管理 Cloud Volumes ONTAP

Cloud Manager 3.8

NetApp
March 25, 2024

目錄

管理 Cloud Volumes ONTAP

瞭解

深入瞭解 Cloud Volumes ONTAP

利用 NetApp 技術、您可以最佳化雲端儲存成本與效能、同時強化資料保護、安全性與法規遵循。 Cloud Volumes ONTAP

不只是軟體的儲存應用裝置、可在雲端上執行功能完善的資料管理軟體。 Cloud Volumes ONTAP ONTAP它提供企業級儲存設備、具備下列主要功能：

- 儲存效率

  運用內建的重複資料刪除技術、資料壓縮、精簡配置及複製技術、將儲存成本降至最低。

- 高可用度

  確保雲端環境發生故障時、企業的可靠性和持續營運。

- 資料保護

  利用 NetApp 領先業界的複寫技術 SnapMirror 、將內部部署資料複寫到雲端、讓次要複本可輕鬆用於多種使用案例。 Cloud Volumes ONTAP

  此外、還整合了支援資料的功能、可提供備份與還原功能、以保護雲端資料、並可長期歸檔。 Cloud Volumes ONTAP Cloud Backup Service

- 資料分層

  在高效能與低效能儲存資源池之間隨需切換、而不需將應用程式離線。

- 應用程式一致性

  使用 NetApp SnapCenter 功能確保 NetApp Snapshot 複本的一致性。

- 資料安全

  支援資料加密、並提供防範病毒和勒索軟體的功能。 Cloud Volumes ONTAP

- 隱私權法規遵循控管

  與 Cloud Compliance 整合可協助您瞭解資料內容並識別敏感資料。

不含適用於功能的授權 ONTAP 。 Cloud Volumes ONTAP

"檢視支援 Cloud Volumes ONTAP 的支援的支援功能"

"深入瞭 Cloud Volumes ONTAP 解功能"

儲存設備

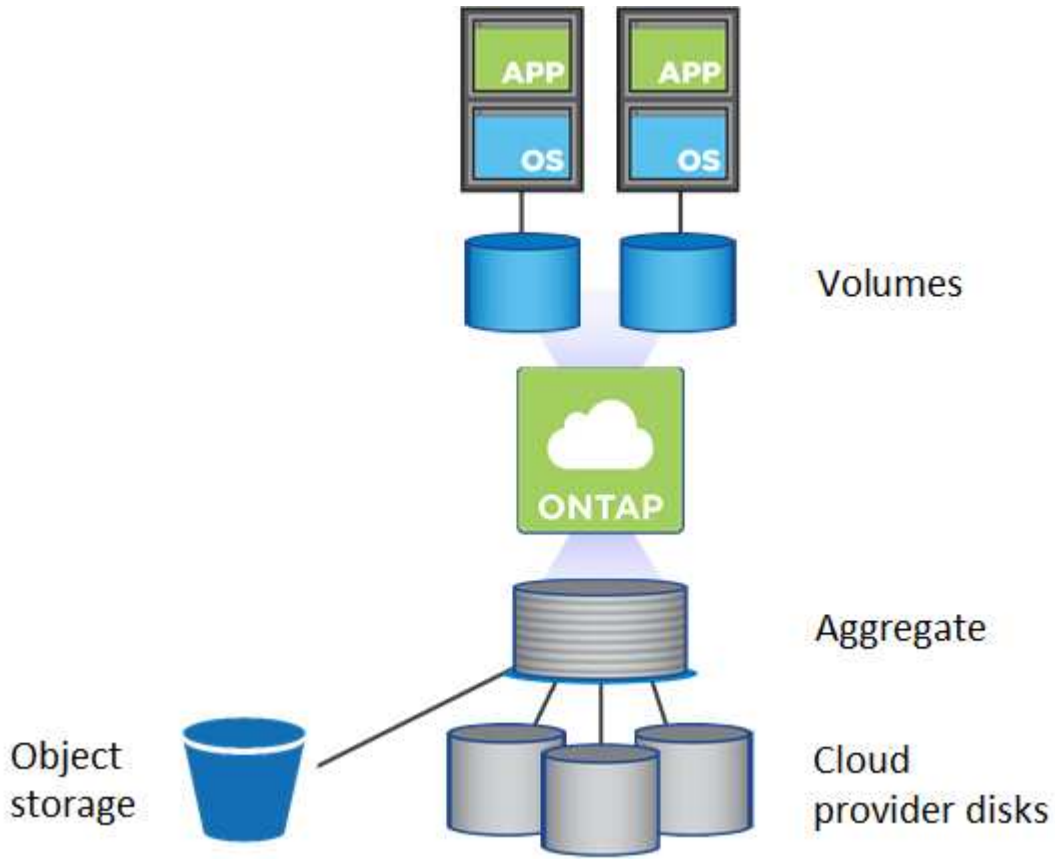
磁碟與集合體

瞭解 Cloud Volumes ONTAP 如何使用雲端儲存設備、有助於瞭解儲存成本。

所有磁碟和集合體都必須直接從 Cloud Manager 建立和刪除。您不應從其他管理工具執行這些動作。這樣做可能會影響系統穩定性、阻礙未來新增磁碟的能力、並可能產生備援雲端供應商費用。

總覽

利用雲端供應商儲存設備做為磁碟、並將其分成一或多個集合體。 Cloud Volumes ONTAPAggregate 可為一或多個磁碟區提供儲存設備。



支援多種類型的雲端磁碟。您可以在建立磁碟區時選擇磁碟類型、並在部署 Cloud Volumes ONTAP 時選擇預設磁碟大小。

向雲端供應商購買的儲存設備總容量為 *rawcapity* 。_ 可用容量 _ 較低、因為大約 12% 至 14% 的成本是保留供 Cloud Volumes ONTAP 作供參考之用的成本。例如、如果 Cloud Manager 建立 500 GB Aggregate 、可用容量為 442.94 GB 。

AWS 儲存設備

在 AWS 中 Cloud Volumes ONTAP 、某些 EC2 執行個體類型使用 EBS 儲存設備來儲存使用者資料、並將本機 NVMe 儲存設備當作 Flash Cache 。

EBS 儲存設備

在 AWS 中、 Aggregate 最多可包含 6 個大小相同的磁碟。磁碟大小上限為 16 TB 。

基礎 EBS 磁碟類型可以是通用 SSD 、已配置的 IOPS SSD 、處理量最佳化 HDD 或冷 HDD 。您可以將 EBS 磁碟與 Amazon S3 配對至 "將非作用中資料分層至低成本物件儲存設備"。

EBS 磁碟類型的差異較高、如下所示：

- _ 通用 SSD/disks 可在各種工作負載的成本與效能之間取得平衡。效能是以 IOPS 定義。
- 配置的 IOPS SS__ 磁碟適用於需要最高效能且成本較高的關鍵應用程式。
- _ 處理量最佳化 HDD_ 磁碟適用於經常存取的工作負載、需要以較低的價格提供快速且一致的處理量。
- *Cold HDD* 磁碟是用於備份、或是不常存取的資料、因為效能非常低。如同處理量最佳化的 HDD 磁碟、效能是以處理量來定義。

> ⓘ HA 組態和資料分層不支援冷 HDD 磁碟。

本機 NVMe 儲存設備

部分 EC2 執行個體類型包括 Cloud Volumes ONTAP 本機 NVMe 儲存設備、這些儲存設備可作為參考用途 "Flash 快取"。

- 相關連結 *
- "AWS 文件： EBS Volume 類型"
- "瞭解如何在 AWS 中為系統選擇磁碟類型和磁碟大小"
- "檢閱 Cloud Volumes ONTAP AWS 的儲存限制"
- "檢閱 Cloud Volumes ONTAP AWS 支援的支援組態"

Azure 儲存設備

在 Azure 中、 Aggregate 最多可包含 12 個大小相同的磁碟。磁碟類型和最大磁碟大小取決於您使用的是單一節點系統或 HA 配對：

單一節點系統

單一節點系統可使用三種 Azure 託管磁碟：

- _Premium SSD 託管磁碟 _ 以更高的成本、為 I/O 密集的工作負載提供高效能。
- _ 標準 SSD 託管磁碟 _ 為需要低 IOPS 的工作負載提供一致的效能。
- 如果您不需要高 IOPS 、而且想要降低成本、那麼 _ 標準 HDD 託管磁碟 _ 是個不錯的選擇。

  每種託管磁碟類型的磁碟大小上限為 32 TB 。

  您可以將託管磁碟與 Azure Blob 儲存設備配對至 "將非作用中資料分層至低成本物件儲存設備"。

HA 配對

HA 配對使用 Premium 分頁區、磁碟大小上限為 8 TB 。

- 相關連結 *
- "Microsoft Azure 文件： Microsoft Azure Storage 簡介"
- "瞭解如何在 Azure 中為您的系統選擇磁碟類型和磁碟大小"
- "檢閱 Cloud Volumes ONTAP Azure 的儲存限制"

GCP 儲存設備

在 GCP 中、 Aggregate 最多可包含 6 個大小相同的磁碟。磁碟大小上限為 16 TB 。

磁碟類型可以是 _ 分區 SSD 持續磁碟 _ 或 _ 分區標準持續磁碟 _ 。您可以將持續的磁碟與 Google 儲存庫配對至 "將非作用中資料分層至低成本物件儲存設備"。

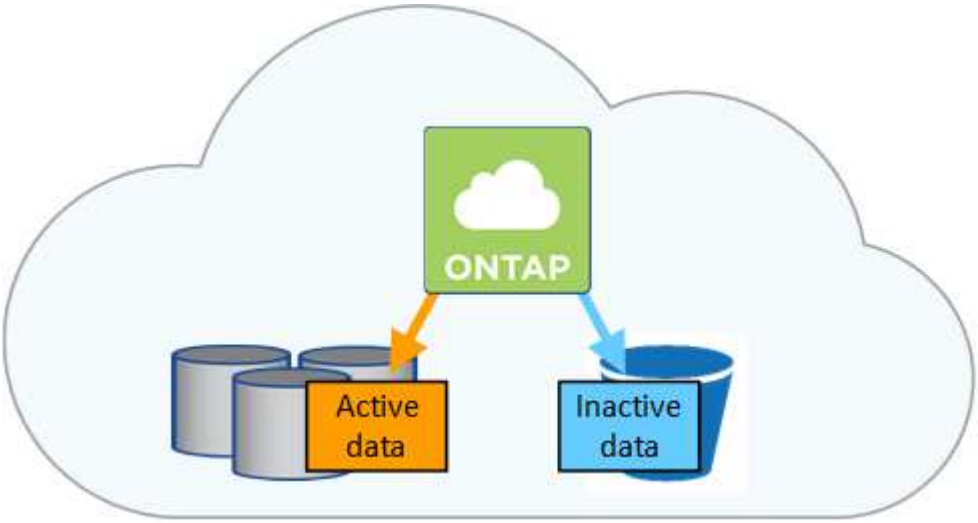
- 相關連結 *
- "Google Cloud Platform 文件：儲存選項"
- "檢閱 Cloud Volumes ONTAP GCP 中的儲存限制"

RAID 類型

每 Cloud Volumes ONTAP 個支援的 RAID 類型都是 RAID0 （分段）。不支援其他 RAID 類型。以雲端供應商為基礎、提供磁碟可用度與持久性。 Cloud Volumes ONTAP

資料分層總覽

將非作用中資料自動分層至低成本的物件儲存設備、藉此降低儲存成本。作用中資料仍保留在高效能 SSD 或 HDD 中、而非作用中資料則分層至低成本物件儲存設備。如此一來、您就能回收主儲存設備上的空間、並縮減二線儲存設備。



支援 AWS 、 Azure 和 Google Cloud Platform 中的資料分層。 Cloud Volumes ONTAP資料分層是 FabricPool 以不同步技術為後盾。

您不需要安裝功能授權、就能啟用資料分層 FabricPool （例如、）。

AWS 中的資料分層

當您在 AWS 中啟用資料分層功能時、 Cloud Volumes ONTAP VMware 會使用 EBS 做為熱資料的效能層、而 AWS S3 則是非作用中資料的容量層。

效能層級

效能層可以是通用 SSD 、已配置的 IOPS SSD 或最佳化處理量的 HDD 。

容量層

利用 *Standard* 儲存類別、將非作用中資料分層至單一 S3 儲存區。 Cloud Volumes ONTAPStandard 適用於儲存在多個可用度區域中的常用資料。

Cloud Manager 會針對每個工作環境建立單一 S3 儲存區、並將其命名為「網路資源池」、「叢集唯一識別碼」。並不會針對每個 Volume 建立不同的 S3 儲存區。

儲存類別

AWS 中階層式資料的預設儲存類別為 *Standard* 。如果您不打算存取非作用中資料、可以將儲存類別變更為下列其中一項、藉此降低儲存成本： _Intelligent Tiering _ 、 _One Zone In頻率 存取 _ 或 _Standard-in頻繁存取 _ 。當您變更儲存類別時、非作用中的資料會從 Standard 儲存類別開始、並轉換至您選取的儲存類別（如果 30 天後仍未存取資料）。

如果您確實存取資料、存取成本就會較高、因此在變更儲存類別之前、請先將此納入考量。 "深入瞭解 Amazon S3 儲存類別"。

您可以在建立工作環境時選取儲存類別、之後隨時變更。如需變更儲存類別的詳細資訊、請參閱 "將非作用中資料分層至低成本物件儲存設備"。

資料分層的儲存類別是全系統範圍、並非每個磁碟區。

Azure 中的資料分層

當您在 Azure 中啟用資料分層功能時、 Cloud Volumes ONTAP VMware 會使用 Azure 託管磁碟做為熱資料的效能層、而 Azure Blob 儲存設備則是非作用中資料的容量層。

效能層級

效能層可以是 SSD 或 HDD 。

容量層

利用 Azure *hot* 儲存層、 Cloud Volumes ONTAP 將非作用中資料分層至單一 Blob 容器。熱層是經常存取資料的理想選擇。

Cloud Manager 會為 Cloud Volumes ONTAP 每個運作環境建立一個新的儲存帳戶、其中包含一個容器。儲存帳戶名稱為隨機。並不會針對每個 Volume 建立不同的容器。

儲存存取層

Azure 中階層式資料的預設儲存存取層為 *hot* 層。如果您不打算存取非作用中資料、可以改用 _cool 儲存層來降低儲存成本。當您變更儲存層時、非作用中的資料會從熱儲存層開始、並在 30 天後無法存取資料時、移轉至冷卻儲存層。

如果您確實存取資料、存取成本就會較高、因此在變更儲存層之前、請先將此納入考量。 "深入瞭解 Azure

Blob 儲存設備存取層"。

您可以在建立工作環境時選取儲存層、之後隨時變更。如需變更儲存層的詳細資訊、請參閱 "將非作用中資料分層至低成本物件儲存設備"。

資料分層的儲存存取層是全系統的、並非每個磁碟區。

GCP 中的資料分層

當您在 GCP 中啟用資料分層功能時 Cloud Volumes ONTAP 、 VMware 會使用持續性磁碟做為熱資料的效能層、並使用 Google Cloud Storage 儲存庫做為非作用中資料的容量層。

效能層級

效能層可以是 SSD 或 HDD （標準磁碟）。

容量層

利用 _Regional 儲存類別、將非作用中資料分層至單一 Google Cloud Storage 儲存庫。 Cloud Volumes ONTAP

Cloud Manager 會為每個工作環境建立單一儲存區、並將其命名為「網路資源池」、「叢集唯一識別碼」。並不會針對每個 Volume 建立不同的儲存區。

儲存類別

階層式資料的預設儲存類別為 *Standard Storage* 類別。如果資料不常存取、您可以改用 *Nearline Storage* 或 *Coldline Storage* 來降低儲存成本。當您變更儲存類別時、非作用中的資料會從 Standard Storage 類別開始、並轉換至您選取的儲存類別、如果資料在 30 天後仍未存取。

如果您確實存取資料、存取成本就會較高、因此在變更儲存類別之前、請先將此納入考量。 "深入瞭解 Google Cloud Storage 的儲存課程"。

您可以在建立工作環境時選取儲存層、之後隨時變更。如需變更儲存類別的詳細資訊、請參閱 "將非作用中資料分層至低成本物件儲存設備"。

資料分層的儲存類別是全系統範圍、並非每個磁碟區。

資料分層和容量限制

如果您啟用資料分層、系統的容量限制會維持不變。此限制分佈於效能層和容量層。

Volume 分層原則

若要啟用資料分層、您必須在建立、修改或複寫磁碟區時、選取磁碟區分層原則。您可以為每個 Volume 選取不同的原則。

有些分層原則具有相關的最低冷卻週期、可設定磁碟區中的使用者資料必須保持非作用中狀態的時間、以便將資料視為「冷」並移至容量層。

Cloud Manager 可讓您在建立或修改 Volume 時、從下列磁碟區分層原則中進行選擇：

僅適用於 **Snapshot**

當 Aggregate 達到 50% 容量後、 Cloud Volumes ONTAP 將不會與作用中檔案系統相關聯的 Snapshot 複本

的 Cold 使用者資料分層至容量層。冷卻期約為 2 天。

如果讀取、容量層上的冷資料區塊會變熱、並移至效能層。

全部

所有資料（不含中繼資料）會立即標示為冷資料、並儘快分層至物件儲存設備。無需等待 48 小時、磁碟區中的新區塊就會變冷。請注意、在設定 All 原則之前、位於磁碟區中的區塊需要 48 小時才能變冷。

如果讀取、雲端層上的 Cold 資料區塊會保持冷卻狀態、不會寫入效能層。本政策從 ONTAP 推出時起即為供應。

自動

當 Aggregate 容量達到 50% 後、 Cloud Volumes ONTAP 將 Volume 中的 Cold 資料區塊分層至容量層。Cold 資料不僅包括 Snapshot 複本、也包括來自作用中檔案系統的冷使用者資料。冷卻期約 31 天。

支援此原則、從 Cloud Volumes ONTAP 支援的功能為 2 。 9.4 。

如果以隨機讀取方式讀取、容量層中的冷資料區塊就會變熱、並移至效能層。如果以連續讀取方式讀取（例如與索引和防毒掃描相關的讀取）、則冷資料區塊會保持冷卻狀態、而不會移至效能層級。

無

將磁碟區的資料保留在效能層中、避免移至容量層。

複寫磁碟區時、您可以選擇是否要將資料分層至物件儲存設備。如果您這麼做、 Cloud Manager 會將 * 備份 * 原則套用至資料保護磁碟區。從 Sich9.6 開始 Cloud Volumes ONTAP 、 * All （全部）的分層原則將取代備份原則。

關閉 **Cloud Volumes ONTAP** 此功能會影響冷卻期間

資料區塊是透過冷卻掃描來冷卻。在此過程中、尚未使用的區塊溫度會移至下一個較低的值（冷卻）。預設的冷卻時間取決於磁碟區分層原則：

- 自動： 31 天
- 僅 Snapshot ： 2 天

冷卻掃描必須執行、才能正常運作。 Cloud Volumes ONTAP如果關閉了這個功能、冷卻也會停止。 Cloud Volumes ONTAP因此、您可能會經歷更長的冷卻時間。

設定資料分層

如需相關指示及支援組態清單、請參閱 "將非作用中資料分層至低成本物件儲存設備"。

儲存管理

Cloud Manager 提供 Cloud Volumes ONTAP 簡化且進階的功能、可管理各種不同步儲存設備。

所有磁碟和集合體都必須直接從 Cloud Manager 建立和刪除。您不應從其他管理工具執行這些動作。這樣做可能會影響系統穩定性、阻礙未來新增磁碟的能力、並可能產生備援雲端供應商費用。

儲存資源配置

Cloud Manager Cloud Volumes ONTAP 可為您購買磁碟並管理 Aggregate 、讓您輕鬆配置資料以利執行效能。您只需建立磁碟區即可。如果需要、您可以使用進階分配選項自行配置集合體。

簡化資源配置

Aggregate 可為磁碟區提供雲端儲存設備。Cloud Manager 會在您啟動執行個體、以及配置其他 Volume 時、為您建立 Aggregate 。

建立 Volume 時、 Cloud Manager 會執行以下三項功能之一：

- 它會將磁碟區放置在現有的 Aggregate 上、該集合體具有足夠的可用空間。
- 它會為現有的 Aggregate 購買更多磁碟、將磁碟區放在現有的 Aggregate 上。
- 它會為新的 Aggregate 購買磁碟、並將該磁碟區放在該 Aggregate 上。

Cloud Manager 會根據以下幾項因素來決定新磁碟區的放置位置： Aggregate 的最大大小、是否啟用精簡配置、以及 Aggregate 的可用空間臨界值。

帳戶管理員可從 * 設定 * 頁面修改可用空間臨界值。

AWS 中集合體的磁碟大小選擇

Cloud Manager 在 Cloud Volumes ONTAP AWS 中建立新的 Aggregate 、隨著系統中的 Aggregate 數量增加、它會逐漸增加集合體中的磁碟大小。Cloud Manager 能確保您在系統達到 AWS 允許的資料磁碟數量上限之前、能夠充分利用系統的最大容量。

例如、 Cloud Manager 可能會針對 Cloud Volumes ONTAP 下列大小的磁碟來選擇適用於下列的磁碟大小、以用於在某個供應端點或 BYOL 系統中的集合體：

Aggregate 編號	磁碟大小	最大 **Aggregate** 容量
1.	500 MB	3 TB
4.	1 TB	6 TB
6.	2 TB	12 TB

您可以使用進階配置選項自行選擇磁碟大小。

進階分配

您可以自行管理 Aggregate 、而非讓 Cloud Manager 管理 Aggregate 。 "從 * 進階分配 * 頁面"、您可以建立新的集合體、包括特定數量的磁碟、新增磁碟至現有的集合體、以及在特定的集合體中建立磁碟區。

容量管理

客戶管理員可以選擇 Cloud Manager 是否通知您儲存容量決策、或 Cloud Manager 是否自動為您管理容量需求。這可能有助於您瞭解這些模式的運作方式。

自動容量管理

容量管理模式預設為自動。在此模式中、 Cloud Manager 會在 Cloud Volumes ONTAP 需要更多容量時自動購買新的磁碟以供執行個體使用、刪除未使用的磁碟集合（集合體）、視需要在集合體之間移動磁碟區、以及嘗試取消故障磁碟。

下列範例說明此模式的運作方式：

- 如果有 5 個或更少 EBS 磁碟的集合體達到容量臨界值、 Cloud Manager 會自動為該集合體購買新的磁碟、讓磁碟區能夠持續成長。
- 如果具有 12 個 Azure 磁碟的 Aggregate 達到容量臨界值、 Cloud Manager 會自動將該 Aggregate 中的磁碟區移至具有可用容量的 Aggregate 、或移至新的 Aggregate 。

  如果 Cloud Manager 為磁碟區建立新的 Aggregate 、則會選擇適合該磁碟區大小的磁碟大小。

  請注意、可用空間現在可在原始 Aggregate 上使用。現有磁碟區或新磁碟區可以使用該空間。在此案例中、空間無法歸還給 AWS 、 Azure 或 GCP 。

- 如果 Aggregate 不包含超過 12 小時的磁碟區、 Cloud Manager 會將其刪除。

利用自動容量管理來管理 **LUN**

Cloud Manager 的自動容量管理不適用於 LUN 。Cloud Manager 建立 LUN 時、會停用自動擴充功能。

利用自動容量管理來管理 **inode**

Cloud Manager 會監控磁碟區上的 inode 使用量。當 85% 的 inode 被使用時、 Cloud Manager 會增加磁碟區的大小、以增加可用的 inode 數量。磁碟區可以包含的檔案數量取決於它擁有的 inode 數量。

手動容量管理

如果帳戶管理員將容量管理模式設為手動、 Cloud Manager 會在必須做出容量決策時、顯示必要行動訊息。自動模式中所述的相同範例適用於手動模式、但您必須接受這些動作。

Flash 快取

AWS 和 Azure 中的 Cloud Volumes ONTAP 某些支援功能組態包括本機 NVMe 儲存設備、 Cloud Volumes ONTAP 這些儲存設備可做為 _Flash Cache 來提供更好的效能。

什麼是**Flash Cache**？

Flash Cache 可透過即時智慧快取來加速資料存取、快取最近讀取的使用者資料和 NetApp 中繼資料。它適用於隨機讀取密集的工作負載、包括資料庫、電子郵件和檔案服務。

AWS 支援的執行個體

選擇下列 EC2 執行個體類型之一、搭配新的 Cloud Volumes ONTAP 或現有的精選版或 BYOL 系統：

- c5d.4xlarge
- c5d.9xlarge
- c5d.18xlarge

- m5d.8xlarge
- m5d.12xlarge
- r5d.2xlarge

Azure 中支援的 VM 類型

在 Cloud Volumes ONTAP Azure 中選擇採用單節點的 Standard_L8s_v2 VM 類型。

限制

- 所有磁碟區都必須停用壓縮、才能充分發揮 Flash Cache 效能的改善效益。

  從 Cloud Manager 建立磁碟區時、請選擇「無儲存效率」、或先建立磁碟區、然後再選擇「無儲存效率」 "使用 CLI 停用資料壓縮"。

- 重新開機後的快取重新溫熱功能不支援 Cloud Volumes ONTAP 使用此功能。

WORM 儲存設備

您可以在 Cloud Volumes ONTAP 一個還原系統上啟動一次寫入、多次讀取（ WORM ）儲存、以未修改的形式保留檔案、保留指定的保留期間。WORM 儲存設備採用 SnapLock 企業模式的支援技術、這表示 WORM 檔案在檔案層級受到保護。

一旦檔案已提交至 WORM 儲存設備、即使保留期間已過、也無法修改。防竄改時鐘可決定 WORM 檔案的保留期間何時結束。

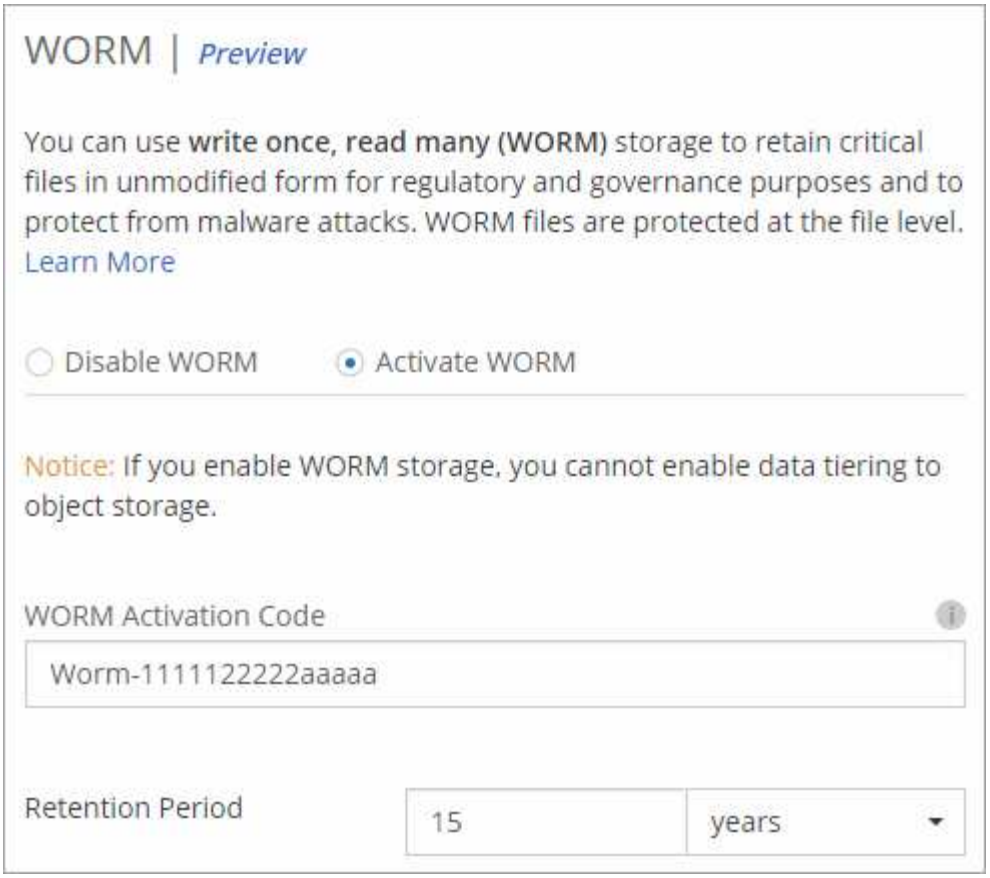
保留期間結束後、您必須負責刪除不再需要的任何檔案。

啟動 WORM 儲存設備

您可以在 Cloud Volumes ONTAP 建立新的工作環境時、在一個可靠的系統上啟動 WORM 儲存設備。這包括指定啟動代碼、以及設定檔案的預設保留期間。您可以使用 Cloud Manager 介面右下角的聊天圖示來取得啟動代碼。

您無法在個別磁碟區上啟動 WORM 儲存設備、 WORM 必須在系統層級啟動。

下圖顯示如何在建立工作環境時啟動 WORM 儲存設備：



將檔案提交至 **WORM**

您可以使用應用程式、透過 NFS 或 CIFS 將檔案提交至 WORM 、或使用 ONTAP CLI 自動將檔案自動提交至 WORM 。您也可以使用 WORM 可應用檔案來保留遞增寫入的資料、例如記錄資訊。

在 Cloud Volumes ONTAP 啟用 WORM 儲存設備之後、您必須使用 ONTAP CLI 來管理 WORM 儲存設備。如需相關指示、請參閱 "本文檔 ONTAP"。

支援 WORM 儲存功能相當於支援功能不只是功能不一的企業模式。 Cloud Volumes ONTAP SnapLock

限制

- 如果您直接從 AWS 或 Azure 刪除或移動磁碟、則可在磁碟區到期日之前刪除該磁碟區。
- 啟動 WORM 儲存設備時、無法啟用資料分層至物件儲存設備的功能。
- 必須停用備份至雲端、才能啟用 WORM 儲存設備。

高可用度配對

AWS 中的高可用度配對

支援高可用度（ HA ）組態、可提供不中斷營運及容錯功能。 Cloud Volumes ONTAP在 AWS 中、資料會在兩個節點之間同步鏡射。

在 AWS 中 Cloud Volumes ONTAP 、不含下列元件：

- 兩 Cloud Volumes ONTAP 個彼此同步鏡射資料的鏡射節點。
- 一種中介執行個體、可在節點之間提供通訊通道、以協助儲存接管和恢復程序。

中介執行個體在 T2.Micro 執行個體上執行 Linux 作業系統、並使用一個 EBS 磁碟、大約 8 GB 。

儲存設備接管與恢復

如果某個節點發生故障、另一個節點可以提供資料給其合作夥伴、以提供持續的資料服務。用戶端可以從合作夥伴節點存取相同的資料、因為資料會同步鏡射至合作夥伴。

節點重新開機後、合作夥伴必須重新同步資料、才能退回儲存設備。重新同步資料所需的時間、取決於節點當機時資料的變更量。

RPO 和 RTO

HA 組態可維持資料的高可用度、如下所示：

- 恢復點目標（ RPO ）為 0 秒。您的資料交易一致、不會遺失任何資料。
- 恢復時間目標（ RTO ）為 60 秒。發生中斷時、資料應可在 60 秒內取得。

HA 部署模式

您可以在多個可用度區域（ AZs ）或單一 AZ 中部署 HA 組態、確保資料的高可用度。您應該檢閱每個組態的詳細資料、以選擇最符合您需求的組態。

多個可用度區域中的可用度Cloud Volumes ONTAP

在多個可用度區域（ AZs ）中部署 HA 組態、可確保當 AZ 或執行 Cloud Volumes ONTAP 此節點的執行個體發生故障時、資料的高可用度。您應該瞭解 NAS IP 位址如何影響資料存取和儲存容錯移轉。

NFS 與 CIFS 資料存取

當 HA 組態分佈於多個可用區域時、 _浮 點 IP 位址 _ 可啟用 NAS 用戶端存取。在發生故障時、浮動 IP 位址必須位於該區域所有 VPC 的 CIDR 區塊之外、可以在節點之間移轉。除非您、否則 VPC 外部的用戶端無法原生存取這些功能 "設定 AWS 傳輸閘道"。

如果您無法設定傳輸閘道、則 VPC 外部的 NAS 用戶端可使用私有 IP 位址。不過、這些 IP 位址是靜態的、無法在節點之間進行容錯移轉。

在跨多個可用區域部署 HA 組態之前、您應該先檢閱浮動 IP 位址和路由表的需求。部署組態時、您必須指定浮動 IP 位址。私有 IP 位址是由 Cloud Manager 自動建立。

如需詳細資訊、請參閱 "AWS 在 Cloud Volumes ONTAP 多個 AZs 中的功能需求"。

iSCSI 資料存取

由於 iSCSI 不使用浮動 IP 位址、因此跨 VPC 資料通訊並非問題。

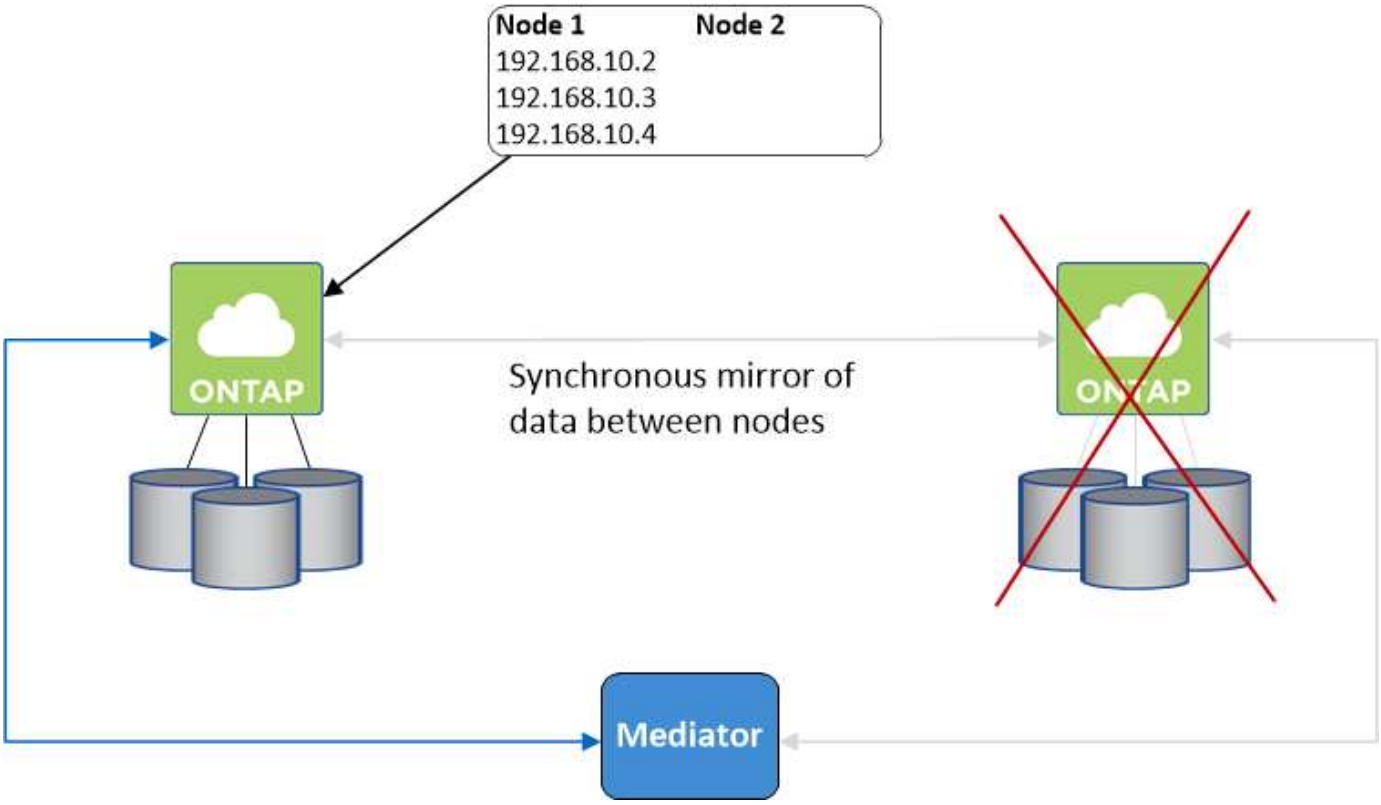
iSCSI的儲存接管與恢復

對於 iSCSI 、 Cloud Volumes ONTAP Reality 使用多重路徑 I/O （ MPIO ）和非對稱邏輯單元存取（ ALUA ）來管理主動最佳化和非最佳化路徑之間的路徑容錯移轉。

如需哪些特定主機組態支援 ALUA 的相關資訊、請參閱 "NetApp 互通性對照表工具" 以及主機作業系統的主機公用程式安裝與設定指南。

NAS的儲存接管與恢復

在使用浮動 IP 的 NAS 組態中進行接管時、用戶端用來存取資料的節點浮動 IP 位址會移至另一個節點。下圖說明使用浮動 IP 的 NAS 組態中的儲存設備接管。如果節點 2 停機、節點 2 的浮動 IP 位址會移至節點 1 。



如果發生故障、用於外部 VPC 存取的 NAS 資料 IP 將無法在節點之間移轉。如果節點離線、您必須使用另一個節點上的 IP 位址、將磁碟區手動重新掛載至 VPC 外部的用戶端。

故障節點恢復上線後、請使用原始 IP 位址將用戶端重新掛載至磁碟區。此步驟是為了避免在兩個 HA 節點之間傳輸不必要的資料、這可能會對效能和穩定性造成重大影響。

您可以從 Cloud Manager 輕鬆識別正確的 IP 位址、方法是選取磁碟區、然後按一下 * Mount Command* 。

在單一可用度區中使用的解決方法 **Cloud Volumes ONTAP**

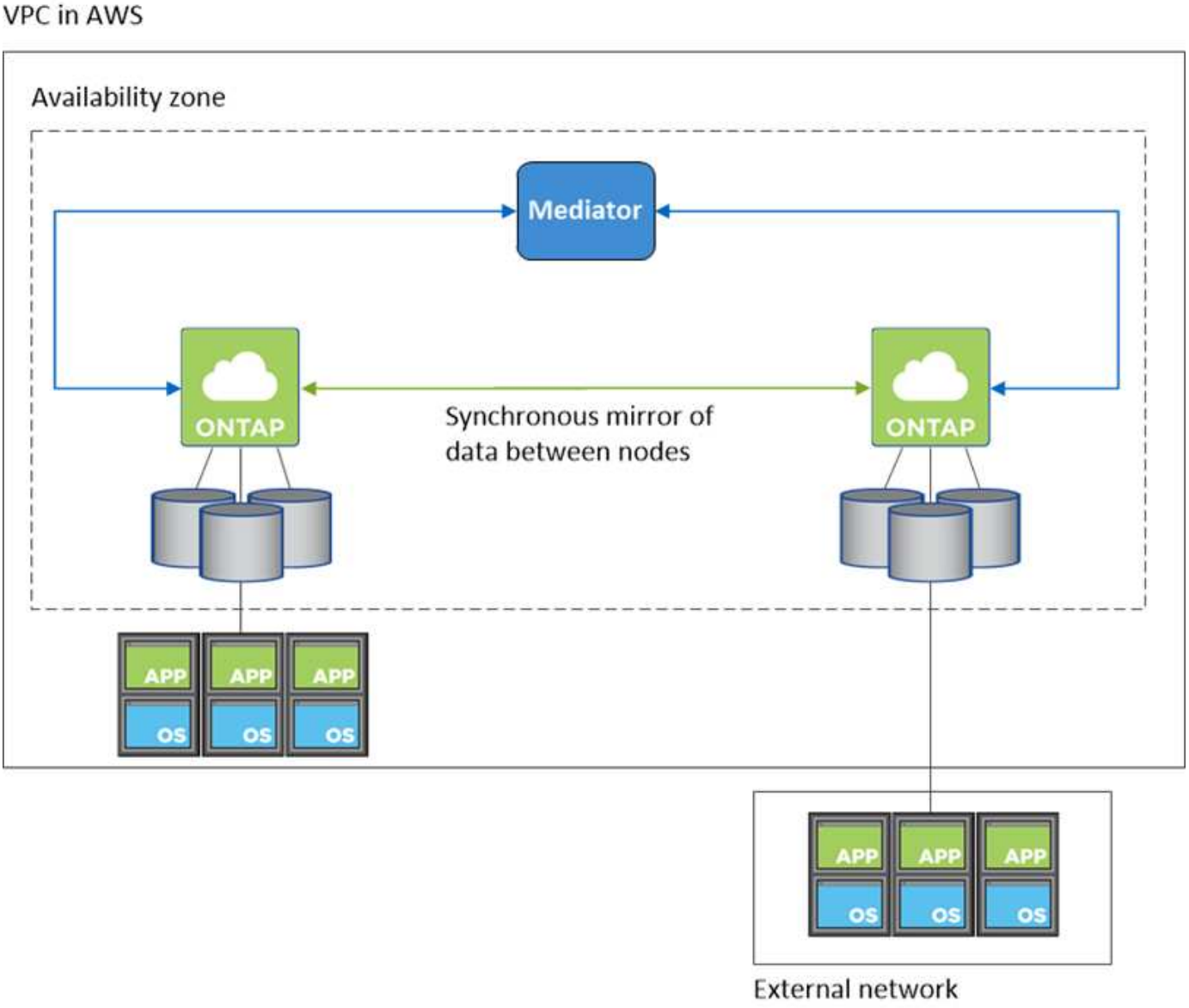
在單一可用度區域（ AZ ）中部署 HA 組態、可確保執行 Cloud Volumes ONTAP 此節點的執行個體故障時、資料的高可用度。所有資料均可從 VPC 外部原生存取。

Cloud Manager 會建立一個 "AWS 分散配置群組" 然後啟動該放置群組中的兩個 HA 節點。放置群組可將執行個體分散到不同的基礎硬體、藉此降低同時發生故障的風險。此功能可從運算角度而非磁碟故障角度改善備援。

資料存取

由於此組態位於單一 AZ 、因此不需要浮動 IP 位址。您可以使用相同的 IP 位址、從 VPC 內部和 VPC 外部存取資料。

下圖顯示單一 AZ 中的 HA 組態。資料可從 VPC 內部及 VPC 外部存取。



儲存設備接管與恢復

對於 iSCSI 、 Cloud Volumes ONTAP Reality 使用多重路徑 I/O （ MPIO ）和非對稱邏輯單元存取（ ALUA ）來管理主動最佳化和非最佳化路徑之間的路徑容錯移轉。

如需哪些特定主機組態支援 ALUA 的相關資訊、請參閱 "NetApp 互通性對照表工具" 以及主機作業系統的主機公用程式安裝與設定指南。

對於 NAS 組態、如果發生故障、資料 IP 位址可以在 HA 節點之間移轉。如此可確保用戶端存取儲存設備。

儲存設備如何在 **HA** 配對中運作

不像 ONTAP 是一個叢集、 Cloud Volumes ONTAP 在節點之間不會共享使用一個不一致的功能。相反地、資料會在節點之間同步鏡射、以便在發生故障時能夠使用資料。

儲存配置

當您建立新的磁碟區並需要額外的磁碟時、 Cloud Manager 會將相同數量的磁碟分配給兩個節點、建立鏡射的 Aggregate 、然後建立新的磁碟區。例如、如果磁碟區需要兩個磁碟、 Cloud Manager 會為每個節點分配兩個磁碟、總共四個磁碟。

儲存組態

您可以使用 HA 配對做為主動 - 主動式組態、讓兩個節點都能將資料提供給用戶端、或做為主動 - 被動式組態、被動節點只有在接管主動節點的儲存設備時、才會回應資料要求。

只有在儲存系統檢視中使用 Cloud Manager 時、才能設定雙主動式組態。

HA 組態的效能期望

使用不同步的功能、可在節點之間複寫資料、進而消耗網路頻寬。 Cloud Volumes ONTAP因此、相較於單一節點 Cloud Volumes ONTAP 的 VMware 、您可以預期下列效能：

- 對於僅從一個節點提供資料的 HA 組態、讀取效能可媲美單一節點組態的讀取效能、而寫入效能則較低。
- 對於同時提供兩個節點資料的 HA 組態、讀取效能高於單一節點組態的讀取效能、寫入效能相同或更高。

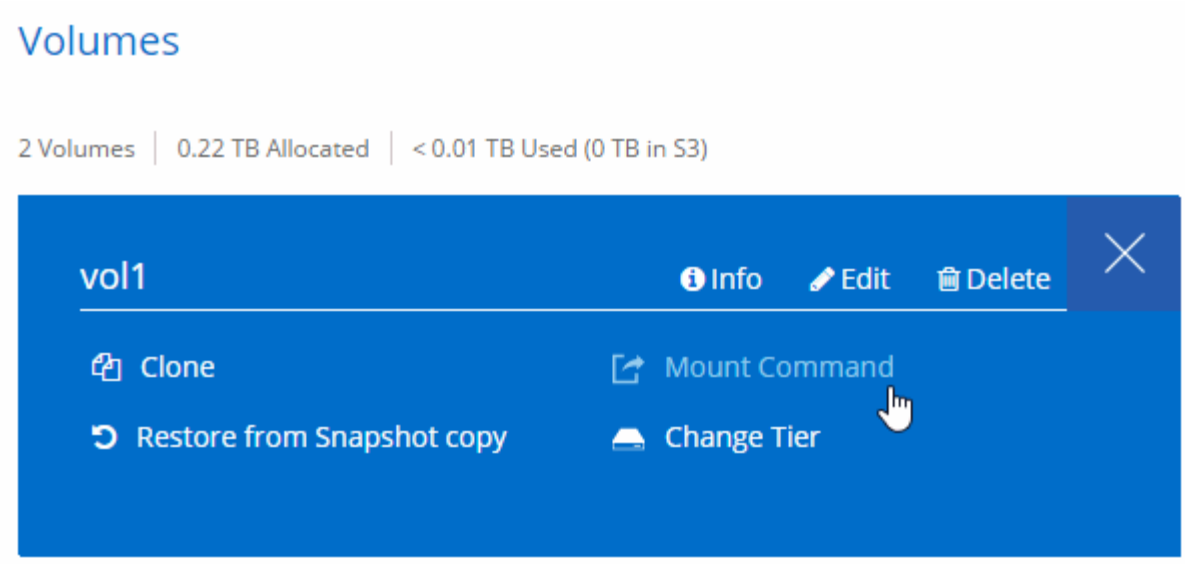
如需 Cloud Volumes ONTAP 更多關於效能的詳細資訊、請參閱 "效能"。

用戶端存取儲存設備

用戶端應使用磁碟區所在節點的資料 IP 位址來存取 NFS 和 CIFS 磁碟區。如果 NAS 用戶端使用合作夥伴節點的 IP 位址來存取磁碟區、則兩個節點之間的流量會降低效能。

如果您在 HA 配對中的節點之間移動磁碟區、則應使用其他節點的 IP 位址來重新掛載磁碟區。否則、您可能會遇到效能降低的情況。如果用戶端支援 NFSv4 轉介或 CIFS 資料夾重新導向、您可以在 Cloud Volumes ONTAP 支撐系統上啟用這些功能、以避免重新掛載磁碟區。如需詳細資料、請參閱 ONTAP 《關於我們的資料》。

您可以從 Cloud Manager 輕鬆識別正確的 IP 位址：

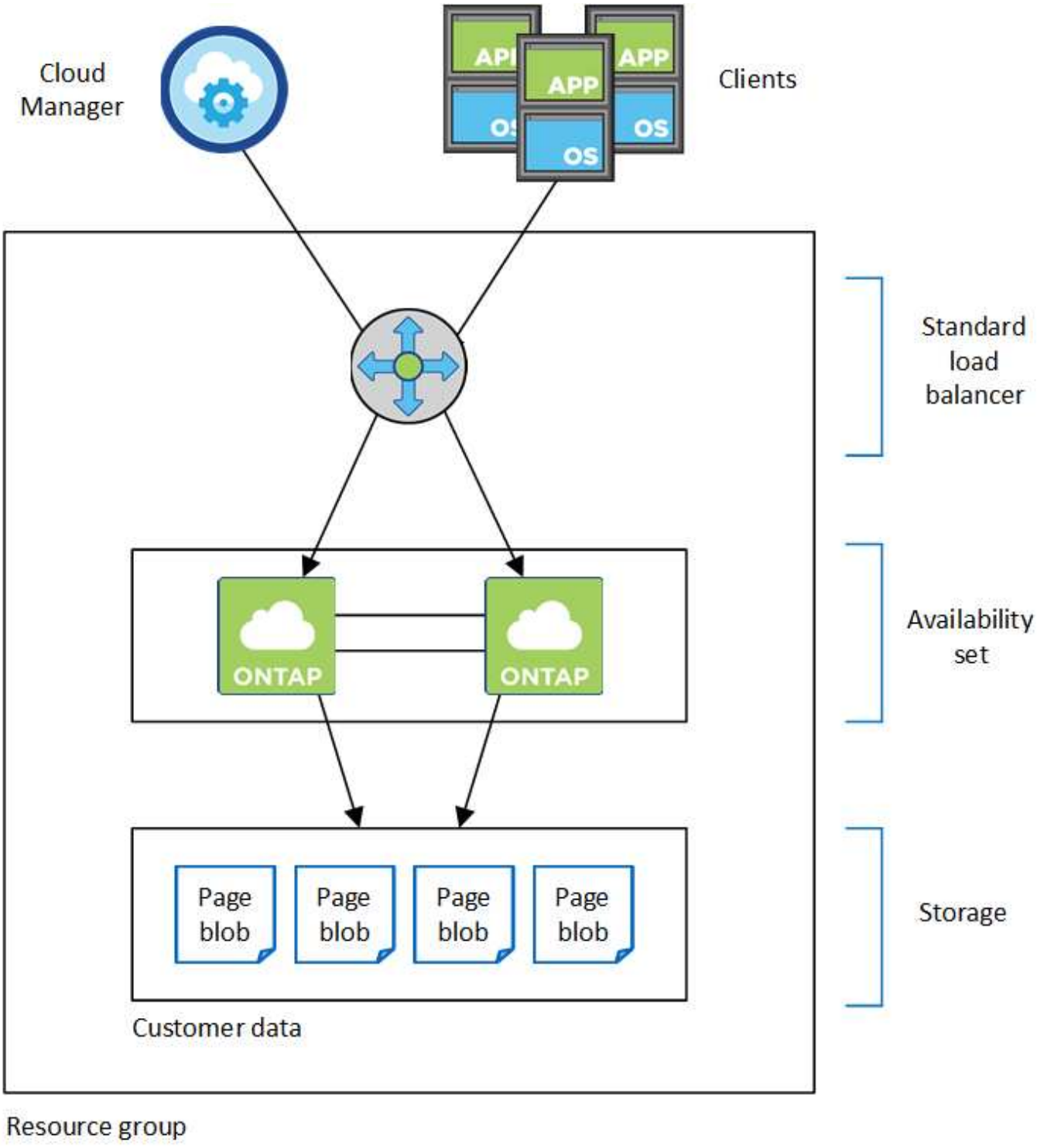


Azure 中的高可用度配對

在雲端環境發生故障時、提供企業級的可靠性和持續運作。 Cloud Volumes ONTAP在 Azure 中、儲存設備會在兩個節點之間共享。

HA 元件

Azure 中的功能介紹 HA 組態包括下列元件： Cloud Volumes ONTAP



請注意 Cloud Manager 為您部署的 Azure 元件：

Azure 標準負載平衡器

負載平衡器負責管理 Cloud Volumes ONTAP 傳入流量至 the ireHA 配對。

可用度設定

可用度集可確保節點位於不同的故障和更新網域中。

磁碟

客戶資料位於 Premium Storage 頁面上。每個節點均可存取其他節點的儲存設備。也需要額外的儲存空間 "開機、 root 和核心資料"。

儲存帳戶

- 託管磁碟需要一個儲存帳戶。
- 由於達到每個儲存帳戶的磁碟容量限制、因此 Premium Storage 頁面區塊需要一個或多個儲存帳戶。

  "Azure 文件： Azure 儲存設備擴充性與儲存帳戶效能目標"。

- 資料分層至 Azure Blob 儲存設備需要一個儲存帳戶。
- 從 NetApp 9.7 開始 Cloud Volumes ONTAP 、 Cloud Manager 為 HA 配對所建立的儲存帳戶就是通用的 v2 儲存帳戶。
- 您可以在 Cloud Volumes ONTAP 建立工作環境時、從一個可疑的 9.7 HA 配對啟用 HTTPS 連線至 Azure 儲存帳戶。請注意、啟用此選項可能會影響寫入效能。您無法在建立工作環境之後變更設定。

RPO 和 RTO

HA 組態可維持資料的高可用度、如下所示：

- 恢復點目標（ RPO ）為 0 秒。您的資料交易一致、不會遺失任何資料。
- 恢復時間目標（ RTO ）為 60 秒。發生中斷時、資料應可在 60 秒內取得。

儲存設備接管與恢復

與實體 ONTAP 的實體叢集類似、 Azure HA 配對中的儲存設備會在節點之間共享。連線至合作夥伴的儲存設備、可讓每個節點在 _ 接管 _ 時存取對方的儲存設備。網路路徑容錯移轉機制可確保用戶端和主機繼續與正常運作的節點通訊。當節點恢復連線時、合作夥伴 _ 會提供 Back_storage 。

對於 NAS 組態、如果發生故障、資料 IP 位址會自動在 HA 節點之間移轉。

對於 iSCSI 、 Cloud Volumes ONTAP Reality 使用多重路徑 I/O （ MPIO ）和非對稱邏輯單元存取（ ALUA ）來管理主動最佳化和非最佳化路徑之間的路徑容錯移轉。

如需哪些特定主機組態支援 ALUA 的相關資訊、請參閱 "NetApp 互通性對照表工具" 以及主機作業系統的主機公用程式安裝與設定指南。

儲存組態

您可以使用 HA 配對做為主動 - 主動式組態、讓兩個節點都能將資料提供給用戶端、或做為主動 - 被動式組態、被動節點只有在接管主動節點的儲存設備時、才會回應資料要求。

HA 限制

下列限制會影響 Cloud Volumes ONTAP Azure 中的功能組合：

- HA 配對支援 Cloud Volumes ONTAP 以支援不含支援功能的標準版、高級版和 BYOL 。不支援 Explore 。
- 不支援 NFSv4 。支援 NFSv3 。

- 某些地區不支援 HA 配對。

  "請參閱支援的 Azure 地區清單"。

"瞭解如何在 Azure 中部署 HA 系統"。

評估

您可以在 Cloud Volumes ONTAP 購買軟體前先評估其功能。最常見的方法是啟動第一個 Cloud Volumes ONTAP 版本的 __LW_YGO 、以獲得 30 天免費試用。試用 BYOL 授權也是一種選擇。

如果您需要概念驗證方面的協助、請聯絡 "銷售團隊" 或是透過聊天選項與您聯絡 "NetApp Cloud Central" 以及 Cloud Manager 。

PAYGO 免費試用 30 天

如果您計畫一 Cloud Volumes ONTAP 次性支付 VMware 的費用、則可免費試用 30 天。您可以 Cloud Volumes ONTAP 在 Cloud Volumes ONTAP 付款人的帳戶中建立第一個的 VMware 系統、從 Cloud Manager 開始 30 天的免費試用版。

舉例來說、並不收取每小時的軟體授權費用、但您的雲端供應商仍需支付基礎架構費用。

免費試用版會在到期時自動轉換為付費的每小時訂閱。如果您在期限內終止執行個體、則您部署的下一個執行個體不屬於免費試用（即使是在 30 天內部署）。

隨用隨付的試用版是透過雲端供應商提供、不得以任何方式延長。

BYOL 的評估授權

如果客戶希望透過 Cloud Volumes ONTAP 向 NetApp 購買稱為「授權」的方式來支付支援費、則可選擇使用 BYOL 試用版。您可以向客戶團隊、銷售工程師或合作夥伴取得評估授權。

評估金鑰適用於 30 天、可多次使用、每次使用 30 天（無論建立日期為何）。

30 天之後、每天都會關機、因此最好事先規劃。您可以在就地升級的評估授權上套用新的 BYOL 授權（這需要重新啟動單一節點系統）。您的託管資料 * 不會 * 在試用期結束時刪除。

使用試用版授權時 Cloud Volumes ONTAP 、您無法升級此軟體。

授權

每 Cloud Volumes ONTAP 個 BYOL 系統都必須安裝有效訂閱的系統授權。Cloud Manager 可為您管理授權、並在授權到期前通知您、藉此簡化程序。BYOL 授權也適用於備份至雲端。

BYOL 系統授權

您可以購買 Cloud Volumes ONTAP 多個適用於某個不含資料的 BYOL 系統授權、以配置超過 368TB 的容量。

例如、您可能會購買兩份授權、以配置多達 736 TB 的容量來 Cloud Volumes ONTAP 供參考。或者、您也可以購買四份授權、最高可達 1.4 PB 。

單一節點系統或 HA 配對可購買的授權數量不受限制。

請注意、磁碟限制可能會讓您無法單獨使用磁碟來達到容量限制。您可以超越磁碟限制 "將非作用中資料分層至物件儲存設備"。如需磁碟限制的相關資訊、請參閱 "《發行說明》中的儲存限制 Cloud Volumes ONTAP"。

新系統的授權管理

當您建立 BYOL 系統時、 Cloud Manager 會提示您輸入授權的序號和 NetApp Support Site 帳戶。Cloud Manager 使用帳戶從 NetApp 下載授權檔案、並將其安裝在 Cloud Volumes ONTAP 整個作業系統上。

"瞭解如何將 NetApp 支援網站帳戶新增至 Cloud Manager"。

如果 Cloud Manager 無法透過安全的網際網路連線存取授權檔案、您可以自行取得檔案、然後手動將檔案上傳至 Cloud Manager 。如需相關指示、請參閱 "管理 BYOL 授權 Cloud Volumes ONTAP 以利執行"。

授權過期警告

Cloud Manager 會在授權到期前 30 天、以及授權到期時再次發出警告。下圖顯示 30 天到期警告：

您可以選取工作環境來檢閱訊息。

如果您未及時續約授權、 Cloud Volumes ONTAP 則無法自行關閉。如果您重新啟動、它會再次自動關機。

> 透過電子郵件、 SNMP traphost 或使用 EMS （事件管理系統）事件通知的 syslog 伺服器、也可以通知您。 Cloud Volumes ONTAP如需相關指示、請參閱 "《 9 EMS 組態快速指南》 ONTAP"。

授權續約

當您透過聯絡 NetApp 代表續約 BYOL 訂閱時、 Cloud Manager 會自動從 NetApp 取得新授權、並將其安裝在 Cloud Volumes ONTAP 該系統上。

如果 Cloud Manager 無法透過安全的網際網路連線存取授權檔案、您可以自行取得檔案、然後手動將檔案上傳至 Cloud Manager 。如需相關指示、請參閱 "管理 BYOL 授權 Cloud Volumes ONTAP 以利執行"。

BYOL 備份授權

BYOL 備份授權可讓您向 NetApp 購買授權、以便在一段時間內使用「備份至雲端」、並獲得最大的備份空間。達到任一限制時、您都需要續約授權。

"深入瞭解 Backup to Cloud BYOL 授權"。

安全性

支援資料加密、並提供防範病毒和勒索軟體的功能。 Cloud Volumes ONTAP

加密閒置的資料

支援下列加密技術： Cloud Volumes ONTAP

- NetApp 加密解決方案（ NVE 和 NAE ）
- AWS 金鑰管理服務
- Azure 儲存服務加密
- Google Cloud Platform 預設加密

您可以使用 NetApp 加密解決方案搭配 AWS 、 Azure 或 GCP 的原生加密、以加密 Hypervisor 層級的資料。這樣做會提供雙重加密、這可能是非常敏感的資料所需要的。存取加密資料時、加密資料會兩次未加密、一次是 Hypervisor 層級（使用雲端供應商提供的金鑰）、然後再次使用 NetApp 加密解決方案（使用外部金鑰管理程式的金鑰）。

NetApp 加密解決方案（ NVE 和 NAE ）

支援 NetApp Volume Encryption （ NVE ）和 NetApp Aggregate Encryption （ NAE ）與外部金鑰管理程式。 Cloud Volumes ONTAPNVE 和 NAE 是軟體型解決方案、可對磁碟區進行（ FIPS ） 140-2 相容的閒置資料加密。

- NVE 一次加密閒置的資料一個磁碟區。每個資料磁碟區都有其專屬的加密金鑰。
- Nae 是 NVE 的延伸、它會加密每個磁碟區的資料、而且磁碟區會在整個集合體之間共用金鑰。Nae 也允許對集合體中所有磁碟區的通用區塊進行重複資料刪除。

NVE 和 NAE 都使用 AES 256 位元加密。

"深入瞭解 NetApp Volume Encryption 和 NetApp Aggregate Encryption"。

從更新版本的支援升級至更新版本的更新版本、在您設定外部金鑰管理程式之後、新的 Aggregate 會預設啟用 NetApp Aggregate Encryption （ NAE ） Cloud Volumes ONTAP 。非 NAE Aggregate 一部分的新磁碟區、預設會啟用 NetApp Volume Encryption （ NVE ）（例如、如果您有在設定外部金鑰管理程式之前建立的現有 Aggregate ）。

設定支援的金鑰管理程式是唯一必要的步驟。如需設定指示、請參閱 "使用 NetApp 加密解決方案加密磁碟區"。

AWS 金鑰管理服務

當您在 Cloud Volumes ONTAP AWS 中啟動一個支援功能系統時、可以使用啟用資料加密 "AWS 金鑰管理服務（ KMS ）"。Cloud Manager 會使用客戶主金鑰（ CMK ）要求資料金鑰。

建立 Cloud Volumes ONTAP 一套系統後、您無法變更 AWS 資料加密方法。

如果您要使用此加密選項、則必須確保 AWS KMS 設定適當。如需詳細資訊、請參閱 "設定 AWS KMS"。

Azure 儲存服務加密

"Azure 儲存服務加密" Azure 中 Cloud Volumes ONTAP 預設會啟用靜止資料的功能、以供資料使用。無需設定。

您可以 Cloud Volumes ONTAP 使用另一個帳戶的外部金鑰、在單一節點的整套系統上加密 Azure 託管磁碟。Cloud Manager API 支援此功能。

您只需在建立單一節點系統時、將下列項目新增至 API 要求：

```
"azureEncryptionParameters": {
      "key": <azure id of encryptionset>
  }
```

客戶管理的金鑰不支援 Cloud Volumes ONTAP 使用不支援的功能。

Google Cloud Platform 預設加密

"Google Cloud Platform 閒置資料加密" 預設為 Cloud Volumes ONTAP 啟用以供使用。無需設定。

雖然 Google Cloud Storage 會在資料寫入磁碟之前先加密資料、但您可以使用 Cloud Manager API 來建立 Cloud Volumes ONTAP 使用 _ 客戶管理的加密金鑰 _ 的支援系統。這些是您使用 Cloud Key Management Service 在 GCP 中產生及管理的金鑰。 "深入瞭解"。

執行防毒掃描 ONTAP

您可以在 ONTAP 更新系統上使用整合式防毒功能、保護資料免受病毒或其他惡意程式碼的侵害。

名為 *VScann* 的還原病毒掃描、結合同級最佳的協力廠商防毒軟體與各種功能、讓您靈活控制掃描檔案的時間與時間。 ONTAP ONTAP

如需 VScan 支援的廠商、軟體及版本資訊、請參閱 "NetApp 互通性對照表"。

如需有關如何設定 ONTAP 及管理作業系統上防毒功能的資訊、請參閱 "《 9 防毒組態指南》 ONTAP"。

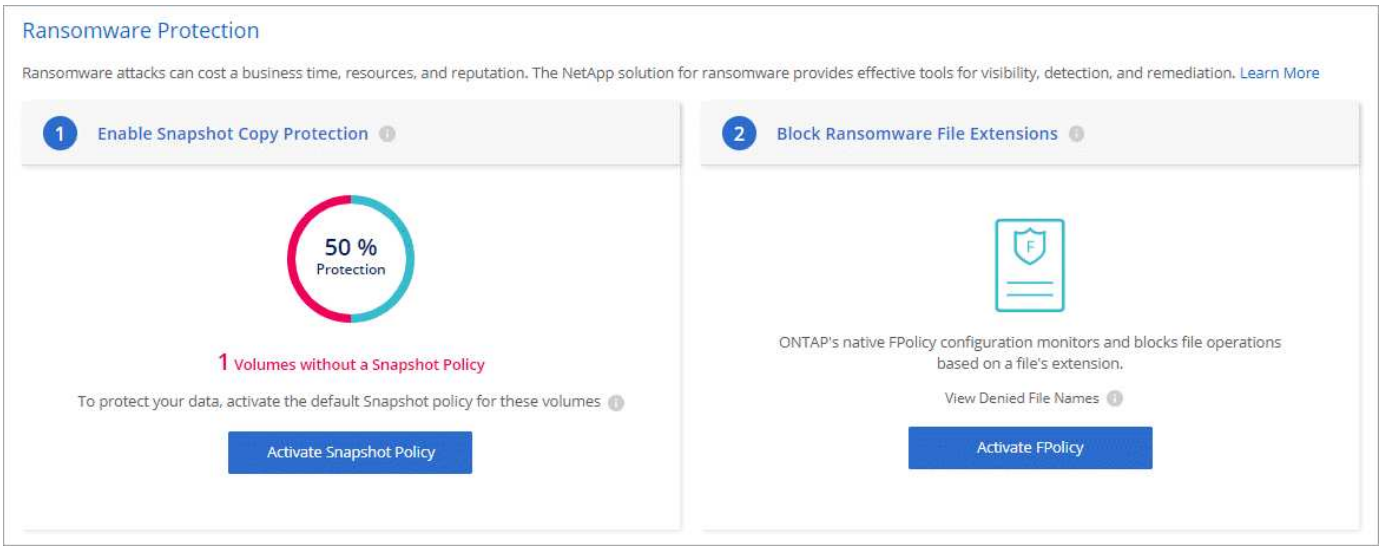
勒索軟體保護

勒索軟體攻擊可能會耗費一定的時間、資源和商譽。Cloud Manager 可讓您針對勒索軟體實作 NetApp 解決方案、提供有效的可見度、偵測及補救工具。

- Cloud Manager 可識別未受 Snapshot 原則保護的磁碟區、並可讓您在這些磁碟區上啟動預設的 Snapshot 原則。

  Snapshot 複本為唯讀、可防止勒索軟體毀損。他們也能提供精細度、以建立單一檔案複本或完整災難恢復解決方案的映像。

- Cloud Manager 也可啟用 ONTAP 的 FPolicy 解決方案、封鎖常見的勒索軟體副檔名。



"瞭解如何實作 NetApp 勒索軟體解決方案"。

效能

您可以檢閱效能結果、協助您決定 Cloud Volumes ONTAP 哪些工作負載適合 VMware 。

- AWS 適用的 Cloud Volumes ONTAP

  "NetApp 技術報告 4383 ： Cloud Volumes ONTAP 運用應用程式工作負載、將 Amazon Web Services 中的功能特性化"。

- 適用於 Microsoft Azure 的 Cloud Volumes ONTAP

  "NetApp 技術報告 4671 ： Cloud Volumes ONTAP 利用應用程式工作負載、將 Azure 中的效能特性化"。

- 適用於 Google Cloud Cloud Volumes ONTAP

  "NetApp 技術報告 4816 ： Cloud Volumes ONTAP 效能特性分析、適用於 Google Cloud"。

的預設組態 **Cloud Volumes ONTAP**

瞭解 Cloud Volumes ONTAP 根據預設設定的功能可協助您設定及管理系統、尤其是熟悉 ONTAP 使用功能時、因為 Cloud Volumes ONTAP 預設的功能與 ONTAP 使用功能不相同、所以使用功能不一。

預設值

- 可在AWS、Azure和GCP中作為單一節點系統使用、也可在AWS和Azure中作為HA配對使用。Cloud Volumes ONTAP
- Cloud Manager 部署 Cloud Volumes ONTAP 時會建立一個資料服務儲存 VM 、部分組態支援額外的儲存 VM 。 "深入瞭解管理儲存 VM"。
- Cloud Manager 會自動在 ONTAP 下列功能授權上安裝 Cloud Volumes ONTAP 於更新：
  - CIFS

- FlexCache
- FlexClone
- iSCSI
- NetApp Volume Encryption （僅適用於 BYOL 或註冊的 PAYGO 系統）
- NFS
- SnapMirror
- SnapRestore
- SnapVault

- 預設會建立多個網路介面：
  - 叢集管理 LIF
  - 叢集間 LIF
  - Azure中HA系統上的SVM管理LIF、AWS中的單一節點系統、以及多個AWS可用性區域中的HA系統（可選）
  - 節點管理 LIF
  - iSCSI 資料 LIF
  - CIFS 與 NFS 資料 LIF

  由於 Cloud Volumes ONTAP EC2 需求、 LIF 容錯移轉功能預設為停用。將 LIF 移轉至其他連接埠會中斷執行個體上 IP 位址與網路介面的外部對應、使 LIF 無法存取。

- 使用 HTTPS 將組態備份傳送至 Connector 。 Cloud Volumes ONTAP

  可從存取備份 https://ipaddress/occm/offboxconfig/ 其中 *ipaddress* 是連接器主機的 IP 位址。

- Cloud Manager 設定的磁碟區屬性與其他管理工具（例如 System Manager 或 CLI ）有所不同。

  下表列出 Cloud Manager 設定的 Volume 屬性與預設值不同：

屬性	**Cloud Manager** 設定的價值
自動調整大小模式	成長
最大自動調整大小	1 、 000 % 帳戶管理員可從「設定」頁面修改此值。
安全風格	適用於 CIFS Volume UNIX for NFS Volume 的 NTFS
空間保證風格	無
UNIX 權限（僅限 NFS ）	777

有關這些屬性的信息，請參見 *volume creation* 手冊頁。

開機和root資料Cloud Volumes ONTAP 以供使用

除了儲存使用者資料之外、Cloud Manager也會購買雲端儲存設備、以便在每Cloud Volumes ONTAP 個作業系統上開機和取得根資料。

AWS

- 每個節點兩個磁碟用於開機和根資料：
  - 9.7 ： 160 GB IO1 磁碟用於開機資料、 220 GB gp2 磁碟用於根資料
  - 9.6 ： 93 GB IO1 磁碟用於開機資料、 140 GB gp2 磁碟用於根資料
  - 9.5 ： 45 GB IO1 磁碟用於開機資料、 140 GB gp2 磁碟用於根資料
- 每個開機磁碟和根磁碟各一份 EBS 快照
- 對於 HA 配對、一個 EBS 磁碟區用於「內化器」執行個體、約 8 GB

Azure （單一節點）

- 三個優質 SSD 磁碟：
  - 一個 10 GB 磁碟用於開機資料
  - 一個 140 GB 磁碟用於根資料
  - 一個 128 GB 磁碟用於 NVRAM

    如果您選擇 Cloud Volumes ONTAP 的虛擬機器支援 Ultra SSD 、則系統會使用 Ultra SSD 來執行 NVRAM 、而非使用 Premium SSD 。
- 一個 10GB 標準 HDD 磁碟、可節省核心
- 每個開機磁碟和根磁碟各一份 Azure 快照

Azure （ **HA** 配對）

- 兩個 10 GB Premium SSD 磁碟用於開機磁碟區（每個節點一個）
- 兩個 140 GB Premium Storage 頁面、用於根磁碟區（每個節點一個）
- 兩個 10GB 標準 HDD 磁碟、可節省核心（每個節點一個）
- 兩個 128 GB Premium SSD 磁碟用於 NVRAM （每個節點一個）
- 每個開機磁碟和根磁碟各一份 Azure 快照

GCP

- 一個 10 GB 標準持續磁碟用於開機資料
- 一個 64 GB 標準持續磁碟用於根資料
- 一個 500 GB 標準持續磁碟用於 NVRAM
- 一個216 GB標準持續磁碟、用於儲存核心
- 每個 GCP 快照一個用於開機磁碟和根磁碟

磁碟所在位置

Cloud Manager 的儲存設備如下所示：

- 開機資料位於附加至執行個體或虛擬機器的磁碟上。

  此磁碟包含開機映像、 Cloud Volumes ONTAP 不適用於 Image.

- 根資料包含系統組態和記錄檔、位於 aggr0 中。
- 儲存虛擬機器（ SVM ）根磁碟區位於 aggr1 中。
- 資料磁碟區也位於 aggr1 中。

加密

Azure 和 Google Cloud Platform 會一律加密開機和根磁碟、因為這些雲端供應商預設會啟用加密功能。

當您使用金鑰管理服務（ KMS ）在 AWS 中啟用資料加密時、 Cloud Volumes ONTAP 也會加密適用於此功能的開機磁碟和根磁碟。這包括 HA 配對中中介執行個體的開機磁碟。磁碟會使用您在建立工作環境時所選取的 CMK 進行加密。

開始使用 AWS

開始使用 Cloud Volumes ONTAP 適用於 AWS 的解決方法

只要幾個步驟、就能開始使用 Cloud Volumes ONTAP 適用於 AWS 的解決方法。


建立連接器

如果您沒有 "連接器" 然而、帳戶管理員需要建立一個帳戶。 "瞭解如何在 AWS 中建立 Connector"。

當您建立第一個 Cloud Volumes ONTAP 運作環境時、如果您還沒有連接器、 Cloud Manager 會提示您部署連接器。


規劃您的組態

Cloud Manager 提供符合工作負載需求的預先設定套件、您也可以建立自己的組態。如果您選擇自己的組態、應該瞭解可用的選項。 "深入瞭解"。


設定您的網路

1. 確保您的 VPC 和子網路支援連接器與 Cloud Volumes ONTAP 支援之間的連線。
2. 啟用從目標 VPC 的傳出網際網路存取、讓 Connector 和 Cloud Volumes ONTAP 支援中心能夠連絡多個端點。

   這個步驟很重要、因為連接器 Cloud Volumes ONTAP 無法在沒有外傳網際網路存取的情況下管理不穩定。

如果您需要限制傳出連線、請參閱的端點清單 "Connector 與 Cloud Volumes ONTAP the"。

3. 設定 S3 服務的 VPC 端點。

   如果您想要將冷資料從 Cloud Volumes ONTAP 不願儲存到低成本物件儲存設備、則需要 VPC 端點。

"深入瞭解網路需求"。

設定 **AWS KMS**

如果您想搭配 Cloud Volumes ONTAP 使用 Amazon 加密搭配使用、則必須確保存在作用中的客戶主金鑰（ CMK ）。您也必須新增 IAM 角色、將連接器的權限提供給作為 _key 使用者 _ 的連接器、以修改每個 CMK 的金鑰原則。 "深入瞭解"。

使用 **Cloud Manager** 啟動 **Cloud Volumes ONTAP**

按一下「 * 新增工作環境 * 」、選取您要部署的系統類型、然後完成精靈中的步驟。 "閱讀逐步指示"。

相關連結

- "評估"
- "從 Cloud Manager 建立 Connector"
- "從 AWS Marketplace 啟動 Connector"
- "在 Linux 主機上安裝 Connector 軟體"
- "Cloud Manager 使用 AWS 權限的功能"

在 **Cloud Volumes ONTAP AWS** 中規劃您的功能

在 Cloud Volumes ONTAP AWS 中部署時、您可以選擇符合工作負載需求的預先設定系統、也可以建立自己的組態。如果您選擇自己的組態、應該瞭解可用的選項。

選擇授權類型

提供兩種定價選項：隨用隨付及自帶授權（ BYOL） Cloud Volumes ONTAP 。若為隨用隨付、您可以從三種授權中選擇： Explore 、 Standard 或 Premium 。每個授權都提供不同的容量和運算選項。

"支援Cloud Volumes ONTAP AWS中的支援的支援組態"

瞭解儲存限制

一個不含資源的系統的原始容量上限 Cloud Volumes ONTAP 與授權有關。其他限制會影響集合體和磁碟區的大小。在規劃組態時、您應該注意這些限制。

"AWS中的更新儲存限制Cloud Volumes ONTAP"

在 AWS 中調整系統規模

調整 Cloud Volumes ONTAP 您的支援規模、有助於滿足效能與容量的需求。在選擇執行個體類型、磁碟類型和磁碟大小時、您應該注意幾個關鍵點：

執行個體類型

- 將工作負載需求與每個 EC2 執行個體類型的最大處理量和 IOPS 配對。
- 如果有多位使用者同時寫入系統、請選擇有足夠 CPU 來管理要求的執行個體類型。
- 如果您的應用程式大多讀取、請選擇具有足夠 RAM 的系統。
  - "AWS 文件： Amazon EC2 執行個體類型"
  - "AWS 文件： Amazon EBS 最佳化執行個體"

EBS 磁碟類型

通用 SSD 是 Cloud Volumes ONTAP 最常見的磁碟類型。若要檢視 EBS 磁碟的使用案例、請參閱 "AWS 文件： EBS Volume 類型"。

EBS 磁碟大小

啟動 Cloud Volumes ONTAP 一套系統時、您需要選擇初始磁碟大小。之後、您就可以了 "讓 Cloud Manager 為您管理系統容量"但如果您想要的話 "自行建置集合體"請注意下列事項：

- 集合體中的所有磁碟大小必須相同。
- EBS 磁碟的效能與磁碟大小有關。大小決定 SSD 磁碟的基準 IOPS 和最大突發持續時間、以及 HDD 磁碟的基準和突發處理量。
- 最後、您應該選擇能提供所需 _ 持續效能 _ 的磁碟大小。
- 即使您選擇較大的磁碟（例如六個 4 TB 磁碟）、也可能無法取得所有 IOPS 、因為 EC2 執行個體可以達到其頻寬限制。

  如需 EBS 磁碟效能的詳細資訊、請參閱 "AWS 文件： EBS Volume 類型"。

請觀看下列影片、以瞭解如何在 Cloud Volumes ONTAP AWS 中調整您的更新功能：

[] | *https://img.youtube.com/vi/GELcXmOuYPw/maxresdefault.jpg*

選擇支援 Flash Cache 的組態

AWS 中的 Cloud Volumes ONTAP 部分支援部分支援 NVMe 儲存設備、 Cloud Volumes ONTAP 這些儲存設備可做為 _Flash Cache 、以獲得更好的效能。 "深入瞭解 Flash Cache"。

AWS 網路資訊工作表

在 Cloud Volumes ONTAP AWS 中啟動時、您需要指定 VPC 網路的詳細資料。您可以使用工作表向系統管理員收集資訊。

網路資訊 Cloud Volumes ONTAP

AWS 資訊	您的價值
區域	

AWS 資訊	您的價值
VPC	
子網路	
安全性群組（如果使用您自己的）	

多個 AZs 中 HA 配對的網路資訊

AWS 資訊	您的價值
區域	
VPC	
安全性群組（如果使用您自己的）	
節點 1 可用度區域	
節點 1 子網路	
節點 2 可用度區域	
節點 2 子網路	
中介可用度區域	
中介子網路	
中介器的金鑰配對	
叢集管理連接埠的浮動 IP 位址	
節點 1 上資料的浮動 IP 位址	
節點 2 上資料的浮動 IP 位址	
浮動 IP 位址的路由表	

選擇寫入速度

Cloud Manager可讓您選擇單一節點Cloud Volumes ONTAP 的寫入速度設定。在您選擇寫入速度之前、您應該先瞭解一般與高設定之間的差異、以及使用高速寫入速度時的風險與建議。

正常寫入速度與高速寫入速度之間的差異

當您選擇正常寫入速度時、資料會直接寫入磁碟、因此可降低發生非計畫性系統中斷時發生資料遺失的可能性。

選擇高速寫入速度時、資料會在寫入磁碟之前先緩衝到記憶體中、以提供更快的寫入效能。由於這種快取、如果發生非計畫性的系統中斷、可能會導致資料遺失。

發生非計畫性系統中斷時可能遺失的資料量、是最後兩個一致點的範圍。一致點是將緩衝資料寫入磁碟的行為。寫入日誌已滿或 10 秒後（以先到者為準）、就會出現一致點。然而、AWS EBS Volume效能可能會影響一致點處理時間。

何時使用高速寫入

如果您的工作負載需要快速寫入效能、而且在非計畫性的系統中斷時、您可以承受資料遺失的風險、那麼高速寫入速度是很好的選擇。

使用高速寫入速度時的建議事項

如果啟用高速寫入、則應確保應用程式層的寫入保護。

選擇 **Volume** 使用設定檔

包含多項儲存效率功能、可減少您所需的總儲存容量。 ONTAP在 Cloud Manager 中建立 Volume 時、您可以選擇啟用這些功能的設定檔、或是停用這些功能的設定檔。您應該深入瞭解這些功能、以協助您決定要使用的設定檔。

NetApp 儲存效率功能提供下列效益：

資源隨需配置

為主機或使用者提供比實體儲存資源池實際擁有更多的邏輯儲存設備。儲存空間不會預先配置儲存空間、而是會在寫入資料時動態分配給每個磁碟區。

重複資料刪除

找出相同的資料區塊、並以單一共用區塊的參考資料取代這些區塊、藉此提升效率。這項技術可消除位於同一個磁碟區的備援資料區塊、進而降低儲存容量需求。

壓縮

藉由壓縮主儲存設備、次儲存設備和歸檔儲存設備上磁碟區內的資料、來減少儲存資料所需的實體容量。

設定您的網路

AWS 的網路需求 **Cloud Volumes ONTAP**

設定 AWS 網路功能、 Cloud Volumes ONTAP 讓各個系統正常運作。

一般需求 **Cloud Volumes ONTAP**

AWS 必須符合下列要求。

對節點的輸出網際網路存取 **Cloud Volumes ONTAP**

支援不需透過外部網際網路存取、即可將訊息傳送至 NetApp 解決方案、以主動監控儲存設備的健全狀況。 Cloud Volumes ONTAP AutoSupport

路由和防火牆原則必須允許 AWS HTTP / HTTPS 流量傳輸至下列端點、 Cloud Volumes ONTAP 才能讓下列端點傳送 AutoSupport 動態訊息：

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

  如果您有 NAT 執行個體、則必須定義傳入安全性群組規則、以允許 HTTPS 流量從私有子網路傳入網際網路。

"瞭解如何設定 AutoSupport 功能"。

HA 中介器的傳出網際網路存取

HA 中介執行個體必須具有 AWS EC2 服務的傳出連線、才能協助進行儲存容錯移轉。若要提供連線、您可以新增公用 IP 位址、指定 Proxy 伺服器或使用手動選項。

手動選項可以是從目標子網路到 AWS EC2 服務的 NAT 閘道或介面 VPC 端點。如需 VPC 端點的詳細資訊、請參閱 "AWS 文件：介面 VPC 端點（ AWS Private Link ）"。

IP 位址數

Cloud Manager 會在 Cloud Volumes ONTAP AWS 中配置下列數量的 IP 位址給功能不全：

- 單一節點： 6 個 IP 位址
- HA 配對單一 AZs ： 15 個位址
- 多個 AZs 中的 HA 配對： 15 或 16 個 IP 位址

  請注意、 Cloud Manager 會在單一節點系統上建立 SVM 管理 LIF 、但不會在單一 AZ 的 HA 配對上建立。您可以選擇是否在多個 AZs 的 HA 配對上建立 SVM 管理 LIF 。

LIF 是與實體連接埠相關聯的 IP 位址。諸如 VMware 的管理工具需要 SVM 管理 LIF SnapCenter 。

安全性群組

您不需要建立安全性群組、因為 Cloud Manager 會為您建立安全性群組。如果您需要使用自己的、請參閱 "安全性群組規則"。

從 **Cloud Volumes ONTAP** 支援資料分層的功能、從功能鏈接至 **AWS S3**

如果您想要將 EBS 當作效能層、將 AWS S3 當作容量層、您必須確保 Cloud Volumes ONTAP 將該連接到 S3 。提供此連線的最佳方法是建立 VPC 端點至 S3 服務。如需相關指示、請參閱 "AWS 文件：建立閘道端點"。

當您建立 VPC 端點時、請務必選取與 Cloud Volumes ONTAP 該實例相對應的區域、 VPC 和路由表。您也必須修改安全性群組、以新增允許流量到 S3 端點的傳出 HTTPS 規則。否則 Cloud Volumes ONTAP 、無法連線至 S3 服務。

如果您遇到任何問題、請參閱 "AWS 支援知識中心：為什麼我無法使用閘道 VPC 端點連線至 S3 儲存區？"

連線 **ONTAP** 至其他網路中的不二系統

若要在 Cloud Volumes ONTAP AWS 系統和 ONTAP 其他網路中的更新系統之間複寫資料、您必須在 AWS VPC 和其他網路之間建立 VPN 連線、例如 Azure vnet 或公司網路。如需相關指示、請參閱 "AWS 文件：設定 AWS VPN 連線"。

適用於 **CIFS** 的 **DNS** 和 **Active Directory**

如果您想要配置 CIFS 儲存設備、則必須在 AWS 中設定 DNS 和 Active Directory 、或將內部部署設定延伸至 AWS 。

DNS 伺服器必須為 Active Directory 環境提供名稱解析服務。您可以將 DHCP 選項集設定為使用預設 EC2 DNS 伺服器、此伺服器不得是 Active Directory 環境所使用的 DNS 伺服器。

如需相關指示、請參閱 "AWS 文件： AWS Cloud 上的 Active Directory 網域服務：快速入門參考部署"。

多個 **AZs** 的 **HA** 配對需求

其他 AWS 網路需求適用於 Cloud Volumes ONTAP 使用多個可用區域（ AZs ）的 SestHA 組態。在啟動 HA 配對之前、您應該先檢閱這些需求、因為您必須在 Cloud Manager 中輸入網路詳細資料。

若要瞭解 HA 配對的運作方式、請參閱 "高可用度配對"。

可用度區域

此 HA 部署模式使用多個 AZs 來確保資料的高可用度。您應該使用專屬的 AZ 來處理每 Cloud Volumes ONTAP 個實例、並使用中介執行個體、以提供 HA 配對之間的通訊通道。

用於 **NAS** 資料和叢集 **/ SVM** 管理的浮動 **IP** 位址

多個 AZs 中的 HA 組態會使用浮動 IP 位址、在發生故障時在節點之間移轉。除非您的選擇、否則無法從 VPC 外部原生存取 "設定 AWS 傳輸閘道"。

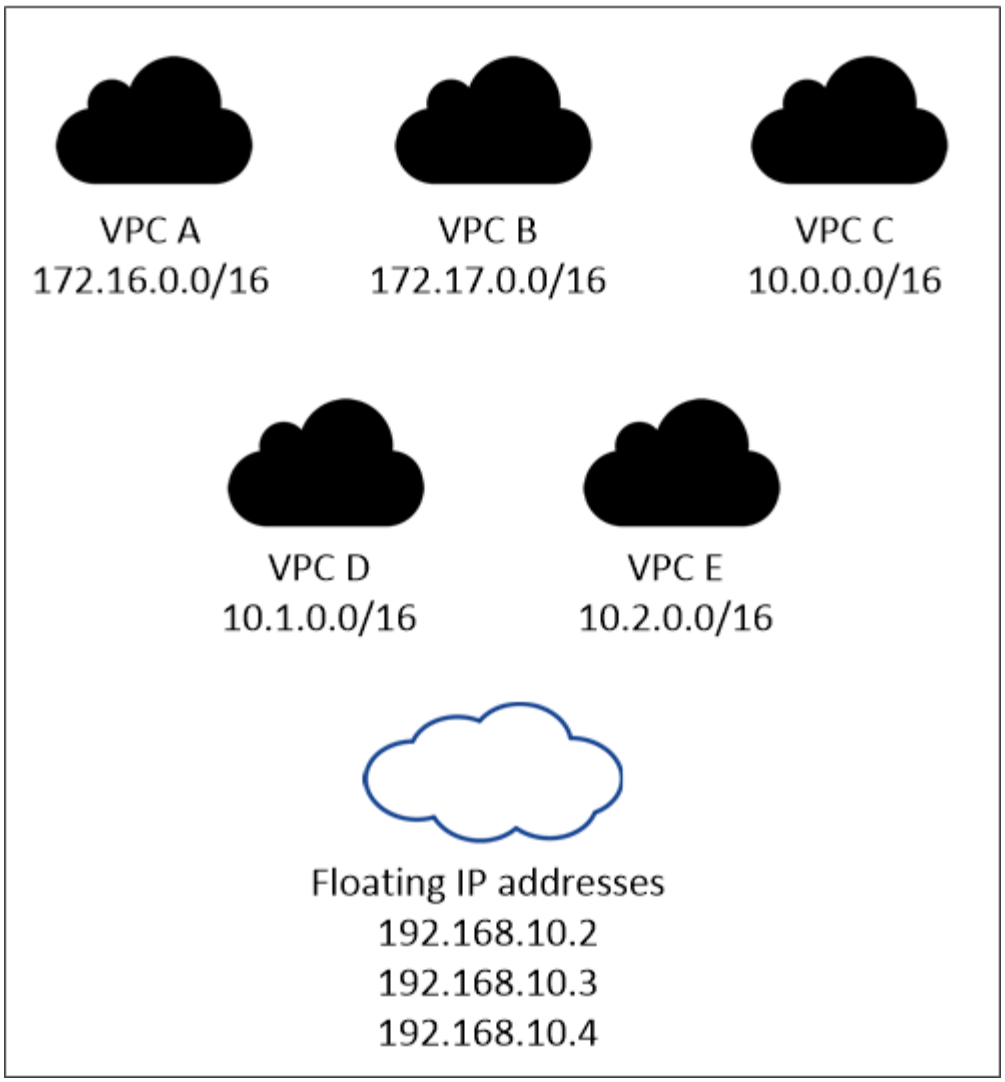
一個浮動 IP 位址是用於叢集管理、一個用於節點 1 上的 NFS/CIFS 資料、另一個用於節點 2 上的 NFS/CIFS 資料。SVM 管理的第四個浮動 IP 位址為選用項目。

如果您使用 SnapDrive 適用於 Windows 的 SHIP 或 SnapCenter 搭配 HA 配對的 SHIP 、則 SVM 管理 LIF 需要一個浮動 IP 位址。如果您在部署系統時未指定 IP 位址、您可以稍後建立 LIF 。如需詳細資訊、請參閱 "設定 Cloud Volumes ONTAP 功能"。

當您建立 Cloud Volumes ONTAP 一個發揮作用的環境時、需要在 Cloud Manager 中輸入浮動 IP 位址。Cloud Manager 會在 HA 配對啟動系統時、將 IP 位址分配給 HA 配對。

在部署 HA 組態的 AWS 區域中、所有 VPC 的浮動 IP 位址都必須位於 CIDR 區塊之外。將浮動 IP 位址視為位於您所在地區 VPC 外部的邏輯子網路。

下列範例顯示 AWS 區域中浮動 IP 位址與 VPC 之間的關係。雖然浮動 IP 位址位於所有 VPC 的 CIDR 區塊之外、但仍可透過路由表路由傳送至子網路。



Cloud Manager 會自動建立靜態 IP 位址、以供 iSCSI 存取及從 VPC 外部用戶端存取 NAS 。您不需要滿足這些類型 IP 位址的任何需求。

傳輸閘道、可從 **VPC** 外部啟用浮動 **IP** 存取

"設定 AWS 傳輸閘道" 可從 HA 配對所在的 VPC 外部存取 HA 配對的浮動 IP 位址。

路由表

在 Cloud Manager 中指定浮動 IP 位址之後、您必須選取路由表、其中應包含通往浮動 IP 位址的路由。這可讓用戶端存取 HA 配對。

如果 VPC 中只有一個子網路路由表（主路由表）、 Cloud Manager 會自動將浮動 IP 位址新增至該路由表。如果您有多個路由表、在啟動 HA 配對時、請務必選取正確的路由表。否則、部分用戶端可能無法存取 Cloud Volumes ONTAP 功能不完全。

例如、您可能有兩個子網路與不同的路由表相關聯。如果您選取路由表 A 而非路由表 B 、則與路由表 A 相關聯的子網路中的用戶端可以存取 HA 配對、但與路由表 B 相關的子網路中的用戶端則無法存取。

如需路由表的詳細資訊、請參閱 "AWS 文件：路由表"。

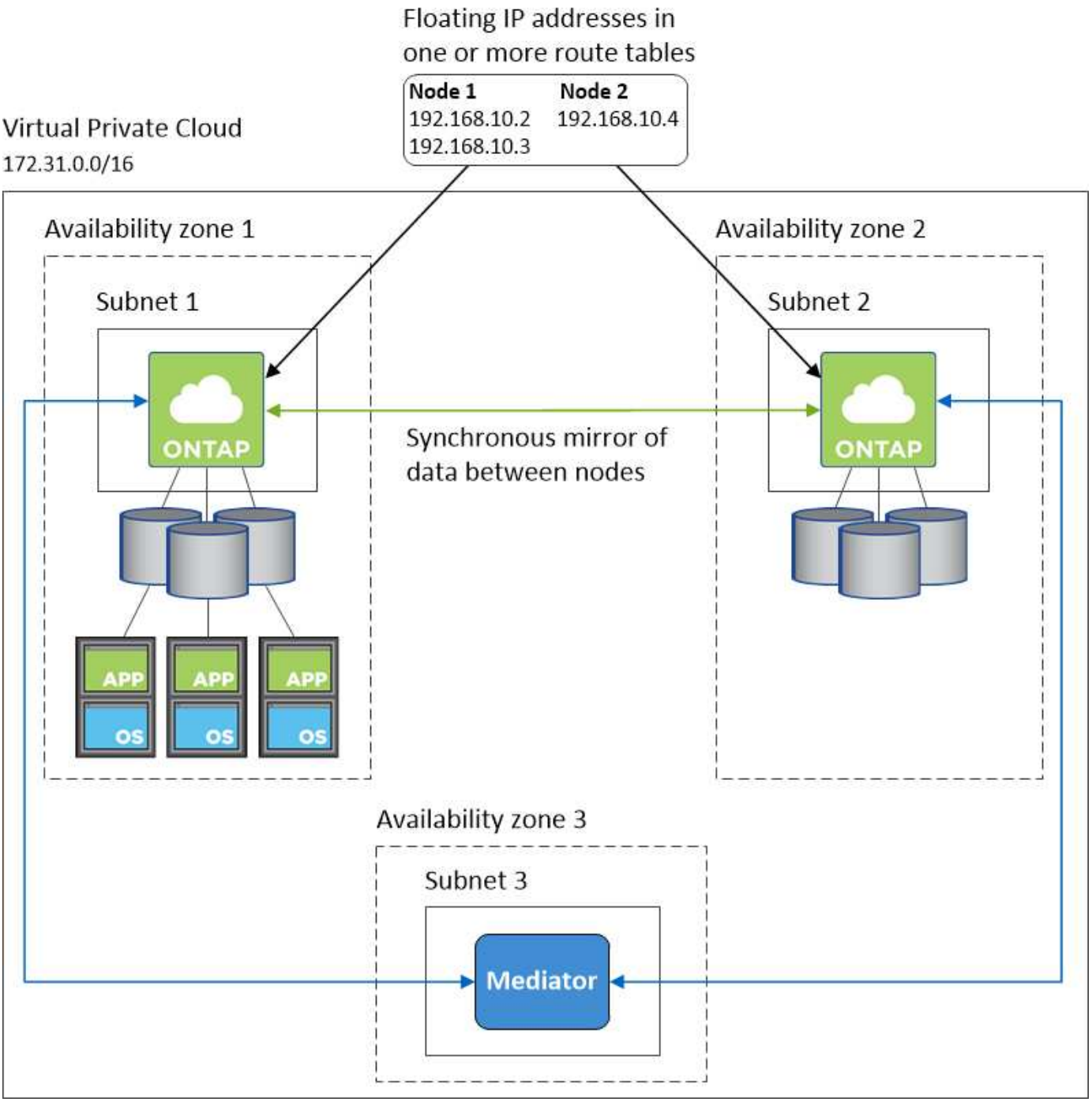
連線至 **NetApp** 管理工具

若要將 NetApp 管理工具搭配多個 AZs 中的 HA 組態使用、您有兩種連線選項：

1. 在不同的 VPC 和中部署 NetApp 管理工具 "設定 AWS 傳輸閘道"。閘道可讓您從 VPC 外部存取叢集管理介面的浮動 IP 位址。
2. 在與 NAS 用戶端相同的 VPC 中部署 NetApp 管理工具、其路由組態與 NAS 用戶端相似。

HA 組態範例

下圖顯示 AWS 以主動 - 被動式組態運作時的最佳 HA 組態：



設定您的網路、讓 Connector 能夠管理公有雲環境中的資源和程序。最重要的步驟是確保從網際網路存取各種端點。

如果您的網路使用 Proxy 伺服器來進行所有與網際網路的通訊、您可以從「設定」頁面指定 Proxy 伺服器。請參閱 "將 Connector 設定為使用 Proxy 伺服器"。

連線至目標網路

連接器需要網路連線至您要部署 Cloud Volumes ONTAP 的 VPC 和 VNets 。

例如、如果您在公司網路中安裝 Connector 、則必須設定 VPN 連線至 VPC 或 vnet 、以便在其中啟動 Cloud Volumes ONTAP 更新。

傳出網際網路存取

連接器需要存取傳出網際網路、才能管理公有雲環境中的資源和程序。在 AWS 中管理資源時、 Connector 會聯絡下列端點：

端點	目的
AWS 服務（ amazonaws.com): • CloudForation • 彈性運算雲端（ EC2 ） • 金鑰管理服務（ KMS ） • 安全性權杖服務（ STOS ） • 簡易儲存服務（ S3 ） 確切的端點取決於您部署 Cloud Volumes ONTAP 的區域。 "如需詳細資料、請參閱 AWS 文件。"	讓Cloud Manager能夠在Cloud Volumes ONTAP AWS中部署及管理功能。
https://api.services.cloud.netapp.com:443	API 要求 NetApp Cloud Central 。
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	提供軟體映像、資訊清單和範本的存取權限。
https://repo.cloud.support.netapp.com	用於下載Cloud Manager相依性。
http://repo.mysql.com/	用於下載MySQL。
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	讓Cloud Manager能夠存取及下載資訊清單、範本及Cloud Volumes ONTAP 升級影像。
https://cloudmanagerinfraprod.azurecr.io	存取執行 Docker 之基礎架構的容器元件軟體映像、並提供與 Cloud Manager 整合服務的解決方案。

端點	目的
https://kinesis.us-east-1.amazonaws.com	讓 NetApp 能夠從稽核記錄串流資料。
https://cloudmanager.cloud.netapp.com	與 Cloud Manager 服務（包括 Cloud Central 帳戶）進行通訊。
https://netapp-cloud-account.auth0.com	與 NetApp Cloud Central 通訊、以進行集中式使用者驗證。
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	用於將AWS帳戶ID新增至允許備份至S3的使用者清單。
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	與 NetApp AutoSupport 通訊
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	與 NetApp 溝通以取得系統授權與支援登錄。
https://ipa-signer.cloudmanager.netapp.com	讓 Cloud Manager 能夠產生授權（例如 FlexCache 、針對 Cloud Volumes ONTAP 功能不全的
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	需要將Cloud Volumes ONTAP 支援的系統與Kubernetes叢集連線。端點可安裝NetApp Trident。
各種協力廠商位置、例如： • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org 第三方據點可能會有所變更。	在升級期間、 Cloud Manager 會針對協力廠商相依性下載最新的套件。

雖然您應該從 SaaS 使用者介面執行幾乎所有的工作、但連接器上仍有本機使用者介面可供使用。執行 Web 瀏覽器的機器必須連線至下列端點：

端點	目的
連接器主機	您必須從網頁瀏覽器輸入主機的 IP 位址、才能載入 Cloud Manager 主控台。 視您與雲端供應商的連線能力而定、您可以使用指派給主機的私有 IP 或公有 IP ： • 如果您有 VPN 並直接連線至虛擬網路、則私有 IP 可正常運作 • 公有 IP 適用於任何網路情境 無論如何、您應該確保安全群組規則僅允許從授權的 IP 或子網路存取、以確保網路存取安全。
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	您的網頁瀏覽器會連線至這些端點、以便透過 NetApp Cloud Central 進行集中式使用者驗證。
https://widget.intercom.io	產品內對談可讓您與 NetApp 雲端專家交談。

在多個 **AZs** 中設定 **HA** 配對的 **AWS** 傳輸閘道

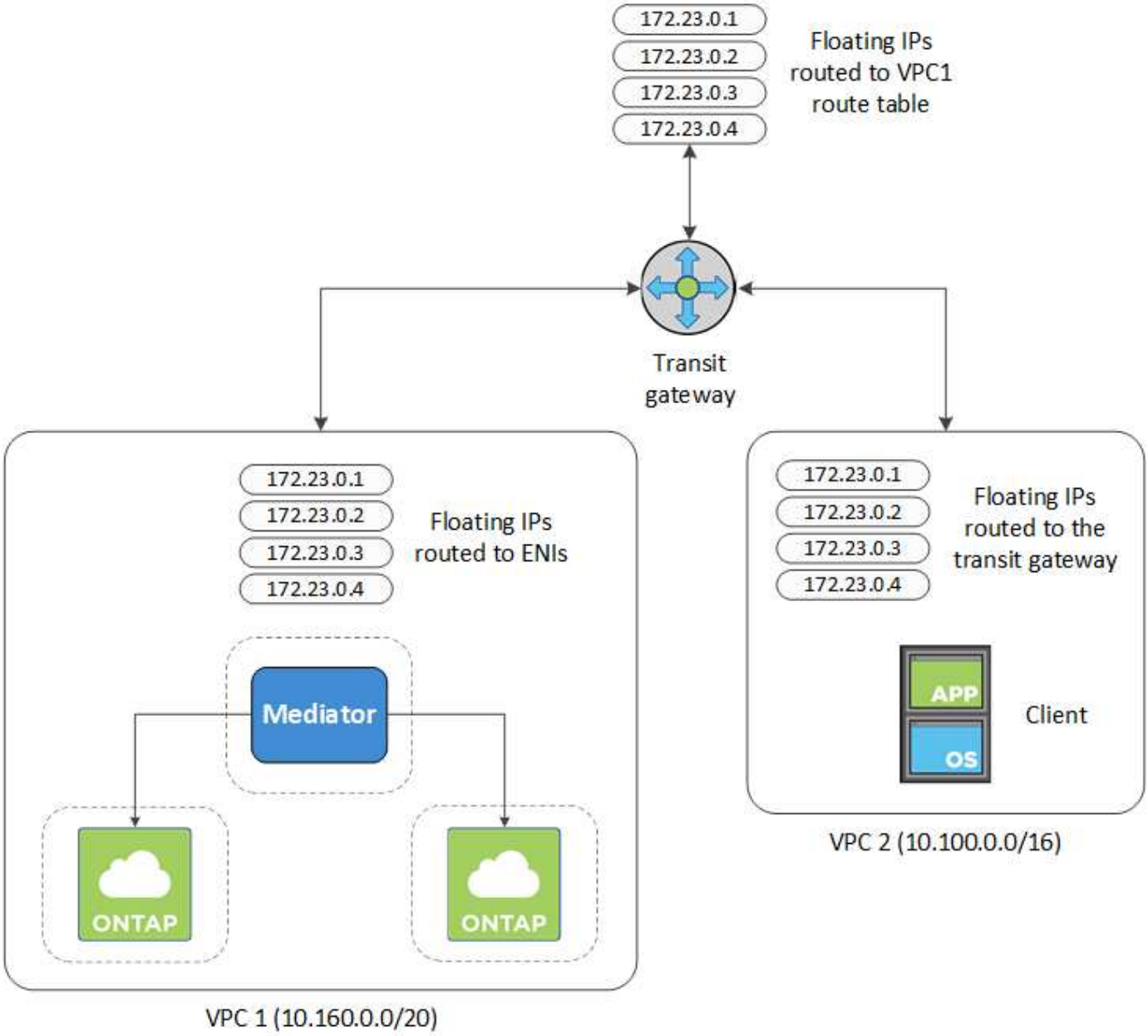
設定 AWS 傳輸閘道、以便存取 HA 配對 "浮動 IP 位址" 從 HA 配對所在的 VPC 外部。

當某個靜態 HA 組態分佈於多個 AWS 可用區域時、從 VPC 內部存取 NAS 資料時、需要使用浮動 IP 位址。Cloud Volumes ONTAP當發生故障時、這些浮動 IP 位址可在節點之間移轉、但無法從 VPC 外部原生存取。獨立的私有 IP 位址可從 VPC 外部存取資料、但無法提供自動容錯移轉功能。

叢集管理介面和選用的 SVM 管理 LIF 也需要浮動 IP 位址。

如果您設定 AWS 傳輸閘道、就能從 HA 配對所在的 VPC 外部存取浮動 IP 位址。這表示 VPC 以外的 NAS 用戶端和 NetApp 管理工具可以存取浮動 IP 。

以下範例顯示兩個透過傳輸閘道連線的 VPC 。HA 系統位於一個 VPC 、而用戶端位於另一個 VPC 。然後、您可以使用浮動 IP 位址、在用戶端上掛載 NAS Volume 。

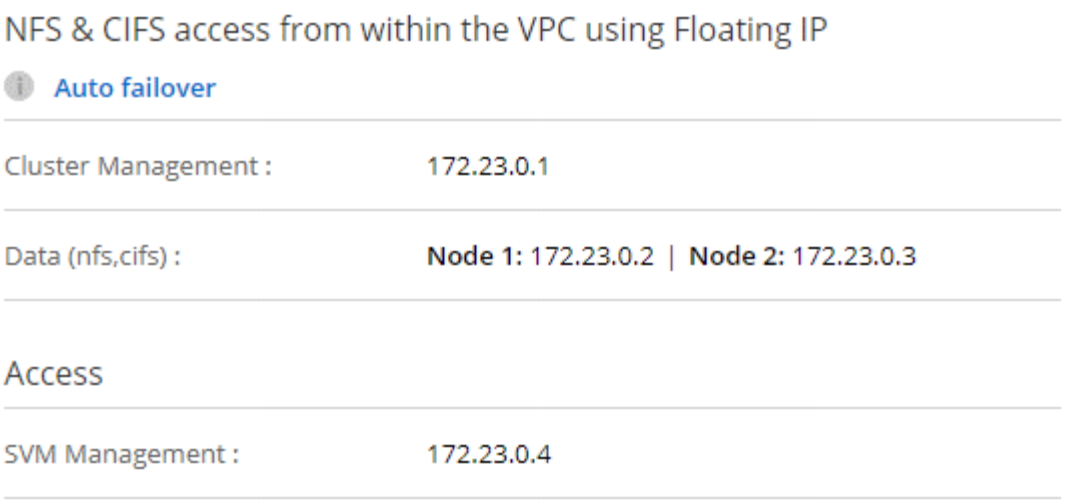


下列步驟說明如何設定類似的組態。

步驟

1. "建立傳輸閘道、並將 VPC 附加至閘道"。
2. 指定 HA 配對的浮動 IP 位址、在傳輸閘道的路由表中建立路由。

   您可以在 Cloud Manager 的「工作環境資訊」頁面找到浮動 IP 位址。範例如下：



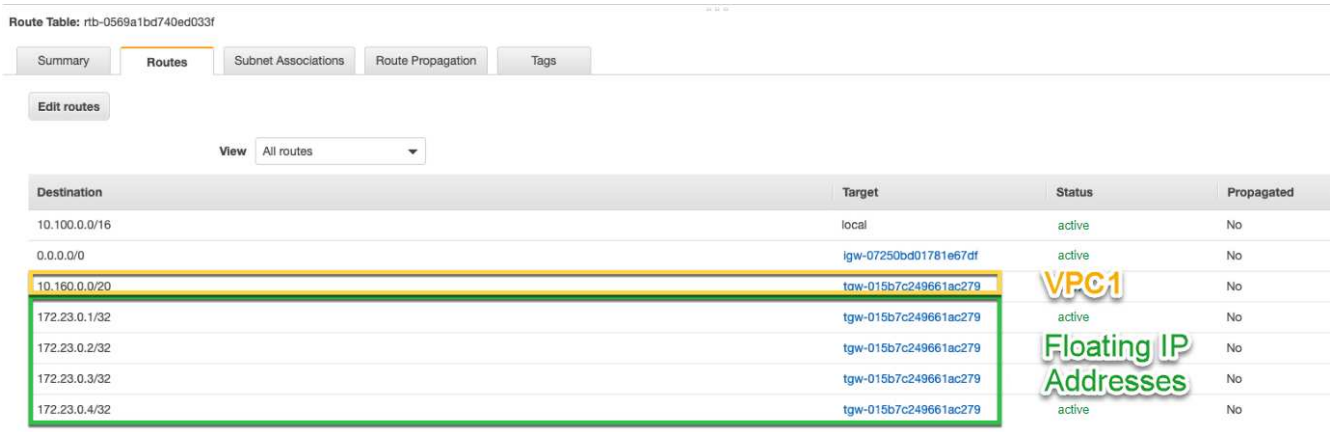
下列範例影像顯示傳輸閘道的路由表。其中包括兩部 VPC 的 CIDR 區塊路由、 Cloud Volumes ONTAP 以及由 R1 使用的四個浮動 IP 位址。

3. 修改需要存取浮動 IP 位址的 VPC 路由表。

   a. 新增路由項目至浮動 IP 位址。

   b. 將路由項目新增至 HA 配對所在 VPC 的 CIDR 區塊。

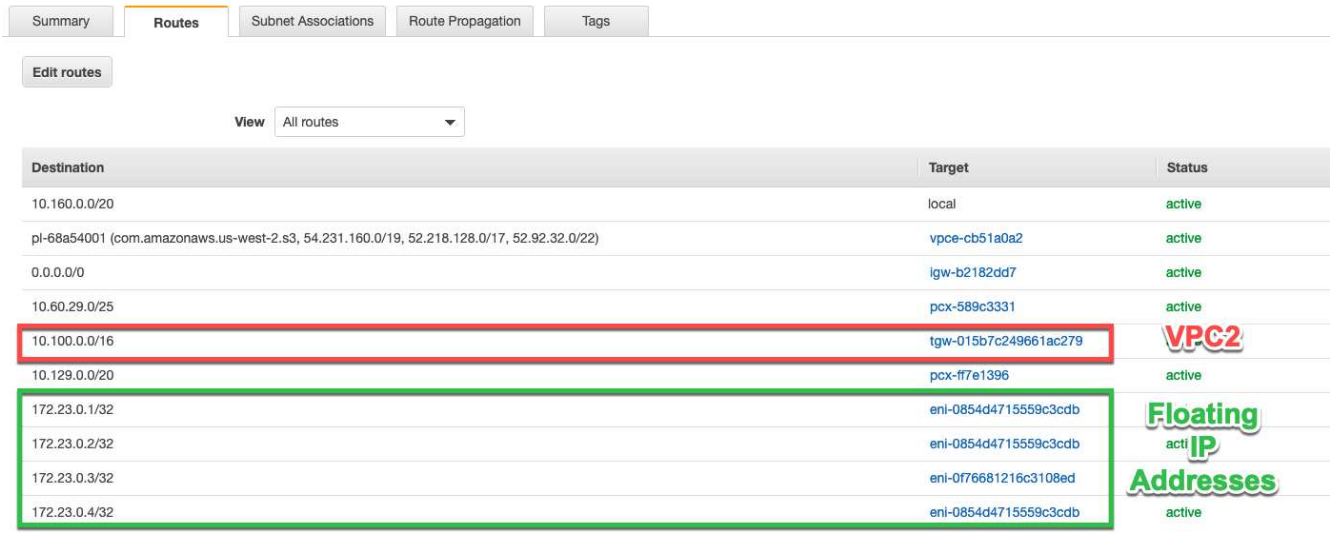
      下列範例影像顯示 VPC 2 的路由表、其中包括通往 VPC 1 的路由和浮動 IP 位址。



4. 將需要存取浮動 IP 位址的路由新增至 VPC 、以修改 HA 配對 VPC 的路由表。

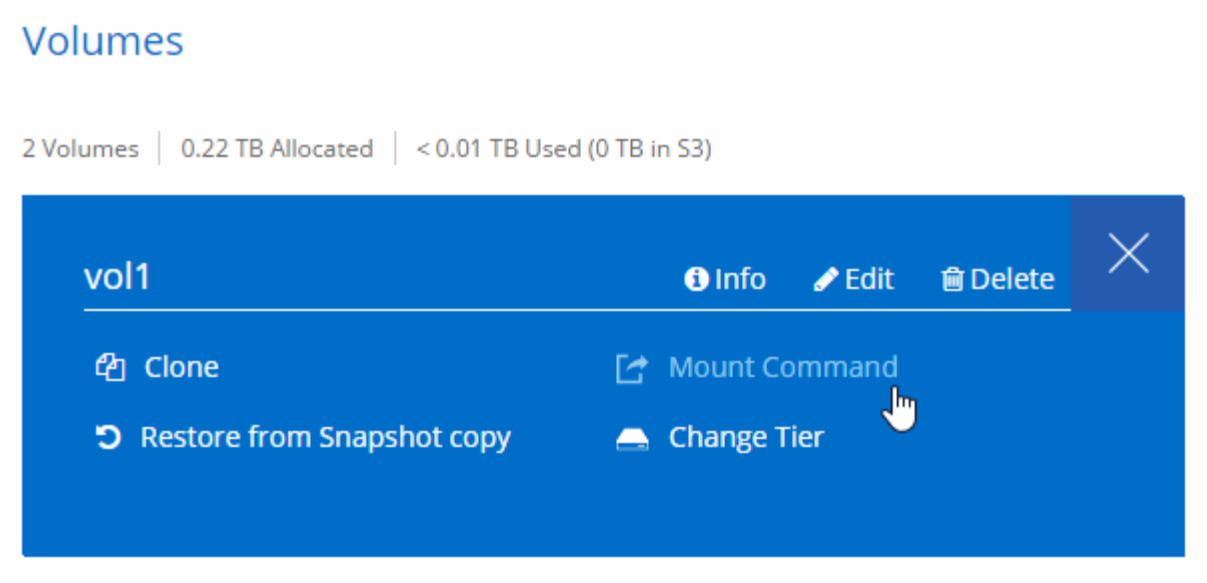
   此步驟非常重要、因為它會完成 VPC 之間的路由。

   下列範例影像顯示 VPC 1 的路由表。其中包括通往浮動 IP 位址和 VPC 2 的路由、而 VPC 2 是用戶端所在的位置。Cloud Manager 會在部署 HA 配對時、自動將浮動 IP 新增至路由表。



5. 使用浮動 IP 位址將磁碟區掛載到用戶端。

   您可以在 Cloud Manager 中找到正確的 IP 位址、方法是選取磁碟區、然後按一下 * Mount Command* 。



- 相關連結 *
- "AWS 中的高可用度配對"
- "AWS 的網路需求 Cloud Volumes ONTAP"

AWS 的安全群組規則

Cloud Manager 會建立 AWS 安全性群組、其中包含 Connector 和 Cloud Volumes ONTAP NetApp 成功運作所需的傳入和傳出規則。您可能需要參照連接埠進行測試、或是偏好使用自己的安全性群組。

規則 **Cloud Volumes ONTAP**

適用於此功能的安全性群組 Cloud Volumes ONTAP 需要傳入和傳出規則。

傳入規則

預先定義之安全性群組中的傳入規則來源為 0.00.0.0/0 。

傳輸協定	連接埠	目的
所有 ICMP	全部	Ping 執行個體
HTTP	80	使用叢集管理 LIF 的 IP 位址、以 HTTP 存取 System Manager Web 主控台
HTTPS	443..	使用叢集管理 LIF 的 IP 位址、以 HTTPS 存取 System Manager 網路主控台
SSH	22	SSH 存取叢集管理 LIF 的 IP 位址或節點管理 LIF
TCP	111.	遠端程序需要 NFS
TCP	139.	CIFS 的 NetBios 服務工作階段
TCP	161-162	簡單的網路管理傳輸協定
TCP	445	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構

傳輸協定	連接埠	目的
TCP	635	NFS 掛載
TCP	749	Kerberos
TCP	2049	NFS 伺服器精靈
TCP	3260	透過 iSCSI 資料 LIF 存取 iSCSI
TCP	4045	NFS 鎖定精靈
TCP	4046	NFS 的網路狀態監控
TCP	10000	使用 NDMP 備份
TCP	11104.	管理 SnapMirror 的叢集間通訊工作階段
TCP	11105.	使用叢集間生命體進行 SnapMirror 資料傳輸
UDP	111.	遠端程序需要 NFS
UDP	161-162	簡單的網路管理傳輸協定
UDP	635	NFS 掛載
UDP	2049	NFS 伺服器精靈
UDP	4045	NFS 鎖定精靈
UDP	4046	NFS 的網路狀態監控
UDP	4049	NFS rquotad 傳輸協定

傳出規則

預先定義 Cloud Volumes ONTAP 的 Security Group for the 旅行團會開啟所有的傳出流量。如果可以接受、請遵循基本的傳出規則。如果您需要更嚴格的規則、請使用進階的傳出規則。

基本傳出規則

適用於此功能的預先定義安全性群組 Cloud Volumes ONTAP 包括下列傳出規則。

傳輸協定	連接埠	目的
所有 ICMP	全部	所有傳出流量
所有 TCP	全部	所有傳出流量
所有的 udp	全部	所有傳出流量

進階傳出規則

如果您需要嚴格的傳出流量規則、可以使用下列資訊、僅開啟 Cloud Volumes ONTAP 那些由真人進行傳出通訊所需的連接埠。

來源是 Cloud Volumes ONTAP 指在整個系統上的介面（ IP 位址）。

服務	傳輸協定	連接埠	來源	目的地	目的
Active Directory	TCP	88	節點管理 LIF	Active Directory 樹系	Kerberos V 驗證
	UDP	137.	節點管理 LIF	Active Directory 樹系	NetBios 名稱服務
	UDP	138	節點管理 LIF	Active Directory 樹系	NetBios 資料報服務
	TCP	139.	節點管理 LIF	Active Directory 樹系	NetBios 服務工作階段
	TCP 與 UDP	389	節點管理 LIF	Active Directory 樹系	LDAP
	TCP	445	節點管理 LIF	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	TCP	464. 64	節點管理 LIF	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	UDP	464. 64	節點管理 LIF	Active Directory 樹系	Kerberos 金鑰管理
	TCP	749	節點管理 LIF	Active Directory 樹系	Kerberos V 變更與設定密碼（ RPCSEC_GSS ）
	TCP	88	資料 LIF （ NFS 、 CIFS 、 iSCSI ）	Active Directory 樹系	Kerberos V 驗證
	UDP	137.	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 名稱服務
	UDP	138	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 資料報服務
	TCP	139.	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 服務工作階段
	TCP 與 UDP	389	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	LDAP
	TCP	445	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	TCP	464. 64	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	UDP	464. 64	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos 金鑰管理
	TCP	749	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos V 變更及設定密碼（ RPCSEC_GSS ）
備份至 S3	TCP	5010 .	叢集間 LIF	備份端點或還原端點	備份與還原備份至 S3 功能的作業

服務	傳輸協定	連接埠	來源	目的地	目的
叢集	所有流量	所有流量	一個節點上的所有 LIF	其他節點上的所有 LIF	叢集間通訊（ Cloud Volumes ONTAP 僅限不含 HA ）
	TCP	3000	節點管理 LIF	HA 中介	ZAPI 呼叫（ Cloud Volumes ONTAP 僅限 RHA ）
	ICMP	1.	節點管理 LIF	HA 中介	Keepive Alive （ Cloud Volumes ONTAP 僅限 HHA ）
DHCP	UDP	68	節點管理 LIF	DHCP	第一次設定的 DHCP 用戶端
DHCPS	UDP	67	節點管理 LIF	DHCP	DHCP 伺服器
DNS	UDP	53.	節點管理 LIF 與資料 LIF （ NFS 、 CIFS ）	DNS	DNS
NDMP	TCP	18600 – 18699	節點管理 LIF	目的地伺服器	NDMP 複本
SMTP	TCP	25	節點管理 LIF	郵件伺服器	可以使用 SMTP 警示 AutoSupport 來執行功能
SNMP	TCP	161.	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	UDP	161.	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	TCP	162 %	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	UDP	162 %	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
SnapMirror	TCP	11104.	叢集間 LIF	叢集間 LIF ONTAP	管理 SnapMirror 的叢集間通訊工作階段
	TCP	11105.	叢集間 LIF	叢集間 LIF ONTAP	SnapMirror 資料傳輸
系統記錄	UDP	514	節點管理 LIF	系統記錄伺服器	系統記錄轉送訊息

HA 協調器外部安全群組的規則

針對此功能、預先定義 Cloud Volumes ONTAP 的外部安全群組包括下列傳入和傳出規則。

傳入規則

傳入規則的來源為 0.00.0.0/0 。

傳輸協定	連接埠	目的
SSH	22	SSH 連線至 HA 中介器
TCP	3000	從 Connector 進行 RESTful API 存取

傳出規則

HA 中介器的預先定義安全性群組會開啟所有傳出流量。如果可以接受、請遵循基本的傳出規則。如果您需要更嚴格的規則、請使用進階的傳出規則。

基本傳出規則

HA 中介器的預先定義安全性群組包括下列傳出規則。

傳輸協定	連接埠	目的
所有 TCP	全部	所有傳出流量
所有的 udp	全部	所有傳出流量

進階傳出規則

如果您需要嚴格的傳出流量規則、可以使用下列資訊、只開啟 HA 中介者傳出通訊所需的連接埠。

傳輸協定	連接埠	目的地	目的
HTTP	80	連接器 IP 位址	下載中介程式升級
HTTPS	443..	AWS API 服務	協助進行儲存容錯移轉
UDP	53.	AWS API 服務	協助進行儲存容錯移轉

您可以建立介面 VPC 端點、從目標子網路到 AWS EC2 服務、而非開啟連接埠 443 和 53 。

HA 中介器內部安全群組的規則

針對此功能、預先定義 Cloud Volumes ONTAP 的內部安全群組包含下列規則：Cloud Manager 一律會建立這個安全群組。您沒有使用自己的選項。

傳入規則

預先定義的安全性群組包含下列傳入規則。

傳輸協定	連接埠	目的
所有流量	全部	HA 中介器與 HA 節點之間的通訊

傳出規則

預先定義的安全性群組包括下列傳出規則。

傳輸協定	連接埠	目的
所有流量	全部	HA 中介器與 HA 節點之間的通訊

Connector 規則

Connector 的安全性群組需要傳入和傳出規則。

傳入規則

預先定義之安全性群組中的傳入規則來源為 0.00.0.0/0 。

傳輸協定	連接埠	目的
SSH	22	提供對 Connector 主機的 SSH 存取權
HTTP	80	提供從用戶端 Web 瀏覽器到本機使用者介面的 HTTP 存取、以及從 Cloud Compliance 建立的連線
HTTPS	443..	提供 HTTPS 存取、從用戶端網頁瀏覽器存取本機使用者介面
TCP	3128	如果您的 AWS 網路不使用 NAT 或 Proxy 、則可提供具有網際網路存取功能的 Cloud Compliance 執行個體

傳出規則

Connector 的預先定義安全性群組會開啟所有傳出流量。如果可以接受、請遵循基本的傳出規則。如果您需要更嚴格的規則、請使用進階的傳出規則。

基本傳出規則

Connector 的預先定義安全性群組包括下列傳出規則。

傳輸協定	連接埠	目的
所有 TCP	全部	所有傳出流量
所有的 udp	全部	所有傳出流量

進階傳出規則

如果您需要嚴格的傳出流量規則、可以使用下列資訊、僅開啟連接器傳出通訊所需的連接埠。

來源 IP 位址為 Connector 主機。

服務	傳輸協定	連接埠	目的地	目的
Active Directory	TCP	88	Active Directory 樹系	Kerberos V 驗證
	TCP	139.	Active Directory 樹系	NetBios 服務工作階段
	TCP	389	Active Directory 樹系	LDAP
	TCP	445	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	TCP	464.64	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	TCP	749	Active Directory 樹系	Active Directory Kerberos V 變更及設定密碼（ RPCSEC_GSS ）
	UDP	137.	Active Directory 樹系	NetBios 名稱服務
	UDP	138	Active Directory 樹系	NetBios 資料報服務
	UDP	464.64	Active Directory 樹系	Kerberos 金鑰管理
API 呼叫與 AutoSupport 功能	HTTPS	443..	傳出網際網路和 ONTAP 叢集管理 LIF	API 呼叫 AWS 和 ONTAP es供 、並傳送 AutoSupport 不只是功能的訊息給 NetApp
API 呼叫	TCP	3000	叢集管理 LIF ONTAP	API 呼叫 ONTAP 至
	TCP	8088	備份至 S3	API 呼叫備份至 S3
DNS	UDP	53.	DNS	用於 Cloud Manager 的 DNS 解析
雲端法規遵循	HTTP	80	雲端法規遵循執行個體	Cloud Compliance for Cloud Volumes ONTAP 解決此問題

設定 **AWS KMS**

如果您想搭配 Cloud Volumes ONTAP 使用 Amazon 加密搭配使用、則需要設定 AWS 金鑰管理服務（ KMS ）。

步驟

1. 確認存在作用中的客戶主金鑰（ CMK ）。

   CMK 可以是 AWS 託管的 CMK 、也可以是客戶託管的 CMK 。它可以與 Cloud Manager 及 Cloud Volumes ONTAP 其他 AWS 帳戶位於相同的 AWS 帳戶中、也可以位於不同的 AWS 帳戶中。

   "AWS 文件：客戶主要金鑰（ CMK ）"

2. 將 IAM 角色新增為 Cloud Manager 提供權限、做為 _key 使用者 _ 、以修改每個 CMK 的金鑰原則。

   將 IAM 角色新增為主要使用者、可讓 Cloud Manager 有權搭配 Cloud Volumes ONTAP 使用 CMK 。

   "AWS 文件：編輯金鑰"

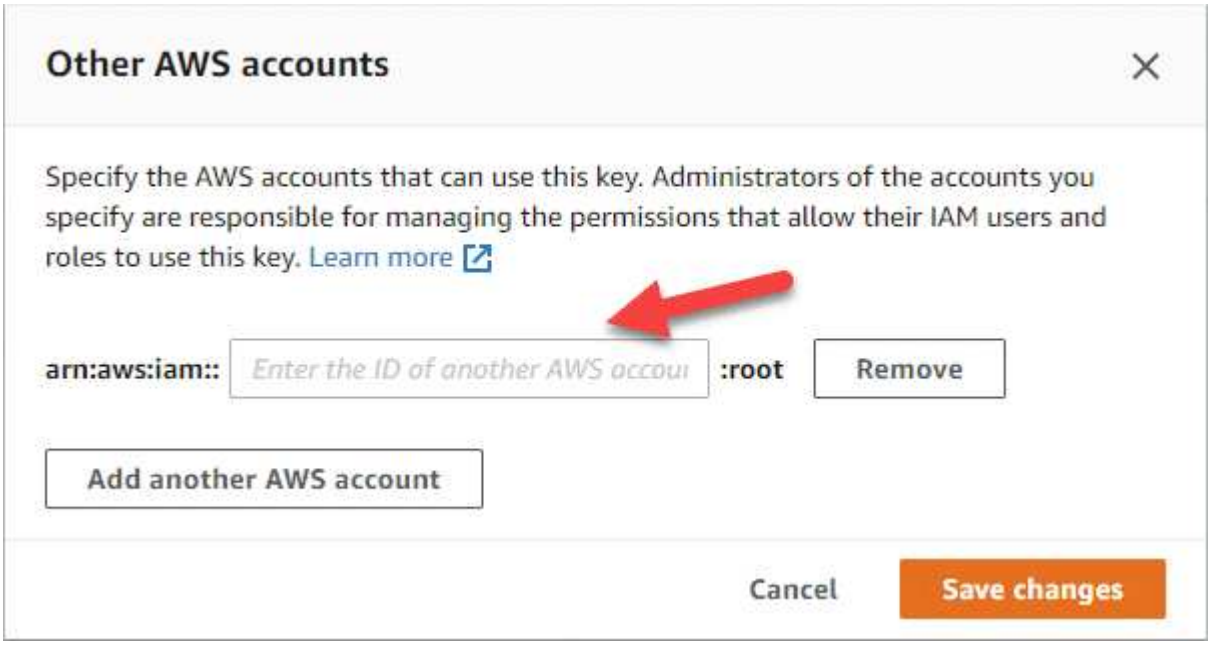
3. 如果 CMK 位於不同的 AWS 帳戶、請完成下列步驟：

   a. 從 CMK 所在的帳戶移至 KMS 主控台。
   b. 選取金鑰。
   c. 在「 * 一般組態 * 」窗格中、複製金鑰的 ARN 。

      建立 Cloud Volumes ONTAP 一套系統時、您必須提供 ARN 給 Cloud Manager 。

   d. 在 * 其他 AWS 帳戶 * 窗格中、新增提供 Cloud Manager 權限的 AWS 帳戶。

      在大多數情況下、這是 Cloud Manager 所在的帳戶。如果 AWS 中未安裝 Cloud Manager 、則您會將 AWS 存取金鑰提供給 Cloud Manager 。



   e. 現在請切換至 AWS 帳戶、該帳戶可為 Cloud Manager 提供權限、並開啟 IAM 主控台。
   f. 建立包含下列權限的 IAM 原則。
   g. 將原則附加至提供 Cloud Manager 權限的 IAM 角色或 IAM 使用者。

下列原則提供 Cloud Manager 從外部 AWS 帳戶使用 CMK 所需的權限。請務必修改「資源」區段中的區域和帳戶 ID 。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

+
如需此程序的其他詳細資料、請參閱 "AWS 文件：允許外部 AWS 帳戶存取 CMK"。

在 Cloud Volumes ONTAP AWS 中啟動

您可以 Cloud Volumes ONTAP 在單一系統組態中或 AWS 中以 HA 配對的形式啟動功能。

在 Cloud Volumes ONTAP AWS 中啟動單一節點的效能不整系統

如果您想 Cloud Volumes ONTAP 要在 AWS 中啟動功能、您需要在 Cloud Manager 中建立新的工作環境。

開始之前

- 您應該擁有 "與工作區相關的連接器"。

> 您必須是帳戶管理員才能建立 Connector 。當您建立第一個 Cloud Volumes ONTAP 運作環境時、如果您還沒有連接器、 Cloud Manager 會提示您建立連接器。

- "您應該隨時準備好讓 Connector 保持運作"。
- 您應該已做好準備、選擇組態、並從系統管理員取得 AWS 網路資訊。如需詳細資訊、請參閱 "規劃 Cloud Volumes ONTAP 您的需求組態"。
- 若要啟動 BYOL 系統、您必須擁有 20 位數的序號（授權金鑰）。
- 如果您想要使用 CIFS 、則必須設定 DNS 和 Active Directory 。如需詳細資訊、請參閱 "AWS 的網路需求 Cloud Volumes ONTAP"。

關於這項工作

建立工作環境之後、 Cloud Manager 會立即在指定的 VPC 中啟動測試執行個體、以驗證連線能力。如果成功、Cloud Manager 會立即終止執行個體、然後開始部署 Cloud Volumes ONTAP 該系統。如果 Cloud Manager 無法驗證連線能力、則無法建立工作環境。測試執行個體為 T2.奈 米（預設 VPC 租賃）或 m3.medium （專屬 VPC 租賃）。

步驟

1. 在「工作環境」頁面上、按一下「 * 新增工作環境 * 」、然後依照提示進行。
2. * 選擇位置 * ：選擇 * Amazon Web Services* 和 * Cloud Volumes ONTAP 《單一節點 * 》。
3. * 詳細資料與認證 * ：選擇性地變更 AWS 認證資料與訂閱、輸入工作環境名稱、視需要新增標記、然後輸入密碼。

   本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

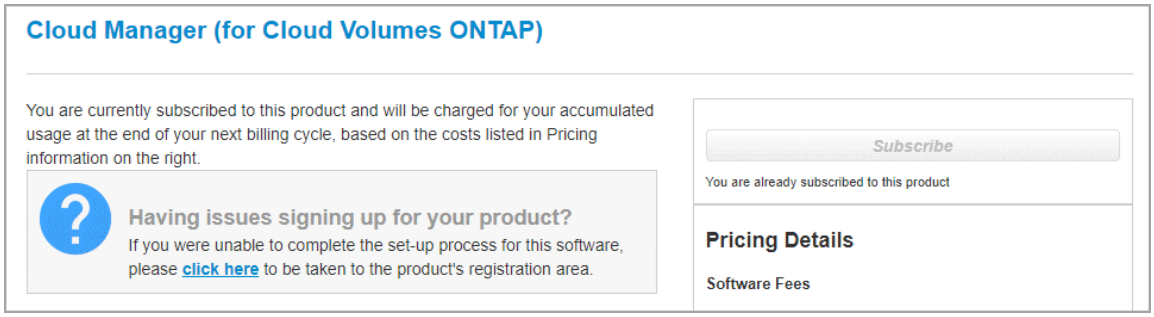
欄位	說明
工作環境名稱	Cloud Manager 會使用工作環境名稱來命名 Cloud Volumes ONTAP 支援系統和 Amazon EC2 執行個體。如果您選取該選項、它也會使用名稱做為預先定義安全性群組的前置詞。
新增標記	AWS 標籤是 AWS 資源的中繼資料。Cloud Manager 會將標記新增至 Cloud Volumes ONTAP 該執行個體、以及與該執行個體相關聯的每個 AWS 資源。建立工作環境時、您最多可以從使用者介面新增四個標記、然後在建立之後新增更多標記。請注意、在建立工作環境時、 API 不會限制您使用四個標記。如需標記的相關資訊、請參閱 "AWS 文件：標記 Amazon EC2 資源"。

欄位	說明
使用者名稱和密碼	這些是 Cloud Volumes ONTAP 適用於整個叢集管理帳戶的認證資料。您可以使用這些認證資料 Cloud Volumes ONTAP 、透過 OnCommand 「系統管理程式」或其 CLI 連線至功能驗證。
編輯認證資料	選擇 AWS 認證資料和市場訂閱、以搭配此 Cloud Volumes ONTAP 款功能系統使用。按一下 * 「新增訂閱」 * 、將選取的認證資料與訂閱建立關聯。若要建立隨用隨付 Cloud Volumes ONTAP 的功能性功能、您必須從 Cloud Volumes ONTAP AWS Marketplace 選取與訂閱功能相關的 AWS 認證資料。此訂閱將會針對 Cloud Volumes ONTAP 您所建立的每個更新版的 PAYGO 系統、以及您啟用的每個附加功能、向您收取費用。"瞭解如何將額外的 AWS 認證資料新增至 Cloud Manager"。

下列影片說明如何將隨用隨付服務市場訂閱與 AWS 認證資料建立關聯：

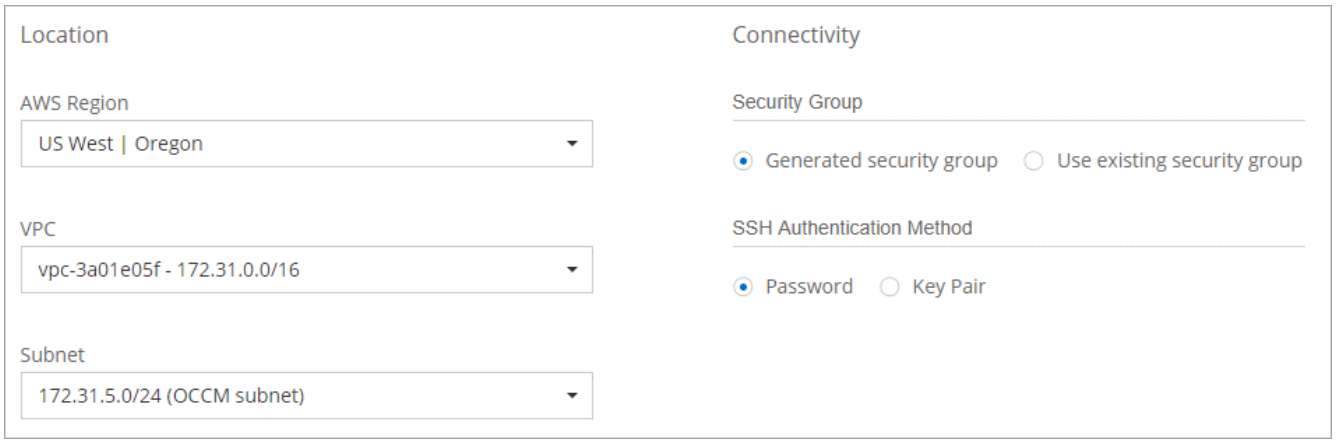
► https://docs.netapp.com/zh-tw/occm38//media/video_subscribing_aws.mp4 *(video)*

如果多位 IAM 使用者使用相同的 AWS 帳戶、則每位使用者都需要訂閱。第一位使用者訂閱之後、 AWS Marketplace 會通知後續使用者他們已經訂閱、如下圖所示。雖然 AWS *account* 已有訂閱、但每個 IAM 使用者都需要將自己與該訂閱建立關聯。如果您看到以下訊息、請按一下 * 按一下此處 * 連結、前往 Cloud Central 並完成程序。



4. * 服務 * ：啟用或停用 Cloud Volumes ONTAP 您不想搭配使用的個別服務。
   - "深入瞭解雲端法規遵循"。
   - "深入瞭解備份到雲端"。
   - "深入瞭解監控"。
5. * 位置與連線 * ：輸入您在 AWS 工作表中記錄的網路資訊。

   下圖顯示已填寫的頁面：



6. * 資料加密 * ：不選擇資料加密或 AWS 管理的加密。

   對於 AWS 管理的加密、您可以從帳戶或其他 AWS 帳戶中選擇不同的客戶主金鑰（ CMK ）。

   建立 Cloud Volumes ONTAP 一套系統後、您無法變更 AWS 資料加密方法。

   "瞭解如何設定 AWS KMS for Cloud Volumes ONTAP the 功能"。

   "深入瞭解支援的加密技術"。

7. * 授權與支援網站帳戶 * ：指定您要使用「隨用隨付」或「 BYOL 」、然後指定 NetApp 支援網站帳戶。

   若要瞭解授權的運作方式、請參閱 "授權"。

   NetApp 支援網站帳戶是隨用隨付的選項、但 BYOL 系統則為必填項目。 "瞭解如何新增 NetApp 支援網站帳戶"。

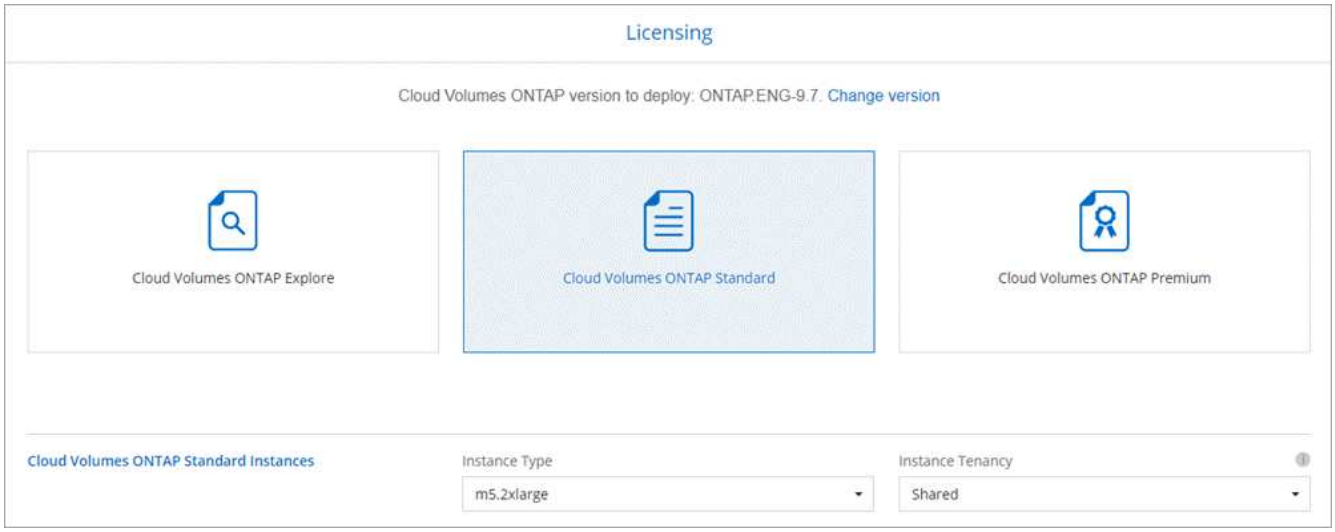
8. * 預先設定的套件 * ：選取其中一個套件以快速啟動 Cloud Volumes ONTAP 功能、或按一下 * 建立我自己的組態 * 。

   如果您選擇其中一個套件、則只需指定一個 Volume 、然後檢閱並核准組態。

9. * IAM 角色 * ：您應該保留預設選項、讓 Cloud Manager 為您建立角色。

   如果您偏好使用自己的原則、就必須符合 "有關節點的原則要求 Cloud Volumes ONTAP"。

10. * 授權 * ：視 Cloud Volumes ONTAP 需要變更版本、選取授權、執行個體類型及執行個體租賃。



如果您在啟動執行個體之後需要變更、您可以稍後修改授權或執行個體類型。

如果所選版本有較新的發行候選版本、一般可用度或修補程式版本、 Cloud Manager 會在建立工作環境時、將系統更新至該版本。例如、如果您選取 Cloud Volumes ONTAP 了「供應的是」「供應的是」「供應的是」「供應的」「供應的是」、就會進行更新。更新不會從一個版本發生到另一個版本、例如從 9.6 到 9.7 。

11. * 基礎儲存資源 * ：選擇初始 Aggregate 的設定：磁碟類型、每個磁碟的大小、以及是否應啟用資料分層。

    請注意下列事項：

    - 磁碟類型適用於初始磁碟區。您可以為後續磁碟區選擇不同的磁碟類型。
    - 磁碟大小適用於初始 Aggregate 中的所有磁碟、以及 Cloud Manager 在使用簡易資源配置選項時所建立的任何其他集合體。您可以使用進階配置選項、建立使用不同磁碟大小的集合體。

      如需選擇磁碟類型和大小的說明、請參閱 "在 AWS 中調整系統規模"。

    - 您可以在建立或編輯磁碟區時、選擇特定的磁碟區分層原則。
    - 如果停用資料分層、您可以在後續的 Aggregate 上啟用。

      "瞭解資料分層的運作方式"。

12. * 寫入速度與 WORM * ：選擇 * 正常 * 或 * 高速 * 寫入速度、並視需要啟動一次寫入、多次讀取（ WORM ）儲存設備。

    只有單一節點系統才支援選擇寫入速度。

    "深入瞭解寫入速度"。

    如果資料分層已啟用、則無法啟用 WORM 。

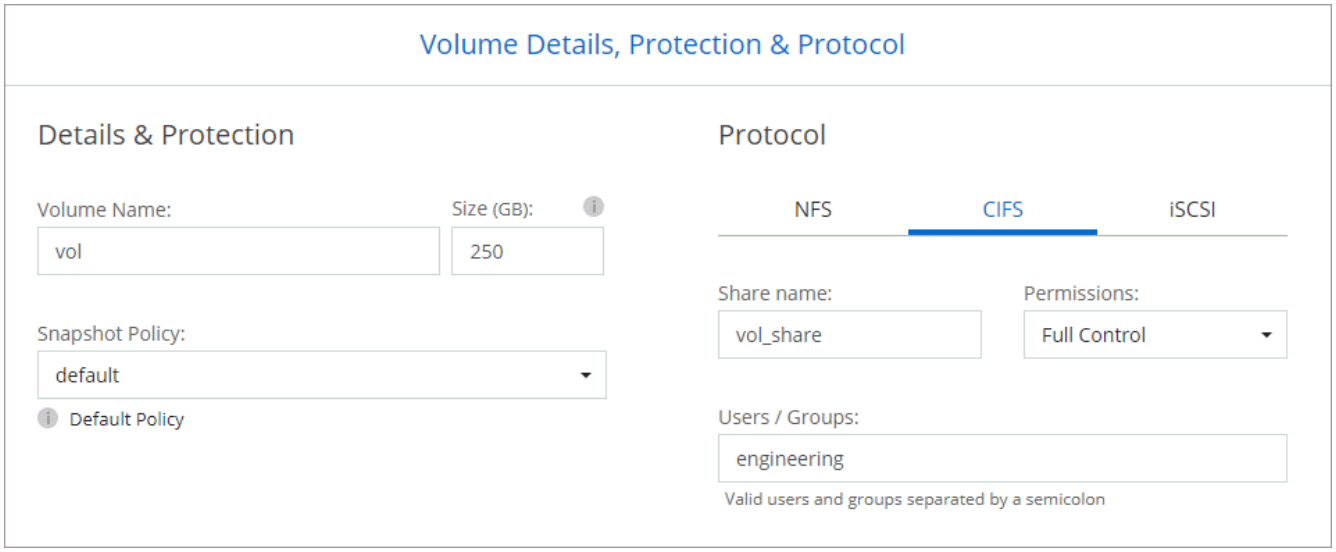
    "深入瞭解 WORM 儲存設備"。

13. * 建立 Volume * ：輸入新磁碟區的詳細資料、或按一下 * 跳過 * 。

    本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

欄位	說明
尺寸	您可以輸入的最大大小、主要取決於您是否啟用精簡配置、這可讓您建立比目前可用實體儲存容量更大的磁碟區。
存取控制（僅適用於 NFS ）	匯出原則會定義子網路中可存取磁碟區的用戶端。根據預設、 Cloud Manager 會輸入一個值、讓您存取子網路中的所有執行個體。
權限與使用者 / 群組（僅限 CIFS ）	這些欄位可讓您控制使用者和群組（也稱為存取控制清單或 ACL ）的共用存取層級。您可以指定本機或網域 Windows 使用者或群組、或 UNIX 使用者或群組。如果您指定網域 Windows 使用者名稱、則必須使用網域 \ 使用者名稱格式來包含使用者的網域。
Snapshot 原則	Snapshot 複製原則會指定自動建立的 NetApp Snapshot 複本的頻率和數量。NetApp Snapshot 複本是一種不影響效能的時間點檔案系統映像、需要最少的儲存容量。您可以選擇預設原則或無。您可以針對暫時性資料選擇「無」：例如、 Microsoft SQL Server 的 Tempdb 。
進階選項（僅適用於 NFS ）	為磁碟區選取 NFS 版本： NFSv3 或 NFSv3 。
啟動器群組和 IQN （僅適用於 iSCSI ）	iSCSI 儲存目標稱為 LUN （邏輯單元）、以標準區塊裝置的形式呈現給主機。啟動器群組是 iSCSI 主機節點名稱的表格、可控制哪些啟動器可存取哪些 LUN 。iSCSI 目標可透過標準乙太網路介面卡（ NIC ）、 TCP 卸載引擎（ TOE ）卡（含軟體啟動器）、整合式網路介面卡（ CNA ）或專用主機匯流排介面卡（ HBA ）連線至網路、並由 iSCSI 合格名稱（ IQN ）識別。建立 iSCSI Volume 時、 Cloud Manager 會自動為您建立 LUN 。我們只要在每個磁碟區建立一個 LUN 、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 "使用 IQN 從主機連線至 LUN"。

下圖顯示 CIFS 傳輸協定的「 Volume 」（磁碟區）頁面：



14. * CIFS 設定 * ：如果您選擇 CIFS 傳輸協定、請設定 CIFS 伺服器。

欄位	說明
DNS 主要和次要 IP 位址	提供 CIFS 伺服器名稱解析的 DNS 伺服器 IP 位址。列出的 DNS 伺服器必須包含所需的服務位置記錄（ SRV), 才能找到 CIFS 伺服器要加入之網域的 Active Directory LDAP 伺服器和網域控制器。

欄位	說明
要加入的 Active Directory 網域	您要 CIFS 伺服器加入之 Active Directory （ AD ）網域的 FQDN 。
授權加入網域的認證資料	具有足夠權限的 Windows 帳戶名稱和密碼、可將電腦新增至 AD 網域內的指定組織單位（ OU ）。
CIFS 伺服器 NetBios 名稱	AD 網域中唯一的 CIFS 伺服器名稱。
組織單位	AD 網域中與 CIFS 伺服器相關聯的組織單位。預設值為「 CN= 電腦」。如果您將 AWS 託管 Microsoft AD 設定為 AD 伺服器 Cloud Volumes ONTAP 以供使用、您應該在此欄位中輸入 * OID=computers,O=corp* 。
DNS 網域	適用於整個儲存虛擬 Cloud Volumes ONTAP 機器（ SVM ）的 DNS 網域。在大多數情況下、網域與 AD 網域相同。
NTP 伺服器	選擇 * 使用 Active Directory 網域 * 來使用 Active Directory DNS 設定 NTP 伺服器。如果您需要使用不同的位址來設定 NTP 伺服器、則應該使用 API 。請參閱 "Cloud Manager API 開發人員指南" 以取得詳細資料。

15. * 使用率設定檔、磁碟類型及分層原則 * ：視需要選擇是否要啟用儲存效率功能、並編輯磁碟區分層原則。

    如需詳細資訊、請參閱 "瞭解 Volume 使用量設定檔" 和 "資料分層總覽"。

16. * 審查與核准 * ：檢閱並確認您的選擇。
    a. 檢閱組態的詳細資料。
    b. 按一下 * 更多資訊 * 以檢閱 Cloud Manager 將購買的支援與 AWS 資源詳細資料。
    c. 選取「 * 我瞭解 … * 」核取方塊。
    d. 按一下「 * 執行 * 」。

結果

Cloud Manager 會啟動 Cloud Volumes ONTAP 此功能。您可以追蹤時間表的進度。

如果您在啟動 Cloud Volumes ONTAP 該實例時遇到任何問題、請檢閱故障訊息。您也可以選取工作環境、然後按一下重新建立環境。

如需其他協助、請前往 "NetApp Cloud Volumes ONTAP 支援"。

完成後

- 如果您已配置 CIFS 共用區、請授予使用者或群組檔案和資料夾的權限、並確認這些使用者可以存取共用區並建立檔案。
- 如果您要將配額套用至磁碟區、請使用 System Manager 或 CLI 。

  配額可讓您限制或追蹤使用者、群組或 qtree 所使用的磁碟空間和檔案數量。

在 **Cloud Volumes ONTAP AWS** 中啟動一個「叢集 **HA** 配對」

如果您想要在 Cloud Volumes ONTAP AWS 中啟動一個「叢集 HA 配對」、就必須在 Cloud Manager 中建立 HA 工作環境。

開始之前

- 您應該擁有 "與工作區相關的連接器"。

> 您必須是帳戶管理員才能建立 Connector 。當您建立第一個 Cloud Volumes ONTAP 運作環境時、如果您還沒有連接器、 Cloud Manager 會提示您建立連接器。

- "您應該隨時準備好讓 Connector 保持運作"。
- 您應該已做好準備、選擇組態、並從系統管理員取得 AWS 網路資訊。如需詳細資訊、請參閱 "規劃 Cloud Volumes ONTAP 您的需求組態"。
- 如果您購買 BYOL 授權、則每個節點都必須有 20 位數的序號（授權金鑰）。
- 如果您想要使用 CIFS 、則必須設定 DNS 和 Active Directory 。如需詳細資訊、請參閱 "AWS 的網路需求 Cloud Volumes ONTAP"。

限制

目前 AWS out貼 文不支援 HA 配對。

關於這項工作

建立工作環境之後、 Cloud Manager 會立即在指定的 VPC 中啟動測試執行個體、以驗證連線能力。如果成功、Cloud Manager 會立即終止執行個體、然後開始部署 Cloud Volumes ONTAP 該系統。如果 Cloud Manager 無法驗證連線能力、則無法建立工作環境。測試執行個體為 T2.奈 米（預設 VPC 租賃）或 m3.medium （專屬 VPC 租賃）。

步驟

1. 在「工作環境」頁面上、按一下「 * 新增工作環境 * 」、然後依照提示進行。
2. * 選擇位置 * ：選擇 * Amazon Web Services* 和 * Cloud Volumes ONTAP 《單一節點 * 》。
3. * 詳細資料與認證 * ：選擇性地變更 AWS 認證資料與訂閱、輸入工作環境名稱、視需要新增標記、然後輸入密碼。

   本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

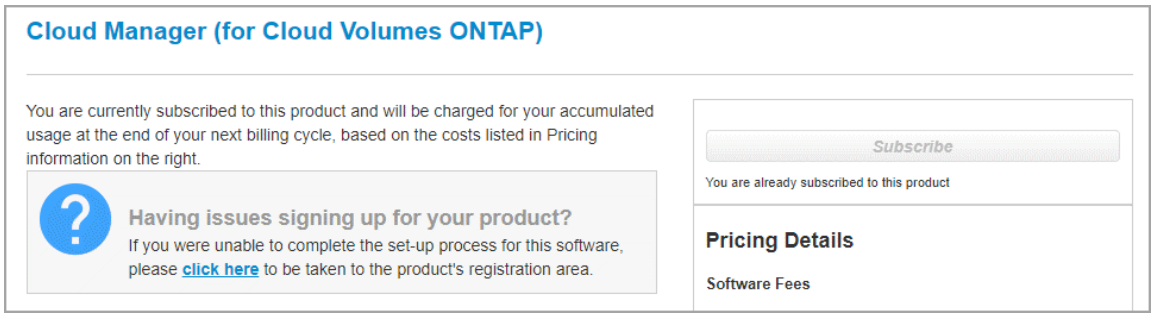
欄位	說明
工作環境名稱	Cloud Manager 會使用工作環境名稱來命名 Cloud Volumes ONTAP 支援系統和 Amazon EC2 執行個體。如果您選取該選項、它也會使用名稱做為預先定義安全性群組的前置詞。
新增標記	AWS 標籤是 AWS 資源的中繼資料。Cloud Manager 會將標記新增至 Cloud Volumes ONTAP 該執行個體、以及與該執行個體相關聯的每個 AWS 資源。建立工作環境時、您最多可以從使用者介面新增四個標記、然後在建立之後新增更多標記。請注意、在建立工作環境時、 API 不會限制您使用四個標記。如需標記的相關資訊、請參閱 "AWS 文件：標記 Amazon EC2 資源"。
使用者名稱和密碼	這些是 Cloud Volumes ONTAP 適用於整個叢集管理帳戶的認證資料。您可以使用這些認證資料 Cloud Volumes ONTAP 、透過 OnCommand 「系統管理程式」或其 CLI 連線至功能驗證。

欄位	說明
編輯認證資料	選擇 AWS 認證資料和市場訂閱、以搭配此 Cloud Volumes ONTAP 款功能系統使用。按一下 * 「新增訂閱」 * 、將選取的認證資料與訂閱建立關聯。若要建立隨用隨付 Cloud Volumes ONTAP 的功能性功能、您必須從 Cloud Volumes ONTAP AWS Marketplace 選取與訂閱功能相關的 AWS 認證資料。此訂閱將會針對 Cloud Volumes ONTAP 您所建立的每個更新版的 PAYGO 系統、以及您啟用的每個附加功能、向您收取費用。"瞭解如何將額外的 AWS 認證資料新增至 Cloud Manager"。

下列影片說明如何將隨用隨付服務市場訂閱與 AWS 認證資料建立關聯：

► https://docs.netapp.com/zh-tw/occm38//media/video_subscribing_aws.mp4 *(video)*

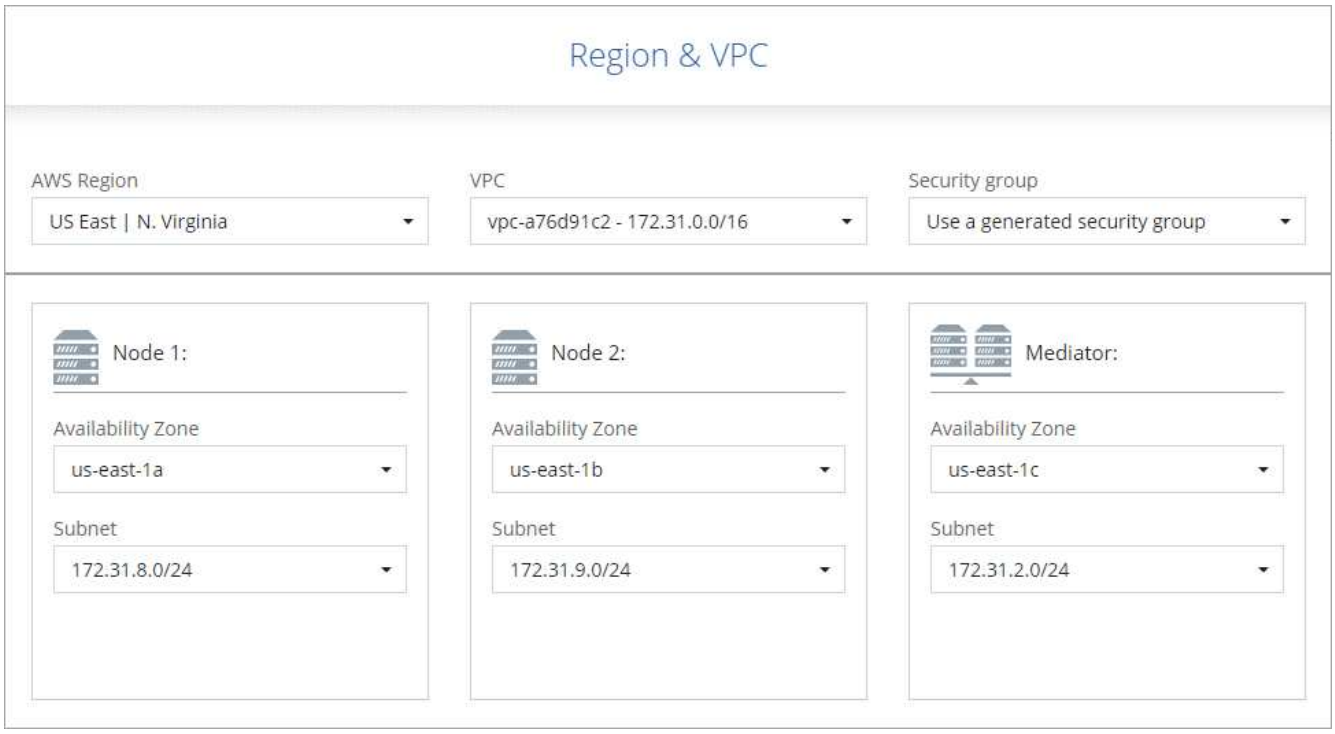
如果多位 IAM 使用者使用相同的 AWS 帳戶、則每位使用者都需要訂閱。第一位使用者訂閱之後、 AWS Marketplace 會通知後續使用者他們已經訂閱、如下圖所示。雖然 AWS *account* 已有訂閱、但每個 IAM 使用者都需要將自己與該訂閱建立關聯。如果您看到以下訊息、請按一下 * 按一下此處 * 連結、前往 Cloud Central 並完成程序。



4. * 服務 * ：讓服務保持啟用或停用您不想搭配 Cloud Volumes ONTAP 此作業系統使用的個別服務。
   - "深入瞭解雲端法規遵循"。
   - "深入瞭解備份到雲端"。
   - "深入瞭解監控"。
5. * HA 部署模式 * ：選擇 HA 組態。

   如需部署模型的總覽、請參閱 "適用於 AWS 的 HA Cloud Volumes ONTAP"。
6. * 地區與 VPC* ：輸入您在 AWS 工作表中記錄的網路資訊。

   下圖顯示為多個 AZ 組態填寫的頁面：



7. * 連線能力與 SSH 驗證 * ：選擇 HA 配對與中介器的連線方法。
8. * 浮動 IPS* ：如果您選擇多個 AZs 、請指定浮動 IP 位址。

   該地區所有 VPC 的 IP 位址必須位於 CIDR 區塊之外。如需其他詳細資料、請參閱 "AWS 在 Cloud Volumes ONTAP 多個 AZs 中的功能需求"。

9. * 路由表 * ：如果您選擇多個 AZs 、請選取應包含浮動 IP 位址路由的路由表。

   如果您有多個路由表、請務必選取正確的路由表。否則、部分用戶端可能無法存取 Cloud Volumes ONTAP 此功能配對。如需路由表的詳細資訊、請參閱 "AWS 文件：路由表"。

10. * 資料加密 * ：不選擇資料加密或 AWS 管理的加密。

    對於 AWS 管理的加密、您可以從帳戶或其他 AWS 帳戶中選擇不同的客戶主金鑰（ CMK ）。

    建立 Cloud Volumes ONTAP 一套系統後、您無法變更 AWS 資料加密方法。

    "瞭解如何設定 AWS KMS for Cloud Volumes ONTAP the 功能"。

    "深入瞭解支援的加密技術"。

11. * 授權與支援網站帳戶 * ：指定您要使用「隨用隨付」或「 BYOL 」、然後指定 NetApp 支援網站帳戶。

    若要瞭解授權的運作方式、請參閱 "授權"。

    NetApp 支援網站帳戶是隨用隨付的選項、但 BYOL 系統則為必填項目。 "瞭解如何新增 NetApp 支援網站帳戶"。

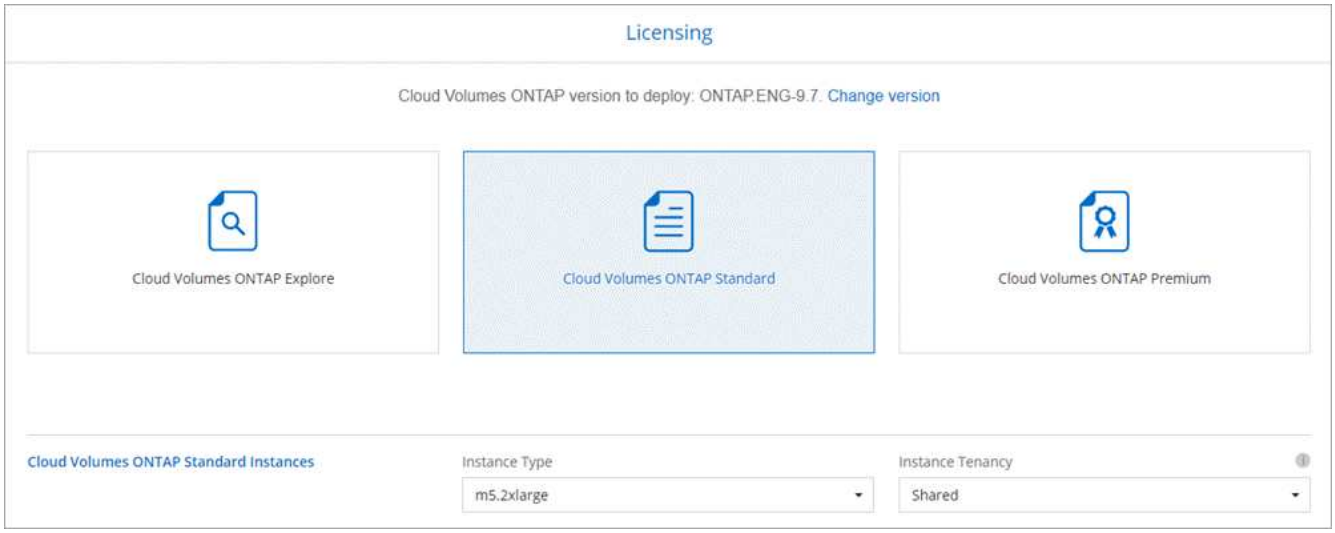
12. * 預先設定的套件 * ：選取其中一個套件以快速啟動 Cloud Volumes ONTAP 某個作業系統、或按一下 * 建立我自己的組態 * 。

如果您選擇其中一個套件、則只需指定一個 Volume 、然後檢閱並核准組態。

13. * IAM 角色 * ：您應該保留預設選項、讓 Cloud Manager 為您建立角色。

    如果您偏好使用自己的原則、就必須符合 "有關節點和 HA 中介器的原則要求 Cloud Volumes ONTAP"。

14. * 授權 * ：視 Cloud Volumes ONTAP 需要變更版本、選取授權、執行個體類型及執行個體租賃。



    如果您在啟動執行個體之後需要變更、您可以稍後修改授權或執行個體類型。

    如果所選版本有較新的發行候選版本、一般可用度或修補程式版本、 Cloud Manager 會在建立工作環境時、將系統更新至該版本。例如、如果您選取 Cloud Volumes ONTAP 了「供應的是」「供應的是」「供應的是」「供應的」「供應的是」、就會進行更新。更新不會從一個版本發生到另一個版本、例如從 9.6 到 9.7 。

15. * 基礎儲存資源 * ：選擇初始 Aggregate 的設定：磁碟類型、每個磁碟的大小、以及是否應啟用資料分層。

    請注意下列事項：

    - 磁碟類型適用於初始磁碟區。您可以為後續磁碟區選擇不同的磁碟類型。
    - 磁碟大小適用於初始 Aggregate 中的所有磁碟、以及 Cloud Manager 在使用簡易資源配置選項時所建立的任何其他集合體。您可以使用進階配置選項、建立使用不同磁碟大小的集合體。

      如需選擇磁碟類型和大小的說明、請參閱 "在 AWS 中調整系統規模"。

    - 您可以在建立或編輯磁碟區時、選擇特定的磁碟區分層原則。
    - 如果停用資料分層、您可以在後續的 Aggregate 上啟用。

      "瞭解資料分層的運作方式"。

16. * WORM * ：視需要啟動一次寫入、多次讀取（ WORM ）儲存設備。

    如果資料分層已啟用、則無法啟用 WORM 。

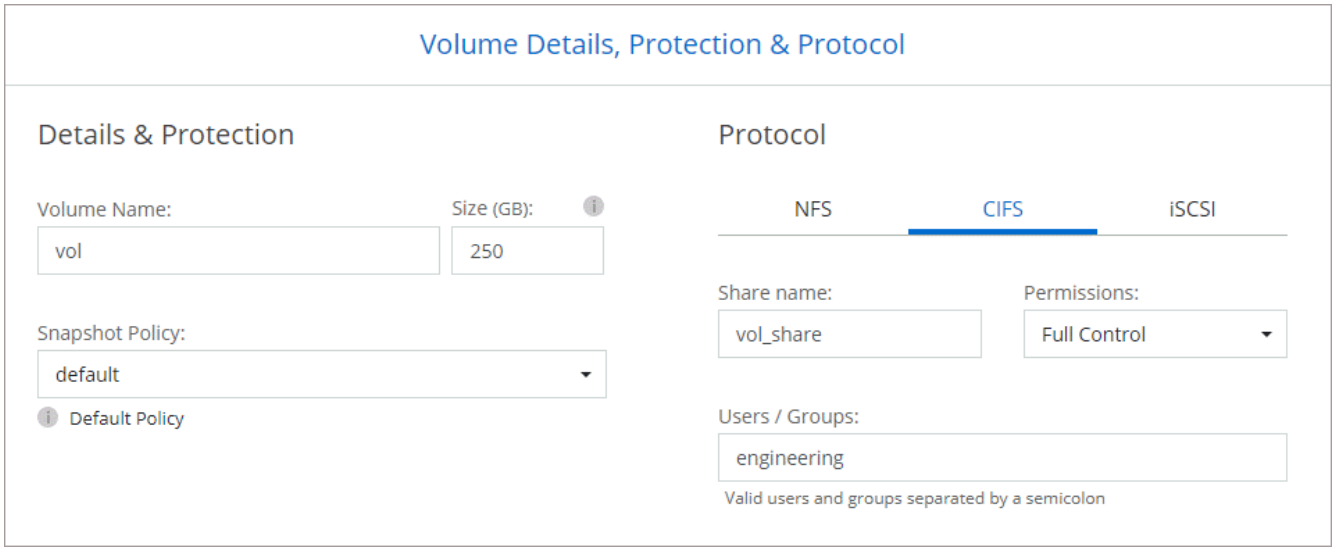
    "深入瞭解 WORM 儲存設備"。

17. * 建立 Volume * ：輸入新磁碟區的詳細資料、或按一下 * 跳過 * 。

本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

欄位	說明
尺寸	您可以輸入的最大大小、主要取決於您是否啟用精簡配置、這可讓您建立比目前可用實體儲存容量更大的磁碟區。
存取控制（僅適用於 NFS ）	匯出原則會定義子網路中可存取磁碟區的用戶端。根據預設、 Cloud Manager 會輸入一個值、讓您存取子網路中的所有執行個體。
權限與使用者 / 群組（僅限 CIFS ）	這些欄位可讓您控制使用者和群組（也稱為存取控制清單或 ACL ）的共用存取層級。您可以指定本機或網域 Windows 使用者或群組、或 UNIX 使用者或群組。如果您指定網域 Windows 使用者名稱、則必須使用網域 \ 使用者名稱格式來包含使用者的網域。
Snapshot 原則	Snapshot 複製原則會指定自動建立的 NetApp Snapshot 複本的頻率和數量。NetApp Snapshot 複本是一種不影響效能的時間點檔案系統映像、需要最少的儲存容量。您可以選擇預設原則或無。您可以針對暫時性資料選擇「無」：例如、 Microsoft SQL Server 的 Tempdb 。
進階選項（僅適用於 NFS ）	為磁碟區選取 NFS 版本： NFSv3 或 NFSv3 。
啟動器群組和 IQN （僅適用於 iSCSI ）	iSCSI 儲存目標稱為 LUN （邏輯單元）、以標準區塊裝置的形式呈現給主機。啟動器群組是 iSCSI 主機節點名稱的表格、可控制哪些啟動器可存取哪些 LUN 。iSCSI 目標可透過標準乙太網路介面卡（ NIC ）、 TCP 卸載引擎（ TOE ）卡（含軟體啟動器）、整合式網路介面卡（ CNA ）或專用主機匯流排介面卡（ HBA ）連線至網路、並由 iSCSI 合格名稱（ IQN ）識別。建立 iSCSI Volume 時、 Cloud Manager 會自動為您建立 LUN 。我們只要在每個磁碟區建立一個 LUN 、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 "使用 IQN 從主機連線至 LUN"。

下圖顯示 CIFS 傳輸協定的「 Volume 」（磁碟區）頁面：



18. * CIFS 設定 * ：如果您選取 CIFS 傳輸協定、請設定 CIFS 伺服器。

欄位	說明
DNS 主要和次要 IP 位址	提供 CIFS 伺服器名稱解析的 DNS 伺服器 IP 位址。列出的 DNS 伺服器必須包含所需的服務位置記錄（ SRV), 才能找到 CIFS 伺服器要加入之網域的 Active Directory LDAP 伺服器和網域控制器。
要加入的 Active Directory 網域	您要 CIFS 伺服器加入之 Active Directory （ AD ）網域的 FQDN 。
授權加入網域的認證資料	具有足夠權限的 Windows 帳戶名稱和密碼、可將電腦新增至 AD 網域內的指定組織單位（ OU ）。
CIFS 伺服器 NetBios 名稱	AD 網域中唯一的 CIFS 伺服器名稱。
組織單位	AD 網域中與 CIFS 伺服器相關聯的組織單位。預設值為「 CN= 電腦」。如果您將 AWS 託管 Microsoft AD 設定為 AD 伺服器 Cloud Volumes ONTAP 以供使用、您應該在此欄位中輸入 * OID=computers,O=corp* 。
DNS 網域	適用於整個儲存虛擬 Cloud Volumes ONTAP 機器（ SVM ）的 DNS 網域。在大多數情況下、網域與 AD 網域相同。
NTP 伺服器	選擇 * 使用 Active Directory 網域 * 來使用 Active Directory DNS 設定 NTP 伺服器。如果您需要使用不同的位址來設定 NTP 伺服器、則應該使用 API 。請參閱 "Cloud Manager API 開發人員指南" 以取得詳細資料。

19. * 使用率設定檔、磁碟類型及分層原則 * ：視需要選擇是否要啟用儲存效率功能、並編輯磁碟區分層原則。

    如需詳細資訊、請參閱 "瞭解 Volume 使用量設定檔" 和 "資料分層總覽"。

20. * 審查與核准 * ：檢閱並確認您的選擇。
    a. 檢閱組態的詳細資料。
    b. 按一下 * 更多資訊 * 以檢閱 Cloud Manager 將購買的支援與 AWS 資源詳細資料。
    c. 選取「 * 我瞭解 … * 」核取方塊。
    d. 按一下「 * 執行 * 」。

結果

Cloud Manager 會啟動 Cloud Volumes ONTAP 「叢集式 HA 配對」。您可以追蹤時間表的進度。

如果您在啟動 HA 配對時遇到任何問題、請檢閱故障訊息。您也可以選取工作環境、然後按一下重新建立環境。

如需其他協助、請前往 "NetApp Cloud Volumes ONTAP 支援"。

完成後

- 如果您已配置 CIFS 共用區、請授予使用者或群組檔案和資料夾的權限、並確認這些使用者可以存取共用區並建立檔案。
- 如果您要將配額套用至磁碟區、請使用 System Manager 或 CLI 。

  配額可讓您限制或追蹤使用者、群組或 qtree 所使用的磁碟空間和檔案數量。

開始使用 **Azure**

Azure 版的功能入門 **Cloud Volumes ONTAP**

只要幾個步驟、 Cloud Volumes ONTAP 就能開始使用適用於 Azure 的功能。

建立連接器

如果您沒有 "連接器" 然而、帳戶管理員需要建立一個帳戶。 "瞭解如何在 Azure 中建立 Connector"。

當您建立第一個 Cloud Volumes ONTAP 運作環境時、如果您還沒有連接器、 Cloud Manager 會提示您部署連接器。

規劃您的組態

Cloud Manager 提供符合工作負載需求的預先設定套件、您也可以建立自己的組態。如果您選擇自己的組態、應該瞭解可用的選項。 "深入瞭解"。

設定您的網路

1. 確保您的 Vnet 和子網路可支援連接器與 Cloud Volumes ONTAP 支援的連接功能。
2. 啟用從目標 vnet 的傳出網際網路存取、讓 Connector 和 Cloud Volumes ONTAP 支援中心能夠連絡多個端點。

   這個步驟很重要、因為連接器 Cloud Volumes ONTAP 無法在沒有外傳網際網路存取的情況下管理不穩定。如果您需要限制傳出連線、請參閱的端點清單 "Connector 與 Cloud Volumes ONTAP the"。

"深入瞭解網路需求"。

使用 **Cloud Manager** 啟動 **Cloud Volumes ONTAP**

按一下「 * 新增工作環境 * 」、選取您要部署的系統類型、然後完成精靈中的步驟。 "閱讀逐步指示"。

相關連結

- "評估"
- "從 Cloud Manager 建立 Connector"
- "從 Azure Marketplace 建立 Connector"
- "在 Linux 主機上安裝 Connector 軟體"
- "Cloud Manager 具備 Azure 權限的功能"

規劃 **Cloud Volumes ONTAP Azure** 的不一樣組態

在 Cloud Volumes ONTAP Azure 中部署時、您可以選擇符合工作負載需求的預先設定系統、也可以自行建立組態。如果您選擇自己的組態、應該瞭解可用的選項。

選擇授權類型

提供兩種定價選項：隨用隨付及自帶授權（ BYOL） Cloud Volumes ONTAP 。若為隨用隨付、您可以從三種授權中選擇： Explore 、 Standard 或 Premium 。每個授權都提供不同的容量和運算選項。

"Azure支援的支援功能組態Cloud Volumes ONTAP"

瞭解儲存限制

一個不含資源的系統的原始容量上限 Cloud Volumes ONTAP 與授權有關。其他限制會影響集合體和磁碟區的大小。在規劃組態時、您應該注意這些限制。

"Azure中的儲存限制Cloud Volumes ONTAP"

在 **Azure** 中調整系統規模

調整 Cloud Volumes ONTAP 您的支援規模、有助於滿足效能與容量的需求。在選擇 VM 類型、磁碟類型和磁碟大小時、您應該注意幾個關鍵點：

虛擬機器類型

請查看中支援的虛擬機器類型 "發行說明 Cloud Volumes ONTAP" 然後檢閱每種受支援 VM 類型的詳細資料。請注意、每種 VM 類型都支援特定數量的資料磁碟。

- "Azure 文件：通用虛擬機器大小"
- "Azure 文件：記憶體最佳化的虛擬機器大小"

Azure 磁碟類型

當您建立 Cloud Volumes ONTAP 用於實現效能不均的磁碟區時、您需要選擇 Cloud Volumes ONTAP 底層的雲端儲存設備、以利將其用作磁碟。

HA 系統使用優質網頁。同時、單一節點系統可使用兩種 Azure 託管磁碟：

- _Premium SSD 託管磁碟 _ 以更高的成本、為 I/O 密集的工作負載提供高效能。
- _ 標準 SSD 託管磁碟 _ 為需要低 IOPS 的工作負載提供一致的效能。
- 如果您不需要高 IOPS 、而且想要降低成本、那麼 _ 標準 HDD 託管磁碟 _ 是個不錯的選擇。

  如需這些磁碟使用案例的其他詳細資料、請參閱 "Microsoft Azure 文件： Azure 提供哪些磁碟類型？"。

Azure 磁碟大小

啟動 Cloud Volumes ONTAP 時、您必須選擇集合體的預設磁碟大小。Cloud Manager 會將此磁碟大小用於初始 Aggregate 、以及使用簡易資源配置選項時所建立的任何其他 Aggregate 。您可以建立使用不同於預設磁碟大小的 Aggregate "使用進階配置選項"。

集合體中的所有磁碟大小必須相同。

在選擇磁碟大小時、您應該考量幾個因素。磁碟大小會影響您支付的儲存成本、您可以在集合體中建立的磁碟區大小、 Cloud Volumes ONTAP 可供使用的總容量、以及儲存效能。

Azure Premium Storage 的效能與磁碟大小有關。較大的磁碟可提供較高的 IOPS 和處理量。例如、選擇 1 TB 磁碟可提供比 500 GB 磁碟更好的效能、而且成本更高。

標準儲存設備的磁碟大小沒有效能差異。您應該根據所需的容量來選擇磁碟大小。

請參閱 Azure 、瞭解每個磁碟大小的 IOPS 與處理量：

- "Microsoft Azure ：託管磁碟定價"
- "Microsoft Azure ：網頁 Blobs 定價"

選擇支援 **Flash Cache** 的組態

Azure 中的一個支援本地 NVMe 儲存設備的組態、可將其用作 _Flash Cache 以獲得更好的效能。 Cloud Volumes ONTAP Cloud Volumes ONTAP "深入瞭解 Flash Cache"。

Azure 網路資訊工作表

在 Cloud Volumes ONTAP Azure 中部署時、您需要指定虛擬網路的詳細資料。您可以使用工作表向系統管理員收集資訊。

Azure 資訊	您的價值
區域	
虛擬網路（ vnet ）	
子網路	
網路安全群組（如果使用您自己的）	

選擇寫入速度

Cloud Manager可讓您選擇單一節點Cloud Volumes ONTAP 的寫入速度設定。在您選擇寫入速度之前、您應該先瞭解一般與高設定之間的差異、以及使用高速寫入速度時的風險與建議。

正常寫入速度與高速寫入速度之間的差異

當您選擇正常寫入速度時、資料會直接寫入磁碟、因此可降低發生非計畫性系統中斷時發生資料遺失的可能性。

選擇高速寫入速度時、資料會在寫入磁碟之前先緩衝到記憶體中、以提供更快的寫入效能。由於這種快取、如果發生非計畫性的系統中斷、可能會導致資料遺失。

發生非計畫性系統中斷時可能遺失的資料量、是最後兩個一致點的範圍。一致點是將緩衝資料寫入磁碟的行為。寫入日誌已滿或 10 秒後（以先到者為準）、就會出現一致點。然而、AWS EBS Volume效能可能會影響一致點處理時間。

何時使用高速寫入

如果您的工作負載需要快速寫入效能、而且在非計畫性的系統中斷時、您可以承受資料遺失的風險、那麼高速寫入速度是很好的選擇。

使用高速寫入速度時的建議事項

如果啟用高速寫入、則應確保應用程式層的寫入保護。

選擇 **Volume** 使用設定檔

包含多項儲存效率功能、可減少您所需的總儲存容量。 ONTAP在 Cloud Manager 中建立 Volume 時、您可以選擇啟用這些功能的設定檔、或是停用這些功能的設定檔。您應該深入瞭解這些功能、以協助您決定要使用的設定檔。

NetApp 儲存效率功能提供下列效益：

資源隨需配置

為主機或使用者提供比實體儲存資源池實際擁有更多的邏輯儲存設備。儲存空間不會預先配置儲存空間、而是會在寫入資料時動態分配給每個磁碟區。

重複資料刪除

找出相同的資料區塊、並以單一共用區塊的參考資料取代這些區塊、藉此提升效率。這項技術可消除位於同一個磁碟區的備援資料區塊、進而降低儲存容量需求。

壓縮

藉由壓縮主儲存設備、次儲存設備和歸檔儲存設備上磁碟區內的資料、來減少儲存資料所需的實體容量。

在**Cloud Volumes ONTAP Azure**中部署及管理功能的網路需求

設定您的 Azure 網路、 Cloud Volumes ONTAP 使其能夠正常運作。這包括連接器和 Cloud Volumes ONTAP 整個過程的網路功能。

需求 **Cloud Volumes ONTAP**

Azure 必須符合下列網路需求。

輸出網際網路存取 **Cloud Volumes ONTAP** 功能

支援向 NetApp 支援部門傳送訊息、以便主動監控儲存設備的健全狀況。 Cloud Volumes ONTAP AutoSupport

路由和防火牆原則必須允許將 HTTP / HTTPS 流量傳送至下列端點、 Cloud Volumes ONTAP 才能讓下列端點傳送 AutoSupport 動態訊息：

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

"瞭解如何設定 AutoSupport 功能"。

安全性群組

您不需要建立安全性群組、因為 Cloud Manager 會為您建立安全性群組。如果您需要使用自己的安全性群組規則、請參閱下列安全性群組規則。

IP 位址數

Cloud Manager 會將下列 IP 位址分配給 Cloud Volumes ONTAP Azure 中的功能：

- 單一節點： 5 個 IP 位址
- HA 配對： 16 個 IP 位址

請注意、 Cloud Manager 會在 HA 配對上建立 SVM 管理 LIF 、但不會在 Azure 中的單一節點系統上建立。

LIF 是與實體連接埠相關聯的 IP 位址。諸如 VMware 的管理工具需要 SVM 管理 LIF SnapCenter 。

從邊到 **Azure Blob** 儲存設備的連線 **Cloud Volumes ONTAP** 、可用於資料分層

如果您想要將冷資料分層至 Azure Blob 儲存設備、只要 Cloud Manager 具備必要的權限、就不需要在效能層與容量層之間建立連線。如果 Cloud Manager 原則具有下列權限、 Cloud Manager 可為您啟用 vnet 服務端點：

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

這些權限包含在最新版本中 "Cloud Manager 原則"。

如需設定資料分層的詳細資訊、請參閱 "將冷資料分層至低成本物件儲存設備"。

連線 **ONTAP** 至其他網路中的不二系統

若要在 Cloud Volumes ONTAP Azure 中的某個更新系統與 ONTAP 其他網路中的其他更新系統之間複寫資料、您必須在 Azure vnet 與其他網路（例如 AWS VPC 或公司網路）之間建立 VPN 連線。

如需相關指示、請參閱 "Microsoft Azure 文件：在 Azure 入口網站中建立站台對站台連線"。

連接器需求

設定您的網路、讓 Connector 能夠管理公有雲環境中的資源和程序。最重要的步驟是確保從網際網路存取各種端點。

如果您的網路使用 Proxy 伺服器來進行所有與網際網路的通訊、您可以從「設定」頁面指定 Proxy 伺服器。請參閱 "將 Connector 設定為使用 Proxy 伺服器"。

連線至目標網路

連接器需要網路連線至您要部署 Cloud Volumes ONTAP 的 VPC 和 VNets 。

例如、如果您在公司網路中安裝 Connector 、則必須設定 VPN 連線至 VPC 或 vnet 、以便在其中啟動 Cloud Volumes ONTAP 更新。

連接器需要存取傳出網際網路、才能管理公有雲環境中的資源和程序。在 Azure 中管理資源時、 Connector 會聯絡下列端點：

端點	目的
https://management.azure.com https://login.microsoftonline.com	讓 Cloud Manager 能夠在 Cloud Volumes ONTAP 大多數 Azure 地區部署及管理功能。
https://management.microsoftazure.de https://login.microsoftonline.de	讓 Cloud Manager 能夠在 Cloud Volumes ONTAP Azure Germany 地區部署及管理功能。
https://management.usgovcloudapi.net https://login.microsoftonline.com	讓 Cloud Manager 能夠在 Cloud Volumes ONTAP Azure US Gov 地區部署及管理功能。
https://api.services.cloud.netapp.com:443	API 要求 NetApp Cloud Central 。
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	提供軟體映像、資訊清單和範本的存取權限。
https://repo.cloud.support.netapp.com	用於下載Cloud Manager相依性。
http://repo.mysql.com/	用於下載MySQL。
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	讓Cloud Manager能夠存取及下載資訊清單、範本及Cloud Volumes ONTAP 升級影像。
https://cloudmanagerinfraprod.azurecr.io	存取執行 Docker 之基礎架構的容器元件軟體映像、並提供與 Cloud Manager 整合服務的解決方案。
https://kinesis.us-east-1.amazonaws.com	讓 NetApp 能夠從稽核記錄串流資料。
https://cloudmanager.cloud.netapp.com	與 Cloud Manager 服務（包括 Cloud Central 帳戶）進行通訊。
https://netapp-cloud-account.auth0.com	與 NetApp Cloud Central 通訊、以進行集中式使用者驗證。
https://mysupport.netapp.com	與 NetApp AutoSupport 通訊
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	與 NetApp 溝通以取得系統授權與支援登錄。
https://ipa-signer.cloudmanager.netapp.com	讓 Cloud Manager 能夠產生授權（例如 FlexCache 、針對 Cloud Volumes ONTAP 功能不全的
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	需要將Cloud Volumes ONTAP 支援的系統與Kubernetes叢集連線。端點可安裝NetApp Trident。
* .blob.core.windows.net	使用 Proxy 時 HA 配對必須具備此功能。

端點	目的
各種協力廠商位置、例如： • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org 第三方據點可能會有所變更。	在升級期間、 Cloud Manager 會針對協力廠商相依性下載最新的套件。

雖然您應該從 SaaS 使用者介面執行幾乎所有的工作、但連接器上仍有本機使用者介面可供使用。執行 Web 瀏覽器的機器必須連線至下列端點：

端點	目的
連接器主機	您必須從網頁瀏覽器輸入主機的 IP 位址、才能載入 Cloud Manager 主控台。 視您與雲端供應商的連線能力而定、您可以使用指派給主機的私有 IP 或公有 IP ： • 如果您有 VPN 並直接連線至虛擬網路、則私有 IP 可正常運作 • 公有 IP 適用於任何網路情境 無論如何、您應該確保安全群組規則僅允許從授權的 IP 或子網路存取、以確保網路存取安全。
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	您的網頁瀏覽器會連線至這些端點、以便透過 NetApp Cloud Central 進行集中式使用者驗證。
https://widget.intercom.io	產品內對談可讓您與 NetApp 雲端專家交談。

安全性群組規則 **Cloud Volumes ONTAP**

Cloud Manager 會建立 Azure 安全性群組、其中包括 Cloud Volumes ONTAP 需要順利運作的傳入和傳出規則。您可能需要參照連接埠進行測試、或是偏好使用自己的安全性群組。

適用於此功能的安全性群組 Cloud Volumes ONTAP 需要傳入和傳出規則。

單一節點系統的傳入規則

下列規則會允許流量、除非說明中註明會封鎖特定的傳入流量。

優先順序和名稱	連接埠與傳輸協定	來源與目的地	說明
1000 inbound SSH	22 TCP	任意	SSH 存取叢集管理 LIF 的 IP 位址或節點管理 LIF

優先順序和名稱	連接埠與傳輸協定	來源與目的地	說明
1001 inbound http	80 TCP	任意	使用叢集管理 LIF 的 IP 位址、以 HTTP 存取 System Manager Web 主控台
1002inbound （入站）_111_TCP	111 TCP	任意	遠端程序需要 NFS
1003 inbound _111_udp	111 udp	任意	遠端程序需要 NFS
1004 inbound （傳入）_139	139 TCP	任意	CIFS 的 NetBios 服務工作階段
1005inbound （傳入）_161-162 _tcp	161-162 TCP	任意	簡單的網路管理傳輸協定
1006 inbound （傳入）_161-162 _udp	161-162 udp	任意	簡單的網路管理傳輸協定
1007 inbound _443	443 TCP	任意	使用叢集管理 LIF 的 IP 位址、以 HTTPS 存取 System Manager 網路主控台
1008 inbound _445	445 TCP	任意	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
1009 inbound _6335_tcp	635 TCP	任意	NFS 掛載
1010 inbound _6335_udp	635 udp	任意	NFS 掛載
1011 inbound （傳入）_749	749 TCP	任意	Kerberos
1012 inbound _2049_tcp	2049 TCP	任意	NFS 伺服器精靈
1013 inbound _2049_udp	2049 udp	任意	NFS 伺服器精靈
1014 inbound （傳入）_3260	3260 TCP	任意	透過 iSCSI 資料 LIF 存取 iSCSI
1015 inbound _4045-4046_tcp	4045-4046 TCP	任意	NFS 鎖定精靈和網路狀態監控
1016 inbound _4045-4046_udp	4045-4046 udp	任意	NFS 鎖定精靈和網路狀態監控
1017 inbound _10000	10000 TCP	任意	使用 NDMP 備份
1018 inbound （傳入）_11104-11105	11104-11105 TCP	任意	SnapMirror 資料傳輸
3000 inbound 拒絕_all_tcp	任何連接埠 TCP	任意	封鎖所有其他 TCP 傳入流量
3001 inbound 拒絕_all_udp	任何連接埠 udp	任意	封鎖所有其他的 UDP 傳入流量
65000 AllowVnetInBound	任何連接埠任何傳輸協定	虛擬網路至虛擬網路	來自 vnet 的傳入流量

優先順序和名稱	連接埠與傳輸協定	來源與目的地	說明
65001 AllowAzureLoad BalancerInBound	任何連接埠任何傳輸協定	將 AzureLoadBalancer 移至任何	Azure Standard 負載平衡器的資料流量
65500 DenyAllInBound	任何連接埠任何傳輸協定	任意	封鎖所有其他傳入流量

HA 系統的傳入規則

下列規則會允許流量、除非說明中註明會封鎖特定的傳入流量。

HA 系統的傳入規則少於單一節點系統、因為傳入資料流量會流經 Azure Standard Load Balancer 。因此、來自負載平衡器的流量應開啟、如「 AllowAzureLoadBalancerInBound 」規則所示。

優先順序和名稱	連接埠與傳輸協定	來源與目的地	說明
100 inbound （傳入） _443	443 任何傳輸協定	任意	使用叢集管理 LIF 的 IP 位址、以 HTTPS 存取 System Manager 網路主控台
101 inbound （傳入） _111_TCP	111 任何傳輸協定	任意	遠端程序需要 NFS
102 inbound _2049_tcp	2049 任何傳輸協定	任意	NFS 伺服器精靈
111 inbound （傳入） _ssh	22 任何傳輸協定	任意	SSH 存取叢集管理 LIF 的 IP 位址或節點管理 LIF
121inbound （傳入） _53	53 任何傳輸協定	任意	DNS 與 CIFS
65000 AllowVnetInBound	任何連接埠任何傳輸協定	虛擬網路至虛擬網路	來自 vnet 的傳入流量
65001 AllowAzureLoad BalancerInBound	任何連接埠任何傳輸協定	將 AzureLoadBalancer 移至任何	Azure Standard 負載平衡器的資料流量
65500 DenyAllInBound	任何連接埠任何傳輸協定	任意	封鎖所有其他傳入流量

傳出規則

預先定義 Cloud Volumes ONTAP 的 Security Group for the 旅行團會開啟所有的傳出流量。如果可以接受、請遵循基本的傳出規則。如果您需要更嚴格的規則、請使用進階的傳出規則。

基本傳出規則

適用於此功能的預先定義安全性群組 Cloud Volumes ONTAP 包括下列傳出規則。

連接埠	傳輸協定	目的
全部	所有 TCP	所有傳出流量
全部	所有的 udp	所有傳出流量

進階傳出規則

如果您需要嚴格的傳出流量規則、可以使用下列資訊、僅開啟 Cloud Volumes ONTAP 那些由真人進行傳出通訊

所需的連接埠。

來源是 Cloud Volumes ONTAP 指在整個系統上的介面（ IP 位址）。

服務	連接埠	傳輸協定	來源	目的地	目的
Active Directory	88	TCP	節點管理 LIF	Active Directory 樹系	Kerberos V 驗證
	137.	UDP	節點管理 LIF	Active Directory 樹系	NetBios 名稱服務
	138	UDP	節點管理 LIF	Active Directory 樹系	NetBios 資料報服務
	139.	TCP	節點管理 LIF	Active Directory 樹系	NetBios 服務工作階段
	389	TCP 與 UDP	節點管理 LIF	Active Directory 樹系	LDAP
	445	TCP	節點管理 LIF	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	464.64	TCP	節點管理 LIF	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	464.64	UDP	節點管理 LIF	Active Directory 樹系	Kerberos 金鑰管理
	749	TCP	節點管理 LIF	Active Directory 樹系	Kerberos V 變更與設定密碼（ RPCSEC_GSS ）
	88	TCP	資料 LIF （ NFS 、 CIFS 、 iSCSI ）	Active Directory 樹系	Kerberos V 驗證
	137.	UDP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 名稱服務
	138	UDP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 資料報服務
	139.	TCP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 服務工作階段
	389	TCP 與 UDP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	LDAP
	445	TCP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	464.64	TCP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	464.64	UDP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos 金鑰管理
	749	TCP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos V 變更及設定密碼（ RPCSEC_GSS ）
DHCP	68	UDP	節點管理 LIF	DHCP	第一次設定的 DHCP 用戶端
DHCPS	67	UDP	節點管理 LIF	DHCP	DHCP 伺服器

服務	連接埠	傳輸協定	來源	目的地	目的
DNS	53.	UDP	節點管理 LIF 與資料 LIF （ NFS 、 CIFS ）	DNS	DNS
NDMP	18600 – 18699	TCP	節點管理 LIF	目的地伺服器	NDMP 複本
SMTP	25	TCP	節點管理 LIF	郵件伺服器	可以使用 SMTP 警示 AutoSupport 來執行功能
SNMP	161.	TCP	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	161.	UDP	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	162%	TCP	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	162%	UDP	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
SnapMirror	11104.	TCP	叢集間 LIF	叢集間 LIF ONTAP	管理 SnapMirror 的叢集間通訊工作階段
	11105.	TCP	叢集間 LIF	叢集間 LIF ONTAP	SnapMirror 資料傳輸
系統記錄	514	UDP	節點管理 LIF	系統記錄伺服器	系統記錄轉送訊息

Connector 的安全群組規則

Connector 的安全性群組需要傳入和傳出規則。

傳入規則

預先定義之安全性群組中的傳入規則來源為 0.00.0.0/0 。

連接埠	傳輸協定	目的
22	SSH	提供對 Connector 主機的 SSH 存取權
80	HTTP	提供從用戶端 Web 瀏覽器到本機使用者介面的 HTTP 存取
443..	HTTPS	提供 HTTPS 存取、從用戶端網頁瀏覽器存取本機使用者介面

傳出規則

Connector 的預先定義安全性群組會開啟所有傳出流量。如果可以接受、請遵循基本的傳出規則。如果您需要更嚴格的規則、請使用進階的傳出規則。

基本傳出規則

Connector 的預先定義安全性群組包括下列傳出規則。

連接埠	傳輸協定	目的
全部	所有 TCP	所有傳出流量
全部	所有的 udp	所有傳出流量

進階傳出規則

如果您需要嚴格的傳出流量規則、可以使用下列資訊、僅開啟連接器傳出通訊所需的連接埠。

來源 IP 位址為 Connector 主機。

服務	連接埠	傳輸協定	目的地	目的
Active Directory	88	TCP	Active Directory 樹系	Kerberos V 驗證
	139.	TCP	Active Directory 樹系	NetBios 服務工作階段
	389	TCP	Active Directory 樹系	LDAP
	445	TCP	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	464.64	TCP	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	749	TCP	Active Directory 樹系	Active Directory Kerberos V 變更及設定密碼（ RPCSEC_GSS ）
	137.	UDP	Active Directory 樹系	NetBios 名稱服務
	138	UDP	Active Directory 樹系	NetBios 資料報服務
	464.64	UDP	Active Directory 樹系	Kerberos 金鑰管理
API 呼叫與 AutoSupport 功能	443..	HTTPS	傳出網際網路和 ONTAP 叢集管理 LIF	API 呼叫 AWS 和 ONTAP es供 、並傳送 AutoSupport 不只是功能的訊息給 NetApp
API 呼叫	3000	TCP	叢集管理 LIF ONTAP	API 呼叫 ONTAP 至
DNS	53.	UDP	DNS	用於 Cloud Manager 的 DNS 解析

在 **Cloud Volumes ONTAP Azure** 中啟動

您可以 Cloud Volumes ONTAP 在 Cloud Manager 中建立運作不正常的環境、在 Azure 中啟動單一節點系統或 HA 配對。

開始之前

- 您應該擁有 "與工作區相關的連接器"。

> 您必須是帳戶管理員才能建立 Connector 。當您建立第一個 Cloud Volumes ONTAP 運作環境時、如果您還沒有連接器、 Cloud Manager 會提示您建立連接器。

- "您應該隨時準備好讓 Connector 保持運作"。
- 您應該已經選擇組態、並從系統管理員取得 Azure 網路資訊。如需詳細資訊、請參閱 "規劃 Cloud Volumes ONTAP 您的需求組態"。
- 若要部署 BYOL 系統、您需要每個節點的 20 位數序號（授權金鑰）。

關於這項工作

Cloud Manager Cloud Volumes ONTAP 在 Azure 中建立一套功能完善的系統時、會建立多個 Azure 物件、例如資源群組、網路介面和儲存帳戶。您可以在精靈結束時檢閱資源摘要。

> 資料遺失的可能性
>
> 由於資料遺失的風險、不建議在 Cloud Volumes ONTAP 現有的共享資源群組中部署此功能。使用 API 部署至現有資源群組時、目前預設會停用復原功能、但刪除 Cloud Volumes ONTAP 功能可能會刪除該共用群組中的其他資源。
>
> 最佳實務做法是使用全新的資源群組 Cloud Volumes ONTAP 來進行支援。從 Cloud Volumes ONTAP Cloud Manager 在 Azure 中部署時、這是預設且唯一建議的選項。

步驟

1. 在「工作環境」頁面上、按一下「 * 新增工作環境 * 」、然後依照提示進行。
2. * 選擇位置 * ：選擇 * Microsoft Azure * 與 * Cloud Volumes ONTAP 《單一節點 * 》或 * Cloud Volumes ONTAP 《高可用度 * 》。
3. * 詳細資料與認證 * ：選擇性變更 Azure 認證與訂閱、指定叢集名稱與資源群組名稱、視需要新增標記、然後指定認證。

   下表說明您可能需要指導的欄位：

欄位	說明
工作環境名稱	Cloud Manager 會使用工作環境名稱來命名 Cloud Volumes ONTAP 整個系統、以及 Azure 虛擬機器。如果您選取該選項、它也會使用名稱做為預先定義安全性群組的前置詞。
資源群組名稱	保留新資源群組的預設名稱、或取消核取 * 使用預設 * 、然後輸入您自己的新資源群組名稱。最佳實務做法是使用全新的資源群組 Cloud Volumes ONTAP 來進行支援。雖然 Cloud Volumes ONTAP 可以使用 API 在現有的共享資源群組中部署功能不實、但由於資料遺失的風險、不建議這麼做。如需詳細資料、請參閱上述警告。
標記	標記是 Azure 資源的中繼資料。當您在此欄位中輸入標記時、 Cloud Manager 會將標記新增至與 Cloud Volumes ONTAP 該系統相關聯的資源群組。建立工作環境時、您最多可以從使用者介面新增四個標記、然後在建立之後新增更多標記。請注意、在建立工作環境時、 API 不會限制您使用四個標記。如需標記的相關資訊、請參閱 "Microsoft Azure 說明文件：使用標籤來組織 Azure 資源"。

欄位	說明
使用者名稱和密碼	這些是 Cloud Volumes ONTAP 適用於整個叢集管理帳戶的認證資料。您可以使用這些認證資料 Cloud Volumes ONTAP 、透過 OnCommand 「系統管理程式」或其 CLI 連線至功能驗證。
[[video ）] 編輯認證資料	您可以選擇不同的 Azure 認證資料和其他 Azure 訂閱、以搭配此 Cloud Volumes ONTAP 款作業系統使用。您必須將 Azure Marketplace 訂閱與所選 Azure 訂閱建立關聯、才能部署隨用隨付 Cloud Volumes ONTAP 的功能。 "瞭解如何新增認證"。

下列影片說明如何將 Marketplace 訂閱與 Azure 訂閱建立關聯：

► https://docs.netapp.com/zh-tw/occm38//media/video_subscribing_azure.mp4 *(video)*

4. * 服務 * ：啟用或停用 Cloud Volumes ONTAP 您不想搭配使用的個別服務。
   - "深入瞭解雲端法規遵循"。
   - "深入瞭解備份到雲端"。
5. 位置與連線：選取位置與安全性群組、然後選取核取方塊、確認Cloud Manager與目標位置之間的網路連線。
6. * 授權與支援網站帳戶 * ：指定您要使用「隨用隨付」或「 BYOL 」、然後指定 NetApp 支援網站帳戶。

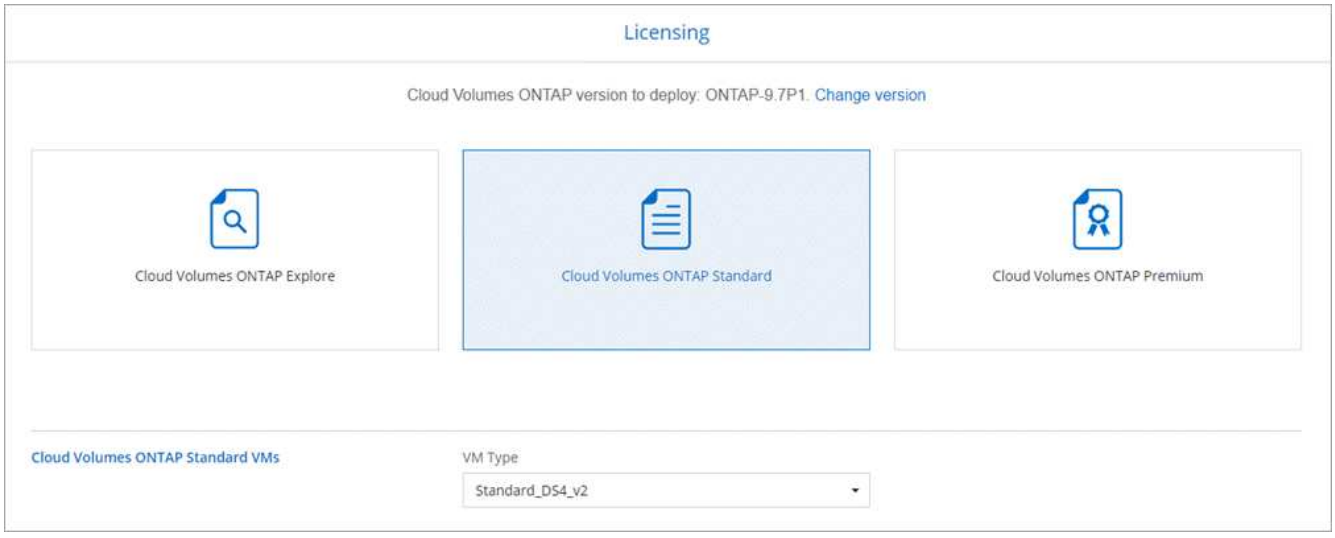
   若要瞭解授權的運作方式、請參閱 "授權"。

   NetApp 支援網站帳戶是隨用隨付的選項、但 BYOL 系統則為必填項目。 "瞭解如何新增 NetApp 支援網站帳戶"。

7. * 預先設定的套件 * ：選取其中一個套件以快速部署 Cloud Volumes ONTAP 某個作業系統、或按一下 * 建立我自己的組態 * 。

   如果您選擇其中一個套件、則只需指定一個 Volume 、然後檢閱並核准組態。

8. * 授權 * ：視 Cloud Volumes ONTAP 需要變更版本、選取授權、然後選取虛擬機器類型。



如果您在啟動系統之後需要變更、您可以稍後修改授權或虛擬機器類型。

如果所選版本有較新的發行候選版本、一般可用度或修補程式版本、 Cloud Manager 會在建立工作環境時、將系統更新至該版本。例如、如果您選取 Cloud Volumes ONTAP 了「供應的是」「供應的是」「供應的是」「供應的」「供應的是」、就會進行更新。更新不會從一個版本發生到另一個版本、例如從 9.6 到 9.7 。

9. * 從 Azure Marketplace 訂閱 * ：如果 Cloud Manager 無法以程式設計方式部署 Cloud Volumes ONTAP 功能、請依照下列步驟進行。
10. * 基礎儲存資源 * ：選擇初始 Aggregate 的設定：磁碟類型、每個磁碟的大小、以及是否應啟用資料分層至 Blob 儲存設備。

    請注意下列事項：

    - 磁碟類型適用於初始磁碟區。您可以為後續磁碟區選擇不同的磁碟類型。
    - 磁碟大小適用於初始 Aggregate 中的所有磁碟、以及 Cloud Manager 在使用簡易資源配置選項時所建立的任何其他集合體。您可以使用進階配置選項、建立使用不同磁碟大小的集合體。

      如需選擇磁碟類型和大小的說明、請參閱 "在 Azure 中調整系統規模"。

    - 您可以在建立或編輯磁碟區時、選擇特定的磁碟區分層原則。
    - 如果停用資料分層、您可以在後續的 Aggregate 上啟用。

      "深入瞭解資料分層"。

11. * 寫入速度與 WORM * （僅限單節點系統）：選擇 * 正常 * 或 * 高速 * 寫入速度、並視需要啟動一次寫入、多次讀取（ WORM ）儲存設備。

    只有單一節點系統才支援選擇寫入速度。

    "深入瞭解寫入速度"。

    如果資料分層已啟用、則無法啟用 WORM 。

    "深入瞭解 WORM 儲存設備"。

12. * 安全通訊至儲存設備與 WORM * （僅限 HA ）：選擇是否啟用 HTTPS 連線至 Azure 儲存帳戶、並視需要啟動一次寫入、多次讀取（ WORM ）儲存設備。

    HTTPS 連線是 Cloud Volumes ONTAP 從一個名為「支援速度」的鏈接至 Azure 儲存帳戶。請注意、啟用此選項可能會影響寫入效能。您無法在建立工作環境之後變更設定。

    "深入瞭解 WORM 儲存設備"。

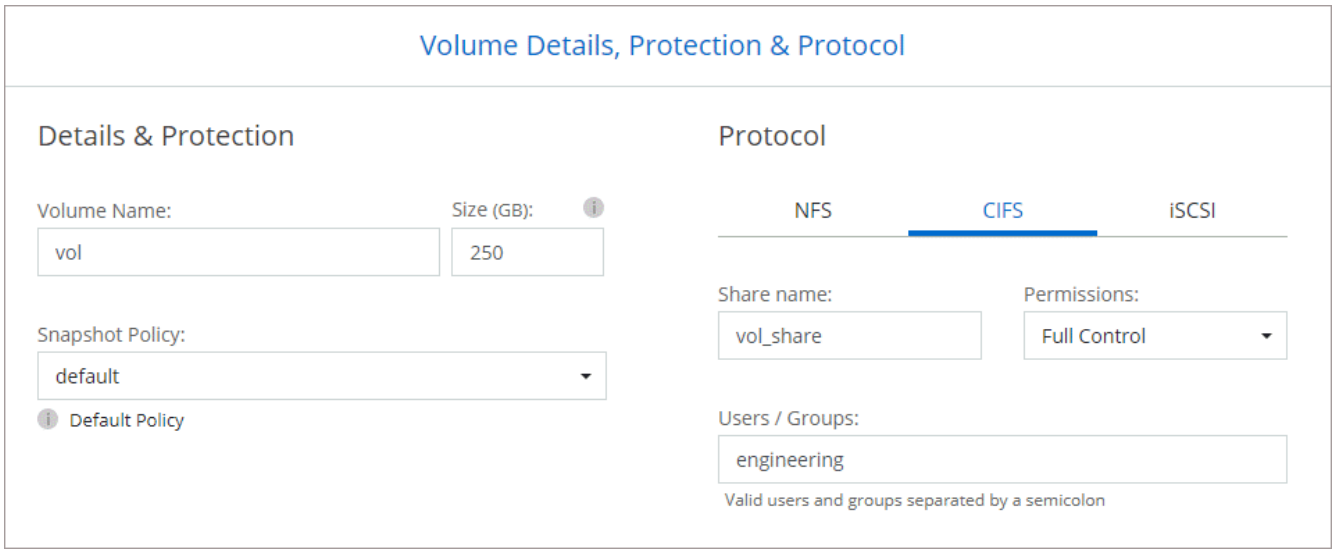
13. * 建立 Volume * ：輸入新磁碟區的詳細資料、或按一下 * 跳過 * 。

    本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

欄位	說明
尺寸	您可以輸入的最大大小、主要取決於您是否啟用精簡配置、這可讓您建立比目前可用實體儲存容量更大的磁碟區。

欄位	說明
存取控制（僅適用於 NFS ）	匯出原則會定義子網路中可存取磁碟區的用戶端。根據預設、 Cloud Manager 會輸入一個值、讓您存取子網路中的所有執行個體。
權限與使用者 / 群組（僅限 CIFS ）	這些欄位可讓您控制使用者和群組（也稱為存取控制清單或 ACL ）的共用存取層級。您可以指定本機或網域 Windows 使用者或群組、或 UNIX 使用者或群組。如果您指定網域 Windows 使用者名稱、則必須使用網域 \ 使用者名稱格式來包含使用者的網域。
Snapshot 原則	Snapshot 複製原則會指定自動建立的 NetApp Snapshot 複本的頻率和數量。NetApp Snapshot 複本是一種不影響效能的時間點檔案系統映像、需要最少的儲存容量。您可以選擇預設原則或無。您可以針對暫時性資料選擇「無」：例如、 Microsoft SQL Server 的 Tempdb 。
進階選項（僅適用於 NFS ）	為磁碟區選取 NFS 版本： NFSv3 或 NFSv3 。
啟動器群組和 IQN （僅適用於 iSCSI ）	iSCSI 儲存目標稱為 LUN （邏輯單元）、以標準區塊裝置的形式呈現給主機。啟動器群組是 iSCSI 主機節點名稱的表格、可控制哪些啟動器可存取哪些 LUN 。iSCSI 目標可透過標準乙太網路介面卡（ NIC ）、 TCP 卸載引擎（ TOE ）卡（含軟體啟動器）、整合式網路介面卡（ CNA ）或專用主機匯流排介面卡（ HBA ）連線至網路、並由 iSCSI 合格名稱（ IQN ）識別。建立 iSCSI Volume 時、 Cloud Manager 會自動為您建立 LUN 。我們只要在每個磁碟區建立一個 LUN 、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 "使用 IQN 從主機連線至 LUN"。

下圖顯示 CIFS 傳輸協定的「 Volume 」（磁碟區）頁面：



14. * CIFS 設定 * ：如果您選擇 CIFS 傳輸協定、請設定 CIFS 伺服器。

欄位	說明
DNS 主要和次要 IP 位址	提供 CIFS 伺服器名稱解析的 DNS 伺服器 IP 位址。列出的 DNS 伺服器必須包含所需的服務位置記錄（ SRV), 才能找到 CIFS 伺服器要加入之網域的 Active Directory LDAP 伺服器和網域控制器。
要加入的 Active Directory 網域	您要 CIFS 伺服器加入之 Active Directory （ AD ）網域的 FQDN 。

欄位	說明
授權加入網域的認證資料	具有足夠權限的 Windows 帳戶名稱和密碼、可將電腦新增至 AD 網域內的指定組織單位（ OU ）。
CIFS 伺服器 NetBios 名稱	AD 網域中唯一的 CIFS 伺服器名稱。
組織單位	AD 網域中與 CIFS 伺服器相關聯的組織單位。預設值為「 CN= 電腦」。若要將 Azure AD 網域服務設定為 Cloud Volumes ONTAP AD 伺服器以供使用、您應在此欄位中輸入 * OID=AADDC computers* 或 * OID=AADDC 使用者 *。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 說明文件：在 Azure AD 網域服務託管網域中建立組織單位（ OU ）"^]
DNS 網域	適用於整個儲存虛擬 Cloud Volumes ONTAP 機器（ SVM ）的 DNS 網域。在大多數情況下、網域與 AD 網域相同。
NTP 伺服器	選擇 * 使用 Active Directory 網域 * 來使用 Active Directory DNS 設定 NTP 伺服器。如果您需要使用不同的位址來設定 NTP 伺服器、則應該使用 API 。請參閱 "Cloud Manager API 開發人員指南" 以取得詳細資料。

15. * 使用率設定檔、磁碟類型及分層原則 * ：視需要選擇是否要啟用儲存效率功能、並變更磁碟區分層原則。

    如需詳細資訊、請參閱 "瞭解 Volume 使用量設定檔" 和 "資料分層總覽"。

16. * 審查與核准 * ：檢閱並確認您的選擇。
    a. 檢閱組態的詳細資料。
    b. 按一下 * 更多資訊 * 以檢閱 Cloud Manager 將購買的支援與 Azure 資源詳細資料。
    c. 選取「 * 我瞭解 … * 」核取方塊。
    d. 按一下「 * 執行 * 」。

結果

Cloud Manager 部署 Cloud Volumes ONTAP 了這個功能。您可以追蹤時間表的進度。

如果您在部署 Cloud Volumes ONTAP 此系統時遇到任何問題、請檢閱故障訊息。您也可以選取工作環境、然後按一下 * 重新建立環境 * 。

如需其他協助、請前往 "NetApp Cloud Volumes ONTAP 支援"。

完成後

- 如果您已配置 CIFS 共用區、請授予使用者或群組檔案和資料夾的權限、並確認這些使用者可以存取共用區並建立檔案。
- 如果您要將配額套用至磁碟區、請使用 System Manager 或 CLI 。

  配額可讓您限制或追蹤使用者、群組或 qtree 所使用的磁碟空間和檔案數量。

開始使用 GCP

開始使用 **Cloud Volumes ONTAP** 適用於 **Google Cloud** 的解決方案

只要幾個步驟、就能開始使用 Cloud Volumes ONTAP 適用於 GCP 的功能。

建立連接器

如果您沒有 "連接器" 然而、帳戶管理員需要建立一個帳戶。 "瞭解如何在 GCP 中建立連接器"。

當您建立第一個 Cloud Volumes ONTAP 運作環境時、如果您還沒有連接器、 Cloud Manager 會提示您部署連接器。

規劃您的組態

Cloud Manager 提供符合工作負載需求的預先設定套件、您也可以建立自己的組態。如果您選擇自己的組態、應該瞭解可用的選項。 "深入瞭解"。

設定您的網路

1. 確保您的 VPC 和子網路支援連接器與 Cloud Volumes ONTAP 支援之間的連線。
2. 啟用從目標 VPC 的傳出網際網路存取、讓 Connector 和 Cloud Volumes ONTAP 支援中心能夠連絡多個端點。

   這個步驟很重要、因為連接器 Cloud Volumes ONTAP 無法在沒有外傳網際網路存取的情況下管理不穩定。如果您需要限制傳出連線、請參閱的端點清單 "Connector 與 Cloud Volumes ONTAP the"。

"深入瞭解網路需求"。

設定**GCP**以進行資料分層

必須滿足兩項要求、才能將冷資料從Cloud Volumes ONTAP 功能性的物件儲存設備（Google Cloud Storage儲存庫）分層至低成本的物件儲存設備（Google Cloud Storage儲存庫）：

1. "設定 Cloud Volumes ONTAP 私有 Google Access 的子網路"。
2. "設定資料分層的服務帳戶"：
   - 將預先定義的 *Storage Admin* 角色指派給分層服務帳戶。
   - 將 Connector 服務帳戶新增為 _ 服務帳戶使用者 _ 至分層服務帳戶。

     您可以提供使用者角色 "在精靈的步驟 3 中、當您建立分層服務帳戶時"或 "在建立服務帳戶後、授予角色"。

     建立 Cloud Volumes ONTAP 一套可運作的環境之後、您需要選擇分層服務帳戶。

如果您在建立 Cloud Volumes ONTAP 一套支援系統時、並未啟用資料分層功能並選取服務帳戶、則必須關

閉系統、 Cloud Volumes ONTAP 並從 GCP 主控台將服務帳戶新增至支援系統。

5 啟用 **Google Cloud API**

"在專案中啟用下列 Google Cloud API"。這些 API 是部署連接器和 Cloud Volumes ONTAP 功能不全的必備條件。

- Cloud Deployment Manager V2 API
- 雲端記錄 API
- Cloud Resource Manager API
- 運算引擎 API
- 身分識別與存取管理（ IAM ） API

6 使用 **Cloud Manager** 啟動 **Cloud Volumes ONTAP**

按一下「 * 新增工作環境 * 」、選取您要部署的系統類型、然後完成精靈中的步驟。 "閱讀逐步指示"。

相關連結

- "評估"
- "從 Cloud Manager 建立 Connector"
- "在 Linux 主機上安裝 Connector 軟體"
- "Cloud Manager 具備 GCP 權限的功能"

在 **Cloud Volumes ONTAP Google Cloud** 規劃您的不一樣組態

在 Cloud Volumes ONTAP Google Cloud 中部署時、您可以選擇符合工作負載需求的預先設定系統、或是建立自己的組態。如果您選擇自己的組態、應該瞭解可用的選項。

選擇授權類型

提供兩種定價選項：隨用隨付及自帶授權（ BYOL ） Cloud Volumes ONTAP 。若為隨用隨付、您可以從三種授權中選擇： Explore 、 Standard 或 Premium 。每個授權都提供不同的容量和運算選項。

"支援的GCP中的VMWare 9.7組態Cloud Volumes ONTAP"

瞭解儲存限制

一個不含資源的系統的原始容量上限 Cloud Volumes ONTAP 與授權有關。其他限制會影響集合體和磁碟區的大小。在規劃組態時、您應該注意這些限制。

"GCP中的更新儲存限制Cloud Volumes ONTAP"

在 GCP 中調整系統規模

調整 Cloud Volumes ONTAP 您的支援規模、有助於滿足效能與容量的需求。在選擇機器類型、磁碟類型和磁碟大小時、您應該注意幾個關鍵點：

機器類型

請查看中支援的機器類型 "發行說明 Cloud Volumes ONTAP" 然後檢視 Google 提供的每種受支援機器類型的詳細資料。將工作負載需求與機器類型的 vCPU 和記憶體數量配對。請注意、每個 CPU 核心都能提升網路效能。

如需詳細資料、請參閱下列內容：

- "Google Cloud 文件： N1 標準機器類型"
- "Google Cloud 文件：效能"

GCP 磁碟類型

當您建立 Cloud Volumes ONTAP 用於資料的 Volume 時、您需要選擇 Cloud Volumes ONTAP 基礎雲端儲存設備、以便將其用於磁碟。磁碟類型可以是 _ 分區 SSD 持續磁碟 _ 或 _ 分區標準持續磁碟 _ 。

SSD 持續式磁碟最適合需要高隨機 IOPS 的工作負載、而標準持續式磁碟則經濟實惠、可處理連續讀寫作業。如需詳細資料、請參閱 "Google Cloud 文件：分區持續磁碟（標準和 SSD ）"。

GCP 磁碟大小

部署 Cloud Volumes ONTAP 一套系統時、您需要選擇初始磁碟大小。之後、您可以讓 Cloud Manager 為您管理系統容量、但如果您想自行建置集合體、請注意下列事項：

- 集合體中的所有磁碟大小必須相同。
- 判斷您需要的空間、同時考量效能。
- 持續性磁碟的效能會隨著磁碟大小和系統可用的 vCPU 數目而自動擴充。

  如需詳細資料、請參閱下列內容：

  - "Google Cloud 文件：分區持續磁碟（標準和 SSD ）"
  - "Google Cloud 文件：最佳化持續磁碟和本機 SSD 效能"

GCP 網路資訊工作表

在 Cloud Volumes ONTAP GCP 中部署時、您需要指定虛擬網路的詳細資料。您可以使用工作表向系統管理員收集資訊。

GCP 資訊	您的價值
區域	
區域	
VPC 網路	
子網路	
防火牆原則（如果使用您自己的）	

選擇寫入速度

Cloud Manager可讓您選擇單一節點Cloud Volumes ONTAP 的寫入速度設定。在您選擇寫入速度之前、您應該先瞭解一般與高設定之間的差異、以及使用高速寫入速度時的風險與建議。

正常寫入速度與高速寫入速度之間的差異

當您選擇正常寫入速度時、資料會直接寫入磁碟、因此可降低發生非計畫性系統中斷時發生資料遺失的可能性。

選擇高速寫入速度時、資料會在寫入磁碟之前先緩衝到記憶體中、以提供更快的寫入效能。由於這種快取、如果發生非計畫性的系統中斷、可能會導致資料遺失。

發生非計畫性系統中斷時可能遺失的資料量、是最後兩個一致點的範圍。一致點是將緩衝資料寫入磁碟的行為。寫入日誌已滿或 10 秒後（以先到者為準）、就會出現一致點。然而、AWS EBS Volume效能可能會影響一致點處理時間。

何時使用高速寫入

如果您的工作負載需要快速寫入效能、而且在非計畫性的系統中斷時、您可以承受資料遺失的風險、那麼高速寫入速度是很好的選擇。

使用高速寫入速度時的建議事項

如果啟用高速寫入、則應確保應用程式層的寫入保護。

選擇 **Volume** 使用設定檔

包含多項儲存效率功能、可減少您所需的總儲存容量。 ONTAP在 Cloud Manager 中建立 Volume 時、您可以選擇啟用這些功能的設定檔、或是停用這些功能的設定檔。您應該深入瞭解這些功能、以協助您決定要使用的設定檔。

NetApp 儲存效率功能提供下列效益：

資源隨需配置

為主機或使用者提供比實體儲存資源池實際擁有更多的邏輯儲存設備。儲存空間不會預先配置儲存空間、而是會在寫入資料時動態分配給每個磁碟區。

重複資料刪除

找出相同的資料區塊、並以單一共用區塊的參考資料取代這些區塊、藉此提升效率。這項技術可消除位於同一個磁碟區的備援資料區塊、進而降低儲存容量需求。

壓縮

藉由壓縮主儲存設備、次儲存設備和歸檔儲存設備上磁碟區內的資料、來減少儲存資料所需的實體容量。

在**GCP**中部署**Cloud Volumes ONTAP** 及管理功能的網路需求

設定您的 Google Cloud Platform 網路功能、 Cloud Volumes ONTAP 讓支援的系統能夠正常運作。這包括連接器和 Cloud Volumes ONTAP 整個過程的網路功能。

需求 **Cloud Volumes ONTAP**

GCP 必須符合下列要求。

虛擬私有雲

支援的對象包括Google Cloud共享VPC和非共享VPC。Cloud Volumes ONTAP

共享 VPC 可讓您設定及集中管理多個專案中的虛擬網路。您可以在 _ 主機專案 _ 中設定共享 VPC 網路、並在 Cloud Volumes ONTAP _ 服務專案 _ 中部署連接器與支援虛擬機器執行個體。 "Google Cloud 文件：共享 VPC 總覽"。

使用共享 VPC 時、唯一的需求是提供 "運算網路使用者角色" 至 Connector 服務帳戶。Cloud Manager 需要這些權限、才能查詢主機專案中的防火牆、 VPC 和子網路。

輸出網際網路存取 **Cloud Volumes ONTAP** 功能

支援向 NetApp 支援部門傳送訊息、以便主動監控儲存設備的健全狀況。 Cloud Volumes ONTAP AutoSupport

路由和防火牆原則必須允許將 HTTP / HTTPS 流量傳送至下列端點、 Cloud Volumes ONTAP 才能讓下列端點傳送 AutoSupport 動態訊息：

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

"瞭解如何設定 AutoSupport 功能"。

IP 位址數

Cloud Manager會在Cloud Volumes ONTAP GCP中分配5個IP位址給功能不全的人。

請注意、Cloud Manager不會在Cloud Volumes ONTAP GCP中建立SVM管理LIF以供使用。

LIF 是與實體連接埠相關聯的 IP 位址。諸如 VMware 的管理工具需要 SVM 管理 LIF SnapCenter 。

防火牆規則

您不需要建立防火牆規則、因為 Cloud Manager 能為您做到這一點。如果您需要使用自己的防火牆、請參閱下列防火牆規則。

從 **Cloud Volumes ONTAP** 功能區連接到 **Google Cloud Storage** 、以利資料分層

如果您想要將冷資料分層至 Google Cloud Storage 資源桶、 Cloud Volumes ONTAP 則必須將駐留的子網路設定為私有 Google Access 。如需相關指示、請參閱 "Google Cloud 文件：設定私有 Google Access"。

如需在 Cloud Manager 中設定資料分層所需的其他步驟、請參閱 "將冷資料分層至低成本物件儲存設備"。

連線 **ONTAP** 至其他網路中的不二系統

若要在 Cloud Volumes ONTAP GCP 中的某個系統與 ONTAP 其他網路中的某個系統之間複寫資料、您必須在 VPC 與另一個網路（例如您的公司網路）之間建立 VPN 連線。

如需相關指示、請參閱 "Google Cloud 文件：雲端 VPN 概述"。

連接器需求

設定您的網路、讓 Connector 能夠管理公有雲環境中的資源和程序。最重要的步驟是確保從網際網路存取各種端點。

如果您的網路使用 Proxy 伺服器來進行所有與網際網路的通訊、您可以從「設定」頁面指定 Proxy 伺服器。請參閱 "將 Connector 設定為使用 Proxy 伺服器"。

連線至目標網路

連接器需要網路連線至您要部署 Cloud Volumes ONTAP 的 VPC 和 VNets 。

例如、如果您在公司網路中安裝 Connector 、則必須設定 VPN 連線至 VPC 或 vnet 、以便在其中啟動 Cloud Volumes ONTAP 更新。

傳出網際網路存取

連接器需要存取傳出網際網路、才能管理公有雲環境中的資源和程序。在 GCP 中管理資源時、 Connector 會聯絡下列端點：

端點	目的
https://www.googleapis.com	讓 Connector 聯絡 Google API 、以便在 Cloud Volumes ONTAP GCP 中部署及管理功能。
https://api.services.cloud.netapp.com:443	API 要求 NetApp Cloud Central 。
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	提供軟體映像、資訊清單和範本的存取權限。
https://repo.cloud.support.netapp.com	用於下載Cloud Manager相依性。
http://repo.mysql.com/	用於下載MySQL。
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	讓 Connector 能夠存取及下載資訊清單、範本及 Cloud Volumes ONTAP 升級影像。
https://cloudmanagerinfraprod.azurecr.io	存取執行 Docker 之基礎架構的容器元件軟體映像、並提供與 Cloud Manager 整合服務的解決方案。
https://kinesis.us-east-1.amazonaws.com	讓 NetApp 能夠從稽核記錄串流資料。
https://cloudmanager.cloud.netapp.com	與 Cloud Manager 服務（包括 Cloud Central 帳戶）進行通訊。
https://netapp-cloud-account.auth0.com	與 NetApp Cloud Central 通訊、以進行集中式使用者驗證。
https://mysupport.netapp.com	與 NetApp AutoSupport 通訊
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	與 NetApp 溝通以取得系統授權與支援登錄。

端點	目的
https://ipa-signer.cloudmanager.netapp.com	讓 Cloud Manager 能夠產生授權（例如 FlexCache 、針對 Cloud Volumes ONTAP 功能不全的
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	需要將Cloud Volumes ONTAP 支援的系統與Kubernetes叢集連線。端點可安裝NetApp Trident。
各種協力廠商位置、例如： • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org 第三方據點可能會有所變更。	在升級期間、 Cloud Manager 會針對協力廠商相依性下載最新的套件。

雖然您應該從 SaaS 使用者介面執行幾乎所有的工作、但連接器上仍有本機使用者介面可供使用。執行 Web 瀏覽器的機器必須連線至下列端點：

端點	目的
連接器主機	您必須從網頁瀏覽器輸入主機的 IP 位址、才能載入 Cloud Manager 主控台。 視您與雲端供應商的連線能力而定、您可以使用指派給主機的私有 IP 或公有 IP ： • 如果您有 VPN 並直接連線至虛擬網路、則私有 IP 可正常運作 • 公有 IP 適用於任何網路情境 無論如何、您應該確保安全群組規則僅允許從授權的 IP 或子網路存取、以確保網路存取安全。
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	您的網頁瀏覽器會連線至這些端點、以便透過 NetApp Cloud Central 進行集中式使用者驗證。
https://widget.intercom.io	產品內對談可讓您與 NetApp 雲端專家交談。

防火牆規則 **Cloud Volumes ONTAP**

Cloud Manager會建立GCP防火牆規則、其中包含Cloud Manager和Cloud Volumes ONTAP NetApp成功運作所需的傳入和傳出規則。您可能需要參照連接埠進行測試、或是偏好使用自己的安全性群組。

適用於此功能的防火牆規則 Cloud Volumes ONTAP 需要傳入和傳出規則。

傳入規則

預先定義之安全性群組中的傳入規則來源為 0.00.0.0/0 。

傳輸協定	連接埠	目的
所有 ICMP	全部	Ping 執行個體
HTTP	80	使用叢集管理 LIF 的 IP 位址、以 HTTP 存取 System Manager Web 主控台
HTTPS	443..	使用叢集管理 LIF 的 IP 位址、以 HTTPS 存取 System Manager 網路主控台
SSH	22	SSH 存取叢集管理 LIF 的 IP 位址或節點管理 LIF
TCP	111.	遠端程序需要 NFS
TCP	139.	CIFS 的 NetBios 服務工作階段
TCP	161-162	簡單的網路管理傳輸協定
TCP	445	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
TCP	635	NFS 掛載
TCP	749	Kerberos
TCP	2049	NFS 伺服器精靈
TCP	3260	透過 iSCSI 資料 LIF 存取 iSCSI
TCP	4045	NFS 鎖定精靈
TCP	4046	NFS 的網路狀態監控
TCP	10000	使用 NDMP 備份
TCP	11104.	管理 SnapMirror 的叢集間通訊工作階段
TCP	11105.	使用叢集間生命體進行 SnapMirror 資料傳輸
UDP	111.	遠端程序需要 NFS
UDP	161-162	簡單的網路管理傳輸協定
UDP	635	NFS 掛載
UDP	2049	NFS 伺服器精靈
UDP	4045	NFS 鎖定精靈
UDP	4046	NFS 的網路狀態監控
UDP	4049	NFS rquotad 傳輸協定

傳出規則

預先定義 Cloud Volumes ONTAP 的 Security Group for the 旅行團會開啟所有的傳出流量。如果可以接受、請遵循基本的傳出規則。如果您需要更嚴格的規則、請使用進階的傳出規則。

基本傳出規則

適用於此功能的預先定義安全性群組 Cloud Volumes ONTAP 包括下列傳出規則。

傳輸協定	連接埠	目的
所有 ICMP	全部	所有傳出流量
所有 TCP	全部	所有傳出流量
所有的 udp	全部	所有傳出流量

進階傳出規則

如果您需要嚴格的傳出流量規則、可以使用下列資訊、僅開啟 Cloud Volumes ONTAP 那些由真人進行傳出通訊所需的連接埠。

來源是 Cloud Volumes ONTAP 指在整個系統上的介面（ IP 位址）。

服務	傳輸協定	連接埠	來源	目的地	目的
Active Directory	TCP	88	節點管理 LIF	Active Directory 樹系	Kerberos V 驗證
	UDP	137.	節點管理 LIF	Active Directory 樹系	NetBios 名稱服務
	UDP	138	節點管理 LIF	Active Directory 樹系	NetBios 資料報服務
	TCP	139.	節點管理 LIF	Active Directory 樹系	NetBios 服務工作階段
	TCP 與 UDP	389	節點管理 LIF	Active Directory 樹系	LDAP
	TCP	445	節點管理 LIF	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	TCP	464. 64	節點管理 LIF	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	UDP	464. 64	節點管理 LIF	Active Directory 樹系	Kerberos 金鑰管理
	TCP	749	節點管理 LIF	Active Directory 樹系	Kerberos V 變更與設定密碼（ RPCSEC_GSS ）
	TCP	88	資料 LIF （ NFS 、 CIFS 、 iSCSI ）	Active Directory 樹系	Kerberos V 驗證
	UDP	137.	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 名稱服務
	UDP	138	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 資料報服務
	TCP	139.	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 服務工作階段
	TCP 與 UDP	389	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	LDAP
	TCP	445	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	TCP	464. 64	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	UDP	464. 64	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos 金鑰管理
	TCP	749	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos V 變更及設定密碼（ RPCSEC_GSS ）
叢集	所有流量	所有流量	一個節點上的所有 LIF	其他節點上的所有 LIF	叢集間通訊（ Cloud Volumes ONTAP 僅限不含 HA ）
	TCP	3000	節點管理 LIF	HA 中介	ZAPI 呼叫（ Cloud Volumes ONTAP 僅限 RHA ）
	ICMP	1.	節點管理 LIF	HA 中介	Keepive Alive （ Cloud Volumes ONTAP 僅限 HHA ）
DHCP	UDP	68	節點管理 LIF	DHCP	第一次設定的 DHCP 用戶端

服務	傳輸協定	連接埠	來源	目的地	目的
DHCPS	UDP	67	節點管理 LIF	DHCP	DHCP 伺服器
DNS	UDP	53.	節點管理 LIF 與資料 LIF （ NFS 、 CIFS ）	DNS	DNS
NDMP	TCP	18600 – 18699	節點管理 LIF	目的地伺服器	NDMP 複本
SMTP	TCP	25	節點管理 LIF	郵件伺服器	可以使用 SMTP 警示 AutoSupport 來執行功能
SNMP	TCP	161.	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	UDP	161.	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	TCP	162%	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	UDP	162%	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
SnapMirror	TCP	11104.	叢集間 LIF	叢集間 LIF ONTAP	管理 SnapMirror 的叢集間通訊工作階段
	TCP	11105.	叢集間 LIF	叢集間 LIF ONTAP	SnapMirror 資料傳輸
系統記錄	UDP	514	節點管理 LIF	系統記錄伺服器	系統記錄轉送訊息

Connector 的防火牆規則

連接器的防火牆規則需要傳入和傳出規則。

傳入規則

預先定義的防火牆規則中的傳入規則來源為0.00.0.0/0。

傳輸協定	連接埠	目的
SSH	22	提供對 Connector 主機的 SSH 存取權
HTTP	80	提供從用戶端 Web 瀏覽器到本機使用者介面的 HTTP 存取
HTTPS	443..	提供 HTTPS 存取、從用戶端網頁瀏覽器存取本機使用者介面

傳出規則

連接器的預先定義防火牆規則會開啟所有傳出流量。如果可以接受、請遵循基本的傳出規則。如果您需要更嚴格的規則、請使用進階的傳出規則。

基本傳出規則

Connector 的預先定義防火牆規則包括下列傳出規則。

傳輸協定	連接埠	目的
所有 TCP	全部	所有傳出流量
所有的 udp	全部	所有傳出流量

進階傳出規則

如果您需要嚴格的傳出流量規則、可以使用下列資訊、僅開啟連接器傳出通訊所需的連接埠。

來源 IP 位址為 Connector 主機。

服務	傳輸協定	連接埠	目的地	目的
Active Directory	TCP	88	Active Directory 樹系	Kerberos V 驗證
	TCP	139.	Active Directory 樹系	NetBios 服務工作階段
	TCP	389	Active Directory 樹系	LDAP
	TCP	445	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	TCP	464.64	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	TCP	749	Active Directory 樹系	Active Directory Kerberos V 變更及設定密碼（ RPCSEC_GSS ）
	UDP	137.	Active Directory 樹系	NetBios 名稱服務
	UDP	138	Active Directory 樹系	NetBios 資料報服務
	UDP	464.64	Active Directory 樹系	Kerberos 金鑰管理
API 呼叫與 AutoSupport 功能	HTTPS	443..	傳出網際網路和 ONTAP 叢集管理 LIF	API 呼叫 GCP 和 ONTAP 功能、並將 AutoSupport 不二的訊息傳送給 NetApp
API 呼叫	TCP	3000	叢集管理 LIF ONTAP	API 呼叫 ONTAP 至
DNS	UDP	53.	DNS	用於 Cloud Manager 的 DNS 解析

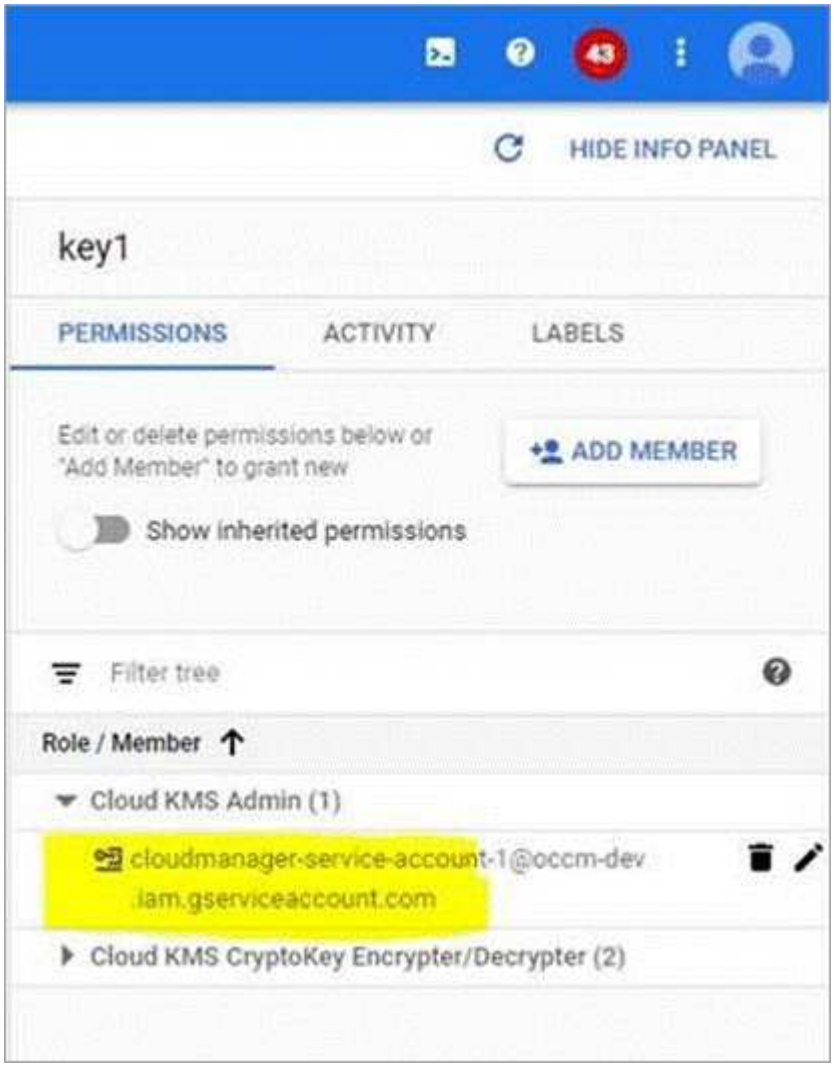
搭配 **Cloud Volumes ONTAP** 使用客戶管理的加密金鑰

雖然 Google Cloud Storage 會在資料寫入磁碟之前先加密資料、但您可以使用 Cloud

Manager API 來建立 Cloud Volumes ONTAP 使用 _ 客戶管理的加密金鑰 _ 的支援系統。這些是您使用 Cloud Key Management Service 在 GCP 中產生及管理的金鑰。

步驟

1. 授予 Connector 服務帳戶使用加密金鑰的權限。



2. 叫用 /GCP / VSA / 中繼資料 / GCP 加密金鑰 API 的 Get 命令、以取得金鑰的「 ID 」。
3. 建立工作環境時、請將「 GcpEncryption 」參數搭配 API 要求使用。

   。範例 *

```
"gcpEncryptionParameters": {
    "key": "projects/tlv-support/locations/us-
east4/keyRings/Nikiskeys/cryptoKeys/generatedkey1"
  }
```

請參閱 "API 開發人員指南" 如需使用「 GcpEncryption 」參數的詳細資訊、

在 **Cloud Volumes ONTAP GCP** 中啟動

您可以Cloud Volumes ONTAP 建立工作環境、在GCP中啟動單一節點的不二系統。

您需要的產品

- 您應該擁有 "與工作區相關的連接器"。

> 您必須是帳戶管理員才能建立 Connector 。當您建立第一個 Cloud Volumes ONTAP 運作環境時、如果您還沒有連接器、 Cloud Manager 會提示您建立連接器。

- "您應該隨時準備好讓 Connector 保持運作"。
- 您應該已經選擇組態、並從系統管理員取得GCP網路資訊。如需詳細資訊、請參閱 "規劃 Cloud Volumes ONTAP 您的需求組態"。
- 若要部署 BYOL 系統、您需要每個節點的 20 位數序號（授權金鑰）。
- 以下是 Google Cloud API "在您的專案中啟用"：
  - Cloud Deployment Manager V2 API
  - 雲端記錄 API
  - Cloud Resource Manager API
  - 運算引擎 API
  - 身分識別與存取管理（ IAM ） API

步驟

1. 在「工作環境」頁面上、按一下「 * 新增工作環境 * 」、然後依照提示進行。
2. * 選擇位置 * ：選擇 * Google Cloud * 和 * Cloud Volumes ONTAP
3. 詳細資料與認證：選取專案、指定叢集名稱、選擇性地新增標籤、然後指定認證資料。

   下表說明您可能需要指導的欄位：

欄位	說明
工作環境名稱	Cloud Manager 會使用工作環境名稱來命名 Cloud Volumes ONTAP 支援系統和 GCP VM 執行個體。如果您選取該選項、它也會使用名稱做為預先定義安全性群組的前置詞。
新增標籤	標籤是 GCP 資源的中繼資料。Cloud Manager 會將標籤新增 Cloud Volumes ONTAP 至與系統相關的支援系統和 GCP 資源。建立工作環境時、您最多可以從使用者介面新增四個標籤、然後在建立之後新增更多標籤。請注意、在建立工作環境時、 API 不會限制您使用四個標籤。如需標籤的相關資訊、請參閱 "Google Cloud 文件：標示資源"。
使用者名稱和密碼	這些是 Cloud Volumes ONTAP 適用於整個叢集管理帳戶的認證資料。您可以使用這些認證資料、 Cloud Volumes ONTAP 透過 System Manager 或其 CLI 連線至功能驗證。

欄位	說明
編輯專案	選取 Cloud Volumes ONTAP 您要駐留的專案。預設專案是 Cloud Manager 所在的專案。 如果您在下拉式清單中沒有看到任何其他專案、則表示您尚未將 Cloud Manager 服務帳戶與其他專案建立關聯。前往 Google Cloud 主控台、開啟 IAM 服務、然後選取專案。將具有 Cloud Manager 角色的服務帳戶新增至該專案。您必須針對每個專案重複此步驟。 這是您為 Cloud Manager 設定的服務帳戶、 "如本頁步驟2b所述"。 按一下 * 「新增訂閱」 * 、將選取的認證資料與訂閱建立關聯。 若要建立隨用隨付 Cloud Volumes ONTAP 的功能性系統、您需要從 Cloud Volumes ONTAP GCP Marketplace 選擇與訂閱功能相關的 GCP 專案。

下列影片說明如何將隨用隨付服務市場訂閱關聯至 GCP 專案：

► https://docs.netapp.com/zh-tw/occm38//media/video_subscribing_gcp.mp4 *(video)*

4. * 位置與連線 * ：選取位置、選擇防火牆原則、然後勾選核取方塊、確認與 Google Cloud 儲存設備的網路連線、以進行資料分層。

   如果您想要將冷資料分層至 Google Cloud Storage 資源桶、 Cloud Volumes ONTAP 則必須將駐留的子網路設定為私有 Google Access 。如需相關指示、請參閱 "Google Cloud 文件：設定私有 Google Access"。

5. * 授權與支援網站帳戶 * ：指定您要使用「隨用隨付」或「 BYOL 」、然後指定 NetApp 支援網站帳戶。

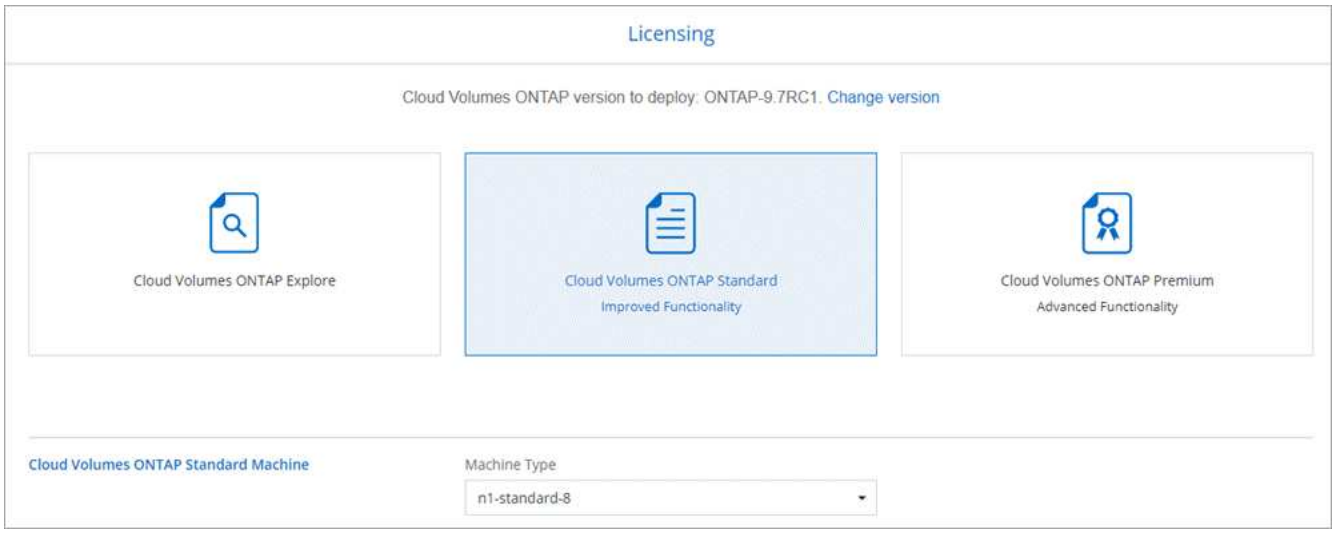
   若要瞭解授權的運作方式、請參閱 "授權"。

   NetApp 支援網站帳戶是隨用隨付的選項、但 BYOL 系統則為必填項目。 "瞭解如何新增 NetApp 支援網站帳戶"。

6. * 預先設定的套件 * ：選取其中一個套件以快速部署 Cloud Volumes ONTAP 某個作業系統、或按一下 * 建立我自己的組態 * 。

   如果您選擇其中一個套件、則只需指定一個 Volume 、然後檢閱並核准組態。

7. * 授權 * ：視 Cloud Volumes ONTAP 需要變更版本、選取授權、然後選取虛擬機器類型。



如果您在啟動系統之後需要變更、您可以稍後修改授權或虛擬機器類型。

如果所選版本有較新的發行候選版本、一般可用度或修補程式版本、 Cloud Manager 會在建立工作環境時、將系統更新至該版本。例如、如果您選取 Cloud Volumes ONTAP 了「供應的是」「供應的是」「供應的是」「供應的」「供應的是」、就會進行更新。更新不會從一個版本發生到另一個版本、例如從 9.6 到 9.7 。

8. * 基礎儲存資源 * ：選擇初始 Aggregate 的設定：每個磁碟的磁碟類型和大小。

   磁碟類型適用於初始磁碟區。您可以為後續磁碟區選擇不同的磁碟類型。

   磁碟大小適用於初始 Aggregate 中的所有磁碟、以及 Cloud Manager 在使用簡易資源配置選項時所建立的任何其他集合體。您可以使用進階配置選項、建立使用不同磁碟大小的集合體。

   如需選擇磁碟類型和大小的說明、請參閱 "在 GCP 中調整系統規模"。

9. * 寫入速度與 WORM * ：選擇 * 正常 * 或 * 高速 * 寫入速度、並視需要啟動一次寫入、多次讀取（ WORM ）儲存設備。

   只有單一節點系統才支援選擇寫入速度。

   "深入瞭解寫入速度"。

   如果資料分層已啟用、則無法啟用 WORM 。

   "深入瞭解 WORM 儲存設備"。

10. * Google Cloud Platform中的資料分層*： 選擇是在初始Aggregate上啟用資料分層、為階層式資料選擇儲存類別、然後選擇具有預先定義儲存管理角色（Cloud Volumes ONTAP 適用於效能提升9.7）的服務帳戶、或是選擇GCP帳戶（Cloud Volumes ONTAP 適用於效能提升9.6）。

    請注意下列事項：

    - Cloud Manager 會在 Cloud Volumes ONTAP 整個過程中設定服務帳戶。此服務帳戶提供資料分層至 Google Cloud Storage 儲存庫的權限。請務必將Cloud Manager服務帳戶新增為分層服務帳戶的使用者、否則您將無法從Cloud Manager選取該帳戶。

- 如需新增 GCP 帳戶的說明、請參閱 "設定和新增 GCP 帳戶、以便使用 9.6 進行資料分層"。
- 您可以在建立或編輯磁碟區時、選擇特定的磁碟區分層原則。
- 如果停用資料分層、您可以在後續的 Aggregate 上啟用、但您需要關閉系統、並從 GCP 主控台新增服務帳戶。

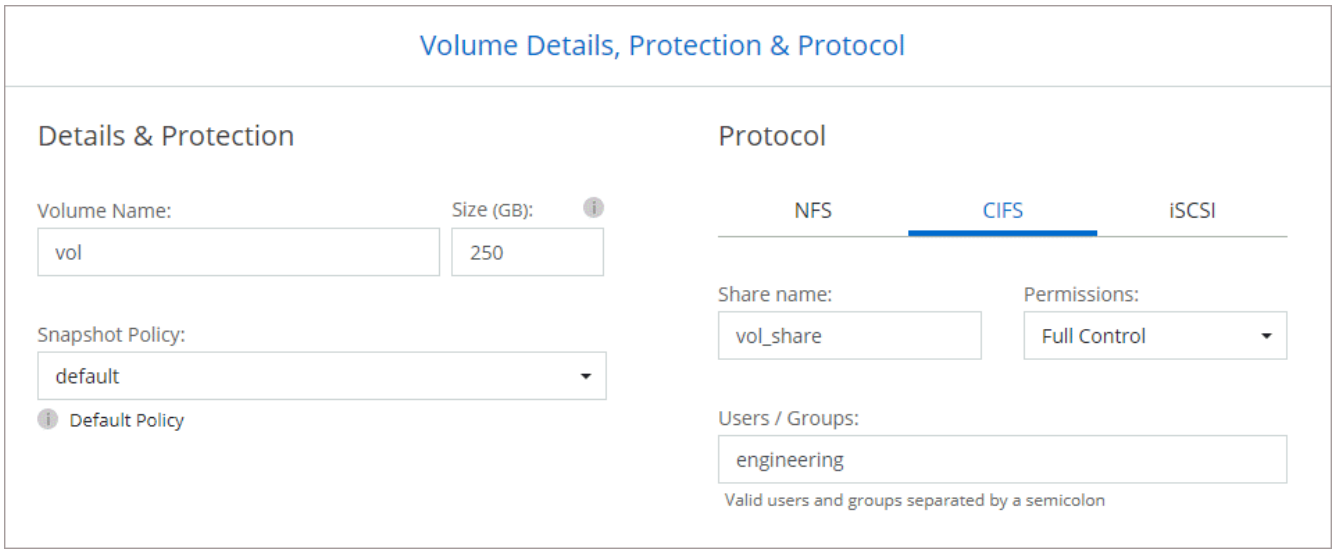
  "深入瞭解資料分層"。

11. * 建立 Volume * ：輸入新磁碟區的詳細資料、或按一下 * 跳過 * 。

本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

欄位	說明
尺寸	您可以輸入的最大大小、主要取決於您是否啟用精簡配置、這可讓您建立比目前可用實體儲存容量更大的磁碟區。
存取控制（僅適用於 NFS ）	匯出原則會定義子網路中可存取磁碟區的用戶端。根據預設、 Cloud Manager 會輸入一個值、讓您存取子網路中的所有執行個體。
權限與使用者 / 群組（僅限 CIFS ）	這些欄位可讓您控制使用者和群組（也稱為存取控制清單或 ACL ）的共用存取層級。您可以指定本機或網域 Windows 使用者或群組、或 UNIX 使用者或群組。如果您指定網域 Windows 使用者名稱、則必須使用網域 \ 使用者名稱格式來包含使用者的網域。
Snapshot 原則	Snapshot 複製原則會指定自動建立的 NetApp Snapshot 複本的頻率和數量。NetApp Snapshot 複本是一種不影響效能的時間點檔案系統映像、需要最少的儲存容量。您可以選擇預設原則或無。您可以針對暫時性資料選擇「無」：例如、 Microsoft SQL Server 的 Tempdb 。
進階選項（僅適用於 NFS ）	為磁碟區選取 NFS 版本： NFSv3 或 NFSv3 。
啟動器群組和 IQN （僅適用於 iSCSI ）	iSCSI 儲存目標稱為 LUN （邏輯單元）、以標準區塊裝置的形式呈現給主機。啟動器群組是 iSCSI 主機節點名稱的表格、可控制哪些啟動器可存取哪些 LUN 。iSCSI 目標可透過標準乙太網路介面卡（ NIC ）、 TCP 卸載引擎（ TOE ）卡（含軟體啟動器）、整合式網路介面卡（ CNA ）或專用主機匯流排介面卡（ HBA ）連線至網路、並由 iSCSI 合格名稱（ IQN ）識別。建立 iSCSI Volume 時、 Cloud Manager 會自動為您建立 LUN 。我們只要在每個磁碟區建立一個 LUN 、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 "使用 IQN 從主機連線至 LUN"。

下圖顯示 CIFS 傳輸協定的「 Volume 」（磁碟區）頁面：



12. * CIFS 設定 * ：如果您選擇 CIFS 傳輸協定、請設定 CIFS 伺服器。

欄位	說明
DNS 主要和次要 IP 位址	提供 CIFS 伺服器名稱解析的 DNS 伺服器 IP 位址。列出的 DNS 伺服器必須包含所需的服務位置記錄（ SRV), 才能找到 CIFS 伺服器要加入之網域的 Active Directory LDAP 伺服器和網域控制器。
要加入的 Active Directory 網域	您要 CIFS 伺服器加入之 Active Directory （ AD ）網域的 FQDN 。
授權加入網域的認證資料	具有足夠權限的 Windows 帳戶名稱和密碼、可將電腦新增至 AD 網域內的指定組織單位（ OU ）。
CIFS 伺服器 NetBios 名稱	AD 網域中唯一的 CIFS 伺服器名稱。
組織單位	AD 網域中與 CIFS 伺服器相關聯的組織單位。預設值為「 CN= 電腦」。
DNS 網域	適用於整個儲存虛擬 Cloud Volumes ONTAP 機器（ SVM ）的 DNS 網域。在大多數情況下、網域與 AD 網域相同。
NTP 伺服器	選擇 * 使用 Active Directory 網域 * 來使用 Active Directory DNS 設定 NTP 伺服器。如果您需要使用不同的位址來設定 NTP 伺服器、則應該使用 API 。請參閱 "Cloud Manager API 開發人員指南" 以取得詳細資料。

13. * 使用率設定檔、磁碟類型及分層原則 * ：視需要選擇是否要啟用儲存效率功能、並變更磁碟區分層原則。

    如需詳細資訊、請參閱 "瞭解 Volume 使用量設定檔" 和 "資料分層總覽"。

14. * 審查與核准 * ：檢閱並確認您的選擇。
    a. 檢閱組態的詳細資料。
    b. 按一下 * 更多資訊 * 以檢閱 Cloud Manager 將購買的支援與 GCP 資源詳細資料。
    c. 選取「 * 我瞭解 … * 」核取方塊。
    d. 按一下「 * 執行 * 」。

結果

Cloud Manager 部署 Cloud Volumes ONTAP 了這個功能。您可以追蹤時間表的進度。

如果您在部署 Cloud Volumes ONTAP 此系統時遇到任何問題、請檢閱故障訊息。您也可以選取工作環境、然後按一下 * 重新建立環境 * 。

如需其他協助、請前往 "NetApp Cloud Volumes ONTAP 支援"。

完成後

- 如果您已配置 CIFS 共用區、請授予使用者或群組檔案和資料夾的權限、並確認這些使用者可以存取共用區並建立檔案。
- 如果您要將配額套用至磁碟區、請使用 System Manager 或 CLI 。

  配額可讓您限制或追蹤使用者、群組或 qtree 所使用的磁碟空間和檔案數量。

配置及管理儲存設備

資源配置儲存設備

您可以 Cloud Volumes ONTAP 透過 Cloud Manager 管理磁碟區和集合體、為您的整個過程提供額外的儲存空間。

所有磁碟和集合體都必須直接從 Cloud Manager 建立和刪除。您不應從其他管理工具執行這些動作。這樣做可能會影響系統穩定性、阻礙未來新增磁碟的能力、並可能產生備援雲端供應商費用。

建立 **FlexVol** 功能區

如果您在啟動 Cloud Volumes ONTAP 完一套功能完善的系統之後需要更多儲存設備、您可以 FlexVol 從 Cloud Manager 為 NFS 、 CIFS 或 iSCSI 建立新的功能完善的功能。

關於這項工作

建立 iSCSI Volume 時、 Cloud Manager 會自動為您建立 LUN 。我們只要在每個磁碟區建立一個 LUN 、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 使用 IQN 從主機連線至 LUN。

您可以從 System Manager 或 CLI 建立其他 LUN 。

開始之前

如果您想在 AWS 中使用 CIFS 、則必須設定 DNS 和 Active Directory 。如需詳細資訊、請參閱 "AWS 的 Cloud Volumes ONTAP 網路需求"。

步驟

1. 在「工作環境」頁面上、按兩下Cloud Volumes ONTAP 您要配置FlexVol 的一套系統名稱。
2. 在任何 Aggregate 或特定 Aggregate 上建立新磁碟區：

行動	步驟
建立新的 Volume 、讓 Cloud Manager 選擇內含的 Aggregate	按一下「 * 新增 Volume * 」。
在特定 Aggregate 上建立新磁碟區	a. 按一下功能表圖示、然後按一下 * 進階 > 進階分配 * 。 b. 按一下功能表以取得 Aggregate 。 c. 按一下「 * 建立 Volume * 」。

3. 輸入新磁碟區的詳細資料、然後按一下 * 繼續 * 。

   本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

欄位	說明
尺寸	您可以輸入的最大大小、主要取決於您是否啟用精簡配置、這可讓您建立比目前可用實體儲存容量更大的磁碟區。
存取控制（僅適用於 NFS ）	匯出原則會定義子網路中可存取磁碟區的用戶端。根據預設、 Cloud Manager 會輸入一個值、讓您存取子網路中的所有執行個體。
權限與使用者 / 群組（僅限 CIFS ）	這些欄位可讓您控制使用者和群組（也稱為存取控制清單或 ACL ）的共用存取層級。您可以指定本機或網域 Windows 使用者或群組、或 UNIX 使用者或群組。如果您指定網域 Windows 使用者名稱、則必須使用網域 \ 使用者名稱格式來包含使用者的網域。
Snapshot 原則	Snapshot 複製原則會指定自動建立的 NetApp Snapshot 複本的頻率和數量。NetApp Snapshot 複本是一種不影響效能的時間點檔案系統映像、需要最少的儲存容量。您可以選擇預設原則或無。您可以針對暫時性資料選擇「無」：例如、 Microsoft SQL Server 的 Tempdb 。
進階選項（僅適用於 NFS ）	為磁碟區選取 NFS 版本： NFSv3 或 NFSv3 。
啟動器群組和 IQN （僅適用於 iSCSI ）	iSCSI 儲存目標稱為 LUN （邏輯單元）、以標準區塊裝置的形式呈現給主機。啟動器群組是 iSCSI 主機節點名稱的表格、可控制哪些啟動器可存取哪些 LUN 。iSCSI 目標可透過標準乙太網路介面卡（ NIC ）、 TCP 卸載引擎（ TOE ）卡（含軟體啟動器）、整合式網路介面卡（ CNA ）或專用主機匯流排介面卡（ HBA ）連線至網路、並由 iSCSI 合格名稱（ IQN ）識別。建立 iSCSI Volume 時、 Cloud Manager 會自動為您建立 LUN 。我們只要在每個磁碟區建立一個 LUN 、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 "使用 IQN 從主機連線至 LUN"。

4. 如果您選擇 CIFS 傳輸協定、但尚未設定 CIFS 伺服器、請在「 Create a CIFS Server （建立 CIFS 伺服器）」對話方塊中指定伺服器的詳細資料、然後按一下 * 「 Save and Continue （儲存並繼續）」 * ：

欄位	說明
DNS 主要和次要 IP 位址	提供 CIFS 伺服器名稱解析的 DNS 伺服器 IP 位址。列出的 DNS 伺服器必須包含所需的服務位置記錄（ SRV), 才能找到 CIFS 伺服器要加入之網域的 Active Directory LDAP 伺服器和網域控制器。
要加入的 Active Directory 網域	您要 CIFS 伺服器加入之 Active Directory （ AD ）網域的 FQDN 。

欄位	說明
授權加入網域的認證資料	具有足夠權限的 Windows 帳戶名稱和密碼、可將電腦新增至 AD 網域內的指定組織單位（ OU ）。
CIFS 伺服器 NetBios 名稱	AD 網域中唯一的 CIFS 伺服器名稱。
組織單位	AD 網域中與 CIFS 伺服器相關聯的組織單位。預設值為「 CN= 電腦」。 • 若要將 AWS 託管 Microsoft AD 設定為 AD 伺服器 Cloud Volumes ONTAP 以供使用、您應在此欄位中輸入 * OID=computers,O=corp* 。 • 若要將 Azure AD 網域服務設定為 Cloud Volumes ONTAP AD 伺服器以供使用、您應在此欄位中輸入 * OID=AADDC computers* 或 * OID=AADDC 使用者 * 。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 說明文件：在 Azure AD 網域服務託管網域中建立組織單位（ OU ）"^]
DNS 網域	適用於整個儲存虛擬 Cloud Volumes ONTAP 機器（ SVM ）的 DNS 網域。在大多數情況下、網域與 AD 網域相同。
NTP 伺服器	選擇 * 使用 Active Directory 網域 * 來使用 Active Directory DNS 設定 NTP 伺服器。如果您需要使用不同的位址來設定 NTP 伺服器、則應該使用 API 。請參閱 "Cloud Manager API 開發人員指南" 以取得詳細資料。

5. 在「使用設定檔」、「磁碟類型」和「分層原則」頁面上、選擇是否要啟用儲存效率功能、選擇磁碟類型、並視需要編輯分層原則。

   如需協助、請參閱下列內容：

   - "瞭解 Volume 使用量設定檔"
   - "在 AWS 中調整系統規模"
   - "在 Azure 中調整系統規模"
   - "資料分層總覽"

6. 按一下「 * 執行 * 」。

結果

供應 Volume 。 Cloud Volumes ONTAP

完成後

如果您已配置 CIFS 共用區、請授予使用者或群組檔案和資料夾的權限、並確認這些使用者可以存取共用區並建立檔案。

如果要將配額套用至磁碟區、則必須使用 System Manager 或 CLI 。配額可讓您限制或追蹤使用者、群組或 qtree 所使用的磁碟空間和檔案數量。

在 **FlexVol HA** 組態的第二個節點上建立功能區

根據預設、 Cloud Manager 會在 HA 組態的第一個節點上建立磁碟區。如果您需要雙節點向用戶端提供資料的雙主動式組態、則必須在第二個節點上建立集合體和磁碟區。

步驟

1. 在「工作環境」頁面上、按兩下Cloud Volumes ONTAP 您要管理集合體的運作環境名稱。
2. 按一下功能表圖示、然後按一下 * 進階 > 進階分配 * 。
3. 按一下「 * 新增 Aggregate * 」、然後建立 Aggregate 。
4. 對於主節點、請在 HA 配對中選擇第二個節點。
5. Cloud Manager 建立 Aggregate 之後、選取該集合體、然後按一下「 * 建立 Volume * 」。
6. 輸入新磁碟區的詳細資料、然後按一下「 * 建立 * 」。

完成後

您可以視需要在此集合體上建立其他磁碟區。

對於部署在多個 AWS 可用性區域中的 HA 配對、您必須使用磁碟區所在節點的浮動 IP 位址、將磁碟區掛載到用戶端。

建立 **Aggregate**

您可以自行建立集合體、或是讓 Cloud Manager 在建立磁碟區時為您執行集合體。自行建立集合體的好處在於、您可以選擇基礎磁碟大小、以便根據所需的容量或效能來調整集合體大小。

步驟

1. 在「工作環境」頁面上、按兩下Cloud Volumes ONTAP 您要管理集合體的執行個體名稱。
2. 按一下功能表圖示、然後按一下 * 進階 > 進階分配 * 。
3. 按一下「 * 新增 Aggregate * 」、然後指定 Aggregate 的詳細資料。

   如需磁碟類型與磁碟大小的說明、請參閱 "規劃組態"。

4. 按一下「 * 執行 * 」、然後按一下「 * 核准並購買 * 」。

將 **LUN** 連線至主機

建立 iSCSI Volume 時、 Cloud Manager 會自動為您建立 LUN 。我們只要在每個磁碟區建立一個 LUN 、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、請使用 IQN 從主機連線至 LUN 。

請注意下列事項：

1. Cloud Manager 的自動容量管理不適用於 LUN 。Cloud Manager 建立 LUN 時、會停用自動擴充功能。
2. 您可以從 System Manager 或 CLI 建立其他 LUN 。

步驟

1. 在「工作環境」頁面上、按兩下Cloud Volumes ONTAP 您要管理磁碟區的功能區環境。
2. 選取磁碟區、然後按一下「 * 目標 IQN* 」。
3. 按一下「 * 複製 * 」以複製 IQN 名稱。
4. 設定從主機到 LUN 的 iSCSI 連線。
   - "適用於 Red Hat Enterprise Linux 的支援 9 iSCSI Express 組態：啟動目標的 iSCSI 工作階段 ONTAP"
   - "適用於 Windows 的 S89 iSCSI Express 組態：以目標啟動 iSCSI 工作階段 ONTAP"

使用功能區來加速資料存取 **FlexCache**

流通量是儲存磁碟區、可快取來源（或來源）磁碟區的 NFS 讀取資料。 FlexCache後續讀取快取資料會加快該資料的存取速度。

您可以使用 FlexCache 功能區來加速資料存取、或卸載大量存取磁碟區的流量。由於資料無需存取來源磁碟區、因此能夠直接提供服務、因此在用戶端需要重複存取相同資料時、支援使用者更能提升效能。 FlexCache適用於讀取密集的系統工作負載的資料量。 FlexCache

Cloud Manager FlexCache 目前並未提供對各個版本的管理、但您可以使用 ONTAP CLI 或 ONTAP 功能完善的系統管理程式來建立及管理 FlexCache 各個版本：

- "《資料存取能力快速指南》的《支援資料量》（英文） FlexCache"
- "在 FlexCache System Manager 中建立功能區"

從 3.7.2 版開始、 Cloud Manager 會為 FlexCache 所有的 Cloud Volumes ONTAP 全新推出的功能介紹系統產生一套功能不全的使用許可證。授權包含 500 GB 使用量限制。

若要產生授權、 Cloud Manager 必須存取 https://ipa-signer.cloudmanager.netapp.com 。請確定此 URL 可從防火牆存取。

管理現有儲存設備

Cloud Manager 可讓您管理磁碟區、集合體及 CIFS 伺服器。它也會提示您移動磁碟區、以避免發生容量問題。

管理現有磁碟區

您可以在儲存需求變更時管理現有的磁碟區。您可以檢視、編輯、複製、還原及刪除磁碟區。

步驟

1. 在「工作環境」頁面上、按兩下Cloud Volumes ONTAP 您要管理磁碟區的功能區環境。
2. 管理您的磁碟區：

工作	行動
檢視磁碟區的相關資訊	選取磁碟區、然後按一下「 * 資訊 * 」。
編輯磁碟區（僅限讀寫磁碟區）	a. 選取磁碟區、然後按一下 * 編輯 * 。 b. 修改磁碟區的 Snapshot 原則、 NFS 傳輸協定版本、 NFS 存取控制清單或共用權限、然後按一下 * 更新 * 。 如果您需要自訂 Snapshot 原則、可以使用 System Manager 來建立。
複製磁碟區	a. 選取磁碟區、然後按一下 * Clone （複製） * 。 b. 視需要修改複本名稱、然後按一下 * Clone （複製） * 。 此程序會建立 FlexClone Volume 。FlexClone Volume 是可寫入的時間點複本、空間效率極高、因為它會使用少量的空間作為中繼資料、然後只會在資料變更或新增時耗用額外空間。 若要深入瞭解 FlexClone Volume 、請參閱 "《 9 邏輯儲存管理指南》 ONTAP"。
將資料從 Snapshot 複本還原至新的 Volume	a. 選取磁碟區、然後按一下 * 從 Snapshot 複本還原 * 。 b. 選取 Snapshot 複本、輸入新磁碟區的名稱、然後按一下 * 還原 * 。
隨需建立 Snapshot 複本	a. 選取一個磁碟區、然後按一下 * 「 Create a Snapshot Copy* （建立 Snapshot 複本 * ）」。 b. 視需要變更名稱、然後按一下「 * 建立 * 」。
取得 NFS 掛載命令	a. 選取磁碟區、然後按一下 * 掛載 Command* 。 b. 按一下 * 複本 * 。
檢視 iSCSI 磁碟區的目標 IQN	a. 選取磁碟區、然後按一下「 * 目標 IQN* 」。 b. 按一下 * 複本 * 。 c. "使用 IQN 從主機連線至 LUN"。

工作	行動
變更基礎磁碟類型	a. 選取磁碟區、然後按一下 * 變更磁碟類型與分層原則 * 。 b. 選取磁碟類型、然後按一下 * 變更 * 。 Cloud Manager 會將磁碟區移至使用所選磁碟類型的現有 Aggregate 、或為磁碟區建立新的 Aggregate 。
變更分層原則	a. 選取磁碟區、然後按一下 * 變更磁碟類型與分層原則 * 。 b. 按一下 * 編輯原則 * 。 c. 選取不同的原則、然後按一下 * 變更 * 。 Cloud Manager 會將磁碟區移至現有的 Aggregate 、該集合體使用所選的磁碟類型進行分層、或是為磁碟區建立新的 Aggregate 。
刪除 Volume	a. 選取磁碟區、然後按一下 * 刪除 * 。 b. 再按一下 * 刪除 * 以確認。

管理現有的集合體

新增磁碟、檢視有關集合體的資訊、以及刪除這些磁碟來管理集合體。

開始之前

如果您要刪除 Aggregate 、則必須先刪除 Aggregate 中的磁碟區。

關於這項工作

如果 Aggregate 空間不足、您可以使用 OnCommand 「系統管理程式」將 Volume 移至其他 Aggregate 。

步驟

1. 在「工作環境」頁面上、按兩下Cloud Volumes ONTAP 您要管理集合體的功能不全環境。
2. 按一下功能表圖示、然後按一下 * 進階 > 進階分配 * 。
3. 管理您的 Aggregate ：

工作	行動
檢視有關 Aggregate 的資訊	選取一個 Aggregate 、然後按一下「 * 資訊 * 」。
在特定 Aggregate 上建立磁碟區	選取一個 Aggregate 、然後按一下「 * 建立 Volume * 」。

工作	行動
將磁碟新增至 Aggregate	a. 選取一個 Aggregate 、然後按一下 * 新增 AWS disks* 或 * 新增 Azure disks* 。 b. 選取您要新增的磁碟數目、然後按一下「 * 新增 * 」。 集合體中的所有磁碟大小必須相同。
刪除 Aggregate	a. 選取不包含任何磁碟區的 Aggregate 、然後按一下 * 刪除 * 。 b. 再按一下 * 刪除 * 以確認。

修改 **CIFS** 伺服器

如果您變更 DNS 伺服器或 Active Directory 網域、您需要在 Cloud Volumes ONTAP 更新版中修改 CIFS 伺服器、以便繼續將儲存設備提供給用戶端。

步驟

1. 在工作環境中、按一下功能表圖示、然後按一下 * 進階 > CIFS 設定 * 。
2. 指定 CIFS 伺服器的設定：

工作	行動
DNS 主要和次要 IP 位址	提供 CIFS 伺服器名稱解析的 DNS 伺服器 IP 位址。列出的 DNS 伺服器必須包含所需的服務位置記錄（ SRV), 才能找到 CIFS 伺服器要加入之網域的 Active Directory LDAP 伺服器和網域控制器。
要加入的 Active Directory 網域	您要 CIFS 伺服器加入之 Active Directory （ AD ）網域的 FQDN 。
授權加入網域的認證資料	具有足夠權限的 Windows 帳戶名稱和密碼、可將電腦新增至 AD 網域內的指定組織單位（ OU ）。
CIFS 伺服器 NetBios 名稱	AD 網域中唯一的 CIFS 伺服器名稱。
組織單位	AD 網域中與 CIFS 伺服器相關聯的組織單位。預設值為「 CN= 電腦」。如果您將 AWS 託管 Microsoft AD 設定為 AD 伺服器 Cloud Volumes ONTAP 以供使用、您應該在此欄位中輸入 * OID=computers,O=corp* 。
DNS 網域	適用於整個儲存虛擬 Cloud Volumes ONTAP 機器（ SVM ）的 DNS 網域。在大多數情況下、網域與 AD 網域相同。
NTP 伺服器	選擇 * 使用 Active Directory 網域 * 來使用 Active Directory DNS 設定 NTP 伺服器。如果您需要使用不同的位址來設定 NTP 伺服器、則應該使用 API 。請參閱 "Cloud Manager API 開發人員指南" 以取得詳細資料。

3. 按一下「 * 儲存 * 」。

結果

利用變更更新 CIFS 伺服器。 Cloud Volumes ONTAP

移動 **Volume**

移動磁碟區以提高容量使用率、改善效能、並達成服務層級協議。

您可以在 System Manager 中移動磁碟區、方法是選取磁碟區和目的地 Aggregate 、啟動磁碟區移動作業、以及選擇性地監控磁碟區移動工作。使用 System Manager 時、磁碟區移動作業會自動完成。

步驟

1. 使用 System Manager 或 CLI 將磁碟區移至 Aggregate 。

   在大多數情況下、您可以使用 System Manager 來移動磁碟區。

   如需相關指示、請參閱 "《》《 9 Volume Move Express Guide 》（英文） ONTAP"。

當 **Cloud Manager** 顯示「需要採取行動」訊息時、請移動 **Volume**

Cloud Manager 可能會顯示「必要行動」訊息、指出移動磁碟區是避免容量問題的必要措施、但無法提供修正問題的建議。如果發生這種情況、您需要找出如何修正問題、然後移動一或多個磁碟區。

步驟

1. 找出如何修正問題。
2. 根據您的分析、移動磁碟區以避免容量問題：
   - 將磁碟區移至其他系統。
   - 將磁碟區移至同一系統上的其他 Aggregate。

找出如何修正容量問題

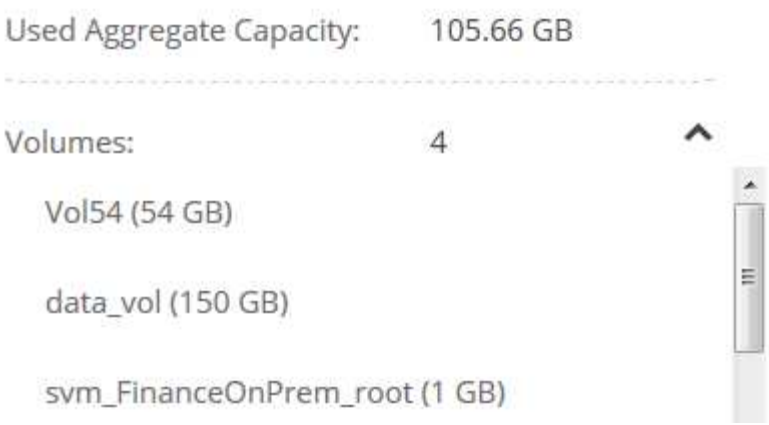
如果 Cloud Manager 無法提供移動磁碟區的建議、以避免發生容量問題、您必須識別需要移動的磁碟區、以及是否應該將其移至同一系統上的其他集合體或其他系統。

步驟

1. 檢視必要行動訊息中的進階資訊、以識別已達到容量上限的集合體。

   例如、進階資訊應該說類似以下的內容： Agggr1 已達到其容量上限。

2. 識別一個或多個要從集合體移出的磁碟區：
   a. 在工作環境中、按一下功能表圖示、然後按一下 * 進階 > 進階配置 * 。
   b. 選取 Aggregate 、然後按一下「 * 資訊 * 」。
   c. 展開 Volume 清單。



d. 檢閱每個磁碟區的大小、然後選擇一或多個磁碟區從集合區移出。

您應該選擇足夠大的磁碟區來釋放集合體中的空間、以避免未來發生額外的容量問題。

3. 如果系統尚未達到磁碟限制、您應該將磁碟區移至同一個系統上的現有集合體或新集合體。

如需詳細資訊、請參閱 "將磁碟區移至另一個 Aggregate 、以避免容量問題"。

4. 如果系統已達到磁碟限制、請執行下列任何一項：

a. 刪除所有未使用的磁碟區。

b. 重新排列磁碟區、以釋放集合體上的空間。

如需詳細資訊、請參閱 "將磁碟區移至另一個 Aggregate 、以避免容量問題"。

c. 將兩個或多個磁碟區移至另一個有空間的系統。

如需詳細資訊、請參閱 "將磁碟區移至其他系統、以避免發生容量問題"。

將磁碟區移至其他系統、以避免發生容量問題

您可以將一個或多個 Volume 移至另 Cloud Volumes ONTAP 一個作業系統、以避免容量問題。如果系統達到磁碟限制、您可能需要這麼做。

關於這項工作

您可以依照此工作中的步驟來修正下列必要行動訊息：

```
 Moving a volume is necessary to avoid capacity issues; however, Cloud
Manager cannot perform this action for you because the system has reached
the disk limit.
```

.步驟

. 找出 Cloud Volumes ONTAP 具備可用容量的系統、或是部署新系統。

. 將來源工作環境拖放到目標工作環境、以執行磁碟區的一次性資料複寫。

+

如需詳細資訊、請參閱 "在系統之間複寫資料"。

1. 移至「複寫狀態」頁面、然後中斷 SnapMirror 關係、將複寫的磁碟區從資料保護磁碟區轉換為讀寫磁碟區。

   如需詳細資訊、請參閱 "管理資料複寫排程和關係"。

2. 設定磁碟區以進行資料存取。

   如需設定目的地 Volume 以進行資料存取的相關資訊、請參閱 "《》 《 9 Volume Disaster Recovery Express 指南》 ONTAP"。

3. 刪除原始 Volume 。

   如需詳細資訊、請參閱 "管理現有磁碟區"。

將磁碟區移至另一個 **Aggregate** 、以避免容量問題

您可以將一個或多個磁碟區移至另一個 Aggregate 、以避免發生容量問題。

關於這項工作

您可以依照此工作中的步驟來修正下列必要行動訊息：

```
 Moving two or more volumes is necessary to avoid capacity issues;
however, Cloud Manager cannot perform this action for you.
```

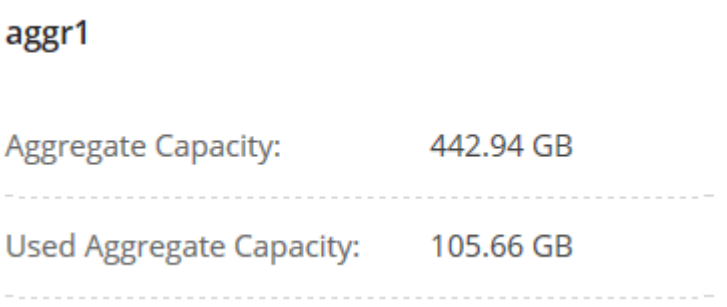
.步驟

. 驗證現有的 `Aggregate` 是否具有您需要移動的磁碟區可用容量：

+

.. 在工作環境中、按一下功能表圖示、然後按一下 * 進階 > 進階配置 * 。
.. 選取每個 Aggregate 、按一下「 * 資訊 * 」、然後檢視可用容量（ Aggregate capcapcape容納 量減去已使用的 Aggregate capcape望 ）。

+



1. 如有需要、請將磁碟新增至現有的 Aggregate ：
   a. 選取 Aggregate 、然後按一下 * 「 Add disks* （新增磁碟 * ）」。
   b. 選取要新增的磁碟數目、然後按一下 * 「 Add* （新增 * ）」。
2. 如果沒有集合體具有可用容量、請建立新的集合體。

   如需詳細資訊、請參閱 "建立 Aggregate"。

3. 使用 System Manager 或 CLI 將磁碟區移至 Aggregate 。
4. 在大多數情況下、您可以使用 System Manager 來移動磁碟區。

   如需相關指示、請參閱 "《》 《 9 Volume Move Express Guide 》 （英文） ONTAP"。

磁碟區移動可能會緩慢執行的原因

如果 Cloud Volumes ONTAP 下列任一情況屬實、則移動 Volume 所需時間可能比預期更長：

- 磁碟區是複製的。
- Volume 是實體複本的父實體。
- 來源或目的地 Aggregate 具有單一資料處理量最佳化 HDD （ ST1 ）磁碟。
- 這個系統位於 AWS 中、其中一個 Aggregate 使用舊的物件命名配置。 Cloud Volumes ONTAP兩個 Aggregate 都必須使用相同的名稱格式。

  如果在 9.4 版或更早版本的 Aggregate 上啟用資料分層、則會使用較舊的命名配置。

- 來源與目的地集合體上的加密設定不相符、或是正在進行重新金鑰。
- 在移動磁碟區時指定了 _ 分層原則 _ 選項、以變更分層原則。
- 磁碟區移動時指定了「 -generation-destination-key_ 」選項。

將非作用中資料分層至低成本物件儲存設備

您可以將熱資料的 SSD 或 HDD 效能層與非作用中資料的物件儲存容量層合併、藉此降低 Cloud Volumes ONTAP VMware 的儲存成本。如需詳細概述、請參閱 "資料分層總覽"。

若要設定資料分層、您只需執行下列動作：


選擇支援的組態

支援大部分的組態。如果您的 Cloud Volumes ONTAP 系統執行的是最新版本、則使用的是「不含更新版本」、「高階」或「 BYOL 」、您應該會很滿意。 "深入瞭解"。


確保 **Cloud Volumes ONTAP** 在物件儲存設備與物件儲存設備之間建立連線

- 對於 AWS 、您需要 VPC 端點對 S3 。 深入瞭解。
- 對於 Azure 而言、只要 Cloud Manager 具備必要的權限、您就不需要執行任何操作。 深入瞭解。
- 對於 GCP 、您需要設定專屬 Google Access 的子網路、並設定服務帳戶。 深入瞭解。


建立、修改或複寫磁碟區時、請選擇分層原則

Cloud Manager 會在您建立、修改或複寫磁碟區時、提示您選擇分層原則。

- "在讀寫磁碟區上分層資料"
- "在資料保護磁碟區上分層資料"

什麼是資料分層不需要的&#8217

- 您不需要安裝功能授權、就能進行資料分層。
- 您不需要建立容量層（ S3 儲存區、 Azure Blob 容器或 GCP 儲存區）。Cloud Manager 能幫您達成這項目標。

支援資料分層的組態

您可以在使用特定組態和功能時啟用資料分層：

- 從下列版本開始、支援使用「資料分層 Cloud Volumes ONTAP 」功能：
  - AWS 版本 9.2
  - Azure 中的 9.4 版、搭配單一節點系統
  - Azure 版本 9.6 、搭配 HA 配對
  - GCP 版本 9.6

    Azure 不支援 DS3_v2 虛擬機器類型的資料分層。
- 在 AWS 中、效能層可以是通用 SSD 、已配置的 IOPS SSD 、或是處理量最佳化的 HDD 。
- 在 Azure 中、效能層級可以是優質 SSD 託管磁碟、標準 SSD 託管磁碟或標準 HDD 託管磁碟。
- 在 GCP 中、效能層可以是 SSD 或 HDD （標準磁碟）。
- 加密技術支援資料分層。
- 必須在磁碟區上啟用精簡配置。

將冷資料分層至 **AWS S3** 的需求

確保 Cloud Volumes ONTAP 與 S3 建立連線。提供此連線的最佳方法是建立 VPC 端點至 S3 服務。如需相關指示、請參閱 "AWS 文件：建立閘道端點"。

當您建立 VPC 端點時、請務必選取與 Cloud Volumes ONTAP 該實例相對應的區域、 VPC 和路由表。您也必須修改安全性群組、以新增允許流量到 S3 端點的傳出 HTTPS 規則。否則 Cloud Volumes ONTAP 、無法連線至 S3 服務。

如果您遇到任何問題、請參閱 "AWS 支援知識中心：為什麼我無法使用閘道 VPC 端點連線至 S3 儲存區？"。

將冷資料分層至 **Azure Blob** 儲存設備的需求

只要 Cloud Manager 具備所需的權限、您就不需要在效能層與容量層之間建立連線。如果 Cloud Manager 原則具有下列權限、 Cloud Manager 可為您啟用 vnet 服務端點：

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

權限包含在最新版本中 "Cloud Manager 原則"。

將冷資料分層至 **Google Cloud Storage** 儲存庫的需求

- 駐留的子網路 Cloud Volumes ONTAP 必須設定為私有 Google Access 。如需相關指示、請參閱 "Google Cloud 文件：設定私有 Google Access"。
- 您需要具有預先定義儲存管理角色的服務帳戶。建立 Cloud Volumes ONTAP 一套可運作的環境時、您必須選擇此服務帳戶。

  "請依照下列步驟設定此分層服務帳戶"：

  a. 將預先定義的 *Storage Admin* 角色指派給分層服務帳戶。

  b. 將 Connector 服務帳戶新增為 _ 服務帳戶使用者 _ 至分層服務帳戶。

     您可以提供使用者角色 "在精靈的步驟 3 中、當您建立分層服務帳戶時"或 "在建立服務帳戶後、授予角色"。

     建立 Cloud Volumes ONTAP 一套可運作的環境之後、您需要選擇分層服務帳戶。

  如果您在建立 Cloud Volumes ONTAP 一套支援系統時、並未啟用資料分層功能並選取服務帳戶、則必須關閉系統、 Cloud Volumes ONTAP 並從 GCP 主控台將服務帳戶新增至支援系統。

從讀寫磁碟區分層資料

可將讀寫磁碟區上的非作用中資料分層保存至具成本效益的物件儲存設備、以釋出效能層以供熱資料使用。Cloud Volumes ONTAP

步驟

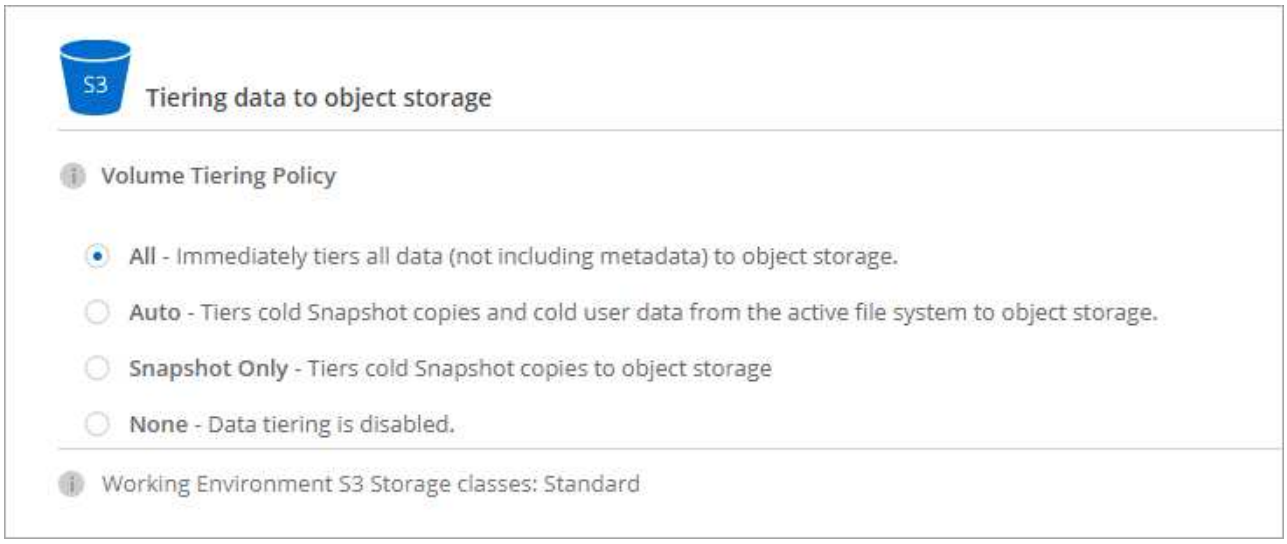
1. 在工作環境中、建立新磁碟區或變更現有磁碟區的層級：

工作	行動
建立新的 Volume	按一下「 * 新增 Volume * 」。
修改現有的 Volume	選取磁碟區、然後按一下 * 變更磁碟類型與分層原則 * 。

2. 選取分層原則。

   如需這些原則的說明、請參閱 "資料分層總覽"。

   ◦ 範例 *



如果啟用資料分層的 Aggregate 不存在、 Cloud Manager 會為磁碟區建立新的 Aggregate 。

如果您偏好自行建立集合體、則可在建立集合體時啟用集合體的資料分層功能。

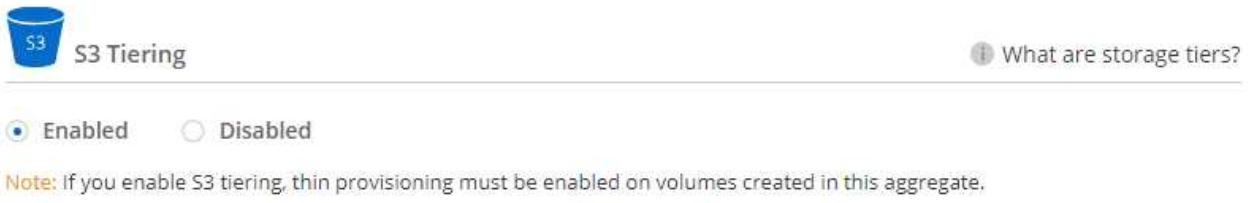
從資料保護磁碟區分層資料

可將資料從資料保護磁碟區分層至容量層。 Cloud Volumes ONTAP如果您啟動目的地 Volume 、資料會隨著讀取而逐漸移至效能層。

步驟

1. 在「工作環境」頁面上、選取包含來源磁碟區的工作環境、然後將其拖曳到您要複寫磁碟區的工作環境。
2. 依照提示操作、直到您到達分層頁面、並啟用資料分層以供物件儲存使用。

    。範例 *



如需複寫資料的說明、請參閱 "在雲端之間複寫資料"。

變更階層式資料的儲存類別

部署 Cloud Volumes ONTAP 完功能後、您可以變更 30 天內未存取的非使用中資料儲存類別、藉此降低儲存成本。如果您確實存取資料、存取成本就會較高、因此在變更儲存類別之前、您必須先將此納入考量。

階層式資料的儲存類別是全系統的、並非每個 Volume 都有。

如需支援的儲存類別資訊、請參閱 "資料分層總覽"。

步驟

1. 在工作環境中、按一下功能表圖示、然後按一下「 * 儲存類別 * 」或「 * Blob 儲存分層 * 」。
2. 選擇一個儲存類別、然後按一下 * 「 Save 」（儲存） * 。

我可以在現有的**Aggregate**上啟用資料分層嗎？

否、您無法在現有的集合體上啟用資料分層。您只能在新的Aggregate上啟用資料分層。

您也可以在新的Aggregate上啟用資料分層 "自行建立Aggregate" 或 建立啟用資料分層的新磁碟區。如果啟用資料分層的Aggregate不存在、Cloud Manager就會為磁碟區建立新的Aggregate。

管理儲存 VM

儲存虛擬機器是 ONTAP 執行於支援內部的虛擬機器、可為您的用戶端提供儲存與資料服務。您可能知道這是 *SVM* 或 *vserver* 。根據預設、系統會設定一個儲存 VM 、但部分組態會支援額外的儲存 VM 。 Cloud Volumes ONTAP

支援的儲存 VM 數量

利用特定組態和附加授權、支援AWS中的多個儲存VM。Cloud Volumes ONTAP "檢視 AWS 中支援的儲存 VM 數量"。請聯絡您的客戶團隊以取得 SVM 附加授權。

所有其他 Cloud Volumes ONTAP 的支援功能均支援單一資料服務儲存 VM 、以及一部用於災難恢復的目的地儲存 VM 。如果來源儲存 VM 發生中斷、您可以啟動目的地儲存 VM 進行資料存取。

儲存虛擬機器橫跨 Cloud Volumes ONTAP 整個整個作業系統（ HA 配對或單一節點）。

建立額外的儲存 VM

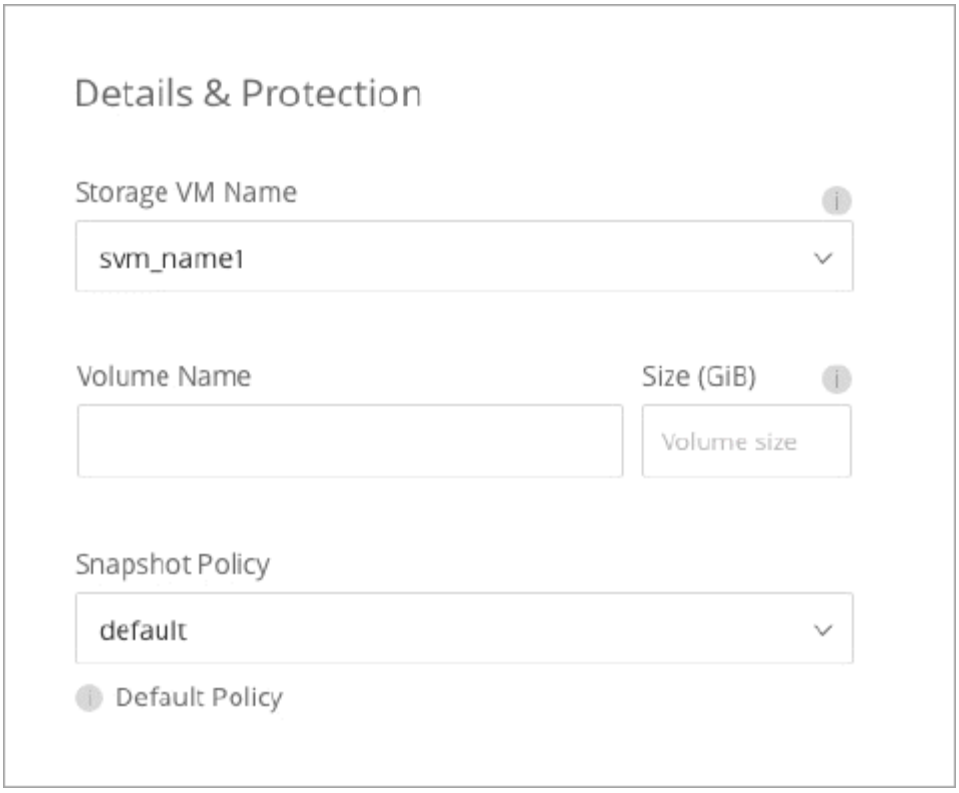
如果組態支援、您可以使用建立其他儲存 VM "System Manager 或 CLI"。

- "建立 SVM 以進行 SMB 存取"
- "建立 SVM 以進行 NFS 存取"
- "建立 SVM 以進行 iSCSI 存取"
- "建立目的地 SVM 以進行災難恢復"

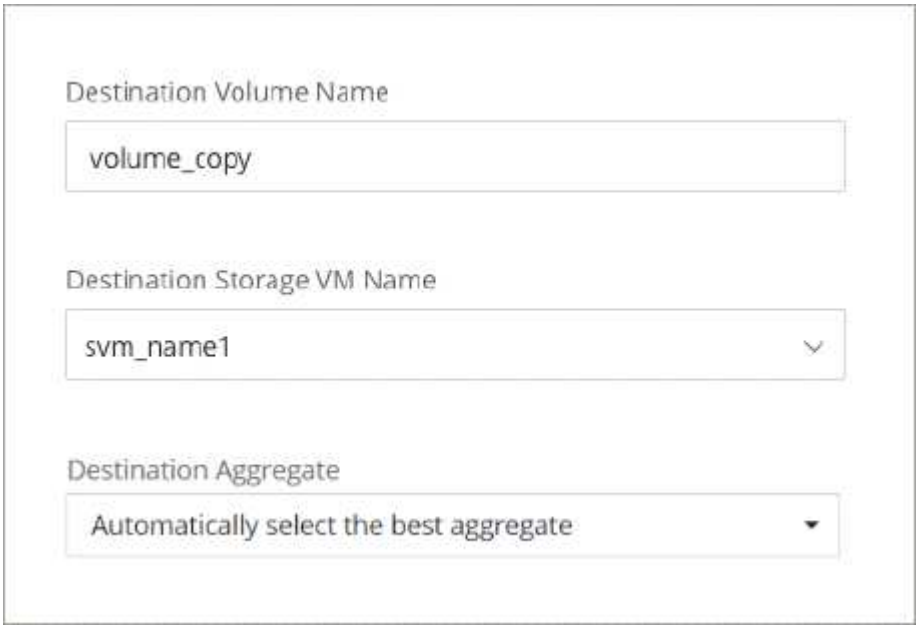
在 Cloud Manager 中使用多個儲存 VM

Cloud Manager 支援您從 System Manager 或 CLI 建立的任何其他儲存 VM 。

例如、下圖顯示如何在建立 Volume 時選擇儲存 VM 。



下圖顯示如何在將磁碟區複寫至其他系統時、選擇儲存 VM 。



管理儲存 **VM** 災難恢復

Cloud Manager 不提供任何儲存 VM 災難恢復的設定或協調支援。您必須使用 System Manager 或 CLI 。

- "SVM 災難恢復準備快速指南"
- "SVM Disaster Recovery Express 指南"

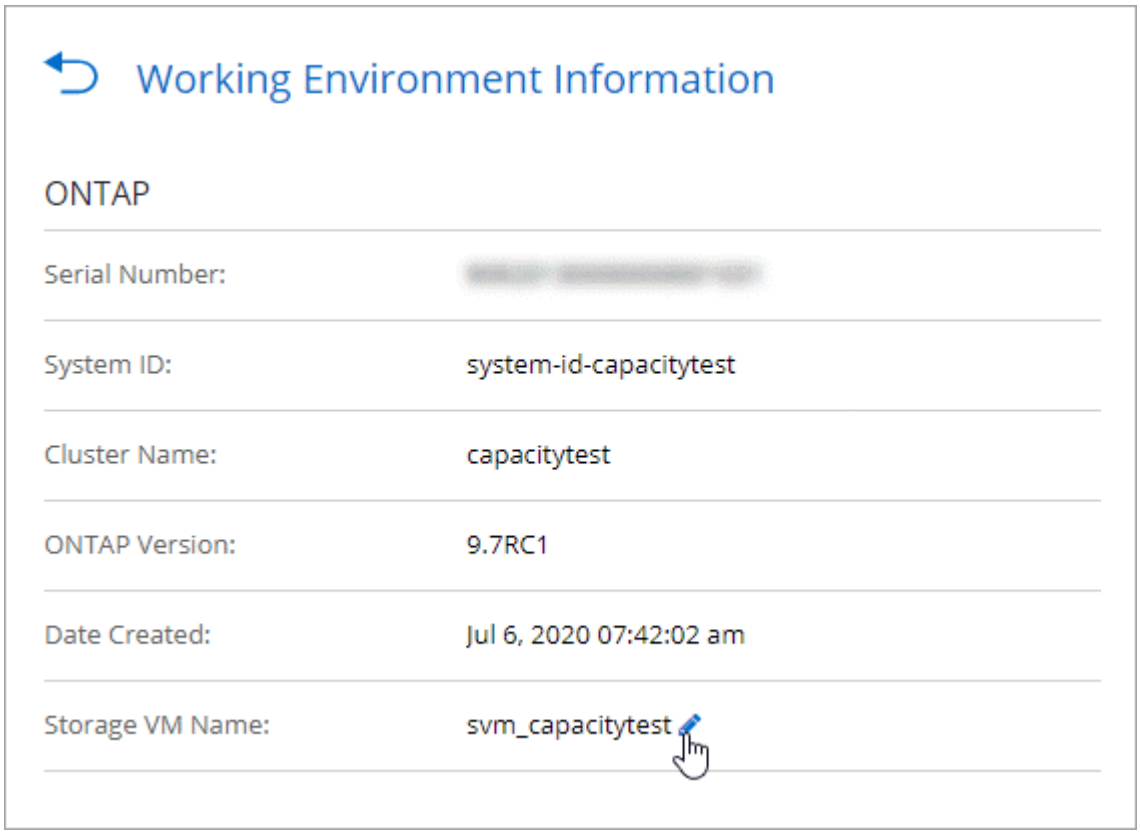
修改儲存 **VM** 名稱

Cloud Manager 會自動為其所建立的 Cloud Volumes ONTAP 單一儲存 VM 命名、以供其使用。如果您有嚴格的命名標準、可以修改儲存 VM 的名稱。例如、您可能希望名稱與您為 ONTAP 自己的叢集命名儲存虛擬機器的方式相符。

如果您建立 Cloud Volumes ONTAP 任何其他的儲存 VM 以供使用、則無法從 Cloud Manager 重新命名儲存 VM 。您必須 Cloud Volumes ONTAP 使用 System Manager 或 CLI 直接從支援功能進行此作業。

步驟

1. 在工作環境中、按一下功能表圖示、然後按一下 * 資訊 * 。
2. 按一下儲存 VM 名稱右側的編輯圖示。



3. 在「修改 SVM 名稱」對話方塊中、變更名稱、然後按一下「 * 儲存 * 」。

使用支援 **Kubernetes** 的不變儲存 **Cloud Volumes ONTAP**

Cloud Manager 可在 Kubernetes 叢集上自動化 NetApp Trident 的部署、讓 Cloud Volumes ONTAP 您可以將 NetApp Trident 用作容器的持續儲存設備。

Trident 是 NetApp 所維護的完全支援的開放原始碼專案。Trident 與 Kubernetes 及其持續 Volume 架構原生整合、可從執行任何 NetApp 儲存平台組合的系統無縫配置及管理 Volume 。 "深入瞭解 Trident"。

內部 ONTAP 的叢集不支援 Kubernetes 功能。僅支援以不支援的功能。 Cloud Volumes ONTAP

快速入門

請依照下列步驟快速入門、或向下捲動至其餘部分以取得完整詳細資料。

 檢閱先決條件

確保您的環境符合先決條件、包括 Kubernetes 叢集與 Cloud Volumes ONTAP 更新之間的連線、 Kubernetes 叢集與連接器之間的連線、最低 Kubernetes 版本 1.14 、叢集中至少有一個工作節點等。 請參閱完整清單。

 將 **Kubernetes** 叢集新增至 **Cloud Manager**

在Cloud Manager中、按一下* Kubernetes*、直接從雲端供應商的託管服務探索叢集、或是提供Kubeconfig檔案來匯入叢集。

 將叢集連線 **Cloud Volumes ONTAP** 至

新增 Kubernetes 叢集後、按一下 * 「 Connect to Working Environment* （連線至工作環境 * ）」 、將叢集連線至一 Cloud Volumes ONTAP 或多個支援系統。

 開始配置持續磁碟區

使用原生 Kubernetes 介面和架構來要求及管理持續磁碟區。Cloud Manager 會建立 NFS 和 iSCSI 儲存類別、供您在配置持續磁碟區時使用。

"深入瞭解如何使用 Kubernetes 的 Trident 來配置第一個 Volume"。

檢閱先決條件

開始之前、請先確定 Kubernetes 叢集和 Connector 符合特定要求。

Kubernetes 叢集需求

- Kubernetes 叢集和 Connector 之間、以及 Kubernetes 叢集與 Cloud Volumes ONTAP 之間、都需要網路連線。

  連接器和 Cloud Volumes ONTAP 鏈接器均需要連線至 Kubernetes API 端點：

  - 對於託管叢集、請在叢集的 VPC 和 Cloud Volumes ONTAP 連接器與 VPC 之間設定路由。
  - 對於其他叢集、連接器 Cloud Volumes ONTAP 和插座必須可存取主節點或負載平衡器的 IP 位址（如 kubeconfig 檔案所列）、而且必須提供有效的 TLS 憑證。
- Kubernetes 叢集可以位於上述網路連線的任何位置。
- Kubernetes 叢集必須至少執行 1.14 版。

  最大支援版本由 Trident 定義。 "按一下此處以查看支援的 Kubernetes 版本上限"。

- Kubernetes 叢集必須至少有一個工作節點。
- 對於以 Amazon Elastic Kubernetes Service （Amazon EKS ）執行的叢集、每個叢集都需要新增 IAM 角色、才能解決權限錯誤。新增叢集之後、 Cloud Manager 會提示您使用確切的 eksctl 命令來解決錯誤。

  "深入瞭解 IAM 權限界限"。

- 對於在 Azure Kubernetes Service （KS ）中執行的叢集、這些叢集必須指派 _Azure Kubernetes Service RBAC 叢集管理 _ 角色。這是必要的、因此 Cloud Manager 可以在叢集上安裝 Trident 並設定儲存類別。
- 對於在 Google Kubernetes Engine （GKE ）中執行的叢集、這些叢集不得使用預設的 Container Optimized OS 。您應該將其切換為使用 Ubuntu 。

  GKE 預設為使用 Google "容器最佳化映像"，它沒有 Trident 掛載 Volume 所需的公用程式。

連接器需求

確認連接器已具備下列網路和權限。

網路

- 連接器在安裝Trident時、需要連出網際網路連線才能存取下列端點：

  https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/

  當您將工作環境連線至叢集時、Cloud Manager會在Kubernetes叢集上安裝Trident。

探索及管理 **EKS** 叢集所需的權限

Connector 需要管理權限、才能探索及管理在 Amazon Elastic Kubernetes Service （EKS ）中執行的 Kubernetes 叢集：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "eks:*",
            "Resource": "*"
        }
    ]
}
```

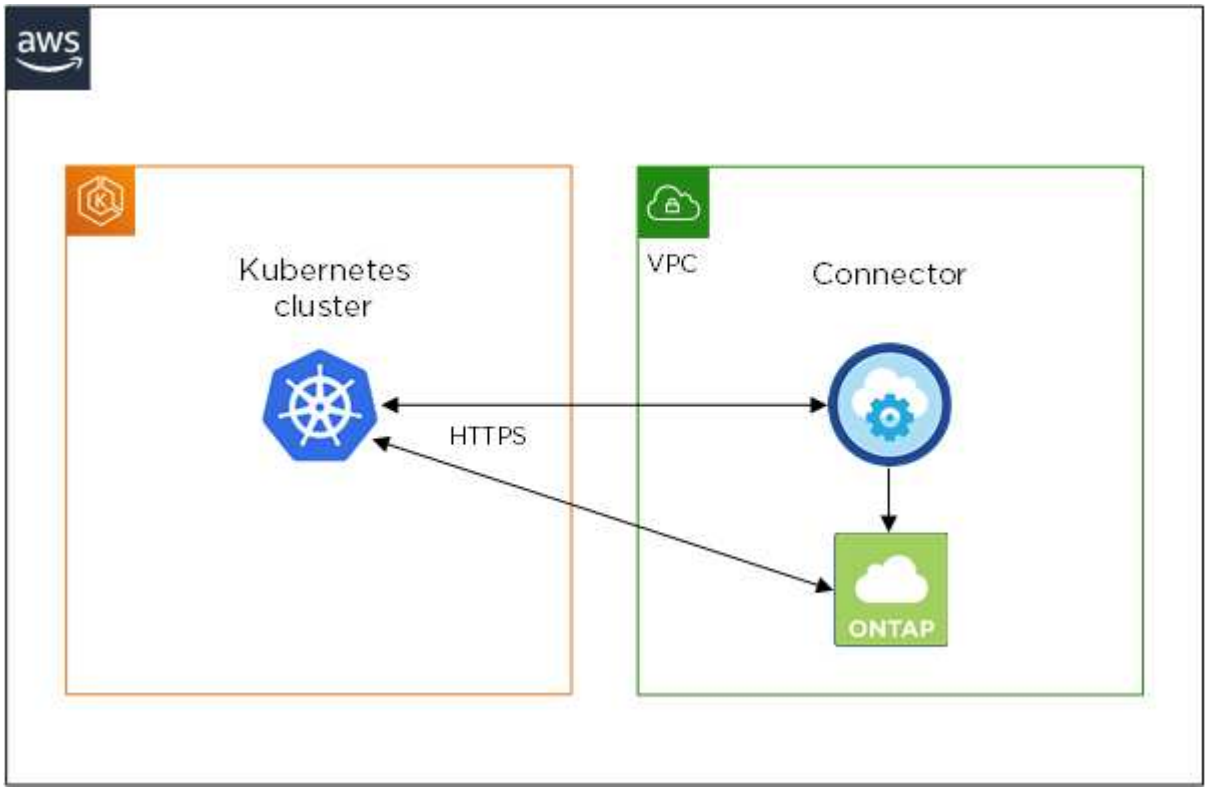
探索及管理 **GKE** 叢集所需的權限

Connector 需要下列權限、才能探索及管理在 Google Kubernetes Engine （GKE ）中執行的 Kubernetes 叢集：

```
container.*
```

設定範例

下圖顯示在 Amazon Elastic Kubernetes Service （Amazon EKS ）中執行 Kubernetes 叢集的範例、以及其與 Connector 和 Cloud Volumes ONTAP EImage 的連線。



新增 **Kubernetes** 叢集

探索雲端供應商託管 Kubernetes 服務中執行的叢集、或匯入叢集的 Kubeconfig 檔案、將 Kubernetes 叢集新增至 Cloud Manager 。

步驟

1. 在Cloud Manager頂端、按一下* Kubernetes*。
2. 單擊 * Add Cluster-* 。
3. 請選擇下列其中一個可用選項：
   - 按一下 * 探索叢集 * 、即可根據您提供給 Connector 的權限、探索 Cloud Manager 可存取的託管叢集。

     例如、如果您的 Connector 是在 Google Cloud 上執行、 Cloud Manager 會使用 Connector 服務帳戶的權限來探索在 Google Kubernetes Engine （ GKE ）中執行的叢集。
   - 按一下 * 匯入叢集 * 、以使用 KUbeconfig 檔案匯入叢集。

     上傳檔案之後、 Cloud Manager 會驗證與叢集的連線、並儲存 Kbeconfig 檔案的加密複本。

結果

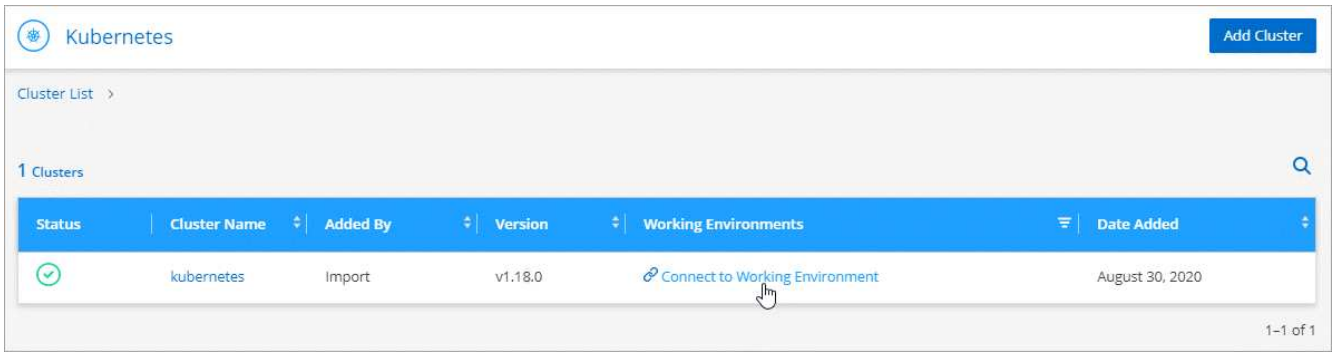
Cloud Manager 會新增 Kubernetes 叢集。您現在可以將叢集連線 Cloud Volumes ONTAP 至

將叢集連線 **Cloud Volumes ONTAP** 至

將 Kubernetes 叢集連線 Cloud Volumes ONTAP 至支援功能、以便 Cloud Volumes ONTAP 將支援功能用作持續儲存容器的功能。

步驟

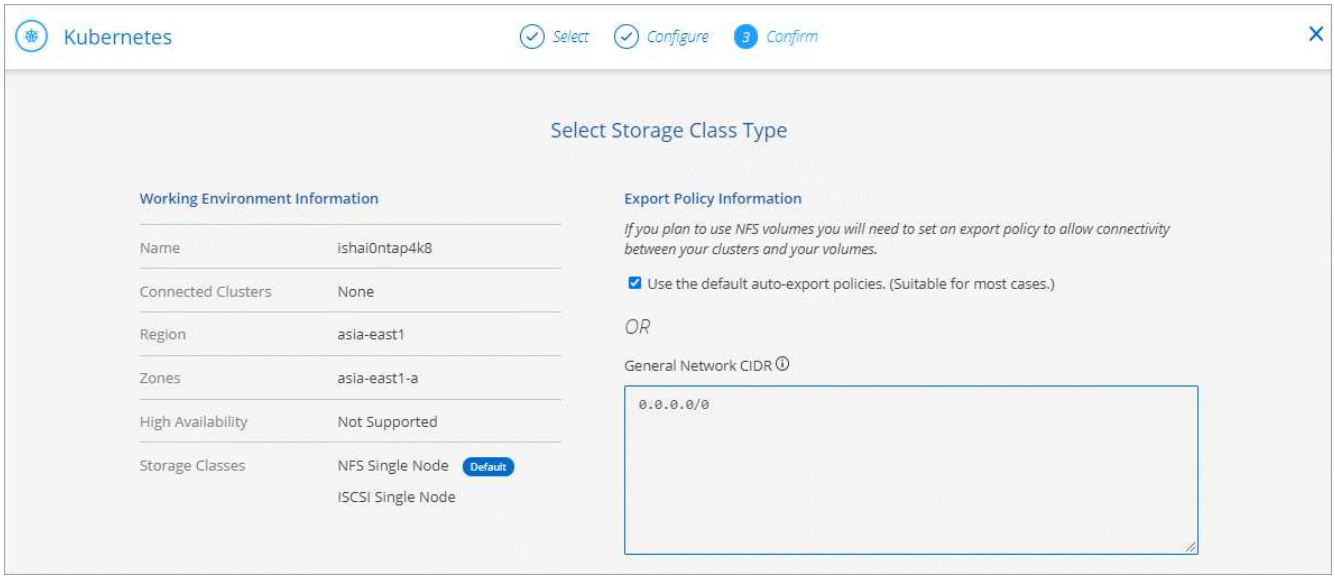
1. 在Cloud Manager頂端、按一下* Kubernetes*。
2. 針對您剛新增的叢集、按一下「 * 連線到工作環境 * 」 。



3. 選取工作環境、然後按一下 * 繼續 * 。
4. 選擇要用作 Kubernetes 叢集預設儲存類別的 NetApp 儲存類別、然後按一下 * 繼續 * 。

   使用者建立持續磁碟區時、 Kubernetes 叢集預設會使用此儲存類別作為後端儲存設備。

5. 選擇是使用預設的自動匯出原則、還是要新增自訂的 CIDR 區塊。



6. 按一下「 * 新增工作環境 * 」 。

結果

Cloud Manager 可將工作環境連線至叢集、最多需要 15 分鐘。

管理叢集

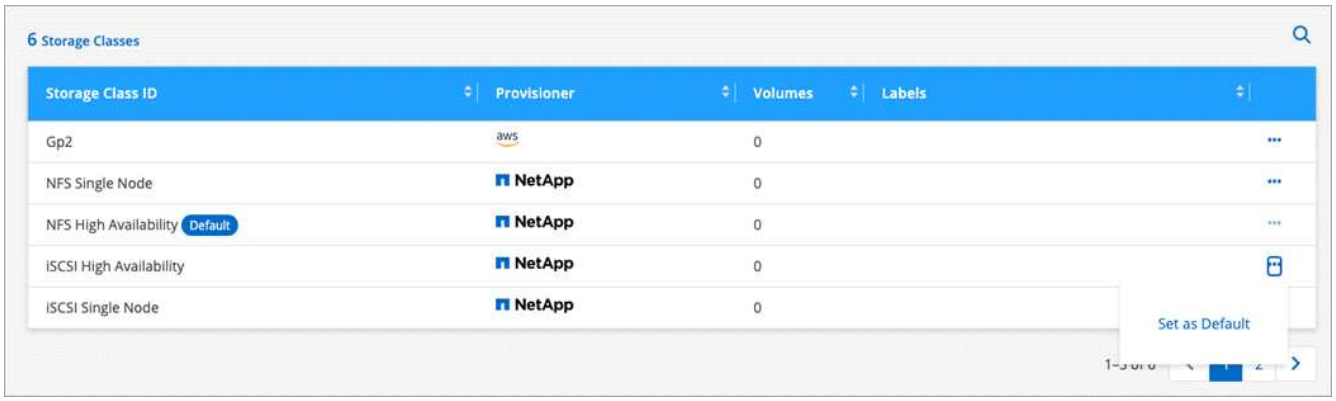
Cloud Manager 可讓您變更預設的儲存類別、升級 Trident 等、藉此管理 Kubernetes 叢集。

變更預設儲存類別

請確定您已將 Cloud Volumes ONTAP 支援功能的儲存類別設為預設的儲存類別、以便叢集使用 Cloud Volumes ONTAP 支援功能來做為後端儲存設備。

步驟

1. 在Cloud Manager頂端、按一下* Kubernetes*。
2. 按一下 Kubernetes 叢集的名稱。
3. 在「 * 儲存類別 * 」表格中、針對您要設為預設的儲存類別、按一下最右側的「動作」功能表。



4. 按一下「 * 設為預設 * 」。

升級 **Trident**

當新版 Trident 可供使用時、您可以從 Cloud Manager 升級 Trident 。

步驟

1. 在Cloud Manager頂端、按一下* Kubernetes*。
2. 按一下 Kubernetes 叢集的名稱。
3. 如果有可用的新版本、請按一下 Trident 版本旁的 * Upgrade* 。

正在更新 **Kbeconfig** 檔案

如果您透過匯入 Kbeconfig 檔案將叢集新增至 Cloud Manager 、您可以隨時將最新的 Kbeconfig 檔案上傳至 Cloud Manager 。如果您已更新認證、變更使用者或角色、或是變更了會影響叢集、使用者、命名空間或驗證的項目、您可以這麼做。

步驟

1. 在Cloud Manager頂端、按一下* Kubernetes*。
2. 按一下 Kubernetes 叢集的名稱。
3. 按一下 * 更新 Kubeconfig * 。
4. 當您的網頁瀏覽器出現提示時、請選取更新的 KUbeconfig 檔案、然後按一下 * 「 Open* （開啟 * ）」 。

結果

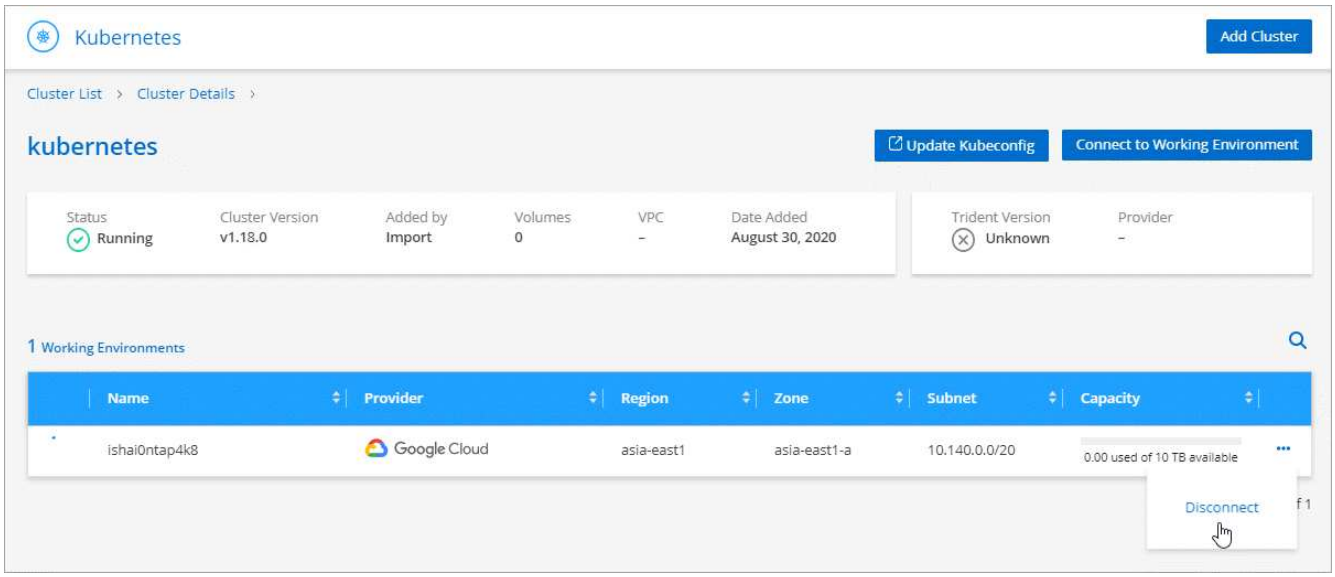
Cloud Manager 會根據最新的 Kubeconfig 檔案、更新 Kubernetes 叢集的相關資訊。

中斷叢集連線

當您中斷叢集 Cloud Volumes ONTAP 與效能不穩定的連線時、您將無法再將 Cloud Volumes ONTAP 該系統當成容器的持續儲存設備。不會刪除現有的持續磁碟區。

步驟

1. 在Cloud Manager頂端、按一下* Kubernetes*。
2. 按一下 Kubernetes 叢集的名稱。
3. 在 * 工作環境 * 表格中、針對您要中斷連線的工作環境、按一下最右側的「動作」功能表。



4. 按一下「 * 中斷連線 * 」 。

結果

Cloud Manager 會中斷叢集與 Cloud Volumes ONTAP 整個系統的連線。

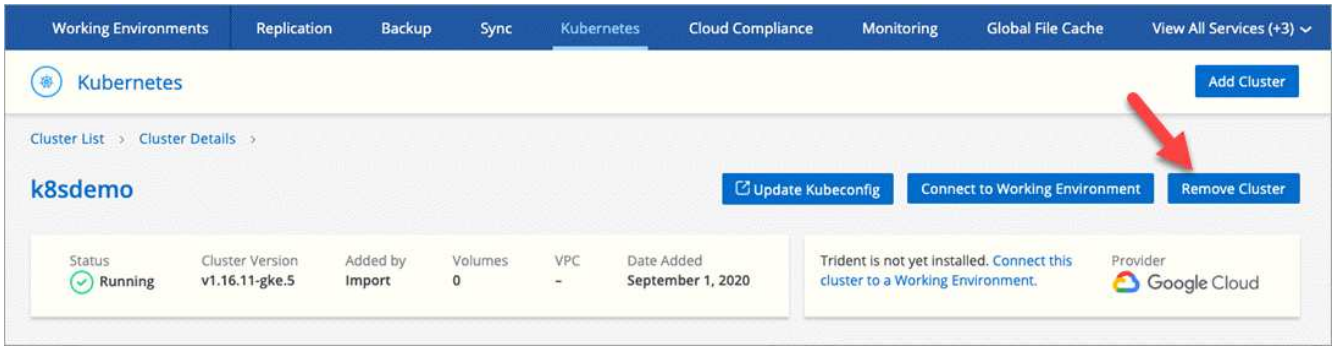
移除叢集

從叢集中斷所有工作環境的連線後、請從 Cloud Manager 移除停用的叢集。

步驟

1. 在Cloud Manager頂端、按一下* Kubernetes*。
2. 按一下 Kubernetes 叢集的名稱。

3. 按一下「 * 移除叢集 * 」。



使用 **NetApp** 加密解決方案加密磁碟區

支援 NetApp Volume Encryption （ NVE ）和 NetApp Aggregate Encryption （ NAE ）與外部金鑰管理程式。 Cloud Volumes ONTAPNVE 和 NAE 是軟體型解決方案、可對磁碟區進行（ FIPS ） 140-2 相容的閒置資料加密。 "深入瞭解這些加密解決方案"。

從更新版本的支援升級至 Cloud Volumes ONTAP 更新版本的更新版本、在您設定外部金鑰管理程式之後、新的 Aggregate 預設會啟用 NAE 。非 NAE Aggregate 一部分的新磁碟區預設會啟用 NVE （例如、如果在設定外部金鑰管理程式之前已建立現有的 Aggregate ）。

不支援內建金鑰管理。 Cloud Volumes ONTAP

您需要的產品

您的支援系統應該已向 NetApp 註冊。 Cloud Volumes ONTAP從 Cloud Manager 3.7.1 開始、 NetApp Volume Encryption 授權會自動安裝在 Cloud Volumes ONTAP 每個已註冊 NetApp 支援的支援系統上。

- "新增 NetApp 支援網站帳戶至 Cloud Manager"
- "註冊隨用隨付系統"

Cloud Manager 不會在中國地區的系統上安裝 NVE 授權。

步驟

1. 檢閱中支援的關鍵管理程式清單 "NetApp 互通性對照表工具"。

   搜尋 * 關鍵經理 * 解決方案。

2. "連線 Cloud Volumes ONTAP 至 CLI"。
3. 安裝 SSL 憑證並連線至外部金鑰管理伺服器。

   "《 NetApp 加密電源指南》（英文） 9 ：設定外部金鑰管理 ONTAP"

在系統之間複寫資料

您可以選擇一次性資料複寫來進行資料傳輸、或是選擇重複排程來進行災難恢復或長期保

留、以便在不同的工作環境之間複寫資料。例如、您可以設定內部 ONTAP 系統的資料複寫、以 Cloud Volumes ONTAP 供災難恢復之用。

Cloud Manager 使用 SnapMirror 和 SnapVault SnapMirror 技術、簡化不同系統上磁碟區之間的資料複寫。您只需識別來源磁碟區和目的地磁碟區、然後選擇複寫原則和排程即可。Cloud Manager 會購買所需的磁碟、設定關係、套用複寫原則、然後在磁碟區之間開始基礎傳輸。

基礎傳輸包含來源資料的完整複本。後續傳輸包含來源資料的差異複本。

Cloud Manager 可在下列工作環境類型之間進行資料複寫：

- 從 Cloud Volumes ONTAP 一個系統到 Cloud Volumes ONTAP 另一個系統
- 在一個不同時的系統和內部的不一樣叢集之間 Cloud Volumes ONTAP ONTAP
- 從內部 ONTAP 的不二叢集到另一個內部 ONTAP 的不二叢集

資料複寫需求

在複寫資料之前、您應該確認 Cloud Volumes ONTAP 是否同時滿足關於功能性的要求、包括功能性的系統和 ONTAP 功能性的叢集。

版本需求

在複寫資料之前、您應該先確認來源和目的地磁碟區是否執行相容 ONTAP 的功能性更新。如需詳細資訊、請參閱 "資料保護電源指南"。

具體需求 **Cloud Volumes ONTAP**

- 執行個體的安全性群組必須包含必要的傳入和傳出規則：特別是 ICMP 和連接埠 11104 和 11105 的規則。

  這些規則包含在預先定義的安全性群組中。

- 若要在 Cloud Volumes ONTAP 不同子網路中的兩個子網路之間複寫資料、必須將子網路路由在一起（這是預設設定）。
- 若要在 Cloud Volumes ONTAP AWS 中的某個系統和 Azure 中的某個系統之間複寫資料、您必須在 AWS VPC 和 Azure vnet 之間建立 VPN 連線。

特定於叢集的需求 **ONTAP**

- 必須安裝主動式 SnapMirror 授權。
- 如果叢集位於內部部署環境中、您應該要從公司網路連線到 AWS 或 Azure 、後者通常是 VPN 連線。
- 叢集必須符合額外的子網路、連接埠、防火牆和叢集需求。 ONTAP

  如需詳細資訊、請參閱叢集與 SVM 對等快速指南、以瞭解您的 ONTAP 版本的資訊。

設定系統之間的資料複寫

您 Cloud Volumes ONTAP 可以選擇一次性資料複寫、 ONTAP 以協助您在雲端之間來回移動資料、或是循環排程、藉此協助災難恢復或長期保留資料、藉此複寫資料。

關於這項工作

Cloud Manager 支援簡單易用、可展開及串聯的資料保護組態：

- 在簡單的組態中、從磁碟區 A 複寫到磁碟區 B
- 在扇出組態中、從磁碟區 A 複寫到多個目的地。
- 在串聯組態中、從磁碟區 A 複寫到磁碟區 B 、從磁碟區 B 複寫到磁碟區 C

您可以在 Cloud Manager 中設定「展開」和「串聯」組態、方法是在系統之間設定多個資料複寫。例如、將磁碟區從系統 A 複寫到系統 B 、然後將相同的磁碟區從系統 B 複寫到系統 C

步驟

1. 在「工作環境」頁面上、選取包含來源磁碟區的工作環境、然後將其拖曳至您要複寫磁碟區的工作環境：

2. 如果出現「來源與目的地對等處理設定」頁面、請選取叢集對等關係的所有叢集間生命體。

   叢集間網路的設定應讓叢集對等端點具有 _ 配對式全網狀連線 _ 、這表示叢集對等關係中的每一對叢集在其所有叢集間生命體之間都具有連線能力。

   如果 ONTAP 來源或目的地是包含多個 lifs 的 Sourc時 叢集、就會出現這些頁面。

3. 在「來源 Volume 選取」頁面上、選取您要複寫的磁碟區。
4. 在「目的地 Volume Name and Tiering 」（目的地磁碟區名稱與分層）頁面上、指定目的地磁碟區名稱、選擇基礎磁碟類型、變更任何進階選項、然後按一下 * 繼續 * 。

   如果目的地是 ONTAP 一個不必要的叢集、您也必須指定目的地 SVM 和 Aggregate 。

5. 在「最大傳輸率」頁面上、指定資料傳輸的最大傳輸率（以百萬位元組 / 秒為單位）。
6. 在「複寫原則」頁面上、選擇其中一個預設原則、或按一下 * 其他原則 * 、然後選取其中一個進階原則。

   如需協助、請參閱 "選擇複寫原則"。

   如果您選擇自訂備份 SnapVault （英文）原則、則與原則相關的標籤必須符合來源 Volume 上 Snapshot 複本的標籤。如需詳細資訊、請參閱 "備份原則的運作方式"。

7. 在「排程」頁面上、選擇一次性複本或週期性排程。

   有多個預設排程可供使用。如果您想要不同的排程、則必須使用 System Manager 在 *destination* 叢集上建立新的排程。

8. 在「檢閱」頁面上、檢閱您的選擇、然後按一下「 * 執行 * 」。

結果

Cloud Manager 會啟動資料複寫程序。您可以在「複寫狀態」頁面中檢視複寫的詳細資料。

管理資料複寫排程和關係

在兩個系統之間設定資料複寫之後、即可從 Cloud Manager 管理資料複寫排程和關係。

步驟

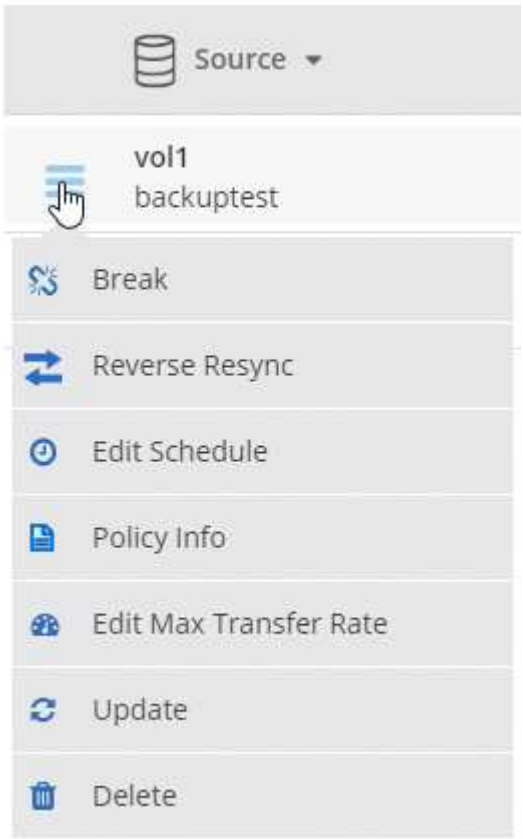
1. 在「工作環境」頁面上、檢視工作區或特定工作環境中所有工作環境的複寫狀態：

選項	行動
工作區中的所有工作環境	在 Cloud Manager 頂端、按一下 * Replication * 。
特定的工作環境	開啟工作環境、然後按一下 * 複製 * 。

2. 檢閱資料複寫關係的狀態、確認它們是否健全。

如果關係的狀態為閒置且鏡射狀態未初始化、則您必須從目的地系統初始化關係、以便根據定義的排程進行資料複寫。您可以使用 System Manager 或命令列介面（ CLI ）初始化關係。當目的地系統故障後恢復連線時、這些狀態可能會出現。

3. 選取來源 Volume 旁的功能表圖示、然後選擇其中一個可用的動作。



下表說明可用的動作：

行動	說明
中斷	中斷來源與目的地磁碟區之間的關係、並啟動目的地磁碟區以進行資料存取。當來源磁碟區因資料毀損、意外刪除或離線狀態等事件而無法提供資料時、通常會使用此選項。如需設定目的地 Volume 以存取資料及重新啟動來源 Volume 的相關資訊、請參閱 ONTAP 《發揮作用》《發揮作用》（《更新指南》）《 9 Volume Disaster Recovery Express 指南》（英文）。
重新同步	重新建立磁碟區之間的中斷關係、並根據定義的排程恢復資料複寫。 當您重新同步磁碟區時、目的地磁碟區上的內容會被來源磁碟區上的內容覆寫。 若要執行反向重新同步、將目的地磁碟區的資料重新同步至來源磁碟區、請參閱 "《》 《 9 Volume Disaster Recovery Express 指南》 ONTAP"。
反轉重新同步	反轉來源與目的地磁碟區的角色。來自原始來源 Volume 的內容會被目的地 Volume 的內容覆寫。當您想要重新啟動離線的來源 Volume 時、這很有幫助。在上次資料複寫與停用來源磁碟區之間寫入原始來源磁碟區的任何資料都不會保留。
編輯排程	可讓您選擇不同的資料複寫排程。
原則資訊	顯示指派給資料複寫關係的保護原則。
編輯最大傳輸率	可讓您編輯資料傳輸的最大速率（以每秒 KB 為單位）。
更新	開始遞增傳輸以更新目的地 Volume 。
刪除	刪除來源與目的地磁碟區之間的資料保護關係、這表示磁碟區之間不再發生資料複寫。此動作不會啟動目的地 Volume 以進行資料存取。如果系統之間沒有其他資料保護關係、此動作也會刪除叢集對等關係和儲存虛擬機器（ SVM ）對等關係。

結果

選取動作之後、 Cloud Manager 會更新關係或排程。

選擇複寫原則

在 Cloud Manager 中設定資料複寫時、您可能需要協助選擇複寫原則。複寫原則定義儲存系統如何將資料從來源磁碟區複寫到目的地磁碟區。

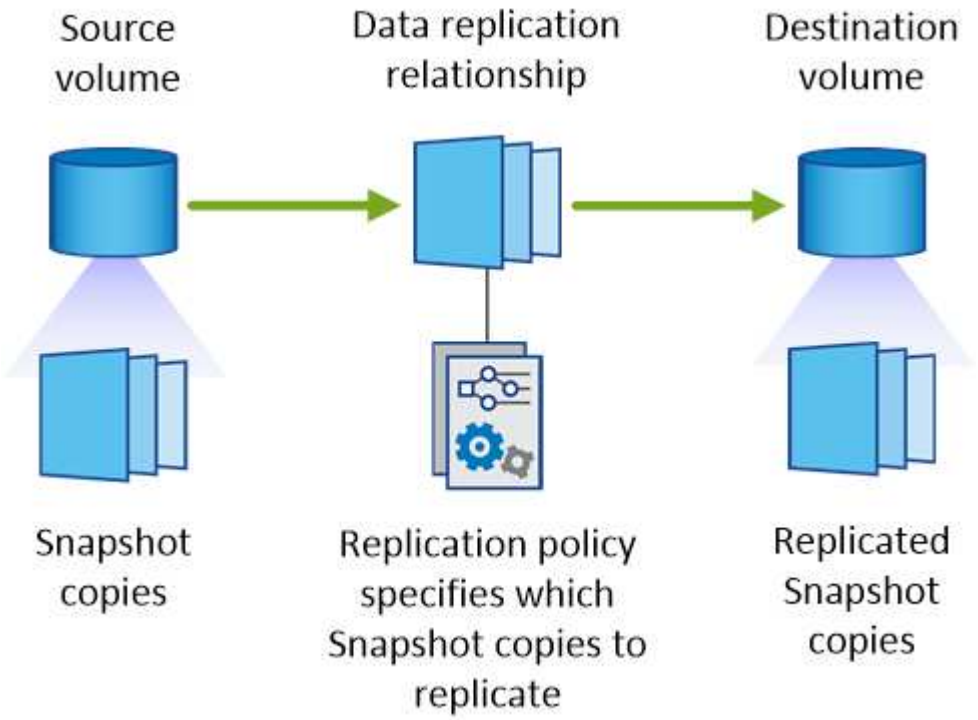
複寫原則的功能

這個作業系統會自動建立稱為 Snapshot 複本的備份。 ONTAPSnapshot 複本是磁碟區的唯讀映像、可在某個時間點擷取檔案系統的狀態。

當您在系統之間複寫資料時、會將 Snapshot 複本從來源磁碟區複寫到目的地磁碟區。複寫原則會指定要從來源磁碟區複寫到目的地磁碟區的 Snapshot 複本。

複寫原則也稱為「 _protection 」原則、因為它們採用 SnapMirror 和 SnapVault SnapMirror 技術、可提供災難恢復保護、以及磁碟對磁碟備份與還原。

下圖顯示 Snapshot 複本與複寫原則之間的關係：



複寫原則類型

複寫原則有三種類型：

- *Mirror* 原則會將新建立的 Snapshot 複本複寫到目的地 Volume 。

  您可以使用這些 Snapshot 複本來保護來源磁碟區、以便做好災難恢復或一次性資料複寫的準備。您可以隨時啟動目的地 Volume 以進行資料存取。

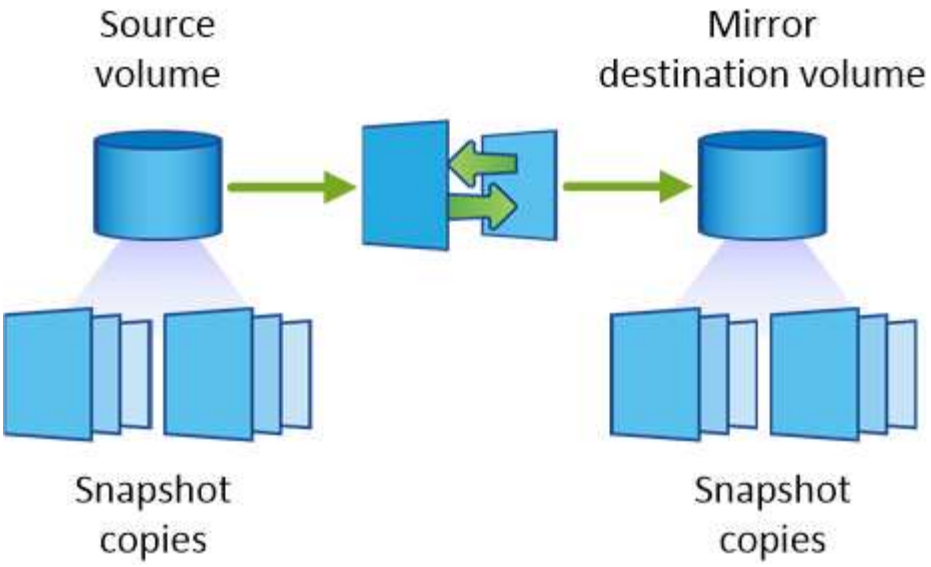
- _Backup 原則會將特定的 Snapshot 複本複寫到目的地磁碟區、通常會將它們保留較長的時間、而不會超過來源磁碟區的時間。

  當資料毀損或遺失時、您可以從這些 Snapshot 複本還原資料、並保留這些複本以符合標準及其他治理相關用途。

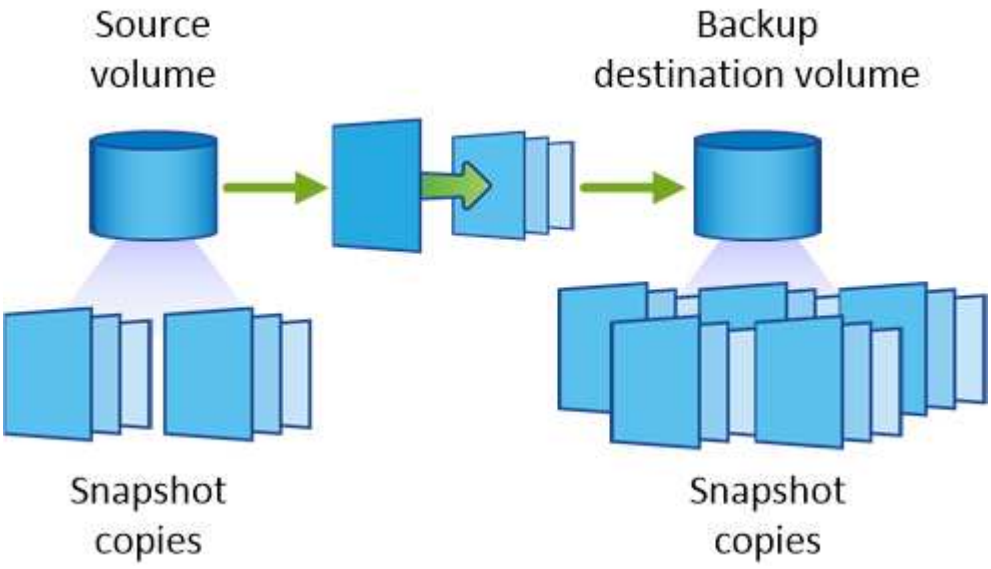
- 鏡射與備份原則提供災難恢復與長期保留。

  每個系統都有預設的鏡射與備份原則、適用於許多情況。如果您發現需要自訂原則、可以使用 System Manager 建立自己的原則。

下列影像顯示鏡射與備份原則之間的差異。鏡射原則會鏡射來源磁碟區上可用的 Snapshot 複本。



備份原則通常會保留快照複本的時間比保留在來源磁碟區上的時間長：



備份原則的運作方式

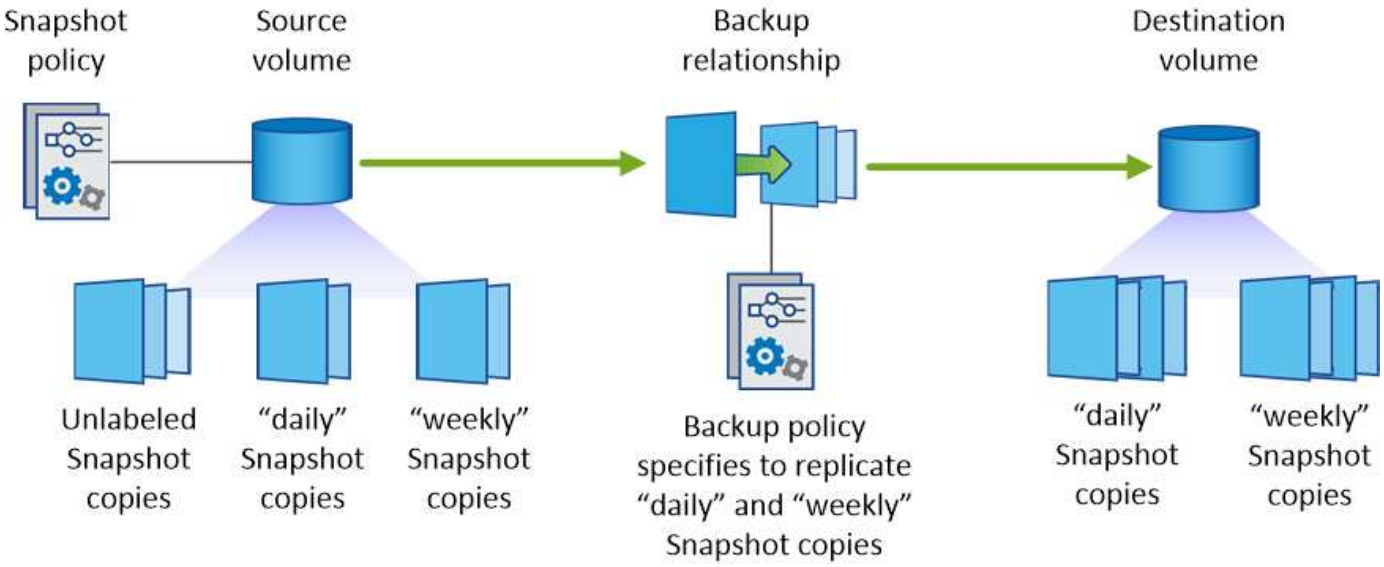
與鏡射原則不同的是、備份 SnapVault （鏡射）原則會將特定的 Snapshot 複本複本複寫到目的地 Volume 。如果您想要使用自己的原則而非預設原則、請務必瞭解備份原則的運作方式。

瞭解 **Snapshot** 複本標籤與備份原則之間的關係

Snapshot 原則定義系統如何建立 Volume 的 Snapshot 複本。原則會指定何時建立 Snapshot 複本、保留多少複本、以及如何標記複本。例如、系統可能會每天在上午 12 ： 10 建立一個 Snapshot 複本、保留兩個最近的複本、並將其標示為「每日」。

備份原則包含指定要複寫到目的地 Volume 的標示 Snapshot 複本、以及要保留多少複本的規則。備份原則中定義的標籤必須符合 Snapshot 原則中定義的一或多個標籤。否則、系統將無法複寫任何 Snapshot 複本。

例如、包含「每日」和「每週」標籤的備份原則、會導致複寫僅包含這些標籤的 Snapshot 複本。不會複寫其他 Snapshot 複本、如下列映像所示：



預設原則和自訂原則

預設的 Snapshot 原則會建立每小時、每日和每週 Snapshot 複本、保留六個每小時、每天兩個和每週兩個 Snapshot 複本。

您可以將預設的備份原則與預設的 Snapshot 原則輕鬆搭配使用。預設的備份原則會複寫每日和每週的 Snapshot 複本、保留七個每日和每 52 個每週 Snapshot 複本。

如果您建立自訂原則、則這些原則所定義的標籤必須相符。您可以使用 System Manager 建立自訂原則。

資料複寫從 **NetApp HCI** 功能複寫到 **Cloud Volumes ONTAP** 功能

如果您嘗試將資料從 NetApp HCI 功能性的資料複製到 Cloud Volumes ONTAP 功能性的更新、可以在 NetApp HCI 執行 NetApp Element SnapMirror 軟體的功能性系統上執行。或者、您也可以將資料複寫到 ONTAP Select 以 NetApp HCI 虛擬來賓身分執行的一套解決方案、以 Cloud Volumes ONTAP 供選擇的功能、建立在以虛擬來賓身分執行的作業系統上。

如需詳細資料、請參閱下列技術報告：

- "技術報告 4641 ： NetApp HCI 《資料保護》"
- "技術報告 4651 ： NetApp SolidFire SnapMirror 架構與組態"

監控效能

瞭解監控服務

利用 "NetApp Cloud Insights 技術服務"Cloud Manager 可讓您深入瞭解 Cloud Volumes ONTAP VMware 執行個體的健全狀況與效能、並協助您疑難排解及最佳化雲端儲存環境的效能。

功能

- 自動監控所有 Volume

- 檢視 IOPS 、處理量和延遲等方面的 Volume 效能資料
- 找出效能問題、將對使用者和應用程式的影響降至最低

支援的雲端供應商

支援適用於 AWS 的 Monitoring 服務 Cloud Volumes ONTAP 。

成本

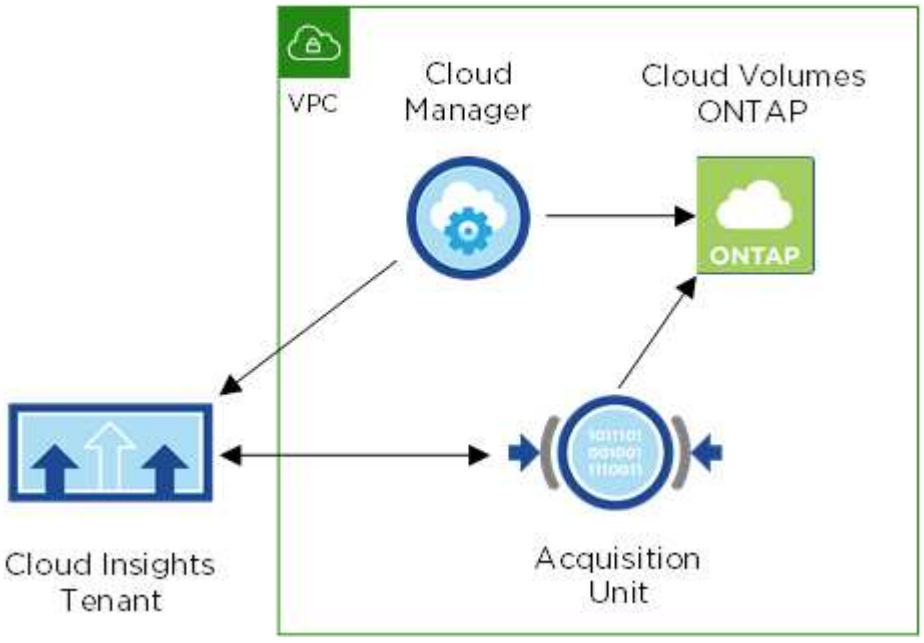
監控功能目前可做為預覽。啟動是免費的、但 Cloud Manager 會在 VPC 中啟動虛擬機器、以利監控。此 VM 會向您的雲端供應商收取費用。

如何搭配 **Cloud Manager** 運作 **Cloud Insights**

在與 Cloud Insights Cloud Manager 的高度整合中、整合了下列功能：

1. 您可以在 Cloud Volumes ONTAP 支援的情況下啟用監控服務。
2. Cloud Manager 可設定您的環境。它會執行下列動作：
    a. 建立 Cloud Insights 一個名為 *environment* 的不完整租戶、並將 Cloud Central 帳戶中的所有使用者與租戶建立關聯。
    b. 提供 Cloud Insights 30 天免費試用版的不二功能。
    c. 在 VPC 中部署稱為「擷取單元」的虛擬機器、以協助監控磁碟區（這是上述「成本」一節中所提及的 VM ）。
    d. 將擷取裝置連接 Cloud Volumes ONTAP 至不實和 Cloud Insights 不實的用戶端。
3. 在 Cloud Manager 中、您可以按一下「監控」、然後使用效能資料來疑難排解及最佳化效能。

下圖顯示這些元件之間的關係：



擷取單位

啟用監控時、 Cloud Manager 會在連接器所在的同一子網路中部署擷取單元。

_Acquisition 採棉頭 _ 會從 Cloud Volumes ONTAP VMware 收集效能資料、並將其傳送給 Cloud Insights 該客戶。然後 Cloud Manager 會查詢資料、並將其呈現給您。

請注意下列關於擷取單位執行個體的資訊：

- 擷取單元執行於 T3.xLarge 執行個體、具有 100 GB GP2 Volume 。
- 執行個體名稱為 *AcquisitionUnity* 、其產生的雜湊（ UUID ）會串連在其中。例如： *AcquitionUnit-FAN7FqeH*
- 每個連接器只部署一個擷取單元。
- 執行個體必須執行才能存取「監控」索引標籤中的效能資訊。

用戶 **Cloud Insights**

啟用監控功能時、 Cloud Manager 會為您設定 _租 戶 _ 。利用此功能、您可以存取擷取單位所收集的效能資料。 Cloud Insights租戶是 NetApp Cloud Insights 解決方案服務中的安全資料分割區。

網路介面 **Cloud Insights**

Cloud Manager 中的 Monitoring （監控）索引標籤可為您的磁碟區提供基本效能資料。您可以 Cloud Insights 從瀏覽器進入「靜態」網頁介面、以執行更深入的監控、並為 Cloud Volumes ONTAP 您的「靜態」系統設定警示。

免費試用與訂閱

Cloud Manager 提供 30 天免費的 Cloud Insights VMware 試用版、可在 Cloud Manager 中提供效能資料、讓您探索 Cloud Insights VMware 標準版的各項功能。

您必須在免費試用結束前訂閱、否則 Cloud Insights 您的 VMware 將最終刪除。您可以訂閱基本版、標準版或優質版、以繼續使用 Cloud Manager 中的監控功能。

"瞭解如何訂閱 Cloud Insights 此功能"。

監控 **Cloud Volumes ONTAP AWS** 的功能

請完成幾個步驟、開始監控 Cloud Volumes ONTAP 效能。

快速入門

請依照下列步驟快速入門、或向下捲動至其餘部分以取得完整詳細資料。

確認您的組態支援

您需要在 Cloud Volumes ONTAP AWS 上的 AWS 上安裝 Cloud Manager 3.8.4 或更新版本、而且您必須是新 Cloud Insights 的支援客戶。

在新的或現有的系統上啟用監控

- 新的工作環境：建立工作環境時（預設為啟用監控）、請務必保持啟用監控。
- 現有工作環境：選取工作環境、然後按一下 * 開始監控 * 。

檢視效能資料

按一下 * 監控 * 、檢視磁碟區的效能資料。

訂閱 **Cloud Insights** 此功能

請在 30 天免費試用結束前訂閱、以繼續在 Cloud Manager 和 Cloud Insights VMware 中看到效能資料。 "瞭解如何訂閱"。

需求

請閱讀下列要求、確認您擁有支援的組態。

支援的 **Cloud Manager** 版本

您需要全新安裝 Cloud Manager 3.8.4 或更新版本。由於需要新的基礎架構才能啟用監控服務、因此需要新的安裝。此基礎架構可從 Cloud Manager 3.8.4 的新安裝開始使用。

支援 **Cloud Volumes ONTAP** 的支援版本

AWS 的 Cloud Volumes ONTAP 任何版本的不一樣。

需求 **Cloud Insights**

您必須是新 Cloud Insights 的客戶。如果您已經 Cloud Insights 擁有一個不支援的用戶、則不支援監控。

Cloud Central 的電子郵件地址

Cloud Central 使用者帳戶的電子郵件地址應為您的企業電子郵件地址。建立 Cloud Insights 一個不支援免費的電子郵件網域、例如 Gmail 和 Hotmai 。

併購單位的網路

擷取單元使用雙向 / 相互驗證來連線 Cloud Insights 至該伺服器。用戶端憑證必須傳遞至 Cloud Insights 驗證伺服器。為達成此目的、必須設定 Proxy 、將 http 要求轉送到 Cloud Insights 該伺服器、而不需解密資料。

擷取單元使用下列兩個端點與 Cloud Insights 下列項目進行通訊。如果您在擷取裝置伺服器和 Cloud Insights 功能間有防火牆、則在設定防火牆規則時需要這些端點：

```
https://aulogin.<Cloud Insights Domain>
https://<your-tenant-ID>.<Cloud Insights Domain>
```

例如：

```
https://aulogin.c01.cloudinsights.netapp.com
https://cg0c586a-ee05-45rb-a5ac-
333b5ae7718d7.c01.cloudinsights.netapp.com
```

如果您需要協助辨識 Cloud Insights 您的域名和租戶 ID 、請透過產品內對談與我們聯絡。

連接器的網路功能

與擷取單元類似、連接器必須具備連往 Cloud Insights 該插座的輸出連線能力。但連接器所接觸的端點則略有不同。它會使用簡短的租戶 ID 來聯絡租戶主機 URL ：

```
https://<your-short-tenant-ID>.<Cloud Insights Domain>
```

例如：

```
https://abcd12345.c01.cloudinsights.netapp.com
```

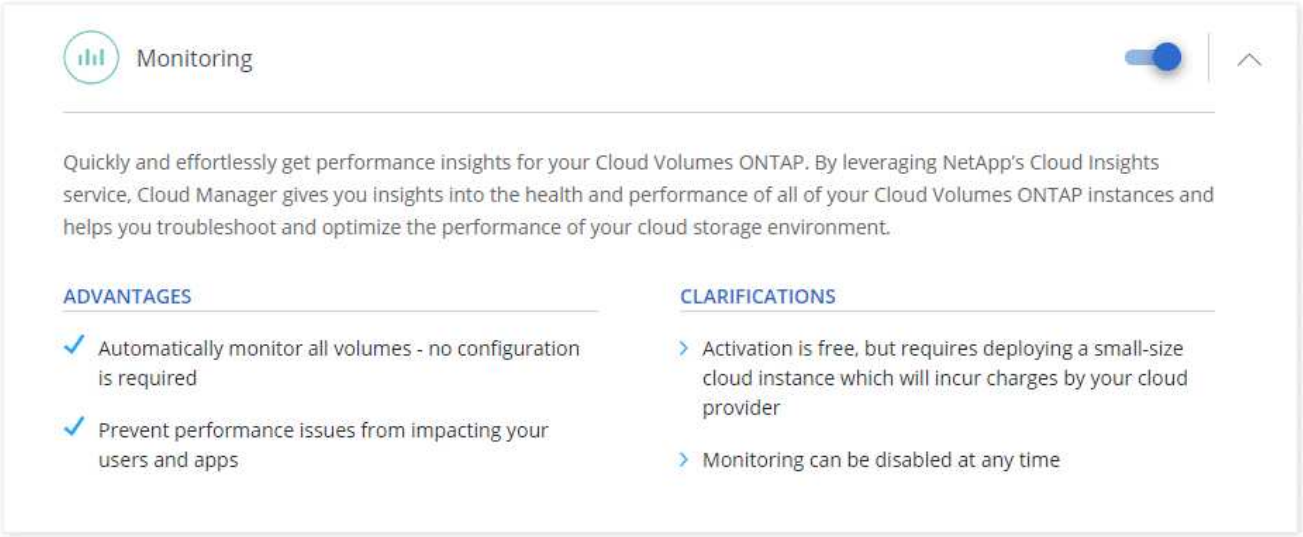
如果您需要識別租戶主機 URL 的協助、也可以透過產品內對談與我們聯絡。

在新系統上啟用監控

監控服務預設會在工作環境精靈中啟用。請務必保持啟用選項。

步驟

1. 按一下「 * 建立 Cloud Volumes ONTAP 參考 * 」。
2. 選取 Amazon Web Services 做為雲端供應商、然後選擇單一節點或 HA 系統。
3. 填寫「詳細資料與認證」頁面。
4. 在「服務」頁面上、讓服務保持啟用狀態、然後按一下 * 繼續 * 。

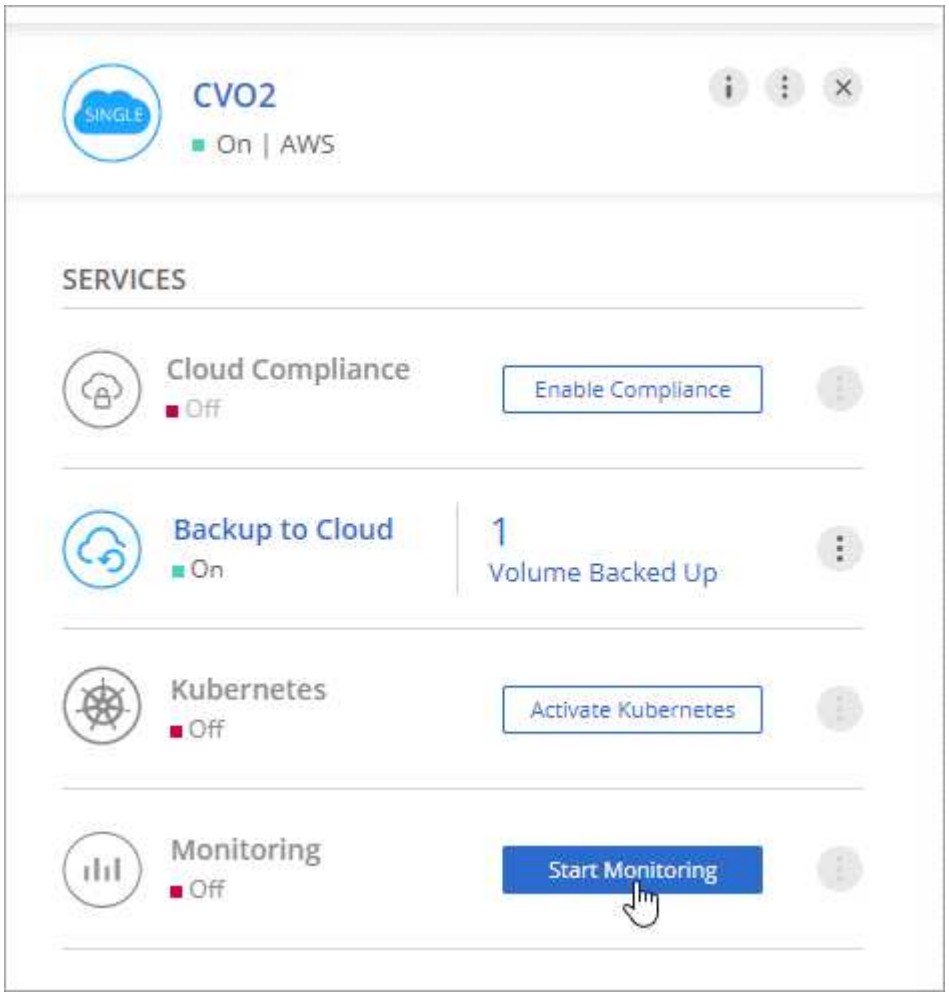


在現有系統上啟用監控

可隨時從工作環境進行監控。

步驟

1. 在Cloud Manager頂端、按一下*工作環境*。
2. 選取工作環境。
3. 在右側窗格中、按一下 * 開始監控 * 。



監控磁碟區

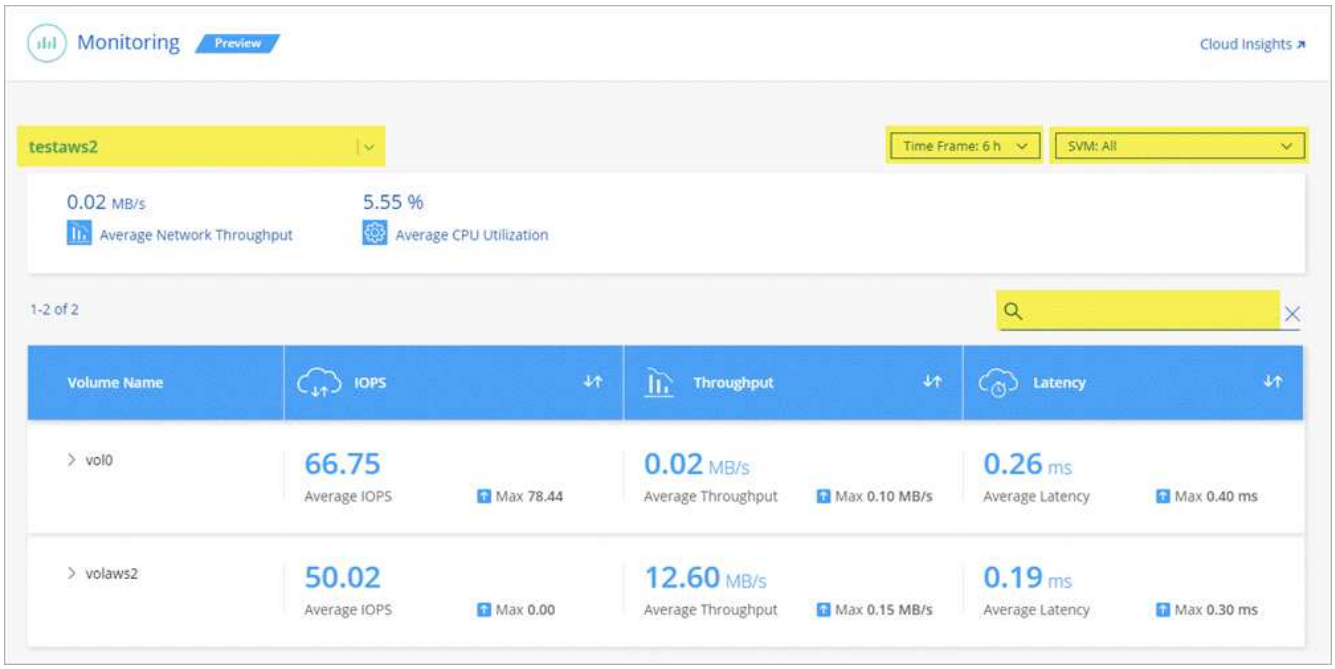
檢視每個磁碟區的 IOPS 、處理量和延遲、以監控效能。

步驟

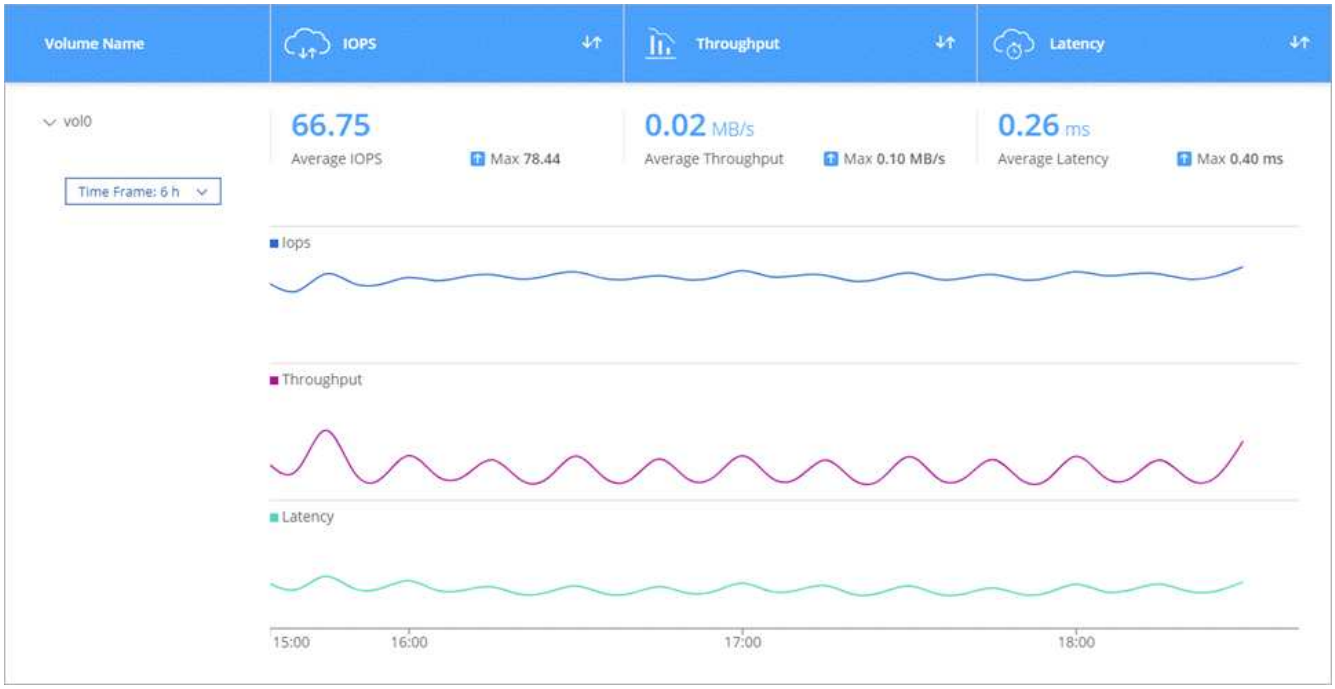
1. 在 Cloud Manager 頂端、按一下 * 監控 * 。
2. 篩選儀表板的內容、以取得所需的資訊。
   - 選取特定的工作環境。
   - 選取不同的時間範圍。
   - 選取特定 SVM 。

◦ 搜尋特定 Volume 。

下圖強調顯示每個選項：



3. 按一下表格中的磁碟區以展開該列、並檢視 IOPS 、處理量和延遲的時間表。



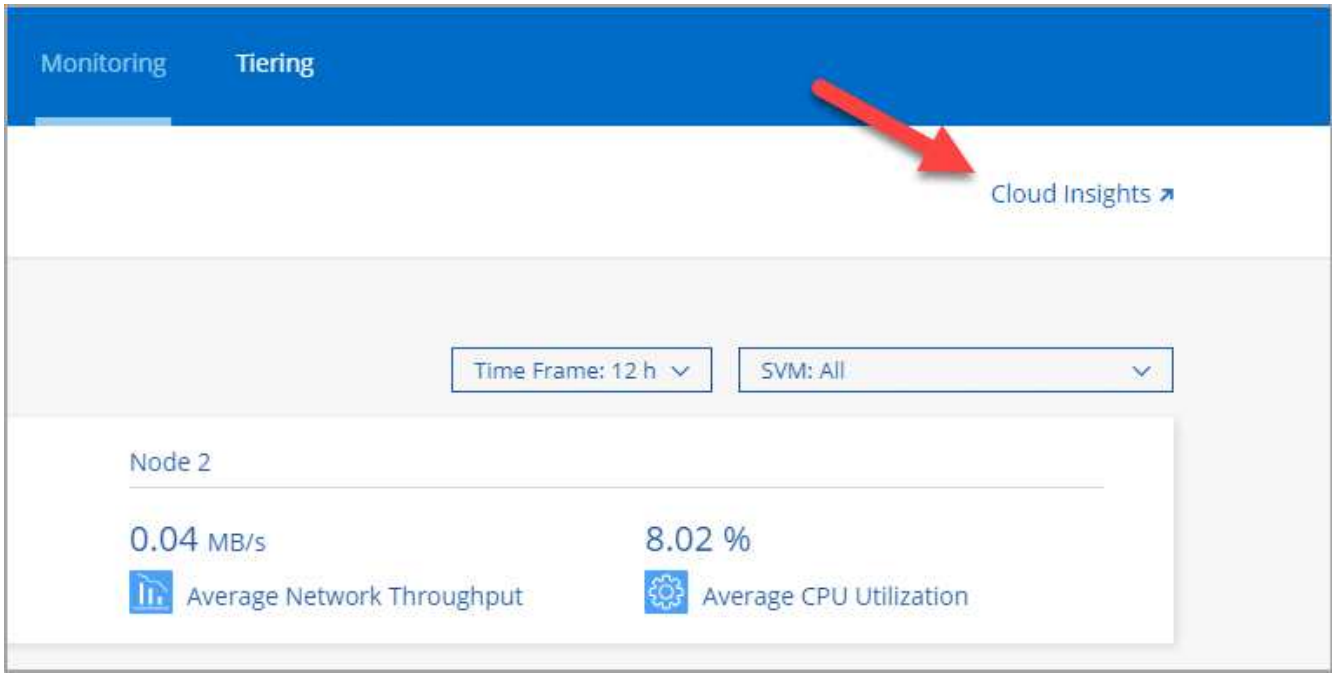
4. 使用資料找出效能問題、將對使用者和應用程式的影響降至最低。

取得 **Cloud Insights** 更多資訊

Cloud Manager 中的 Monitoring （監控）索引標籤可為您的磁碟區提供基本效能資料。您可以 Cloud Insights 從瀏覽器進入「靜態」網頁介面、以執行更深入的監控、並為 Cloud Volumes ONTAP 您的「靜態」系統設定警示。

步驟

1. 在 Cloud Manager 頂端、按一下 * 監控 * 。
2. 按一下 * Cloud Insights 《 * 》連結。



結果

可在新的瀏覽器索引標籤中開啟。 Cloud Insights如果您需要協助、請參閱 "本文檔 Cloud Insights"。

停用監控

如果您不想再監控 Cloud Volumes ONTAP 不穩定、可以隨時停用服務。

如果您停用每個工作環境的監控功能、則必須自行刪除 EC2 執行個體。執行個體名稱為 *AcquisitionUnity* 、其產生的雜湊（ UUID ）會串連在其中。例如： *AcquitionUnit-FAN7FqeH*

步驟

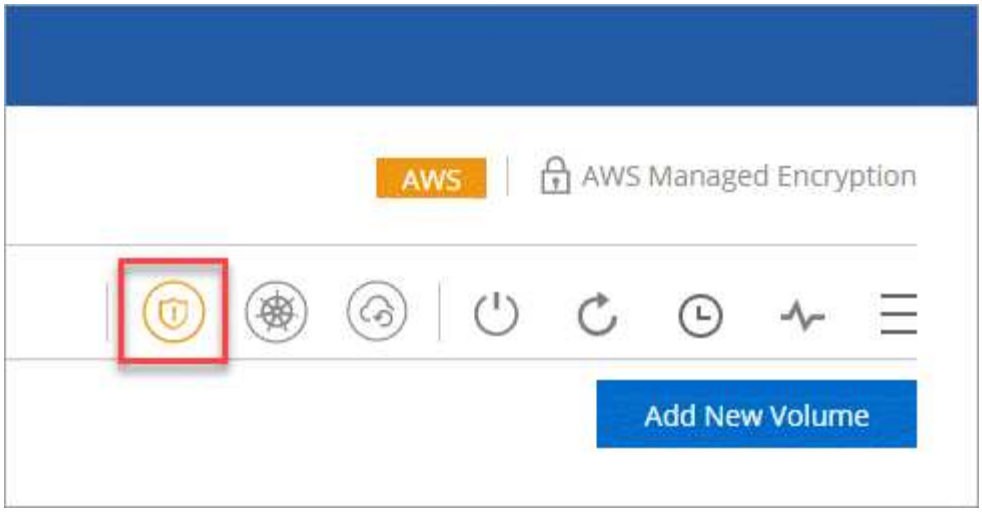
1. 在Cloud Manager頂端、按一下*工作環境*。
2. 選取工作環境。
3. 在右側窗格中、按一下 圖示並選取 * 停用掃描 * 。

改善防範勒索軟體的能力

勒索軟體攻擊可能會耗費一定的時間、資源和商譽。Cloud Manager 可讓您針對勒索軟體實作 NetApp 解決方案、提供有效的可見度、偵測及補救工具。

步驟

1. 在工作環境中、按一下 * 勒索軟體 * 圖示。



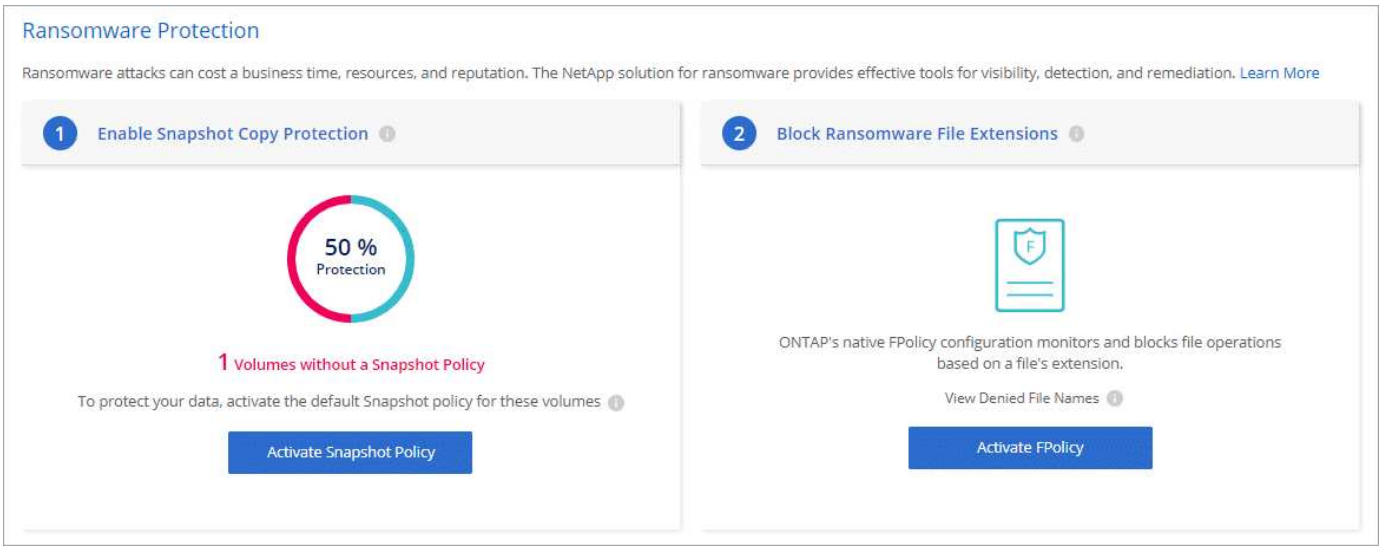
2. 實作 NetApp 勒索軟體解決方案：

   a. 如果您的磁碟區未啟用 Snapshot 原則、請按一下「 * 啟動 Snapshot Policy* 」。

      NetApp Snapshot 技術提供業界最佳的勒索軟體補救解決方案。成功還原的關鍵在於從未受感染的備份還原。Snapshot 複本為唯讀、可防止勒索軟體毀損。他們也能提供精細度、以建立單一檔案複本或完整災難恢復解決方案的映像。

   b. 按一下「 * 啟動 FPolicy* 」以啟用 ONTAP 的 FPolicy 解決方案、此解決方案可根據檔案副檔名來封鎖檔案作業。

      這項預防解決方案可封鎖常見的勒索軟體檔案類型、藉此改善保護、避免勒索軟體攻擊。



管理

註冊隨用隨付系統

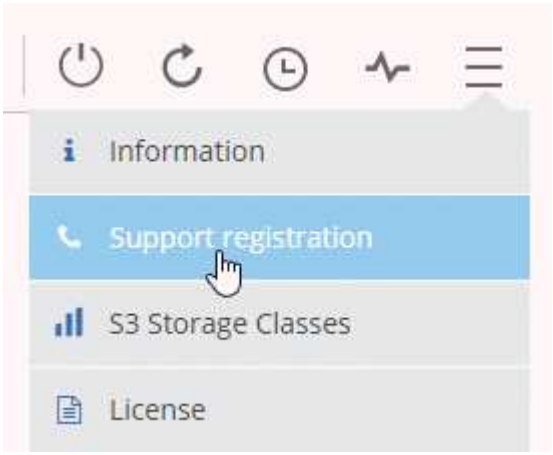
NetApp 的支援包含 Cloud Volumes ONTAP 在 NetApp 的《 Explore 》、《 Standard 》和《 Premium 》系統中、但您必須先向 NetApp 註冊系統、才能啟動支援。

步驟

1. 如果您尚未將 NetApp 支援網站帳戶新增至 Cloud Manager 、請前往 * 帳戶設定 * 、立即新增帳戶。

   "瞭解如何新增 NetApp 支援網站帳戶"。

2. 在「工作環境」頁面上、按兩下您要登錄的系統名稱。
3. 按一下功能表圖示、然後按一下 * 支援註冊 * ：



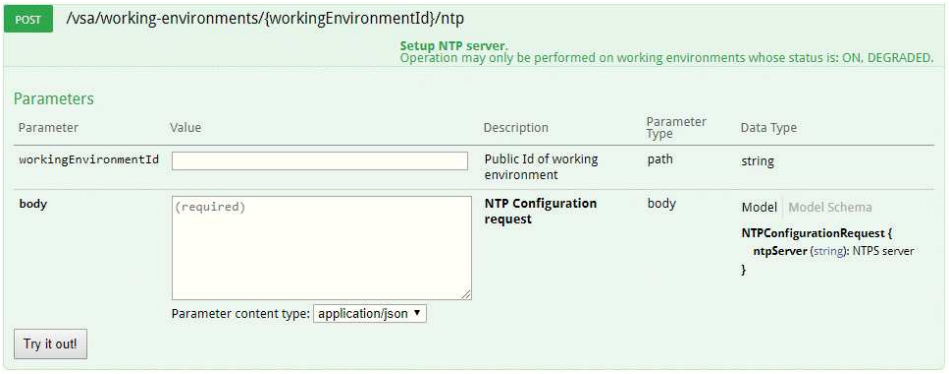
4. 選擇 NetApp 支援網站帳戶、然後按一下 * 註冊 * 。

結果

Cloud Manager 會向 NetApp 註冊系統。

設定 **Cloud Volumes ONTAP** 功能

部署 Cloud Volumes ONTAP 完整套功能後、您可以使用 NTP 同步系統時間、並從 System Manager 或 CLI 執行幾項選用工作來設定。

工作	說明
使用 NTP 同步系統時間	指定 NTP 伺服器可同步處理網路中系統之間的時間、有助於避免時間差異所造成的問題。 在設定 CIFS 伺服器時、使用 Cloud Manager API 或從使用者介面指定 NTP 伺服器。 • "修改 CIFS 伺服器" • "Cloud Manager API 開發人員指南" 例如、以下是 AWS 中單節點系統的 API ： 
選用：設定 AutoSupport 功能	可主動監控系統健全狀況、並依預設自動傳送訊息給 NetApp 技術支援部門。AutoSupport如果帳戶管理員在您啟動執行個體之前、已將 Proxy 伺服器新增至 Cloud Manager 、 Cloud Volumes ONTAP 則會將此伺服器設定為使用該 Proxy 伺服器來接收 AutoSupport 資訊。您應該測試 AutoSupport 此功能、以確保它能傳送訊息。如需相關指示、請參閱系統管理員說明或 "《系統管理參考資料》（英文） ONTAP"。
選用：將 Cloud Manager 設定為 AutoSupport 不受影響的 Proxy	如果您的環境需要 Proxy 伺服器來傳送 AutoSupport 功能不全的訊息、您可以設定 Cloud Manager 做為 Proxy 。除了網際網路存取、不需要 Cloud Manager 的組態。您只需移至 CLI Cloud Volumes ONTAP 執行下列命令即可執行下列功能： `system node autosupport modify -proxy-url <cloud-manager-ip-address>`
選用：設定 EMS	事件管理系統（ EMS ）會收集 Cloud Volumes ONTAP 並顯示有關發生在故障系統上的事件資訊。若要接收事件通知、您可以針對特定事件嚴重性設定事件目的地（電子郵件地址、 SNMP 設陷主機或 syslog 伺服器）和事件路由。您可以使用 CLI 設定 EMS 。如需相關指示、請參閱 "《 9 EMS 組態快速指南》 ONTAP"。

工作	說明
選用：在多個 AWS 可用性區域中、為 HA 系統建立 SVM 管理網路介面（ LIF ）	如果您想搭配 SnapCenter HA 配對使用 Windows 的功能、則需要儲存虛擬機器（ SVM ）管理網路介面（ LIF ） SnapDrive 。當在多個 AWS 可用區域之間使用 HA 配對時、 SVM 管理 LIF 必須使用 _浮 點 IP 位址。 Cloud Manager 會在您啟動 HA 配對時提示您指定浮動 IP 位址。如果未指定 IP 位址、您可以從 System Manager 或 CLI 自行建立 SVM 管理 LIF 。以下範例說明如何從 CLI 建立 LIF ： `network interface create -vserver svm_cloud -lif svm_mgmt -role data -data-protocol none -home-node cloud-01 -home-port e0a -address 10.0.2.126 -netmask 255.255.255.0 -status-admin up -firewall -policy mgmt`
選用：變更組態檔的備份位置	支援自動建立組態備份檔案、其中包含可設定選項的相關資訊、這些選項需要適當操作。 Cloud Volumes ONTAP根據預設 Cloud Volumes ONTAP 、每八小時將檔案備份至 Connector 主機。如果您想要將備份傳送到其他位置、可以將位置變更為資料中心或 AWS 中的 FTP 或 HTTP 伺服器。例如 FAS 、您可能已經有一個適用於您的支援系統的備份位置。您可以使用 CLI 變更備份位置。請參閱 "《系統管理參考資料》（英文） ONTAP"。

管理 BYOL 授權 Cloud Volumes ONTAP 以利執行

新增 Cloud Volumes ONTAP 一個「功能完善」系統授權、以新增額外容量、更新現有的系統授權、以及管理「備份至雲端」的 BYOL 授權。

管理系統授權

您可以購買 Cloud Volumes ONTAP 多個適用於某個不含資料的 BYOL 系統授權、以配置超過 368TB 的容量。例如、您可能會購買兩份授權、以配置多達 736 TB 的容量來 Cloud Volumes ONTAP 供參考。或者、您也可以購買四份授權、最高可達 1.4 PB 。

單一節點系統或 HA 配對可購買的授權數量不受限制。

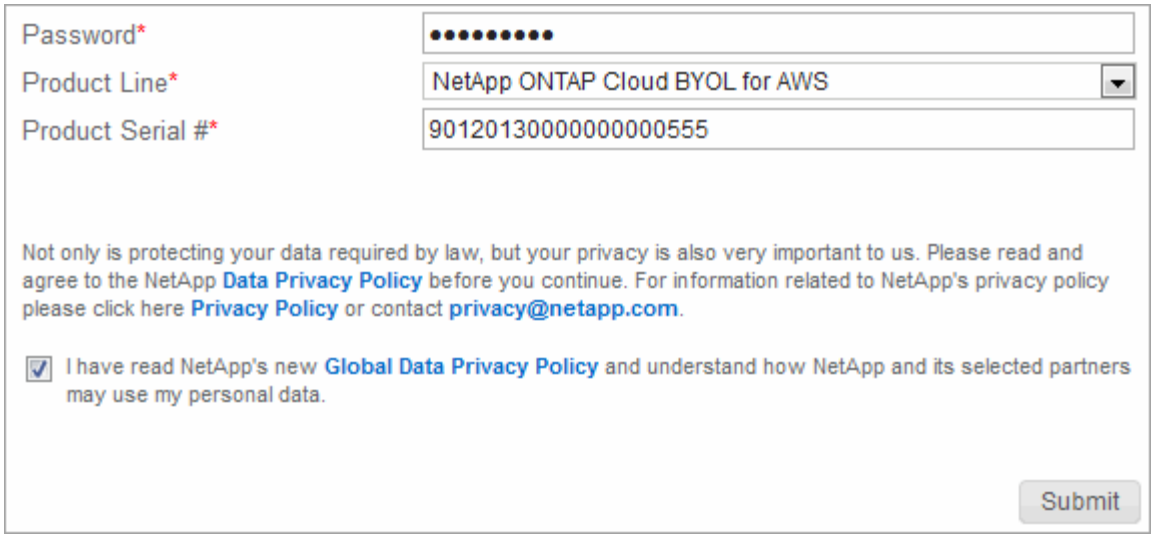
取得系統授權檔案

在大多數情況下、 Cloud Manager 會使用您的 NetApp 支援網站帳戶自動取得授權檔案。但如果無法、則需要手動上傳授權檔案。如果您沒有授權檔案、可以從 netapp.com 取得。

步驟

1. 前往 "NetApp 授權檔案產生器" 並使用您的 NetApp 支援網站認證登入。
2. 輸入您的密碼、選擇產品、輸入序號、確認您已閱讀並接受隱私權政策、然後按一下 * 提交 * 。

    。範例 *



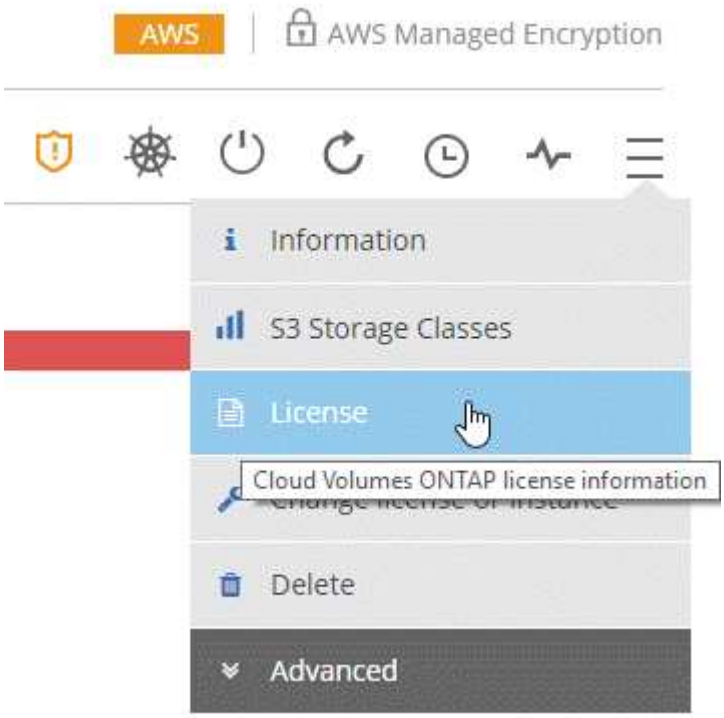
3. 選擇您要透過電子郵件或直接下載來接收 serialNumber.NLF Json 檔案。

新增系統授權

隨時新增 BYOL 系統授權、為 Cloud Volumes ONTAP 您的 BYOL 系統分配額外的 368TB 容量。

步驟

1. 在 Cloud Manager 中、開啟 Cloud Volumes ONTAP 「 NetApp BYOL 」工作環境。
2. 按一下功能表圖示、然後按一下 * 授權 * 。



3. 按一下 * 新增 CVO 系統授權 * 。

4. 選擇輸入序號或上傳授權檔案。
5. 按一下「 * 新增授權 * 」。

結果

Cloud Manager 會將新的授權檔案安裝在 Cloud Volumes ONTAP 更新的作業系統上。

更新系統授權

當您透過聯絡 NetApp 代表續約 BYOL 訂閱時、 Cloud Manager 會自動從 NetApp 取得新授權、並將其安裝在 Cloud Volumes ONTAP 該系統上。

如果 Cloud Manager 無法透過安全的網際網路連線存取授權檔案、您可以自行取得檔案、然後手動將檔案上傳至 Cloud Manager 。

步驟

1. 在 Cloud Manager 中、開啟 Cloud Volumes ONTAP 「 NetApp BYOL 」工作環境。
2. 按一下功能表圖示、然後按一下 * 授權 * 。
3. 按一下 * 更新 CVO 系統授權 * 。

4. 按一下 * 上傳檔案 * 、然後選取授權檔案。
5. 按一下 * 更新授權 * 。

結果

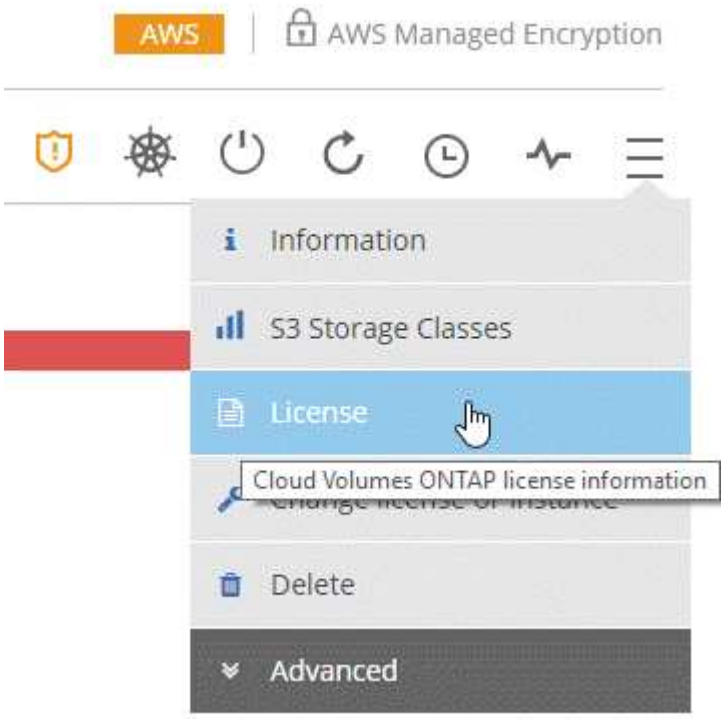
Cloud Manager 會更新 Cloud Volumes ONTAP 整個作業系統的授權。

新增及更新備份 **BYOL** 授權

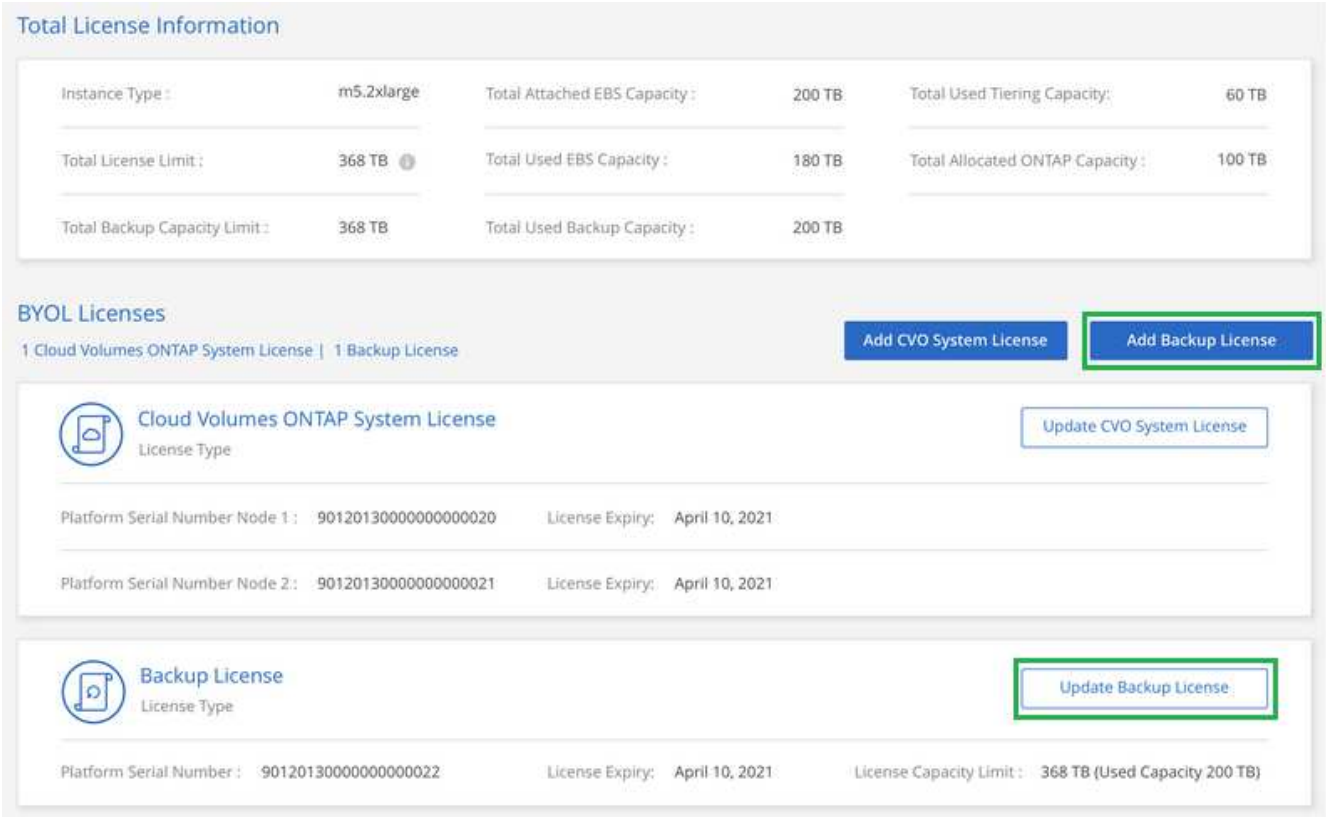
您可以使用「 BYOL 授權」頁面來新增或更新您的備份 BYOL 授權。

步驟

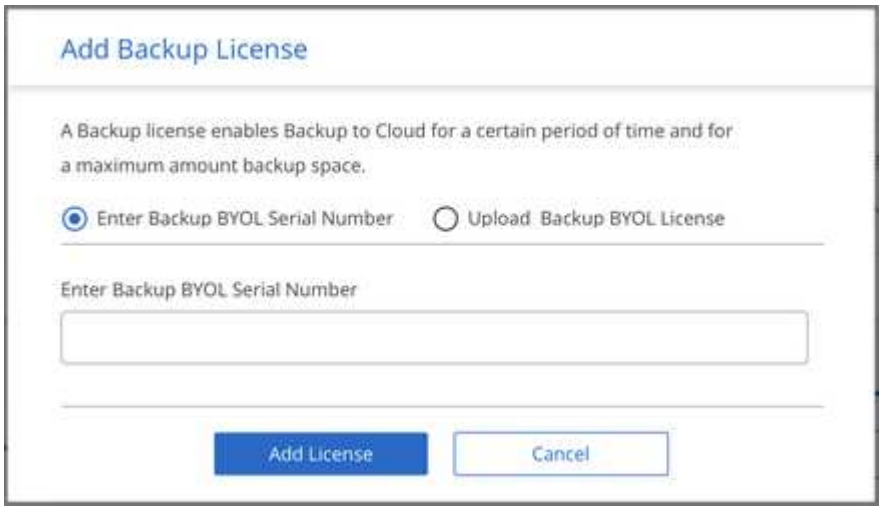
1. 在 Cloud Manager 中、開啟 Cloud Volumes ONTAP 「 NetApp BYOL 」工作環境。
2. 按一下功能表圖示、然後按一下 * 授權 * 。



3. 視您要新增授權或更新現有授權而定、按一下 * 「新增備份授權 * 」或 * 「更新備份授權 * 」。



4. 輸入授權資訊、然後按一下 * 新增授權 * ：
   - 如果您有序號、請選取 * 輸入備份 BYOL 序號 * 選項、然後輸入序號。
   - 如果您有備份授權檔案、請選取 * 上傳備份 BYOL 授權 * 選項、然後依照提示附加檔案。



結果

Cloud Manager 會新增或更新授權、讓您的 Backup to Cloud 服務處於作用中狀態。

更新**Cloud Volumes ONTAP** 軟體

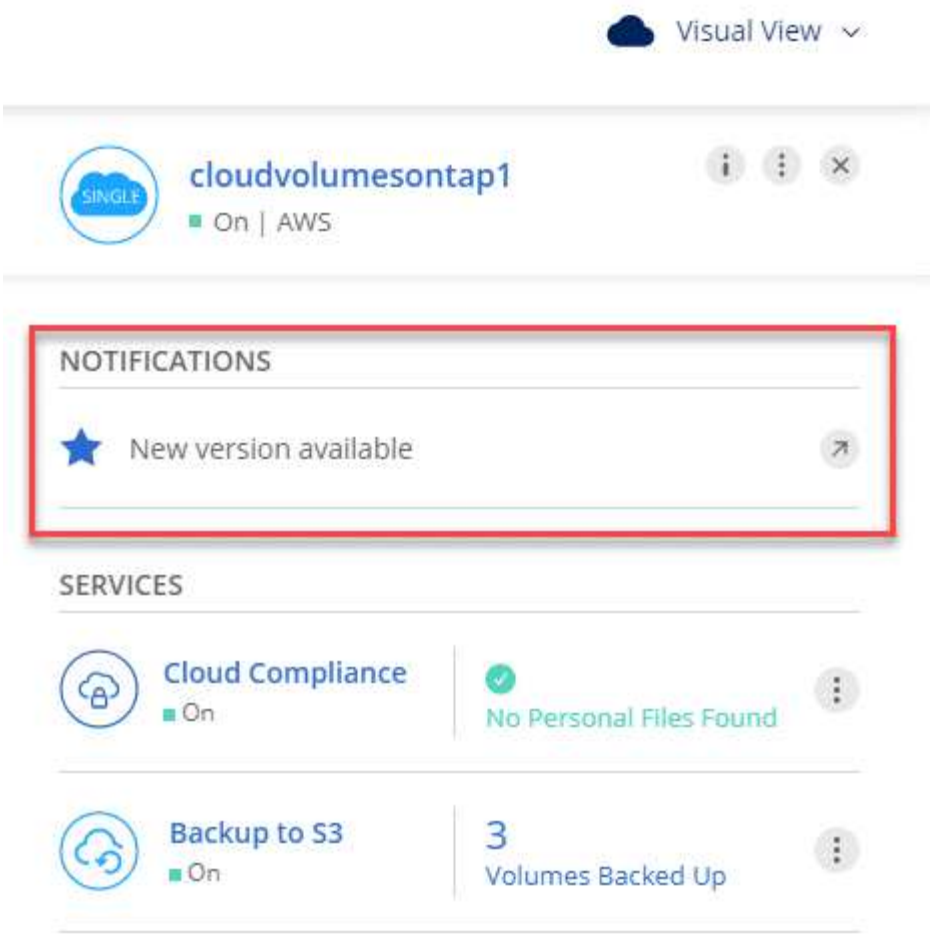
Cloud Manager提供多種選項、可讓您升級至目前Cloud Volumes ONTAP 的版本、或將Cloud Volumes ONTAP 版本降級至舊版。升級或降級軟體之前、您應該先準備Cloud Volumes ONTAP 好用的不一樣系統。

軟體更新必須由**Cloud Manager**完成

必須從 Cloud Manager 完成升級。 Cloud Volumes ONTAP您不應 Cloud Volumes ONTAP 使用 System Manager 或 CLI 來升級功能。這樣做可能會影響系統穩定性。

更新**Cloud Volumes ONTAP** 方法

Cloud Manager Cloud Volumes ONTAP 會在出現新版 Cloud Volumes ONTAP 的功能時、於不支援功能的環境中顯示通知：



您可以從此通知開始升級程序、從 S3 儲存區取得軟體映像、安裝映像、然後重新啟動系統、藉此自動化程序。如需詳細資訊、請參閱 從 Cloud Volumes ONTAP Cloud Manager 通知升級。

對於 AWS 中的 HA 系統、 Cloud Manager 可能會將 HA 中介程式升級為升級程序的一部分。

軟體更新的進階選項

Cloud Manager也提供下列進階選項來更新Cloud Volumes ONTAP 支援的功能：

- 使用外部URL上的映像進行軟體更新

  如果Cloud Manager無法存取S3儲存區來升級軟體、如果您已取得修補程式、或您想要將軟體降級至特定版本、此選項就很有幫助。

  如需詳細資訊、請參閱 使用HTTP或FTP伺服器升級Cloud Volumes ONTAP 或降級。

- 使用系統上的替代映像進行軟體更新

  您可以使用此選項將替代軟體映像設為預設映像、以降級至舊版。此選項不適用於 HA 配對。

  如需詳細資訊、請參閱 使用本機映像降級Cloud Volumes ONTAP。

準備更新Cloud Volumes ONTAP 軟件

在執行升級或降級之前、您必須先確認系統已就緒、並進行任何必要的組態變更。

- [規劃停機時間]
- [檢閱版本需求]
- [驗證是否仍啟用自動還原]
- 暫停 SnapMirror 傳輸
- 驗證 Aggregate 是否在線上

規劃停機時間

當您升級單節點系統時、升級程序會使系統離線長達 25 分鐘、在此期間 I/O 會中斷。

升級 HA 配對不中斷營運、而且 I/O 不中斷。在此不中斷營運的升級程序中、會同時升級每個節點、以繼續為用戶端提供 I/O 服務。

檢閱版本需求

您可以升級或降級至的版本會因系統上目前執行的版本不一而有所差異。ONTAP ONTAP

若要瞭解版本需求、請參閱 "VMware Update文檔：叢集更新要求ONTAP"。

驗證是否仍啟用自動還原

自動恢復必須在 Cloud Volumes ONTAP 一個「無法恢復的 HA 配對」上啟用（這是預設設定）。如果沒有、則作業將會失敗。

"供應說明文件：設定自動恢復的命令 ONTAP"

暫停 **SnapMirror** 傳輸

如果 Cloud Volumes ONTAP 某個不活躍的 SnapMirror 關係、最好在更新 Cloud Volumes ONTAP 該軟件之前暫停傳輸。暫停傳輸可防止 SnapMirror 故障。您必須暫停來自目的地系統的傳輸。

關於這項工作

這些步驟說明如何使用系統管理程式來執行 9.3 版及更新版本。

步驟

1. "登入 System Manager" 從目的地系統。
2. 按一下 * 保護 > 關係 * 。
3. 選取關係、然後按一下 * 作業 > 靜止 * 。

驗證 **Aggregate** 是否在線上

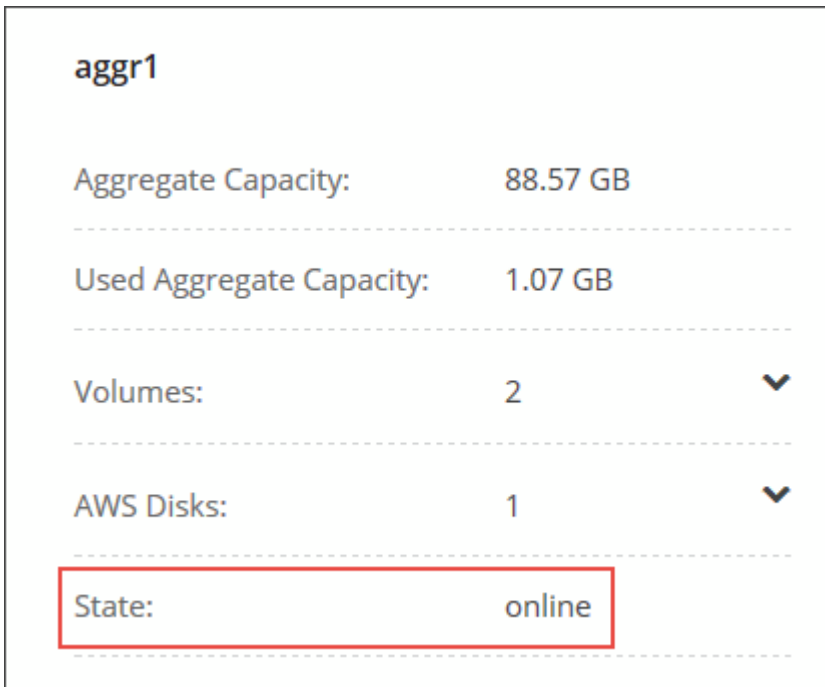
更新軟體之前、必須先在線上安裝適用於 Cloud Volumes ONTAP 此功能的 Aggregate 。在大多數的組態中、Aggregate 都應該處於線上狀態、但如果沒有、則應該將其上線。

關於這項工作

這些步驟說明如何使用系統管理程式來執行 9.3 版及更新版本。

步驟

1. 在工作環境中、按一下功能表圖示、然後按一下 * 進階 > 進階配置 * 。
2. 選取 Aggregate 、按一下 * Info* 、然後確認狀態為線上。



3. 如果 Aggregate 離線、請使用 System Manager 將 Aggregate 上線：
   a. "登入 System Manager"。
   b. 按一下「 * 儲存設備 > 集合體與磁碟 > Aggregate * 」 。
   c. 選取 Aggregate 、然後按一下 * 更多動作 > 狀態 > 線上 * 。

從 **Cloud Volumes ONTAP Cloud Manager** 通知升級

Cloud Manager 會在 Cloud Volumes ONTAP 推出新版的功能時通知您。按一下通知以開始升級程序。

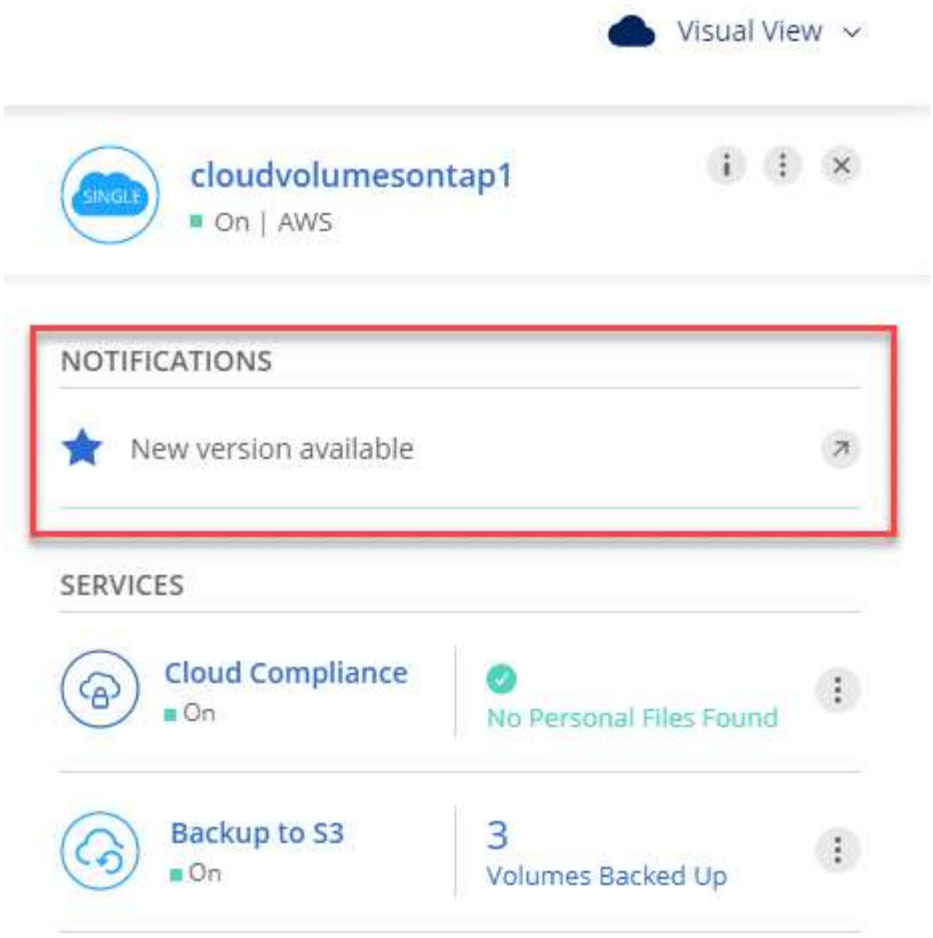
開始之前

Cloud Manager 的作業（例如 Volume 或 Aggregate 建立）不得在 Cloud Volumes ONTAP 進行中、以利執行。

步驟

1. 按一下*工作環境*。
2. 選取工作環境。

   如果有新版本可用、則右窗格中會出現通知：



3. 如果有可用的新版本、請按一下 * 升級 * 。
4. 在「版本資訊」頁面中、按一下連結以閱讀指定版本的「版本說明」、然後選取「 * 我讀過 … * 」核取方塊。
5. 在「終端使用者授權合約（ EULA ）」頁面中、閱讀 EULA 、然後選取「 * 我閱讀並核准 EULA* 」。
6. 在「檢閱與核准」頁面中、閱讀重要附註、選取 * 我瞭解 …* 、然後按一下 * 執行 * 。

結果

Cloud Manager 會啟動軟體升級。軟體更新完成後、即可在工作環境中執行動作。

完成後

如果您暫停 SnapMirror 傳輸、請使用 System Manager 繼續傳輸。

使用**HTTP**或**FTP**伺服器升級**Cloud Volumes ONTAP** 或降級

您可以將Cloud Volumes ONTAP 「更新」軟體映像放在HTTP或FTP伺服器上、然後從Cloud Manager啟動軟體更新。如果Cloud Manager無法存取S3儲存區來升級軟體、或是想要降級軟體、您可以使用此選項。

步驟

1. 設定 HTTP 伺服器或 FTP 伺服器、以裝載 Cloud Volumes ONTAP 支援此功能的軟體映像。
2. 如果您有虛擬網路的 VPN 連線、可以將 Cloud Volumes ONTAP 該 Imagesoftware 映像放在您自己網路中

的 HTTP 伺服器或 FTP 伺服器上。否則、您必須將檔案放在雲端的 HTTP 伺服器或 FTP 伺服器上。

3. 如果您使用自己的安全性群組 Cloud Volumes ONTAP 來執行功能、請確定傳出規則允許 HTTP 或 FTP 連線 Cloud Volumes ONTAP 、以便讓支援者存取軟體映像。

   預設的 Cloud Volumes ONTAP 「預先定義的功能」安全群組允許輸出 HTTP 和 FTP 連線。

4. 從取得軟體映像 "NetApp 支援網站"。
5. 將軟體映像複製到 HTTP 或 FTP 伺服器上的目錄、以便從中提供檔案。
6. 在 Cloud Manager 的工作環境中、按一下功能表圖示、然後按一下 * 進階 > 更新 Cloud Volumes ONTAP * 。
7. 在更新軟體頁面上、選擇 * 從 URL* 選取可用的映像、輸入 URL 、然後按一下 * 變更映像 * 。
8. 按 * Proceed* 確認。

結果

Cloud Manager 會啟動軟體更新。軟體更新完成後、即可在工作環境中執行動作。

完成後

如果您暫停 SnapMirror 傳輸、請使用 System Manager 繼續傳輸。

使用本機映像降級**Cloud Volumes ONTAP**

將同一版本系列中的某個舊版本（Cloud Volumes ONTAP 例如9.5至9.4）轉換為降級。降級新叢集或測試叢集時無需協助即可降級、但如果您想要降級正式作業叢集、請聯絡技術支援部門。

每 Cloud Volumes ONTAP 個功能完善的系統都能容納兩個軟體映像：目前執行的映像、以及可開機的替代映像。Cloud Manager 可將替代映像變更為預設映像。如果您目前的映像發生問題、可以使用此選項降級至Cloud Volumes ONTAP 舊版的版的版次。

關於這項工作

此降級程序Cloud Volumes ONTAP 僅適用於單一版的系統。HA配對無法使用此功能。

步驟

1. 在工作環境中、按一下功能表圖示、然後按一下 * 「進階」 > 「更新 Cloud Volumes ONTAP 」 * 。
2. 在更新軟體頁面上、選取替代映像、然後按一下 * 變更映像 * 。
3. 按 * Proceed* 確認。

結果

Cloud Manager 會啟動軟體更新。軟體更新完成後、即可在工作環境中執行動作。

完成後

如果您暫停 SnapMirror 傳輸、請使用 System Manager 繼續傳輸。

修改 **Cloud Volumes ONTAP** 功能系統

您可能需要在 Cloud Volumes ONTAP 儲存需求改變時、變更不必要的功能組態。例如、您可以在隨用隨付組態之間變更、變更執行個體或 VM 類型等。

變更 **Cloud Volumes ONTAP** 執行個體或機器類型以供使用

在 Cloud Volumes ONTAP AWS 、 Azure 或 GCP 中啟動時、您可以從多種執行個體或機器類型中進行選擇。如果判斷執行個體的大小過小或過大、您可以隨時變更執行個體或機器類型。

關於這項工作

- 自動恢復必須在 Cloud Volumes ONTAP 一個「無法恢復的 HA 配對」上啟用（這是預設設定）。如果沒有、則作業將會失敗。

  "供應說明文件：設定自動恢復的命令 ONTAP"

- 變更執行個體或機器類型會影響雲端供應商的服務費用。
- 此作業會重新啟動 Cloud Volumes ONTAP 。

  對於單一節點系統、 I/O 會中斷。

  對於 HA 配對、變更不中斷營運。HA 配對可繼續提供資料。

> Cloud Manager 會啟動接管作業並等待回饋、一次只能正常變更一個節點。NetApp 的 QA 團隊在這段過程中測試了寫入和讀取檔案的能力、並未發現客戶端有任何問題。隨著連線變更、我們確實看到 I/O 層級的重試次數、但應用程式層卻取代了 NFS/CIFS 連線的這些短「重新連線」。

步驟

1. 在工作環境中、按一下功能表圖示、然後按一下 * 變更 AWS 授權或執行個體 * 、 * 變更 Azure 授權或 VM* 、或 * 變更 GCP 授權或機器 * 。
2. 如果您使用的是隨用隨付組態、您可以選擇不同的授權。
3. 選取執行個體或機器類型、選取核取方塊以確認您瞭解變更的影響、然後按一下 * 確定 * 。

結果

以新組態重新開機。 Cloud Volumes ONTAP

在隨用隨付組態之間切換

啟動「隨用隨付 Cloud Volumes ONTAP 」功能的更新版本後、您可以隨時修改授權、以變更 Explore 、 Standard 和 Premium 組態。變更授權會增加或減少原始容量限制、並可讓您從不同的 AWS 執行個體類型或 Azure 虛擬機器類型中進行選擇。

> 在 GCP 中、每個隨用隨付組態都有一種機器類型可供使用。您無法在不同的機器類型之間進行選擇。

關於這項工作

請注意下列關於在隨用隨付授權之間變更的資訊：

- 此作業會重新啟動 Cloud Volumes ONTAP 。

  對於單一節點系統、 I/O 會中斷。

對於 HA 配對、變更不中斷營運。HA 配對可繼續提供資料。

- 變更執行個體或機器類型會影響雲端供應商的服務費用。

步驟

1. 在工作環境中、按一下功能表圖示、然後按一下 * 變更 AWS 授權或執行個體 * 、 * 變更 Azure 授權或 VM* 、或 * 變更 GCP 授權或機器 * 。
2. 選取授權類型和執行個體類型或機器類型、選取核取方塊以確認您瞭解變更的影響、然後按一下 * 確定 * 。

結果

使用新的授權、執行個體類型或機器類型重新開機、或同時使用兩者。 Cloud Volumes ONTAP

改用替代 **Cloud Volumes ONTAP** 的功能

如果您想要在隨用隨付訂閱和 BYOL 訂閱之間切換、或是在單 Cloud Volumes ONTAP 一版的不間斷系統和 HA 配對之間切換、則需要部署新系統、然後將資料從現有系統複寫到新系統。

步驟

1. 打造全新 Cloud Volumes ONTAP 的運作環境。

   "在 Cloud Volumes ONTAP AWS 中啟動"
   "在 Cloud Volumes ONTAP Azure 中啟動"
   "在 Cloud Volumes ONTAP GCP 中啟動"

2. "設定一次性資料複寫" 每個必須複寫的磁碟區的系統之間。
3. 終止 Cloud Volumes ONTAP 不再需要的作業系統 "刪除原始工作環境"。

將寫入速度變更為正常或高速

Cloud Manager可讓您選擇單一節點Cloud Volumes ONTAP 的寫入速度設定。預設寫入速度為正常。如果工作負載需要快速寫入效能、您可以改為高速寫入。在變更寫入速度之前、您應該先進行 "瞭解一般與高設定之間的差異"。

關於這項工作

- 確保磁碟區或集合體建立等作業未在進行中。
- 請注意、這項變更會重新啟動Cloud Volumes ONTAP 、這表示I/O中斷。

步驟

1. 在工作環境中、按一下功能表圖示、然後按一下 * 進階 > 寫入速度 * 。
2. 選擇 * 正常 * 或 * 高 * 。

   如果您選擇「高」、則必須閱讀「我瞭解 … 」聲明、並勾選方塊以確認。

3. 按一下「 * 儲存 * 」、檢閱確認訊息、然後按一下「 * 繼續 * 」。

修改儲存 **VM** 名稱

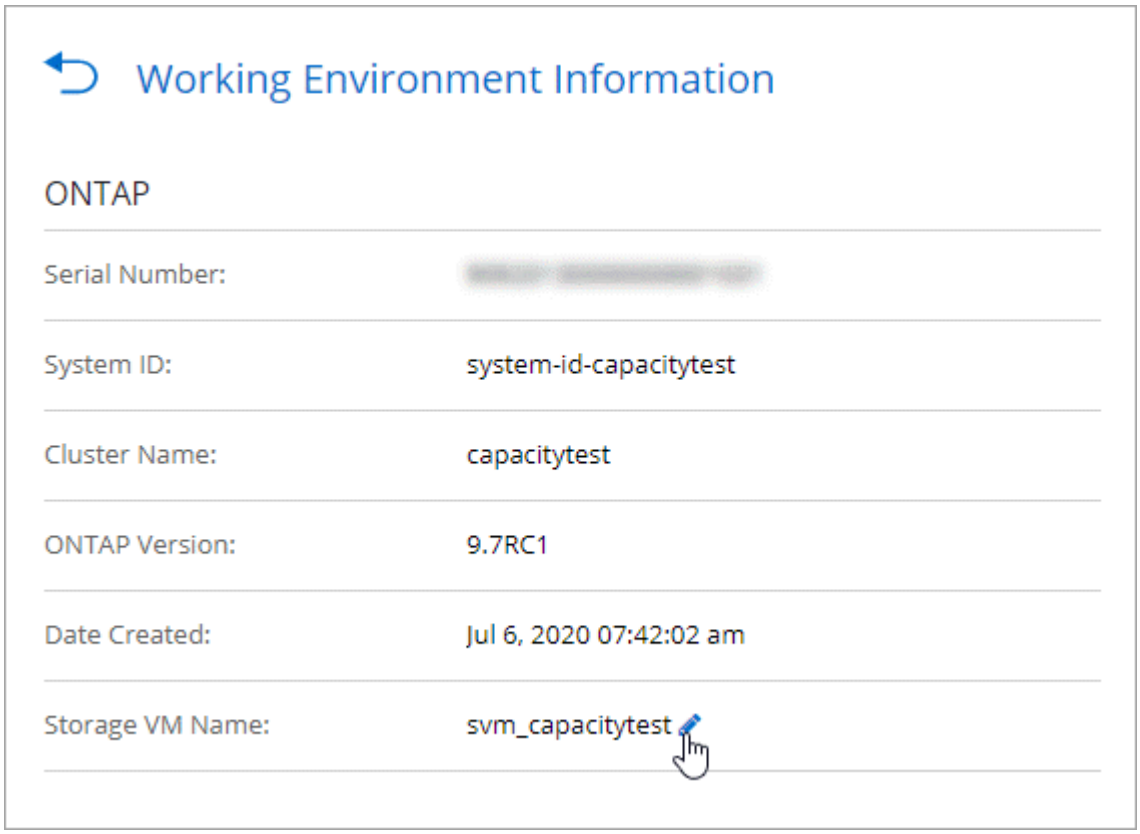
Cloud Manager 會自動為其建立的單一儲存 VM （ SVM ）命名 Cloud Volumes ONTAP 、以供其使用。如果您有嚴格的命名標準、可以修改 SVM 的名稱。例如、您可能希望名稱與您為 ONTAP 自己的叢集命名 SVM 的方

式相符。

但是如果您建立 Cloud Volumes ONTAP 任何其他的 SVM 來進行支援、那麼您就無法從 Cloud Manager 重新命名 SVM 。您必須 Cloud Volumes ONTAP 使用 System Manager 或 CLI 直接從支援功能進行此作業。

步驟

1. 在工作環境中、按一下功能表圖示、然後按一下 * 資訊 * 。
2. 按一下儲存 VM 名稱右側的編輯圖示。



3. 在「修改 SVM 名稱」對話方塊中、變更名稱、然後按一下「 * 儲存 * 」。

變更 **Cloud Volumes ONTAP** 密碼以供使用

包含叢集管理帳戶。 Cloud Volumes ONTAP如有需要、您可以從 Cloud Manager 變更此帳戶的密碼。

您不應透過 System Manager 或 CLI 變更管理帳戶的密碼。密碼不會反映在 Cloud Manager 中。因此 Cloud Manager 無法正確監控執行個體。

步驟

1. 在工作環境中、按一下功能表圖示、然後按一下 * 進階 > 設定密碼 * 。
2. 輸入新密碼兩次、然後按一下「 * 儲存 * 」。

   新密碼必須與您最近使用的六個密碼之一不同。

變更 **c4.4xLarge** 和 **c4.8xLarge** 執行個體的網路 **MTU**

根據預設、 Cloud Volumes ONTAP 當您在 AWS 中選擇 c4.4xlarge 執行個體或 c4.8xlarge 執行個體時、將使用 9 、 000 MTU （也稱為巨型框架）。如果網路 MTU 更適合您的網路組態、您可以將其變更為 1 、 500 位元組。

關於這項工作

網路最大傳輸單元（ MTU ）可提供特定組態所能達到的最高網路處理量。

如果同一 VPC 中的用戶端與 Cloud Volumes ONTAP 該系統通訊、而部分或所有用戶端也支援 9 、 000 MTU 、則是理想的選擇。如果流量離開 VPC 、可能會發生封包分散、進而降低效能。

如果 VPC 外部的用戶端或系統與 Cloud Volumes ONTAP 該系統通訊、則使用 1 、 500 位元組的網路 MTU 是很好的選擇。

步驟

1. 在工作環境中、按一下功能表圖示、然後按一下 * 進階 > 網路使用率 * 。
2. 選擇 * 標準 * 或 * 巨型框架 * 。
3. 按一下 * 變更 * 。

在多個 **AWS AZs** 中變更與 **HA** 配對相關的路由表

您可以修改 AWS 路由表、其中包含通往 HA 配對浮動 IP 位址的路由。如果新的 NFS 或 CIFS 用戶端需要存取 AWS 中的 HA 配對、您可以這麼做。

步驟

1. 在工作環境中、按一下功能表圖示、然後按一下 * 資訊 * 。
2. 按一下 * 路由表 * 。
3. 修改所選路由表的清單、然後按一下「 * 儲存 * 」。

結果

Cloud Manager 會傳送 AWS 要求來修改路由表。

管理 **Cloud Volumes ONTAP** 功能不全

您可以從 Cloud Volumes ONTAP Cloud Manager 停止並開始執行功能、以管理雲端運算成本。

排程 **Cloud Volumes ONTAP** 自動關閉功能

您可能想要在 Cloud Volumes ONTAP 特定時間間隔內關閉此功能、以降低運算成本。您可以將 Cloud Manager 設定為在特定時間自動關機、然後重新啟動系統、而非手動執行此動作。

關於這項工作

排定 Cloud Volumes ONTAP 自動關機功能時、如果執行中的資料傳輸正在進行、 Cloud Manager 會將關機時間延後。Cloud Manager 會在傳輸完成後關閉系統。

此工作會排程 HA 配對中兩個節點的自動關機。

步驟

1. 在工作環境中、按一下時鐘圖示：

2. 指定關機排程：

   a. 選擇您要每天、每個工作日、每個週末或三種選項的任意組合來關閉系統。

   b. 指定您要關閉系統的時間、以及關閉系統的時間長度。

      ▪ 範例 *

      下圖顯示每週六上午 12 ： 00 指示 Cloud Manager 關閉系統的排程48 小時。Cloud Manager 每週一上午 12 ： 00 重新啟動系統

3. 按一下「 * 儲存 * 」 。

結果

Cloud Manager 會儲存排程。時鐘圖示會變更、表示已設定排程：

停止 **Cloud Volumes ONTAP**

停止 Cloud Volumes ONTAP 使用功能可節省運算成本、並建立根磁碟和開機磁碟的快照、有助於疑難排解。

關於這項工作

當您停止 HA 配對時、 Cloud Manager 會關閉兩個節點。

步驟

1. 在工作環境中、按一下 * 關閉 * 圖示。

2. 保留建立快照的選項、因為快照可以啟用系統還原。

3. 按一下 * 關閉 * 。

   停止系統可能需要幾分鐘的時間。您可以稍後從工作環境頁面重新啟動系統。

監控 AWS 資源成本

Cloud Manager 可讓您檢視在 Cloud Volumes ONTAP AWS 中執行功能的相關資源成本。您也可以瞭解使用 NetApp 功能來降低儲存成本、省下多少成本。

關於這項工作

當您重新整理頁面時、 Cloud Manager 會更新成本。如需最終成本詳細資料、請參閱 AWS 。

步驟

1. 確認 Cloud Manager 可從 AWS 取得成本資訊：
   a. 確保提供 Cloud Manager 權限的 IAM 原則包括下列動作：

      ```
      "ce:GetReservationUtilization",
      "ce:GetDimensionValues",
      "ce:GetCostAndUsage",
      "ce:GetTags"
      ```

      這些行動包含在最新的中 "Cloud Manager 原則"。從 NetApp Cloud Central 部署的新系統會自動包含這些權限。

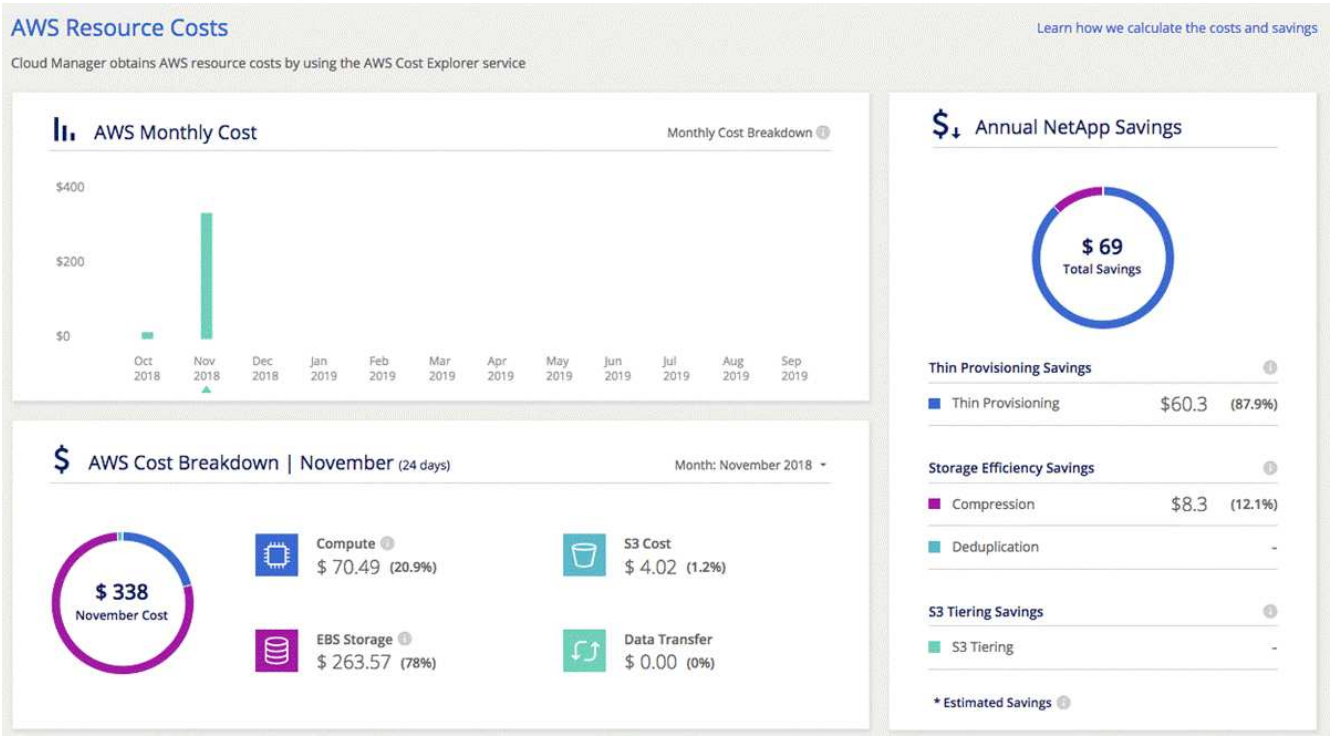
   b. "啟動 * 工作環境 Id* 標籤"。

      為了追蹤 AWS 成本、 Cloud Manager 會指派成本分配標籤給 Cloud Volumes ONTAP 各個執行個體。建立第一個工作環境之後、請啟動 * 工作環境 Id* 標籤。使用者定義的標記不會出現在 AWS 帳單報告上、除非您在帳單和成本管理主控台中啟動它們。

2. 在「工作環境」頁面上、選取Cloud Volumes ONTAP 一個「運作環境」、然後按一下「成本」。

   「成本」頁面會顯示目前和過去幾個月的成本、並顯示您每年的 NetApp 節約效益（如果您已啟用 NetApp 的 Volume 節約功能）。

   下圖顯示成本頁範例：



連線 **Cloud Volumes ONTAP** 至

如果您需要執行 Cloud Volumes ONTAP 進階的支援管理功能、可以使用 OnCommand 支援功能的支援中心或命令列介面來執行。

正在連線至 **System Manager**

您可能需要從 Cloud Volumes ONTAP System Manager 執行部分功能、 System Manager 是一種瀏覽器型管理工具、可在 Cloud Volumes ONTAP 整個系統上執行。例如、如果您想要建立 LUN 、則需要使用 System Manager 。

開始之前

您要從其中存取 Cloud Manager 的電腦、必須有連至 Cloud Volumes ONTAP NetApp 的網路連線。例如、您可能需要從 AWS 或 Azure 的跨接主機登入 Cloud Manager 。

> 當部署於多個 AWS 可用性區域時、 Cloud Volumes ONTAP 使用浮動 IP 位址進行叢集管理介面、這表示外部路由無法使用。您必須從屬於同一個路由網域的主機連線。

步驟

1. 在「工作環境」頁面中、按兩下Cloud Volumes ONTAP 您要使用System Manager管理的「功能完善」系統。
2. 按一下功能表圖示、然後按一下 * 進階 > 系統管理員 * 。
3. 按一下 * 「 Launch * 」 。

   系統管理程式會載入新的瀏覽器索引標籤。

4. 在登入畫面的「使用者名稱」欄位中輸入 * admin* 、輸入您在建立工作環境時所指定的密碼、然後按一下 * 登入 * 。

結果

系統管理程式主控台會載入。您現在可以使用它來管理 Cloud Volumes ONTAP 功能。

連線 **Cloud Volumes ONTAP** 至 **CLI**

利用此功能、您可以執行所有的管理命令、這是進階工作或使用 CLI 時的最佳選擇。 Cloud Volumes ONTAP您可以使用 Secure Shell （ SSH ）連線至 CLI 。

開始之前

您使用 SSH 連線 Cloud Volumes ONTAP 到 Suse 的主機必須有連至 Cloud Volumes ONTAP Suse 的網路連線。例如、您可能需要從 AWS 或 Azure 中的跨接主機使用 SSH 。

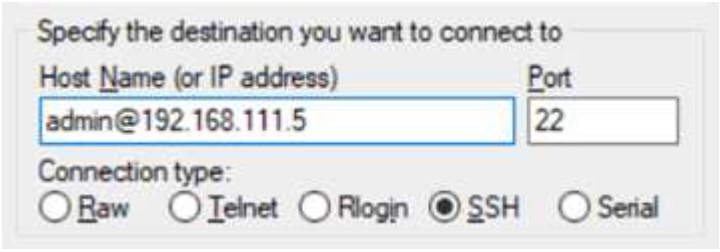
當部署於多個 AZs 時 Cloud Volumes ONTAP 、使用浮動 IP 位址進行叢集管理介面、這表示外部路由無法使用。您必須從屬於同一個路由網域的主機連線。

步驟

1. 在 Cloud Manager 中、識別叢集管理介面的 IP 位址：
   a. 在「工作環境」頁面上、選取Cloud Volumes ONTAP 「不適用系統」。
   b. 複製右窗格中顯示的叢集管理 IP 位址。
2. 使用 SSH 連線至使用管理帳戶的叢集管理介面 IP 位址。

   ◦ 範例 *

   下圖顯示使用 Putty 的範例：



3. 在登入提示下、輸入 admin 帳戶的密碼。

   ◦ 範例 *

```
Password: ********
COT2::>
```

將現有 **Cloud Volumes ONTAP** 的功能系統新增至 **Cloud Manager**

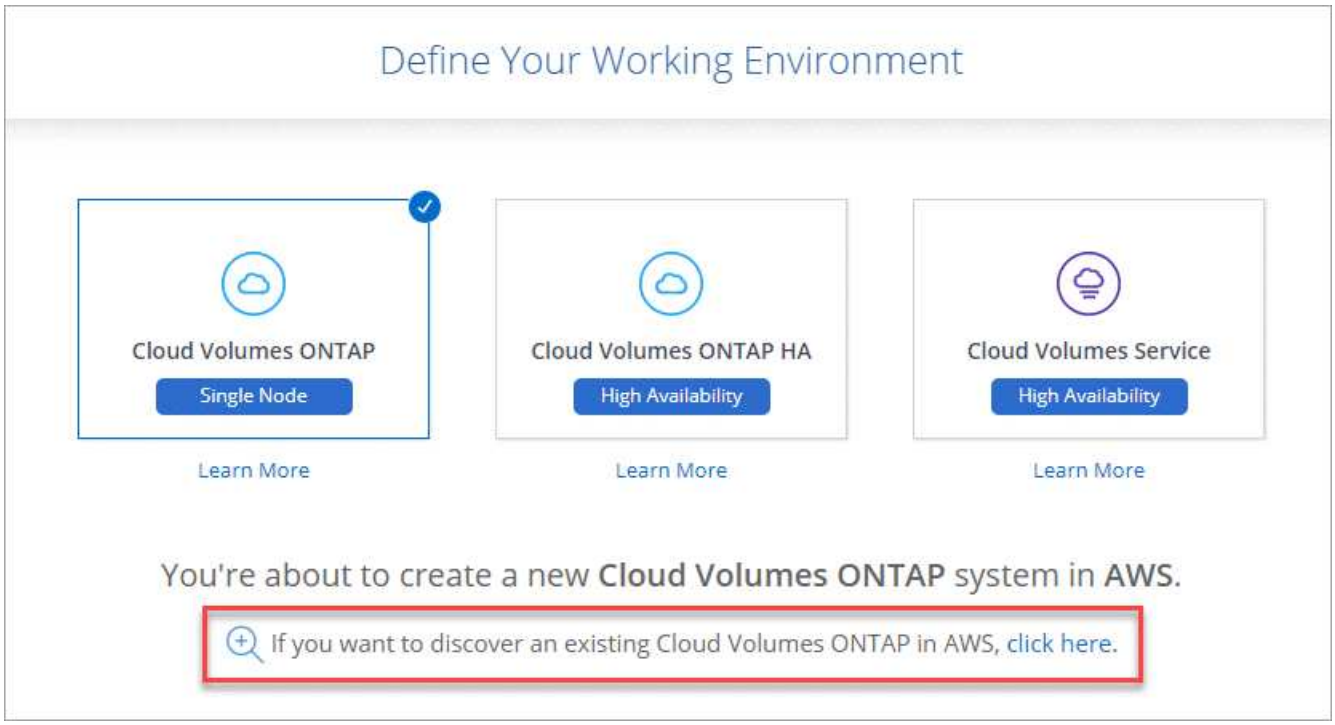
您可以探索並新增 Cloud Volumes ONTAP 現有的 NetApp 系統至 Cloud Manager 。如果您部署了新的 Cloud Manager 系統、您可以這麼做。

開始之前

您必須知道 Cloud Volumes ONTAP 該密碼才能使用此功能。

步驟

1. 在「工作環境」頁面上、按一下「新增工作環境」。
2. 選取系統所在的雲端供應商。
3. 選擇 Cloud Volumes ONTAP 哪種類型的系統。
4. 按一下連結以探索現有系統。



5. 在「區域」頁面上、選擇執行個體所在的區域、然後選取執行個體。
6. 在「認證資料」頁面上、輸入 Cloud Volumes ONTAP for the fu位 管理員使用者的密碼、然後按一下「 * 執行 * 」。

結果

Cloud Manager 會將 Cloud Volumes ONTAP 這些不全的執行個體新增至工作區。

刪除 **Cloud Volumes ONTAP** 功能不正常的環境

最好是從 Cloud Volumes ONTAP Cloud Manager 刪除不要從雲端供應商的主控台刪除。例如、如果您從 Cloud Volumes ONTAP AWS 終止授權的樣例、則無法將授權金鑰用於其他執行個體。您必須從 Cloud Manager 刪除工作環境、才能釋出授權。

關於這項工作

刪除工作環境時、 Cloud Manager 會終止執行個體、刪除磁碟和快照。

支援終止保護功能的執行個體可防止 AWS 意外終止。 Cloud Volumes ONTAP不過、如果您確實從 Cloud Volumes ONTAP AWS 終止一個實體執行個體、則必須移至 AWS CloudForation 主控台、然後刪除執行個體的堆疊。堆疊名稱是工作環境的名稱。

步驟

1. 在工作環境中、按一下功能表圖示、然後按一下 * 刪除 * 。
2. 輸入工作環境的名稱、然後按一下 * 刪除 * 。

   刪除工作環境最多可能需要 5 分鐘。