 Cyber Protect 監視器中的 Proxy 伺服器設定會影響安裝在相同電腦上的所有代理程式。

若要變更 Proxy 伺服器設定

1. 開啟 Cyber Protect 監視器，然後按一下右上角的齒輪圖示。
2. 按一下 **[設定]**，然後按一下 **[Proxy]**。
3. 啟用 **[使用 Proxy 伺服器]** 開關，然後指定 Proxy 伺服器位址和連接埠。
4. [如果 Proxy 伺服器存取受到密碼保護] 啟用 **[需要密碼]** 開關，然後指定使用者名稱和密碼以存取 Proxy 伺服器。
5. 按一下 **[儲存]**。

29 可開機媒體

可開機媒體是 CD、DVD、USB 快閃磁碟機或其他卸除式媒體，可讓您無需作業系統的協助，即可在 Linux 環境或 Windows 預先安裝環境/Windows 復原環境 (WinPE/WinRE) 中執行 Cyber Protection 代理程式。可開機媒體的主要用途是復原無法啟動的作業系統。

注意事項

可開機媒體不支援混合式磁碟機。

29.1 自訂或現成的可開機媒體？

您可以使用 Bootable Media Builder，為 Windows、Linux 或 macOS 電腦，建立自訂的可開機媒體 (Linux 型或 WinPE 型)。在 Linux 型和 WinPE/WinRE 型自訂可開機媒體中，您可以進行其他設定，例如，自動註冊、網路設定或 Proxy 伺服器設定。在 WinPE/WinRE 型自訂可開機媒體中，您也可以新增其他磁碟機。

或者，您可以下載現成的可開機媒體 (僅限 Linux 型)。您可以將現成的可開機媒體用於復原作業，以及存取 Universal Restore 功能。

29.2 Linux 型或 WinPE/WinRE 型可開機媒體？

29.2.1 Linux

Linux 型可開機媒體包含以 Linux 核心為基礎的 Cyber Protection 代理程式。代理程式可在任何 PC 相容硬體上開機並執行作業，包括裸機和含有已損壞或不支援的檔案系統的電腦。

29.2.2 WinPE/WinRE 型

WinPE 型可開機媒體包含一個稱為 Windows 預先安裝環境 (WinPE) 的最小 Windows 系統和 WinPE 用 Cyber Protection 外掛程式，這個外掛程式是 Cyber Protection 代理程式的改版，可在預先安裝環境中執行。WinRE 型可開機媒體使用 Windows 復原環境，而且不需要安裝其他 Windows 套件。

WinPE 被證明是用於含有各種硬體的較大環境中最方便的開機解決方案。

優點：

- 相較於使用 Linux 型可開機媒體，在 Windows 預先安裝環境中使用 Cyber Protection 可享受更多功能。開機 PC 相容硬體進入 WinPE 後，您不僅可以使用 Cyber Protection 代理程式，而且還可以使用 PE 命令和指令碼，以及已新增到 PE 的其他外掛程式。
- PE 型可開機媒體有助於克服某些與 Linux 相關的可開機媒體問題，如僅支援特定 RAID 控制器或特定層級的 RAID 陣列。以 WinPE 2.x 及更新版本為基礎的媒體允許動態載入所需的裝置驅動程式。

限制：

- 在使用整合可延伸韌體介面 (UEFI) 的電腦上，以舊於 4.0 之 WinPE 版本為基礎的可開機媒體無法開機。

29.3 建立實體可開機媒體

強烈建議您在開始使用磁碟層級備份時，立即建立並測試可開機媒體。此外，在 Cyber Protection 代理程式的每次重大更新後重新建立媒體，也是相當不錯的作法。

您可以透過使用相同的媒體復原 Windows 或 Linux。若要復原 Mac OS，請在執行 Mac OS 的電腦上另行建立單獨的媒體。

在 Windows 或 Linux 中建立實體可開機媒體

1. 建立自訂的可開機媒體 ISO 檔案或下載現成的 ISO 檔案。
若要建立自訂 ISO 檔案，請使用 "可開機媒體組建" (第 522 頁)。
若要下載現成的 ISO 檔案，請在 Cyber Protection 服務主控台中選擇一部電腦，然後按一下 **[復原]** > **[更多復原方式...]** > **[下載 ISO 影像]**。
2. [選擇性] 在 Cyber Protection 服務主控台中，產生註冊權杖。當您下載現成的 ISO 檔案時，會自動顯示註冊權杖。
此權杖允許可開機媒體存取雲端儲存，而不必提示您輸入登入和密碼。
3. 透過下列其中一種方式，建立實體可開機媒體：
 - 將 ISO 檔案燒錄到 CD/DVD。
 - 透過使用 ISO 檔及其中一個可在線上取得的免費工具，來建立可開機 USB 快閃磁碟機。
如果您需要啟動 UEFI 電腦，請使用 [ISO 至 USB] 或 [RUFUS]。若是 BIOS 電腦，則請使用 [Win32DiskImager]。在 Linux 中，應使用 dd 公用程式。
若是虛擬機器，您可以將 ISO 檔案當作 CD/DVD 光碟機，連接至您要復原的電腦。

在 macOS 中建立實體可開機媒體

1. 在已安裝 Mac 用代理程式的電腦上，按一下 **[應用程式]** > **[Rescue Media Builder]**。
2. 軟體會顯示已連接的卸除式媒體。選擇您要使之成為可開機的那一個媒體。

警告！

磁碟上的所有資料將被清除。

3. 按一下 **[建立]**。
4. 等候軟體建立可開機媒體。

29.4 可開機媒體組建

Bootable Media Builder 是建立可開機媒體的專用工具。它會當作選用的元件，安裝在安裝 Cyber Protection 代理程式所在的電腦上。

29.4.1 為什麼要使用 Bootable Media Builder?

可供在服務主控台中下載的現成可開機媒體是以 Linux 核心為基礎。與 Windows PE 不同，其不允許即時插入自訂驅動程式。

Bootable Media Builder 可讓您建立自訂的 Linux 型和 WinPE 型可開機媒體影像。

29.4.2 32 位元或 64 位元？

Bootable Media Builder 會建立同時包含 32 位元及 64 位元元件的可開機媒體。在大多數的情況下，使用整合可延伸韌體介面 (UEFI) 的電腦需要有 64 位元的媒體才能開機。

29.4.3 Linux 可開機媒體

若要建立 Linux 可開機媒體

1. 啟動 **Bootable Media Builder**。
2. 在 **[可開機媒體類型]** 中，選擇 **[預設 (Linux 媒體)]**。
3. 選擇表示磁碟區和網路資源的方式：
 - 採用類似 Linux 磁碟區表示方式的可開機媒體，會將磁碟區顯示為以下格式：`hda1` 和 `sdb2`。這種媒體在開始復原前，會先嘗試重建 MD 裝置和邏輯磁碟區 (LVM)。
 - 採用類似 Windows 磁碟區表示方式的可開機媒體，會將磁碟區顯示為以下格式：`C:` 與 `D:`。這種媒體可讓您存取動態磁碟區 (LDM)。
4. 指定 Linux 核心的參數。使用空格分隔多個參數。
例如，為了能夠在每次媒體啟動時選擇可開機代理程式的顯示模式，請輸入：`vga=ask`。如需有關可用參數的詳細資訊，請參閱 "核心參數" (第 523 頁)。
5. [選用] 選擇用於可開機媒體的語言。
6. [選用] 選擇 Windows 在復原後將使用的開機模式 (BIOS 或 UEFI)。
7. 選擇要放在媒體上的元件 – Cyber Protection 可開機代理程式。
8. [選用] 指定開機功能表的逾時間隔。如果未進行此設定，載入器將會等待您選擇要啟動作業系統 (如果有) 還是元件。
9. [選用] 如果您想要將可開機代理程式作業自動化，請選擇 **[使用下列指令碼]** 核取方塊。然後，選擇指令碼之一並指定指令碼參數。如需有關指令碼的詳細資訊，請參閱 "可開機媒體中的指令碼" (第 525 頁)。
10. [選用] 選擇在開機時要如何在 Cyber Protection 服務中註冊可開機媒體。如需有關註冊設定的詳細資訊，請參閱 "註冊可開機媒體" (第 533 頁)。
11. 指定已開機電腦網路介面卡的網路設定，或保留自動 DHCP 設定。
12. [選用] 如果您的網路中已啟用 Proxy 伺服器，請指定其主機名稱/IP 位址和連接埠。
13. 選擇已建立之可開機媒體的檔案類型：
 - ISO 影像
 - ZIP 檔案
14. 指定可開機媒體檔案的檔案名稱。
15. 在摘要畫面中檢查您的設定，然後按一下 **[繼續]**。

核心參數

您可以指定將會在可開機媒體啟動時自動套用的一或多個 Linux 核心參數。這些參數通常在使用可開機媒體遇到問題時使用。一般來說，可將此欄位留空。

您也可以在開機功能表中按下 F11 鍵來指定這些參數中的任何參數。

參數

指定多個參數時，使用空格將它們隔開。

- **acpi=off**

停用進階組態與電源介面 (ACPI)。遇到特定硬體組態問題時，您可能需要使用此參數。

- **noapic**

停用進階可程式中斷控制卡 (APIC)。遇到特定硬體組態問題時，您可能需要使用此參數。

- **vga=ask**

提示可開機媒體的圖形化使用者介面要使用的視訊模式。若沒有 **vga** 參數，則會自動偵測視訊模式。

- **vga=mode_number**

指定可開機媒體的圖形化使用者介面要使用的視訊模式。模式編號由 *mode_number* 以十六進位格式提供，例如：**vga=0x318**

與某個模式編號相對應的螢幕解析度和顏色數量在不同的電腦上可能會有所不同。建議先使用 **vga=ask** 參數來選擇 *mode_number* 的值。

- **quiet**

載入 Linux 核心時停用啟動訊息顯示，並在載入核心後啟動管理主控台。

此參數是在建立可開機媒體時以隱含的方式指定，但是您可以在開機功能表中移除此參數。

如果移除此參數，將顯示所有啟動訊息，然後顯示命令提示字元。若要從命令提示字元啟動管理主控台，請執行命令：**/bin/product**

- **nousb**

停用 USB (通用序列匯流排) 子系統的載入。

- **nousb2**

停用 USB 2.0 支援。使用此參數，USB 1.1 裝置仍可運作。某些 USB 磁碟機無法在 USB 2.0 模式下運作時，此參數可讓您以 USB 1.1 模式使用這些磁碟機。

- **nodma**

停用所有 IDE 硬碟機的直接記憶體存取 (DMA)。防止核心在某些硬體上停止回應。

- **nofw**

停用 FireWire (IEEE1394) 介面支援。

- **nopcmcia**

停用 PCMCIA 硬體偵測。

- **nomouse**

停用滑鼠支援。

- **module_name=off**

停用 *module_name* 指定之名稱的模組。例如，若要停用 SATA 模組，請指定：**sata_sis=off**

- **pci=bios**

強制使用 PCI BIOS，而不直接存取硬體裝置。如果電腦使用非標準 PCI 主機橋接器，則您可能需要使用此參數。

- **pci=nobios**

停用 PCI BIOS, 僅允許使用直接硬體存取方式。可開機媒體無法啟動 (可能由 BIOS 造成) 時, 您可能需要使用此參數。

- **pci=biosirq**

使用 PCI BIOS 呼叫, 以取得中斷路由表。如果核心無法配置中斷請求 (IRQ) 或無法找到主機板上的次要 PCI 匯流排, 則您可能需要使用此參數。

這些呼叫在部分電腦上可能無法正常運作。但這可能是取得中斷路由表的唯一方法。

- **LAYOUTS=en-US, de-DE, fr-FR, ...**

指定可開機媒體的圖形化使用者介面可使用的鍵盤配置。

若沒有此參數, 則只能使用兩種配置: 英文 (美國) 和對應到媒體開機功能表中所選語言的配置。

您可以指定以下任一配置:

比利時文: **be-BE**

捷克文: **cz-CZ**

英文: **en-GB**

英文 (美國): **en-US**

法文: **fr-FR**

法文 (瑞士): **fr-CH**

德文: **de-DE**

德文 (瑞士): **de-CH**

義大利文: **it-IT**

波蘭文: **pl-PL**

葡萄牙文: **pt-PT**

葡萄牙文 (巴西): **pt-BR**

俄文: **ru-RU**

塞爾維亞文 (斯拉夫文): **sr-CR**

塞爾維亞文 (拉丁文): **sr-LT**

西班牙文: **es-ES**

在可開機媒體下作業時, 使用 CTRL + SHIFT 可在可用配置循環。

可開機媒體中的指令碼

如果您希望可開機媒體執行一組預先定義的作業, 可以指定指令碼, 同時使用 Bootable Media Builder 建立媒體。因此, 每次從媒體啟動電腦時, 將會執行指定的指令碼, 而且不會顯示使用者介面。

您可按照指令碼處理慣例選取其中一個預先定義的指令碼或建立自訂指令碼。

預先定義腳本

可開機媒體建立程式提供以下預定義腳本:

- 從雲端存放區復原 (**entire_pc_cloud**)
- 從網路共用復原 (**entire_pc_share**)

指令碼位於安裝 Bootable Media Builder 所在電腦上的下列資料夾中:

- 在 Windows 中 : %ProgramData%\Acronis\MediaBuilder\scripts\
- 在 Linux 中 : /var/lib/Acronis/MediaBuilder/scripts/

從雲端存放區復原

在可開機媒體開機程式中, 指定以下腳本參數:

1. 備份檔案名稱。
2. [選用] 指令碼將用於存取加密備份的密碼。

從網路共用復原

在可開機媒體開機程式中, 指定以下腳本參數:

- 網路共用的路徑。
- 網路共用的使用者名稱和密碼。
- 備份檔案名稱。找出備份檔案名稱:
 - a. 在 Cyber Protection 服務主控台中, 移至 **【備份儲存】>【位置】**。
 - b. 選擇網路共用(如果共用未列出, 請按一下 **【新增位置】**)。
 - c. 選擇備份。
 - d. 按一下 **【詳細資料】**。檔案名顯示在 **【備份檔案名稱】** 下方。
- [選用] 指令碼將用於存取加密備份的密碼。

自訂指令碼

重要事項

建立自訂指令碼需要瞭解 Bash 命令語言及 JavaScript 物件標記法 (JSON)。如果您不熟悉 Bash, 則可以前往以下網址瞭解: <http://www.tldp.org/LDP/abs/html>。JSON 規格位於以下網址: <http://www.json.org>

指令碼的檔案

指令碼必須位於安裝可開機媒體建立程式之電腦上的下列目錄中:

- 在 Windows 中 : %ProgramData%\Acronis\MediaBuilder\scripts\
- 在 Linux 中 : /var/lib/Acronis/MediaBuilder/scripts/

指令碼必須包含至少三個檔案:

- **<script_file>.sh** - 具有 Bash 指令碼的檔案。建立指令碼時, 僅使用一組有限的 Shell 命令, 這些命令位於: <https://busybox.net/downloads/BusyBox.html>。系統也可以使用下列命令:
 - **acrocmd** - 用於備份及復原的命令列公用程式
 - **product** - 啟動可開機媒體使用者介面的命令
 此檔案以及指令碼包括之任何其他檔案(例如, 透過使用 **dot** 命令)必須位於 **bin** 子資料夾中。在指令碼中, 將其他檔案路徑指定為 **/ConfigurationFiles/bin/<some_file>**。
- **自動啟動** - 用於啟動 **<script_file>.sh** 的檔案。檔案內容必須如下所示:

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** - 包含下列項目的 JSON 檔案：
 - 要在可開機媒體建立程式中顯示的指令碼名稱和說明。
 - 要透過可開機媒體建立程式設定之指令碼變數的名稱。
 - 將針對每個變數顯示在可開機媒體建立程式中的控制參數。

autostart.json 的結構

29.4.4 最上層物件

配對		需要	描述
名稱	值類型		
displayName	string	是	要在可開機媒體建立程式中顯示的指令碼名稱。
description	string	否	要在可開機媒體建立程式中顯示的指令碼說明。
timeout	number	否	啟動指令碼之前開機功能表的逾時值 (秒)。如果未指定配對, 則逾時值將為 10 秒。
variables	物件	否	您要透過可開機媒體建立程式設定之 <script_file>.sh 的任何變數。 該值應該是以下一組配對: 變數的字串識別碼與變數的物件 (請參閱下表)。

29.4.5 變數物件

配對		需要	描述
名稱	值類型		
displayName	string	是	<script_file>.sh 中使用的變數名稱。
type	string	是	可開機媒體建立程式中顯示的控制類型。此控制用於設定變數值。 如需所有受支援的類型, 請參閱下表。
description	string	是	可開機媒體建立程式中控制項上方顯示的控制標籤。
default	如果 type 是 string、multiString、	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)

	password 或 enum, 則為字串 如果 type 是 number、spinner 或 checkbox, 則為數字		狀態)。
order	number (非負數)	是	可開機媒體建立程式中的控制命令。該值越高, 相對於 autostart.json 中定義之其他控制放置的控制越低。起始值必須是 0。
min (僅限 spinner)	number	否	微調方塊中微調控制的最小值。如果未指定配對, 則該值將為 0。
max (僅限 spinner)	number	否	微調方塊中微調控制的最高值。如果未指定配對, 則該值將為 100。
step (僅限 spinner)	number	否	微調方塊中微調控制的步驟值。如果未指定配對, 則該值將為 1。
items (僅限 enum)	字串陣列	是	下拉式清單的值。
required (針對 string、multiString、password 和 enum)	number	否	指定控制值是可以為空 (0), 還是不可以為空 (1)。如果未指定配對, 則控制值可以為空。

29.4.6 控制類型

名稱	描述
string	用來輸入或編輯短字串的单一行、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单一行、無限制文字方塊。
number	用來輸入或編輯數字的单一行、僅限數字的文字方塊。
spinner	用來輸入或編輯數字的单一行、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
    }
}
}

```

29.4.7 WinPE 型和 WinRE 型可開機媒體

您不需要任何額外的準備，就可以建立 WinRE 影像，也可以在安裝 [Windows 自動化安裝套件 \(AIK\)](#) 或 [Windows 評定及部署套件 \(ADK\)](#) 後建立 WinPE 影像。

WinRE 影像

下列作業系統支援建立 WinRE 影像：

- Windows 7 (64 位元)
- Windows 8、8.1、10 (32 位元及 64 位元)
- Windows Server 2012、2016、2019 (64 位元)

WinPE 影像

安裝 Windows 自動化安裝套件 (AIK) 或 Windows 評定及部署套件 (ADK) 之後，Bootable Media Builder 支援基於下列任何核心的 WinPE 發行版：

- Windows Vista (PE 2.0)
- Windows Vista SP1 和 Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0), 無論是否有 Windows 7 SP1 (PE 3.1) 的補充
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE 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。

注意事項

WinPE 4 及更新版本的 PE 影像需要約 1 GB 的 RAM 才能運作。

建立 WinPE 或 WinRE 可開機媒體

Bootable Media Builder 提供將 Cyber Protection 與 WinPE 和 WinRE 整合在一起的兩種方法：

- 使用 Cyber Protection 外掛程式, 從頭開始建立 ISO 檔案。
- 出於未來任何使用目的 (手動建立 ISO、將其他工具新增至影像等), 將 Cyber Protection 外掛程式新增至 WIM 檔案。

建立 WinPE 或 WinRE 可開機媒體

1. 在安裝 Cyber Protection 代理程式所在的電腦上, 執行 Bootable Media Builder。
2. 在 **[可開機媒體類型]** 中, 選取 **[Windows PE]** 或 **[Windows PE (64 位元)]**。使用整合可延伸韌體介面 (UEFI) 的電腦需要有 64 位元的媒體才能開機。
3. 選擇可開機媒體的子類型: **[WinRE]** 或 **[WinPE]**。

建立 WinRE 可開機媒體不需要安裝其他任何套件。

若要建立 64 位元 WinPE 媒體, 您必須下載 Windows 自動化安裝套件 (AIK) 或 Windows 評定及部署套件 (ADK)。若要建立 32 位元 WinPE 媒體, 除了下載 AIK 或 ADK 之外, 您還需要執行下列操作：

- a. 按一下下載 **WinPE(32 位元) 外掛程式**。
 - b. 將外掛程式儲存到 **%PROGRAM_FILES%\BackupClient\BootableComponents\WinPE32**。
4. [選用] 選擇用於可開機媒體的語言。
 5. [選用] 選擇 Windows 在復原後將使用的開機模式 (BIOS 或 UEFI)。
 6. 指定已開機電腦網路介面卡的網路設定, 或保留自動 DHCP 設定。
 7. [選用] 選擇在開機時要如何在 Cyber Protection 服務中註冊可開機媒體。如需有關註冊設定的詳細資訊, 請參閱 "註冊可開機媒體" (第 533 頁)。
 8. [選擇性] 指定要新增至可開機媒體的 Windows 驅動程式。

電腦開機進入 Windows PE 或 Windows RE 後, 驅動程式即可協助您存取備份所在的裝置。如果您使用 32 位元 WinPE 或 WinRE 發行版本, 請新增 32 位元驅動程式; 如果您使用 64 位元 WinPE 或 WinRE 發行版本, 則新增 64 位元驅動程式。

若要新增驅動程式：

- 按一下 **[新增]**, 然後指定對應 SCSI、RAID、SATA 控制器、網路介面卡、磁帶機或其他裝置所需 .inf 檔案的路徑。
 - 對要包含在所產生 WinPE 或 WinRE 媒體中的每個驅動程式重複此程序。
9. 選擇已建立之可開機媒體的檔案類型：
 - ISO 影像
 - WIM 影像
 10. 指定所產生影像檔案的完整路徑, 包括檔案名稱。
 11. 在摘要畫面中檢查您的設定, 然後按一下 **[繼續]**。

從產生的 WIM 檔案建立 PE 影像 (ISO 檔案)

- 以新建立的 WIM 檔案取代 Windows PE 資料夾中的預設 boot.wim 檔案。以上述範例為例, 請輸入：

```
copy c:\RecoveryWIMMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- 使用 **Oscdimg** 工具。以上述範例為例, 請輸入：

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
```

警告！

請勿複製貼上此範例。請手動輸入命令, 否則命令將會失敗。

準備工作: WinPE 2.x 與 3.x

若要能建立或修改 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] 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。

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。

29.4.8 註冊可開機媒體

在 Cyber Protection 服務中註冊可開機媒體後, 允許存取雲端儲存進行備份。您可以在建立可開機媒體時預先設定註冊。如果未預先設定註冊, 您葛以在使用媒體啟動電腦後註冊。

在 Cyber Protection 服務中預先設定註冊

1. 在 Bootable Media Builder 中, 瀏覽至 **[可開機媒體註冊]**。
2. 在 **[服務 URL]** 中, 指定 Cyber Protection 服務位址。
3. [選用] 在 **[顯示名稱]** 中, 指定已開機電腦的名稱。
4. 若要在 Cyber Protection 服務中設定自動註冊, 選擇 **[自動註冊可開機媒體]** 核取方塊, 然後選擇自動註冊層級:
 - **開機時要求註冊權杖**
權杖必須在每次從此可開機媒體啟動電腦時提供。
 - **使用下列權杖**
從此可開機媒體啟動電腦時, 將會自動註冊。

從可開機媒體啟動電腦後註冊

1. 從可開機媒體啟動電腦。
2. 在啟動視窗中, 按一下 **[註冊媒體]**。
3. 在 **[伺服器]** 中, 指定 Cyber Protection 服務位址。
4. 在 **[註冊權杖]** 中, 輸入註冊權杖。
5. 按一下 **[註冊]**。

29.4.9 網路設定

建立可開機媒體時，您可以預先設定將由可開機代理程式使用的網路連線。您可以預先設定下列參數：

- IP 位址
- 子網路遮罩
- 閘道
- DNS 伺服器
- WINS 伺服器

之後可開機代理程式在電腦上啟動時，該設定會套用到電腦的網路介面卡 (NIC)。如果尚未預先設定設定，代理程式將使用 DHCP 自動設定。

當可開機代理程式在電腦上執行時，您也可以手動設定網路設定。

預先設定多個網路連線

您可以為多達 10 個網路介面卡 (NIC) 預先設定 TCP/IP 設定。為確保為每個 NIC 指定適合設定，在相應伺服器上建立將被自訂的媒體。當您在精靈視窗中選擇一個現有的 NIC 時，會選擇其設定並儲存在媒體上。每個現有 NIC 的 MAC 位址也將儲存在該媒體上。

您可以變更 MAC 位址之外的設定；或為不存在的 NIC 進行設定。

一旦可開機代理程式在伺服器上啟動之後，它將擷取可用 NIC 的清單。此清單按 NIC 佔用的插槽排序，最接近處理器的位於最上方。

可開機代理程式會為每個已知的 NIC 指派適合的設定，並透過其 MAC 位址識別 NIC。在設定包含已知 MAC 位址的 NIC 後，將從上部未指派的 NIC 開始，為剩餘的 NIC 指派您為不存在的 NIC 所進行的設定。

您可以為任何電腦自訂可開機媒體，而不僅限於建立媒體所在的電腦。若要進行此作業，根據它們在該電腦上的插槽順序設定 NIC：NIC1 佔用最接近處理器的插槽，NIC2 位於下一個插槽，依此類推。當可開機代理程式在該電腦上啟動時，它將找不到具有已知 MAC 位址的 NIC，因此將採用與您所使用的相同順序設定 NIC。

範例

可開機代理程式可以使用其中一個網路介面卡，透過生產網路與管理主控台通訊。可以自動設定此連線。用於復原且可變更大小的資料可透過第二個 NIC 傳輸，使用靜態 TCP/IP 設定的方式包括在專用備份網路中。

29.5 連線到從可開機媒體開機的電腦

29.5.1 本機連線

如果要直接在從可開機媒體開機的電腦上操作，請按一下啟動視窗中的 **[本機管理此電腦]**。

電腦從可開機媒體開機後，電腦終端機將顯示一個啟動視窗，其中包含向 DHCP 取得或根據預先設定的值設定的 IP 位址。

29.5.2 進行網路設定

若要變更目前工作階段的網路設定，請按一下啟動視窗中的 **[設定網路]**。隨即會顯示 **[網路設定]** 視窗，您可在其中為電腦上的每張網路介面卡 (NIC) 進行網路設定。

電腦重新開機後，將會失去在工作階段期間所做的變更。

新增 VLAN

您可以在 **[網路設定]** 視窗中，新增虛擬區域網路 (VLAN)。如果您需要存取包含於特定 VLAN 中的備份位置，可以使用此功能。

VLAN 主要用於將區域網路分為多個區段。連接到交換器 **[存取]** 連接埠的 NIC 一律可以存取連接埠設定中指定的 VLAN。而連接到交換器 **[主幹]** 連接埠的 NIC，則僅在您於網路設定中有指定 VLAN 時，才能存取連接埠設定中允許的 VLAN。

透過主幹連接埠提供 VLAN 存取

1. 按一下 **[新增 VLAN]**。
2. 選擇可供存取包含所需 VLAN 之區域網路的 NIC。
3. 指定 VLAN 識別碼。

當您按下 **[確定]** 之後，網路介面卡清單中會出現新項目。

如果您需要移除 VLAN，請按一下所需的 VLAN 項目，然後按一下 **[移除 VLAN]**。

29.6 可開機媒體的相關作業

可開機媒體的相關作業與在執行中作業系統下執行的復原作業類似。差異如下：

1. 在以類似 Windows 磁碟區表示的可開機媒體下，磁碟區的磁碟機代號與 Windows 中的磁碟機代號相同。如果磁碟區在 Windows 中沒有磁碟機代號 (例如系統保留磁碟區)，系統會依磁碟區在磁碟中的順序，將可用代號指定給磁碟區。

如果可開機媒體無法在電腦上偵測到 Windows，或者偵測到一個以上的 Windows，則系統會依磁碟區在磁碟中的順序，將可用代號指派給所有磁碟區，包括沒有磁碟機代號的磁碟區。因此，磁碟區代號可能與 Windows 中看到的不同。例如，D: 磁碟機在可開機媒體下可能對應的是 Windows 中的 E: 磁碟機。

注意事項

建議為磁碟區指派唯一的名稱。

2. 以類似 Linux 磁碟區表示的可開機媒體會將本機磁碟和磁碟區顯示為已卸載 (sda1, sda2...)。
3. 無法排程工作。如果您需要重複作業，則需要從頭開始設定。
4. 記錄的存留期僅限於當前工作階段。您可將整份記錄或篩選出來的記錄項目儲存為一個檔案。

29.6.1 設定顯示模式

當您透過 Linux 可開機媒體啟動電腦時，會根據硬體組態 (監視器和圖形卡規格) 自動偵測顯示視訊模式。如果視訊模式偵測錯誤，請執行下列動作：

1. 在開機功能表中，按下 F11。
2. 在命令列上，輸入 **vga=ask**，然後繼續進行開機。
3. 從所支援的視訊模式清單中選擇適當模式，其方法是輸入其編號 (例如 **318**)，然後按 **Enter**。

如果您不想每次在特定硬體組態上開機時都依照此程序執行，請重新建立可開機媒體，並在 **[核心參數]** 欄位中指定適當的模式編號 (在上述範例中為 **vga=0x318**)。

29.6.2 復原

1. 從可開機媒體啟動電腦。
2. 按一下 **[在本機管理這部電腦]**。
3. 按一下 **[復原]**。
4. 在 **[復原內容]** 中，按一下 **[選擇資料]**。
5. 選擇您要復原的來源備份檔案。
6. 在左下方窗格中，選擇您要復原的磁碟機/磁碟區或檔案/資料夾，然後按一下 **[確定]**。
7. 設定覆寫規則。
8. 設定復原排除。
9. 設定復原選項。
10. 檢查您的設定是否正確，然後按一下 **[確定]**。

29.7 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，您要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。

若要使用 Startup Recovery Manager，您必須先將其啟用。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** 項目新增到 GRUB 功能表)。

注意事項

若要在系統磁碟區未加密的電腦上啟動 Startup Recovery Manager, 此電腦上至少需要 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。

若要在使用 BitLocker 加密其系統磁碟區的電腦上啟動 Startup Recovery Manager, 在相同的電腦上至少需要有一個未加密的磁碟區。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, 則需要另外 500 MB 的可用空間。

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。

在具有 Windows 用代理程式或 Linux 用代理程式的電腦上啟用 Startup Recovery Manager

1. 在 Cyber Protection 服務主控台中, 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。

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的提示 **[按下 F11, 執行 Acronis Startup Recovery Manager]** (或 GRUB 中的功能表項目)。

30 監控

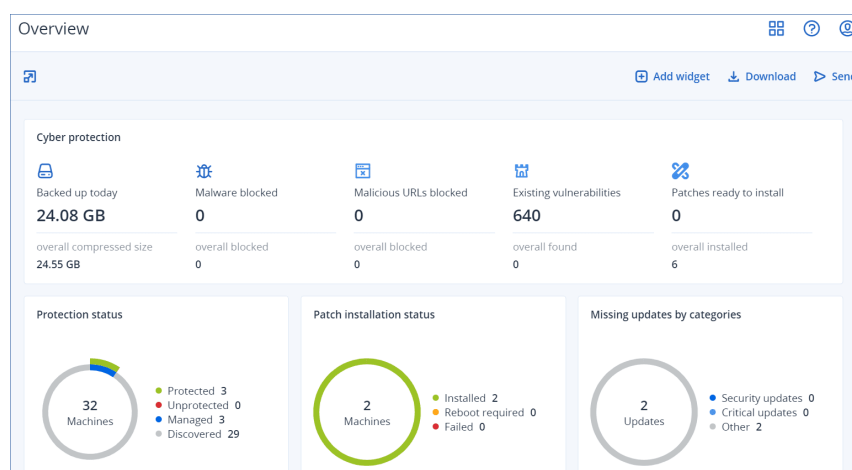
30.1 概觀儀表板

【概觀】儀表板提供許多可自訂的動態桌面小工具，可概覽與 Cyber Protection 服務有關的作業。針對其他服務的動態小工具將在未來版本中提供。

系統會每五分鐘更新一次桌面小工具。動態小工具帶有可按一下的元素，可讓您調查問題並進行疑難排解。您可以透過 .pdf 和/或 .xlsx 格式下載最新狀態的儀表板或透過電子郵件進行傳送。

您可以從各種桌面小工具中選擇：顯示為表格、長條圖和樹狀圖。您可以新增具有不同篩選的相同類型動態小工具。

【監控】>【概觀】中的**【下載】**和**【傳送】**按鈕無法用於 Cyber Protection 服務的 Standard 版本。



重新排列儀表板上的動態小工具

透過在動態小工具的名稱上按一下，可拖曳它們。

編輯動態小工具

按一下動態小工具名稱旁的鉛筆圖示。編輯桌面小工具可讓您將它重新命名、變更時間範圍、設定篩選，以及為列分組。

新增動態小工具

按一下**【新增動態小工具】**，然後執行下列其中一項操作：

- 按一下您要新增的動態小工具。接著會以預設設定新增動態小工具。
- 若要在新增之前編輯桌面小工具，請在選取桌面小工具時按一下**【自訂】**。編輯動態小工具之後，按一下**【完成】**。

移除動態小工具

按一下動態小工具名稱旁的 X 符號。

30.2 [活動] 儀表板

[活動] 儀表板提供目前與過去活動的概觀。依預設，保留期為 90 天。

若要自訂 **[活動]** 儀表板的檢視，請按一下齒輪圖示，然後選擇您要查看的欄。

若要即時查看活動進度，請選擇 **[自動重新整理]** 核取方塊。不過，經常更新多個活動會降低管理伺服器的效能。

您可以依下列條件搜尋列出來的活動：

- **裝置名稱**

這是執行活動所在的電腦。

- **啟動者**

這是啟動活動的帳戶。

您也可以依下列屬性篩選活動：

- **狀態**

例如，成功、失敗、進行中、已取消。

- **類型**

例如，套用計劃、刪除備份、安裝軟體更新。

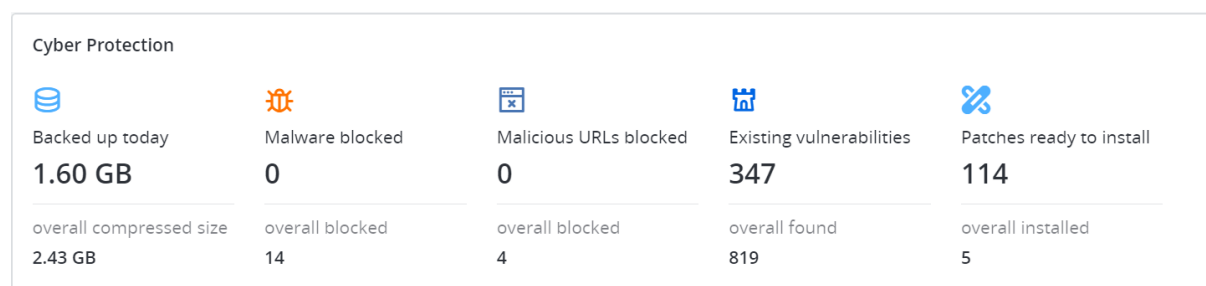
- **時間**

例如，最近的活動、過去 24 小時的活動，或是預設保留期內特定期間的活動。

若要查看有關活動的更多詳細資料，請從清單中選擇此活動，然後在 **[活動詳細資料]** 面板中，按一下 **[所有屬性]**。如需有關可用屬性的詳細資訊，請參閱開發人員網路入口網站中的 [\[活動\]](#) 和 [\[工作\]](#) API 參考資料。

30.3 網路保護

此桌面小工具會顯示有關備份大小、已封鎖之惡意程式碼、已封鎖之 URL、已發現之弱點，以及已安裝之修補程式的整體資訊。



上排會顯示目前的統計資料：

- **今天備份的資料** – 過去 24 小時的復原點大小總和
- **已封鎖的惡意程式碼** – 已封鎖之惡意程式碼目前作用中警示的數目
- **已封鎖的 URL** – 已封鎖之 URL 目前作用中警示的數目

- **現有的弱點** – 目前現有弱點的數目
- **已準備好安裝的修補程式** – 要安裝之目前可用修補程式的數目

下排會顯示整體的統計資料：

- 所有備份的壓縮大小
- 所有電腦中已封鎖之惡意程式碼的累積數目
- 所有電腦中已封鎖之 URL 的累積數目
- 所有電腦中已發現之弱點的累積數目
- 所有電腦中已安裝之更新/修補程式的累積數目

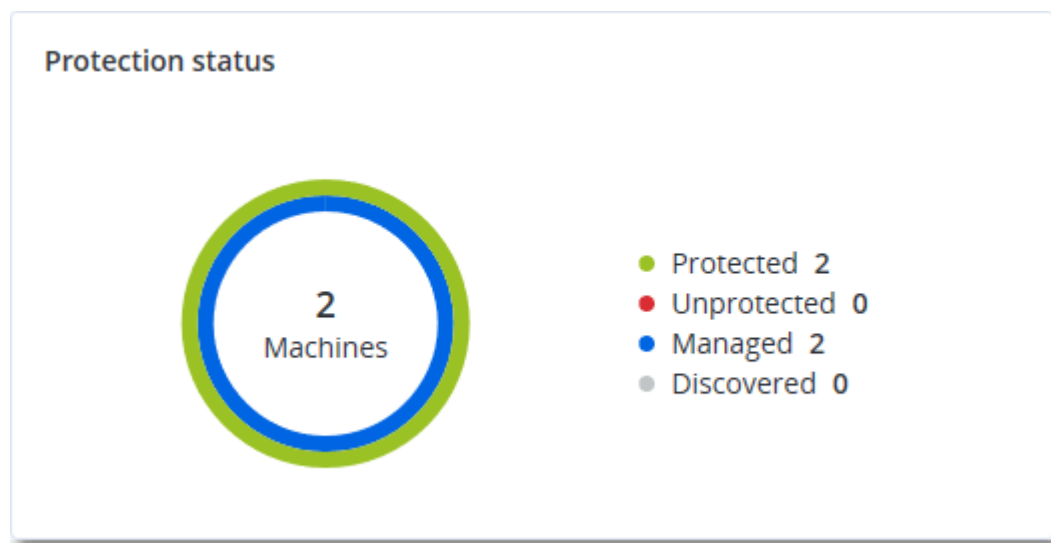
30.4 保護狀態

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。



30.4.1 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。

Discovered machines				
Device name ↑	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual

30.5 依電腦分類的 #CyberFit 分數

此桌面小工具可針對每部電腦顯示 #CyberFit 總分、其綜合分數，以及每個評估指標的結果：

- 反惡意程式碼
- 備份
- 防火牆
- VPN
- 加密
- NTLM 流量

若要提高每個指標的分數，您可以檢視報告中提供的建議。

如需有關 #CyberFit 分數的詳細資訊，請參閱「[電腦的 #CyberFit 分數](#)」。

#CyberFit Score by machine ?		
Metric	#CyberFit Score	Findings
DESKTOP-2N2TRE8 625 / 850		
Anti-malware	275 / 275	You have anti-malware protection enabled
Backup	175 / 175	You have a backup solution protecting your data
Firewall	175 / 175	You have a firewall enabled for public and private networks
VPN	0 / 75	No VPN solution was found, your connection to public and shared networks is n...
Encryption	0 / 125	No disk encryption was found, your device is at risk from physical tampering
NTLM traffic	0 / 25	Outgoing NTLM traffic to remote servers is not denied, your credentials may be ...

30.6 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。

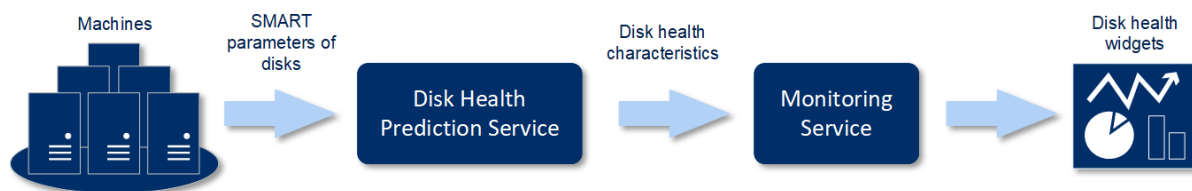
磁碟健全狀況以下列其中一種狀態表示：

- **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**
目前的磁碟狀態和預測正在計算中。

30.6.1 運作原理

磁碟健全狀況預測服務使用以 AI 為基礎的預測模型。

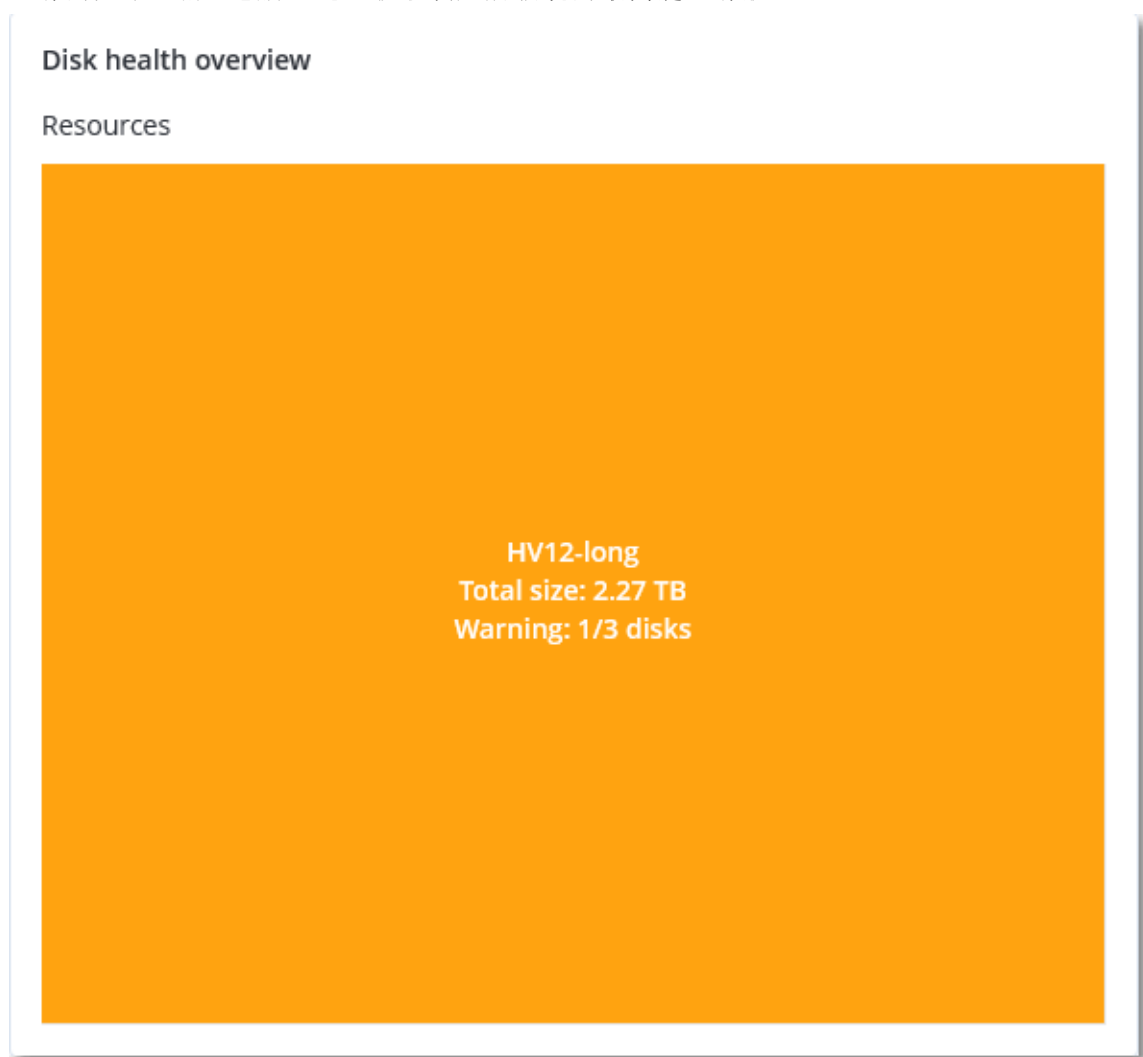
1. 保護代理程式會收集磁碟的 SMART 參數，並將此資料傳遞給磁碟健全狀況預測服務：
 - SMART 5 – 重新配置的磁區計數。
 - SMART 9 – 開機時數。
 - SMART 187 – 報告的無法更正錯誤數。
 - SMART 188 – 命令逾時。
 - SMART197 – 目前擱置中的磁區計數。
 - SMART 198 – 離線的無法更正磁區計數。
 - SMART 200 – 寫入錯誤率。
2. 磁碟健全狀況預測服務會處理收到的 SMART 參數、進行預測，然後提供下列磁碟健全狀況特徵：
 - 磁碟健全狀況目前狀態：正常、警告、嚴重。
 - 磁碟健全狀況預測：負面、穩定、正面。
 - 磁碟健全狀況預測機率 (百分比)。預測期間為一個月。
3. 監控服務會收到這些特徵，然後在服務主控台的磁碟健全狀況桌面小工具中顯示相關的資訊。



30.6.2 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服務主控台中提供的下列桌面小工具內。

- **磁碟健全狀況概觀**是一個樹狀圖桌面小工具，其中包含可以透過查找切換的兩個詳細資料層級。
 - 電腦層級
針對選取的客戶電腦，顯示磁碟健全狀況狀態的摘要資訊。只有最嚴重的磁碟狀態才會顯示。當您將滑鼠暫留在特定區塊時，工具提示中會顯示其他狀態。電腦區塊大小取決於電腦所有磁碟的大小總計。電腦區塊色彩取決於所發現的最關鍵磁碟狀態。



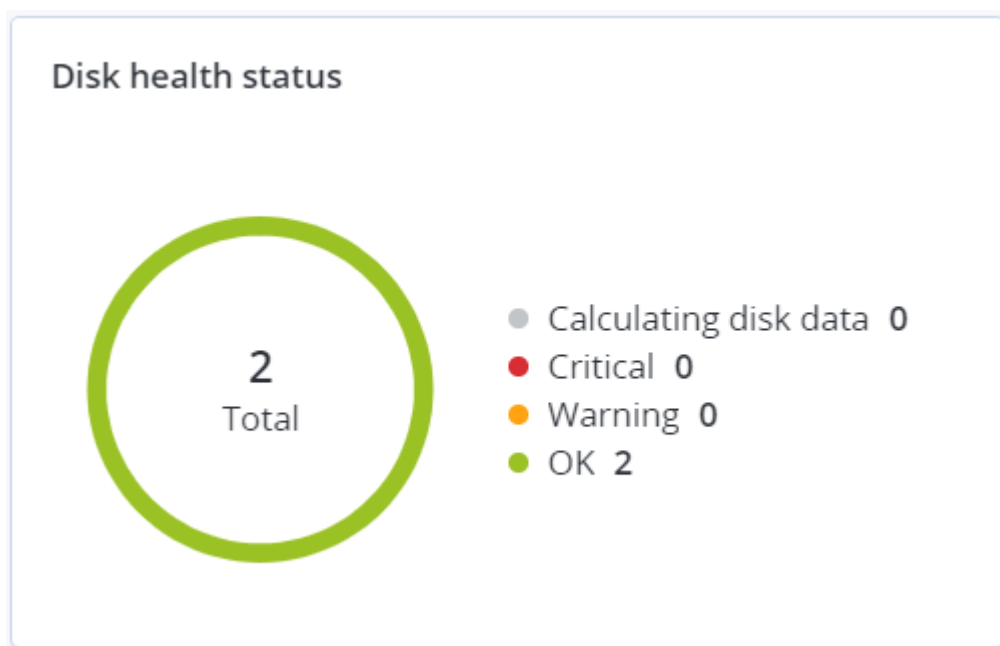
- 磁碟層級
針對所選電腦，顯示所有磁碟目前的磁碟健全狀況狀態。每個磁碟區塊都會顯示下列其中一

個磁碟健全狀況預測及其機率 (百分比):

- 將降級
- 將保持穩定
- 將改善



- 磁碟健全狀況狀態是一個圓形圖桌面小工具, 可顯示每個狀態的磁碟數。



30.6.3 磁碟健全狀況狀態警示

磁碟健全狀況檢查每 30 分鐘執行一次，而對應的警示則一天產生一次。當磁碟健全狀況從 **[警告]** 變更為 **[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。

30.7 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客戶/電腦所屬所有重要檔案的總數/大小總計。

注意事項

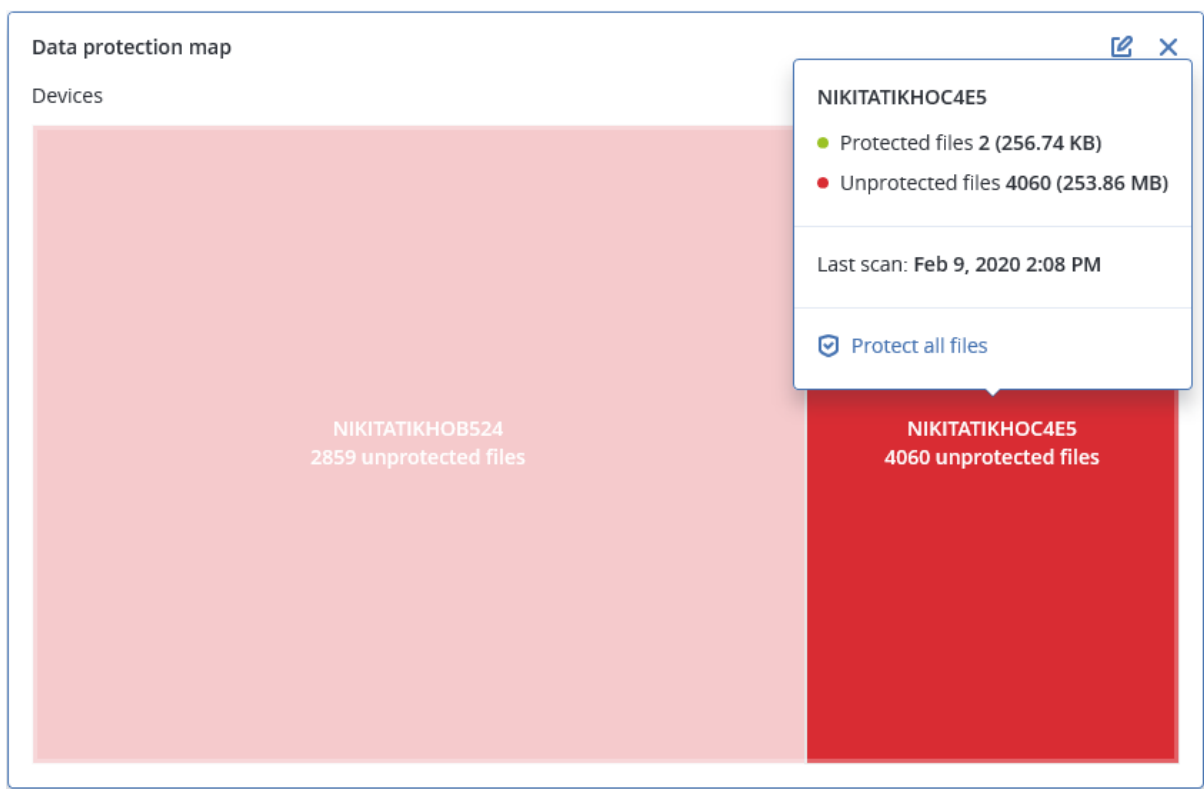
是否能夠使用此功能視您帳戶啟用的服務配額而定。

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) 的監控儀表板上找到：

- 電腦層級 - 針對所選客戶的每部電腦，顯示重要檔案保護狀態的相關資訊。



若要保護未受保護的檔案，請將滑鼠移至該區塊，然後按一下 **[保護所有檔案]**。在對話視窗中，您可以找到未受保護檔案數目及其位置的相關資訊。若要保護這些檔案，按一下 **[保護所有檔案]**。

您也可以下載 CSV 格式的詳細報告。

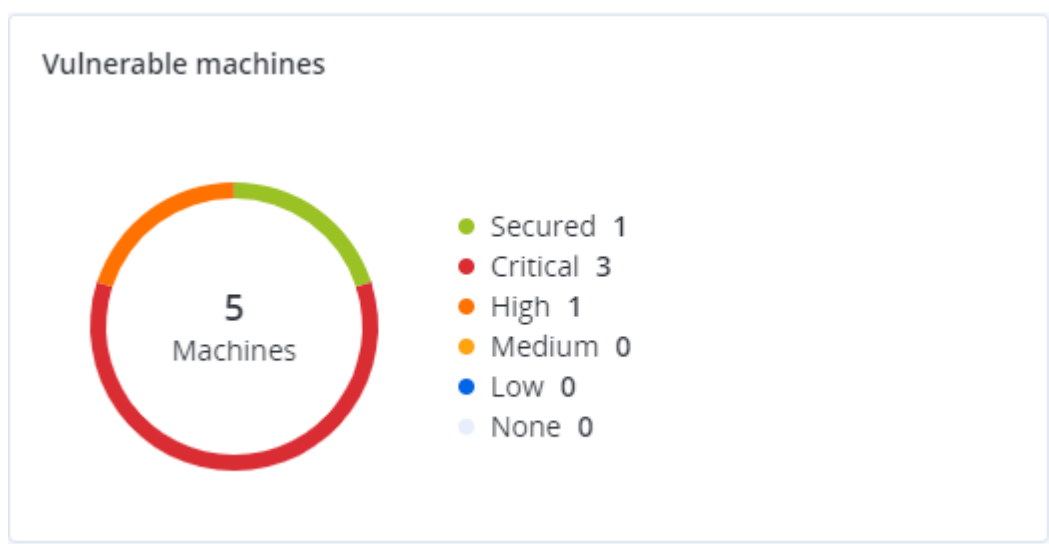
30.8 弱點評估桌面小工具

30.8.1 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



30.8.2 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。

Machine name	Vendor	Product	Vulnerability name/ID	Severity ↓	Last detected	First detected	⚙
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSC	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
More							

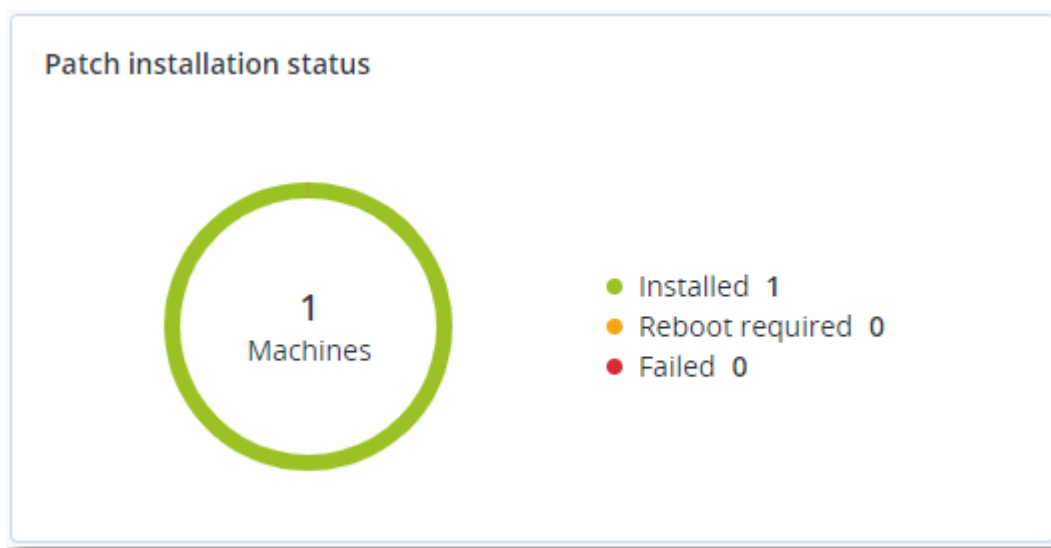
30.9 修補程式安裝桌面小工具

有四個與修補程式管理功能相關的桌面小工具。

30.9.1 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



30.9.2 修補程式安裝摘要

此桌面小工具會在電腦上顯示依修補程式安裝狀態排列的修補程式摘要。

Patch installation summary							
Installation status	Total number of machines	Total number of updates	Microsoft updates	Application updates	Critical severity	High severity	Medium severity
Installed	1	2	1	1	2	0	0

30.9.3 修補程式安裝歷史記錄

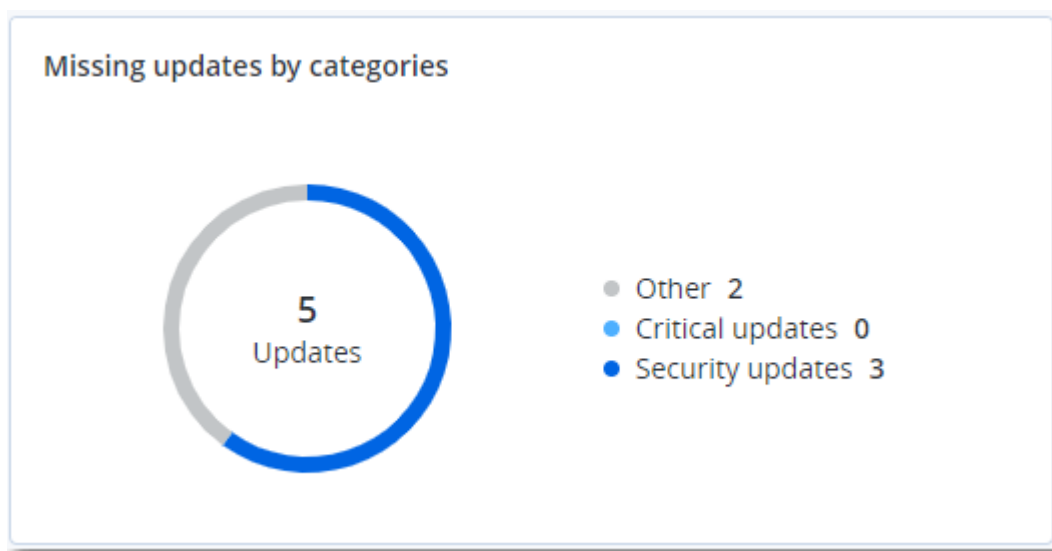
此桌面小工具會顯示電腦上修補程式的詳細資訊。

Patch installation history							
Machine name	Update name	Version	Severity	Approval status	Installation status	Installation date	
NIKITATIKHOC4E5	FastStone Soft FastStone I...	5.9	Medium	New	Installed	02/05/2020	
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020	
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020	
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020	
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020	
NIKITATIKHOC4E5	Oracle Java Runtime Envir...	8.0.2410.7	High	New	Failed	02/04/2020	
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020	
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020	
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020	
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020	

30.9.4 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



30.10 備份掃描詳細資料

此桌面小工具會顯示備份中偵測到之威脅的詳細資訊。

Device name	Plan name	Backup Date and time	Contents type	Location	Threat name	Affected files	Date and time	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\server\share\...	Gen.Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:40 AM	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\server\share\...	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\server\share\...	Gen.Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:45 AM	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\server\share\...	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\server\share\...	Gen.Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:50 AM	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\server\share\...	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\server\share\...	Gen.Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:10 PM	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\server\share\...	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\server\share\...	Gen.Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:33 PM	
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	\\server\share\...	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:33 PM	

30.11 最近受影響

此桌面小工具會顯示受到病毒、惡意程式碼和勒索軟體之類威脅影響的工作負載的詳細資訊。您可以找到的相關資訊包括偵測到的威脅、偵測到威脅的時間，以及受感染檔案數目。

Recently affected					
Machine name	Protection plan	Threat	Affected files	Detection time	
Ubuntu_14.04_x64-1	Total protection	Adware.DealPlyIgen2	15	27.12.2	Folder
Ubuntu_14.04_x64-1	Protection plan	Bloodhound.MalMacroIgen1	274	27.12.2	Customer
dc_w2k12_r2	Protection plan	Backdoor:Win32/Caphaw...	13	27.12.2	✓ Machine name
Win2012_r2-Hyper-V	Protection plan	W97M.DownloaderIgen32	5	27.12.2	✓ Protection plan
HyperV_for12A	Total protection	Miner.XMRigIgen1	68	27.12.2	Detected by
vm-sql_2012	Total protection	Backdoor:Win32/Caphaw...	61	27.12.2	✓ Threat
vm-sql_2012	Protection plan	Adware.DealPlyIgen2	9	27.12.2	File name
MF_2012_R2	Total protection	MSH.DownloaderIgen8	73	27.12.2	File path
MF_2012_R2	Total protection	Bloodhound.MalMacroIgen1	182	27.12.2	✓ Affected files
MF_2012_R2	Protection plan	Bloodhound.MalMacroIgen1	18	27.12.2	✓ Detection time
ESXirestore	Protection plan	MSH.DownloaderIgen8	682	27.12.2017 11:23 AM	
MF_2012_R2	Protection plan	Miner.XMRigIgen1	13	27.12.2017 11:23 AM	
Ubuntu_14.04_x64-1	Total protection	Adware.DealPlyIgen2	3	27.12.2017 11:23 AM	
Win2012_r2-Hyper-V	Total protection	W97M.DownloaderIgen32	27	27.12.2017 11:23 AM	

30.11.1 下載最近受影響工作負載的資料

您可以下載最近受影響工作負載的資料、產生 CSV 檔案，然後將其傳送給您指定的收件者。

若要下載最近受影響工作負載的資料

1. 在 **[最近受影響]** 桌面小工具中，按一下 **[下載資料]**。
2. 在 **[時間期限]** 欄位中，輸入您要下載資料的天數。您可以輸入的天數上限為 200。
3. 在 **[收件者]** 欄位中，輸入將收到電子郵件的所有人員的電子郵件地址，且電子郵件中會包含用於下載 CSV 檔案的連結。
4. 按一下 **[下載]**。

系統會使用您指定的時間期限內受影響工作負載的資料，開始產生 CSV 檔案。當 CSV 檔案完成時，系統會傳送一封電子郵件給收件者。接著，每個收件者都可以下載 CSV 檔案。

30.12 雲端應用程式

此桌面小工具會顯示雲端對雲端資源的詳細資訊：

- Microsoft 365 使用者 (信箱、OneDrive)
- Microsoft 365 群組 (信箱、群組網站)
- Microsoft 365 公用資料夾
- Microsoft 365 網站集合
- Microsoft 365 Teams
- Google Workspace 使用者 (Gmail、Google 雲端硬碟)
- Google Workspace 共用磁碟機

Cloud applications					 
Device name	Protection status 	Last successful backup	Next backup	Number of backups	
 HR - Onboarding	 OK	06/17/2020 10:48 AM	06/18/2020 7:34 AM	1	
 Sales and Marketing	 OK	06/17/2020 10:49 AM	06/18/2020 4:48 AM	1	
 HR Leadership Team	 OK	06/17/2020 10:48 AM	06/18/2020 6:51 AM	1	
 Retail	 OK	06/17/2020 10:47 AM	06/18/2020 2:53 AM	1	
 Contoso	 OK	06/17/2020 10:47 AM	06/17/2020 3:23 PM	1	
 U.S. Sales	 OK	06/17/2020 10:48 AM	06/18/2020 3:30 AM	1	
 IT	 OK	06/17/2020 10:48 AM	06/17/2020 10:35 PM	1	
 Mark 8 Project Team	 Warning	06/17/2020 10:49 AM	06/18/2020 3:06 AM	1	
 Finance	 OK	06/17/2020 10:47 AM	06/17/2020 4:38 PM	1	
 Sales	 Warning	06/17/2020 10:47 AM	06/17/2020 2:06 PM	1	
More					

有關雲端對雲端資源的其他資訊也可以在下列桌面小工具中取得：

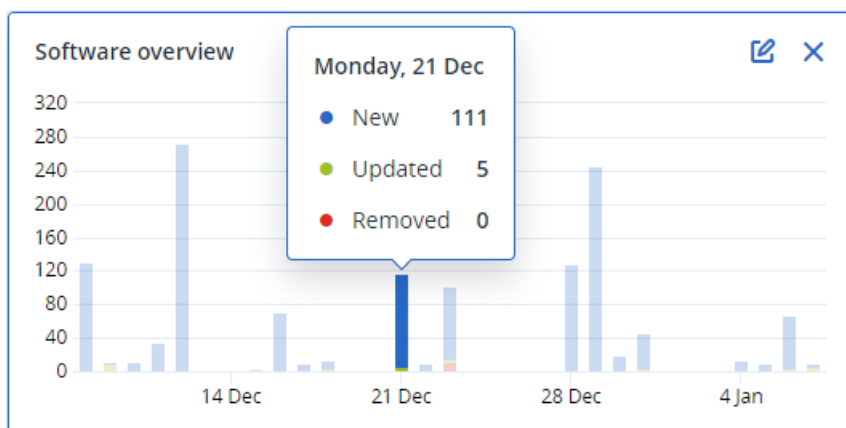
- 活動
- 活動清單
- 5 個最新的警示
- 警示歷程記錄
- 作用中警示摘要
- 歷史警示摘要
- 作用中警示詳細資訊
- 位置摘要

30.13 軟體清查桌面小工具

[軟體清查] 表格桌面小工具會顯示安裝在組織中 Windows 和 macOS 裝置上的所有軟體的詳細資訊。

Software inventory										
Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User	
 Ivelins-Mac-mini-2.local										
Ivelins-Mac-mini-2.local	-	15.0.26046	-	No change	-	12/12/2020, 9:26 AM	12/14/2020, 10:24 AM	/Library/Application Supp...	root	
Ivelins-Mac-mini-2.local	-	5989	Apple	No change	-	12/04/2020, 10:59 AM	12/14/2020, 10:24 AM	/Applications/Pages.app	root	
Ivelins-Mac-mini-2.local	-	5989	Apple	No change	-	12/04/2020, 10:59 AM	12/14/2020, 10:24 AM	/Applications/Keynote.app	root	
Ivelins-Mac-mini-2.local	-	5989	Apple	No change	-	12/04/2020, 10:59 AM	12/14/2020, 10:24 AM	/Applications/Numbers.a...	root	
Ivelins-Mac-mini-2.local	Canon iJScanner2	4.0.0	Canon Inc. (XE2XNRRXZ5)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Image Capture/D...	root	
Ivelins-Mac-mini-2.local	Canon iJScanner4	4.0.0	Canon Inc. (XE2XNRRXZ5)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Image Capture/D...	root	
Ivelins-Mac-mini-2.local	Canon iJScanner6	4.0.0	Canon Inc. (XE2XNRRXZ5)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Image Capture/D...	root	
Ivelins-Mac-mini-2.local	commandFilter	1.71	EPSON (TXAEAVSRN4)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Printers/EPSONV...	root	
Ivelins-Mac-mini-2.local	Cyber Protect Agent Assis...	1	Acronis International Gm...	No change	-	12/12/2020, 10:01 AM	12/14/2020, 10:24 AM	/Applications/Utilities/Cy...	root	
Ivelins-Mac-mini-2.local	Cyber Protect Agent Unin...	1	Acronis International Gm...	No change	-	12/12/2020, 9:28 AM	12/14/2020, 10:24 AM	/Library/Application Supp...	root	
More										

[軟體概觀] 桌面小工具會顯示指定的期間 (7 天、30 天或當月), 組織中 Windows 和 macOS 裝置上新的、已更新和已刪除的應用程式的數目。



當您將滑鼠暫留在圖表上的某一列時，就會顯示包含下列資訊的工具提示：

新的 - 新安裝的應用程式的數目。

已更新 - 已更新的應用程式的數目。

已移除 - 已移除的應用程式的數目。

當您按一下某個狀態列的部分時，就會將您重新導向至 **[軟體管理]** -> **[軟體清查]** 頁面。系統會針對對應的日期和狀態，篩選頁面中的資訊。

30.14 硬體清查桌面小工具

[硬體清查] 和 **[硬體詳細資料]** 表格桌面小工具會顯示安裝在組織中實體與虛擬 Windows 和 macOS 裝置上的所有硬體的相關資訊。

Hardware inventory												
Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard serial	BIOS version	Domain	Registered owner	Registered organization	Scan date and time
Ivelins-Mac-mini-2.local	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User	Acronis Inc.	12/14/2020 10:23 AM
00003079.corp...	Microsoft Windows	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User	Acronis Inc.	12/13/2020 8:18 PM

Hardware details						
Machine name	Hardware category	Hardware name	Hardware details	Manufacturer	Status	Scan date
Ivelins-Mac-mini-2.local	Motherboard	Macmini8,1	Mac-7BA5B2DFE22DD08C	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Ethernet	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Wi-Fi	IEEE80211, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Bluetooth PAN	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 1	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 2	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 3	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 4	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt Bridge	Bridge, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Disk	disk1	APPLE SSD AP0256M, SSD, 250685575...	-	-	12/14/2020, 10:23 AM

[硬體變更] 表格桌面小工具會顯示指定的期間 (7 天、30 天或當月)，組織中實體與虛擬 Windows 和 macOS 裝置上新增、移除和變更的硬體的相關資訊。

Hardware changes						
Machine name	Hardware category	Status	Old value	New value	Modification date and time 	
▼ DESKTOP-0FF9TTF						
DESKTOP-0FF9TTF	Network adapter	Changed	Oracle Corporation, Ethernet 802.3,...	Oracle Corporation, Ethernet 802.3, ...	01/11/2021 9:28 AM	
DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor Corp., Ether...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Toronto 5C1, PF0PJB10	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), WDC WD10JP...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 802.3, 00:0...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ethernet 802.3, ...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00 GB	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows Provider V9...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM	
More						

31 報告

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

關於操作的報告可能包括任何一組儀表板桌面小工具。所有桌面小工具都會顯示整個公司的摘要資訊。

根據桌面小工具類型，報告包含時間範圍和瀏覽或報告產生時的資料。請參閱 "根據桌面小工具類型回報的資料" (第 557 頁)。

所有歷史桌面小工具都會顯示相同時間範圍的資料。您可在報告設定中變更此範圍。

您可以使用預設報告或建立自訂報告。

預設報告的集合取決於您所擁有的 Cyber Protection 服務版本。預設報告如下所列：

報告名稱	描述
依電腦分類的 #CyberFit 分數	根據每部電腦的安全指標和設定的評估，顯示 #CyberFit 分數以及改進的建議。
警示	顯示指定期間發生的警示。
備份掃描詳細資料	顯示備份中偵測到的威脅的詳細資訊。
每日活動	顯示指定期間所執行活動的摘要資訊。
資料保護圖	顯示電腦上所有重要檔案之數目、大小、位置、保護狀態的詳細資訊。
偵測到的威脅	按照遭封鎖的威脅數目，以及狀況良好與易受攻擊電腦的數目，顯示受影響電腦的詳細資料。
探索到的電腦	顯示組織網路中所有找到的電腦。
磁碟健全狀況預測	顯示 HDD/SSD 故障時間的預測以及目前的磁碟狀態。
現有的弱點	顯示組織中作業系統和應用程式現有的弱點。此報告也會針對網路中所列出的每個產品，顯示受影響電腦的詳細資料。
軟體清查	顯示安裝在公司裝置上的軟體的相關資訊。
硬體清查	顯示適用於公司裝置上的硬體的相關資訊。
修補程式管理摘要	顯示遺漏的修補程式數目、已安裝的修補程式數目，以及適用的修補程式數目。您可以向下鑽研報告以取得遺漏/已安裝的修補程式資訊，以及所有系統的詳細資料。
摘要	顯示指定期間受保護裝置的摘要資訊。
每週各項活動	顯示指定期間所執行活動的摘要資訊。

若要檢視報告，請按一下其名稱。

若要存取有報告的操作，請按一下報告行上的省略符號圖示。從報告內也可以使用相同操作。

31.0.1 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，請按一下 **[自訂]**、按一下報告名稱 (預設指定的名稱看起來像 **[Custom (1)]**)，然後新增動態小工具到報告。
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。

31.0.2 編輯報告

若要編輯報告，請按一下其名稱，然後按一下 **[設定]**。在編輯報告時，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。

General

Name

Backup scanning details

☐ Set one tenant for all widgets

Range

7 days

Scheduled



Recipients

user1@example.com; user2@example.com

File format

Excel and PDF

Language

English

Days of week

Monthly

SUN

MON

TUE

WED

THU

FRI

SAT

Send at

12:00 AM

31.0.3 排程報告

1. 按一下報告名稱, 然後按一下 **[設定]**。
2. 啟用 **[排程]** 開關。
3. 指定收件者的電子郵件地址。
4. 選取報告格式: .pdf、.xlsx 或兩者。

5. 選取要傳送報告的日期和時間。
6. 按一下右上角的 **【儲存】**。

注意事項

在 .pdf 檔案中匯出的項目數目上限為 1000; 在 .xlsx 檔案中為 10000。

31.0.4 匯出和匯入報告結構

您可將報告結構 (動態小工具集和報告設定) 匯出及匯入 .json 檔案中。

若要匯出報告結構, 請按一下報告名稱、按一下右上角的省略符號圖示, 然後按一下 **【匯出】**。

要匯入報告結構, 請按一下 **【新增報告】**, 然後按一下 **【匯入】**。

31.0.5 下載報告

您可以下載報告, 方法是, 按一下 **【下載】**, 然後選擇所需的格式:

- Excel 和 PDF
- Excel
- PDF

31.0.6 傾印報告資料

您可將傾印報告資料以 .csv 檔案透過電子郵件傳送。傾印包括所有自訂時間範圍的報告資料 (不篩選)。CSV 報告中的時間戳記採用 UTC 格式, 而在 Excel 和 PDF 報告中, 時間戳記則採用目前的系統時區。

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. 按一下報告名稱。
2. 按一下右上角的省略符號圖示, 然後按一下 **【傾印資料】**。
3. 指定收件者的電子郵件地址。
4. 在 **時間範圍** 中, 指定時間範圍。
5. 按一下 **【傳送】**。

注意事項

在 .csv 檔案中匯出的項目數目上限為 150000。

31.1 根據桌面小工具類型回報的資料

根據所顯示的資料範圍, 儀表板上的桌面小工具有兩種類型:

- 顯示瀏覽或報告產生時實際資料的桌面小工具。
- 顯示歷史資料的桌面小工具。

當您在報告設定中，將資料範圍設定為特定期間的傾印資料時，所選時間範圍僅適用於顯示歷史資料的桌面小工具。若是顯示瀏覽時實際資料的桌面小工具，則時間範圍參數不適用。

下表列出可用的桌面小工具及其資料範圍。

桌面小工具名稱	顯示在桌面小工具和報告中的資料
依電腦分類的 #CyberFit 分數	實際
5 個最新的警示	實際
作用中警示詳細資訊	實際
作用中警示摘要	實際
活動	歷史報告
活動清單	歷史報告
警示歷程記錄	歷史報告
攻擊手法統計資料	歷史報告
備份掃描詳細資料 (威脅)	歷史報告
備份狀態	歷史 - 在 [執行總計] 和 [成功執行的數量] 欄中 實際 - 在其他所有欄中
已封鎖的 URL	實際
雲端應用程式	實際
Cyber protection	實際
資料保護圖	歷史報告
裝置	實際
探索到的電腦	實際
磁碟健全狀況概觀	實際
實體裝置的磁碟健全狀況狀態	實際
現有的弱點	歷史報告
硬體變更	歷史報告
硬體詳細資料	實際
硬體清查	實際
歷史警示摘要	歷史報告
事件嚴重性歷程記錄	歷史報告

位置摘要	實際
遺漏的更新 (依類別)	實際
未保護	實際
修補程式安裝歷史記錄	歷史報告
修補程式安裝狀態	歷史報告
修補程式安裝摘要	歷史報告
保護狀態	實際
最近受影響	歷史報告
安全性事件待執行工作	歷史報告
安全性事件 MTTR	歷史報告
軟體清查	實際
軟體概觀	歷史報告
威脅狀態	實際
易受攻擊的電腦	實際
工作負載網路狀態	實際

32 內部部署管理伺服器的授權管理

如需有關如何啟用內部部署管理伺服器或如何為其配置授權的詳細資訊，請參閱 [Cyber Protect 使用指南](#) 中的「授權」一節。

33 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. 選擇您要收集記錄檔的來源電腦。
2. 按一下 **[活動]**。
3. 按一下 **[收集系統資訊]**。
4. 如果 Web 瀏覽器出現提示，請指定要儲存檔案的位置。

34 附錄 A. 站台對站台 OpenVPN - 其他資訊

當您建立復原伺服器時，您要設定其在**實際執行網路**中的 IP 位址及其**測試 IP 位址**。

執行容錯移轉 (在雲端執行虛擬機器)，並登入虛擬機器檢查伺服器的 IP 位址之後，您會看到**實際執行網路**中的 IP 位址。

當您執行測試容錯移轉時，只有使用僅能在復原伺服器設定中看到的**測試 IP 位址**，才能連線測試伺服器。

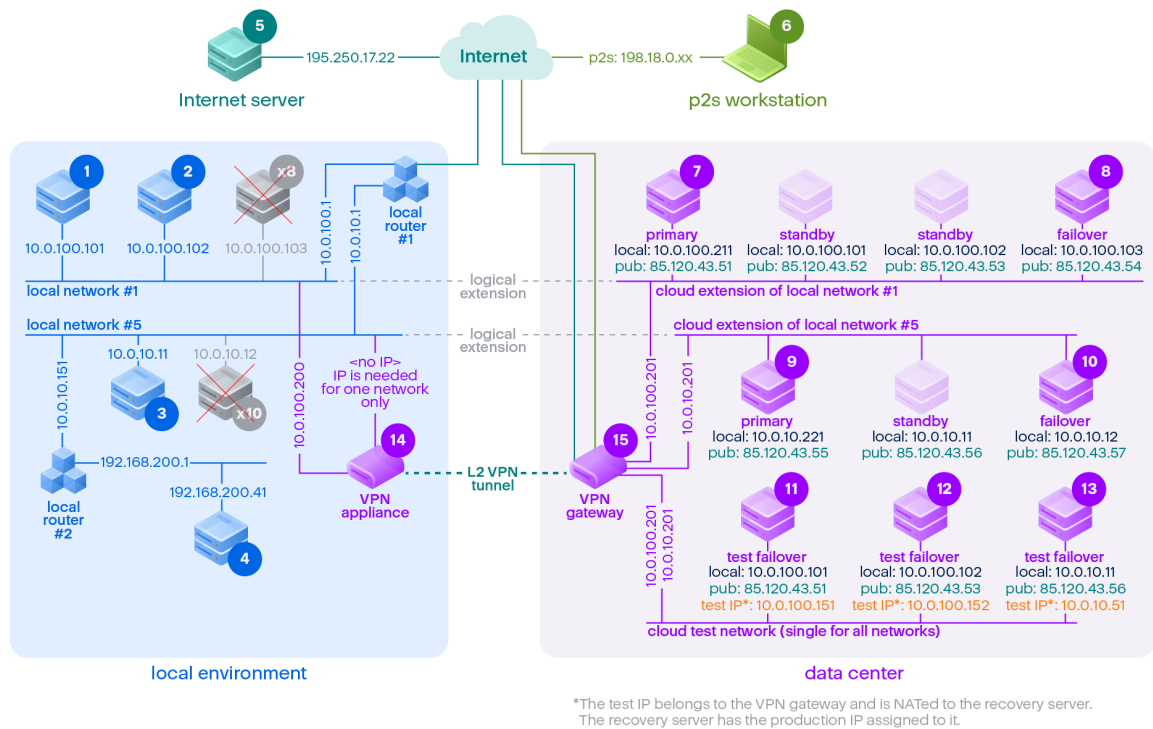
若要從本機站台連線測試伺服器，您必須使用**測試 IP 位址**。

注意事項

伺服器的網路設定一律會顯示**實際執行網路**中的 IP 位址 (因為測試伺服器會鏡像實際執行伺服器的外觀)。發生這種情況是因為測試 IP 位址不屬於測試服務器，而是屬於 VPN 閘道，而且會使用 NAT 轉換為實際執行 IP 位址。

下圖顯示站台對站台 OpenVPN 設定的範例。本機環境中的部分伺服器會使用容錯移轉復原到雲端 (當網路基礎架構正常時)。

1. 客戶透過下列方式啟用 Disaster Recovery:
 - a. 設定 VPN 設備 (14)，然後將其連線至雲端 VPN 伺服器 (15)
 - b. 使用 Disaster Recovery (1、2、3、x8 和 x10) 保護部分本機伺服器
本機站台上的部分伺服器 (如 4) 連線至未連線到 VPN 設備的網路。這類伺服器沒有受到 Disaster Recovery 保護。
2. 部分伺服器 (已連線到不同的網路) 在本機站台運作：(1、2、3 和 4)
3. 受保護的伺服器 (1、2 和 3) 正在使用測試容錯移轉 (11、12 和 13) 進行測試
4. 本機站台中的一部分伺服器無法使用 (x8、x10)。執行容錯移轉之後，這些伺服器變得可在雲端使用 (8 和 10)
5. 連線至不同網路的部分主要伺服器 (7 和 9) 可在雲端環境中使用
6. (5) 是網際網路中擁有公用 IP 位址的伺服器
7. (6) 是使用站台對站台 VPN 連線 (p2s) 連線至雲端的工作站



在此範例中，下列連線設定可用於 (例如, "ping") **[來源:]** 列中的伺服器到 **[目的地:]** 欄中的伺服器。

	至:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
從:		本機	本機	本機	本機	網際網路	p2s	主要	容錯移轉	主要	容錯移轉	測試容錯移轉	測試容錯移轉	測試容錯移轉	VPN設備	VPN伺服器
1	本機	直接	透過本機路由器1	透過本機路由器2	透過本機路由器1和網際網路	否	透過通道: 本機	透過通道: 本機	透過通道: 本機	透過通道: 本機	透過通道: 本機	透過通道: NAT (VPN伺服器)	透過通道: NAT (VPN伺服器)	透過本機路由器和通道: NAT (VPN伺服器)	直接	否

	至:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
														ub		
2	本機	直接		透過本機路由器 1	透過本機路由器 2	透過本機路由器 1 和網際網路	否	透過通道: 本機透過本機路由器 1 和網際網路:p ub	透過通道: 本機透過本機路由器 1 和網際網路:p ub	透過通道: 本機透過本機路由器 1 和網際網路:p ub	透過通道: 本機透過本機路由器 1 和網際網路:p ub	透過通道:N AT (VPN 伺服器) 透過本機路由器 1 和網際網路:p ub	透過通道:N AT (VPN 伺服器) 透過本機路由器 1 和網際網路:p ub	透過本機路由器 1 和通道:N AT (VPN 伺服器) 透過本機路由器 1 和網際網路:p ub	直接	否
3	本機	透過本機路由器 1	透過本機路由器 1		透過本機路由器 2	透過本機路由器 1 和網際網路	否	透過通道: 本機透過本機路由器 1 和網際網路:p ub	透過通道: 本機透過本機路由器 1 和網際網路:p ub	透過通道: 本機透過本機路由器 1 和網際網路:p ub	透過通道: 本機透過本機路由器 1 和網際網路:p ub	透過通道:N AT (VPN 伺服器) 透過本機路由器 1 和網際網路:p ub	透過通道:N AT (VPN 伺服器) 透過本機路由器 1 和網際網路:p ub	透過本機路由器 1 和通道:N AT (VPN 伺服器) 透過本機路由器 1 和網際網路:p ub	透過本機路由器	否
4	本機	透過本機路	透過本機路	透過本機路		透過本機路	否	透過本機路由器 2 和通	透過本機路由器 2 和通	透過本機路由器 2 和通	透過本機路由器 2 和通	透過通道:N AT (VPN	透過通道:N AT (VPN	透過通道:N AT (VPN	透過本機路	否

	至:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		由器 2 和路由器 1	由器 2 和路由器 1	由器 2		由器 2 和路由器 1 和網際網路		道：本機 透過本機 路由器 2 和本機 路由器 1 和網際 網路：pub	道：本機 透過本機 路由器 2 和本機 路由器 1 和網際 網路：pub	道：本機 透過本機 路由器 2 和本機 路由器 1 和網際 網路：pub	道：本機 透過本機 路由器 2 和本機 路由器 1 和網際 網路：pub	伺服器) 透過本機 路由器 2 和路 由器 1 和網際 網路：pub	伺服器) 透過本機 路由器 2 和路 由器 1 和網際 網路：pub	伺服器) 透過本機 路由器 2 和路 由器 1 和網際 網路：pub	由器 2	
5	網際網路	否	否	否	否		不適用	透過網際 網路：pub	透過網際 網路：pub	透過網際 網路：pub	透過網際 網路：pub	透過網際 網路：pub	透過網際 網路：pub	透過網際 網路：pub	否	否
6	p2s	否	否	否	否	透過網際 網路		透過 p2s VPN (VPN 伺服器): 本機 透過網際 網路：pub	透過 p2s VPN (VPN 伺服器): 本機 透過網際 網路：pub	透過 p2s VPN (VPN 伺服器): 本機 透過網際 網路：pub	透過 p2s VPN (VPN 伺服器): 本機 透過網際 網路：pub	透過 p2s VPN - NAT (VPN 伺服器) 透過網際 網路：pub	透過 p2s VPN - NAT (VPN 伺服器) 透過網際 網路：pub	透過 p2s VPN - NAT (VPN 伺服器) 透過網際 網路：pub	否	否
7	主要	透過通道	透過通道	透過通道	透過通道	透過網際 網路 (透過 VPN 伺	否		在雲端直接： 本機	透過通道 和本機路 由器 1: 本 機	透過通道 和本機路 由器 1: 本 機	透過 VPN 伺 服器: NAT	透過 VPN 伺 服器: NAT	透過 通道 和本機路 由器 1: NAT	否	僅限 DHCP 和 DNS 通訊 協定

	至:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
					和 2	服 器)										
8	容 錯 移 轉	透 過 通 道	透 過 通 道	透 過 通 道 和 本 機 路 由 器 1	透 過 通 道 和 本 機 路 由 器 1 和 2	透 過 網 際 網 路 (透 過 VP N 伺 服 器)	否	在 雲 端 直 接: 本 機		透 過 通 道 和 本 機 路 由 器 1:本 機	透 過 通 道 和 本 機 路 由 器 1:本 機	透 過 VPN 伺 服 器:N AT	透 過 VPN 伺 服 器:N AT	透 過 通 道 和 本 機 路 由 器 1:NA T	否	僅 限 DH CP 和 DNS 通 訊 協 定
9	主 要	透 過 通 道 和 本 機 路 由 器 1	透 過 通 道 和 本 機 路 由 器 1	透 過 通 道	透 過 通 道	透 過 網 際 網 路 (透 過 VP N 伺 服 器)	否	透 過 通 道 和 本 機 路 由 器 1:本 機	透 過 通 道 和 本 機 路 由 器 1:本 機		在 雲 端 直 接: 本 機	透 過 通 道 和 本 機 路 由 器 1:NA T	透 過 通 道 和 本 機 路 由 器 1:NA T	透 過 VPN 伺 服 器:N AT	否	僅 限 DH CP 和 DNS 通 訊 協 定
10	容 錯 移 轉	透 過 通 道 和 本 機 路 由 器 1	透 過 通 道 和 本 機 路 由 器 1	透 過 通 道	透 過 通 道	透 過 網 際 網 路 (透 過 VP N 伺 服 器)	否	透 過 通 道 和 本 機 路 由 器 1:本 機	透 過 通 道 和 本 機 路 由 器 1:本 機	在 雲 端 直 接: 本 機		透 過 通 道 和 本 機 路 由 器 1:NA T	透 過 通 道 和 本 機 路 由 器 1:NA T	透 過 VPN 伺 服 器:N AT	否	僅 限 DH CP 和 DNS 通 訊 協 定
11	測	否	否	否	否	透	否	否	否	否	否		在 雲 端 直	透 過	否	僅

	至:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	試容錯移轉					過網際網路(透過VPN伺服器)							接：本機	VPN伺服器：本機(路由)		限DHCP和DNS通訊協定
12	測試容錯移轉	否	否	否	否	透過網際網路(透過VPN伺服器)	否	否	否	否	否	在雲端直接：本機		透過VPN伺服器：本機(路由)	否	僅限DHCP和DNS通訊協定
13	測試容錯移轉	否	否	否	否	透過網際網路(透過VPN伺服器)	否	否	否	否	否	透過VPN伺服器：本機(路由)	透過VPN伺服器：本機(路由)		否	僅限DHCP和DNS通訊協定
14	VPN設備	直接	直接	透過本機路	透過本機路	透過網際網路	否	否	否	否	否	否	否	否		否

	至:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
				由 器 1	由 器 2	路 (本 機 路 由 器 1)										
15	VP N 伺 服 器	否	否	否	否	否	否	否	否	否	否	否	否	否	否	

辭彙表

R

Runbook

[災難復原] 計劃的案例，其中包含可自動執行災難復原動作的可設定步驟。

U

USB 裝置資料庫

[裝置控制] 裝置控制模組會維護 USB 裝置的資料庫，您可以從該資料庫中，將 USB 裝置新增到裝置存取控制的排除清單。此資料庫會依裝置 ID 登錄 USB 裝置，您可以手動輸入或從服務主控台中的已知裝置選取。

V

VPN 設備

[災難復原] 特殊的虛擬機器，可透過安全的 VPN 通道，在區域網路和雲端站台之間連線。VPN 設備是在本機站台上部署的。

VPN 閘道 (前身為 VPN 伺服器或連線閘道)

[災難復原] 特殊的虛擬機器，可透過安全的 VPN 通道，提供本機站台和雲端站台網路間的連線。VPN 閘道是在雲端站台上部署的。

公

公共 IP 位址

[災難復原] 讓雲端伺服器可以從網際網路使用所需的 IP 位址。

主

主要伺服器

[災難復原] 在本機站台 (例如，復原伺服器) 上沒有連結電腦的虛擬機器。主要伺服器用於保

護應用程式或執行各種輔助服務 (例如，網頁伺服器)。

本

本機站台

[災難復原] 在公司內部部署上部署的本機基礎架構。

完

完整備份

包含已選要備份的所有資料的獨立備份。您無需存取任何其他備份來從完整備份復原資料。

孤

孤立備份

孤立備份是與保護計劃不再有關聯的備份。

保

保護代理程式

保護代理程式是要安裝在電腦上以保護資料的代理程式。

保護計劃

保護計劃是一種結合資料保護模組的計劃，包括備份、防毒和反惡意程式碼保護、URL 篩選、Windows Defender 防毒軟體、Microsoft Security Essentials、弱點評估、修補程式管理、資料保護圖、裝置控制。

容

容錯回復

將工作負載從備用伺服器 (例如，虛擬機器複本或在雲端執行的復原伺服器) 切換回實際執行

伺服器。

容錯移轉

將工作負載從實際執行伺服器切換到備用伺服器 (例如, 虛擬機器複本或在雲端執行的復原伺服器)。

差

差異備份

差異備份能對照最新的完整備份, 儲存資料的變更。您需要存取相對應的完整備份, 以從差異備份復原資料。

站

站台對站台 (S2S) 連線

[災難復原] 將區域網路透過安全的 VPN 通道延伸至雲端的連線。

備

備份集

可套用個別保留規則的一組備份。如果是 [自訂] 備份配置, 備份集會對應備份方法 ([完整]、[差異] 與 [增量])。在其他所有案例中, 備份集為 [每月]、[每日]、[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]) 選擇的那一天所建立的第一個備份。如果每週備份指的是每月一開始所建立的第一個備份, 則此備份會被視為每月備份。在此情況下, 每週備份將會在下一週選擇的那天建立。除非此備份落在每月或每週備份的定義範圍內, 否則每日備份指的是每日一開始所建立的第一個備份。除非此備份落在每月、每週或每日備份的定義範圍內, 否則每小時備份指的是每小時一開始所建立的第一個備份。

單

單一檔案備份格式

備份格式, 會將初始完整備份及後續增量備份儲存為單一的 .tibx 檔案。此格式可以善用了增量備份方法的速度, 同時避免其主要的缺點 - 不容易刪除過期備份。軟體會將過期備份所使用的區塊標示為「可用」, 並在區塊中寫入新備份。結果會以耗費最少資源的方式, 產生極快速的清理。備份至不支援隨機存取讀寫的位置時, 無法使用單一檔案備份格式。

復

復原伺服器

[災難復原] 原始電腦的 VM 複本, 以儲存在雲端的受保護伺服器備份為基礎。復原伺服器在發生災難時, 用於從原始伺服器切換工作負載。

復原點目標 (RPO)

[災難復原] 因電力中斷而遺失的資料量, 以計劃的電力中斷或災難事件發生的時間量計算。RPO 閾值會定義上次適合容錯移轉的復原點和目前時間之間允許的最大時間間隔。

最

最終化

將從備份執行的臨時虛擬機器變成永久虛擬機器的作業。實際上, 這表示將所有虛擬機器磁碟, 以及在電腦執行時發生的變更, 復原至儲存這些變更的資料存放區。

測

測試 IP 位址

[災難復原] 測試容錯移轉時所需的 IP 位址, 可防止實際執行 IP 位址重複。

測試網路

[災難復原] 隔離的虛擬網路，用於測試容錯移轉程序。

虛

虛擬機器

外部代理程式 (例如 VMware 用代理程式或 Hyper-V 用代理程式) 在 Hypervisor 層級備份的虛擬機器。從備份觀點來看，內部具有代理程式的虛擬機器會被視為實體機器。

雲

雲端伺服器

[災難復原] 復原或主要伺服器的一般參考。

雲端站台 (或 DR 網站)

[災難復原] 在雲端託管並用於執行復原基礎架構的遠端站台 (萬一發生災難)。

裝

裝置控制模組

裝置控制模組運用每個受保護電腦上的資料洩漏防禦代理程式功能子集，偵測並防止本機電腦通道上未經授權的資料存取和傳輸，作為保護計劃的一部分。這些包括使用者對週邊裝置和連接埠的存取、文件列印、剪貼簿複製/貼上作業、媒體格式化和退出作業，以及與本機連線行動裝置的同步。裝置控制模組對允許使用者在受保護的電腦上存取的裝置和連接埠的類型，以及使用者可以在這些裝置上執行的動作，提供精細的情境控制。

資

資料洩漏防禦 (先前稱為資料外洩防禦)

一種整合式技術和組織措施的系統，旨在偵測和防止組織內外部未經授權的實體有意和無意

地洩露/存取機密、受保護或敏感的資料，或將此類資料傳輸到不受信任的環境。

資料洩漏防禦代理程式

資料洩漏防禦系統的用戶端元件，可透過套用環境和內容分析技術的組合，並強制執行集中管理的資料洩漏防禦政策，保護其主機電腦，免於未經授權者使用、傳輸和儲存機密、受保護或敏感的資料。網路保護提供一個功能全面的資料洩漏防禦代理程式。但是，代理程式在受保護電腦上的功能受限於網路保護授權使用的一組資料洩漏防禦功能，並取決於套用至該電腦的保護計劃。

實

實際執行網路

[災難復原] 透過 VPN 通道延伸，並涵蓋本機和雲端站台的內部網路。本機伺服器和雲端伺服器可以在實際執行網路中彼此通訊。

實體電腦

作業系統中所安裝之代理程式備份的電腦。

增

增量備份

這種備份能對照最新的備份，儲存資料的變更。您需要存取其他備份，以便從增量備份中復原資料。

模

模組

模組是保護計劃的一部分，可提供特定的資料保護功能，例如，備份模組、防毒和反惡意程式碼保護模組等等。

點

點對站台 (P2S) 連線

[災難復原] 使用端點裝置 (例如電腦或筆記型電腦), 從外部到雲端和本機站台進行的安全 VPN 連線。

驗

驗證

此作業會檢查從備份復原資料的可能性。驗證檔案備份會模擬將所有檔案從備份復原到虛擬目的地。磁碟備份的驗證作業會計算備份中所儲存之各資料區塊的檢查碼。這兩個程序都屬於資源密集型。儘管成功驗證代表成功復原的可能性很高, 但無法檢查影響復原過程的所有因素。

索引

#

#CyberFit 評分機制 137

.

...我想要變更第二要素裝置? 41

...我遺失了第二要素裝置? 41

[

[活動] 儀表板 539

[管理] 索引標籤 510

3

32 位元或 64 位元? 523

A

Active Protection 402

Active Protection 設定 402

autostart.json 的結構 527

C

calculate hash 194

CPU 優先順序 199

Cyber Backup Standard 中的 Active Protection
設定 411

Cyber Backup Standard 版本中的 Active
Protection 411

Cyber Backup 版本 17

Cyber Disaster Recovery Cloud 試用版產品 343

Cyber Protect 版本 17

Cyber Protect 監視器 30, 520

Cyber Protection 服務版本和子版本 17

D

Downloader 元件所需的連接埠 47

E

ESXi 虛擬機器的需求 242

Exchange 用代理程式 (適用於信箱備份) 26

Exchange 伺服器 [叢集] 概觀 246

F

File Sync & Share 用代理程式 26

Flashback 231

G

get content 194

Google Workspace 保護是什麼意思? 293

H

Hyper-V 用代理程式 29

Hyper-V 虛擬機器的需求 242

I

IP 位址重新設定 366

IPsec/IKE 安全性設定 361

L

Linux 148, 521

Linux 中的 Universal Restore 221

Linux 中的自動安裝或解除安裝 67

Linux 可開機媒體 523

Linux 用代理程式 27

Linux 的選擇規則 150

Linux 型或 WinPE/WinRE 型可開機媒體? 521

Linux 套件 48

Linux 電腦的弱點評估 453

list backups 193

list content 193

LVM 快照 196

M

Mac 148

Mac OS 的選擇規則 150

Mac 用代理程式 28

Mac 使用者注意事項 211

McAfee 端點加密和 PGP 全磁碟機加密 37

Microsoft 365 用代理程式 27, 268

Microsoft 365 授權報告 270

Microsoft Azure 和 Amazon EC2 虛擬機器 340

Microsoft BitLocker 磁碟機加密 37

Microsoft Defender 防毒軟體 422

Microsoft Defender 防毒軟體與 Microsoft Security Essentials 422

Microsoft Exchange Server 184

Microsoft Security Essentials 422

Microsoft SQL Server 183

Microsoft 產品 457

MySQL/MariaDB 用代理程式 27

O

oVirt 用代理程式 30

oVirt 用代理程式 – 所需角色和連接埠 104

oVirt/Red Hat Virtualization 4.2 和 4.3/Oracle Virtualization Manager 4.3 104

oVirt/Red Hat Virtualization 4.4 104

P

Plesk 和 cPanel 的整合 317

Proxy 伺服器設定 51

R

Runbook 的相關作業 398

S

Scale Computing HC3 用代理程式 30

Scale Computing HC3 用代理程式 – 必要角色 91

SID 變更 233

SQL Server高可用性解決方案概觀 245

SQL 用代理程式、Active Directory 用代理程式、Exchange 用代理程式 (適用於資料庫備份及應用程式感知備份) 26

Startup Recovery Manager 536

U

Universal Restore 設定 220

Universal Restore 程序 221

URL 421

URL 篩選 415

URL 篩選設定 417

URL 篩選設定工作流程 417

USB 裝置允許名單 502

USB 裝置資料庫 503

USB 裝置資料庫管理頁面 503

V

Virtuozzo Hybrid Infrastructure 用代理程式 29

Virtuozzo Hybrid Infrastructure 用代理程式 (虛擬裝置) 的網路需求 93

Virtuozzo 用代理程式 29

VM 電源管理 234, 325

VMware 用代理程式 - 不透過 LAN 備份 326

VMware 用代理程式 - 必要權限 334

VMware 用代理程式 (Windows) 29

VMware 用代理程式 (虛擬裝置) 29

VPN 設備 351

VPN 裝置的需求 357

VPN 閘道 351, 355

VPN 閘道網路設定 351

W

Windows 148

Windows OS 支援的第三方產品 450

Windows 中的 Universal Restore 220

Windows 中的自動安裝或解除安裝 61

Windows 用代理程式 25

Windows 事件日誌 209, 234

Windows 協力廠商產品 457

Windows 的選擇規則 149

WinPE 型和 WinRE 型可開機媒體 530

WinPE 影像 530

WinPE/WinRE 型 521

WinRE 影像 530

一

一般安裝規則 37

一般備份規則 37

一般需求 241

下

下載 Cyber Protection 代理程式 55

下載 IPsec VPN 記錄檔 376

下載 OpenVPN 的設定 373

下載報告 557

下載最近受影響工作負載的資料 550

工

工作失敗處理 207

工作開始條件 207

已

已知問題 310

已復原虛擬機器的高可用性 337

已標示為機密 444

不

不可變動儲存空間 487

不要在使用計量付費連線時開始 166

不要在連線至下列 Wi-Fi 網路時開始 167

中

中間快照 519

什

什麼是備份檔案? 178

什麼會觸發原則規則? 432

仍

仍要安裝的大型存放驅動程式 221

允

允許透過 L2 VPN 的 DHCP 流量 372

元

元件自動更新 113

內

內建群組 120

內部部署管理伺服器的授權管理 560

公

公司白名單 426

公共和測試 IP 位址 352

公證 173, 307

公證含鑑識資料的備份 190

分

分配演算法 330

分割 206

切

切換站台對站台連線類型 369

升

升級程序 292

升級雲端代理程式 292

反

反惡意程式碼功能 400

反惡意程式碼和 Web 保護 400

手

手動安裝套件 50

手動更新代理程式 107

手動核准修補程式 463

手動啟動備份 173

手動執行軟體清查掃描 465

手動執行硬體清查掃描 470

手動執行雲端對雲端備份 511

手動註冊電腦 74

手動新增至白名單 426

手動繫結 331

支

支付卡產業資料安全標準 (PCI DSS) 444

支援的 Apple 和協力廠商產品 451

支援的 Apple 產品 451

支援的 Linux 產品 451

支援的 MariaDB 版本 31

支援的 Microsoft Exchange Server 版本 30

支援的 Microsoft SharePoint 版本 30

支援的 Microsoft SQL Server 版本 30

支援的 Microsoft 和第三方產品 449

支援的 Microsoft 產品 449

支援的 MySQL 版本 31

支援的 Plesk 和 cPanel 版本 317

支援的 SAP HANA 版本 31

支援的目的地 153

支援的行動裝置 261

支援的位置 170, 512, 514-515

支援的作業系統 341

支援的作業系統和環境 25

支援的虛擬化平台 31, 342

支援的虛擬機器類型 517

支援的資料來源 153

支援的網頁瀏覽器 25

支援的適用於 macOS 的協力廠商產品 451

支援的檔案系統 38

支援的叢集組態 245, 247

支援虛擬機器移轉 332

支援語言 440-441, 444

主

主要功能 341

主要伺服器 354

主要伺服器的操作 391

代

代理程式的系統需求 45, 86, 88, 92, 100

以

以電腦屬性加密 171

加

加密 171

加密如何運作 172

加強安全性模式 485

包

包含特殊字元或空格的密碼 77

可

可以復原哪些項目？ 265, 271, 275, 280, 283, 286, 297, 301, 304

可備份的內容 261

可開機媒體 521

可開機媒體中的指令碼 525

可開機媒體的相關作業 535

可開機媒體組建 522

必

必要條件 78, 104, 108, 151, 241, 310, 318, 332, 359, 364, 376-377, 385, 389, 466, 468, 470, 472

必要條件：368, 371-372

本

本機站台的 VPN 存取 373

本機連線 534

正

正在停用代理程式的自動指派 331

正在部署 oVirt 用代理程式 (虛擬裝置) 100

正在部署 Scale Computing HC3 用代理程式 (虛擬裝置) 88

用

用於內容偵測的邏輯運算式 441, 443-444

用於日文之外所有支援的語言的邏輯運算式 443

用於日文的邏輯運算式 443

白

白名單設定 427

全

全文檢索 298

各

各 Device 群組 120

向

向 Notary Service 驗證檔案真實性 224, 308

在

在 Cyber Protection 服務中 270, 293

在 Google Workspace 中 293

在 Linux 中 52, 112

在 Linux 中安裝 Cyber Protection 代理程式 56

在 macOS 上啟用裝置控制模組 491

在 macOS 中 53, 112

在 macOS 中安裝 Cyber Protection 代理程式
58

在 macOS 中自動安裝和解除安裝 72

在 Microsoft 365 中 270

在 Virtuozzo Hybrid Infrastructure 中設定使用
者帳戶 93

在 Virtuozzo Hybrid Infrastructure 中設定網路
93

在 vSphere Client 中檢視備份狀態 334

在 Windows 中 51, 111

在 Windows 中安裝 Cyber Protection 代理程式
55

在可開機媒體中 54

在保護計劃中啟用進階版資料洩漏防禦 437

在您開始之前 86, 88, 92, 100

多

多重磁碟區快照(M) 197

多租用戶支援 128

多站台 IPsec VPN 記錄檔 376

多站台 IPsec VPN 連線 355

如

如何在雲端設定備份掃描 428

如何刪除 Secure Zone 158

如何使用公證 173, 307

如何使用本機 DNS 執行伺服器的容錯移轉
382

如何建立 Secure Zone 157

如何指派使用者權限 60

如何執行 DHCP 伺服器的容錯移轉 382

如何執行遠端協助工作階段 476

如何將資料復原至行動裝置 263

如何從備份取得鑑識資料? 189

如何透過服務主控台檢閱資料 263

如何連線至遠端電腦 475

如何開始備份資料 262

如果使用重新開機復原失敗, 請儲存系統資
訊。231

如果您選擇在虛擬化伺服器建立虛擬機器 519

如果您選擇將虛擬機器儲存為一組檔案 519

存

存取 Cyber Protection 服務 42

存取固定儲存空間中已刪除的備份 488

存取設定 496

存檔內重複資料刪除 182

安

安全復原 211

安裝 Cyber Protection 代理程式 54

安裝在 macOS 中的服務 116

安裝在 Windows 中的服務 116

安裝在您環境中的 Cyber Protection 服務 116

安裝參數 62, 68

安裝軟體 43

有

有用的提示 273, 294

自

自訂或現成的可開機媒體？ 521

自訂指令碼 526

自訂群組 120

自動安裝或解除安裝 61

自動安裝或解除安裝參數 62, 68

自動刪除雲端站台上未使用的客戶環境 357

自動更新代理程式 109

自動核准修補程式 460

自動偵測目的地 440

自動執行凍結前和解除凍結後指令碼 332

自動探索和手動探索 80

自動探索運作方式 78

自動探索電腦 77

自動新增至白名單 426

何

何處取得 Cyber Protect 應用程式 262

作

作用中的點對站台連線 373

作業系統支援的 Cyber Protect 功能。 19

作業系統通知和服務警示 500

刪

刪除 Microsoft 365 組織 274

刪除自訂 DNS 伺服器 371

刪除所有警示 481

刪除備份 238

刪除電腦 319

即

即時保護 401, 423

完

完成檢查 398

快

快速获取儲存空間 114

快速增量/差異備份 186

我

我可以在哪裡看到備份檔案名稱？ 179

我需要多少個代理程式？ 86, 88, 92, 100

我需要哪種代理程式？ 43

更

更新公司或單位中一或多個使用者的原則 435

更新公司或單位的原則 435

更新代理程式 107

步

步驟 1 46

步驟 1。針對您要更新的產品，閱讀並接受授權合約 461

步驟 1: 產生註冊權杖 105

步驟 2 46

步驟 2。設定自動核准的設定 461

步驟 2: 建立 .mst 轉換和解壓縮安裝套件 106

步驟 3 46

步驟 3。準備測試修補保護計劃 462

步驟 3: 設定群組原則物件 106

步驟 4 47

步驟 4。準備實際運作修補保護計劃 462

步驟 5 47

步驟 5。執行「測試修補」保護計劃並檢查結果
463

步驟 6 48

步驟和動作 397

每

每週備份 209

沒

沒有變數的名稱 180

災

災難復原 341

災難復原附加元件 18

系

系統需求 357

防

防止未經授權者解除安裝或修改代理程式 110

防毒和反惡意程式碼保護 400

防毒和反惡意程式碼保護設定 401

事

事件屬性 162

事前/事後命令 202, 232, 325

使

使用 .mst 轉換來安裝產品 61

使用 ASign 簽署檔案 224

使用 Microsoft Azure 虛擬機器進行操作 389

使用 Secure Zone 的方法 37

使用 Universal Restore 219

使用 Web 介面復原檔案 222

使用加密備份 388

使用可開機媒體復原磁碟 218

使用可開機媒體復原檔案 225

使用本機安裝的 Office 365 用代理程式 270

使用本機附加的存放區 329

使用者已登出 165

使用者空閒時 164

使用者帳戶控制 (UAC) 的需求 82

使用重新啟動復原 213

使用原則規則 146, 149

使用情境 236

使用雲端 Microsoft 365 用代理程式 273

使用裝置控制 491

使用範例 169, 181, 318, 321, 331

使用調適型執行模式來更新使用者原則 436

使用應用程式感知備份時需要什麼？ 248

使用變數 180

使用觀察模式來更新使用者原則 436

依

依排程更新 Cyber Protection 定義 114

依電腦分類的 #CyberFit 分數 541

依據事件排程 161

其

其他參數 65, 70

其他排程選項 160

具

具有保護計劃的可用動作 135

具有保護計劃的作業 135

初

初始連線設定 357

初始複本種子 325

協

協同作業和通訊應用程式的保護 448

取

取得已備份資料的 "tibxread" 工具 192

取得含鑑識資料之備份的憑證 191

受

受支援的 Oracle 資料庫版本 31

受保護的健康資訊 (PHI) 440

定

定期轉換為虛擬機器和從備份執行虛擬機器
518

忽

忽略損壞的磁區 185

所

所需角色 104

所需的使用者權限 250, 270, 293

所需的套件是否已安裝? 49

所需連接埠 104

於

於 VMware vSphere 中進行作業 321

易

易受攻擊的電腦 546

服

服務主控台 117

版

版本比較 17

直

直接選擇 146, 149

附

附加 SQL Server 資料庫 253

附錄 A. 站台對站台 OpenVPN - 其他資訊 562

保

保留規則 168

保護 Always On 可用性群組 (AAG) 245

保護 Exchange Online 信箱 271

保護 Exchange Online 資料 275

保護 Gmail 資料 297

保護 Google Workspace 資料 293

保護 Google 雲端硬碟檔案 301

保護 Microsoft 365 Teams 286

保護 Microsoft 365 資料 268

保護 Microsoft SharePoint 240

保護 Microsoft SQL Server 和 Microsoft Exchange Server 240

保護 Microsoft 應用程式 240

保護 MySQL 和 MariaDB 資料 309

保護 OneDrive 檔案 280

保護 Oracle 資料庫 308

保護 SAP HANA 308

保護 SharePoint Online 網站 283

保護 Web 託管伺服器 317

保護共用磁碟機檔案 304

保護行動裝置 261

保護狀態 540

保護計劃 510

保護計劃中的加密 171

保護計劃和模組 129

保護計劃速查表 143

保護託管的 Exchange 資料 264

保護設定 113

保護資料庫可用性群組 (DAG) 246

保護網站 314

保護網站和託管伺服器 314

保護網域控制站 240

信

信箱備份 249

威

威脅饋送 479

建

建立 .mst 轉換和解壓縮安裝套件 61

建立 Runbook 396

建立 Secure Zone 如何轉換磁碟 157

建立 WinPE 或 WinRE 可開機媒體 531

建立主要伺服器 389

建立災難復原保護計劃 345

建立保護計劃 129

建立個人 Google Cloud 專案 294

建立動態群組 121

建立復原伺服器 377

建立資料流程原則和原則規則 429

建立實體可開機媒體 522

建立複寫計劃 322

建立靜態群組 121

建議 230

後

後續步驟 346

指

指令碼的檔案 526

按

按需修補程式安裝 463

為

為什麼使用 Runbook? 396

為什麼要使用 Bootable Media Builder? 522

為什麼要使用 Secure Zone? 156

為什麼要備份 Microsoft 365 資料? 268

為何使用應用程式感知備份? 248

若

若建立 VM 快照期間發生錯誤, 會重新嘗試
186

要

要篩選的類別 417

計

計劃與已經套用的計劃發生衝突 134

計算點 343

重

重新分配 330

重新安裝 VPN 閘道 368

重新指派 IP 位址 370

重新產生設定 373

重複資料刪除 39

限

限制 35, 93, 101, 151, 156, 223, 230, 269, 283,
286, 293, 298, 301, 304-305, 309, 314,
321, 327, 342, 485, 511, 518, 542

限制同時備份的虛擬機器總數。337

修

修補程式安裝狀態 547

修補程式安裝桌面小工具 547

修補程式安裝摘要 548

修補程式安裝歷史記錄 548

修補程式管理 455

修補程式管理設定 457

個

個人識別資訊 (PII) 441

原

原則檢閱與管理 434

哪

哪些項目可以備份? 264, 271, 275, 280, 283,
286, 297, 301, 304, 314

容

容錯回復 324

容錯回復至目標虛擬機器 383

容錯回復至目標實體機器 387

容錯回復的運作方式 383

容錯回復選項 325

容錯至複本 323

容錯移轉的運作方式 379

弱

弱點評估 449

弱點評估和修補程式管理 449

弱點評估桌面小工具 546

弱點評估設定 452

效

效能 232, 325

效能和備份時窗 198

核

核心參數 523

根

根據桌面小工具類型回報的資料 557

站

站台對站台 OpenVPN 連線 349, 364

記

記錄截斷 196

配

配額 317

假

假如... 41

停

停止 Runbook 執行 398

停止容錯移轉 323

停用代理程式的自動 DRS 86

偵

偵測到時採取的動作 412

副

副檔名和例外規則 483

動

動作 434

動作參數 397

動作欄位值 508

動態安裝與解除安裝元件 60

參

參數 524

啟

啟用 VSS 完整備份 208

啟用和停用固定儲存空間 487

啟用和停用站台對站台連線 368

啟用或停用作業系統通知和服務警示 493

啟用或停用裝置控制 491

啟用帳戶 40

啟用軟體清查掃描 465

啟用硬體清查掃描 469

執

執行 #CyberFit 分數掃描 140

執行 Runbook 398

執行永久容錯移轉 323

執行容錯移轉 381

執行測試容錯移轉 380

執行電腦 318

基

基本參數 62, 68

將

將保護計劃套用到群組 127

將備份格式變更為 12 版 (TIBX) 182

將隔離的檔案新增到白名單 427

將數個計劃套用至一個裝置 134

從

從本機備份解壓縮檔案 226

從存取控制排除個別 USB 裝置 494

從存取控制排除程序 505

從存取控制排除裝置子類別 494

從存放庫安裝套件 49

從服務主控台移除電腦 112

從備份執行虛擬機器(立即復原) 317

從備份掛載磁碟區 236

從雲端存放區復原 526

從雲端備份執行電腦最終化 320

從雲端儲存下載檔案 223

從資料庫新增或移除 USB 裝置 494

從網路共用復原 526

從應用程式感知備份復原資料 310

您

您需要知道的其他事項 169

掃

掃描內容 452

掃描類型 400

授

授權問題 135

排

排除 421, 424

排除符合特定條件的檔案。186

排程 159, 205, 452, 458, 482

排程掃描 401, 422

排程報告 556

掛

掛載 Exchange Server 資料庫 255

掛載點 197, 232

探

探索到的電腦 540

控

控制類型 528

敏

敏感資料定義 440

清

清理 515

清單中的修補程式存留時間 464

現

現有的弱點 547

略

略過工作執行 207

移

移除 VMware 用代理程式 (虛擬裝置) 112

符

符合時間間隔時 165

脫

脫離主機資料處理 512

處

處理時不顯示訊息和對話方塊 (無訊息模式) 185, 231

被

被視為 PCI DSS 的資料 444

被視為受保護的健康資訊的資料 441

被視為個人識別資訊 (PII) 的資料 442

規

規則結構 431

設

設定 CDP 備份 154

設定主要伺服器 389

設定加密密碼 485

設定本機路由 372

設定多站台 IPsec VPN 359

設定多站台 IPsec VPN 設定 359

設定自訂 DNS 伺服器 371

設定自動核准修補程式 461

設定災難復原功能 344

設定站台對站台 OpenVPN 357

設定站台對站台 OpenVPN 連線 358

設定連線 347

設定復原伺服器 377

設定虛擬裝置 87, 90, 96, 102

設定雲端伺服器的防火牆規則 393

設定僅雲端模式 357

設定應用程式感知備份 310

設定點對站台遠端 VPN 存取 363

設定顯示模式 536

軟

軟體特定的復原程序 37

軟體清查 465

軟體清查桌面小工具 551

軟體需求 25, 341

透

透過手動指定參數來安裝或解除安裝產品 62

透過群組原則部署代理程式 104

逐

逐一磁區備份 206

連

連接埠 358

連線到從可開機媒體開機的電腦 534

連續資料保護 (CDP) 151

連續數天未成功的備份已達指定的數量 177

部

部署 OVA 範本 101

部署 OVF 範本 86

部署 QCOW2 範本 89, 96

部署 Virtuozzo Hybrid Infrastructure 用代理程式 (虛擬裝置) 92

部署 VMware 用代理程式 (虛擬裝置) 86

備

備份 142

備份 AAG 中包含的資料庫 245

備份 Exchange 叢集資料 247

備份合併 177

備份位置的主機可用 165

備份事前命令 202

備份事後命令 203

備份的反惡意程式碼掃描 427

備份的相關作業 234

備份格式 181

備份格式和備份檔案 182

備份配置 159

備份掃描計劃 511

備份掃描詳細資料 549

備份期間的輸出速度 200

備份視窗 198

備份雲端伺服器 395

備份網站 314

備份網站需要什麼？ 314

備份與復原 142

備份複寫 512

備份選項 174

備份選項的可用性 174

備份儲存索引標籤 234

備份檔案名稱 178

備份檔案名稱的限制 179

備份叢集 Hyper-V 虛擬機器 337

備份驗證 182, 229

報

報告 554

復

復原 209, 536

復原 AAG 中包含的資料庫 246

復原 ESXi 設定 227

復原 Exchange 信箱和信箱項目 255

復原 Exchange 資料庫 253

復原 Exchange 叢集資料 248

復原 Google 雲端硬碟和 Google 雲端硬碟檔案 302

復原 Google 雲端硬碟檔案 303

復原 master 資料庫 253

復原 OneDrive 和 OneDrive 檔案 281

復原 OneDrive 檔案 282

復原 SharePoint Online 資料 285

復原 SQL 資料庫 251

復原小組信箱 290

復原小組網站或特定的網站項目 291

復原小組頻道或小組頻道中的檔案 288

復原公用資料夾和資料夾項目 279

復原共用磁碟機和共用磁碟機檔案 306

復原共用磁碟機檔案 306

復原至 Exchange Server 256

復原至 Microsoft 365 256

復原伺服器 351

復原完成時開啟目標虛擬機器 234

復原完整路徑 232

復原快速鍵清單 209

復原系統狀態 227

復原系統資料庫 252

復原信箱 257, 266, 272, 277, 299

復原信箱和信箱項目 266, 272, 277, 299

復原信箱項目 258, 266, 272, 278, 300

復原前命令 232

復原後命令 233

復原執行個體 311

復原備份 486

復原虛擬機器 217

復原資料表 313

復原資料庫 312

復原電子郵件訊息和會議 290

復原電腦 212

復原實體電腦 212

復原網站 316

復原整個 Google 雲端硬碟 302

復原整個 OneDrive 281

復原整個小組 287

復原整個共用磁碟機 306

復原整個伺服器 311

復原選項 228

復原選項的可用性 228

復原應用程式 240

復原檔案 222

惡

惡意網站存取 417

智

智慧型保護 479

最

最上層物件 527

最近受影響 549

最終化須知 320

最終化電腦 320

最終化與一般復原 320

測

測試容錯移轉 380

測試複本 322

無

無法復原哪些項目? 284

登

登入帳戶所需的權限 59

發

發生 Windows 事件記錄中的事件時 162

發生錯誤時重新嘗試 185, 230

硬

硬體清查 469

硬體清查桌面小工具 552

程

程序 421

等

等到符合排程中的條件 207

結

結合資料流程原則規則 434

虛

虛擬機器如何定期轉換 518

虛擬機器的其他需求 249

虛擬機器的特殊作業 317

虛擬機器的磁碟區陰影複製服務 (VSS) 208

虛擬機器的磁碟區陰影複製服務 VSS 325

虛擬機器的複寫 321

虛擬機器繫結 330

視

視需要更新 Cyber Protection 定義 114

註

註冊可開機媒體 533

註冊參數 64, 69

進

進行網路設定 535

進階 424

進階版資料洩漏防禦 429

進階保護 429

進階設定 439

進階儲存選項 155

開

開始條件 163

開始復原時關閉目標虛擬機器 234

開機模式 229

雲

雲端伺服器的防火牆規則 392

雲端網路基礎架構 347

雲端儲存 185

雲端應用程式 550

雲端應用程式的備份計劃 511

須

須知事項 262

傾

傾印報告資料 557

僅

僅雲端模式 348, 366

匯

匯出和匯入報告結構 557

匯出備份 238

搜

搜尋條件 121

新

新增 Google Workspace 組織 294

新增 Microsoft 365 組織 270, 273

新增 VLAN 535

新增報告 555

新增裝置到靜態群組 121

概

概觀儀表板 538

概觀儀表板上的進階版資料洩漏防禦桌面小工具 447

準

準則 187

準備 46, 220

準備工作: WinPE 2.x 與 3.x 532

準備工作: WinPE 4.0 及更新版本 533

準備電腦以進行遠端安裝 82

準備驅動程式 220

節

節省電池電力 166

裝

裝置計劃與群組計劃發生衝突 135

裝置控制 489

裝置控制警示 507

裝置類型允許名單 500

解

解決計劃衝突 134

解除安裝代理程式 111

解除安裝參數 66, 71

資

資料保護圖 482, 545

資料保護圖設定 482

資料洩漏防禦用代理程式 26

資料洩漏防禦事件 445

資料流程原則更新 435

資料流程原則結構 431

資料庫備份 243

資料擷取事前命令 204

資料擷取事後命令 205

資料擷取前/後命令 203

資訊參數 70

路

路由的運作方式 349, 351, 355

運

運作原理 137, 151, 173, 191, 211, 307, 411,
415, 456, 461, 475, 479, 482, 514, 542

運算子 126

隔

隔離 424

電

電腦上的 USB 裝置清單 505

電腦上的隔離位置 425

電腦的 #CyberFit 分數 137

電腦移轉 338

預

預先更新備份 459

預先定義腳本 525

預先設定多個網路連線 534

預設保護計劃 130

預設計劃選項 131

預設動作 423

預設備份選項 174

預設備份檔案名稱 179

實

實際執行容錯移轉 379

實體資料運送 200

實體資料運送程序概觀 201

實體機器到虛擬 215

對

對於 Active Directory 網域服務可用性的建議 363

對於本機站台的一般建議 361

對於使用者帳戶的要求 256

對虛擬機器執行容錯回復 385

對實體機器執行容錯回復 387

疑

疑難排解 85, 561

疑難排解 IPsec VPN 設定 374

疑難排解 IPsec VPN 設定問題 374

監

監控 538

磁

磁碟佈建 324

磁碟或磁碟區備份儲存哪些內容？ 147

磁碟健全狀況狀態警示 545

磁碟健全狀況桌面小工具 543

磁碟健全狀況監控 541

磁碟區陰影複製服務 (VSS) 207

管

管理 VPN 設備設定 368

管理工作負載 120

管理在不同層級新增的 Microsoft 365 組織 274

管理找到的弱點 454

管理修補程式清單 459

管理偵測到的未受保護檔案 482

管理探索到的電腦 84

管理虛擬化環境 333

管理雲端伺服器 391

管理隔離的檔案 425

管理網路 364

管理點對站台連線設定 373

網

網路保護 539

網路設定 534

網路概念 347

網路管理 364

與

與加密軟體的相容性 36

與使用者共用遠端連線 476

與其他備份選項互動 203

遠

遠端存取 (RDP 和 HTML5 用戶端) 474

遠端安裝代理程式的運作方式 80

遠端抹除 478

遠端桌面存取 474

遠端連線 114

需

需求 226, 236

需要有 TCP 連接埠才能備份和複寫 VMware 虛擬機器 47

範

範例 66, 71-73, 94-95, 164-168

範例：「損壞區塊」緊急備份 163

範例:在 Fedora 14 中手動安裝套件 51

編

編排 (Runbook) 396

編輯報告 555

編輯復原伺服器預設參數 346

複

複本可以執行的動作 321

複製 Microsoft Exchange Server 程式庫 260

複寫 169

複寫與備份之比較 321

複寫選項 324

調

調整資料流程原則規則中的權限 433

適

適用於 L2 OpenVPN 連線的 Active Directory 網域控制站 363

適用於 L3 IPsec VPN 連線的 Active Directory 網域控制站 363

適用於 Linux 的規則 147

適用於 macOS 的規則 147

適用於 macOS 裝置的弱點評估 454

適用於 Oracle 的代理程式 27

適用於 Windows 的規則 147

適用於 Windows 電腦的弱點評估 453

適用於 Windows、Linux 及 macOS 的規則 146

選

選取 OneDrive 檔案 280

選取信箱 265, 271, 275, 298

選項描述 195

選擇 ESXi 設定 150

選擇 Exchange Server 信箱 250

選擇 Exchange Server 資料 244

選擇 Google 雲端硬碟檔案 301

選擇 SharePoint Online 資料 284

選擇 SQL 資料庫 243

選擇小組 287

選擇公用資料夾 276

選擇目的地 155

選擇共用磁碟機檔案 305

選擇系統狀態 150

選擇要安裝的元件 83

選擇要備份的資料 145

選擇磁碟/磁碟區 146

選擇整部機器 145

選擇檔案/資料夾 148

遺

遺漏的更新 (依類別) 548

錯

錯誤處理 185, 230, 324-325

隨

隨選自助服務自訂資料夾 426

壓

壓縮層級 184

應

應用程式感知備份 248

應用程式感知備份所需的使用者權限 249

應用程式感知備份的額外需求 242

檔

檔案日期與時間 230

檔案如何進入隔離資料夾？ 425

檔案排除 231

檔案層級安全性 231

檔案層級備份快照 187

檔案篩選器 186

檢

檢查是否能在可開機環境中存取驅動程式 220

檢查雲端防火牆活動 395

檢查裝置 IP 位址 168

檢視分配結果 330

檢視白名單中關於項目的詳細資料 427

檢視或變更存取設定 493

檢視執行歷程記錄 399

檢視單一裝置的軟體清查 468

檢視單一裝置的硬體 472

檢視裝置控制警示 496

還

還原為原始的初始 RAM 磁碟 221

點

點對站台遠端 VPN 存取 356

叢

叢集備份模式 183

叢集感知備份 246

叢集感知備份和復原需要多少個代理程式？ 247

叢集資料備份和復原需要多少代理程式？ 245

瀏

瀏覽軟體清查 466

瀏覽硬體清查 470

舊

舊版功能的參數 71

轉

轉換為虛擬機器 516

雙

雙重驗證機制 40

關

關於 Cyber Disaster Recovery Cloud 341

關於 Secure Zone 156

關於「實體資料運送」服務 201

關於備份排程 293

關於轉換, 您需要知道的内容 517

關鍵字群組 445

警

警示 177

驅

驅動程式自動搜尋 220

權

權限 434

鑑

鑑識備份程序 188

鑑識資料 188

變

變更 Microsoft 365 存取認證 273

變更 SQL Server 或 Exchange Server 存取認證
261

變更 Windows 電腦上的登入帳戶 59

變更加密密碼 486

變更區塊追蹤 (CBT) 183, 324

變更電腦的服務配額 115

變更網路保護代理程式所使用的連接埠 48

變數物件 527

驗

驗證 513

驗證備份 237