

Backup Exec 私人雲端服務

規劃和部署指南



目錄

第 1 章	Backup Exec 私人雲端服務簡介	5
	關於 Backup Exec 私人雲端服務	5
	Backup Exec 私人雲端服務的安全性考量	6
	多租用者 Backup Exec 伺服器組態安全需求	7
	Backup Exec 私人雲端服務的系統需求	8
第 2 章	架構 Backup Exec 私人雲端服務	11
	架構 Backup Exec 私人雲端服務	11
	關於 Backup Exec 私人雲端服務組態	13
	關於多租用者雲端 Backup Exec 伺服器組態	14
	關於雲端受管 Backup Exec 伺服器離站複本組態	15
	關於雲端中央管理伺服器離站複本組態	16
	關於直接備份組態	17
	設定多租用者或雲端離站複本組態	18
	安裝 Backup Exec 中央管理伺服器	19
	安裝受管 Backup Exec 伺服器	20
	為多租用者和離站複本組態設定儲存裝置	21
	關於播散離站複本組態的重複資料刪除磁碟儲存裝置	23
	設定直接備份組態	26
	架構直接備份組態的私人雲端重複資料刪除磁碟儲存裝置	26
	關於播散直接備份組態的重複資料刪除磁碟儲存裝置	27
第 3 章	使用 Backup Exec 私人雲端服務	31
	關於使用離站複本組態的 Backup Exec 私人雲端服務	31
	建立離站複本組態的備份定義	32
	關於使用離站複本組態從私人雲端還原資料	33
	在中央管理伺服器發生故障時從受管 Backup Exec 伺服器還原資料	35
	關於使用 Backup Exec 私人雲端服務和直接備份組態	36
	啟用直接備份組態的用戶端重複資料刪除	37
	建立直接備份組態的備份定義	37
	使用直接備份組態從私人雲端透過傳輸磁碟機還原資料	38
	關於雲端災難復原服務	39
	從容錯轉移復原伺服器或網站	39

從故障回復復原伺服器或網站	41
Backup Exec 重複資料刪除磁碟儲存裝置需求	42
WAN 延遲的限制	42
精細回復技術與離站復本的限制	43
Windows Small Business Server (SBS) 的限制和多租用者 Backup Exec 伺服器組態	43

第 4 章

架構 OpenVPN	45
關於架構 OpenVPN	45
架構 OpenVPN	45
在私人雲端 Backup Exec 實例上設定 OpenVPN	46
在電腦 2 上設定 OpenVPN	47
設定區域網路路由	48
關於設定防火牆	49
驗證 OpenVPN 連線	49
關於為多個用戶端設定 OpenVPN	51
網路問題疑難排解	52

Backup Exec 私人雲端服務 簡介

本章包含以下主題：

- [關於 Backup Exec 私人雲端服務](#)
- [Backup Exec 私人雲端服務的安全性考量](#)
- [Backup Exec 私人雲端服務的系統需求](#)

關於 Backup Exec 私人雲端服務

Backup Exec 私人雲端服務主要是提供給有興趣為客戶提供受管備份服務的受管型服務供應商(MSP)。Backup Exec 私人雲端服務可讓合作夥伴在其資料中心內以「私人雲端」組態方式主控備份儲存。

受管型服務供應商(MSP)可透過 Internet 提供備份服務給合作夥伴私人雲端，作為管理離站磁帶複本的替代方式。備份已進行加密和重複資料刪除，使透過 WAN 的傳輸既安全又有效率。本機備份仍可於內部部署時使用，以取得快速的還原功能。此外，Backup Exec 私人雲端服務可讓使用者直接備份至雲端。使用者可直接從雲端還原完整或詳細資料。

Backup Exec 私人雲端服務也可提供給具有分散極廣之網路的 Backup Exec 客戶。客戶可以從遠端辦公室，將重複的備份複本傳送到中央資料中心私人雲端位置內的磁碟儲存及磁帶儲存。

下表進一步說明一些相當重要的 Backup Exec 術語，有助於瞭解 Backup Exec 私人雲端服務。

表 1-1 Backup Exec 術語

術語	定義
重複資料刪除磁碟儲存	重複資料刪除磁碟儲存裝置在 Backup Exec 伺服器上提供整合式重複資料刪除。 附註： 您可以在雲端中使用 Symantec NetBackup 5000/5020 系列重複資料刪除儲存硬體裝置，而不是整合式 Backup Exec 重複資料刪除儲存裝置。硬體裝置可能提供更具可擴充性的選項，特別是針對大型多租用者組態。
最佳化複製	這是一種複製，允許從某一個 OpenStorage 裝置將經過重複資料刪除處理的資料直接複製到相同廠商的另一個 OpenStorage 裝置。
精細回復技術 (GRT)	備份選項，可讓您從資料庫備份還原個別項目。不需要對單一項目進行單獨的備份就可以復原該項目。

請參閱第 6 頁的「[Backup Exec 私人雲端服務的安全性考量](#)」。

請參閱第 8 頁的「[Backup Exec 私人雲端服務的系統需求](#)」。

請參閱第 11 頁的「[架構 Backup Exec 私人雲端服務](#)」。

請參閱第 13 頁的「[關於 Backup Exec 私人雲端服務組態](#)」。

Backup Exec 私人雲端服務的安全性考量

Backup Exec 私人雲端服務使用 Backup Exec 目前的工作和資源憑證模型，提供安全的體驗。另外，賽門鐵克建議您在客戶位置和使用 VPN 解決方案的資料中心之間使用安全的網路連線。有各種不同的 IPsec、SSL 層和其他 VPN 解決方案可供使用。

當您使用任何支援多個客戶的組態時，應使用 VLAN 或路由限制，讓客戶網路彼此保持隔離。

您可以使用慣用的任何 VPN 解決方案。本指南提供 OpenVPN 的參考組態指示。OpenVPN SSL VPN 開放原始碼套件會在私人雲端 Backup Exec 實例與本機 Backup Exec 伺服器之間提供安全且經過加密的連線。此元件通常需要開啟防火牆上的預設通訊埠 1194。不過，OpenVPN 可讓您架構改用其他通訊埠。OpenVPN 同時提供金鑰型和憑證型驗證方法。本文件提供設定這兩種方法的參考。

請參閱第 5 頁的「[關於 Backup Exec 私人雲端服務](#)」。

請參閱第 45 頁的「[關於架構 OpenVPN](#)」。

多租用者 Backup Exec 伺服器組態具有其他應考量的安全需求。

請參閱第 7 頁的「多租用者 Backup Exec 伺服器組態安全需求」。

多租用者 Backup Exec 伺服器組態安全需求

您可以將 Backup Exec 架構在私人雲端中，讓單一 Backup Exec 伺服器能夠安全地支援多個客戶或租用者。當您使用多租用者 Backup Exec 伺服器時，必須遵循額外的安全預防措施，因為伺服器中包含多個客戶的共用內容。

請參閱第 14 頁的「關於多租用者雲端 Backup Exec 伺服器組態」。

請參閱第 6 頁的「Backup Exec 私人雲端服務的安全性考量」。

當您架構多租用者 Backup Exec 伺服器時，應該考量下列安全需求：

- 內部部署受管 Backup Exec 伺服器必須安裝在實體電腦上。
- 內部部署受管 Backup Exec 伺服器必須啟用 Microsoft Windows BitLocker 功能，而且已在系統磁碟區上啟動該功能。
BitLocker 密碼不得洩漏給任何客戶。您也可以使用硬體磁碟加密解決方案，當作 BitLocker 的替代方案。
- 多租用者 Backup Exec 伺服器位於私人雲端，而內部部署 Backup Exec 伺服器必須是服務供應商網域的成員。
Backup Exec 伺服器不應允許登入客戶適用的協助工具。若要做額外的隔離，您可考慮將每一個客戶的受管 Backup Exec 伺服器放置在不同的服務供應商子網域中。
- 用於內部部署受管 Backup Exec 伺服器的服務供應商網域憑證，應該是本機管理員而非網域管理員的憑證。
- 多租用者雲端伺服器的重複資料刪除磁碟儲存裝置不得啟用用戶端重複資料刪除。
- 內部部署受管 Backup Exec 伺服器不應使用「無限制存取目錄和備份集以進行還原」選項進行安裝。您只能使用「集中管理 Backup Exec 伺服器」選項進行安裝。
- 您可以針對內部部署受管 Backup Exec 伺服器使用雙重驗證(若適用)，以提供額外的安全性。
賽門鐵克建議您使用 VeriSign VIP 驗證服務：
<http://www.verisign.com/authentication/two-factor-authentication/vip-authentication/index.html>

警告：遵循這些安全性建議，僅可為共用的 Backup Exec 網路和儲存裝置提供一定程度的存取安全性。若有人實體存取受管 Backup Exec 伺服器，並蓄意執行惡意動作，則理論上該人員可能會設法規避這些安全措施。對於您的內部部署受管 Backup Exec 伺服器，您可能需要考慮使用其他實體存取保護措施。

Backup Exec 私人雲端服務的系統需求

下表列出執行 Backup Exec 私人雲端服務的最低系統需求與建議：

表 1-2 Backup Exec 私人雲端服務的系統需求

需求	說明
Backup Exec 伺服器	<p>您可以採用三種不同方式的其中一種來架構 Backup Exec 私人雲端服務。</p> <p>請參閱第 13 頁的「關於 Backup Exec 私人雲端服務組態」。</p> <p>雲端中的任何 Backup Exec 伺服器，都必須包含 Backup Exec Deduplication Option。本機伺服器的唯一需求是，這些伺服器必須符合 Backup Exec 2012 的需求。</p> <p>您可以透過下列的 URL 找到相容的作業系統、平台和應用程式清單：</p> <p>http://entsupport.symantec.com/umi/V-269-1</p>
Deduplication Option 授權	<p>您必須同時在私人雲端伺服器和任何本機 Backup Exec 伺服器上安裝 Symantec Backup Exec Deduplication Option。</p> <p>您不需要在本機 Backup Exec 伺服器上建立重複資料刪除磁碟儲存裝置。不過，您必須在本機 Backup Exec 伺服器上安裝 Deduplication Option，如此才能在雲端中的伺服器上存取共用的重複資料刪除磁碟儲存裝置。在雲端 Backup Exec 伺服器上，所有組態都需要重複資料刪除磁碟儲存裝置。</p>
Central Admin Server Option 授權	<p>如果您使用多租用戶或離站複本組態，則必須在本機和雲端電腦上安裝 Symantec Backup Exec Enterprise Server Option 及其 Central Admin Server Option。</p>
作用中的 Internet 連線	<p>您必須擁有作用中的 Internet 連線，才能將資料傳輸到私人雲端重複資料刪除磁碟儲存裝置。</p>

需求	說明
虛擬私人網路 (VPN)	<p>賽門鐵克建議您在客戶位置和使用 VPN 解決方案的資料中心之間使用安全的網路連線。另提供各種不同的 IPsec 和 SSL 層 VPN 解決方案。</p> <p>本指南提供 OpenVPN 的組態指示。 OpenVPN SSLVPN 開放原始碼套件會在私人雲端 Backup Exec 實例與本機 Backup Exec 伺服器之間提供安全且經過加密的連線。</p>

架構 Backup Exec 私人雲端服務

本章包含以下主題：

- [架構 Backup Exec 私人雲端服務](#)
- [關於 Backup Exec 私人雲端服務組態](#)
- [設定多租用者或雲端離站複本組態](#)
- [設定直接備份組態](#)

架構 Backup Exec 私人雲端服務

若要架構 Backup Exec 私人雲端服務，您必須完成下列步驟。

表 2-1 如何架構 Backup Exec 私人雲端服務

步驟	說明
步驟 1	您必須在私人雲端 Backup Exec 伺服器實例與在區域網路上執行的任何電腦之間架構 VPN。 請參閱第 45 頁的「 架構 OpenVPN 」。 請參閱第 51 頁的「 關於為多個用戶端設定 OpenVPN 」。

步驟	說明
步驟 2	<p>考量哪個 Backup Exec 私人雲端服務組態最符合您的需求，然後選取一個組態。您可以為多個客戶選擇單一多租用者組態。或者，您也可以為每個客戶選擇使用專用的雲端離站複本組態或直接備份組態。</p> <p>請參閱第 13 頁的「關於 Backup Exec 私人雲端服務組態」。</p> <p>您必須架構 Backup Exec 私人雲端服務。</p> <p>請參閱第 18 頁的「設定多租用者或雲端離站複本組態」。</p> <p>請參閱第 26 頁的「設定直接備份組態」。</p>
步驟 3	<p>架構 VPN 和 Backup Exec 之後，您便可以開始使用 Backup Exec 私人雲端服務。</p> <p>請參閱第 31 頁的「關於使用離站複本組態的 Backup Exec 私人雲端服務」。</p> <p>請參閱第 36 頁的「關於使用 Backup Exec 私人雲端服務和直接備份組態」。</p>
步驟 4	<p>如果您使用具有通訊埠限制的 VPN 閘道，則可能需要同時在內部部署和雲端 VPN 閘道上開啟通訊埠例外。通訊埠例外可讓位於雲端的 Backup Exec 伺服器與內部部署 Backup Exec 伺服器 and 代理程式通訊。</p> <p>您也應將 CAS Backup Exec SQL 通訊埠從動態指派的通訊埠變更為靜態通訊埠。</p> <p>附註：如果您使用 OpenVPN，則可能不需要架構閘道防火牆通訊埠例外。OpenVPN 通常會架構為通過防火牆的通道。</p> <p>下列 Backup Exec 支援文章列出 Backup Exec 需要的所有通訊埠號，以及必須開啟哪些通訊埠號：</p> <p>http://www.symantec.com/business/support/index?page=content&id=HOWTO22990#id-SF700155293</p> <p>http://www.symantec.com/business/support/index?page=content&id=HOWTO22989</p> <p>http://www.symantec.com/business/support/index?page=content&id=HOWTO23022</p> <p>下列 Backup Exec 支援文章詳細說明如何架構 SQL 靜態通訊埠：</p> <p>http://www.symantec.com/business/support/index?page=content&id=HOWTO22985</p>

關於 Backup Exec 私人雲端服務組態

您可以採用四種方式的其中一種來架構 Backup Exec 私人雲端服務。

表 2-2 Backup Exec 私人雲端服務的特定組態

組態類型	詳細資訊
多租用者雲端 Backup Exec 伺服器	<p>多租用者雲端 Backup Exec 伺服器組態會提供離站複本及直接備份給位於私人雲端內的 Backup Exec 伺服器或中央管理伺服器。單一私人雲端 Backup Exec 伺服器可用來為多個客戶備份資料。</p> <p>請參閱第 14 頁的「關於多租用者雲端 Backup Exec 伺服器組態」。</p>
雲端受管 Backup Exec 伺服器離站複本	<p>雲端受管 Backup Exec 伺服器離站複本組態會使用受管 Backup Exec 伺服器、中央管理伺服器和網域控制器。此組態針對位於私人雲端內的受管 Backup Exec 伺服器，提供離站複本功能。此組態需要每個客戶一部受管 Backup Exec 伺服器。</p> <p>請參閱第 15 頁的「關於雲端受管 Backup Exec 伺服器離站複本組態」。</p>
雲端中央管理伺服器離站複本	<p>雲端中央管理伺服器離站複本組態與第一個組態類似，其差異在於系統會預先保留中央管理伺服器和受管 Backup Exec 伺服器的位置。此組態針對位於私人雲端內的中央管理伺服器，提供離站複本功能。此組態需要每個客戶一部中央管理伺服器</p> <p>請參閱第 16 頁的「關於雲端中央管理伺服器離站複本組態」。</p>
直接備份	<p>直接備份組態使用 Backup Exec Agent for Windows 或 Backup Exec Agent for Linux，而不使用受管 Backup Exec 伺服器或中央管理伺服器。此組態使用位於私人雲端內的 Backup Exec 伺服器，提供直接備份功能。此組態需要每個客戶一部 Backup Exec 伺服器。</p> <p>請參閱第 17 頁的「關於直接備份組態」。</p>

請參閱第 45 頁的「[關於架構 OpenVPN](#)」。

請參閱第 18 頁的「[設定多租用者或雲端離站複本組態](#)」。

請參閱第 26 頁的「[設定直接備份組態](#)」。

關於多租用者雲端 Backup Exec 伺服器組態

多租用者雲端 Backup Exec 伺服器組態涉及多部電腦。

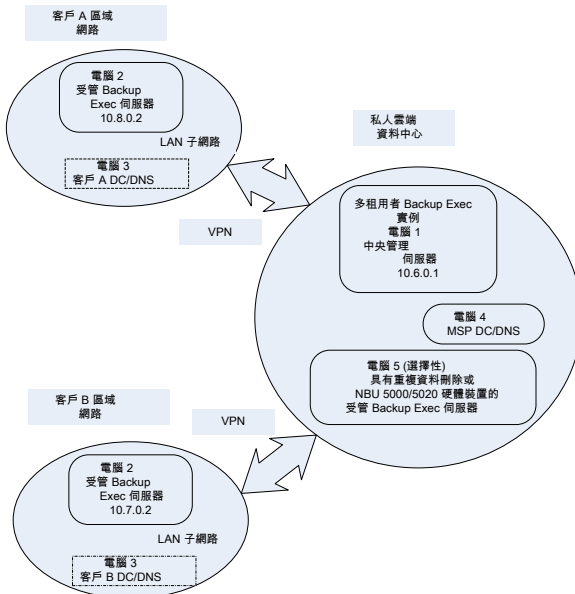
表 2-3 多租用者雲端 Backup Exec 伺服器組態

電腦	角色
電腦 1	第一部電腦(C1)是 Windows 64 位元伺服器，這個伺服器上已經安裝 Backup Exec 2012。C1 架構為中央管理伺服器，而且位於私人雲端中。
電腦 2	第二部電腦(C2)是 Windows 伺服器，這個伺服器上已經安裝 Backup Exec 2012。C2 是位於區域網路上的受管 Backup Exec 伺服器，並且是服務提供者的雲端網域 (C4) 的成員。 附註： 如果不需要本機重複資料刪除磁碟儲存裝置，可以為 C2 使用 32 位元本機 Backup Exec 伺服器。
電腦 3	第三部電腦(C3)是一個網域控制器和 DNS。您必須針對每個客戶位置架構 C3 電腦。
電腦 4	第四部電腦(C4)是位於私人雲端的網域控制器和 DNS。
電腦 5 (選擇性)	第五部電腦(C5)是選用的 (但是建議使用) 受管 Backup Exec 伺服器。C5 包含可用於複寫 C1 電腦之重複資料刪除儲存裝置的重複資料刪除儲存資料夾，以增加額外的容錯功能和可靠性。C5 可以與 C1 共置於私人雲端中的相同位置，也可以位於不同的實體位置。 您可以在雲端 Backup Exec 伺服器上架構 NetBackup 5000/5020 系列重複資料刪除儲存硬體裝置作為 OST 裝置，來代替位於相同位置的 C5 電腦。

此組態可讓您管理私人雲端資料中心內的所有 Backup Exec 工作。不過，它會要求中央管理伺服器和受管 Backup Exec 伺服器之間的網路連線永遠處於作用中狀態。即使您是在本機執行工作，網路連線還是必須處於作用中狀態。

警告： 如果您使用單一雲端 Backup Exec 伺服器支援多個客戶，賽門鐵克要求 C1、C2、C4 及 C5 位於只有您可以存取的網域中。為了避免任何可能造成安全風險的意外或惡意活動，請切勿授予客戶任何類型的 C2 登入存取權。

圖 2-1 多租用者雲端 Backup Exec 伺服器



請參閱第 13 頁的「關於 Backup Exec 私人雲端服務組態」。

關於雲端受管 Backup Exec 伺服器離站複本組態

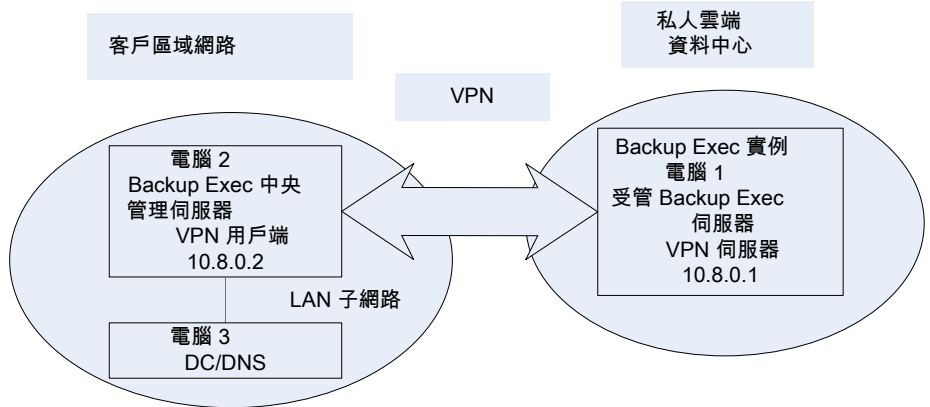
雲端受管 Backup Exec 伺服器離站複本組態涉及三部電腦。

表 2-4 雲端受管 Backup Exec 伺服器離站複本組態

電腦	角色
電腦 1	第一部電腦(C1)是 Windows 64 位元伺服器，這個伺服器上已經安裝 Backup Exec 2012。C1 架構為受管 Backup Exec 伺服器，而且位於私人雲端中。
電腦 2	第二部電腦(C2)是 Windows 64 位元伺服器，這個伺服器上已經安裝 Backup Exec 2012。C2 是位於區域網路上的中央管理伺服器。 附註： 如果不希望使用本機重複資料刪除磁碟儲存裝置，可以為 C2 使用 32 位元本機 Backup Exec 伺服器。
電腦 3	第三部電腦 (C3) 是一個網域控制器和 DNS。

中央管理伺服器 and 受管 Backup Exec 伺服器之間的網路連線不需要一直處於作用中狀態。只有在您執行涉及私人雲端中受管 Backup Exec 伺服器的任何工作時，才需要網路連線。對於本機工作而言，網路連線不需要處理作用中狀態。

圖 2-2 雲端受管 Backup Exec 伺服器離站複本



請參閱第 13 頁的「關於 Backup Exec 私人雲端服務組態」。

關於雲端中央管理伺服器離站複本組態

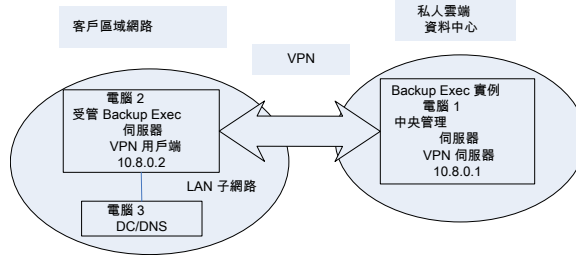
雲端中央管理伺服器離站複本組態涉及三部電腦。

表 2-5 雲端中央管理伺服器離站複本組態

電腦	角色
電腦 1	第一部電腦(C1)是 Windows 64 位元伺服器，這個伺服器上已經安裝 Backup Exec 2012。C1 架構為中央管理伺服器，而且位於私人雲端中。
電腦 2	第二部電腦(C2)是 Windows 64 位元伺服器，這個伺服器上已經安裝 Backup Exec 2012。C2 是位於區域網路上的受管 Backup Exec 伺服器。 附註： 如果不希望使用本機重複資料刪除磁碟儲存裝置，可以為 C2 使用 32 位元本機 Backup Exec 伺服器。
電腦 3	第三部電腦(C3)是一個網域控制器和 DNS。

此組態可讓您管理私人雲端之資料中心內的所有 Backup Exec 工作。不過，它會要求中央管理伺服器 and 受管 Backup Exec 伺服器之間的網路連線永遠處於作用中狀態。即使您是在本機執行工作，網路連線還是必須處於作用中狀態。

圖 2-3 雲端中央管理伺服器離站複本



請參閱第 13 頁的「關於 Backup Exec 私人雲端服務組態」。

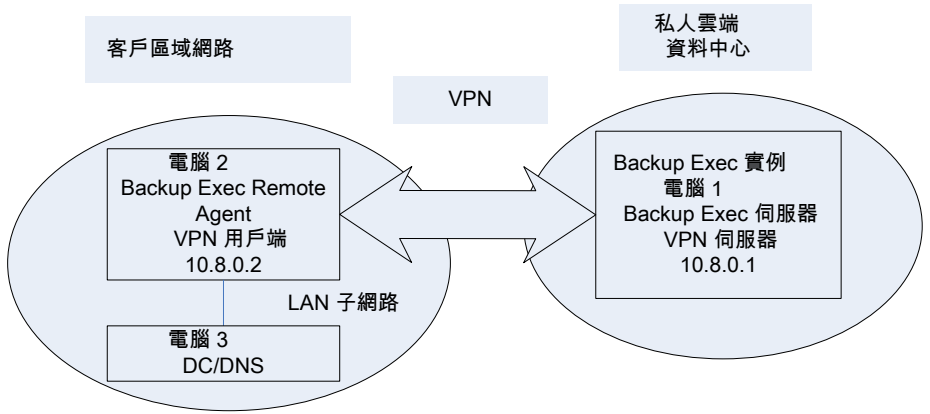
關於直接備份組態

直接備份組態至少包含三部電腦。

表 2-6 直接備份組態

電腦	角色
電腦 1	第一部電腦 (C1) 是位於私人雲端資料中心的 Windows 64 位元伺服器 Backup Exec 2012 伺服器。
電腦 2	第二部電腦 (C2) 是位於區域網路的 Agent for Windows 或 Agent for Linux 用戶端。您可以架構多部代理程式用戶端電腦。
電腦 3	第三部電腦 (C3) 是一個網域控制器和 DNS。

圖 2-4 直接備份



請參閱第 13 頁的「關於 Backup Exec 私人雲端服務組態」。

設定多租用者或雲端離站複本組態

在私人雲端伺服器上架構 VPN 之後，應架構 Backup Exec 伺服器或服務。

請參閱第 11 頁的「架構 Backup Exec 私人雲端服務」。

您可以從多租用者組態選取，或從兩個雲端離站複本組態中選取其中一個：

請參閱第 14 頁的「關於多租用者雲端 Backup Exec 伺服器組態」。

請參閱第 15 頁的「關於雲端受管 Backup Exec 伺服器離站複本組態」。

請參閱第 16 頁的「關於雲端中央管理伺服器離站複本組態」。

表 2-7 如何架構雲端離站複本組態

步驟	說明
步驟 1	安裝 Backup Exec 中央管理伺服器。 請參閱第 19 頁的「安裝 Backup Exec 中央管理伺服器」。
步驟 2	安裝受管 Backup Exec 伺服器。 請參閱第 20 頁的「安裝受管 Backup Exec 伺服器」。
步驟 3	架構儲存裝置。 請參閱第 21 頁的「為多租用者和離站複本組態設定儲存裝置」。

步驟	說明
步驟 4	使用資料播散重複資料刪除磁碟儲存裝置。 請參閱第 23 頁的「關於播散離站複本組態的重複資料刪除磁碟儲存裝置」。

安裝 Backup Exec 中央管理伺服器

您必須在作為 Backup Exec 中央管理伺服器的電腦上安裝 Backup Exec for Windows Servers。

請參閱第 18 頁的「設定多租用者或雲端離站複本組態」。

如果您使用多租用者雲端 Backup Exec 伺服器組態，則必須將雲端 Backup Exec 伺服器安裝為中央管理伺服器 (電腦 1 或 C1)。

如果您使用雲端受管 Backup Exec 伺服器離站複本組態，則中央管理伺服器會安裝在當地辦公室 Backup Exec 伺服器 (電腦 2 或 C2) 上。否則，中央管理伺服器會安裝為雲端中央管理伺服器離站複本組態所使用的雲端 Backup Exec 伺服器 (電腦 1 或 C1)。

您必須將中央管理伺服器新增至某個網域。在中央管理伺服器上安裝 Enterprise Server Option 及其 Central Admin Server Option (CASO)。

表 2-8 如何安裝 Backup Exec 中央管理伺服器

步驟	說明
步驟 1	若要架構多租用者 Backup Exec 伺服器，請將 Backup Exec 伺服器新增至雲端網域。 若要架構多租用者 Backup Exec 伺服器組態以外的任何組態，請完成下列步驟，將 Backup Exec 伺服器新增至您的本機網域： <ul style="list-style-type: none"> ■ 使用 Windows 中的「電腦內容」對話方塊，將伺服器新增至該網域。 ■ 出現提示時，重新啟動電腦。
步驟 2	伺服器重新啟動後，使用您要授與本機 Backup Exec 實例管理員權限的網域帳戶登入。
步驟 3	使用適當的授權碼安裝 Backup Exec 2012。 如需安裝 Backup Exec 的詳細資訊，請參閱「Symantec Backup Exec 管理指南」。 Backup Exec 合作夥伴可以從賽門鐵克 PartnerNet 網站取得授權資訊，連結如下： https://partnernet.symantec.com/Partnercontent/Login.jsp

步驟	說明
步驟 4	<p>安裝 Backup Exec 時，包含 Enterprise Server Option 及其 Central Admin Server Option (CASO)。</p> <p>如需安裝 CASO 的詳細資訊，請參閱「Symantec Backup Exec 管理指南」。</p> <p>若您使用多租用者或雲端中央管理伺服器離站複本組態，請安裝 Deduplication Option。對於雲端受管 Backup Exec 伺服器離站複本組態而言，在中央管理伺服器上使用本機重複資料刪除磁碟儲存裝置是選擇性的。</p>
步驟 5	<p>安裝 Backup Exec 時，使用網域憑證作為預設系統登入帳戶。</p>
步驟 6	<p>如果您要針對雲端執行增量 Exchange GRT 複製備份工作，請在安裝完成後，將下列登錄值設定為 1。變更該登錄值會停用 Backup Exec 伺服器上重複資料刪除磁碟儲存裝置的 GRT 對 GRT 複製複本功能。</p> <p>dword HKEY LOCAL MACHINE\SOFTWARE\Symantec\Backup Exec for Windows\Backup Exec\Engine\Misc\DisablePDI2PDISetCopy</p> <p>現在這部電腦是中央管理伺服器，可跨 WAN 控制受管 Backup Exec 伺服器。</p> <p>如需離站複本精細回復技術 (GRT) 之限制的詳細資訊，請參閱下列主題：</p> <p>請參閱第 43 頁的「精細回復技術與離站複本的限制」。</p>

安裝受管 Backup Exec 伺服器

您必須安裝受管 Backup Exec 伺服器。如果您使用雲端受管 Backup Exec 伺服器離站複本組態，則受管 Backup Exec 伺服器會安裝為雲端 Backup Exec 伺服器 (電腦 1 - C1)。否則，受管 Backup Exec 伺服器會安裝在當地辦公室 Backup Exec 伺服器 (電腦 2 - C2) 上。

請參閱第 18 頁的「[設定多租用者或雲端離站複本組態](#)」。

安裝受管 Backup Exec 伺服器

1 執行下列其中一項動作：

多租用者組態：

將 Backup Exec 伺服器新增至雲端網域。

任何其他組態：

完成下列步驟，將 Backup Exec 伺服器新增至您的本機網域：

- 使用 Windows 中的「電腦內容」對話方塊，將伺服器新增至網域。
- 出現提示時，重新啟動電腦。

- 2 伺服器重新啟動後，使用具備本機 Backup Exec 伺服器管理員權限的網域帳戶登入。
- 3 在伺服器上安裝 Backup Exec 2012，然後選取「**受管 Backup Exec 伺服器**」安裝選項。
- 4 出現提示時，指定您用來安裝中央管理伺服器的同一個系統登入帳戶憑證。
- 5 如果您要使用雲端受管 Backup Exec 伺服器離站複本組態，請選取 **Deduplication Option**。

對於雲端中央管理伺服器離站複本組態而言，在受管 Backup Exec 伺服器上使用本機重複資料刪除磁碟儲存裝置是選擇性的。

- 6 當 Backup Exec 提示您提供中央管理伺服器時，請輸入本機 Backup Exec 中央管理伺服器的資訊。
- 7 選取「**集中管理 Backup Exec 伺服器**」選項。

如果使用多租用者組態，請勿選取「**無限制存取目錄和備份集以進行還原**」。

- 8 如果您要針對雲端執行增量 Exchange GRT 複製備份工作，請在安裝完成後，將下列登錄值設定為 **1**。

dword HKEY LOCAL MACHINE\SOFTWARE\Symantec\Backup Exec for Windows\Backup Exec\Engine\Misc\DisablePDI2PDISetCopy

變更該登錄值會停用 Backup Exec 伺服器上重複資料刪除磁碟儲存裝置的 GRT 對 GRT 複製複本功能。

- 9 在中央管理伺服器上開啟 Backup Exec。
- 10 選取「**儲存**」標籤，然後連按兩下位於私人雲端資料中心的 Backup Exec 伺服器。
- 11 在左窗格中，按下「**設定**」。
- 12 在「**私人雲端伺服器**」欄位中，選取「**已啟用**」。

為多租用者和離站複本組態設定儲存裝置

在您可以針對私人雲端執行備份工作之前，必須架構儲存裝置。

請參閱第 18 頁的「[設定多租用者或雲端離站複本組態](#)」。

表 2-9 如何為離站複本組態設定儲存裝置

步驟	說明
步驟 1	<p>在本機電腦 2 (C2) 上建立新的本機磁碟儲存裝置。您可以建立重複資料刪除磁碟儲存裝置 (如有需要)。</p> <p>如需建立儲存裝置的詳細資訊，請參閱「Symantec Backup Exec 管理指南」。</p>
步驟 2	<p>在您的私人雲端 Backup Exec 實例上建立新的重複資料刪除磁碟儲存裝置。</p> <p>您可以為多租用者組態架構 NetBackup 5000/5020 系列重複資料刪除儲存硬體裝置，而無須使用整合式重複資料刪除儲存。在多租用者中央管理伺服器上，將硬體裝置架構為 OST 儲存裝置。</p> <p>如需建立重複資料刪除磁碟儲存裝置的詳細資訊，請參閱「Symantec Backup Exec 管理指南」。</p> <p>如果您使用多租用者組態，則必須完成下列步驟，以停用私人雲端重複資料刪除磁碟儲存裝置的用戶端重複資料刪除：</p> <ul style="list-style-type: none"> ■ 在「儲存」標籤上連接兩下私人雲端 Backup Exec 伺服器的重複資料刪除磁碟儲存裝置。 ■ 選取「內容」。 ■ 在「用戶端重複資料刪除」欄位中，選取「已停用」。 ■ 重新啟動 Backup Exec 伺服器的服務。 <p>賽門鐵克建議您針對重複資料刪除磁碟儲存裝置使用專用的磁碟區 (如有可能)。為重複資料刪除磁碟儲存裝置指定一個唯一的名稱，讓您可以輕鬆區別本機重複資料刪除磁碟儲存裝置 (如果已建立的話)。</p>
步驟 3	<p>如果您希望在私人雲端重複資料刪除磁碟儲存裝置上加密靜態資料，請在架構新的重複資料刪除磁碟儲存裝置時，選取「是，在資料傳輸到此重複資料刪除磁碟儲存裝置期間以及在其中儲存時加密資料」。對於現有的重複資料刪除裝置，您可以修改重複資料刪除裝置內容中的「加密」欄位。</p> <p>附註：VPN 會在本機 Backup Exec 伺服器和雲端 Backup Exec 伺服器之間加密傳輸中的資料。</p>
步驟 4	<p>與本機 Backup Exec 電腦共用新的雲端重複資料刪除磁碟儲存裝置。</p> <p>如需共用重複資料刪除磁碟儲存裝置的詳細資訊，請參閱「Symantec Backup Exec 管理指南」。</p>

步驟	說明
步驟 5	<p>使用 Backup Exec Services Manager 停止本機 Backup Exec 伺服器上的所有 Backup Exec 服務，然後再重新啟動。</p> <p>與本機 Backup Exec 伺服器共用雲端重複資料刪除磁碟儲存裝置的程序現在已完成。私人雲端重複資料刪除磁碟儲存裝置應該會出現，而且現在可以同時從 C1 和 C2 存取。</p>
步驟 6 (選擇性)	<p>針對多租用戶組態，您可以在雲端安裝包含重複資料刪除儲存裝置的額外受管 Backup Exec 伺服器。該額外受管 Backup Exec 伺服器可以和主要雲端 Backup Exec 伺服器共用，以複寫主要伺服器的重複資料刪除儲存裝置。</p> <p>您可以安裝 NetBackup 5000/5020 系列重複資料刪除儲存硬體裝置來代替額外受管 Backup Exec 伺服器。該硬體裝置可用於複寫。在主要雲端 Backup Exec 伺服器上，將該硬體裝置新增為 OST 儲存裝置。</p> <p>警告：您必須停用其中任一項選用組態的用戶端重複資料刪除。</p>

關於播散離站複本組態的重複資料刪除磁碟儲存裝置

為避免透過 Internet 傳輸時花費太長時間，您可以在雲端中利用需要開始使用的資料，播散重複資料刪除磁碟儲存裝置。播散重複資料刪除磁碟儲存裝置是將任何初始組態檔或備份集放置到重複資料刪除磁碟儲存裝置中備用的程序。傳輸時間取決於要複製和備份至私人雲端 Backup Exec 實例的資料量。

您可以根據資料類型，使用兩種方法之一來播散初始資料：

- 您可以利用「系統狀態」作業系統備份，播散重複資料刪除磁碟儲存裝置。藉由執行在私人雲端中執行之其他電腦的「系統狀態」資料複製備份工作，播散重複資料刪除磁碟儲存裝置。備份電腦的「系統狀態」資料，這些電腦執行的作業系統與您要備份的本機電腦作業系統相同。
請參閱第 23 頁的「[播散離站複本組態的作業系統檔案](#)」。
- 您可以從本機 Backup Exec 伺服器將包含相關資料之備份集的實體傳輸磁碟機傳送至私人雲端資料中心。
請參閱第 24 頁的「[關於使用傳輸磁碟機播散離站複本組態的重複資料刪除磁碟儲存裝置](#)」。

播散離站複本組態的作業系統檔案

為避免透過 Internet 傳輸時花費太長時間，您可以在雲端中利用需要開始使用的資料，播散重複資料刪除磁碟儲存裝置。播散重複資料刪除磁碟儲存裝置的其中一種方式，就是使用其他已共置電腦的「系統狀態」備份資料。

請參閱第 23 頁的「[關於播散離站複本組態的重複資料刪除磁碟儲存裝置](#)」。

表 2-10 如何播散離站複本組態的作業系統檔案

步驟	說明
步驟 1	<p>在已共置於私人雲端的任何電腦上安裝 Agent for Windows 或 Agent for Linux。</p> <p>如需安裝 Backup Exec 代理程式的相關資訊，請參閱「Symantec Backup Exec 管理指南」。</p> <p>電腦執行的作業系統版本應該與客戶區域網路上要備份的伺服器所執行的作業系統相同。</p>
步驟 2	<p>在私人雲端 Backup Exec 伺服器上建立和執行備份工作。將這些已共置電腦的「系統狀態」和系統磁碟區，備份至私人雲端重複資料刪除磁碟儲存裝置。</p>

關於使用傳輸磁碟機播散離站複本組態的重複資料刪除磁碟儲存裝置

為避免透過 Internet 傳輸時花費太長時間，您可以在雲端中利用需要開始使用的資料，播散重複資料刪除磁碟儲存裝置。播散重複資料刪除磁碟儲存裝置的其中一種方式，就是使用實體傳輸磁碟機。

請參閱第 23 頁的「關於播散離站複本組態的重複資料刪除磁碟儲存裝置」。

賽門鐵克提供了一個計算機工具，可讓您比較使用傳輸磁碟機所需的時間與透過網際網路複製資料所需的時間。計算機位於下列連結：

<http://entsupport.symantec.com/umi/V-269-34>

若要使用傳輸磁碟機播散您的私人雲端 Backup Exec 實例，請完成以下程序：

請參閱第 24 頁的「使用傳輸磁碟機播散離站複本組態的重複資料刪除磁碟儲存裝置」。

使用傳輸磁碟機播散離站複本組態的重複資料刪除磁碟儲存裝置

您可以使用實體傳輸磁碟機，播散私人雲端 Backup Exec 重複資料刪除磁碟儲存裝置。使用重複資料刪除磁碟儲存裝置一開始採用的檔案進行播散，可為您省下透過 Internet 執行大型備份的時間。

請參閱第 24 頁的「關於使用傳輸磁碟機播散離站複本組態的重複資料刪除磁碟儲存裝置」。

使用傳輸磁碟機播散離站複本組態的重複資料刪除磁碟儲存裝置

- 1 在本機 Backup Exec 伺服器 (即電腦 2 (C2)) 的可攜式磁碟機上建立磁碟儲存。
- 2 使用以下其中一種方法，複製一個備份集到磁碟儲存，並利用軟體加密將資料加密。

在安裝期間若未建立 DisablePDI2PDISetCopy 登錄機碼，就可以複製備份集

完成下列步驟：

- 針對您要用來播散私人雲端重複資料刪除磁碟儲存裝置的資料，選取複製該資料的最新完整備份集。
- 在「複製工作」對話方塊中，選取您建立為儲存目的地的磁碟儲存。
- 在「複製工作」對話方塊中，架構軟體加密。
您必須建立或選取軟體加密的加密金鑰。

您若在安裝期間建立了 DisablePDI2PDISetCopy 登錄機碼，就應建立完整的備份工作

完成下列步驟：

- 針對具備賽門鐵克精細回復技術 (GRT) 的任何應用程式，建立使用磁碟儲存的完整備份工作。
- 針對您要備份的任何具備 GRT 功能的特定應用程式，停用 GRT。
如需 GRT 離站複本限制的相關資訊，請參閱下列主題。
請參閱第 43 頁的「[精細回復技術與離站複本的限制](#)」。
- 在「儲存」面板上，啟用軟體加密。
您必須建立或選取軟體加密的加密金鑰。

- 3 執行您在上一個步驟中建立的工作。
- 4 將可攜式磁碟送至私人雲端資料中心。
- 5 將可攜式磁碟連接至私人雲端 Backup Exec 伺服器。
- 6 使用原本建立於磁碟機之磁碟儲存，在已連接可攜式磁碟機上建立磁碟儲存。
- 7 在可攜式磁碟儲存裝置上，建立並執行 Backup Exec 盤點作業。
- 8 在可攜式磁碟儲存裝置上，建立並執行 Backup Exec 目錄作業。

- 9 在磁碟儲存裝置上複製備份集，並將雲端重複資料刪除磁碟儲存裝置當作目的儲存裝置使用。
- 10 當複製作業完成時，您可以使用 Backup Exec 淘汰及刪除磁碟儲存中的檔案。使用磁碟公用程式將可攜式磁碟機清除乾淨。
當成功播散私人雲端重複資料刪除磁碟儲存裝置之後，就完成了組態程序。您可以繼續進行下列主題，開始在 Backup Exec 中執行工作：
請參閱第 31 頁的「關於使用離站複本組態的 Backup Exec 私人雲端服務」。

設定直接備份組態

在私人雲端伺服器上架構 OpenVPN 之後，應架構 Backup Exec 伺服器或服務。
請參閱第 11 頁的「架構 Backup Exec 私人雲端服務」。
直接備份組態至少包含三部電腦。
請參閱第 17 頁的「關於直接備份組態」。

表 2-11 如何架構直接備份組態

步驟	說明
步驟 1	架構私人雲端重複資料刪除磁碟儲存裝置。 請參閱第 26 頁的「架構直接備份組態的私人雲端重複資料刪除磁碟儲存裝置」。
步驟 2	使用資料播散私人雲端重複資料刪除磁碟儲存裝置。 請參閱第 27 頁的「關於播散直接備份組態的重複資料刪除磁碟儲存裝置」。

架構直接備份組態的私人雲端重複資料刪除磁碟儲存裝置

您必須在私人雲端實例上建立 Backup Exec 磁碟儲存裝置和重複資料刪除磁碟儲存裝置。
請參閱第 26 頁的「設定直接備份組態」。

表 2-12 如何架構私人雲端 Backup Exec 實例重複資料刪除磁碟儲存裝置

步驟	說明
步驟 1	使用具備本機伺服器管理員權限的網域帳戶登入 C1。
步驟 2	在 C1 上安裝 Backup Exec 2012，並指定系統登入。

步驟	說明
步驟 3	<p>在 C1 上的 Backup Exec 中，建立新的重複資料刪除磁碟儲存裝置。</p> <p>如果您希望在私人雲端重複資料刪除磁碟儲存裝置上加密靜態資料，請在架構新的重複資料刪除磁碟儲存裝置時，選取「是，在資料傳輸到此重複資料刪除磁碟儲存裝置期間以及在其中儲存時加密資料」。對於現有的重複資料刪除裝置，您可以修改重複資料刪除裝置內容中的「加密」欄位。</p> <p>附註：VPN 會在本機 Backup Exec 伺服器 and 雲端 Backup Exec 伺服器之間加密傳輸中的資料。</p> <p>如需建立重複資料刪除磁碟儲存裝置的詳細資訊，請參閱「Symantec Backup Exec 管理指南」。</p>
步驟 4	<p>啟用私人雲端伺服器設定：</p> <ul style="list-style-type: none"> ■ 在 Backup Exec 伺服器上開啟 Backup Exec。 ■ 按下 Backup Exec 按鈕，選取「組態與設定」，然後按下「本機伺服器內容」。 ■ 在左窗格中，按下「設定」。 ■ 在「私人雲端伺服器」欄位中，選取「已啟用」。

關於播散直接備份組態的重複資料刪除磁碟儲存裝置

為避免透過 Internet 傳輸時花費太長時間，您可以在雲端中利用需要開始使用的資料，播散重複資料刪除磁碟儲存裝置。播散重複資料刪除磁碟儲存裝置是將任何初始組態檔或備份集放置到重複資料刪除磁碟儲存裝置中備用的程序。傳輸時間取決於要複製和備份至私人雲端 Backup Exec 實例的資料量。

您可以根據要播散的資料類型，使用兩種方法之一來播散初始資料：

- 您可以利用「系統狀態」作業系統備份，播散重複資料刪除磁碟儲存裝置。藉由執行在私人雲端中執行之其他電腦的「系統狀態」資料備份工作，播散重複資料刪除磁碟儲存裝置。備份電腦的「系統狀態」資料，這些電腦執行的作業系統與您要備份的本機電腦作業系統相同。
請參閱第 28 頁的「播散直接備份組態的作業系統檔案」。
- 您可以從本機 Backup Exec 伺服器將包含相關資料之備份集的實體傳輸磁碟機傳送至私人雲端資料中心。
請參閱第 28 頁的「使用傳輸磁碟機播散直接備份組態的重複資料刪除磁碟儲存裝置」。

播散直接備份組態的作業系統檔案

為避免透過 Internet 傳輸時花費太長時間，您可以在雲端中利用需要開始使用的資料，播散重複資料刪除磁碟儲存裝置。播散重複資料刪除磁碟儲存裝置的其中一種方式，就是使用其他已共置電腦的「系統狀態」備份資料。

請參閱第 27 頁的「[關於播散直接備份組態的重複資料刪除磁碟儲存裝置](#)」。

表 2-13 如何播散直接備份組態的作業系統檔案

步驟	說明
步驟 1	<p>在您打算在本機客戶網路上進行備份的任何電腦上，安裝 Agent for Windows 及 Agent for Linux。</p> <p>如需安裝 Backup Exec 代理程式的相關資訊，請參閱「Symantec Backup Exec 管理指南」。</p> <p>用來播散資料的電腦所執行的作業系統版本應該與要備份的電腦相同。</p>
步驟 2	<p>在私人雲端 Backup Exec 伺服器上建立和執行備份工作。將這些已共置電腦的「系統狀態」和系統磁碟區，備份至私人雲端重複資料刪除磁碟儲存裝置。</p>

使用傳輸磁碟機播散直接備份組態的重複資料刪除磁碟儲存裝置

您可以使用實體傳輸磁碟機，播散私人雲端 Backup Exec 重複資料刪除磁碟儲存裝置。使用重複資料刪除磁碟儲存裝置一開始採用的檔案進行播散，可為您省下透過 Internet 執行大型備份的時間。

請參閱第 27 頁的「[關於播散直接備份組態的重複資料刪除磁碟儲存裝置](#)」。

表 2-14 如何使用傳輸磁碟機播散直接備份組態的重複資料刪除磁碟儲存裝置

步驟	說明
步驟 1	連接可攜式磁碟機至電腦 (C2)。
步驟 2	從 C2 將播散檔案複製到可攜式磁碟機。
步驟 3	使用任何協力廠商加密工具，加密磁碟上的檔案。
步驟 4	將傳輸磁碟機送至私人雲端資料中心。
步驟 5	將傳輸磁碟機連接至電腦 1 (C1)。
步驟 6	使用原本用來加密資料的相同工具，暫時解密傳輸磁碟機上的資料。

步驟	說明
步驟 7	建立並執行備份已解密檔案的備份工作。將雲端中的重複資料刪除磁碟儲存裝置當作目的地使用。
步驟 8	備份工作完成時，可以刪除複製的來源檔案。使用磁碟公用程式將可攜式磁碟機清除乾淨。

當成功播散私人雲端重複資料刪除磁碟儲存裝置之後，就完成了組態程序。

您可以繼續進行下列主題，開始使用 Backup Exec。

請參閱第 36 頁的「關於使用 Backup Exec 私人雲端服務和直接備份組態」。

使用 Backup Exec 私人雲端服務

本章包含以下主題：

- 關於使用離站複本組態的 Backup Exec 私人雲端服務
- 關於使用 Backup Exec 私人雲端服務和直接備份組態
- 關於雲端災難復原服務
- Backup Exec 重複資料刪除磁碟儲存裝置需求
- WAN 延遲的限制
- 精細回復技術與離站複本的限制
- Windows Small Business Server (SBS) 的限制和多租用者 Backup Exec 伺服器組態

關於使用離站複本組態的 Backup Exec 私人雲端服務

Backup Exec 私人雲端服務可讓您使用 Central Admin Server Option (CASO) 和 Deduplication Option 管理備份定義。

賽門鐵克提供了一個有用的計算機工具，可讓您估計透過網際網路複製資料所需的時間。雲端備份時間計算機也能幫助您規劃雲端備份策略。您可以使用計算機判斷系統資源是否適合在指定的備份時段內備份客戶的資料。時間估計可幫助您決定可合理支援的資料量，以及應分配給雲端備份的時間長度。

計算機位於下列連結：

<http://entsupport.symantec.com/umi/V-269-34>

請參閱第 32 頁的「[建立離站複本組態的備份定義](#)」。

請參閱第 33 頁的「關於使用離站複本組態從私人雲端還原資料」。

請參閱第 34 頁的「使用離站複本組態從私人雲端還原資料」。

請參閱第 34 頁的「使用離站複本組態，從私人雲端透過傳輸磁碟機還原資料」。

建立離站複本組態的備份定義

您可以藉由建立含複製階段的備份定義，將備份資料複製到私人雲端 Backup Exec 實例。備份定義位於中央管理伺服器上。該定義包含備份工作，用於將資料備份到本機重複資料刪除磁碟儲存裝置。該定義也包含複製階段，用於將那些備份集複製到私人雲端重複資料刪除磁碟儲存裝置。

您可以選擇性地將其他複製階段新增至備份定義，複製從雲端重複資料刪除儲存裝置複製的備份集。您可以將備份集複製到亦位於雲端的磁帶裝置，或是複製到受管 Backup Exec 伺服器上的另一個重複資料刪除儲存裝置。受管 Backup Exec 伺服器可以位於私人雲端，也可在不同的實體位置。

附註：如需建立備份定義的相關資訊，請參閱「Symantec Backup Exec 管理指南」。

建立離站複本組態的備份定義

- 1 在中央管理伺服器上，開啟 Backup Exec。
- 2 在「備份與還原」標籤上，執行下列其中一項作業：
 - 若要備份單一伺服器，請以滑鼠右鍵按下伺服器名稱。
 - 若要備份多部伺服器，請按 Shift 或 Ctrl 同時按下伺服器名稱，然後以滑鼠右鍵按下其中一個選取的伺服器。
- 3 在「備份」功能表上，選取要使用的備份選項。
- 4 在「名稱」欄位中，輸入備份定義的唯一名稱。

附註：如果從多部伺服器備份資料，Backup Exec 會將伺服器名稱附加到您在「名稱」欄位中輸入的文字。Backup Exec 會使用伺服器名稱和您輸入的文字，為每個備份定義建立唯一名稱。

- 5 執行下列任一項：

測試或編輯 Backup Exec 用來存取備份選取項目的憑證 在「選取項目」方塊中，按下「測試/編輯憑證」。

變更備份選取項目 在「選取項目」方塊中，按下「編輯」。

將階段新增至備份定義

完成下列步驟：

- 在「備份」方塊中，按下「新增階段」。
- 按下「複製」以新增複製階段。
- 在「複製」方塊中，按下「編輯」。
- 在「儲存」窗格中，選取私人雲端重複資料刪除磁碟儲存裝置作為複製作業的儲存。
- 依需要完成任何其他設定。
賽門鐵克建議您將複製作業當成個別工作進行驗證。如果您選取在工作結束時驗證作業，工作效能便會降低。您可以在「驗證」窗格上架構驗證作業。

附註：您可以將其他複製階段新增至備份定義。例如，您可以將其他複本傳送到遠端受管 Backup Exec 伺服器上已共置的磁帶裝置或重複資料刪除儲存裝置。

修改工作設定

完成下列步驟：

- 在「備份」方塊中，按下「編輯」。
- 在「儲存」窗格中，選取本機重複資料刪除磁碟儲存裝置作為備份工作的儲存。
- 依需要完成任何其他設定。

6 完成架構備份定義時，按下「備份內容」對話方塊中的「確定」。

請參閱第 31 頁的「[關於使用離站複本組態的 Backup Exec 私人雲端服務](#)」。

關於使用離站複本組態從私人雲端還原資料

您將資料備份至私人雲端 Backup Exec 實例之後，可以隨時還原該資料。從私人雲端 Backup Exec 重複資料刪除磁碟儲存裝置還原資料的程序，與一般在 Backup Exec 中還原資料的程序十分相似。

請參閱第 34 頁的「[使用離站複本組態從私人雲端還原資料](#)」。

使用實體傳輸磁碟機從 Backup Exec 私人雲端實例還原大量資料的效率會比較高。您可以使用傳輸磁碟機將資料傳輸到本機 Backup Exec 伺服器。然後使用本機 Backup Exec 伺服器執行還原工作。

請參閱第 34 頁的「[使用離站複本組態，從私人雲端透過傳輸磁碟機還原資料](#)」。

使用離站複本組態從私人雲端還原資料

您可以從私人雲端 Backup Exec 實例將資料還原至本機 Backup Exec 用戶端電腦。請參閱第 33 頁的「[關於使用離站複本組態從私人雲端還原資料](#)」。

使用離站複本組態從私人雲端還原資料

- 1 確認您還原的伺服器包含能讓伺服器與電腦 1 (C1) 進行通訊的網路路由指令，如下列程序所述：
請參閱第 48 頁的「[設定區域網路路由](#)」。
 - 2 在中央管理伺服器上開啟 Backup Exec。
 - 3 在「備份與還原」標籤處，按下「還原」。
 - 4 選取您要還原的資料以及其他任何必要的工作選項，然後提交工作。
- 請參閱第 31 頁的「[關於使用離站複本組態的 Backup Exec 私人雲端服務](#)」。

使用離站複本組態，從私人雲端透過傳輸磁碟機還原資料

您可以使用傳輸磁碟機，從私人雲端 Backup Exec 實例將資料複製到本機 Backup Exec 伺服器。如果您想要一次還原大量資料，則傳輸磁碟機可能會相當實用。依據可用的頻寬數量和完成工作的時間長度而定，大型還原工作可能會影響系統資源。

請參閱第 33 頁的「[關於使用離站複本組態從私人雲端還原資料](#)」。

使用傳輸磁碟機和離站複本組態從私人雲端還原資料

- 1 在電腦 1 (C1) (私人雲端 Backup Exec 實例) 的可攜式磁碟機上建立磁碟儲存。
- 2 複製要從雲端式重複資料刪除磁碟儲存裝置還原的備份集。選取要建立成目的儲存裝置的磁碟儲存。
請確定您選取使用軟體加密將資料加密。您必須建立或選取軟體加密的加密金鑰。
如需加密資料的相關資訊，請參閱「Symantec Backup Exec 管理指南」。
- 3 工作完成之後，將傳輸磁碟機送至當地辦公室。
- 4 收到可攜式磁碟機之後，將磁碟機連接至本機 Backup Exec 伺服器。
- 5 將可攜式磁碟機當成路徑使用，在電腦 2 (C2) 上建立磁碟儲存。
- 6 在磁碟儲存上建立並執行 Backup Exec 盤點和目錄作業。
- 7 將新磁碟儲存的資料還原到適當目的地。
- 8 清除傳輸磁碟機的資料。

請參閱第 31 頁的「[關於使用離站複本組態的 Backup Exec 私人雲端服務](#)」。

在中央管理伺服器發生故障時從受管 Backup Exec 伺服器還原資料

如果硬體故障或其他災難影響了您的中央管理伺服器，它可以讓您的受管 Backup Exec 伺服器執行備份或還原工作。您可以透過架構取代電腦，並重新安裝 Backup Exec 中央管理伺服器，復原中央管理伺服器。不過，您也可以將受管 Backup Exec 伺服器轉換為獨立式 Backup Exec 伺服器以還原中央管理伺服器。

將受管 Backup Exec 伺服器轉換為獨立式 Backup Exec 伺服器以還原中央管理伺服器

- 1 在受管 Backup Exec 伺服器上，記下任何本機磁碟儲存的名稱和目錄路徑。

附註：在「儲存」標籤上連按兩下該磁碟儲存。然後按下左窗格中的「內容」，以檢視儲存內容。

- 2 如果受管 Backup Exec 伺服器有其自己的重複資料刪除磁碟儲存裝置，請記下該裝置的名稱、路徑、登入帳戶及密碼內容。

附註：在「儲存」標籤上連按兩下該重複資料刪除磁碟儲存裝置。然後按下左窗格中的「內容」，以檢視儲存內容。

- 3 從 Windows「控制台」開啟「程式和功能」(或「新增或移除程式」)對話方塊或「移除安裝程式」對話方塊。
- 4 選取 Symantec Backup Exec 的「變更」選項。
- 5 在左窗格中，選取「其他選項」(如果尚未選取)。
- 6 按「下一步」，直到進入「架構受管 Backup Exec 伺服器」面板為止。
- 7 選取「本機管理 Backup Exec 伺服器」選項。
- 8 按「下一步」。
- 9 當您收到「無法聯絡 {中央管理伺服器}。請確定中央管理伺服器正在執行」訊息時，請執行下列其中一項作業。

如果中央管理伺服器無法使用，而您希望 按下「確定」以繼續。
本機管理此受管 Backup Exec 伺服器

如果您要在中央管理伺服器正在執行時重 按下「取消」以結束程序。
試此作業

安裝完成後，該電腦將不再是集中管理 Backup Exec 伺服器。

- 10 按「下一步」。
- 11 出現提示時，重新啟動電腦。

- 12 開啟 Backup Exec，然後選取「儲存」標籤。

如果 Backup Exec 無法連線至 Backup Exec 伺服器，請重新啟動 Backup Exec 服務，然後再試一次。

- 13 使用您在步驟 1 中記下的相同名稱和路徑匯入原始磁碟儲存，重新建立任何本機磁碟儲存。
- 14 使用您在步驟 2 中記下的相同資訊匯入原始重複資料刪除磁碟儲存裝置，重新建立任何重複資料刪除磁碟儲存裝置。

附註：重新建立現有的儲存裝置可能比建立新的儲存裝置需要更長的時間。該時間長度視儲存裝置所包含的備份集數量，以及此受管 Backup Exec 伺服器對於其網域控制器和 DNS 是否具有存取權而定。

- 15 在您重新建立的每個儲存裝置上，建立並執行 Backup Exec 盤點和目錄作業。
現在您便可以使用獨立式 Backup Exec 伺服器來還原任何儲存在 Backup Exec 伺服器的儲存裝置上的備份集。
- 16 如果您使用獨立式 Backup Exec 伺服器來復原中央管理伺服器，則可能需要刪除獨立式 Backup Exec 伺服器上的現有中央管理伺服器資源。然後在還原中央管理伺服器之前，先將 Agent for Windows 推送安裝至該伺服器。

復原中央管理伺服器後，您可以再次使用 Backup Exec 變更安裝對話方塊，將本機管理 Backup Exec 伺服器轉換回集中管理 Backup Exec 伺服器。選取「集中管理 Backup Exec 伺服器」選項，以將電腦重新架構為受管 Backup Exec 伺服器。

關於使用 Backup Exec 私人雲端服務和直接備份組態

Backup Exec 私人雲端服務可讓您利用直接備份組態的用戶端重複資料刪除功能來管理備份定義。

您可以選擇在執行工作時，手動開始和停止私人雲端 Backup Exec 實例和 VPN 連結連線。或者選擇連接 VPN 連結並且讓實例永久執行。您還可以選擇透過將 OpenVPN 服務排程為在備份工作時段附近開始和停止的方式，自動化此程序。您可以使用「Windows 排程任務」公用程式為服務建立排程。

賽門鐵克提供了一個有用的計算機工具，可讓您估計透過網際網路複製資料所需的時間。雲端備份時間計算機也能幫助您規劃雲端備份策略。您可以使用計算機判斷系統資源是否適合在指定的備份時段內備份客戶的資料。時間估計可幫助您決定可合理支援的資料量，以及應分配給雲端備份的時間長度。

計算機位於下列連結：

<http://entsupport.symantec.com/umi/V-269-34>

請參閱第 37 頁的「[啟用直接備份組態的用戶端重複資料刪除](#)」。

請參閱第 37 頁的「[建立直接備份組態的備份定義](#)」。

請參閱第 38 頁的「[使用直接備份組態從私人雲端透過傳輸磁碟機還原資料](#)」。

啟用直接備份組態的用戶端重複資料刪除

您必須先啟用戶端重複資料刪除，才能在私人雲端 Backup Exec 實例中，建立和執行直接備份工作。

附註：如果您使用多租用戶組態，請勿啟用中央管理伺服器重複資料刪除磁碟儲存裝置的用戶端重複資料刪除。

啟用直接備份組態的用戶端重複資料刪除

- 1 在「儲存」標籤上，連按兩下您要編輯其內容的儲存。
- 2 在左窗格中，按下「內容」。
- 3 在「用戶端重複資料刪除」欄位中，選取「已啟用」。
- 4 按下「套用」。
- 5 重新啟動 Backup Exec 服務。

附註：您必須在 C1 上停止 Backup Exec 服務，然後再重新啟動該服務。

啟用戶端重複資料刪除之後，您就可以建立和執行直接備份工作。

如需建立使用用戶端重複資料刪除之備份工作的詳細資訊，請參閱「Symantec Backup Exec 管理指南」。

請參閱第 37 頁的「[建立直接備份組態的備份定義](#)」。

請參閱第 36 頁的「[關於使用 Backup Exec 私人雲端服務和直接備份組態](#)」。

建立直接備份組態的備份定義

針對遠端代理程式共用和用戶端重複資料刪除架構 VPN 並啟用其他任何電腦之後，就可以建立和執行直接備份工作。

請參閱第 37 頁的「[啟用直接備份組態的用戶端重複資料刪除](#)」。

附註：如需建立備份定義的相關資訊，請參閱「Symantec Backup Exec 管理指南」。

使用下列程序將資料直接備份到私人雲端 Backup Exec 實例。

建立直接備份組態的備份工作

- 1 在電腦 1 (C1) 上，開啟 Backup Exec。
- 2 在「備份與還原」標籤上，執行下列其中一項作業：
 - 若要備份單一伺服器，請以滑鼠右鍵按下伺服器名稱。
 - 若要備份多部伺服器，請按 Shift 或 Ctrl 同時按下伺服器名稱，然後以滑鼠右鍵按下其中一個選取的伺服器。
- 3 在「備份」功能表上，選取要使用的備份選項。
- 4 在「名稱」欄位中，輸入備份定義的唯一名稱。

附註：如果從多部伺服器備份資料，Backup Exec 會將伺服器名稱附加到您「名稱」欄位中輸入的文字。Backup Exec 會使用伺服器名稱和您輸入的文字，為每個備份定義建立唯一名稱。

- 5 執行下列任一項：

測試或編輯 Backup Exec 用來存取備份選取項目的憑證	在「選取項目」方塊中，按下「測試/編輯憑證」。
變更備份選取項目	在「選取項目」方塊中，按下「編輯」。
將階段新增至備份定義	在「備份」方塊中，按下「新增階段」。
修改工作設定	完成下列步驟： <ul style="list-style-type: none">■ 在「備份」方塊中，按下「編輯」。■ 請確定選取「如果支援，可讓遠端電腦直接存取儲存裝置並執行用戶端重複資料刪除」選項。■ 依需要完成任何其他設定。

- 6 完成架構備份定義時，按下「備份內容」對話方塊中的「確定」。
請參閱第 36 頁的「關於使用 Backup Exec 私人雲端服務和直接備份組態」。

使用直接備份組態從私人雲端透過傳輸磁碟機還原資料

您可以建立一般的還原工作，將資料從私人雲端 Backup Exec 實例還原到本機用戶端。不過，如果您要一次還原大量的資料，使用實體傳輸磁碟機可能才有意義。傳輸大量資料所需的時間，取決於可用頻寬的數量以及完成工作的時間。

使用直接備份組態從私人雲端透過傳輸磁碟機還原資料

- 1 在電腦 1 (C1) 上建立和執行還原工作，以便將檔案還原到可攜式磁碟機上的資料夾。
- 2 工作完成之後，請使用任何協力廠商加密工具，將磁碟上的檔案加密。
- 3 將可攜式磁碟機送至當地辦公室。
- 4 收到可攜式磁碟機時，使用原本用來加密檔案的相同工具來為檔案解密。
- 5 將解密的檔案傳輸到電腦 2 (C2) 上的正確目的地。
- 6 從傳輸磁碟機完全消除或清除檔案，以確保已永久移除資料。

請參閱第 36 頁的「關於使用 Backup Exec 私人雲端服務和直接備份組態」。

關於雲端災難復原服務

Backup Exec 2012 Simplified Disaster Recovery (SDR) 功能和轉換成虛擬機器功能可讓服務提供者或客戶提供雲端災難復原服務。發生災難時，儲存在雲端中的備份資料可以用來在私人雲端中建立暫存取代虛擬或實體伺服器。

特定網路組態和故障狀況都可能影響進行容錯移轉和故障回復所需的特定步驟。本節僅提供在 Backup Exec 私人雲端環境內，使用 SDR 和轉換成虛擬機器功能提供災難復原服務的基本準則。

可能發生的主要災難復原情形有兩種。第一種情形是伺服器容錯移轉和故障回復，在這種情形中，一或多個內部部署伺服器失敗，但是現場網路則完好無損。第二種情形是網站容錯移轉和故障回復，在這種情形中，整個網站已失敗。

請參閱第 39 頁的「從容錯移轉復原伺服器或網站」。

請參閱第 41 頁的「從故障回復復原伺服器或網站」。

從容錯移轉復原伺服器或網站

若要為伺服器容錯移轉情形做準備，您應針對所有重要的商業伺服器，架構並執行規律排程之啟用 Simplified Disaster Recovery (SDR) 的備份定義。這些備份定義必須包含將備份資料複製到私人雲端重複資料刪除磁碟儲存裝置的複製階段。發生伺服器容錯移轉時，您可以使用私人雲端 Backup Exec 伺服器來復原取代虛擬或實體伺服器。

請參閱第 39 頁的「關於雲端災難復原服務」。

若要復原取代實體伺服器，請使用 Simplified Disaster Recovery 光碟來執行裸機還原。使用私人雲端重複資料刪除磁碟儲存裝置上最新的啟用 SDR 的備份。您可以將取代伺服器傳輸至內部部署網站，以取代失敗的伺服器。網站容錯移轉需要以位於雲端的 Hypervisor 環境中的虛擬機器來取代整個重要的商業伺服器群組。

如需 Simplified Disaster Recovery 的詳細資訊，請參閱「Symantec Backup Exec 管理指南」。

附註：特定網路組態和故障狀況都可能影響進行故障回復所需的特定步驟。下列程序僅提供使用 Backup Exec 私人雲端環境提供災難復原服務的基本準則。

從容錯移轉復原伺服器或網站

- 1 在雲端位置中建立 Hyper-V 或 VMWare ESX Hypervisor 環境。
- 2 為將在 Hypervisor 上執行的取代虛擬機器建立受防護的虛擬網路。若為整個網站的容錯移轉情形，取代伺服器應保留其原始的內部部署 IP 位址。

附註：復原網站時，取代伺服器應保留其原始的內部部署 IP 位址。您應依邏輯順序還原取代電腦。例如，您應先還原任何網域控制器和 DNS 伺服器。

- 3 執行下列其中一項動作：

從實體電腦進行容錯移轉

完成下列步驟：

- 建立並執行轉換成虛擬機器。針對所有取代電腦，將 SDR 時間點系統磁碟區和系統狀態資料轉換成虛擬機器。這些虛擬機器應以 Hypervisor 為目標。請勿在此時選取任何應用程式資源。
- 為取代虛擬機器架構任何固定 IP 位址 (如有必要)。
- 在取代虛擬機器和私人雲端 Backup Exec 伺服器之間建立網路連線。
- 針對每個取代的伺服器，從相同的啟用 SDR 的時間點備份建立並執行還原工作。選取該時間點可用的所有電腦資源。將還原資料重新導向至取代伺服器。

從虛擬機器進行容錯移轉

從每個取代伺服器的最新 SDR 時間點備份建立並執行重新導向的還原工作。應為內部部署和雲端伺服器使用相同類型的 Hypervisor。

- 4 若只要復原單一伺服器，請在取代虛擬機器和內部部署網路之間建立 VPN 連線，並為取代虛擬機器的 IP 位址架構任何內部部署 DNS 項目。

- 5 如果失敗的伺服器之前透過外部 IP 位址顯示 (例如 Exchange 郵件伺服器)，請顯示任何新的來自雲端網路的外部位址，並變更任何外部 DNS 記錄。
- 6 為取代虛擬機器架構並執行規律排程的 Hypervisor 主機備份定義。使用私人雲端重複資料刪除磁碟儲存裝置作為備份目的地。

如果內部部署 Backup Exec 伺服器具有本機重複資料刪除磁碟儲存，則備份定義必須包含將備份複製到內部部署重複資料刪除磁碟儲存裝置的複製階段。

從故障回復復原伺服器或網站

您可以在發生故障回復時復原伺服器或網站。網站故障回復情形需要將整個重要的商業伺服器群組還原為內部部署實體伺服器或虛擬機器。

請參閱第 39 頁的「關於雲端災難復原服務」。

您可以逐步復原內部部署伺服器，而無須一次將它們全部復原。您一開始可以先復原部分伺服器，然後經過幾天或幾週的時間後再復原其他伺服器。此策略可能需要變更其餘連線至內部部署網路的取代雲端伺服器的 VPN 連線和 IP 位址。

如需 Simplified Disaster Recovery 的詳細資訊，請參閱「Symantec Backup Exec 管理指南」。

附註：特定網路組態和故障狀況都可能影響進行故障回復所需的特定步驟。下列程序僅提供使用 Backup Exec 私人雲端環境提供災難復原服務的基本準則。

從故障回復復原伺服器或網站

- 1 執行啟用 Simplified Disaster Recovery (SDR) 的備份，並包含所有複製階段。
- 2 關閉取代虛擬機器。
- 3 如果啟用 SDR 的備份定義不包含將備份集傳送至內部部署重複資料刪除磁碟儲存的複製階段，請完成下列步驟：
 - 將可攜式磁碟儲存裝置新增至私人雲端 Backup Exec 伺服器上的 Backup Exec。
 - 從所有取代電腦之資料的最後時間點備份複製備份集。使用可攜式磁碟儲存裝置作為目的地。
 - 將可攜式磁碟儲存裝置送至內部部署位置。
 - 將可攜式磁碟儲存裝置新增至內部部署 Backup Exec 伺服器上的 Backup Exec。
 - 盤點內部部署 Backup Exec 伺服器上的磁碟儲存裝置並建立目錄。
- 4 執行下列其中一項：

故障回復至內部部署實體伺服器

完成下列步驟：

- 使用 Simplified Disaster Recovery 光碟以執行裸機還原。選取內部部署 Backup Exec 伺服器上最新的啟用 SDR 的備份。
- 為復原的電腦架構固定 IP 位址 (如有必要)。
- 為復原的電腦或復原電腦的 IP 位址架構任何內部部署 DNS 項目 (如有必要)。

故障回復至內部部署虛擬伺服器

完成下列步驟：

- 從取代伺服器的最新時間點備份建立並執行重新導向的還原工作。應為內部部署和雲端伺服器使用相同類型的 Hypervisor。
- 為復原的虛擬機器架構固定 IP 位址 (如有必要)。
- 為復原的虛擬機器或虛擬機器的 IP 位址架構任何內部部署 DNS 項目 (如有必要)。

- 5 如果失敗的伺服器之前透過外部 IP 位址顯示 (例如 Exchange 郵件伺服器)，請還原外部 DNS 記錄中的原始位址。
- 6 刪除取代雲端伺服器的備份定義。
- 7 繼續執行任何還原的內部部署電腦的原始備份定義。

Backup Exec 重複資料刪除磁碟儲存裝置需求

Backup Exec 重複資料刪除磁碟儲存裝置需求適用於所有的私人雲端組態。如果達到特定雲端 Backup Exec 伺服器上的共用限制，您必須新增其他雲端 Backup Exec 伺服器。

如需重複資料刪除磁碟儲存裝置需求的相關資訊，請參閱「Symantec Backup Exec 管理指南」。

WAN 延遲的限制

如果您的網路延遲問題嚴重，對於初始直接雲端備份工作的效能便會有不利的影響。延遲問題也會影響在當地辦公室和私人雲端 Backup Exec 伺服器之間傳輸資料的某些複製備份工作。雖然您總是以播散裝置的方式提升效能，如果使用傳輸磁碟播散重複資料刪除磁碟儲存裝置，您可能會遇到效能問題。在初始備份工作期

問，Backup Exec 會識別並快取有關資料區段的資訊，其可為後續工作提供更有有效的效能。

附註：高延遲值可視為超過 30 毫秒的平均來回時間延遲。延遲越嚴重，Backup Exec 效能受影響的程度越高。

當來源裝置和目標裝置都是重複資料刪除磁碟儲存裝置時，此限制便不適用於複製備份工作。

以下為在高延遲環境使用 Backup Exec 私人雲端服務的限制：

- 將重複資料刪除磁碟儲存裝置和私人雲端重複資料刪除磁碟儲存裝置以外的來源裝置當作目的地使用的複製備份工作，可能會遇到效能問題。將重複資料刪除磁碟儲存裝置當作本機來源儲存裝置使用，可避免發生這些效能問題。
- 您可能會發現，直接備份到雲端組態的方式並不適用於備份大量資料。
- 如果刪除並重新建立相同資源的備份定義，Backup Exec 必須重新快取資料指紋。因此，您可能會遇到和初始直接雲端備份工作一樣的效能問題。

精細回復技術與離站複本的限制

以下是搭配離站複本組態使用 Backup Exec 之精細回復技術 (GRT) 選項的限制：

- 將本機 Exchange 啟用 GRT 的增量備份集備份至私人雲端重複資料刪除磁碟儲存裝置，便會以 MTF 磁帶格式建立備份資料。您可以還原這些備份集的詳細資料，但需要在還原工作期間在雲端 Backup Exec 伺服器上將備份集分段。對於設定到雲端重複資料刪除磁碟儲存裝置之啟用 GRT 的備份集的直接備份，則沒有這個限制。
- 不建議將啟用 GRT 的重複備份集，從本機磁帶裝置直接複製到雲端重複資料刪除磁碟儲存裝置，這樣做可能會導致工作執行時間過多。
- 直接將啟用 GRT 的備份集備份至雲端 Backup Exec 伺服器，可能會導致高延遲環境中的效能降低情況加重。在初始備份之後，可能會遇到效能降低的情況。如果效能問題持續存在，您可能需要停用 GRT 以進行直接備份。

Windows Small Business Server (SBS) 的限制和多租用者 Backup Exec 伺服器組態

多租用者 Backup Exec 伺服器組態需要所有本機受管 Backup Exec 伺服器都是私人雲端網域的成員。因此，您不可以將客戶的 SBS 伺服器架構為受管 Backup Exec 伺服器 (如果其屬於客戶網域的一部分)。受管 Backup Exec 伺服器必須安裝為個別的伺服器。

架構 OpenVPN

本章包含以下主題：

- [關於架構 OpenVPN](#)
- [網路問題疑難排解](#)

關於架構 OpenVPN

OpenVPN SSL VPN 開放原始碼套件會在私人雲端 Backup Exec 實例與本機 Backup Exec 伺服器之間提供安全且經過加密的連線。您必須在私人雲端 Backup Exec 伺服器實例與在區域網路上執行的任何電腦之間架構 SSL VPN。

Backup Exec 私人雲端服務組態對於此單一用戶端 OpenVPN 範例具有以下網路限制：

- 區域網路必須包含在單一子網路內。
- 本機網域控制器和 DNS 必須位於同一部伺服器上。

請參閱第 45 頁的「[架構 OpenVPN](#)」。

Backup Exec 私人雲端服務的基本 OpenVPN 組態指示是使用單一用戶端。如果您的用戶端全部包含在相同的子網路上，則這些指示可用於支援一或多部本機用戶端電腦。提供給私人雲端實例的所有資料都是透過單一 OpenVPN 用戶端進行路由。若是更複雜的網路或要使用憑證型的身份驗證，您可以使用選用的 OpenVPN 多用戶端組態。

請參閱第 51 頁的「[關於為多個用戶端設定 OpenVPN](#)」。

架構 OpenVPN

OpenVPN SSL VPN 開放原始碼套件會在私人雲端 Backup Exec 實例與本機 Backup Exec 伺服器之間提供安全且經過加密的連線。您必須在私人雲端 Backup Exec 伺服器實例與在區域網路上執行的任何電腦之間架構 SSL VPN。

請參閱第 45 頁的「關於架構 OpenVPN」。

表 4-1 如何架構 OpenVPN

步驟	說明
步驟 1	在私人雲端 Backup Exec 實例上架構 OpenVPN。 請參閱第 46 頁的「在私人雲端 Backup Exec 實例上設定 OpenVPN」。
步驟 2	在電腦 2 上架構 OpenVPN。 請參閱第 47 頁的「在電腦 2 上設定 OpenVPN」。
步驟 3	架構區域網路路由。 請參閱第 48 頁的「設定區域網路路由」。
步驟 4	架構防火牆 (如有需要)。 請參閱第 49 頁的「關於設定防火牆」。
步驟 5	驗證 OpenVPN 連線。 請參閱第 49 頁的「驗證 OpenVPN 連線」。

在私人雲端 Backup Exec 實例上設定 OpenVPN

為確保安全且經過加密的連線，您必須在私人雲端 Backup Exec 實例上架構 OpenVPN。

請參閱第 45 頁的「關於架構 OpenVPN」。

在私人雲端 Backup Exec 實例上架構 OpenVPN

- 1 從下列連結下載 OpenVPN 2.1.4，並將它安裝在電腦 1 (C1) 上的預設位置：
<http://swupdate.openvpn.net/community/releases/openvpn-2.1.4-install.exe>
- 2 在 C1 上，透過選取以下各項，在 OpenVPN 組態資料夾中開啟「Windows 檔案總管」視窗：
「開始」>「所有程式」> OpenVPN > Shortcuts > OpenVPN Configuration File Directory
- 3 透過在 \Program Files (x86)\OpenVPN\bin 資料夾中從指令提示執行下列指令，以產生 OpenVPN 靜態金鑰：

```
c:\Program Files (x86)\Open VPN\bin\openvpn --genkey --secret static.key
```

- 4 在您在 C1 上開啟的資料夾中建立伺服器組態檔，並且將該檔案儲存為 `server.ovpn`：

`server.ovpn` 檔的外觀如下列範例所示：

```
dev tun

ifconfig 10.8.0.1 10.8.0.2

secret static.key

keepalive 10 120
```

附註：如果區域網路上已使用子網路 10.8.x.x，請在 `ifconfig` 指令中使用不同的子網路範圍。

附註：OpenVPN 預設使用 UDP 通訊埠 1194。如有需要，您可以指定另一個埠號，只要將 `Port` 指令加入至 OpenVPN 伺服器 and 用戶端組態檔即可。

- 5 使用 Windows Services 公用程式，將「OpenVPN Service 的啟動類型」內容變更為「自動」。
- 6 在 C1 上開啟指令提示，輸入下列指令，並且取代區域 DNS (電腦 3) 的子網路位址和 DNS 子網路遮罩：

附註：不包括角括號。

```
route add -p <DNS subnet> mask <DNS subnet mask> 10.8.0.2
```

在電腦 2 上設定 OpenVPN

為確保安全且經過加密的連線，您在電腦 1 (C1) 上架構 OpenVPN 之後，必須在電腦 2 (C2) 上架構 OpenVPN。

請參閱第 45 頁的「關於架構 OpenVPN」。

在電腦 2 上架構 OpenVPN

- 1 從下列連結下載 OpenVPN 2.1.4，並將它安裝在 C2 上的預設位置：

<http://swupdate.openvpn.net/community/releases/openvpn-2.1.4-install.exe>

- 2 複製下列程序的步驟 2 中所產生的靜態金鑰：

[在私人雲端 Backup Exec 實例上設定 OpenVPN](#)

- 3 將金鑰貼在 C2 上的下列位置：
 \Program Files (x86)\OpenVPN\config
- 4 在 C2 上的下列位置建立用戶端組態檔，並且將該檔案儲存為 `client.ovpn`：
 \Program Files (x86)\OpenVPN\config
 `client.ovpn` 檔的外觀如下列範例所示：

```
dev tun  
  
remote <電腦 1 的靜態 IP 位址>  
  
ifconfig 10.8.0.2 10.8.0.1  
  
keepalive 10 120  
  
secret static.key
```
- 5 在 **remote** 陳述式中輸入私人雲端 Backup Exec 電腦的靜態 IP 位址。

附註：不包括角括號。

- 6 如果區域網路上已使用子網路 10.8.x.x，請編輯檔案以便在 **ifconfig** 陳述式中使用不同的子網路範圍。
- 7 使用 Windows Services 公用程式，將「OpenVPN Service 的啟動類型」內容變更為「自動」。

設定區域網路路由

若要架構區域網路路由，您必須同時在 TAP-Win32 Adapter V9 和實體網路介面上啟用 IP 轉送。

請參閱第 45 頁的「[關於架構 OpenVPN](#)」。

架構區域網路路由

- 1 在電腦 2 (C2) 上，啟動登錄編輯器並找出下列金鑰：
 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
- 2 設定下列登錄值：
 值名稱：**IPEnableRouter**
 值類型：**REG_DWORD**
 值資料：**1**

附註：值為 1 時，會啟用電腦上所安裝及使用的所有網路連線的 TCP/IP 轉送。

- 3 重新啟動 C2。
- 4 在電腦 3 (C3) 上的指令視窗中輸入下列指令，並且取代 C2 的本機 IP 位址：

附註：輸入 IP 位址時，不包括角括號。

```
Route add -p 10.8.0.0 mask 255.255.255.0 <電腦 2 的本機 IP 位址>
```

附註：您必須在每一部需要與雲端中的 OpenVPN 伺服器電腦進行通訊的區域網路電腦上執行這個指令。另外還必須在執行 Backup Exec 代理程式，而且會作為從私人雲端 Backup Exec 伺服器進行之還原工作目標的任何伺服器上執行此指令。

關於設定防火牆

您應該依照表中詳述的方式架構網路防火牆，以確保本機服务器和雲端服务器之間的通訊正常。

表 4-2 關於設定防火牆

防火牆實例	動作
電腦 1 (C1)	您應該針對 OpenVPN 網路配接卡停用 Windows 防火牆。 您應該將 Windows 防火牆架構為允許 OpenVPN 架構使用之任何通訊埠上的入埠流量。根據預設，OpenVPN 會使用通訊埠 1194 UDP。
電腦 2 (C2)	您應該針對 OpenVPN TAP 網路配接卡停用本機 Windows 防火牆。
區域網路	如果您使用外部本機或企業防火牆，則應該將防火牆架構為允許 OpenVPN 架構使用之任何通訊埠上的離埠流量。根據預設，OpenVPN 會使用通訊埠 1194 UDP。

請參閱第 45 頁的「關於架構 OpenVPN」。

驗證 OpenVPN 連線

設定 OpenVPN 完成時，應進行測試以確認 OpenVPN 服务器和用戶端能夠成功連線。

請參閱第 45 頁的「[關於架構 OpenVPN](#)」。

驗證 OpenVPN 連線

- 1 使用 Windows Services 公用程式，同時在電腦 1 (C1) 和電腦 2 (C2) 上啟動 OpenVPN 服務。
- 2 開啟位於 C1 和 C2 上下列目錄中的 OpenVPN 日誌檔：
C:\Program Files (x86)\OpenVPN\log
- 3 確認「Initialization Sequence Completed」(初始化序列已完成) 字樣出現在這兩個檔案中。
- 4 在 C1 上，架構 TAP-Win32 網路配接卡指向本機網域的 DNS 伺服器，作為其慣用的 DNS 伺服器。

請參閱第 50 頁的「[設定 TAP-Win32 網路配接器](#)」。

您可以在執行工作時，手動開始和停止私人雲端 Backup Exec 實例 VPN 連結連線。或是保持 VPN 連結連線，並讓該實例永久執行。您可以將 OpenVPN 服務排定為隨已排程的備份工作開始和停止，藉以自動化此程序。您也可以使用「Windows 排程任務」公用程式為服務建立排程。

設定 TAP-Win32 網路配接器

若要驗證 OpenVPN 連線，您必須架構 TAP-Win32 網路配接卡指向本機網域的 DNS 伺服器，作為其慣用的 DNS 伺服器。

請參閱第 49 頁的「[驗證 OpenVPN 連線](#)」。

架構 TAP-Win32 網路配接器

- 1 開啟「TAP 網路介面卡內容」。
- 2 按下「IPv4 內容」。
- 3 按下「進階」。
- 4 在「DNS」標籤上，輸入區域網路 DNS 伺服器的 IP 位址。
- 5 在「尾碼」欄位中，加入網域 FQDN 尾碼，然後將其移到尾碼清單的頂端。
- 6 按下「確定」，結束所有對話方塊。
- 7 在電腦 1 (C1) 上的指令提示中，輸入下列指令：

```
ipconfig /flushdns  
  
ipconfig /registerdns
```

驗證 OpenVPN 連線完成之後，您可以架構 Backup Exec 伺服器。

請參閱第 18 頁的「[設定多租用者或雲端離站複本組態](#)」。

請參閱第 26 頁的「[設定直接備份組態](#)」。

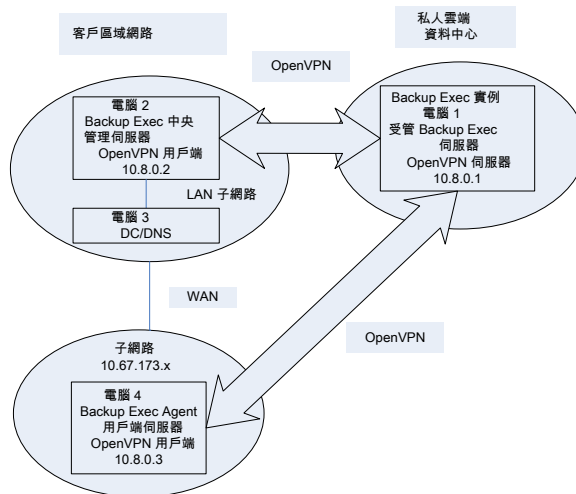
關於為多個用戶端設定 OpenVPN

您可以架構 OpenVPN 來搭配多個用戶端使用。如果您的區域網路很複雜，可能需要使用多個用戶端的 VPN 組態。例如，如果您使用多個本機子網路，可能會從多個用戶端的 VPN 組態獲得益處。

請參閱第 45 頁的「關於架構 OpenVPN」。

警告： OpenVPN 不應該安裝在網域控制器上。Backup Exec 私人雲端服務不支援多重主目錄的網域控制器組態。

圖 4-1 多個用戶端的 VPN 組態



OpenVPN 伺服器是私人雲端實例。用戶端是區域 LAN 上的電腦。使用多個 OpenVPN 用戶端時，需要使用安全性憑證，而非用於單一用戶端組態的共用金鑰文字檔。在多個用戶端的組態中，每個 OpenVPN 用戶端都有自己的金鑰和憑證。

附註： 金鑰檔案相當重要。如果金鑰檔案遭到破壞，您應該重新產生它。如果憑證授權中心 (CA) 金鑰檔案遭到破壞，您應該重新產生以該 CA 為基礎的所有金鑰。

若要為多個用戶端架構 OpenVPN，請使用公開提供的範例完成該程序。下列網站提供設定 OpenVPN 憑證與多個 OpenVPN 用戶端的完整指示：

<http://www.runpcrun.com>

<http://openvpn.net>

更複雜網路的其他選擇是，在區域網路間道路器上使用 OpenVPN。區域網路間道路器提供對點的 OpenVPN 連線。其他本機電腦可以路由至 VPN，而不必新

增其他 OpenVPN 用戶端與電腦網路路由。若需 OpenVPN 支援的更多詳細資訊，請洽詢您的路由器製造商並參閱相關文件。

協力廠商軟體組織也會提供包含 OpenVPN 支援的路由器韌體更新。下列網站會提供範例：

<http://www.dd-wrt.com>

一旦您為多個用戶端架構 OpenVPN 之後，就可以建立和執行直接備份工作以備份用戶端的資料。您可以使用私人雲端實例作為直接備份工作或複製備份作業的備份目的地。

網路問題疑難排解

如果 Backup Exec 私人雲端服務有網路問題，您應該驗證 OpenVPN 伺服器 and 用戶端是否可以成功連線。

網路問題疑難排解

- 1 針對 Backup Exec 私人雲端服務組態中的所有電腦，暫時關閉 Windows 防火牆，或新增適當的 ICMP 防火牆例外狀況。
- 2 同時在電腦 1 (C1) 和電腦 2 (C2) 上使用 Windows Services 公用程式，啟動 OpenVPN 服務。
- 3 同時在 C1 和 C2 上，開啟下列目錄中的 OpenVPN 日誌檔，然後確認每個檔案都包含「Initialization Sequence Completed」(初始化序列已完成)的字樣：
C:\Program Files (X86)\OpenVPN\log
- 4 從 C1、C2 和電腦 3 (C3) Ping 10.8.0.1 與 10.8.0.2 來測試連線。
- 5 從 C1 Ping C2 的本機 IP 位址和 C3 的本機 IP 位址。

OpenVPN 連線時，請確認 OpenVPN 區域網路配接卡 DNS 內容包含本機網域尾碼。