

Cyber Disaster Recovery Cloud

25.01



目錄

關於 Cyber Disaster Recovery Cloud	5
主要功能	5
軟體需求	5
支援的作業系統	5
支援的虛擬化平台	6
限制	7
使用 Microsoft Azure 虛擬機器進行操作	8
Cyber Disaster Recovery Cloud 試用版產品	8
使用異地備援雲端儲存時的限制	8
Disaster Recovery 與加密軟體的相容性	9
自動刪除雲端站台上未使用的客戶環境	9
使用 Disaster Recovery 雲端	10
建立災難復原保護計劃	11
後續步驟	11
編輯復原伺服器的預設設定	12
預設雲端網路基礎架構	13
連線和網路	14
僅雲端模式	14
路由的運作方式	15
設定僅雲端模式	15
在僅限雲端模式下管理網路	16
站台對站台 OpenVPN 連線	16
路由的運作方式	18
VPN 閘道	18
VPN 設備	18
啟用站台對站台連線	18
設定站台對站台 OpenVPN	19
管理 VPN 設備設定	20
管理站台對站台 OpenVPN 的網路	21
允許透過 L2 VPN 的 DHCP 流量	24
從站台對站台 OpenVPN 切換至多站台 IPsec VPN	24
停用站台對站台連線	25
多站台 IPsec VPN 連線	26
VPN 閘道	26
路由的運作方式	27

設定多站台 IPsec VPN	27
從多站台 IPsec VPN 切換至站台對站台 OpenVPN	31
疑難排解 IPsec VPN 設定	32
點對站台遠端 VPN 存取	34
設定點對站台遠端 VPN 存取	35
管理點對站台連線設定	36
作用中的點對站台連線	37
對於 Active Directory 網域服務可用性的建議	38
網路管理	39
公用和測試 IP 位址	39
重新安裝 VPN 閘道	42
設定自訂 DNS 伺服器	42
刪除自訂 DNS 伺服器	43
設定本機路由	44
下載 MAC 位址	44
使用記錄	44
雲端伺服器	47
設定復原伺服器	47
建立復原伺服器	47
次要伺服器的操作	50
設定主要伺服器	51
建立主要伺服器	51
主要伺服器的操作	54
檢視有關雲端伺服器的詳細資料	55
雲端伺服器的備份	55
雲端伺服器的防火牆規則	56
設定雲端伺服器的防火牆規則	57
檢查雲端防火牆活動	59
計算點	60
測試容錯移轉	61
執行測試容錯移轉	61
自動測試容錯移轉	63
設定自動測試容錯移轉	63
檢視自動測試容錯移轉狀態	64
停用自動測試容錯移轉	64
實際執行容錯移轉	65
執行容錯移轉	66

如何使用本機 DNS 執行伺服器的容錯移轉	67
如何執行 DHCP 伺服器的容錯移轉	67
停止容錯移轉	68
容錯回復	69
代理程式型容錯回復 (透過可開機媒體)	69
執行代理程式型容錯回復 (透過可開機媒體)	70
無代理程式容錯回復 (透過 Hypervisor 代理程式)	72
執行無代理程式容錯回復 (透過 Hypervisor 代理程式)	74
手動容錯回復	76
執行手動容錯回復	77
編排 (Runbook)	79
建立 Runbook	79
Runbook 參數	81
Runbook 的相關作業	82
執行 Runbook	82
停止 Runbook 執行	83
檢視執行歷程記錄	83
Disaster Recovery 儀表板	84
Disaster Recovery - 符合資格的裝置	84
健全狀況檢查	84
自動測試容錯移轉	85
移除災難復原網站	86
站台對站台 OpenVPN - 其他資訊	87
辭彙表	94
索引	96

關於 Cyber Disaster Recovery Cloud

Cyber Disaster Recovery Cloud (DR) 是 Cyber Protection 的一部分，可提供災難復原即服務 (DRaaS)。Cyber Disaster Recovery Cloud 可為您提供一個快速且穩定的解決方案，以便在雲端站台上啟動確切的電腦複本，並在發生人為或自然災害時，將工作負載從損毀的原始電腦切換到雲端的復原伺服器。

主要功能

注意事項

部分功能可能需要額外的授權，端視適用的授權模型而定。

- 從單一主控台管理 Cyber Disaster Recovery Cloud 服務
- 使用安全的 VPN 通道，將最多 23 個區域網路延伸至雲端
- 建立與雲端站台的連線，而不需要部署任何 VPN 設備¹ (僅雲端模式)
- 建立本機站台²和雲端站台³的點對站台連線⁴
- 使用雲端的復原伺服器⁵保護您的電腦
- 使用雲端的主要伺服器⁶保護應用程式和裝置
- 為加密的備份執行自動災難復原作業
- 在隔離的網路中執行測試容錯移轉
- 使用 Runbook⁷ 在雲端啟動實際執行環境

軟體需求

支援的作業系統

使用復原伺服器的保護，已針對下列作業系統進行測試：

- CentOS 6.6, 7.x, 8.x
- Debian 9.x, 10.x, 11.x
- Red Hat Enterprise Linux 6.6, 7.x, 8.x
- Ubuntu 18.04, 20.x, 21.x
- Oracle Linux 7.3 and 7.9 with Unbreakable Enterprise Kernel

¹特殊的虛擬機器，可透過安全的 VPN 通道，在區域網路和雲端站台之間連線。VPN 設備是在本機站台上部署的。

²在公司內部部署上部署的本機基礎架構。

³在雲端託管並用於執行復原基礎架構的遠端網站 (萬一發生災難)。

⁴使用端點裝置 (例如電腦或筆記型電腦)，從外部對雲端和本機站台進行的安全 VPN 連線。

⁵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。

⁶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)。

⁷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。

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – 所有安裝選項, Nano Server 除外
- Windows Server 2019 – 所有安裝選項, Nano Server 除外
- Windows Server 2022 – 所有安裝選項, Nano Server 除外

軟體可能可搭配其他 Windows 作業系統或 Linux 版本使用, 但不提供保證。

注意事項

使用復原伺服器的保護, 已針對安裝下列作業系統的 Microsoft Azure VM 進行測試。

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – 所有安裝選項, Nano Server 除外
- Windows Server 2019 – 所有安裝選項, Nano Server 除外
- Windows Server 2022 – 所有安裝選項, Nano Server 除外
- Ubuntu Server 20.04 LTS - Gen2 (Canonical)。如需有關存取復原伺服器主控台的詳細資訊, 請參閱 <https://kb.acronis.com/content/71616>。

支援的虛擬化平台

使用復原伺服器的虛擬機器保護, 已針對下列虛擬化平台進行測試:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- 帶 Hyper-V 的 Windows Server 2008 R2
- 帶 Hyper-V 的 Windows Server 2012/2012 R2
- Windows Server 2016 with Hyper-V – 所有安裝選項, Nano Server 除外
- Windows Server 2019 與 Hyper-V – 所有安裝選項, Nano Server 除外
- Windows Server 2022 with Hyper-V – 所有安裝選項, Nano Server 除外
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- 核心虛擬機器 (KVM) — 僅限完全虛擬化的客體 (HVM)。不支援半虛擬化的客體 (PV)。
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2

VPN 設備已針對下列虛擬化平台進行測試:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- 帶 Hyper-V 的 Windows Server 2008 R2
- 帶 Hyper-V 的 Windows Server 2012/2012 R2
- Windows Server 2016 with Hyper-V – 所有安裝選項, Nano Server 除外
- Windows Server 2019 與 Hyper-V – 所有安裝選項, Nano Server 除外
- Windows Server 2022 with Hyper-V – 所有安裝選項, Nano Server 除外

- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

支援從客體作業系統進行無代理程式備份且具有邏輯磁碟區管理員 (LVM) 組態之磁碟區的 Linux 工作負載。

支援從客體作業系統進行無代理程式備份並且有動態磁碟 (LDM) 組態的 Windows 工作負載。

軟體可能可搭配其他虛擬化平台或版本使用，但無法保證。

限制

在 Cyber Disaster Recovery Cloud 中不支援下列平台和設定：

1. 不支援的平台：

- Virtuozzo 用代理程式
- macOS
- 由於 Microsoft 產品條款的緣故，不支援 Windows 桌面作業系統。
- Windows Server Azure Edition

Azure Edition 是專門建置的 Windows Server 特殊版本，可在 Azure 中當作 Azure IaaS 虛擬機器 (VM) 執行，或在 Azure Stack HCI 叢集上當作 VM 執行。與 Standard 和 Datacenter Edition 不同的是，Azure Edition 未獲授權，無法在裸機硬體、Windows 用戶端 Hyper-V、Windows Server Hyper-V、第三方虛擬機器 Hypervisor 或第三方雲端中執行。

2. 不支援的設定：

Microsoft Windows

- 不支援 Windows 桌面作業系統 (由於 Microsoft 產品條款的緣故)。
- 不支援具有 FRS 複寫的 Active Directory 服務。
- 不支援非 GPT 或 MBR 格式 (所謂的「超級軟碟」) 的卸除式媒體。

Linux

- 不含磁碟分割表的檔案系統。
- 使用客體 OS 的代理程式備份，而且擁有包含下列進階邏輯磁碟區管理員 (LVM) 設定之磁碟區的 Linux 工作負載：等量磁碟區、鏡像磁碟區、RAID 0、RAID 4、RAID 5、RAID 6 或 RAID 10 磁碟區。

注意事項

不支援已安裝多個作業系統的工作負載。

3. 不支援的租用戶模式：

- 為租用戶啟用 [合規] 模式時，無法使用災難復原。

4. 不支援的備份類型：

- 連續資料保護 (CDP) 復原點不相容。

重要事項

如果您從擁有 CDP 復原點的備份建立復原伺服器，則在容錯回復或建立復原伺服器備份期

間，您將失去 CDP 復原點中所包含的資料。

- 鑑識備份無法用於建立復原伺服器。

復原伺服器擁有一個網路介面。如果原始電腦有數個網路介面，則只模擬一個。

雲端伺服器未加密。

使用 Microsoft Azure 虛擬機器進行操作

注意事項

部分功能可能需要額外的授權，端視適用的授權模型而定。

您可以將 Microsoft Azure 虛擬機器容錯移轉至 Acronis Cyber Protect Cloud。如需詳細資訊，請參閱 "執行容錯移轉" (第 66 頁)。

之後，您可以從 Acronis Cyber Protect Cloud 容錯回復到 Azure 虛擬機器。容錯回復程序與容錯回復至實體機器的程序相同。如需詳細資訊，請參閱 "執行代理程式型容錯回復 (透過可開機媒體)" (第 70 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 27 頁)。

Cyber Disaster Recovery Cloud 試用版產品

您可以使用 Acronis Cyber Disaster Recovery Cloud 的試用版產品 30 天。在此情況下，Disaster Recovery 對於合作夥伴租用戶具備下列限制：

- 復原伺服器和主要伺服器無法存取公用網際網路。您無法將公共 IP 位址指派給伺服器。
- IPsec 多站台 VPN 無法使用。

使用異地備援雲端儲存時的限制

異地備援雲端儲存為您的備份資料提供次要位置。次要位置位於地理上與主要存位置不同的區域。區域的地理區隔可確保發生影響其中一個區域並導致備份資料無法復原的災難時，另一個區域將不會受到影響，而且操作將繼續。

重要事項

如果備份儲存位置從主要位置切換到異地備援次要位置，則不支援 Disaster Recovery 服務。

Disaster Recovery 與加密軟體的相容性

災難復原與下列磁碟層級加密軟體相容：

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

注意事項

- 對於具有磁碟層級加密的工作負載，建議您在工作負載的客體作業系統中安裝保護代理程式，並執行代理程式型備份。
- 加密工作負載的無代理程式備份不支援故障移轉和故障回復。

如需有關與加密軟體相容性的詳細資訊，請參閱《資安防護使用者指南》。

自動刪除雲端站台上未使用的客戶環境

Disaster Recovery 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 通道以及與租用戶相關的所有雲端資源。
- 取消登錄 VPN 設備。

非作用中的租用戶會回復到其連線設定前的狀態。

使用 Disaster Recovery 雲端

注意事項

部分功能可能需要額外的授權，端視適用的授權模型而定。

使用災難復原的基本工作流程如下：

1. 以下列其中一種方式建立要保護的工作負載的復原伺服器：
 - a. 建立一個保護計劃，其中包括 **[Disaster Recovery]** 模組和 **[備份]** 模組，並將 **[備份內容]** 設定為 **[整部電腦]** 或系統和開機磁碟區。
 - b. 將計劃套用至您的裝置。這將會自動設定預設的災難復原基礎架構。如需詳細資訊，請參閱 [建立災難復原保護計劃](#)。
 - 手動設定災難復原雲端基礎架構並控制每個步驟。請參閱 "建立復原伺服器" (第 47 頁)。
2. 設定與雲端站台的連線。
 - [僅雲端模式](#)
 - [站台對站台 OpenVPN 連線](#)
 - [多站台 IPsec VPN 連線](#)
 - [點對站台連線](#)
3. 設定自動測試容錯移轉。
4. 執行測試容錯移轉。
5. [發生災難時] 執行實際執行容錯移轉。
6. [發生災難後] 執行容錯回復至本機站台。
7. [選用] 設定 Runbook。

建立災難復原保護計劃

災難復原保護計劃是啟用 **[Disaster Recovery]** 模組的保護計劃。

在您啟用災難復原功能並將計劃套用至您的裝置之後，就會建立雲端網路基礎架構。如需詳細資訊，請參閱 "預設雲端網路基礎架構" (第 13 頁)。

注意事項

- 套用災難復原保護計劃只有在復原雲端網路基礎架構不存在時才會加以建立。系統不會變更或重新建立現有的雲端網路。
- 在設定災難復原之後，您將能夠從針對裝置建立復原伺服器之後產生的任何復原點，執行測試或實際執行容錯移轉。在裝置受到災難復原保護之前產生的復原點 (備份) (例如，在建立復原伺服器之前) 無法用於容錯移轉。
- 如果無法偵測裝置的 IP 位址，無法啟用災難復原保護計劃。例如，虛擬機器無代理程式備份且未指派 IP 位址時。
- 當您套用保護計劃時，系統會在雲端站台中指派相同的網路和 IP 位址。IPsec VPN 連線要求雲端站台和本機站台的網路區段不要重疊。如果已設定多站台 IPsec VPN 連線，且您之後將保護計劃套用至一或數個裝置，則您必須另外更新雲端網路，並重新指派雲端伺服器的 IP 位址。如需詳細資訊，請參閱 "重新指派 IP 位址" (第 41 頁)。

建立災難復原保護計劃

1. 在 Cyber Protect 主控台，前往 **[裝置]** > **[所有裝置]**。
2. 選擇您要保護的電腦。
3. 按一下 **[保護]**，然後按一下 **[建立計劃]**。
保護計劃預設設定隨即開啟。
4. 設定備份選項。
若要使用災難復原功能，此計劃必須在雲端儲存空間備份整部電腦，或僅備份開機及提供必要服務所需的磁碟。
5. 按一下模組名稱旁邊的開關，以啟用 **[災難復原]** 模組。
6. 按一下 **[建立]**。
已建立計劃並套用至所選電腦。已使用預設參數建立預設網路基礎架構和復原伺服器。如需詳細資訊，請參閱 "編輯復原伺服器的預設設定" (第 12 頁) 和 "預設雲端網路基礎架構" (第 13 頁)。

後續步驟

- 您可以編輯復原伺服器的預設設定。如需詳細資訊，請參閱 "編輯復原伺服器的預設設定" (第 12 頁)。
- 您可以編輯預設網路設定。如需詳細資訊，請參閱 "連線和網路" (第 14 頁)。

編輯復原伺服器的預設設定

當您建立並套用災難復原保護計劃時，會使用預設設定建立復原伺服器。必要時，您可以編輯這些預設設定。

注意事項

復原伺服器只有在不存在時才會建立。系統不會變更或重新建立現有的復原伺服器。

若要編輯復原伺服器的預設設定

1. 移至 **[裝置] > [所有裝置]**。
2. 選擇一個裝置，然後按一下 **[災難復原]**。
3. 編輯復原伺服器的預設設定。

下表描述復原伺服器設定。

設定	預設值	描述
CPU 和 RAM	自動	復原伺服器的虛擬 CPU 數量和 RAM 數量。系統將會根據原始裝置的 CPU 和 RAM 設定，自訂決定預設設定。
雲端網路	自動	將與伺服器連線的雲端網路。如需有關如何設定雲端網路的詳細資訊，請參閱 雲端網路基礎架構 。
實際執行網路中的 IP 位址	自動	伺服器將在實際執行網路中具備的 IP 位址。依預設，會設定原始電腦的 IP 位址。
測試 IP 位址	已停用	測試 IP 位址可讓您有能力在隔離的測試網路中測試容錯移轉，並在測試容錯移轉期間，透過 RDP 或 SSH 連線到復原伺服器。在測試容錯移轉模式中，VPN 開道將會使用 NAT 通訊協定，將測試 IP 位址取代為實際執行 IP 位址。如果未指定測試 IP 位址，則在測試容錯移轉期間只能使用主控台存取伺服器。
網際網路存取	已啟用	可讓復原伺服器在實際或測試容錯移轉期間存取網際網路。預設拒絕 TCP 連接埠 25，以供輸出連線使用。
使用公共位址	已停用	具有公共 IP 位址可在容錯移轉或測試容錯移轉期間，讓復原伺服器從網際網路使用。如果您沒有使用公共 IP 位址，則只能在您的實際執行網路中使用該伺服器。若要使用公共 IP 位址，您必須啟用網際網路存取。公共 IP 位址將在您完成設定之後顯示。預設開放 TCP 連接埠 443，以供輸入連線使用。
設定 RPO 閾值	已停用	RPO 閾值會定義上次復原點和目前時間之間的最

		大可允許時間間隔。此值可以設定在 15 - 60 分鐘、1 - 24 小時、1 - 14 天內。
--	--	--

預設雲端網路基礎架構

將災難復原保護計劃套用至您的工作負載時自動建立的雲端網路基礎架構包含下列元件：

- 每個受保護裝置的復原伺服器。
復原伺服器是雲端中所選裝置複本的虛擬機器。
針對每個所選裝置會在 **[待機]** 狀態 (虛擬機器未執行) 下建立具有預設設定的復原伺服器。復原伺服器的大小會依受保護裝置的 CPU 和 RAM 自動調整。
- 雲端站台上的 VPN 開道。
- 復原伺服器連線的雲端網路。

系統會檢查裝置 IP 位址，如果沒有 IP 位址適用的現有雲端網路，就會自動建立適合的雲端網路。如果您已經有復原伺服器 IP 位址適用的現有雲端網路，將不會變更或重新建立現有的雲端網路。

- 如果您沒有現有的雲端網路或者您是第一次設定災難復原設定，將會根據您裝置的 IP 位址範圍，使用 IANA 建議的最大範圍建立私人用途的雲端網路 (10.0.0.0/8、172.16.0.0/12、192.168.0.0/16)。您可以透過編輯網路遮罩來縮小網路的範圍。
- 如果在多個區域網路上都有您的裝置，則雲端站台上的網路將會變成區域網路的超集。您可以在 **[連線]** 區段中重新設定網路。請參閱 "管理站台對站台 OpenVPN 的網路" (第 21 頁)。
- 如果您需要設定站台對站台的 OpenVPN 連線，請下載並設定 VPN 裝置。請參閱 "設定站台對站台 OpenVPN" (第 19 頁)。請確認您的雲端網路範圍符合連線到 VPN 裝置的區域網路範圍。
- 若要變更預設網路設定，請導覽至 **[Disaster Recovery] > [連線]**，或在保護計劃的 **[災難復原]** 模組中，按一下 **[Disaster Recovery]**。

如果您撤銷、刪除或關閉保護計劃的 **[Disaster Recovery]** 模組，將不會自動刪除復原伺服器和雲端網路。如有需要，您可以手動移除災難復原基礎架構。

連線和網路

注意事項

部分功能可能需要額外的授權，端視適用的授權模型而定。

您可以透過 Cyber Disaster Recovery Cloud，定義下列雲端站台的連線類型：

- **僅雲端模式**

這種類型的連線不需要在本機站台上部署 VPN 設備。

區域網路和雲端網路是兩個獨立的網路。這種類型的連線意味著容錯移轉所有本機站台受保護的伺服器，或部分容錯移轉不需要與本機站台通訊的獨立伺服器。

雲端站台上的雲端伺服器可以透過點對站台 VPN，以及公共 IP 位址 (如果已指派) 存取。

- **站台對站台 OpenVPN 連線**

這種類型的連線必須在本機站台上部署 VPN 設備。

站台對站台 OpenVPN 連線允許將您的網路延伸至雲端，並保留 IP 位址。

您的區域網路會透過安全的 VPN 通道連線至雲端站台。如果您在本機站台上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 通道。

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 Disaster Recovery 情境。

如果其中一部伺服器發生部分容錯移轉，系統會在雲端站台上重新建立該伺服器，而其他伺服器則保留在本機站台上，而且這些伺服器仍然能夠透過 IPsec VPN 通道，與彼此通訊。

如果其中一個本機站台發生部分容錯移轉，其餘的本機站台則維持運作，而且將仍然能夠透過 IPsec VPN 通道，與彼此通訊。

- **點對站台遠端 VPN 存取**

使用端點裝置，從外部進行雲端和本機站台工作負載的安全點對站台遠端 VPN 存取。

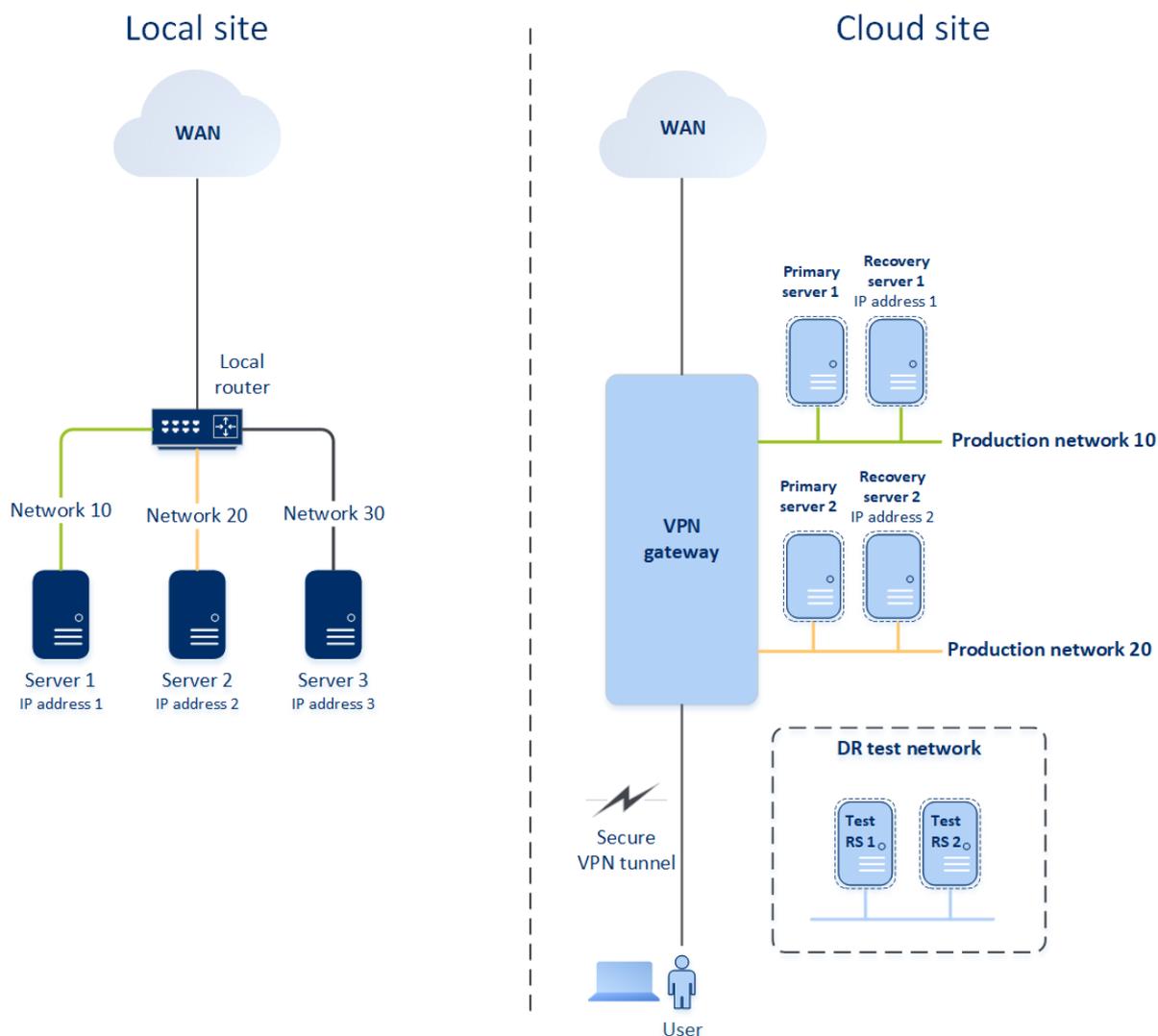
對於本機站台存取，這種類型的連線必須在本機站台上部署 VPN 設備。

僅雲端模式

僅雲端模式不需要在本機站台上部署 VPN 設備。這意味著您有兩個獨立網路：一個在本機站台上，另一個在雲端站台上。路由是使用路由器，在雲端站台上執行的。

路由的運作方式

如果已建立僅雲端模式，則會使用雲端站台上的路由器執行路由，讓不同雲端網路的伺服器可以彼此通訊。



設定僅雲端模式

僅雲端模式是將災難復原計劃套用至工作負載時自動建立的預設連線類型。

若要在僅雲端模式下設定連線

1. 在 Cyber Protect 主控台中，移至 **[Disaster Recovery]** > **[連線]**。
2. 選取 **[僅雲端]**，然後按一下 **[設定]**。

因此，將會在雲端站台上部署具有已定義之位址和遮罩的 VPN 閘道與雲端網路。

在僅限雲端模式下管理網路

您在雲端最多可以新增和管理 23 個網路。

新增網路

若要新增雲端網路

1. 移至 **[Disaster Recovery]** > **[連線]**。
2. 在 **[雲端站台]** 上, 按一下 **[新增雲端網路]**。
3. 定義雲端網路參數: 網路位址和遮罩, 然後按一下 **[完成]**。

因此, 將會在雲端站台上建立具有已定義之位址和遮罩的其他雲端網路。

刪除網路

必要條件

要刪除的網路中的所有雲端伺服器都會遭到刪除。

若要刪除雲端網路

1. 移至 **[Disaster Recovery]** > **[連線]**。
2. 在 **[雲端站台]** 上, 按一下您要刪除的網路位址。
3. 按一下 **[刪除]** 以確認作業。

變更參數

若要變更雲端網路參數

1. 移至 **[Disaster Recovery]** > **[連線]**。
2. 在 **[雲端站台]** 上, 按一下您要編輯的網路位址。
3. 按一下 **[編輯]**。
4. 定義網路位址和遮罩, 然後按一下 **[完成]**。

站台對站台 OpenVPN 連線

注意事項

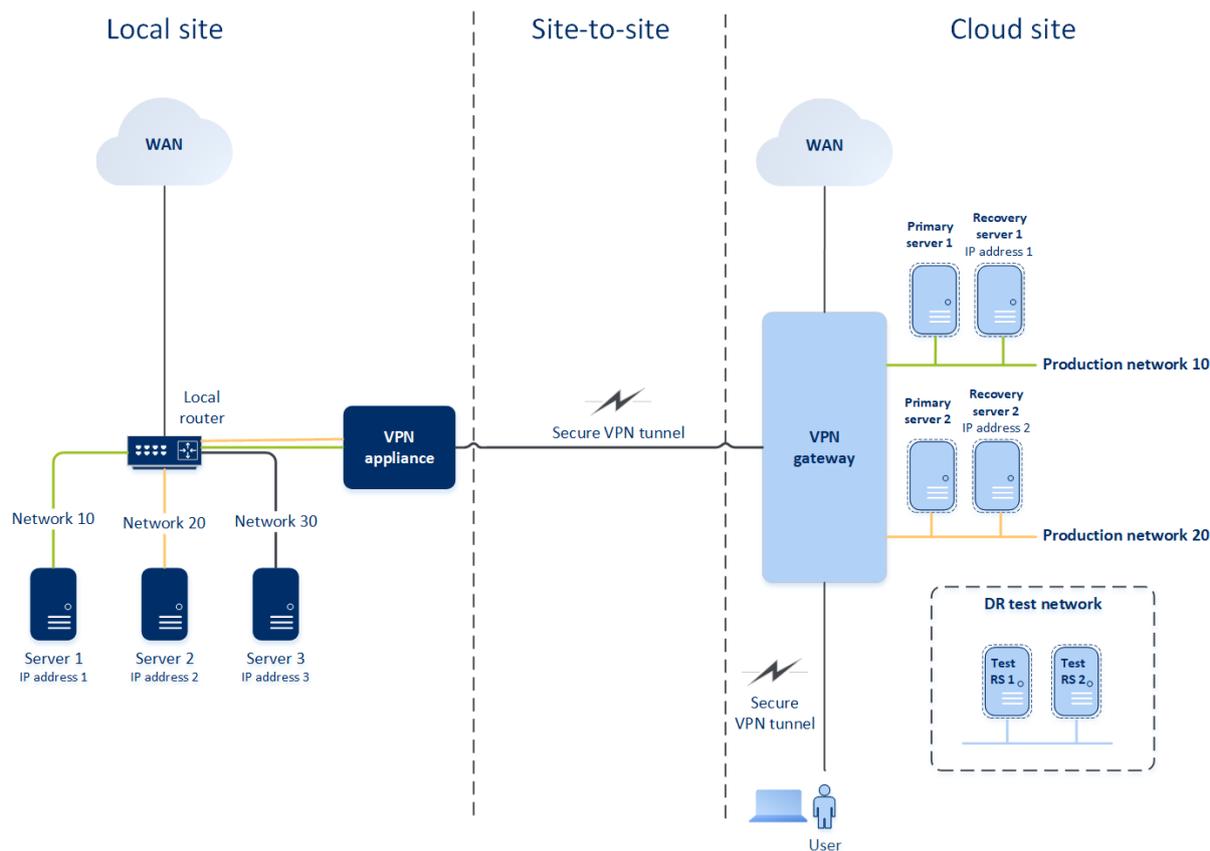
是否能夠使用此功能視您帳戶啟用的服務配額而定。

為瞭解網路在 Cyber Disaster Recovery Cloud 中運作的方式, 我們將考慮當您有三個網路時, 每個本機站台都有一部電腦的情況。您將為下列兩個網站設定災難防護: 網路 10 和網路 20。

在以下的圖表中, 您可以看到託管電腦所在的本機站台, 以及發生災難時啟動雲端伺服器所在的雲端站台。

您可以使用 Cyber Disaster Recovery Cloud, 將所有工作負載從本機站台中損毀的電腦容錯移轉至雲端的雲端伺服器。

您在雲端最多可以新增和管理 23 個網路。



若要在本機站台和雲端站台之間建立站台對站台 OpenVPN 連線，會使用 **VPN 裝置** 和 **VPN 閘道**。當您開始在 Cyber Protect 主控台中設定站台對站台 OpenVPN 連線時，會在雲端站台中自動部署 VPN 閘道。

部署 VPN 閘道器後，您必須執行下列動作：

- 在本機站台上部署 VPN 裝置。
- 新增要受保護的網路。
- 在雲端註冊 VPN 裝置。

Cyber Disaster Recovery Cloud 會在雲端建立您的區域網路複本。VPN 裝置與 VPN 閘道之間將會建立一個安全的 VPN 通道。此 VPN 通道可讓您的區域網路延伸至雲端。雲端的實際執行網路將與您的區域網路進行橋接。本機伺服器與雲端伺服器將透過此 VPN 通道進行通訊，就像它們都在相同的乙太網路區段中一樣。路由將由您的本機路由器執行。

對於要保護的每部來源電腦，您必須在雲端站台上建立一部復原伺服器。發生容錯移轉事件之前，其會維持在 **[待命]** 狀態。如果發生災難，而且您開始容錯移轉程序 (在 **實際執行模式** 下)，將會在雲端啟動代表您受保護電腦確切複本的復原伺服器。其可能會獲指派與來源電腦相同的 IP 位址，而且其可以在相同的乙太網路區段中啟動。您的用戶端將繼續使用伺服器，而不會注意到任何背景變更。

您也可以 **在測試模式下** 啟動容錯移轉程序。也就是說，來源電腦仍在運作中，同時，擁有相同 IP 位址的個別復原伺服器將會在雲端啟動。若要防止 IP 位址發生衝突，將會在雲端建立一個特殊的虛擬網路 - **測試網路**。測試網路會加以隔離，以防某個乙太網路區段中的來源電腦 IP 位址重複。若要

在測試容錯移轉模式下存取復原伺服器，當您建立復原伺服器時，必須將 **[測試 IP 位址]** 指派給該復原伺服器。您也可以設定復原伺服器的其他參數。

路由的運作方式

建立站台對站台連線時，本機路由器會在雲端網路之間執行路由。VPN 伺服器不會在不同雲端網路中的雲端伺服器間執行路由。如果某個網路中的雲端伺服器想要與另一個雲端網路中的伺服器通訊，流量會通過 VPN 通道到達本機站台上的本機路由器，接著本機路由器會將其路由傳送到另一個網路，然後再通過該通道到達雲端站台上的目的地伺服器。

VPN 閘道

VPN 閘道是允許在本機站台和雲端站台間通訊的主要元件。這是雲端中安裝特殊軟體，並專門設定網路所在的虛擬機器。VPN 閘道具備下列功能：

- 在 L2 模式下，連線雲端中區域網路和實際執行網路的乙太網路區段。
- 提供 iptables 和 ebtables 規則。
- 當做預設路由器和 NAT 使用，以供測試和實際執行網路中的電腦使用。
- 當做 DHCP 伺服器使用。實際執行與測試網路中的所有電腦都會透過 DHCP 取得網路設定 (IP 位址、DNS 設定)。每次雲端伺服器都將從 DHCP 伺服器取得相同的 IP 位址。如果您需要設定自訂 DNS 設定，應該連絡支援小組。
- 當做快取 DNS 使用。

VPN 閘道網路設定

VPN 閘道有數個網路介面：

- 外部介面，連線至網際網路
- 實際執行介面，連線至實際執行網路
- 測試介面，連線至測試網路

此外，系統會新增兩個虛擬介面，分別供點對站台連線和站台對站台連線使用。

部署並初始化 VPN 閘道時，系統會建立橋接 (一個供外部介面使用，一個供用戶端和實際執行介面使用)。雖然用戶端實際執行橋接和測試介面使用相同的 IP 位址，但是 VPN 閘道可以使用特定技術，正確路由傳送套件。

VPN 設備

VPN 裝置是本機站台上已安裝 Linux 的一部虛擬機器，其中安裝了特殊軟體，而且具有特殊網路設定。此裝置允許在本機站台和雲端站台之間進行通訊。

啟用站台對站台連線

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

在下列情況下，您可以啟用站台對站台連線：

- 如果您需要雲端站台上的雲端伺服器與本機站台上的伺服器通訊。
- 容錯移轉至雲端之後，會復原本機基礎架構，而且您會想要將伺服器容錯回復至本機站台。

若要啟用站台對站台連線

1. 移至 **[Disaster Recovery]** > **[連線]**。
2. 按一下 **[顯示屬性]**，然後啟用 **[站台對站台連線]** 選項。

因此會在本機站台和雲端站台之間啟用站台對站台 VPN 連線。Cyber Disaster Recovery Cloud 服務會從 VPN 設備取得網路設定，並將區域網路延伸至雲端站台。

設定站台對站台 OpenVPN

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

VPN 裝置的需求

系統需求

- 1 顆 CPU
- 1 GB RAM
- 8 GB 磁碟空間

連接埠

- TCP 443 (輸出) - 用於 VPN 連線
- TCP 80 (輸出) - 用於自動更新設備

請確認您的防火牆以及您網路安全性系統的其他元件允許透過這些連接埠連線到任何 IP 位址。

設定站台對站台 OpenVPN 連線

VPN 設備會將您的區域網路透過安全的 VPN 通道延伸至雲端。此類連線通常稱為「站台對站台」(S2S) 連線。您可以依照下方的程序或觀看[影片教學](#)。

透過 VPN 設備設定連線

1. 在 Cyber Protect 主控台中，移至 **[Disaster Recovery]** > **[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 Disaster Recovery 功能，則會將它刪除，也就是說，雲端會有七天沒有主要伺服器或復原伺服器。

3. 在 **[VPN 設備]** 區塊中, 按一下 **[下載並部署]**。根據您所使用的虛擬化平台, 下載使用, 下載適用於 VMware vSphere 或 Microsoft Hyper-V 的 VPN 設備。
4. 部署設備, 並將其連線至實際執行網路。
在 vSphere 中, 確認已啟用 **[混合模式]** 和 **[偽造傳輸]**, 並針對將 VPN 設備連線到實際執行網路的所有虛擬交換器, 設定為 **[接受]**。若要存取這些設定, 請在 vSphere Client 中選取主機 > **[摘要]** > **[網路]**, 然後選取交換器 > **[編輯設定...]** > **[安全性]**。
在 Hyper-V 中, 建立具有 1024 MB 記憶體的第 1 代虛擬機器。此外, 建議您為該電腦啟用 **[動態記憶體]**。建立電腦之後, 前往 **[設定]** > **[硬體]** > **[網路卡]** > **[進階功能]** 並選取 **[啟用 MAC 位址詐騙]** 核取方塊。
5. 開啟設備電源。
6. 開啟設備主控台, 並以 "admin"/"admin" 使用者名稱和密碼登入。
7. **[選用]** 變更密碼。
8. **[選用]** 如有需要, 變更網路設定。定義將當做網際網路連線的 WAN 介面使用的介面。
9. 使用公司系統管理員的認證, 在 Cyber Protection 服務中登錄設備。
這些認證僅能用於擷取憑證一次。資料中心 URL 是預先定義的。

注意事項

如果為您的帳戶設定雙重驗證機制, 系統也將提示您輸入 TOTP 代碼。如左已啟用雙重驗證機制, 但尚未為您的帳戶是定, 則您無法登錄 VPN 設備。首先, 您必須移至 Cyber Protect 主控台登入頁面, 並為您的帳戶完成雙重驗證機制設定。如需有關雙重驗證機制的更多詳細資訊, 請參閱 [管理入口網站系統管理員指南](#)。

設定完成之後, 該設備將顯示 **[線上]** 狀態。此設備會連線到 VPN 閘道, 並開始將網路相關資訊從所有作用中介面回報到 Cyber Disaster Recovery Cloud 服務。Cyber Protect 主控台會根據來自 VPN 裝置的資訊, 顯示介面。

管理 VPN 設備設定

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

在 **[Disaster Recovery]** > **[連線]** 索引標籤上, 您可以:

- 下載記錄檔。
- 取消登錄裝置 (如果您需要重設 VPN 裝置設定或切換到僅雲端模式)。

若要存取這些設定, 請按一下 **[VPN 裝置]** 區塊中的 **i** 圖示。

在 VPN 設備主控台中, 您可以:

- 變更設備的密碼。
- 檢視/變更網路設定, 並定義將當做網際網路連線的 WAN 使用的介面。
- 註冊/變更註冊帳戶 (透過重複註冊)。
- 重新啟動 VPN 服務。

- 重新啟動 VPN 設備。
- 執行 Linux 殼層命令 (僅適用於進階疑難排解情況)。

管理站台對站台 OpenVPN 的網路

注意事項

部分功能可能需要額外的授權，端視適用的授權模型而定。

您在雲端最多可以新增和管理 23 個網路。

新增網路

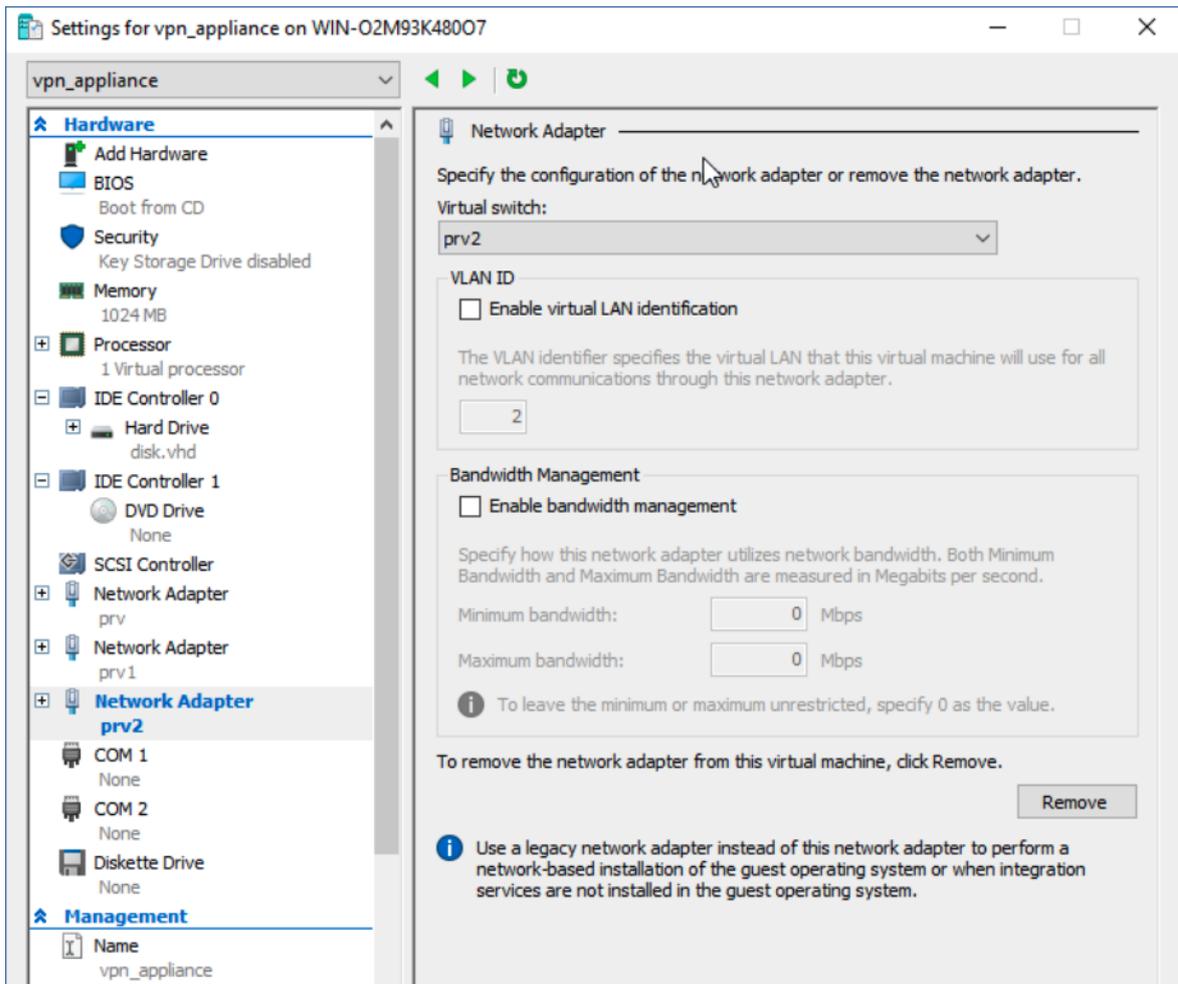
必要條件

已設定站台對站台 OpenVPN 連線，如 "設定站台對站台 OpenVPN" (第 19 頁) 中所述。

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. [選用] 若要新增一個或多個網路，則針對每個額外的網路，將一個虛擬網路介面 (網路介面卡) 新增至執行虛擬裝置所在的虛擬裝置上。

下列範例示範在 Hyper-V Hypervisor 上執行的虛擬機器的步驟。



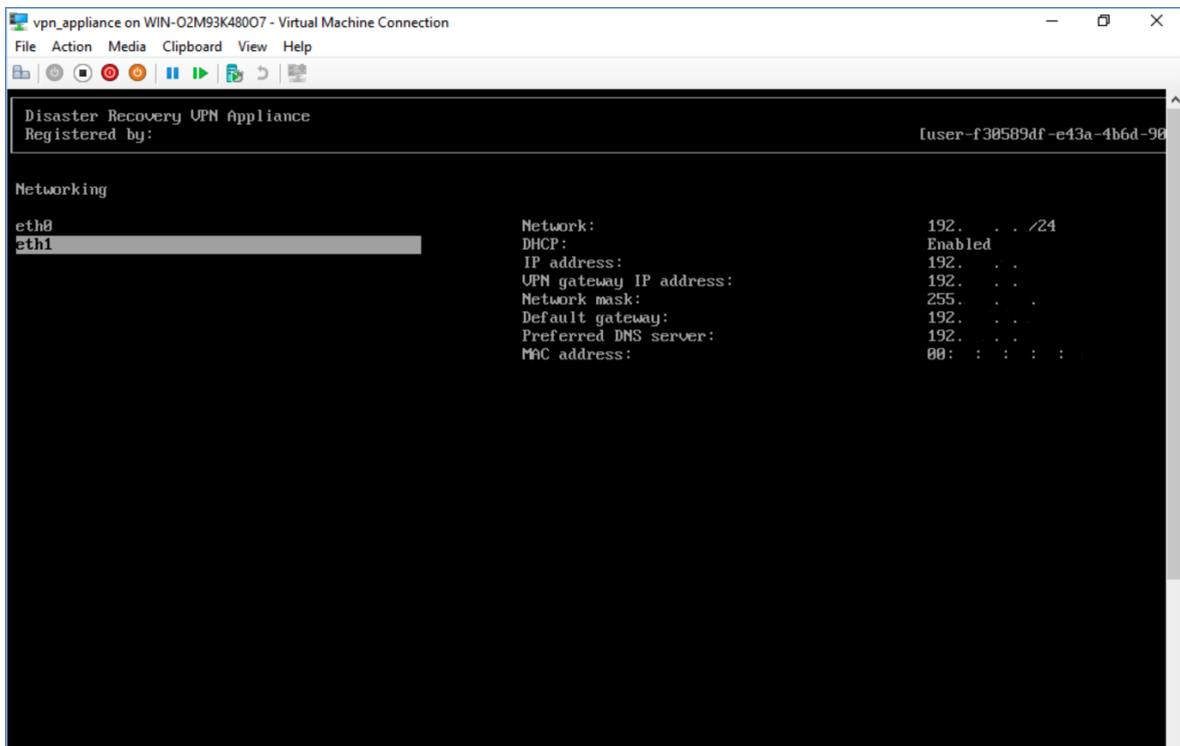
注意事項

您必須使用您要延伸至雲端的本機虛擬網路設定新的虛擬網路介面卡。

3. 登入 VPN 裝置主控台, 然後在 **[網路]** 區段, 設定其中一個介面 (網路卡) 的網路設定。

注意事項

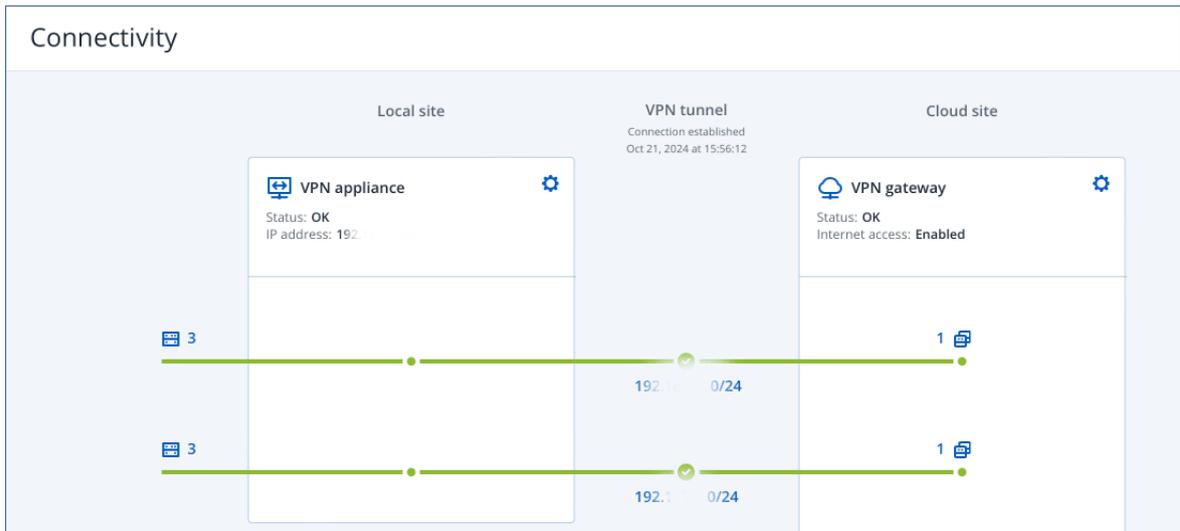
- IP 位址設定僅對其中一個虛擬網路介面是必要的, 以啟用網際網路存取。您可以跳過其他網路介面的 IP 設定。
 - 您必須針對每個介面卡啟用混合模式和偽造的傳輸或 MAC 位址詐騙。如需詳細資訊, 請參閱這篇知識庫文章。
-



```
vpn_appliance on WIN-O2M93K48007 - Virtual Machine Connection
File Action Media Clipboard View Help
Disaster Recovery VPN Appliance
Registered by: [user-f38589df-e43a-4b6d-98
Networking
eth0
eth1
Network: 192.168.1.0/24
DHCP: Enabled
IP address: 192.168.1.1
VPN gateway IP address: 192.168.1.1
Network mask: 255.255.255.0
Default gateway: 192.168.1.1
Preferred DNS server: 192.168.1.1
MAC address: 00:00:00:00:00:00
```

VPN 裝置會自動開始將網路相關資訊從所有作用中介面回報到 Cyber Disaster Recovery Cloud。

4. 登入 Cyber Protect 主控台, 然後前往 **[災難復原]** > **[連線]**。



所有區域網路都會自動延伸至雲端站台。

刪除網路

若要刪除延伸至雲端的網路

1. 登入 VPN 設備主控台。
2. 在 **網路** 區段中，選取您要刪除的介面，然後按一下 **清除網路設定**。
3. 確認作業。

因此，透過安全的 VPN 通道延伸至雲端的區域網路將會遭到停止。此網路將會當作獨立的雲端區段運作。如果使用此介面將流量傳遞到雲端站台或從雲端站台傳遞流量，將會中斷與雲端站台的網路連線。

變更參數

若要變更網路參數

1. 登入 VPN 設備主控台。
2. 在 **網路** 區段中，選取您要編輯的介面。
3. 按一下 **編輯網路設定**。
4. 選擇其中一個選項：
 - 若要透過 DHCP 自動設定網路，按一下 **使用 DHCP**，然後確認操作。

- 若要手動設定網路，按一下 **[設定靜態 IP 位址]**，進行設定，然後按一下 **Enter**。

設定	描述
IP 位址	區域網路中介面的 IP 位址。
VPN 閘道 IP 位址	為網路的雲端區段保留的特殊 IP 位址，可讓 Cyber Disaster Recovery Cloud 服務正常運作。
網路遮罩	區域網路的網路遮罩。
預設閘道	本機站台上的預設閘道。
慣用的 DNS 伺服器	本機站台上的主要 DNS 伺服器。
替代的 DNS 伺服器	本機站台上的次要 DNS 伺服器。

```

Disaster Recovery VPN Appliance
Registered by:                               9.0.1.234
                                              [dagny@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:

```

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 Disaster Recovery 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

- 移至 **[Disaster Recovery] > [連線]** 索引標籤。
- 按一下 **[顯示屬性]**。
- 啟用 **[允許透過 L2 VPN 的 DHCP 流量]** 開關。

從站台對站台 OpenVPN 切換至多站台 IPsec VPN

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以輕鬆地從站台對站台 OpenVPN 連線切換到多站台 IPsec VPN 連線，也可以輕鬆地從多站台 IPsec VPN 連線切換到站台對站台 OpenVPN 連線。

當您切換連線類型時，作用中的 VPN 連線會遭到刪除，但是會保留雲端伺服器 and 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 Cyber Protect 主控台中，移至 **[Disaster Recovery] > [連線]**。
2. 按一下 **[顯示屬性]**。
3. 按一下 **[切換到多站台 IPsec VPN]**。
4. 按一下 **[重新設定]**。
5. 針對雲端網路和雲端伺服器，**重新指派 IP 位址**。
6. **設定多站台 IPsec 連線設定**。

停用站台對站台連線

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

如果您不需要雲端站台上的雲端伺服器與本機站台上的伺服器通訊，您可以停用站台對站台連線。

若要停用站台對站台連線

1. 移至 **[Disaster Recovery] > [連線]**。
2. 按一下 **[顯示屬性]**，然後停用 **[站台對站台連線]** 選項。

因此，本機站台將與雲端站台中斷連線。

多站台 IPsec VPN 連線

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以使用多站台 IPsec VPN 連線來連線單一本機站台，或透過安全的 L3 IPsec VPN 連線，將多個本機站台連線到 Cyber Disaster Recovery Cloud。

如果您有下列其中一個使用案例，此連線類型適用於 Disaster Recovery 情境：

- 您有一個本機站台主控重要工作負載。
- 您有多個本機站台主控重要工作負載，例如不同地點的辦公室。
- 您使用第三方軟體站台或受管理服務供應商站台，並透過 IPsec VPN 通道，連線到這些站台。

若要在本機站台和雲端站台之間建立多站台 IPsec VPN 通訊，會使用 **VPN 閘道**。當您開始在 Cyber Protect 主控台中設定多站台 IPsec VPN 連線時，會在雲端站台中自動部署 VPN 閘道。您應該設定雲端網路區段，並確認這些區段沒有與區域網路區段重疊。系統會在本機站台和雲端站台之間建立一個安全的 VPN 通道。本機伺服器 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。

注意事項

使用多站台 IPsec VPN 連線時，VPN 閘道會自動獲指派公用 IP 位址。

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 42 頁)。

- 當做快取 DNS 使用。

路由的運作方式

使用雲端站台上的路由器執行雲端網路之間的路由，讓不同雲端網路的伺服器可以彼此通訊。

設定多站台 IPsec VPN

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以透過下列兩種方式，設定多站台 IPsec VPN 連線：

- 從 **[Disaster Recovery]** > **[連線]** 索引標籤。
- 在一或數個裝置上套用保護計劃，然後從自動建立的站台對站台 OpenVPN 連線，自動切換到多站台 IPsec VPN 連線、設定多站台 IPsec VPN 設定，並重新指派 IP 位址。

[連線] 索引標籤

從 **[連線]** 標籤設定多站台 IPsec VPN 連線

1. 在 Cyber Protect 主控台中，移至 **[Disaster Recovery]** > **[連線]**。
2. 在 **[多站台 VPN 連線]** 區段中，按一下 **[設定]**。
VPN 閘道是在雲端站台上部署的。
3. 設定多站台 IPsec VPN 設定。

保護計劃

從保護計劃設定多站台 IPsec VPN 連線

1. 在 Cyber Protect 主控台中，移至 **[裝置]**。
2. 將保護計劃套用到清單中的一或多個裝置。
系統會針對站台對站台的 OpenVPN 連線，自動設定復原伺服器和雲端基礎架構設定。
3. 移至 **[Disaster Recovery]** > **[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 **[Disaster Recovery]** > **[連線]** 索引標籤上設定雲端站台和本機站台設定。

必要條件

- 已設定多站台 IPsec VPN 連線。如需有關設定多站台 IPsec VPN 連線的詳細資訊，請參閱 "設定多站台 IPsec VPN" (第 27 頁)。
- 每個本機 IPsec VPN 閘道都有一個公共 IP 位址。
- 您的雲端網路具備足夠的 IP 位址，可供作為受保護電腦複本的雲端伺服器 (在實際執行網路中) 以及復原伺服器 (根據您的需求，擁有一或兩個 IP 位址) 使用。
- [如果您在本機站台和雲端站台之間使用防火牆] 在本機站台上要允許下列 IP 通訊協定和 UDP 連接埠：IP 通訊協定 ID 50 (ESP)、UDP 連接埠 500 (IKE) 和 UDP 連接埠 4500。
- 本機站台上的 NAT-T 設定遭到停用。

設定多站台 IPsec VPN 連線

1. 將一或多個網路新增到雲端站台。
 - a. 按一下 **[新增網路]**。

注意事項

新增雲端網路時，系統將會自動新增擁有相同網路位址和遮罩的對應測試網路，以執行測試容錯移轉。測試網路中的雲端伺服器與雲端實際執行網路中的雲端伺服器擁有相同的 IP 位址。如果您需要在測試容錯移轉期間，從實際執行網路存取雲端伺服器，請在建立復原伺服器時，為其指派另一個測試 IP 位址。

- b. 在 **[網路位址]** 欄位中，輸入網路的 IP 位址。

注意事項

請確認雲端網路沒有與您環境中的任何區域網路重疊。否則，無法建立通道。

- c. 在 **[網路遮罩]** 欄位中，輸入網路的遮罩。
 - d. 按一下 **[新增]**。
2. 依照適用於本機站台的建議，為您希望連線到雲端站台的每個本機站台進行設定。如需有關這些建議的詳細資訊，請參閱 "對於本機站台的一般建議" (第 29 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 29 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 開道會起始連線)，但是您可以將其變更為 **【啟動】** (雲端 VPN 開道會起始連線) 或 **【路由】** (適用於支援路由選項的防火牆)。

h. 設定 **【網路政策】**。

網路政策會指定 IPsec VPN 所連線的網路。使用 CIDR 格式，輸入網路的 IP 位址和遮罩。區域網路區段和雲端網路區段不應重疊。

i. 按一下 **【儲存】**。

對於本機站台的一般建議

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

當您為多站台 IPsec VPN 連線設定本機站台時，請考慮下列建議：

- 針對每個 IKE 階段，請為下列參數設定至少一個在雲端站台中設定的值：加密演算法、雜湊演算法以及 Diffie-Hellman 群組號碼。
- 針對為 IKE 階段 2 在雲端站台中設定的 Diffie-Hellman 群組號碼，使用至少其中一個值，啟用 **【完整轉寄密碼】**。
- 針對 IKE 階段 1 和 IKE 階段 2，設定與雲端站台中相同的 **【存留時間】** 值。
- 不支援使用 NAT 周遊 (NAT-T) 的設定。停用本機站台上的 NAT-T 設定。否則，無法交涉其他 UDP 封裝。
- **【啟動動作】** 設定可定義哪一端起始連線。預設值 **【新增】** 意指本機站台起始連線，而雲端站台正在等待連線起始。如果您希望雲端站台起始連線，請將值變更為 **【啟動】**；如果您希望兩端都能夠起始連線 (適用於支援路由選項的防火牆)，則將該值變更為 **【路由】**。

如需詳細資訊以及不同解決方案的設定範例，請參閱：

- [本系列的知識庫文章](#)
- [本影片範例](#)

IPsec/IKE 安全性設定

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

下表提供有關 IPsec/IKE 安全性參數的詳細資訊。

參數	描述
加密演算法	將用於確保在傳輸中無法檢視資料的加密演算法。預設會選擇所有演算法。您必須在本機開道裝置上，針對每個 IKE 階段設定至少其中一個所選演算

參數	描述
	法。
雜湊演算法	將用於驗證資料完整性和真實性的雜湊演算法。預設會選擇所有演算法。您必須在本機開道裝置上，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。您必須在本機開道裝置上，針對每個 IKE 階段設定至少其中一個所選群組。
存留時間 (秒)	存留時間值可透過使用者封包的一組加密/驗證金鑰，決定從成功交涉到過期的連線執行個體持續時間。 階段 1 的範圍：900-28800 秒，預設為 28800。 階段 2 的範圍：900-3600 秒，預設為 3600。 階段 2 的存留時間必須小於階段 1 的存留時間。 連線會在過期之前，透過金鑰處理通道進行重新交涉，請參閱 重設金鑰寬限時間 。如果本機和遠端的存留時間不一致，則存留時間較長的那一端將會發生替換連線的混亂情況。另請參閱 重設金鑰寬限時間 和 重設金鑰模糊資料 。
重設金鑰寬限時間 (秒)	連線過期或金鑰處理通道過期之前的寬限時間，在此期間內，VPN 連線的本機端會嘗試交涉替換。系統會根據 重設金鑰模糊資料 的值，隨機選擇重設金鑰的確切時間。僅在本機相關，遠端無需對此達成共識。範圍：900-3600 秒。預設值為 3600。
重新執行視窗大小 (封包)	此連線的 IPsec 重新執行視窗大小。 預設值 -1 使用在 strongswan.conf 檔案中，以 charon.replay_window 設定的值。 只有在使用 Netlink 後端時，才支援大於 32 的值。 值為 0 時，會停用 IPsec 重新執行保護。
重設金鑰模糊資料 (%)	隨機增加寬限位元組、寬限封包和寬限時間的百分比上限以隨機選擇重設金鑰間隔 (對於具有許多連線的主機很重要)。 重設金鑰模糊資料值可以超過 100%。marginTYPE 的值在隨機增加之後，不得超過 lifeTYPE，其中 TYPE 是其中一個位元組 (封包或時間)。

參數	描述
	值為 0% 時，會停用隨機選擇。僅在本機相關，遠端無需對此達成共識。
DPD 逾時 (秒)	發生無作用對等偵測 (DPD) 逾時前等待的時間。您可以將值指定為 30 或更高。預設值為 30。
無作用對等偵測 (DPD) 逾時動作	無作用對等偵測 (DPD) 逾時發生後採取的動作。 重新啟動 - DPD 逾時發生時，重新啟動工作階段。 清除 - DPD 逾時發生時，結束工作階段。 無 - DPD 逾時發生時，不採取任何動作。
啟動動作	決定哪一端起始連線，並為 VPN 連線建立通道。 新增 - 您的本機 VPN 閘道會起始連線。 啟動 - 雲端 VPN 閘道會起始連線。 路由 - 適用於支援路由選項的 VPN 閘道。只有在存在從本機 VPN 閘道或雲端 VPN 閘道起始的流量時，通道才會啟動。

從多站台 IPsec VPN 切換至站台對站台 OpenVPN

您可以輕鬆地從多站台 IPsec VPN 連線切換到站台對站台 OpenVPN 連線。

當您切換連線類型時，作用中的 VPN 連線會遭到刪除，但是會保留雲端伺服器 and 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。

下表比較站台對站台 OpenVPN 連線與多站台 IPsec VPN 連線的基本特性。

	站台對站台 OpenVPN	多站台 IPsec VPN
本機站台支援	單一	單一、多個
VPN 閘道模式	L2 Open VPN	L3 IPsec VPN
網路區段	將區域網路延伸到雲端網路	區域網路區段和雲端網路區段不應重疊
支援本機站台的點對站台存取	是	否
支援雲端站台的點對站台存取	是	是
需要公共 IP 產品項目	否	是

若要從多站台 IPsec VPN 連線切換到站台對站台 OpenVPN 連線

1. 在 Cyber Protect 主控台中, 移至 **[Disaster Recovery]** > **[連線]**。
2. 按一下 **[顯示屬性]**。
3. 按一下 **[切換到站台對站台 OpenVPN]**。
4. 按一下 **[重新設定]**。
5. 針對雲端網路和雲端伺服器, 重新指派 IP 位址。
6. 設定切換站台對站台連線設定。

疑難排解 IPsec VPN 設定

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

當您設定或使用 IPsec VPN 連線時, 可能會遇到問題。

您可以在 IPsec 記錄檔中深入瞭解您所遇到的問題, 並查閱「疑難排解 IPsec VPN 設定問題」主題, 以找出部分可能會發生的常見問題的可能解決方案。

疑難排解 IPsec VPN 設定問題

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

下表描述最常發生的 IPsec VPN 設定問題, 並說明其疑難排解方式。

問題	可能的解決方案
我看到下列錯誤訊息: IKE 第 1 階段交涉錯誤。請檢查雲端和本機站台上的 IPsec IKE 設定。	<p>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。</p> <hr/> <p>注意事項 基於安全性, 下列限制適用於 IPsec VPN 連線:</p> <ul style="list-style-type: none"> • 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。	<p>檢查:</p> <ul style="list-style-type: none"> • 是否已開放 UDP 連接埠 500 (當您使用防火牆時)。

問題	可能的解決方案
	<ul style="list-style-type: none"> • 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。	<p>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。</p> <p>從本機站台起始連線。</p>
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。	<p>當雲端站台的 [啟動動作] 設定為 [路由] 時, 您會看到這個狀態。</p> <p>如果您希望從本機站台起始連線, 請執行下列操作:</p> <ul style="list-style-type: none"> • 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。	<p>此問題可能是由於下列原因所造成:</p> <ul style="list-style-type: none"> • 雲端 IPsec 站台的網路對應與本機站台的網路對應不同。 請確認本機站台和雲端站台的網路對應和網路政策順序完全相符。 • 當本機站台和/或雲端站台的 [啟動動作] 設定為 [路由] (例如, 在 Cisco ASA 裝置上), 而且目前沒有流量時, 此狀態是正確的。您可以嘗試 Ping 以確認是否已建立通道。如果 Ping 沒有作用, 請檢查本機站台和雲端站台的網路對應。
我想要重新啟動特定的 IPsec 連線。	<p>重新啟動特定的 IPsec 連線:</p> <ol style="list-style-type: none"> 1. 在 [災難復原] > [連線] 畫面中, 按一下 IPsec 連線。 2. 按一下 [停用連線]。 3. 再按一下 IPsec 連線。 4. 按一下 [啟用連線]。

下載 IPsec VPN 記錄檔

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以在 VPN 伺服器上的記錄檔中, 找到 IPsec 連線的其他資訊。記錄檔會壓縮成您可以下載並解壓縮的 .zip 存檔。

必要條件

已設定多站台 IPsec VPN 連線。

下載包含記錄檔的 .zip 存檔

1. 在 Cyber Protect 主控台中，移至 **[Disaster Recovery]** > **[連線]**。
2. 按一下雲端站台 VPN 閘道旁的齒輪圖示。
3. 按一下 **[下載記錄檔]**。
4. 按一下**[完成]**。
5. 當 .zip 存檔準備就緒可供下載時，請按一下**下載記錄**，然後將其儲存在本機。

多站台 IPsec VPN 記錄檔

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

下列清單描述 zip 存檔中的 IPsec VPN 記錄檔及其包含的資訊。

- ip.txt - 此檔案包含網路介面設定中的記錄。您必須看到兩個 IP 位址：公共 IP 位址和本機 IP 位址。如果您在記錄中看不到這些 IP 位址，則表示有問題。請聯絡支援小組。

注意事項

公共 IP 位址的遮罩必須是 32。

- swanctl-list-loaded-config.txt - 此檔案包含所有 IPsec 站台的相關資訊。
如果您在檔案中看不到站台，則表示未套用 IPsec 設定。請嘗試更新設定並加以儲存，或聯絡支援小組。
- swanctl-list-active-sas.txt - 此檔案包含處於作用中或正在連線狀態的連線和政策。

點對站台遠端 VPN 存取

注意事項

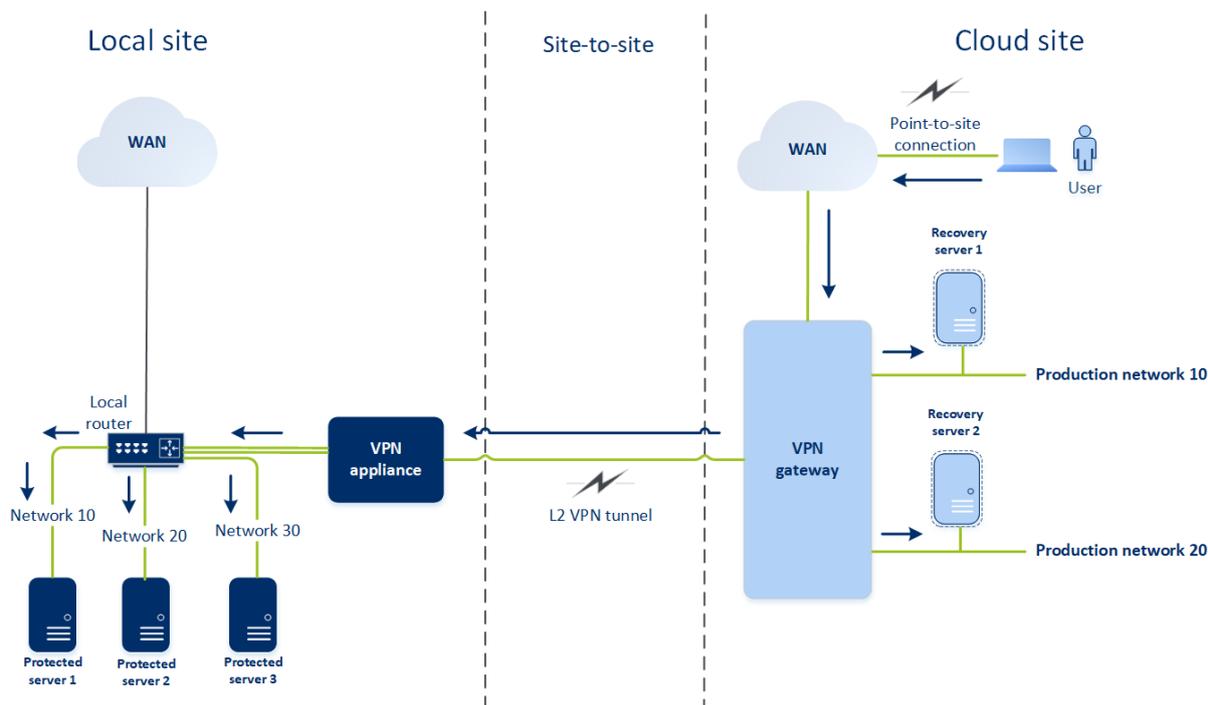
是否能夠使用此功能視您帳戶啟用的服務配額而定。

點對站台連線是一種使用端點裝置 (例如電腦或筆記型電腦)，從外部透過 VPN 對雲端站台和本機站台進行的安全連線。在您建立與 Cyber Disaster Recovery Cloud 站台的站台對站台 OpenVPN 連線之後，即可供使用。此類型的連線在下列情況中非常有用：

- 在許多公司中，僅能從公司網路取得公司服務和 Web 資源。您可以使用點對站台連線，安全地連線到本機站台。
- 如果發生災難，當工作負載切換到雲端站台，且您的區域網路斷線時，您可能需要直接存取雲端伺服器。這可以透過雲端站台的點對站台連線完成。

對於本機站台的點對站台連線，您需要在本機站台上安裝 VPN 設備、設定站台對站台連線，然後設定本機站台的點對站台連線。因此，您的遠端員工將透過 L2 VPN 存取公司網路。

以下配置顯示本機站台、雲端站台，以及以綠色醒目提示的伺服器間的通訊。L2 VPN 通道可連線本機站台和雲端站台。當使用者建立點對站台連線時，會透過雲端站台對本機站台執行通訊。



點對站台設定會使用憑證向 VPN 用戶端進行驗證。此外，使用者認證用於驗證。請注意有關本機站台的點對站台連線的下列資訊：

- 使用者應該使用其 Cyber Protect Cloud 認證，在 VPN 用戶端中進行驗證。他們必須具備「公司系統管理員」或「網路保護」使用者角色。
- 如果您重新產生 OpenVPN 設定，則您必須將更新的設定提供給使用點對站連線與雲端站台連線的所有使用者。

設定點對站台遠端 VPN 存取

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

如果您需要從遠端連線到本機站台，可以設定本機站台的點對站台連線。您可以依照下方的程序或觀看影片教學。

必要條件

- 已設定站台到站台 OpenVPN 連線。
- 已在本機站台上安裝 VPN 裝置。

設定本機站台的點對站台連線

1. 在 Cyber Protect 主控台中，移至 **[Disaster Recovery] > [連線]**。
2. 按一下 **[顯示屬性]**。

3. 啟用 **[本機站台的 VPN 存取]** 選項。
4. 確認需要建立本機站台的點對站台連線的使用者：
 - 在 Cyber Protect Cloud 中擁有使用者帳戶。這些認證在 VPN 用戶端中用於驗證。否則，請在 [Cyber Protect Cloud](#) 中建立使用者帳戶。
 - 具備「公司系統管理員」或「網路保護」使用者角色。
5. 設定 OpenVPN 用戶端：
 - a. 從下列位置下載 OpenVPN 用戶端 2.4.0 版或更新版本：<https://openvpn.net/community-downloads/>。

注意事項

不支援 OpenVPN Connect 用戶端。

- b. 將 OpenVPN 用戶端安裝在您要連線到本機站台的來源電腦上。
- c. 按一下 **[下載 OpenVPN 的設定]**。設定檔適用於貴組織中擁有「公司系統管理員」或「網路保護」使用者角色的使用者。
- d. 將已下載的設定匯入 OpenVPN 用戶端。
- e. 使用 Cyber Protect Cloud 使用者認證，登入 OpenVPN 用戶端 (請參閱上述的步驟 4)。
- f. **[選用]** 如果針對貴組織啟用雙重驗證機制，則您應該提供 **產生的一次性 TOTP 代碼**。

重要事項

如果為您的帳戶啟用雙重驗證機制，您需要重新產生設定檔，並為您現有的 OpenVPN 用戶端更新設定檔。使用者必須重新登入 Cyber Protect Cloud，才能為其帳戶設定雙重驗證機制。

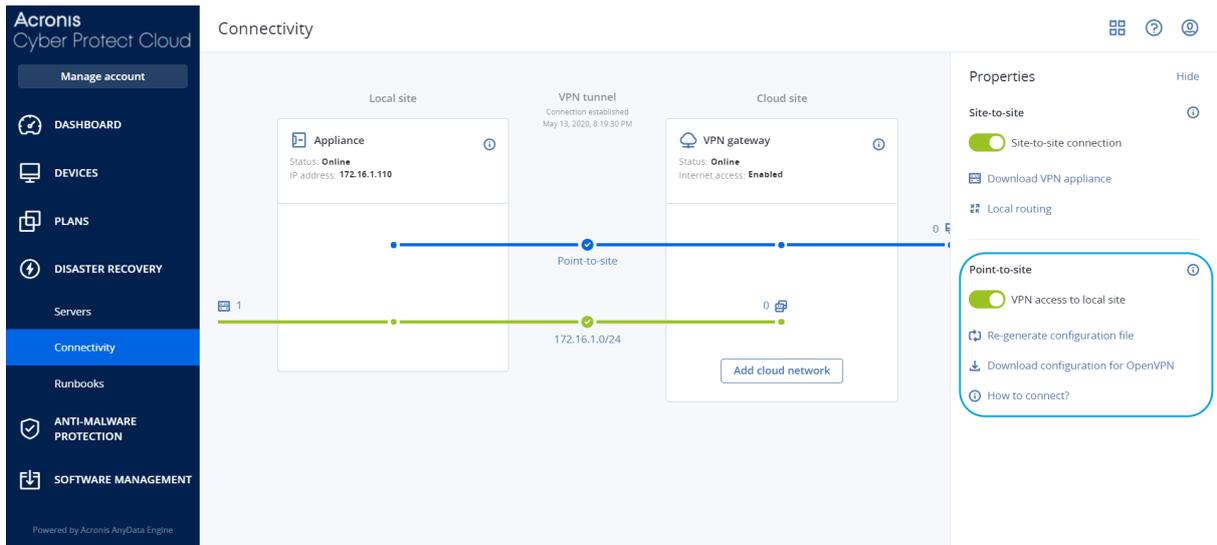
因此，您將可以連線到本機站台上的電腦。

管理點對站台連線設定

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

在 Cyber Protect 主控台中，移至 **[Disaster Recovery] > [連線]**，然後按一下右上角的 **[顯示屬性]**。



本機站台的 VPN 存取

此選項用於管理對本機站台的 VPN 存取。預設為啟用狀態。如果遭到停用，將不允許對本機站台的點對站台存取。

下載 OpenVPN 的設定

這會下載 OpenVPN 用戶端的設定檔。若要建立與雲端站台的點對站台連線，需要這個檔案。

重新產生設定

您可以重新產生 OpenVPN 用戶端的設定檔。

在下列情況下，這是必要的：

- 如果您懷疑設定檔已損壞。
- 如果您的帳戶已啟用雙重驗證機制。

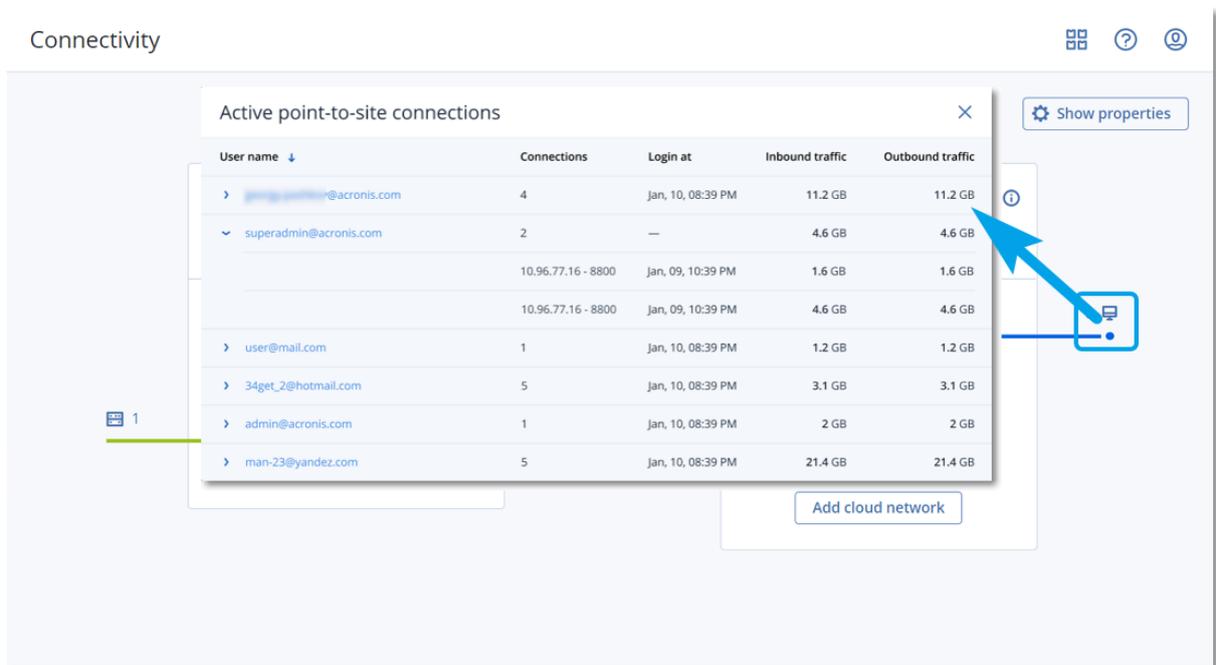
當設定檔更新之後，將無法透過舊的設定檔連線。確認將新檔案散發給獲允許使用點對站台連線的使用者。

作用中的點對站台連線

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以在 **[災難復原] > [連線]** 中檢視所有作用中的點對站台連線。按一下 **點對站台** 藍線上的電腦圖示，您將會看到依使用者名稱分組的作用中點對站台連線的詳細資訊。



對於 Active Directory 網域服務可用性的建議

如果受保護的工作負載需要在網域控制站中進行驗證，建議您在 Disaster Recovery 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 42 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。

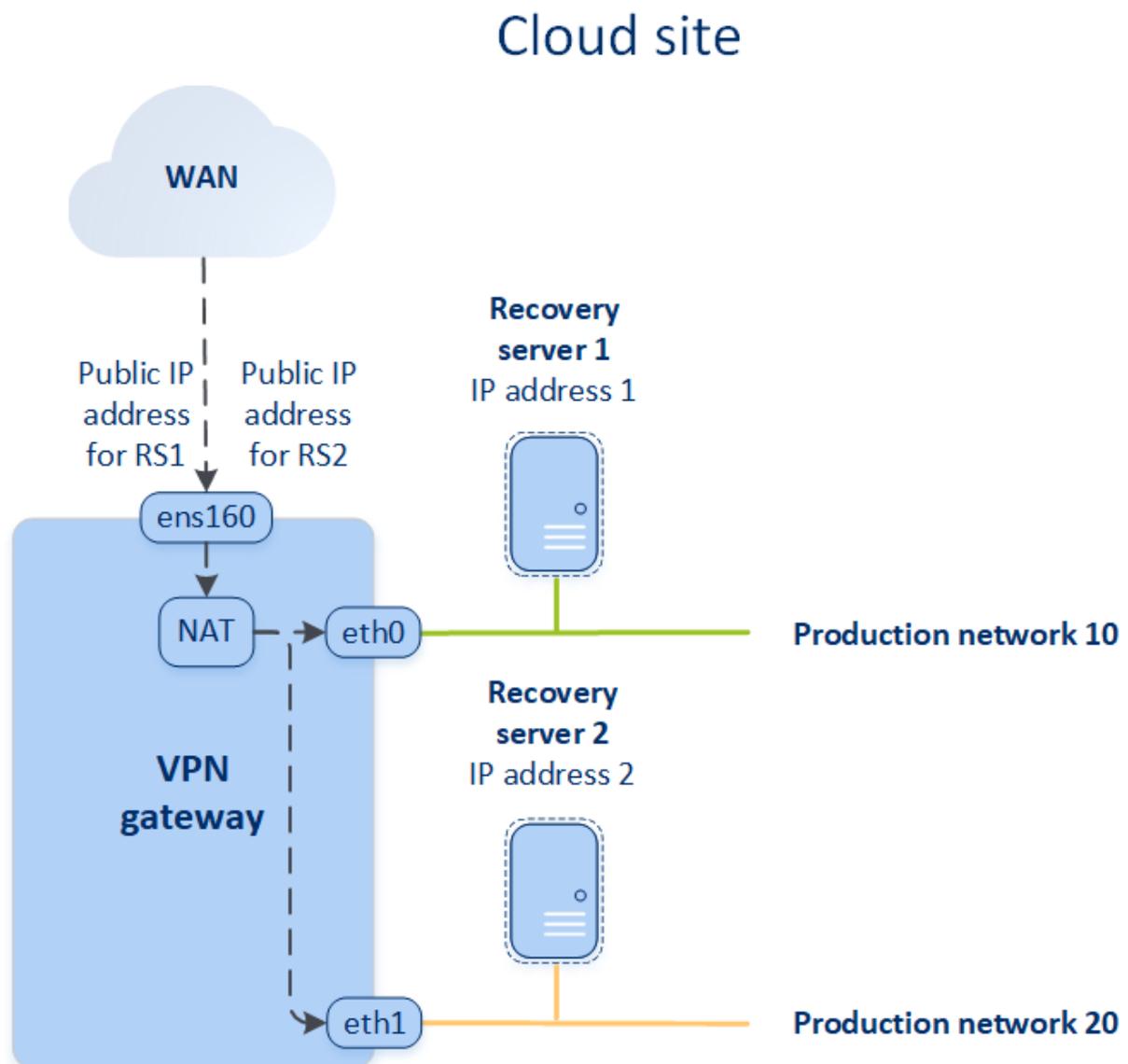
您可以透過自訂 DNS，為所有雲端伺服器設定您自己的自訂 DNS 伺服器。如需詳細資訊，請參閱 "設定自訂 DNS 伺服器" (第 42 頁)。

網路管理

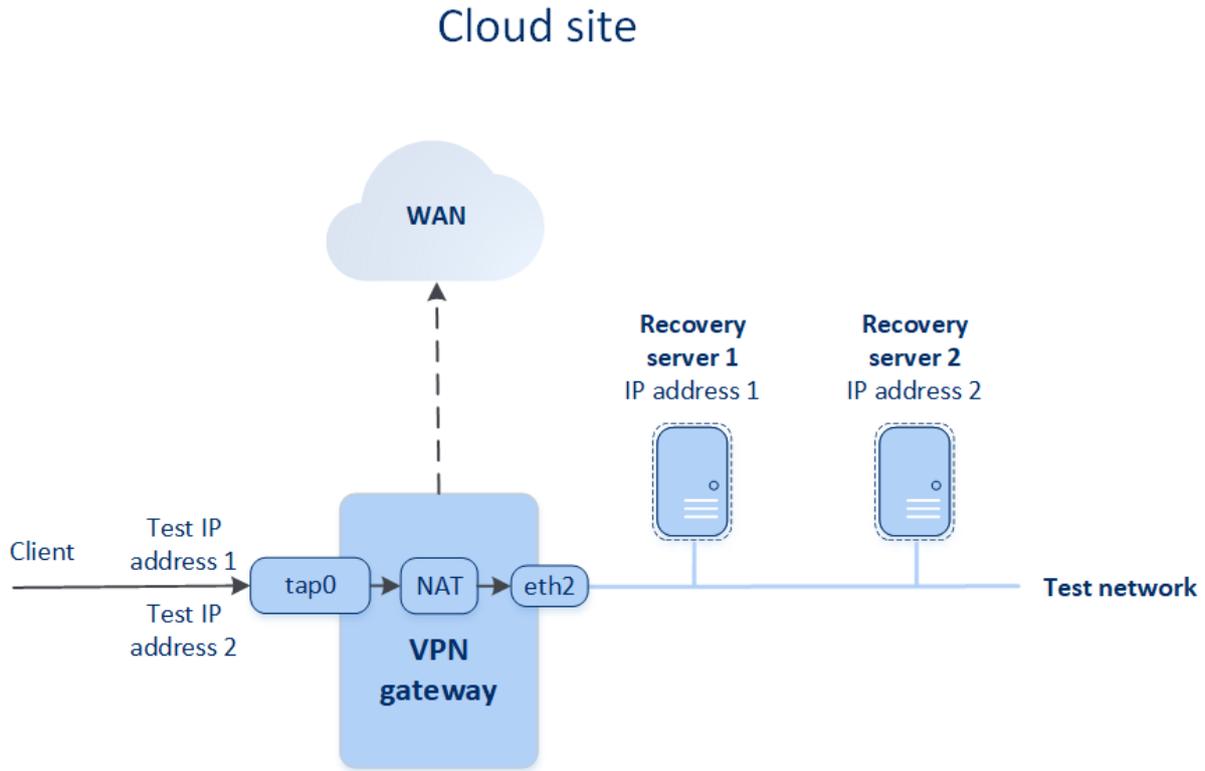
本節描述網路管理案例。

公用和測試 IP 位址

如果您在建立復原伺服器時指派公共 IP 位址，則復原伺服器會變成可以透過此 IP 位址，從網際網路使用。當具有目的地公共 IP 位址的封包來自網際網路時，VPN 閘道會使用 NAT，將其重新對應到個別的實際執行 IP 位址，然後將其傳送至對應的復原伺服器。



如果您在建立復原伺服器時指派測試 IP 位址，則復原伺服器會變成可以透過此 IP 位址，在測試網路中使用。如果您執行測試容錯移轉，當具有相同 IP 位址的復原伺服器在雲端的測試網路中啟動的同時，原始電腦仍在執行中。IP 位址不會發生衝突，因為測試網路遭到隔離。測試網路中的復原伺服器可透過其測試 IP 位址聯繫，這些 IP 位址會透過 NAT，重新對應到實際執行 IP 位址。



如需有關站台對站台 OpenVPN 的詳細資訊，請參閱 "站台對站台 OpenVPN - 其他資訊" (第 87 頁)。

IP 位址重新設定

為獲得適當的災難復原效能，指派給本機伺服器和雲端伺服器的 IP 位址必須一致。如果 IP 位址有任何不一致或不相符，您將會在 **[Disaster Recovery] > [連線]** 中對應網路的旁邊看到一個驚嘆號。

IP 位址不一致的部分常見原因列在下方：

1. 復原伺服器是從一個網路移轉到另一個網路，或者雲端網路的網路遮罩遭到變更。因此，雲端伺服器的 IP 位址來自未連線的網路。
2. 連線類型從沒有站台對站台連線切換到站台對站台連線。因此，本機伺服器置於不同於針對雲端站台上的復原伺服器而建立的網路。
3. 連線類型從站台對站台 OpenVPN 切換到多站台 IPsec VPN，或從多站台 IPsec VPN 切換到站台對站台 OpenVPN。如需有關此案例的詳細資訊，請參閱[切換連線](#)、"[從多站台 IPsec VPN 切換至站台對站台 OpenVPN](#)" (第 31 頁)和[重新指派 IP 位址](#)。
4. 在 VPN 設備站台上編輯下列網路參數：
 - 透過網路設定新增介面
 - 透過介面設定手動編輯網路遮罩
 - 透過 DHCP 編輯網路遮罩
 - 透過介面設定手動編輯網位址和路遮罩
 - 透過 DHCP 編輯網路遮罩和位址

上列動作的結果是，雲端站台上的網路可能會變成區域網路的子集或超集，或者 VPN 設備介面可能會針對不同的介面回報相同的網路設定。

若要解決網路設定的問題

1. 按一下需要 IP 位址重新設定的網路。
您將會看到所選網路中伺服器、其狀態以及 IP 位址的清單。其網路設定不一致的伺服器會以驚嘆號標示。
2. 若要變更伺服器的網路設定，按一下 **[前往伺服器]**。若要一次變更所有伺服器的網路設定，按一下通知區塊中的 **[變更]**。
3. 如有需要，請在 **[新 IP]** 和 **[新的測試 IP]** 欄位中進行變更，以變更 IP 位址。
4. 準備就緒後，按一下 **[確認]**。

將伺服器移至合適的網路

當您建立災難復原保護計劃，並將其套用到所選裝置時，系統會檢查裝置 IP 位址，如果沒有 IP 位址適用的現有雲端網路，就會自動建立雲端網路。預設會使用 IANA 建議的最大範圍，設定私人用途的雲端網路 (10.0.0.0/8、172.16.0.0/12、192.168.0.0/16)。您可以透過編輯網路遮罩來縮小網路的範圍。

如果選取的裝置位於多個區域網路上，則雲端站台上的網路可能會變成區域網路的超集。在此情況下，若要重新設定雲端網路：

1. 按一下需要重新設定網路大小的雲端網路，然後按一下 **[編輯]**。
2. 使用正確的設定，重新設定網路大小。
3. 建立其他所需的網路。
4. 按一下連線到網路的裝置數量旁邊的通知圖示。
5. 按一下 **[移至合適的網路]**。
6. 選擇您想要移至合適網路的伺服器，然後按一下 **[移動]**。

重新指派 IP 位址

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

在下列情況下，您必須重新指派雲端網路和雲端伺服器的 IP 位址以完成設定：

- 從站台對站台 OpenVPN 切換到多站台 IPsec VPN，或從多站台 IPsec VPN 切換到站台對站台 OpenVPN 之後。
- 套用保護計劃之後 (如果已設定多站台 IPsec VPN 連線)。

雲端網路

重新指派雲端網路的 IP 位址

1. 在 **[連線]** 索引標籤中，按一下雲端網路的 IP 位址。
2. 在 **[網路]** 快顯視窗中，按一下 **[編輯]**。
3. 輸入新的網路位址和網路遮罩。
4. 按一下 **[完成]**。

重新指派雲端網路的 IP 位址之後，您必須重新指派屬於重新指派之雲端網路的雲端伺服器。

雲端伺服器

重新指派伺服器的 IP 位址

1. 在 **[連線]** 索引標籤中，按一下伺服器在雲端網路中的 IP 位址。
2. 在 **[伺服器]** 快顯視窗中，按一下 **[變更 IP 位址]**。
3. 在 **[變更 IP 位址]** 快顯視窗中，輸入伺服器的新 IP 位址，或使用自動產生的 IP 位址 (重新指派的雲端網路一部分)。

注意事項

Cyber Disaster Recovery Cloud 會將雲端網路中的 IP 位址自動指派給雲端網路所屬的所有雲端伺服器，然後再重新指派網路 IP 位址。您可以使用建議的 IP 位址，一次重新指派所有雲端伺服器的 IP 位址。

4. 按一下 **[確認]**。

重新安裝 VPN 閘道

如果有您無法解決的 VPN 閘道問題，您可能需要重新安裝 VPN 閘道。可能的問題包括：

- VPN 閘道處於 **[錯誤]** 狀態。
- VPN 閘道長時間處於 **[等候中]** 狀態。
- VPN 閘道狀態長時間未確定。

重新安裝 VPN 閘道程序包括下列自動動作：完全刪除現有的 VPN 閘道虛擬機器、從範本安裝新的虛擬機器，然後在新的虛擬機器上套用先前 VPN 閘道的設定。

必要條件：

必須設定雲端站台的其中一個連線類型。

若要重新安裝 VPN 閘道

1. 在 Cyber Protect 主控台中，移至 **[Disaster Recovery]** > **[連線]**。
2. 按一下 VPN 閘道的齒輪圖示，然後選擇 **[重新安裝 VPN 閘道]**。
3. 在 **[重新安裝 VPN 閘道]** 對話方塊中，輸入您的登入資料。
4. 按一下 **[重新安裝]**。

設定自訂 DNS 伺服器

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

當您設定連線時，Cyber Disaster Recovery Cloud 會建立雲端網路基礎架構。雲端 DHCP 伺服器會將預設 DNS 伺服器自動指派給復原伺服器和主要伺服器，但是您可以變更預設設定，並設定自訂 DNS 伺服器。新的 DNS 設定將在下次對 DHCP 伺服器提出要求時套用。

必要條件

必須設定雲端站台的其中一個連線類型。

設定自訂 DNS 伺服器

1. 在 Cyber Protect 主控台中, 移至 **[Disaster Recovery]** > **[連線]**。
2. 按一下 **[顯示屬性]**。
3. 按一下 **[預設 (雲端站台所提供)]**。
4. 選擇 **[自訂伺服器]**。
5. 輸入 DNS 伺服器的 IP 位址。
6. [選用] 如果您想要新增其他 DNS 伺服器, 按一下 **[新增]**, 然後輸入 DNS 伺服器 IP 位址。

注意事項

新增自訂 DNS 伺服器之後, 您也可以新增預設 DNS 伺服器。如此一來, 如果自訂 DNS 伺服器無法使用, Cyber Disaster Recovery Cloud 將使用預設 DNS 伺服器。

7. 按一下**[完成]**。

刪除自訂 DNS 伺服器

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以從自訂 DNS 清單刪除 DNS 伺服器。

必要條件：

已設定自訂 DNS 伺服器。

刪除自訂 DNS 伺服器

1. 在 Cyber Protect 主控台中, 移至 **[Disaster Recovery]** > **[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 **[Disaster Recovery] > [連線]**。
2. 按一下 **[顯示屬性]**，然後按一下 **[本機路由]**。
3. 以 CIDR 標記法指定區域網路。
4. 按一下 **[儲存]**。

因此，來自指定之區域網路的伺服器可以與雲端伺服器通訊。

下載 MAC 位址

您可以下載 MAC 位址清單，然後加以解壓縮並匯入您自訂 DHCP 伺服器的組態中。

必要條件：

- 必須設定雲端站台的其中一個連線類型。
- 至少必須設定一個具有 MAC 位址的主要或復原伺服器。

若要下載 MAC 位址清單

1. 在 Cyber Protect 主控台中，移至 **[Disaster Recovery] > [連線]**。
2. 按一下 **[顯示屬性]**。
3. 按一下 **[下載 MAC 位址清單]**，然後儲存 CSV 檔案。

使用記錄

Disaster Recovery 會收集 VPN 設備和 VPN 開道的記錄。這些記錄會以 .txt 檔案形式儲存，這些檔案會壓縮在 .zip 存檔中。您可以下載並解壓縮存檔，然後使用該資訊進行疑難排解或監視。

下列清單描述 .zip 存檔中的記錄檔及其包含的資訊。

dnsmasq.config.txt - 該檔案包含有關提供 DNS 及 DHCP 位址之服務設定的資訊。

dnsmasq.leases.txt - 該檔案包含有關目前 DHCP 位址租用的資訊。

dnsmasq_log.txt - 該檔案包含 dnsmasq 服務的記錄。

eatables.txt - 該檔案包含有關防火牆資料表的資訊。

free.txt - 該檔案包含有關可用記憶體體的資訊。

ip.txt - 該檔案包含網路介面設定的記錄，包括可在進行**擷取網路封包**設定時使用的名稱。

NetworkManager_log.txt - 該檔案包含 NetworkManager 服務的記錄。

NetworkManager_status.txt - 該檔案包含有關 NetworkManager 服務狀態的資訊。

openvpn@p2s_log.txt - 該檔案包含 OpenVPN 服務的記錄。

openvpn@p2s_status.txt - 該檔案包含有關 VPN 通道狀態的資訊。

ps.txt - 該檔案包含有關目前在 VPN 閘道或 VPN 設備上執行的處理程序的資訊。

resolv.conf.txt - 該檔案包含有關 DNS 伺服器設定的資訊。

routes.txt - 該檔案包含有關網路路由的資訊。

uname.txt - 該檔案包含有關作業系統核心之目前版本的資訊。

uptime.txt - 該檔案包含有關尚未重新啟動作業系統之期間長度的資訊。

vpnserver_log.txt - 該檔案包含 VPN 服務的記錄。

vpnserver_status.txt - 該檔案包含有關 VPN 伺服器狀態的資訊。

如需有關 IPsec VPN 連線之特定記錄檔的詳細資訊，請參閱 "多站台 IPsec VPN 記錄檔" (第 34 頁)。

下載 VPN 設備的記錄

您可以下載並解壓縮包含 VPN 設備記錄的存檔，然後使用該資訊進行疑難排解或監視。

若要下載 VPN 設備的記錄，請執行下列動作

1. 在**連線**頁面上，按一下 VPN 設備旁的齒輪圖示。
2. 按一下**下載記錄**。
3. [選用] 選擇**擷取網路封包**，然後進行設定。如需詳細資訊，請參閱 "擷取網路封包" (第 45 頁)。
4. 按一下**[完成]**。
5. 當 .zip 存檔準備就緒可供下載時，請按一下**下載記錄**，然後將其儲存在本機。

下載 VPN 閘道的記錄

您可以下載並解壓縮包含 VPN 閘道記錄的存檔，並使用該資訊進行疑難排解或監視。

若要下載 VPN 閘道的記錄，請執行下列動作

1. 在**連線**頁面上，按一下 VPN 閘道旁的齒輪圖示。
2. 按一下**下載記錄**。
3. [選用] 選擇**擷取網路封包**，然後進行設定。如需詳細資訊，請參閱 "擷取網路封包" (第 45 頁)。
4. 按一下**[完成]**。
5. 當 .zip 存檔準備就緒可供下載時，請按一下**下載記錄**，然後將其儲存在本機。

擷取網路封包

若要對本機生產站台與主要或復原伺服器之間的通訊進行疑難排解及分析，您可以選擇以收集 VPN 閘道或 VPN 設備上的網路封包。

收集 32,000 個網路封包或達到時間限制後，網路封包擷取即會停止，而結果會寫入 .libpcap 檔案，且該檔案會新增至記錄的 .zip 存檔。

下表提供有關您可以設定之**擷取網路封包**設定的詳細資訊。

設定	描述
網路 介面 名稱	擷取網路封包所在的網路介面。如果要擷取所有網路介面上的網路封包，請選擇任何。
時間 限制 (秒)	擷取網路封包的時間限制。您可以設定的最大值為 1800。
篩選	<p>要在擷取的網路封包上套用的額外篩選條件。</p> <p>您可以輸入包含通訊協定、連接埠、方向及其組合的字串，並以空格分隔，例如："and"、"or"、"not"、"("、")"、"src"、"dst"、"net"、"host"、"port"、"ip"、"tcp"、"udp"、"icmp"、"arp"、"esp"。</p> <p>如果要使用括弧，請在前後加上空格。您也可以輸入 IP 位址及網路位址，例如："icmp or arp" 及 "port 67 or 68"。</p> <p>如需有關您可以輸入的值的詳細資訊，請參閱 Linux tcpdump 說明。</p>

雲端伺服器

您可以透過災難復原，使用兩種類型的雲端伺服器：主要和復原。

主要伺服器是未與本機站台上的電腦連結的虛擬機器。您可以使用主要伺服器來保護特定應用程式或執行各種輔助服務 (例如網頁伺服器)。

復原伺服器是原始電腦 (受保護伺服器) 複本的虛擬機器。復原伺服器是以儲存在雲端的受保護伺服器備份為基礎。發生災難時，復原伺服器用於從原始伺服器切換工作負載。

設定復原伺服器

復原伺服器：原始電腦的一個複本，以儲存在雲端的受保護伺服器備份為基礎。復原伺服器在發生災難時，用於從原始伺服器切換工作負載。

建立復原伺服器時，您必須指定下列網路參數：

參數	描述
雲端網路	(必填) 將與復原伺服器連線的雲端網路。
實際執行網路中的 IP 位址	(必填) 將啟動復原伺服器之虛擬機器所使用的 IP 位址。此位址同時用於實際執行網路和測試網路。啟動前，系統會設定虛擬機器以透過 DHCP 取得 IP 位址。
測試 IP 位址	(選填) 在測試容錯移轉期間，從用戶端實際執行網路存取復原伺服器所使用的 IP 位址，以防實際執行 IP 位址在相同網路中重複。此 IP 位址不同於實際執行網路中的 IP 位址。本機站台中的伺服器可以在測試容錯移轉期間，透過測試 IP 位址聯繫復原伺服器，但是無法反向進行存取。如果在復原伺服器建立期間選取 [網際網路存取] 選項，則可以在測試網路中從復原伺服器進行網際網路存取。
公用 IP 位址	(選填) 從網際網路存取復原伺服器所使用的 IP 位址。如果伺服器沒有公用 IP 位址，則僅能從區域網路聯繫該伺服器。
網際網路存取	(選填) 可讓復原伺服器存取網際網路 (在實際執行和測試容錯移轉的情況下)。

建立復原伺服器

若要建立將成為工作負載副本的復原伺服器，請遵循以下程序進行。您還可以觀看演示過程的 [影片教學](#)。

重要事項

當您執行容錯移轉時，您僅能選取建立復原伺服器之後所建立的復原點。

必要條件

- 保護計劃必須套用到您要保護的原始電腦。此計劃必須在雲端儲存空間備份整部電腦，或僅備份開機及提供必要服務所需的磁碟。
- 必須設定雲端站台的其中一個連線類型。

建立復原伺服器

1. 在 **[所有裝置]** 索引標籤上，選取您要保護的電腦。
2. 按一下 **[災難復原]**，然後按一下 **[建立復原伺服器]**。
3. 在 **[建立復原伺服器]** 精靈的 **[伺服器組態]** 索引標籤上，執行下列動作：
 - a. 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 60 頁)。

- b. [選用] 變更復原伺服器的預設名稱。
 - c. [選用] 新增說明。
4. 在 **[網路]** 索引標籤上，執行下列動作：
 - a. 指定將與伺服器連線的雲端網路。
 - b. 選擇 **[DHCP]** 選項。

DHCP 選項	描述
雲端站台所提供	這是預設設定。伺服器的 IP 位址將由雲端中自動設定的 DHCP 伺服器提供。
自訂	伺服器的 IP 位址將由雲端中您自己的 DHCP 伺服器提供。

- c. 指定 **[MAC 位址]**。
MAC 位址是指派給伺服器網路介面卡的唯一識別碼。如果使用自訂 DHCP，您可以將其設定為一律指派特定的 IP 位址給特定的 MAC 位址。因此，您將確保復原伺服器一律取得相同的 IP 位址。您可以執行具有以 MAC 位址註冊之授權的應用程式。
- d. 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。

- e. [選用] 選取 **[測試 IP 位址]** 核取方塊，然後指定 IP 位址。
如果選擇此設定，則您可以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。在測試容錯移轉期間，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。
如果您未選擇此設定，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。

您可以選擇其中一個建議的 IP 位址，或輸入其他位址。

- f. [選用] 選取 **[網際網路存取]** 核取方塊。

如果您選擇此設定，復原伺服器將可在實際執行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。

- g. [選用] 選取 **[使用公共 IP 位址]** 核取方塊。

您可以使用公用 IP 位址，在容錯移轉或測試容錯移轉期間，從網際網路存取復原伺服器。若未選擇此選項，則伺服器僅適用於實際執行網路。

[使用公共 IP 位址] 選項需要選擇 **[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 **[使用公共 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。

5. 在 **[設定]** 索引標籤上，選擇 **[設定 RPO 閾值]**，然後設定值。

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。

6. [選擇性][如果所選電腦的備份是使用加密作為電腦屬性來加密的]，請指定從加密備份建立用於復原伺服器的虛擬機器時將會自動使用的密碼。

- a. 按一下 **[輸入密碼]**，然後輸入加密備份的密碼，並定義認證的名稱。

根據預設，您將會在清單中看到最新的備份。

- b. 若要檢視所有備份，選取 **[顯示所有備份]**。

- c. 按一下 **[儲存]**。
-

注意事項

雖然您指定的密碼將會儲存在安全的認證存放區中，但儲存密碼可能會違反您的合規義務。

7. 在 **[雲端防火牆規則]** 索引標籤上，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 57 頁)。

8. 按一下 **[建立]**。

復原伺服器將會出現在主控台的 **[Disaster Recovery] > [伺服器] > [復原伺服器]** 索引標籤中。

Name	Status	State	RPO compliance	VM state
Win16	OK	Standby	—	—
cen7-sg7	OK	Standby	—	—
Cen_vg-1	OK	Fallover	Not set	On
Cen_mb-3	OK	Testing fallover	Not set	On
Cen_mb-2	OK	Fallback	Not set	Off
Cen_mb-1	OK	Fallback	Not set	Off

次要伺服器的操作

在 Cyber Protect 主控台中，主要伺服器會顯示在 **[Disaster Recovery] > [伺服器] > [復原伺服器]** 索引標籤上。

開啟電源

若要開啟復原伺服器電源

1. 在 **[復原伺服器]** 索引標籤上，按一下復原伺服器。
2. 按一下 **[開啟電源]**。

關閉電源

若要關閉復原伺服器電源

1. 在 **[復原伺服器]** 索引標籤上，按一下復原伺服器。
2. 按一下 **[關閉電源]**。
3. 在 **[關閉伺服器電源]** 畫面中，按一下 **[關閉電源]**。

強制關閉電源

若要強制關閉復原伺服器電源

1. 在 **[復原伺服器]** 索引標籤上，按一下復原伺服器。
2. 按一下 **[關閉電源]**。
3. 在 **[關閉伺服器電源]** 畫面中，選擇 **[強制關閉伺服器]**，然後按一下 **[關閉電源]**。

停止

若要停止復原伺服器

1. 在 **[復原伺服器]** 索引標籤上，按一下復原伺服器。
2. 按一下 **[停止]**。

編輯設定

若要編輯復原伺服器的設定

1. 在 **[復原伺服器]** 索引標籤上，按一下復原伺服器。
2. 按一下 **[停止]**。
3. 按一下 **[編輯]**，然後編輯設定。

套用保護計劃

若要將計劃套用到主要伺服器

1. 在 **[主要伺服器]** 索引標籤上，按一下主要伺服器。
2. 在 **[計劃]** 索引標籤上，按一下 **[建立]**。

您將會看到預先定義的保護計劃，您只能在其中變更排程和保留規則。如需詳細資訊，請參閱「[備份雲端伺服器](#)」。

設定主要伺服器

主要伺服器是一部虛擬機器，相較於復原伺服器，在本機站台上沒有連結的機器。主要伺服器用於透過複寫保護應用程式，或用於執行各種輔助服務（例如，網頁伺服器）。

一般而言，主要伺服器用於執行重要應用程式之伺服器之間的即時資料複寫。您應使用應用程式的原生工具，自行設定複寫。例如：可以在本機伺服器和主要伺服器之間設定 Active Directory 複寫或 SQL 複寫。

或者，主要伺服器可以包含在 AlwaysOn 可用性群組 (AAG) 或資料庫可用性群組 (DAG) 中。

這兩種方法都需要深入瞭解應用程式和系統管理員權限。主要伺服器會持續消耗快速災難復原儲存空間上的計算資源與空間。它需要您那一端的維護：監控複寫、安裝軟體更新以及備份。其優點是最小的 RPO 和 RTO，以及實際執行環境的最小負載（相較於將整個伺服器備份到雲端而言）。

主要伺服器一律僅在實際執行網路中啟動，而且有下列網路參數：

參數	描述
雲端網路	(必填) 將與主要伺服器連線的雲端網路。
實際執行網路中的 IP 位址	(必填) 主要伺服器將在實際執行網路中具備的 IP 位址。根據預設，會設定您實際執行網路中的第一個可用 IP 位址。
公用 IP 位址	(選填) 從網際網路存取主要伺服器所使用的 IP 位址。如果伺服器沒有公用 IP 位址，則僅能從區域網路（而無法透過網際網路）聯繫該伺服器。
網際網路存取	(選填) 可讓主要伺服器存取網際網路。

建立主要伺服器

必要條件

- 必須設定雲端站台的其中一個連線類型。

建立主要伺服器

1. 移至 **[Disaster Recovery]** > **[伺服器]** > **[主要伺服器]** 索引標籤。
2. 按一下 **[建立]**。
3. 在 **[建立主要伺服器]** 精靈的 **[伺服器組態]** 索引標籤上，執行下列動作：
 - a. 為新的虛擬機器選取範本。
 - b. 選擇設定類別 (虛擬核心數目以及 RAM 大小)。

下表顯示每個類別的磁碟空間總數上限 (GB)。

類型	vCPU	RAM (GB)	磁碟空間總數上限 (GB)
F1	1	2	500
F2	1	4	1,000
F3	2	8	2,000
F4	4	16	4,000
F5	8	32	8,000
F6	16	64	16,000
F7	16	128	32,000
F8	16	256	64,000

- c. [選擇性] 變更虛擬磁碟大小。如果您需要多個硬碟，請按一下 **[新增磁碟]**，然後指定新磁碟的大小。您可以針對主要伺服器新增最多 10 個磁碟。
 - d. 變更復原伺服器的預設名稱。
 - e. 新增說明。
4. 在 **[網路]** 索引標籤上，執行下列動作：
 - a. 指定主要伺服器將包含在內的雲端網路。
 - b. 選擇 **[DHCP]** 選項。

DHCP 選項	描述
雲端站台所提供	這是預設設定。伺服器的 IP 位址將由雲端中自動設定的 DHCP 伺服器提供。
自訂	伺服器的 IP 位址將由雲端中您自己的 DHCP 伺服器提供。

- c. 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。
 - d. 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。

- e. [選用] 選取 **[網際網路存取]** 核取方塊。

如果您選擇此選項，主要伺服器將可存取網際網路。預設開放 TCP 連接埠 25，以供與公用 IP 位址的輸出連線使用。

- f. [選用] 選取 **[使用公共 IP 位址]** 核取方塊。

您可以使用公用 IP 位址，從網際網路存取主要伺服器。若未選擇此設定，則伺服器僅適用於實際執行網路。

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 **[使用公共 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。

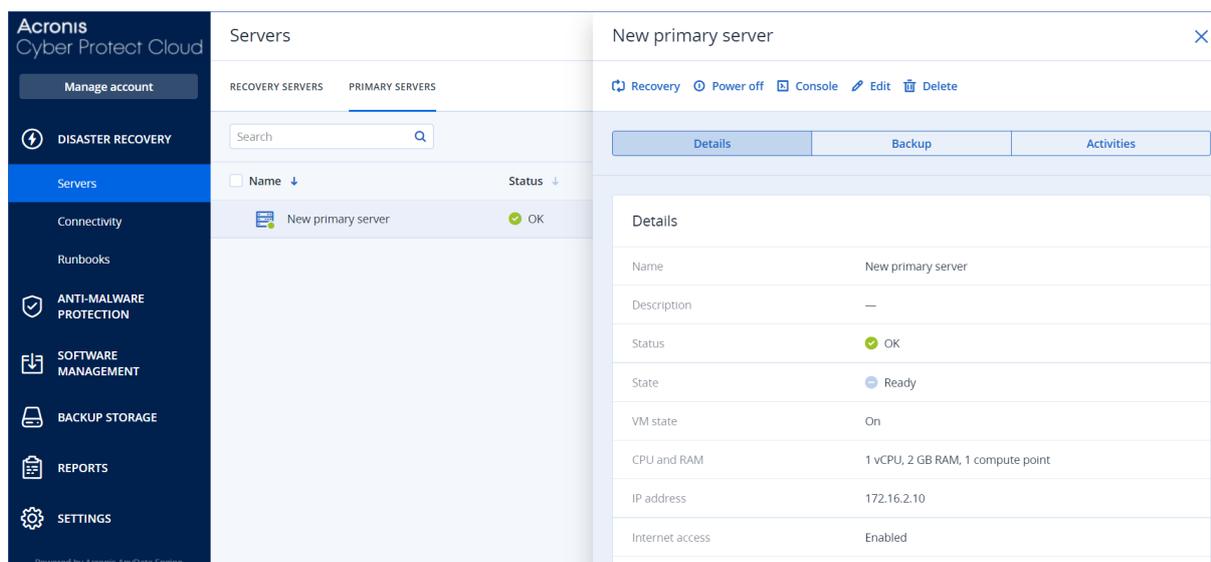
5. [選擇性] 在 **[設定]** 索引標籤上，選擇 **[設定 RPO 閾值]**，然後設定值。

RPO 閾值會定義上次復原點和目前時間之間的最大時間間隔。此值可以設定在 15 - 60 分鐘、1 - 24 小時、1 - 14 天內。

6. [選擇性] 在 **[雲端防火牆規則]** 索引標籤上，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 57 頁)。

7. 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。



The screenshot displays the Acronis Cyber Protect Cloud management console. On the left is a dark blue navigation sidebar with icons for 'Manage account', 'DISASTER RECOVERY', 'Servers', 'Connectivity', 'Runbooks', 'ANTI-MALWARE PROTECTION', 'SOFTWARE MANAGEMENT', 'BACKUP STORAGE', 'REPORTS', and 'SETTINGS'. The main area is titled 'Servers' and has tabs for 'RECOVERY SERVERS' and 'PRIMARY SERVERS'. A search bar is present. Below it, a table lists servers, with one entry 'New primary server' having a status of 'OK'. A modal window titled 'New primary server' is open, showing a 'Details' tab. The details include: Name: New primary server; Description: —; Status: OK; State: Ready; VM state: On; CPU and RAM: 1 vCPU, 2 GB RAM, 1 compute point; IP address: 172.16.2.10; Internet access: Enabled. At the bottom of the sidebar, it says 'Powered by Acronis AnyData Engine'.

主要伺服器的操作

在 Cyber Protect 主控台中，主要伺服器會顯示在 **[Disaster Recovery] > [伺服器] > [主要伺服器]** 索引標籤上。

開啟電源

若要開啟主要伺服器電源

1. 在 **[主要伺服器]** 索引標籤上，按一下主要伺服器。
2. 按一下 **[開啟電源]**。

關閉電源

若要關閉主要伺服器電源

1. 在 **[主要伺服器]** 索引標籤上，按一下主要伺服器。
2. 按一下 **[關閉電源]**。
3. 在 **[關閉伺服器電源]** 畫面中，按一下 **[關閉電源]**。

強制關閉電源

若要強制關閉主要伺服器電源

1. 在 **[主要伺服器]** 索引標籤上，按一下主要伺服器。
2. 按一下 **[關閉電源]**。
3. 在 **[關閉伺服器電源]** 畫面中，選擇 **[強制關閉伺服器]**，然後按一下 **[關閉電源]**。

停止

若要停止主要伺服器

1. 在 **[主要伺服器]** 索引標籤上，按一下主要伺服器。
2. 按一下 **[停止]**。

編輯設定

若要編輯主要伺服器的設定

1. 在 **[主要伺服器]** 索引標籤上，按一下主要伺服器。
2. 按一下 **[停止]**。
3. 按一下 **[編輯]**，然後編輯設定。

套用保護計劃

若要將計劃套用到主要伺服器

1. 在 **[主要伺服器]** 索引標籤上，按一下主要伺服器。
2. 在 **[計劃]** 索引標籤上，按一下 **[建立]**。

您將會看到預先定義的保護計劃，您只能在其中變更排程和保留規則。如需詳細資訊，請參閱「[備份雲端伺服器](#)」。

檢視有關雲端伺服器的詳細資料

若要檢視雲端伺服器的詳細資料，請移至 **[Disaster Recovery] > [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	<p>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。</p> <p>其計算方式如下：</p> <p>RPO 合規 = 實際 RPO/RPO 閾值</p> <p>其中：</p> <p>實際 RPO = 目前時間 - 上次復原點時間</p> <p>RPO 合規狀態</p> <p>根據實際 RPO 和 RPO 閾值間比率的值，會使用下列狀態：</p> <ul style="list-style-type: none"> • 合規。RPO 合規 < 1x。伺服器符合 RPO 閾值。 • 超過。RPO 合規 <= 2x。伺服器違反 RPO 閾值。 • 嚴重超過。RPO 合規 <= 4x。伺服器違反 RPO 閾值超過 2x 次。 • 極度超過。RPO 合規 > 4x。伺服器違反 RPO 閾值超過 4x 次。 • 擱置中 (無備份)。伺服器受到保護計劃保護，但備份正在建立，而且還未完成。
實際 RPO	自上次建立復原點後經過的時間
上次復原點	建立上次復原點的日期與時間

雲端伺服器的備份

主要伺服器和復原伺服器是無代理程式備份在雲端站台上。這些備份具有以下限制。

- 唯一的備份位置是雲端儲存。主要伺服器會備份到**主要伺服器備份**儲存空間。

注意事項

不支援 Microsoft Azure 備份位置。

- 備份計劃無法套用到多個伺服器。每個伺服器必須有自己的備份計劃，即使所有備份計劃具有相同設定也一樣。
- 只有一個備份計劃可以套用到網站。
- 不支援應用程式感知備份。
- 加密不可使用。
- 備份選項不可使用。

當您刪除主要伺服器時，也同時刪除其備份。

復原伺服器僅在容錯移轉狀態中才會備份。其備份會繼續原始伺服器的備份順序。執行容錯回復時，原始伺服器會繼續此備份順序。因此，復原伺服器的備份只能以手動方式刪除，或當做套用保留規則的結果。當刪除復原伺服器時，其備份一律會保留。

注意事項

雲端伺服器的備份計劃是根據 UTC 時間執行的。

雲端伺服器的防火牆規則

您可以將防火牆規則設定為控制雲端站台上，主要伺服器和復原伺服器的輸入及輸出流量。

您可以在佈建雲端伺服器的公用 IP 位址後設定輸入規則。預設允許 TCP 連接埠 443，並拒絕其他所有輸入連線。您可以變更預設防火牆規則，並新增或移除輸入例外。如果未佈建公用 IP，您僅能檢視輸入規則，但無法進行設定。

您可以在佈建雲端伺服器的網際網路存取後設定輸出規則。預設拒絕 TCP 連接埠 25，並允許其他所有輸出連線。您可以變更預設防火牆規則，並新增或移除輸出例外。如果未佈建網際網路存取，您僅能檢視輸出規則，但無法進行設定。

注意事項

基於安全性原因，有一些預先定義且您無法變更的防火牆規則。

針對輸入和輸出連線：

- 允許 Ping: ICMP echo-request (type 8, code 0) and ICMP echo-reply (type 0, code 0)
- Permit ICMP need-to-frag (type 3, code 4)
- Permit TTL exceeded (type 11, code 0)

僅針對輸入連線：

- 無法設定的部分：全部拒絕

僅針對輸出連線：

- 無法設定的部分：全部拒絕
-

設定雲端伺服器的防火牆規則

您可以針對雲端的主要伺服器和復原伺服器編輯預設防火牆規則。

若要編輯雲端站台上伺服器的防火牆規則

1. 在 Cyber Protect 主控台中，移至 **[Disaster Recovery] > [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： <ul style="list-style-type: none">• 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： <ul style="list-style-type: none">• 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： <ul style="list-style-type: none">• 特定 IP 位址 (例如，192.168.0.0)

防火牆參數	描述
	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 特定 IP 位址 (例如, 192.168.0.0) • 使用 CIDR 標記法的 IP 位址範圍 (例如, 192.168.0.0/24) • 任何 IP 位址。如果您希望將規則套用到任何 IP 位址, 請使用 *。

10. 如果您要移除現有的輸出例外, 按一下旁邊的垃圾桶圖示。
11. 按一下 **[儲存]**。

檢查雲端防火牆活動

雲端伺服器防火牆規則設定更新後，更新活動記錄會出現在 Cyber Protect 主控台中。您可以檢視記錄並檢查下列資訊：

- 更新設定之使用者的使用者名稱
- 更新的日期和時間
- 輸入和輸出連線的防火牆設定
- 輸入和輸出連線的預設動作
- 輸入和輸出連線例外的通訊協定、連接埠和 IP 位址

若要檢視有關雲端防火牆規則設定變更的詳細資訊

1. 在 Cyber Protect 主控台中，按一下 **[監控] > [活動]**。
2. 按一下對應的活動，然後按一下 **[所有屬性]**。
活動的描述應該是 **[正在更新雲端伺服器設定]**。
3. 在 **[內容]** 欄位中，檢查您感興趣的資訊。

計算點

在 [Disaster Recovery] 中，計算點在測試容錯移轉和實際執行容錯移轉期間用於主要伺服器及復原伺服器。計算點會反映在雲端執行伺服器 (虛擬機器) 所使用的計算資源。

計算點在災難復原期間的耗用量取決於伺服器的參數，以及伺服器處於容錯移轉狀態期間的持續時間。伺服器越強大且時間越長，耗用的計算點越多。此外，耗用的計算點越多，您要支付的價格就越高。

在 Acronis Cloud 中執行的所有伺服器，無論其狀態為開啟或關閉，都將根據計算點設定的類別收費。

處於 [待命] 狀態的復原伺服器不會耗用計算點，也不會產生計算點費用。

在下表中，您可以看到雲端中 8 部不同類別伺服器的範例，及其每小時耗用的對應計算點。您可以在 [\[詳細資料\]](#) 索引標籤中變更伺服器的類別。

類型	CPU	RAM	計算點
F1	1 個 vCPU	2 GB	1
F2	1 個 vCPU	4 GB	2
F3	2 個 vCPU	8 GB	4
F4	4 個 vCPU	16 GB	8
F5	8 個 vCPU	32 GB	16
F6	16 個 vCPU	64 GB	32
F7	16 個 vCPU	128 GB	64
F8	16 個 vCPU	256 GB	128

您可以使用表格中的資訊，輕鬆地估計一部伺服器 (虛擬機器) 將耗用的計算點數量。

例如，如果您要使用 [Disaster Recovery] 保護一部擁有 4 個 vCPU* 16 GB RAM 的虛擬機器，以及一部擁有 2 個 vCPU 8 GB RAM 的虛擬機器，則第一部虛擬機器每小時將耗用 8 個計算點，第二部虛擬機器每小時將耗用 4 個計算點。如果兩部虛擬機器都處於容錯移轉狀態，則總耗用量將為每小時 12 個計算點，或整天 288 個計算點 (12 個計算點 x 24 小時 = 288 個計算點)。

* vCPU 指的是指派給虛擬機器的實體中央處理器 (CPU)，而且是與時間相關的實體。

注意事項

如果達到**計算點**配額的超額，所有主要伺服器和復原伺服器都將關閉。在下一個計費週期開始之前，或在您增加配額之前，將無法使用這些伺服器。預設計費週期是一整個月。

測試容錯移轉

執行測試容錯移轉指的是在與您工作網路分開的測試 VLAN 中，啟動復原伺服器。您一次可以測試數部復原伺服器，並檢查其互動。在測試網路中，伺服器會使用其實際執行 IP 位址進行通訊，但它們無法啟動與您區域網路內工作負載的 TCP 或 UDP 連線。

在測試容錯移轉期間，虛擬機器 (復原伺服器) 並未最終化。代理程式會直接從備份讀取虛擬磁碟的內容，並隨機存取備份的不同部分。這可能會使處於測試容錯移轉狀態的復原伺服器的效能比其正常效能慢。

執行測試容錯移轉

雖然執行測試容錯移轉是選擇性的，但我們建議您就成本和安全考量，以適當頻率定期執行。有一個好作法是建立 Runbook，也就是一組說明如何在雲端啟動實際執行環境的指示。

重要事項

您必須事先 [建立復原伺服器](#) 以保護您的裝置免受災難影響。

您只能從建立裝置的復原伺服器後所建立的復原點 (備份) 執行容錯移轉。

容錯移轉至復原伺服器之前，必須至少建立一個復原點。支援的復原點數量上限為 100。

執行測試容錯移轉

1. 選取原始電腦或選取您要測試的復原伺服器。
2. 按一下 **[Disaster Recovery]**。
接著會開啟復原伺服器的說明。
3. 按一下 **[容錯移轉]**。
4. 選取容錯移轉類型 **[測試容錯移轉]**。
5. 選擇復原點 (備份)，然後按一下 **[開始]**。
6. 如果您選擇的備份是使用加密作為機器屬性加密的：
 - a. 輸入備份集的加密密碼。

注意事項

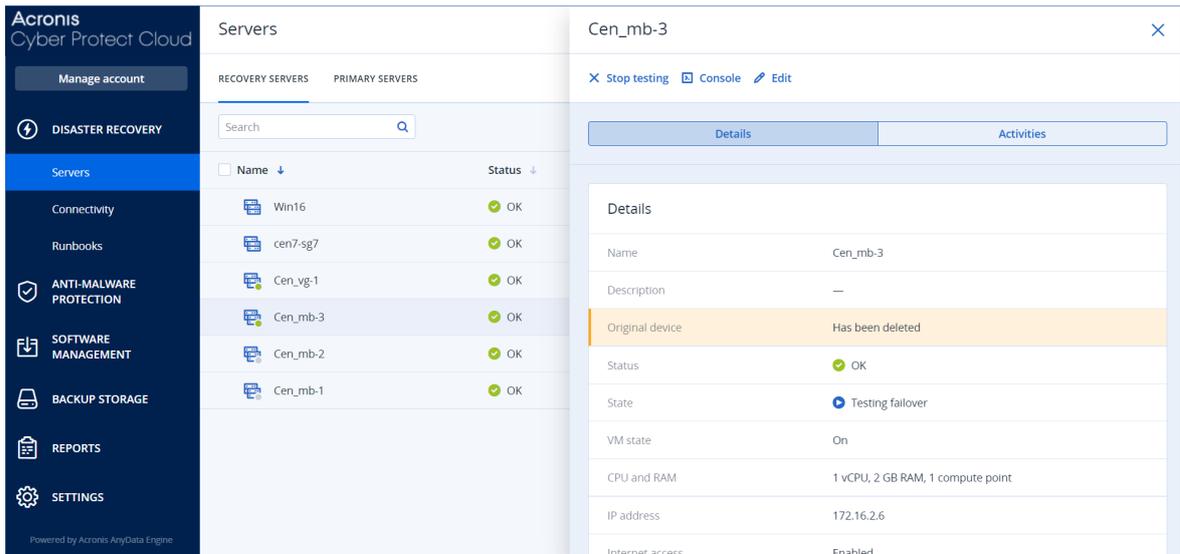
此密碼僅會暫時儲存，而且將僅用於目前的測試容錯移轉作業。在測試容錯移轉停止時或測試容錯移轉作業完成後，此密碼會自動從認證存放區中刪除。

- b. **[選用]** 若要儲存備份集的密碼並將其用於後續的容錯移轉作業，請選擇 **[將密碼儲存在安全的認證存放區中...]** 核取方塊，然後在 **[認證名稱]** 欄位中，輸入認證的名稱。
-

重要事項

密碼將儲存在安全的認證存放區中，而且將在後續的容錯移轉作業中自動套用。但是，儲存密碼可能會與法規遵循義務相衝突。

- c. 按一下 **[完成]**。
當復原伺服器啟動時，其狀態會變更為 **[正在測試容錯移轉]**。



7. 使用下列任何一個方法測試復原伺服器：

- 在 **[Disaster Recovery] > [伺服器]** 中，選取復原伺服器，然後按一下 **[主控台]**。
- 使用 RDP 或 SSH，以及您在建立復原伺服器時指定的測試 IP，連線到復原伺服器。在實際執行網路內部和外部皆嘗試連線 (如「點對站台連線」中所述)。
- 在復原伺服器內執行指令碼。
指令碼可檢查登入畫面、應用程式是否啟動、網際網路連線，以及其他電腦連線到復原伺服器的能力。
- 如果復原伺服器具備網際網路存取權和公共 IP 位址，您可能會想使用 TeamViewer。

8. 當測試完成時，按一下 **[停止測試]**。

復原伺服器隨即停止。在測試容錯移轉期間針對復原伺服器所做的變更都不會保留。

注意事項

在 Runbook 中，或在手動啟動測試容錯移轉時，**[啟動伺服器]** 和 **[停止伺服器]** 動作都不適用於測試容錯移轉作業。如果您嘗試執行此種動作，將會失敗，並出現下列錯誤訊息：

失敗：此動作不適用於目前的伺服器狀態。

自動測試容錯移轉

使用自動測試容錯移轉，每月自動測試復原伺服器一次，無需任何手動互動。

自動測試容錯移轉程序包含下列部分：

1. 從最後一個復原點建立虛擬機器
2. 擷取虛擬機器的螢幕擷取畫面
3. 分析虛擬機器的作業系統是否啟動成功
4. 通知您有關測試容錯移轉狀態

注意事項

自動測試容錯移轉會使用計算點。

您可以在復原伺服器的設定中設定自動測試容錯移轉。如需詳細資訊，請參閱 "設定自動測試容錯移轉" (第 63 頁)。

請注意，在極少數情況下，自動測試容錯移轉可能會被跳過，而且可能不會在排程時間執行。這是因為生產故障容錯移轉的優先順序高於自動測試容錯移轉，因此配置給自動測試容錯移轉的硬體資源 (CPU 和 RAM) 可能會暫時受限，以確保有足夠資源用於並行的生產容錯移轉。

如果出於某種原因而跳過自動測試容錯移轉，則會發出警示。

注意事項

如果原始機器的反斜線使用加密作為機器屬性進行加密，並且在創建復原後的磁碟區序列化程式時未指定加密傳遞磁碟，則自動化測試容錯回復將會失敗。有關指定加密傳遞磁碟的更多資訊，請參見 "建立復原伺服器" (第 47 頁)。

設定自動測試容錯移轉

透過設定自動測試容錯移轉，可以每月測試您的復原伺服器，無需執行任何手動動作。

若要設定自動測試容錯移轉

1. 在主控台中，移至 **[災難復原] > [伺服器] > [復原伺服器]**，然後選擇復原伺服器。
2. 按一下 **[編輯]**。
3. 在 **[自動測試容錯移轉]** 索引標籤的 **[排程]** 欄位中，選擇 **[每月]**。
4. 在 **[螢幕擷取畫面逾時]** 中，變更系統嘗試執行自動測試容錯移轉的最長時間預設值 (以分鐘為單位)。
5. 如果您想要將 **[螢幕擷取畫面逾時]** 值儲存為預設值，並在啟用其他復原伺服器的自動測試容錯移轉時將其自動填入，請選擇 **[設為預設逾時]**。
6. 按一下 **[儲存]**。

檢視自動測試容錯移轉狀態

您可以檢視完整的自動測試容錯移轉詳細資料，例如狀態、開始時間、結束時間、持續時間，以及虛擬機器的螢幕擷取畫面。

注意事項

虛擬機器的螢幕擷取畫面會保留，直到自動測試容錯移轉再次執行並產生新的螢幕擷取畫面為止。

若要檢視復原伺服器的自動測試容錯移轉狀態

1. 在主控台中，移至 **[災難復原] > [伺服器] > [復原伺服器]**，然後選擇復原伺服器。
2. 在 **[自動測試容錯移轉]** 區段中，查看上次自動測試容錯移轉的詳細資料。
3. 若要檢視虛擬機器的螢幕擷取畫面，請按一下 **[顯示螢幕擷取畫面]**。

停用自動測試容錯移轉

如果想要節省資源，或者某個復原伺服器不需要執行自動測試容錯移轉，您可以停用自動測試容錯移轉。

若要停用自動測試容錯移轉

1. 在主控台中，移至 **[災難復原] > [伺服器] > [復原伺服器]**，然後選擇復原伺服器。
2. 按一下 **[編輯]**。
3. 在 **[自動測試容錯移轉]** 區段的 **[排程]** 欄位中，選擇 **[永不]**。
4. 按一下 **[儲存]**。

實際執行容錯移轉

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

復原伺服器建立時，它會維持在 **【待命】** 狀態。在開始容錯移轉之前，對應的虛擬機器不存在。開始容錯移轉程序之前，您必須為原始電腦建立至少一個磁碟映像備份 (含可開機磁碟區)。

開始容錯移轉程序時，您要選擇原始電腦的復原點 (備份)，您將會從該復原點使用預先定義的參數建立虛擬機器。容錯移轉作業會使用「從備份執行 VM」功能。復原伺服器的過渡狀態為 **【最終化】**。此程序意味著將伺服器的虛擬磁碟從備份儲存空間 (「冷」儲存) 傳送到災難復原儲存空間 (「熱」儲存)。

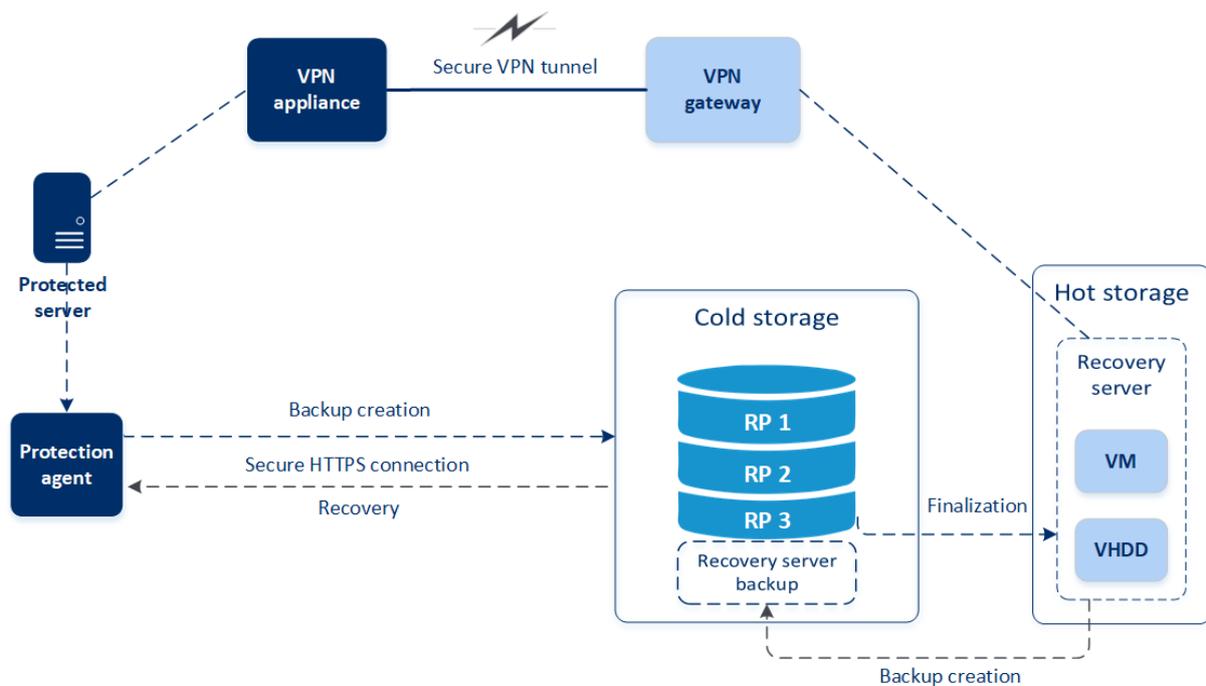
注意事項

在 **【最終化】** 期間，雖然效能低於正常狀態，但仍然可以存取和操作。您可以按一下 **【主控台就緒】** 連結來開啟伺服器主控台。此連結可在 **【Disaster Recovery】 > 【伺服器】** 畫面上的 **【VM 狀態】** 欄中，以及伺服器的 **【詳細資料】** 檢視中取得。

當 **【最終化】** 完成後，伺服器效能就會達到其正常值。伺服器狀態會變更為 **【容錯移轉】**。工作負載現在會從原始電腦切換到雲端站台中的復原伺服器。

如果復原伺服器內部有保護代理程式，則會停止代理程式服務，以避免干擾 (例如開始備份或將過期的狀態報告至備份元件)。

在以下的圖表中，您可以同時看到容錯移轉和容錯回復程序。



執行容錯移轉

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

容錯移轉是從您本機將工作負載移到雲端的程序，也是工作負載保留在雲端的狀態。

當您開始容錯移轉時，復原伺服器會在實際執行網路中啟動。為避免干擾和不必要的問題，請確保原始工作負載不在線上且無法透過 VPN 存取。

為了避免對同一個雲端存檔的備份干擾，請手動撤銷目前處於**容錯移轉**狀態之工作負載的保護計劃。如需有關撤銷計劃的詳細資訊，請參閱[撤銷保護計劃](#)。

重要事項

您必須事先[建立復原伺服器](#)以保護您的裝置免受災難影響。

您只能從建立裝置的復原伺服器後所建立的復原點(備份)執行容錯移轉。

容錯移轉至復原伺服器之前，必須至少建立一個復原點。支援的復原點數量上限為 100。

您可以依照下方的程序或觀看[影片教學](#)。

執行容錯移轉

1. 確認原始電腦在網路上無法使用。
2. 在 Cyber Protect 主控台中，移至 **[災難復原] > [伺服器] > [復原伺服器]**，然後選擇復原伺服器。
3. 按一下 **[容錯移轉]**。
4. 選擇 **[實際執行容錯移轉]**。
5. 選擇復原點(備份)，然後按一下 **[開始]**。
6. [如果您選擇的備份是使用加密作為機器屬性加密的]
 - a. 輸入備份集的加密密碼。

注意事項

此密碼僅會暫時儲存，而且將僅用於目前的容錯移轉作業。在容錯移轉作業完成且伺服器回復到 **[待命]** 狀態時，此密碼會自動從認證存放區中刪除。

- b. [選用] 若要儲存備份集的密碼並將其用於後續的容錯移轉作業，請選擇 **[將密碼儲存在安全的認證存放區中...]** 核取方塊，然後在 **[認證名稱]** 欄位中，輸入認證的名稱。

重要事項

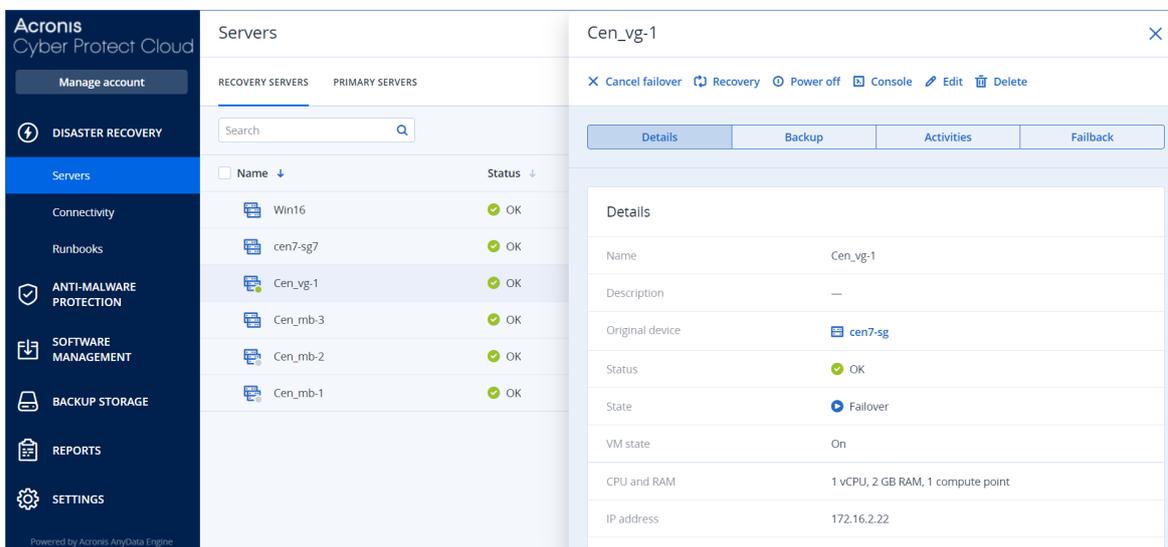
密碼將儲存在安全的認證存放區中，而且將在後續的容錯移轉作業中自動套用。但是，儲存密碼可能會與法規遵循義務相衝突。

- c. 按一下 **[完成]**。

當復原伺服器啟動時，其狀態會變更為 **[最終化]**，一段時間後則會變更為 **[容錯移轉]**。

重要事項

瞭解伺服器 [最終化] 和 [容錯移轉] 這兩種狀態下都可以使用至關重要。在 [最終化] 狀態期間，您可以按一下 [主控台就緒] 連結來存取伺服器主控台。此連結可在 [Disaster Recovery] > [伺服器] 畫面上的 [VM 狀態] 欄中，以及伺服器的 [詳細資料] 檢視中取得。



7. 透過檢視其主控台，確認復原伺服器已啟動。按一下 [Disaster Recovery] > [伺服器]、選取復原伺服器，然後按一下 [主控台]。
8. 確認可使用您在建立復原伺服器時指定的實際執行 IP 位址存取復原伺服器。

復原伺服器最終化之後，會自動建立新的保護計劃並套用至復原伺服器。此保護計劃是以用來建立復原伺服器的保護計劃為基礎，其有特定限制。在此計劃中，您可以變更的只有排程和保留規則。如需詳細資訊，請參閱 < 備份雲端伺服器 >。

如何使用本機 DNS 執行伺服器的容錯移轉

如果您的本機站台使用 DNS 伺服器解析電腦名稱，則在容錯移轉後，復原伺服器可能無法進行通訊。這是因為雲端的 DNS 伺服器與本機站台的 DNS 伺服器不同。預設情況下，新建立的雲端伺服器會使用雲端站台的 DNS 伺服器，但您可以設定自訂 DNS 設定。如需詳細資訊，請參閱 "設定自訂 DNS 伺服器" (第 42 頁)。

如何執行 DHCP 伺服器的容錯移轉

您本機基礎架構的 DHCP 伺服器可能位於 Windows 或 Linux 主機。當這種主機容錯移轉至雲端站台時，會發生 DHCP 伺服器重複問題，因為雲端中的 VPN 閘道也會執行 DHCP 角色。若要解決這個問題，請執行下列其中一項操作：

- 如果只有 DHCP 主機容錯移轉至雲端，雖然其餘的雲端伺服器仍在本機站台，但您還是必須登入雲端的 DHCP 主機，並關閉其上的 DHCP 伺服器。因此，將不會發生衝突，而且只有 VPN 閘道將會當做 DHCP 伺服器。

- 如果您的雲端伺服器已經從 DHCP 主機取得 IP 位址，則您必須登入雲端的 DHCP 主機，並關閉其上的 DHCP 伺服器。您也必須登入雲端伺服器並更新 DHCP 租賃，以指派從正確的 DHCP 伺服器 (在 VPN 閘道上託管) 配置的新 IP 位址。

注意事項

當您的雲端 DHCP 伺服器設定為 **[自訂 DHCP]** 選項時，這些指示無效，而且某些復原或主要伺服器會從此 DHCP 伺服器獲得其 IP 位址。

停止容錯移轉

您可以在處理程序的每個階段，隨時停止實際執行容錯移轉。

注意事項

停止容錯移轉會還原從容錯移轉開始執行時所做的所有變更，但復原伺服器備份除外。

若要停止實際執行容錯移轉

1. 在 Cyber Protect 主控台中，前往 **[災難復原] > [伺服器] > [復原伺服器]**。
2. 選擇處於 **[容錯移轉]** 狀態的復原伺服器。
3. 按一下復原伺服器。
4. 按一下 **[停止容錯移轉]**。
5. 在出現的確認視窗中，選擇核取方塊，然後按一下 **[停止容錯移轉]**。
容錯移轉隨即停止。復原伺服器會回復至 **[待機]** 狀態。

容錯回復

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

容錯回復是從雲端將工作負載移回您本機站台上的實體或虛擬機器的程序。您可以在**容錯移轉**狀態下對復原伺服器執行容錯回復，並在本機站台上繼續使用伺服器。

您可以對本機站台上的虛擬或實體目標機器執行自動容錯移轉。在容錯回復期間，您可以在雲端的虛擬機器繼續執行時，將備份資料傳輸到本機站台。此技術有助於達到非常短的停機期間，且此停機期間可以估算並顯示在 Cyber Protect 主控台中。您可以檢視此停機期間，並使用這項資訊規劃您的活動，必要時，對您的用戶端提出停機期間即將到來的警告。如果您透過可開機媒體執行代理程式型容錯回復，停機時間甚至更短，因為只有差異變更將傳輸到本機站台。

若要容錯回復至目標實體機器，您可以透過可開機媒體使用代理程式型容錯回復。如需詳細資訊，請參閱 "執行代理程式型容錯回復 (透過可開機媒體)" (第 70 頁)。

若要容錯回復至目標虛擬機器，您可以透過可開機媒體使用代理程式型容錯回復，或透過 Hypervisor 代理程式使用無代理程式容錯回復。如需詳細資訊，請參閱 "執行代理程式型容錯回復 (透過可開機媒體)" (第 70 頁) 和 "執行無代理程式容錯回復 (透過 Hypervisor 代理程式)" (第 74 頁)。

在您無法使用自動容錯回復程序的特定情況下，可以執行手動容錯回復。如需詳細資訊，請參閱 "手動容錯回復" (第 76 頁)。

注意事項

Runbook 作業僅支援手動模式下的容錯回復。也就是說，如果您透過執行包含**容錯回復伺服器**步驟的 Runbook 來開始容錯回復程序，此程序將需要手動互動：您必須手動復原機器，並從 **[Disaster Recovery] > [伺服器]** 索引標籤確認或取消容錯回復程序。

代理程式型容錯回復 (透過可開機媒體)

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

代理程式型容錯回復 (透過可開機媒體) 程序已經過最佳化，可容錯回復至原始實體或虛擬機器。在此程序中，僅將增量變更傳輸至本機站台。

透過可開機媒體至目標實體或虛擬機器的代理程式型容錯回復 (透過可開機媒體) 程序包括下列階段：

1. **規劃**。在此階段期間，您要在本機站台還原 IT 基礎架構 (例如，主機和網路設定)、設定容錯回復參數，以及規劃開始資料傳輸的時間。
2. **資料傳輸**。在此階段期間，資料會在雲端的虛擬機器繼續執行時，從雲端站台傳輸到本機站台。您可以在資料傳輸階段期間，隨時開始下一個階段 (轉換)，但是您應該考慮下列關係。
您維持在資料傳輸階段的時間越長，

- 雲端的虛擬機器繼續執行的時間越長，
- 傳輸到本機站台的資料越多，
- 您將支付的成本越高 (您花費的計算點越多)。
- 您在轉換階段經歷的停機期間越短。

如果您要將停機時間減至最少，請在超過 90% 的資料傳輸到本機站台之後，就開始轉換階段。如果您可以承受經歷較長的停機期間，而且不想要花費更多的計算點執行雲端的虛擬機器，您可以更早開始轉換階段。

注意事項

資料傳輸程序使用 Flashback 技術。此技術會比較目標電腦上存在的資料與虛擬機器在雲端的資料。如果目標電腦上已存在部分資料，則不會再次傳輸這些資料。此技術會加快資料傳輸階段的速度。

因此，建議您將伺服器還原到您本機站台上的原始電腦。

3. **轉換。**此階段期間會關閉雲端的虛擬機器，而且包括上次備份增量在內的剩餘資料會傳輸到本機站台。如果在復原伺服器上未套用任何備份計劃，將會在轉換階段期間自動執行備份，這會減慢該程序。
4. **驗證。**在此階段期間，本機站台上的實體機器已準備就緒，您可以使用 Linux 可開機媒體將其重新開機。您可以確認虛擬機器正確運作，而且：
 - 如果一切如預期般運作，請確認容錯回復。容錯回復確認之後，雲端的虛擬機器就會遭到刪除，且復原伺服器會回復到**待命**狀態。這是容錯回復程序的結尾。
 - 如果發生問題，您可以取消容錯移轉，並返回規劃階段。

注意事項

可開機媒體重新開機後，您將無法再次使用它。如果在驗證階段發生問題，則您必須註冊新的可開機媒體，並再次開始容錯回復程序。

但是在使用 Flashback 技術時，將不會再次傳輸本機站台上已經存在的資料，因此容錯回復程序將會快很多。

執行代理程式型容錯回復 (透過可開機媒體)

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以對本機站台上的目標實體或虛擬機器，透過可開機媒體執行代理程式型容錯回復。

注意事項

資料傳輸程序使用 Flashback 技術。此技術會比較目標電腦上存在的資料與虛擬機器在雲端的資料。如果目標電腦上已存在部分資料，則不會再次傳輸這些資料。此技術會加快資料傳輸階段的速度。

因此，建議您將伺服器還原到您本機站台上的原始電腦。

必要條件

- 您將用於執行容錯回復的代理程式已連線，且目前未用於其他容錯回復作業。
- 您的網際網路連線穩定。
- 已註冊的可開機媒體可供使用。如需詳細資訊，請參閱 **Cyber Protection 使用指南** 中的「建立可開機媒體以復原作業系統」。
- 目標機器是本機站台上的原始機器，或者與原始機器擁有相同的韌體。
- 雲端至少有一個虛擬機器的完整備份。

對實體機器執行容錯回復

1. 在 Cyber Protect 主控台中，移至 **[災難復原] > [伺服器]**。
2. 選擇處於 **[容錯移轉]** 狀態的復原伺服器。
3. 按一下 **[容錯回復]** 索引標籤。
4. 在 **[容錯回復類型]** 欄位中，選擇 **[代理程式型 (透過可開機媒體)]**。
5. 在 **[目標可開機媒體]** 欄位中，按一下 **[指定]**，選擇可開機媒體，然後按一下 **[完成]**。

注意事項

建議您使用已設定的現成可開機媒體。如需詳細資訊，請參閱 **Cyber Protection 使用指南** 中的「建立可開機媒體以復原作業系統」。

6. [選用] 若要變更預設磁碟對應，請在 **[磁碟對應]** 欄位中，按一下 **[指定]**，將備份的磁碟對應到目標電腦的磁碟，然後按一下 **[完成]**。
7. 按一下 **[開始資料傳輸]**，然後在確認視窗中，按一下 **[開始]**。

注意事項

如果雲端中沒有虛擬機器的備份，系統將在資料傳輸階段之前自動執行備份。

資料傳輸階段隨即開始。主控台會顯示以下資訊：

欄位	描述
進度	此參數會顯示已經傳輸到本機站台的資料量以及必須傳輸的總資料量。 總資料量包括資料傳輸階段開始前最後備份的資料，以及新產生資料的備份 (備份增量)，因為虛擬機器在資料傳輸階段期間會繼續執行。因此， [進度] 值會隨著時間而增加。 由於系統在資料傳輸期間使用 Flashback 技術，且不傳輸目標電腦上已存在的資料，因此進度可能比主控台最初計算的速度更快。
停機時間預估	此參數會顯示如果您現在開始轉換階段，將無法使用雲端的虛擬機器的時間。這個值是根據 [進度] 參數的值計算得來，而且會隨著時間而減少。 由於系統在資料傳輸期間使用 Flashback 技術，且不傳輸目標電腦上已存在的資料，因此停機時間可能比主控台中最初顯示的值短很多。

8. 按一下 **[轉換]**，然後在確認視窗中，再按一下 **[轉換]**。

轉換階段隨即開始。主控台會顯示以下資訊：

欄位	描述
進度	此參數會顯示在本機站台上還原電腦的進度。
估計的完成時間	此參數會顯示將完成轉換階段, 而且您將能夠啟動本機站台上電腦的大約時間。

注意事項

如果雲端虛擬機器上未套用任何備份計劃, 將會在轉換階段期間自動執行備份, 從而導致停機時間較長。

9. **轉換**階段完成後, 請使用可開機媒體重新開機, 然後驗證本機站台上的實體機器是否如預期般運作。
如需詳細資訊, 請參閱《Cyber Protection 使用指南》中的「使用可開機媒體復原磁碟」。
10. 按一下 **[確認容錯回復]**, 然後在確認視窗中, 按一下 **[確認]** 以結束程序。
雲端的虛擬機器會遭到刪除, 且復原伺服器會回復到**待命**狀態。

注意事項

在復原的伺服器上套用保護計劃不是容錯回復程序的一部分。在容錯回復程序完成之後, 在復原的伺服器上套用保護計劃以確保其再次受到保護。您可以套用在原始伺服器上套用的相同保護計劃, 也可以套用已啟用 **[Disaster Recovery]** 模組的新保護計劃。

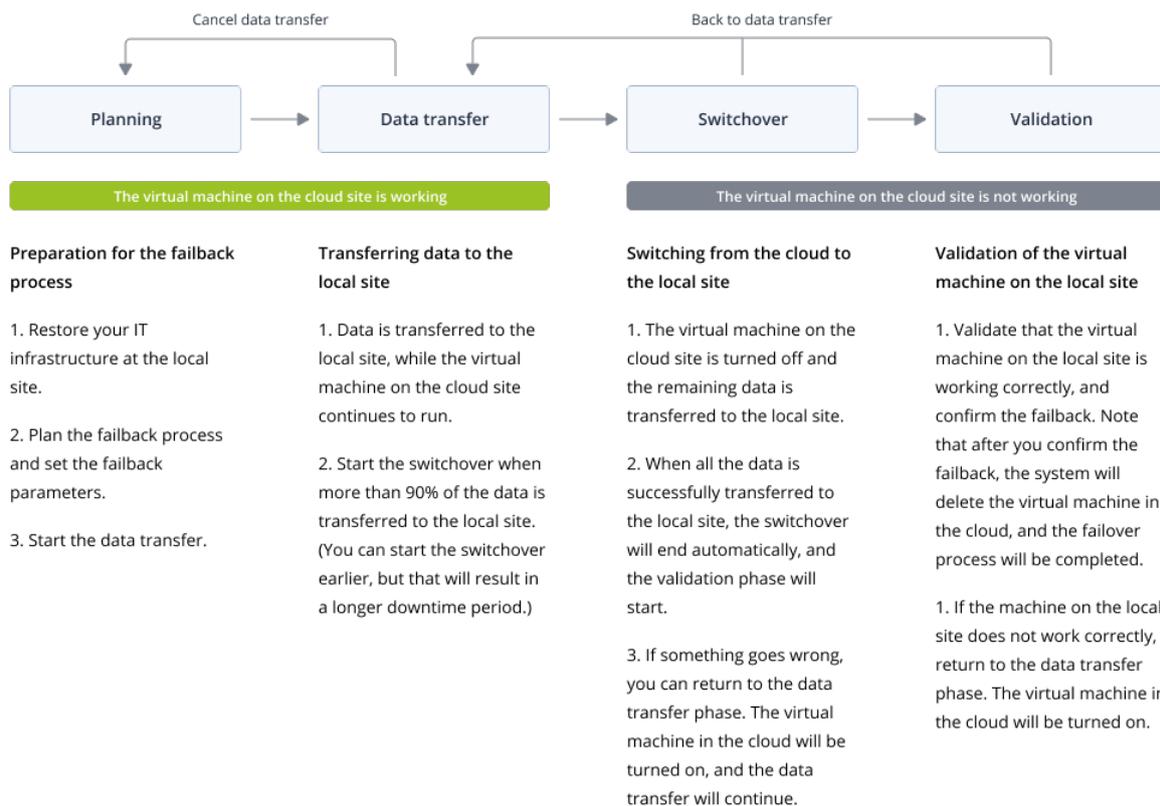
無代理程式容錯回復 (透過 Hypervisor 代理程式)

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

無代理程式容錯回復 (透過 Hypervisor 代理程式) 程序已經過最佳化, 可容錯回復至新的虛擬機器。若要容錯回復至原始虛擬機器, 請依照代理程式型容錯回復 (透過可開機媒體) 的程序執行。

無代理程式容錯回復 (透過 Hypervisor 代理程式) 包括四個階段。



1. **規劃**。在此階段期間，您要在本機站台還原 IT 基礎架構 (例如，主機和網路設定)、設定容錯回復參數，以及規劃開始資料傳輸的時間。

注意事項

為將容錯回復程序的全部時間減至最少，建議您在設定本機伺服器後立即開始資料傳輸階段，然後在資料傳輸階段期間，繼續設定網路以及其餘的本機基礎架構。

2. **資料傳輸**。在此階段期間，資料會在雲端的虛擬機器繼續執行時，從雲端站台傳輸到本機站台。您可以在資料傳輸階段期間，隨時開始下一個階段 (轉換)，但是您應該考慮下列關係。

您維持在資料傳輸階段的時間越長，

- 雲端的虛擬機器繼續執行的時間越長，
- 傳輸到本機站台的資料越多，
- 您將支付的成本越高 (您花費的計算點越多)。
- 您在轉換階段經歷的停機期間越短。

如果您要將停機時間減至最少，請在超過 90% 的資料傳輸到本機站台之後，就開始轉換階段。

如果您可以承受經歷較長的停機期間，而且不想要花費更多的計算點執行雲端的虛擬機器，您可以更早開始轉換階段。

如果您在資料傳輸階段期間取消容錯回復程序，已傳輸的資料將不會從本機站台刪除。為避免可能的問題，請先手動刪除已傳輸的資料，然後再開始新的容錯回復程序。下列資料傳輸程序將從頭開始。

3. **轉換**。此階段期間會關閉雲端的虛擬機器，而且包括上次備份增量在內的剩餘資料會傳輸到本機站台。如果在復原伺服器上未套用任何備份計劃，將會在轉換階段期間自動執行備份，這會減慢該程序。

您可以在 Cyber Protect 主控台中，檢視完成此階段的估計時間 (停機期間)。當所有資料都傳輸到本機站台 (不會失去任何資料，而且本機站台上的虛擬機器為雲端虛擬機器完全相符的複本) 時，轉換階段便完成。系統會復原本機站台上的虛擬機器，而且會自動開始驗證階段。

4. **驗證**。在此階段期間，本機站台上的虛擬機器已準備就緒，並已自動啟動。您可以確認虛擬機器正確運作，而且：
 - 如果一切如預期般運作，請確認容錯回復。容錯回復確認之後，雲端的虛擬機器就會遭到刪除，且復原伺服器會回復到**待命**狀態。這是容錯回復程序的結尾。
 - 如果發生問題，您可以取消轉換，並返回資料傳輸階段。

執行無代理程式容錯回復 (透過 Hypervisor 代理程式)

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以透過 Hypervisor 代理程式，在本機站台對目標虛擬機器執行無代理程式容錯回復。

必要條件

- 您將用於執行容錯回復的代理程式已連線，且目前未用於其他容錯回復作業。
- 您的網際網路連線穩定。
- 雲端至少有一個虛擬機器的完整備份。

若要透過 Hypervisor 代理程式對虛擬機器執行無代理程式容錯回復

1. 在 Cyber Protect 主控台中，移至 **[災難復原] > [伺服器]**。
2. 選擇處於 **[容錯移轉]** 狀態的復原伺服器。
3. 按一下 **[容錯回復]** 索引標籤。
4. 在 **[容錯回復參數]** 區段的 **[容錯回復類型]** 欄位中，選擇 **[無代理程式 (透過 Hypervisor 代理程式)]**，然後設定其他參數。

請注意，部分 **[容錯回復參數]** 預設會自動填入建議的值，但是您可以加以變更。

下表提供有關 **[容錯回復參數]** 的詳細資訊。

參數	描述
備份大小	在容錯回復程序期間傳輸到本機站台的資料量。 在您開始容錯回復到目標虛擬機器的程序之後， [備份大小] 將會在 [資料傳輸] 階段增加，因為雲端的虛擬機器將繼續執行並產生新資料。 若要計算容錯回復至目標虛擬機器程序期間的預估停機期間，請使用 10% 的 [備份大小] 值 (因為我們建議您在 90% 的資料傳輸到本機站台之後再開始 [轉換] 階段)，並將其除以您網際網路速度的值。

參數	描述
	<p>注意事項</p> <p>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。</p>
目標電腦位置	<p>容錯回復位置：VMware ESXi 主機或 Microsoft Hyper-V 主機。</p> <p>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。</p>
代理程式	<p>將執行容錯回復作業的代理程式。</p> <p>您可以同時使用一個代理程式執行一個容錯回復作業。</p> <p>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。</p> <p>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。</p>
目標電腦設定	<p>虛擬機器設定：</p> <ul style="list-style-type: none"> • 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。 <p>當您準備好進行變更時，按一下 [完成]。</p>
路徑	<p>(適用於 Microsoft Hyper-V 主機) 將存放您電腦所在主機上的資料夾。</p> <p>請確認電腦的主機上有足夠的可用記憶體空間。</p>
資料存放區	<p>(適用於 VMware ESXi 主機) 將存放您電腦所在主機上的資料存放區。</p> <p>請確認電腦的主機上有足夠的可用記憶體空間。</p>
佈建模式	<p>虛擬磁碟配置的方法。</p> <p>若是 Microsoft Hyper-V 主機：</p> <ul style="list-style-type: none"> • 動態擴充 (預設值)。 • 固定大小。 <p>若是 Microsoft Hyper-V 主機：</p> <ul style="list-style-type: none"> • 精簡 (預設值)。 • 密集。
目標電腦名稱	<p>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。</p> <p>目標電腦名稱在所選目標電腦位置上必須是唯一的。</p>

5. 按一下 **[開始資料傳輸]**，然後在確認視窗中，按一下 **[開始]**。

注意事項

如果雲端中沒有虛擬機器的備份，系統將在資料傳輸階段之前自動執行備份。

資料傳輸階段隨即開始。主控台會顯示以下資訊：

欄位	描述
進度	此參數會顯示已經傳輸到本機站台的資料量以及必須傳輸的總資料量。 總資料量包括資料傳輸階段開始前最後備份的資料，以及新產生資料的備份 (備份增量)，因為虛擬機器在資料傳輸階段期間會繼續執行。因此， [進度] 參數的這兩個值會隨著時間而增加。
停機時間 預估	此參數會顯示如果您現在開始轉換階段，將無法使用雲端的虛擬機器的時間。這個值是根據 [進度] 參數的值計算得來，而且會隨著時間而減少。

- 按一下 **[轉換]**，然後在確認視窗中，再按一下 **[轉換]**。

轉換階段隨即開始。主控台會顯示以下資訊：

欄位	描述
進度	此參數會顯示在本機站台上還原電腦的進度。
估計的完成時間	此參數會顯示將完成轉換階段，而且您將能夠啟動本機站台上電腦的大約時間。

注意事項

如果雲端虛擬機器上未套用任何備份計劃，將會在轉換階段期間自動執行備份，從而導致停機時間較長。

- 轉換階段完成且本機站台上的虛擬機器自動啟動後，驗證是否如預期般運作。
- 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 **[Disaster Recovery]** 模組的新保護計劃。

手動容錯回復

注意事項

建議您僅在支援團隊建議時，才在手動模式下使用容錯回復程序。

您也可以在手動模式下開始容錯回復程序。在此情況下，資料將不會自動從雲端的備份傳輸到本機站台。此程序必須在雲端的虛擬機器關閉之後手動完成。這會使手動模式下的容錯回復程序慢很多，因此您應該預期停機時間會更長。

手動模式下的容錯回復程序包括下列階段：

1. **規劃**。在此階段期間，您要在本機站台還原 IT 基礎架構 (例如，主機和網路設定)、設定容錯回復參數，以及規劃開始資料傳輸的時間。
2. **轉換**。此階段期間會關閉雲端的虛擬機器，並備份新產生的資料。如果在復原伺服器上未套用任何備份計劃，將會在轉換階段期間自動執行備份，這會減慢該程序。備份完成後，您要手動將電腦復原到本機站台。您可以使用可開機媒體復原磁碟，或從雲端備份儲存空間復原整部電腦。
3. **驗證**。在此階段期間，您要確認本機站台的實體或虛擬機器正確運作並確認容錯回復。確認之後，雲端站台的虛擬機器會遭到刪除，且復原伺服器會回復到**待命**狀態。

執行手動容錯回復

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

您可以對本機站台上的目標實體或虛擬機器執行手動容錯回復。

若要執行手動容錯回復

1. 在 Cyber Protect 主控台中，移至 **[災難復原] > [伺服器]**。
2. 選擇處於**[容錯移轉]**狀態的復原伺服器。
3. 按一下 **[容錯回復]** 索引標籤。
4. 在 **[目標]** 欄位中，選擇 **[實體機器]**。
5. 按一下齒輪圖示，然後啟用 **[使用手動模式]** 開關。
6. [選用] 將 **[備份大小]** 值除以您網際網路速度的值，以計算容錯回復程序期間的預估停機期間。

注意事項

當您同時執行數個容錯回復程序時，網際網路速度的值將會減少。

7. 按一下 **[轉換]**，然後在確認視窗中，再按一下 **[轉換]**。
雲端站台上的虛擬機器隨即關閉。

注意事項

如果雲端虛擬機器上未套用任何備份計劃，將會在轉換階段期間自動執行備份，從而導致停機時間較長。

8. 將伺服器從雲端備份復原到本機站台上的實體或虛擬機器。如需詳細資訊，請參閱 **Cyber Protection 使用指南** 中的「復原機器」。
9. 確認復原已完成且復原的電腦正常運作，然後按一下 **[電腦已還原]**。
10. 如果一切如預期般運作，按一下 **[確認容錯回復]**，然後在確認視窗中，再按一下 **[確認]**。
復原伺服器和復原點會變成準備就緒供下次容錯移轉之用。若要建立新的復原點，請將保護計劃套用到新的本機伺服器。

注意事項

在復原的伺服器上套用保護計劃不是容錯回復程序的一部分。在容錯回復程序完成之後，在復原的伺服器上套用保護計劃以確保其再次受到保護。您可以套用在原始伺服器上套用的相同保護計劃，也可以套用已啟用 **[Disaster Recovery]** 模組的新保護計劃。

編排 (Runbook)

注意事項

部分功能可能需要額外的授權，端視適用的授權模型而定。

Runbook 是一組指令，用來描述如何在雲端啟動實際執行環境。您可以在 Cyber Protect 主控台中建立 Runbook。

透過 Runbook，您可以：

- 自動容錯移轉一或多部伺服器。
- Ping 伺服器 IP 位址並檢查您指定之連接埠的連線，以便自動檢查容錯移轉結果。
- 針對執行分散式應用程式的伺服器，設定操作順序。
- 在工作流程中包含手動作業。
- 在測試模式下執行 Runbook，以確認災難復原解決方案的完整性。

若要存取 **[Runbook]** 畫面，請選擇 **[災難復原] > [Runbook]**。

建立 Runbook

Runbook 包含連續執行的步驟。步驟則包含同時開始的動作。

若要建立 Runbook，請依照下列程序或影片教學課程中的指示進行。

若要建立 Runbook

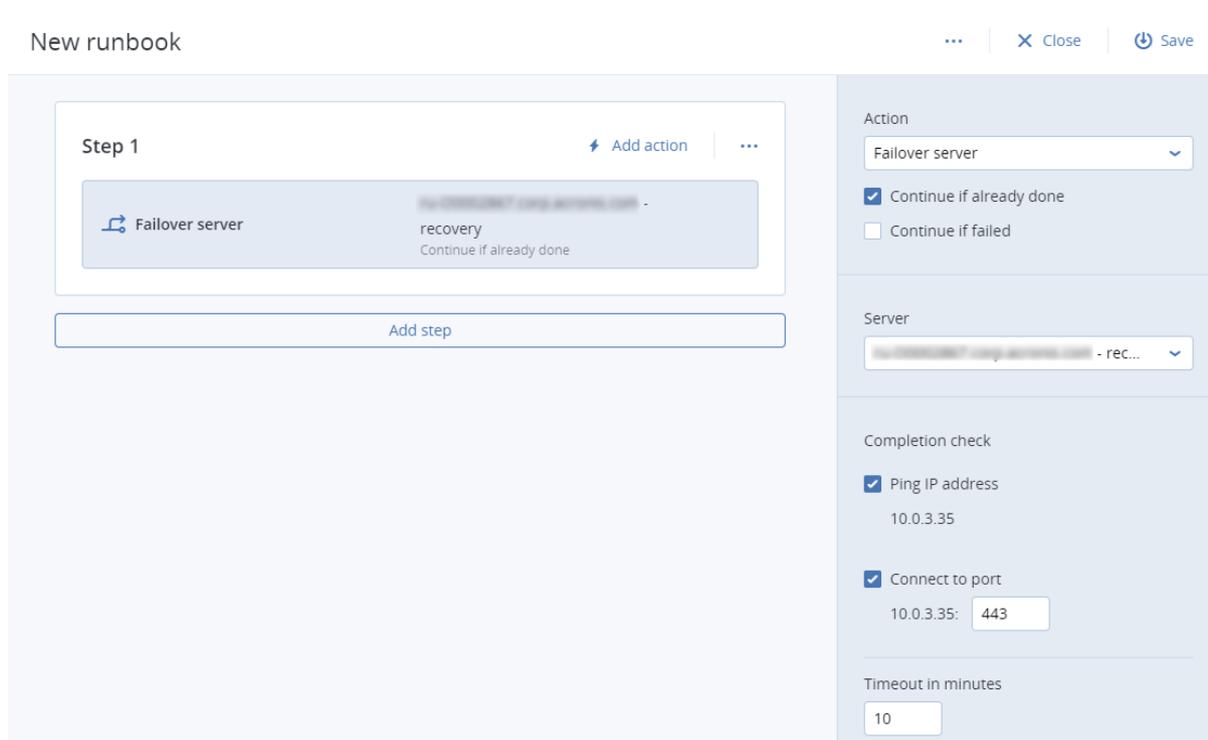
1. 在 Cyber Protection 主控台中，移至 **[災難復原] > [Runbook]**。
2. 按一下 **[建立 Runbook]**。
3. 按一下 **[新增步驟]**。
4. 按一下 **[新增動作]**，然後選擇您想要新增到步驟中的動作。

動作	描述
容錯移轉伺服器	<p>執行雲端伺服器的容錯移轉。若要定義此動作，您必須選擇一部雲端伺服器，並設定可用於此動作的 Rrunbook 參數。如需有關這些參數的詳細資訊，請參閱 "Runbook 參數" (第 81 頁)。</p> <hr/> <p>注意事項 如果您選擇的伺服器備份是使用加密作為機器屬性加密的，則 [容錯移轉伺服器] 動作將會遭到暫停，而且將自動變更為 [需要互動]。若要繼續執行 Runbook，您必須提供加密備份的密碼。</p>
容錯回復伺服器	<p>執行雲端伺服器的容錯回復。若要定義此動作，您必須選擇一部雲端伺服器，並設定可用於此動作的 Rrunbook 參數。如需有關這些設定的詳細資訊，請參閱 "Runbook 參數" (第 81 頁)。</p>

動作	描述
	<p>注意事項 Runbook 作業僅支援手動模式下的容錯回復。也就是說, 如果您透過執行包含容錯回復伺服器步驟的 Runbook 來開始容錯回復程序, 此程序將需要手動互動: 您必須手動復原機器, 並從 [Disaster Recovery] > [伺服器] 索引標籤確認或取消容錯回復程序。</p>
<p>啟動伺服器</p>	<p>啟動雲端伺服器。若要定義此動作, 您必須選擇一部雲端伺服器, 並設定可用於此動作的 Rrunbook 參數。如需有關這些設定的詳細資訊, 請參閱 "Runbook 參數" (第 81 頁)。</p> <hr/> <p>注意事項 [啟動伺服器] 動作不適用於 Runbook 中的測試容錯移轉作業。如果您嘗試執行此類動作, 將會出現以下的錯誤訊息: 失敗: 此動作不適用於目前的伺服器狀態。</p>
<p>停止伺服器</p>	<p>停止雲端伺服器。若要定義此動作, 您必須選擇一部雲端伺服器, 並設定可用於此動作的 Rrunbook 參數。如需有關這些設定的詳細資訊, 請參閱 "Runbook 參數" (第 81 頁)。</p> <hr/> <p>注意事項 [停止伺服器] 動作不適用於 Runbook 中的測試容錯移轉作業。如果您嘗試執行此類動作, 將會出現以下的錯誤訊息: 失敗: 此動作不適用於目前的伺服器狀態。</p>
<p>手動作業</p>	<p>手動作業需要使用者的互動。若要定義此動作, 您必須輸入描述。 當 Runbook 順序達到手動作業時, 該 Runbook 將會遭到暫停, 而且在使用者執行所需的手動作業 (例如, 按一下確認按鈕) 之前不會繼續執行。</p>
<p>執行 Runbook</p>	<p>執行另一個 Runbook。若要定義此動作, 您必須選擇一個 Runbook。 一個 Runbook 僅能包含一個指定 Runbook 的執行。例如, 如果您新增「執行 Runbook A」動作, 您可以新增「執行 Runbook B」動作, 但無法新增另一個「執行 Runbook A」動作。</p>

5. 為動作定義 Runbook 參數。如需有關這些參數的詳細資訊, 請參閱 "Runbook 參數" (第 81 頁)。
6. [選用] 若要新增步驟的描述:
 - a. 按一下省略符號圖示, 然後按一下 **[描述]**。
 - b. 輸入步驟的描述。
 - c. 按一下**[完成]**。
7. 重複步驟 3-6, 直到您建立所需的步驟和動作順序為止。
8. [選用] 若要變更 Runbook 的預設名稱:
 - a. 按一下省略符號圖示。
 - b. 輸入 Runbook 的名稱。
 - c. 輸入 Runbook 的描述。
 - d. 按一下**[完成]**。

9. 按一下 [儲存]。
10. 按一下 [關閉]。



Runbook 參數

Runbook 參數是您必須設定，才能定義 Runbook 動作的特定設定。Runbook 參數有兩種類型：動作參數和完成檢查參數。

動作參數會根據動作的初始狀態或結果，定義 Runbook 行為。

完成檢查參數可確保伺服器可供使用，並提供所需的服務。如果完成檢查失敗，則會將該動作視為失敗。

下表描述每個動作可設定的 Runbook 參數。

Runbook 參數	類別	可用於動作	描述
完成時繼續	動作參數	<ul style="list-style-type: none"> • 容錯移轉伺服器 • 啟動伺服器 • 停止伺服器 • 容錯回復伺服器 	<p>此參數會定義所需動作已經完成時的 Runbook 行為 (例如，已經執行容錯移轉或伺服器已經在執行)。啟用時，Runbook 會發出警告並繼續。停用時，動作和 Runbook 都將失敗。</p> <p>根據預設，此參數為啟用狀態。</p>
失敗時繼續	動作參數	<ul style="list-style-type: none"> • 容錯移轉伺服器 • 啟動伺服器 • 停止伺服器 	<p>此參數會定義所需動作失敗時的 Runbook 行為。啟用時，Runbook 會發出警告並繼續。停用時，動作和 Runbook 都將失敗。</p> <p>根據預設，此參數為停用狀態。</p>

Runbook 參數	類別	可用於動作	描述
		<ul style="list-style-type: none"> 容錯回復伺服器 	
Ping IP 位址	完成檢查	<ul style="list-style-type: none"> 啟動伺服器 	此軟體將會 Ping 雲端伺服器的實際運作 IP 位址，直到伺服器回覆或逾時到期為止 (以先到者為準)。
連線到連接埠 (預設為 443)	完成檢查	<ul style="list-style-type: none"> 容錯移轉伺服器 啟動伺服器 	此軟體將會嘗試使用其實際運作 IP 位址和您指定的連接埠，連線至雲端伺服器，直到建立連線或逾時到期為止 (以先到者為準)。如此一來，您就可以確認接聽指定之連接埠的應用程式是否正在執行。
逾時 (分鐘)	完成檢查	<ul style="list-style-type: none"> 容錯移轉伺服器 啟動伺服器 	預設逾時為 10 分鐘。

Runbook 的相關作業

注意事項

是否能夠使用此功能視您帳戶啟用的服務配額而定。

若要存取作業清單，請將滑鼠暫留在 Runbook 上，然後按一下省略符號圖示。當 Runbook 沒有在執行時，可以使用下列作業：

- 執行
- 編輯
- 複製
- 刪除

執行 Runbook

每次按一下 **[執行]** 時，都會收到執行參數的提示。這些參數適用於 Runbook 中包含的所有容錯移轉和容錯回復作業。在 **[執行 Runbook]** 作業中指定的 Runbook 會從主要 Runbook 繼承這些參數。

- **容錯移轉和容錯回復模式**

選擇您要執行測試容錯移轉 (預設) 還是實際 (實際運作) 容錯移轉。容錯回復模式將對應到選擇的容錯移轉模式。

- **容錯移轉復原點**

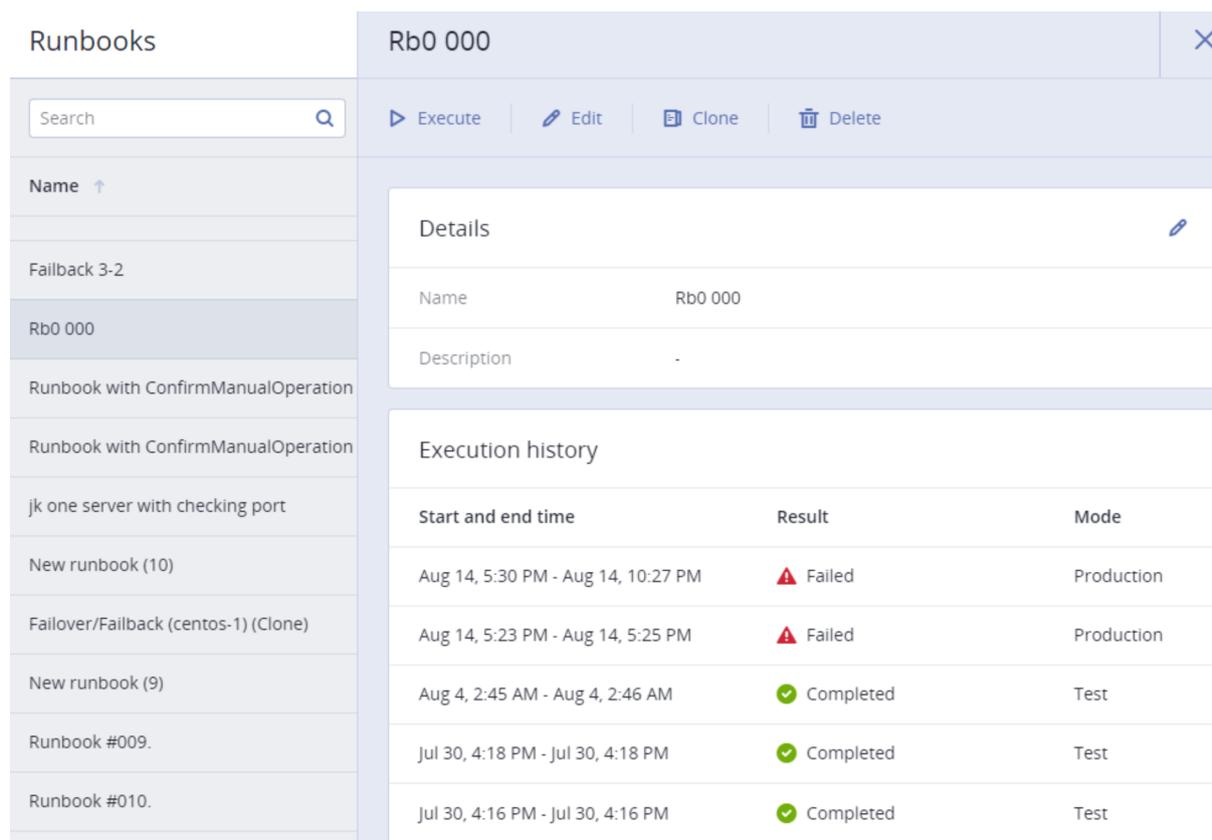
選擇最近的復原點 (預設) 或選取過去的時間點。如果是後者，將會為每部伺服器選取最接近指定之日期和時間前的復原點。

停止 Runbook 執行

在 Runbook 執行期間，您可以選取作業清單中的 **[停止]**。此軟體將會完成所有已經開始的動作，但需要使用者互動的動作除外。

檢視執行歷程記錄

在 **[Runbook]** 索引標籤上選取 Runbook 時，此軟體會顯示 Runbook 詳細資料以及執行歷程記錄。按一下對應到特定執行的行可檢視執行記錄。



The screenshot displays the 'Runbooks' management interface. On the left is a list of runbooks, with 'Rb0 000' selected. The main panel shows the details for 'Rb0 000', including its name and description. Below the details is a table of execution history.

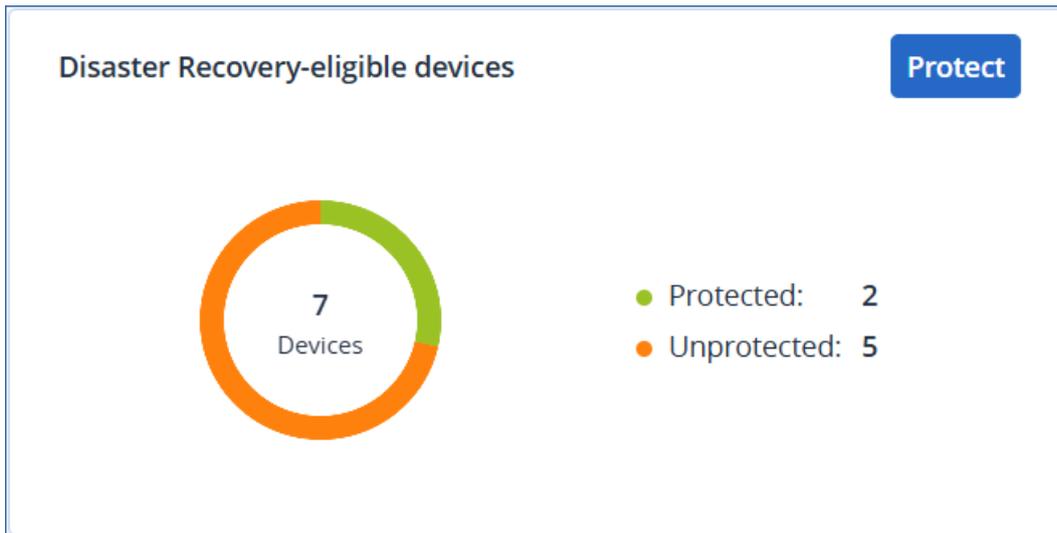
Start and end time	Result	Mode
Aug 14, 5:30 PM - Aug 14, 10:27 PM	Failed	Production
Aug 14, 5:23 PM - Aug 14, 5:25 PM	Failed	Production
Aug 4, 2:45 AM - Aug 4, 2:46 AM	Completed	Test
Jul 30, 4:18 PM - Jul 30, 4:18 PM	Completed	Test
Jul 30, 4:16 PM - Jul 30, 4:16 PM	Completed	Test

Disaster Recovery 儀表板

Disaster Recovery 的 **儀表板** 頁面中包含小工具，可針對您的災難復原網站在其生命週期提供即時概觀以及可採取行動的見解。

Disaster Recovery - 符合資格的裝置

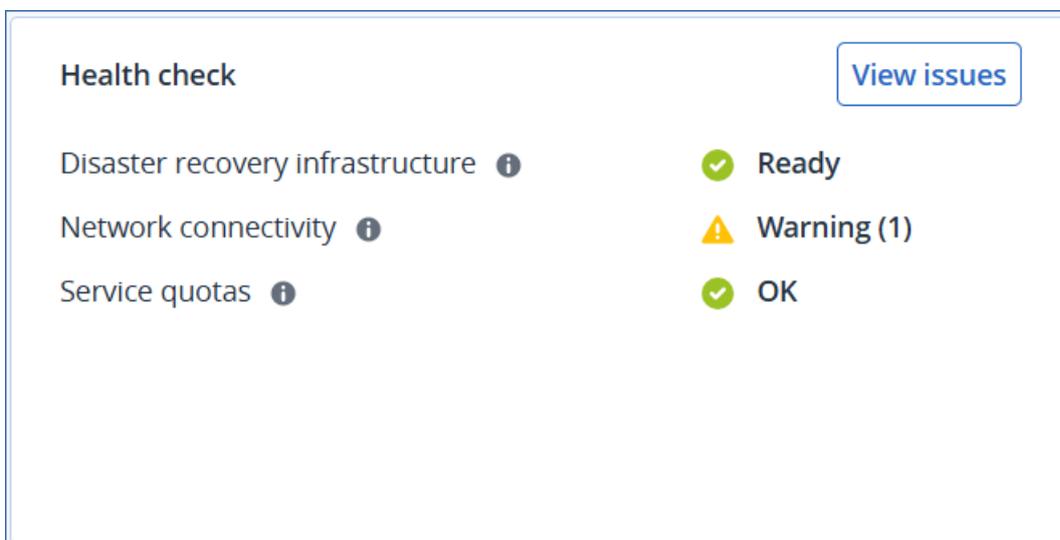
此小工具會顯示受 Disaster Recovery 保護 (具有復原伺服器) 的裝置總數，以及符合受 Disaster Recovery 保護資格的裝置總數。



若要前往 **所有裝置** 頁面，讓您可以在其中為符合資格的裝置設定 Disaster Recovery，請按一下 **保護**。

健全狀況檢查

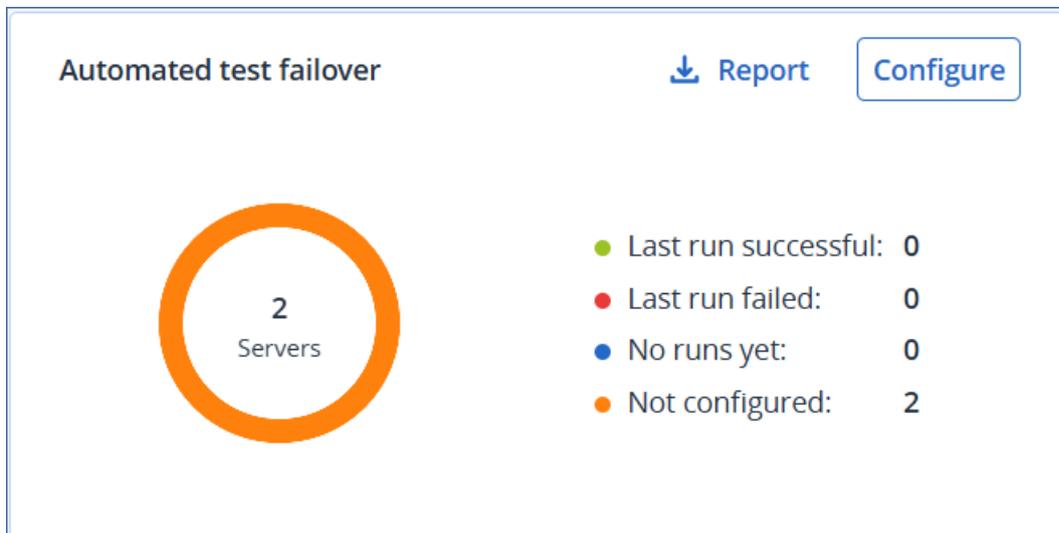
此小工具會顯示 Disaster Recovery 基礎架構健全狀態的相關資訊。您可以檢查網站組態、網路可用性的狀態，以及是否有缺少服務配額。



若要檢視有關偵測到的問題 (警告或錯誤) 的詳細資訊, 請按一下 **[檢視問題]**。

自動測試容錯移轉

此小工具會顯示復原伺服器的自動測試容錯移轉作業的相關資訊。



若要開始為伺服器設定自動測試容錯移轉, 請按一下 **[設定]**。

若要從小工具下載資料, 請按一下 **[報告]**。

移除災難復原網站

您可以移除災難復原網站。此動作將會自動刪除 VPN 閘道、VPN 連線以及在網站上設定的所有 Runbook。

必要條件

災難復原網站上沒有可用的雲端伺服器。

若要移除災難復原網站

1. 在 Cyber Protect 主控台中，移至 **[Disaster Recovery]** > **[連線]**。
2. 按一下 **[顯示屬性]**。
3. 按一下 **[移除災難復原網站]**。
4. 在確認視窗中，按一下 **[移除]**。

站台對站台 OpenVPN - 其他資訊

當您建立復原伺服器時，您要設定其**實際執行網路中的 IP 位址**及其**測試 IP 位址**。

執行容錯移轉 (在雲端執行虛擬機器)，並登入虛擬機器檢查伺服器的 IP 位址之後，您會看到**實際執行網路中的 IP 位址**。

當您執行測試容錯移轉時，只有使用僅能在復原伺服器設定中看到的**測試 IP 位址**，才能連線測試伺服器。

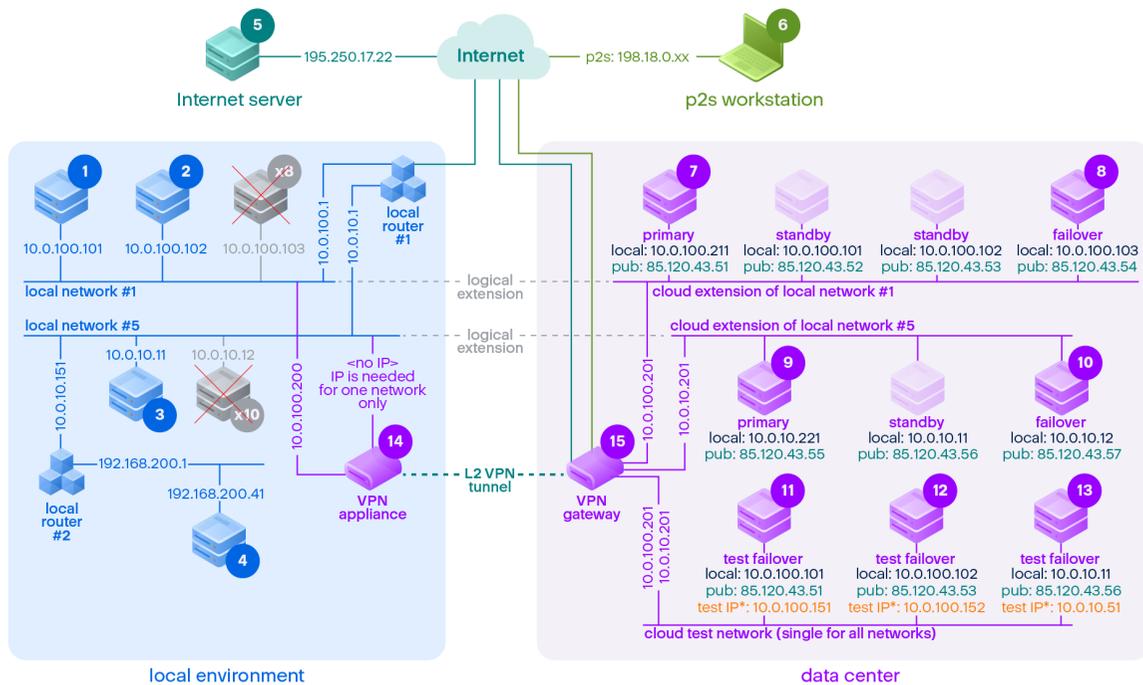
若要從本機站台連線測試伺服器，您必須使用**測試 IP 位址**。

注意事項

伺服器的網路設定一律會顯示**實際執行網路中的 IP 位址** (因為測試伺服器會鏡像實際執行伺服器的外觀)。發生這種情況是因為測試 IP 位址不屬於測試服務器，而是屬於 VPN 閘道，而且會使用 NAT 轉換為實際執行 IP 位址。

下圖顯示站台對站台 OpenVPN 設定的範例。本機環境中的部分伺服器會使用容錯移轉復原到雲端 (當網路基礎架構正常時)。

1. 客戶透過下列方式啟用 Disaster Recovery:
 - a. 設定 VPN 設備 (14)，然後將其連線至雲端 VPN 伺服器 (15)
 - b. 使用 Disaster Recovery (1、2、3、x8 和 x10) 保護部分本機伺服器
本機站台上的部分伺服器 (如 4) 連線至未連線到 VPN 設備的網路。這類伺服器沒有受到 Disaster Recovery 保護。
2. 部分伺服器 (已連線到不同的網路) 在本機站台運作:(1、2、3 和 4)
3. 受保護的伺服器 (1、2 和 3) 正在使用測試容錯移轉 (11、12 和 13) 進行測試
4. 本機站台中的部分伺服器無法使用 (x8、x10)。執行容錯移轉之後，這些伺服器變得可在雲端使用 (8 和 10)
5. 連線至不同網路的部分主要伺服器 (7 和 9) 可在雲端環境中使用
6. (5) 是網際網路中擁有公用 IP 位址的伺服器
7. (6) 是使用站台對站台 VPN 連線 (p2s) 連線至雲端的工作站



*The test IP belongs to the VPN gateway and is NATed to the recovery server. The recovery server has the production IP assigned to it.

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	透過本機路由	透過本機路由 1 和	否	透過通道: 本機	透過通道: 本機	透過通道: 本機	透過通道: 本機	透過通道: NAT (VPN 伺	透過通道: NAT (VPN 伺	透過本機路由 1 和通	直接	否

	至:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
				機 路 由 器 1	器 2	網際網 路		透過本機 路由器 1 和網際網 路:pub	透過本機 路由器 1 和網際網 路:pub	透過本機 路由器 1 和網際網 路:pub	透過本機 路由器 1 和網際網 路:pub	服 器) 透 過 本 機 路 由 器 1 和 網 際 網 路 : pub	服 器) 透 過 本 機 路 由 器 1 和 網 際 網 路 : pub	道:NAT (VPN 伺 服器) 透 過 本 機 路 由 器 1 和 網 際 網 路 : pub		
2	本機	直接		透 過 本 機 路 由 器 1	透 過 本 機 路 由 器 2	透 過 本 機 路 由 器 1 和 網 際 網 路	否	透 過 通 道: 本 機 透 過 本 機 路 由 器 1 和 網 際 網 路: pub	透 過 通 道: 本 機 透 過 本 機 路 由 器 1 和 網 際 網 路: pub	透 過 通 道: 本 機 透 過 本 機 路 由 器 1 和 網 際 網 路: pub	透 過 通 道: 本 機 透 過 本 機 路 由 器 1 和 網 際 網 路: pub	透 過 通 道: NAT (VPN 伺 服器) 透 過 本 機 路 由 器 1 和 網 際 網 路: pub	透 過 通 道: NAT (VPN 伺 服器) 透 過 本 機 路 由 器 1 和 網 際 網 路: pub	透 過 本 機 路 由 器 1 和 通 道: NAT (VPN 伺 服器) 透 過 本 機 路 由 器 1 和 網 際 網 路: pub	直接	否
3	本機	透 過 本 機 路 由 器 1	透 過 本 機 路 由 器 1		透 過 本 機 路 由 器 2	透 過 本 機 路 由 器 1 和 網 際 網 路	否	透 過 通 道: 本 機 透 過 本 機 路 由 器 1 和 網 際 網 路: pub	透 過 通 道: 本 機 透 過 本 機 路 由 器 1 和 網 際 網 路: pub	透 過 通 道: 本 機 透 過 本 機 路 由 器 1 和 網 際 網 路: pub	透 過 通 道: 本 機 透 過 本 機 路 由 器 1 和 網 際 網 路: pub	透 過 通 道: NAT (VPN 伺 服器) 透 過 本 機 路 由 器 1 和 網 際 網 路: pub	透 過 通 道: NAT (VPN 伺 服器) 透 過 本 機 路 由 器 1 和 網 際 網 路: pub	透 過 本 機 路 由 器 1 和 通 道: NAT (VPN 伺 服器) 透 過 本 機 路 由 器 1	透 過 本 機 路 由 器	否

	至:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
														和網際網路:pub		
4	本機	透過本機路由器 2 和路由器 1	透過本機路由器 2 和路由器 1	透過本機路由器 2		透過本機路由器 2 和路由器 1 和網際網路	否	透過本機路由器 2 和通道:本機 透過本機路由器 2 和本機路由器 1 和網際網路:pub	透過通道:NAT (VPN 伺服器) 透過本機路由器 2 和路由器 1 和網際網路:pub	透過通道:NAT (VPN 伺服器) 透過本機路由器 2 和路由器 1 和網際網路:pub	透過通道:NAT (VPN 伺服器) 透過本機路由器 2 和路由器 1 和網際網路:pub	透過本機路由器 2	否			
5	網際網路	否	否	否	否		不適用	透過網際網路:pub	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 - NAT (VPN 伺服器) 透過網際網路:pub	透過 p2s VPN - NAT (VPN 伺服器) 透過網際網路:pub	透過 p2s VPN - NAT (VPN 伺服器) 透過網際網路:pub	否	否			
7	主要	透過通道	透過通道	透過通道	透過通道和本機路	透過網際網路 (透過 VPN 伺	否		在雲端直接:本機	透過通道和本機路由器 1:本機	透過通道和本機路由器 1:本機	透過 VPN 伺服器:NAT	透過 VPN 伺服器:NAT	透過通道和本機路由器 1:NAT	否	僅限 DHCP 和 DNS 通訊協

	至:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
				和本機路由 器 1	由器 1 和 2	服务器)										定
8	容錯移轉	透過通道	透過通道	透過通道和本機路由 器 1	透過通道和本機路由 器 1 和 2	透過國際網路(透過 VPN 伺服器)	否	在雲端直接:本機		透過通道和本機路 由器 1: 本機	透過通道和本機路 由器 1: 本機	透過 VPN 伺 服器:NAT	透過 VPN 伺 服器:NAT	透過通道和本機路 由器 1:NAT	否	僅限 DHCP 和 DNS 通訊協定
9	主要	透過通道和本機路 由器 1	透過通道和本機路 由器 1	透過通道	透過通道	透過國際網路(透過 VPN 伺服器)	否	透過通道和本機路 由器 1: 本機	透過通道和本機路 由器 1: 本機		在雲端直接:本機	透過通道和本機路 由器 1:NAT	透過通道和本機路 由器 1:NAT	透過 VPN 伺 服器:NAT	否	僅限 DHCP 和 DNS 通訊協定
10	容錯移轉	透過通道和本機路	透過通道和本機路	透過通道	透過通道	透過國際網路(透過 VPN 伺	否	透過通道和本機路 由器 1: 本機	透過通道和本機路 由器 1: 本機	在雲端直接:本機		透過通道和本機路 由器 1:NAT	透過通道和本機路 由器 1:NAT	透過 VPN 伺 服器:NAT	否	僅限 DHCP 和 DNS 通訊協

	至:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		由器 1	由器 1			服器)										定
11	測試 容錯 移轉	否	否	否	否	透過網 際網路 (透過 VPN 伺 服器)	否	否	否	否	否		在雲端直 接:本機	透過 VPN 伺服器: 本機(路 由)	否	僅限 DHCP 和 DNS 通訊協 定
12	測試 容錯 移轉	否	否	否	否	透過網 際網路 (透過 VPN 伺 服器)	否	否	否	否	否	在雲端直 接:本機		透過 VPN 伺服器: 本機(路 由)	否	僅限 DHCP 和 DNS 通訊協 定
13	測試 容錯 移轉	否	否	否	否	透過網 際網路 (透過 VPN 伺 服器)	否	否	否	否	否	透過 VPN 伺服器: 本機(路 由)	透過 VPN 伺服器: 本機(路 由)		否	僅限 DHCP 和 DNS 通訊協 定
14	VPN 設備	直接	直接	透過 本機 路由 器 1	透過 本機 路由 器 2	透過網 際網路 (本機 路由器 1)	否	否	否	否	否	否	否	否		否
15	VPN	否	否	否	否	否	否	否	否	否	否	否	否	否	否	

	至:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	伺服器															

辭彙表

R

Runbook

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。

V

VPN 設備

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)

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

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

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

在公司內部部署上部署的本機基礎架構。

受

受保護的伺服器

客戶所擁有並受到此服務所保護的實體或虛擬機器。

容

容錯回復

伺服器在容錯移轉期間移動到雲端之後，將這些伺服器還完到本機站台的程序。

容錯移轉

在本機站台上發生自然或人為災難時，將工作負載或應用程式切換到雲端站台。

站

站台對站台 (S2S) 連線

將區域網路透過安全的 VPN 通道延伸至雲端的連線。

復

復原伺服器

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)

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

實際執行容錯移轉的中繼狀態或雲端伺服器的復原程序。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。

測

測試 IP 位址

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

隔離的虛擬網路, 用於測試容錯移轉程序。

雲

雲端伺服器

復原或主要伺服器的一般參考。

雲端站台 (或 DR 網站)

在雲端託管並用於執行復原基礎架構的遠端網站 (萬一發生災難)。

實

實際執行網路

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。

點

點對站台 (P2S) 連線

使用端點裝置 (例如電腦或筆記型電腦), 從外部對雲端和本機站台進行的安全 VPN 連線。

索引

C

Cyber Disaster Recovery Cloud 試用版產品 8

D

Disaster Recovery - 符合資格的裝置 84

Disaster Recovery 與加密軟體的相容性 9

Disaster Recovery 儀表板 84

I

IP 位址重新設定 40

IPsec/IKE 安全性設定 29

R

Runbook 的相關作業 82

Runbook 參數 81

V

VPN 設備 18

VPN 裝置的需求 19

VPN 閘道 18, 26

VPN 閘道網路設定 18

下

下載 IPsec VPN 記錄檔 33

下載 MAC 位址 44

下載 OpenVPN 的設定 37

下載 VPN 設備的記錄 45

下載 VPN 閘道的記錄 45

允

允許透過 L2 VPN 的 DHCP 流量 24

公

公用和測試 IP 位址 39

手

手動容錯回復 76

支

支援的作業系統 5

支援的虛擬化平台 6

主

主要功能 5

主要伺服器的操作 54

代

代理程式型容錯回復 (透過可開機媒體) 69

必

必要條件 16, 28, 34-35, 43, 71, 74

必要條件: 42-44

本

本機站台的 VPN 存取 37

在

在僅限雲端模式下管理網路 16

多
多站台 IPsec VPN 記錄檔 34
多站台 IPsec VPN 連線 26

如
如何使用本機 DNS 執行伺服器的容錯移轉 67
如何執行 DHCP 伺服器的容錯移轉 67

次
次要伺服器的操作 50

自
自動刪除雲端站台上未使用的客戶環境 9
自動測試容錯移轉 63, 85

作
作用中的點對站台連線 37

刪
刪除自訂 DNS 伺服器 43

系
系統需求 19

使
使用 Microsoft Azure 虛擬機器進行操作 8
使用 Disaster Recovery 雲端 10
使用記錄 44
使用異地備援雲端儲存時的限制 8

建
建立 Runbook 79
建立主要伺服器 51

建立災難復原保護計劃 11
建立復原伺服器 47

後
後續步驟 11

計
計算點 60

重
重新安裝 VPN 閘道 42
重新指派 IP 位址 41
重新產生設定 37

限
限制 7

容
容錯回復 69

站
站台對站台 OpenVPN - 其他資訊 87
站台對站台 OpenVPN 連線 16

停
停止 Runbook 執行 83
停止容錯移轉 68
停用自動測試容錯移轉 64
停用站台對站台連線 25

健
健全狀況檢查 84

啟
啟用站台對站台連線 18

執
執行 Runbook 82
執行手動容錯回復 77
執行代理程式型容錯回復 (透過可開機媒體) 70
執行容錯移轉 66
執行測試容錯移轉 61
執行無代理程式容錯回復 (透過 Hypervisor 代理程式) 74

從
從多站台 IPsec VPN 切換至站台對站台 OpenVPN 31
從站台對站台 OpenVPN 切換至多站台 IPsec VPN 24

移
移除災難復原網站 86

設
設定主要伺服器 51
設定本機路由 44
設定多站台 IPsec VPN 27
設定多站台 IPsec VPN 設定 27
設定自訂 DNS 伺服器 42
設定自動測試容錯移轉 63
設定站台對站台 OpenVPN 19
設定站台對站台 OpenVPN 連線 19
設定復原伺服器 47

設定雲端伺服器的防火牆規則 57
設定僅雲端模式 15
設定點對站台遠端 VPN 存取 35

軟
軟體需求 5
連
連接埠 19
連線和網路 14

測
測試容錯移轉 61

無
無代理程式容錯回復 (透過 Hypervisor 代理程式) 72

雲
雲端伺服器 47
雲端伺服器的防火牆規則 56
雲端伺服器的備份 55

僅
僅雲端模式 14
路
路由的運作方式 15, 18, 27

預
預設雲端網路基礎架構 13

實
實際執行容錯移轉 65

對	點
對於 Active Directory 網域服務可用性的建議 38	點對站台遠端 VPN 存取 34
對於本機站台的一般建議 29	擷
疑	擷取網路封包 45
疑難排解 IPsec VPN 設定 32	關
疑難排解 IPsec VPN 設定問題 32	關於 Cyber Disaster Recovery Cloud 5
管	
管理 VPN 設備設定 20	
管理站台對站台 OpenVPN 的網路 21	
管理點對站台連線設定 36	
網	
網路管理 39	
編	
編排 (Runbook) 79	
編輯復原伺服器的預設設定 12	
適	
適用於 L2 OpenVPN 連線的 Active Directory 網 域控制站 38	
適用於 L3 IPsec VPN 連線的 Active Directory 網 域控制站 38	
檢	
檢查雲端防火牆活動 59	
檢視有關雲端伺服器的詳細資料 55	
檢視自動測試容錯移轉狀態 64	
檢視執行歷程記錄 83	