Cloud Volumes ONTAP文檔

Cloud Volumes ONTAP

NetApp
March 10, 2026

目錄

Cloud Volumes ONTAP文檔

發行說明

Cloud Volumes ONTAP的新功能

了解NetApp Console中Cloud Volumes ONTAP管理的新功能。

本頁所述的增強功能特定於透過控制台管理Cloud Volumes ONTAP 。要了解Cloud Volumes ONTAP軟體本身的新功能， "前往Cloud Volumes ONTAP發行說明" 。

2026 年 3 月 10 日

能夠管理 **Cloud Volumes ONTAP** 的 **Console** 代理程式 **Proxy** 設定

您現在可以在 NetApp Console agent 上管理 Cloud Volumes ONTAP 的代理伺服器設定，即使您失去連線或代理伺服器設定錯誤也沒問題。先前，如果 Console agent 無法在 20 分鐘內連接到 Cloud Volumes ONTAP，則會將您的手動代理伺服器設定覆蓋為預設設定。這會導致通訊失敗，包括 AutoSupport 訊息的問題。若要保留現有系統的代理伺服器設定，請執行以下 API 呼叫：

```
PUT /occm/config
```

請在請求內文中包含以下參數：

```
{
  "proxyMode": "No_Overwrites"
}
```

預設模式為標準模式，這表示如果 Console 代理程式在 20 分鐘內無法連線至 Cloud Volumes ONTAP，則會將您的 Proxy 設定覆寫為預設值。

"設定可修改的 NetApp Console 參數"

2026 年 2 月 26 日

支援私有模式部署的 **Google Infrastructure Manager**

Cloud Volumes ONTAP 9.16.1 及更高版本現在支援 "Google Cloud Infrastructure Manager"（IM），而非 "Cloud Deployment Manager"（DM），用於 Google Cloud 中的新私有模式部署。Google 將在不久的將來棄用 Deployment Manager 作為基礎架構服務，改用更進階的 Infrastructure Manager。

自 2026 年 2 月 25 日起，Cloud Volumes ONTAP 使用 Infrastructure Manager 進行新的和現有的私有模式部署。此表說明了基本工作流程：

情境	行動	代理程式的新 **API**	代理程式的新權限	適用於 **Cloud Volumes ONTAP** 的全新 **Google Cloud API**	文件資源
現有代理程式和私有模式中的現有部署	從 NetApp 支援網站下載安裝程式，將 NetApp Console 代理程式升級至最新版本，然後手動將代理程式安裝到主機上，以便其能夠使用 Infrastructure Manager API。之後，將現有的 Cloud Volumes ONTAP 系統轉換為使用 Infrastructure Manager。	• Cloud Infrastructure Manager API • 雲端配額 API • Cloud Build API	Console 版本的所有權限如下： • "2025 年 12 月 8 日" • "2026 年 2 月 09 日" • cloudbuild.workerpools.get • cloudbuild.workerpools.get	• https://cloudbuild.googleapis.com/v1 • https://www.googleapis.com/upload/storage/v1 • https://config.googleapis.com/v1	"為 Google Cloud Infrastructure Manager 設定現有的 Cloud Volumes ONTAP 部署"
新代理程式和新部署	建立一個新代理，並在私有模式下部署一個新的 Cloud Volumes ONTAP 系統。				• "從 Google Cloud 建立 Console 代理" • "私有模式部署快速入門"

在私有模式部署中，您需要進行一些組態變更，Cloud Volumes ONTAP 才能開始使用 Infrastructure Manager。請參閱 "私有模式部署的 Infrastructure Manager 組態"。

相關連結

- "NetApp Console Agent 4.2.0 發行說明"
- "Google Cloud Infrastructure Manager 所需的權限"

2026 年 2 月 19 日

Azure 支援的新區域

現在您可以在下列區域的 Azure 中的單一和多個可用區域中部署Cloud Volumes ONTAP 9.12.1 GA 及更高版本。這包括對單節點和高可用性 (HA) 部署的支援。

- 日本西部 (japanwest)
- 印尼中部 (indonesiacentral)

有關所有地區的列表，請參閱 "Azure 下的全球區域地圖"。

2026 年 2 月 17 日

Cloud Volumes ONTAP 支援下一代 **Google Cloud VM**

在 9.18.1 版本中，NetApp 將新的 Cloud Volumes ONTAP 部署從 N2 虛擬機遷移到新一代 Google Cloud C3 系列虛擬機，帶來更快、更具可擴展性的體驗。現在，您可以在 Google Cloud 中部署 Cloud Volumes ONTAP 9.18.1 及更高版本時充分利用 C3 系列虛擬機器的優勢。C3 系列虛擬機器採用 Google Virtual NIC（gVNIC）和 Hyperdisk Balanced 磁碟，可確保為高強度工作負載提供動態效能，從而提供更高的效能和更大的容量限制。

目前，Cloud Volumes ONTAP 僅支援單節點部署中的 C3 系列。

如果您的 Cloud Volumes ONTAP 系統執行 9.18.1 或更新版本，用於輕鬆進行單節點部署的預先設定套件會自動使用 C3 VM，同時讓您能夠根據工作負載需求自訂 IOPS 和處理量參數。同樣地，在建立 Aggregate 時，您可以新增 Hyperdisk Balanced 磁碟，以在 Google Cloud 中實現更好的效能和擴充性。此外，您可以選擇 C3 系列機器的 LSSD 變體，以獲得預設的 Flash Cache 支援。

在向 Aggregate 中新增 Volume 時，無法變更 C3 VM 的磁碟類型，因為 C3 僅支援 Hyperdisk Balanced 磁碟。同樣，將 N2 VM 類型的系統複製到 C3 VM 時，磁碟類型預設為 Hyperdisk Balanced。

"Google Cloud 中 Cloud Volumes ONTAP 支援的組態"

"Google 文件：C3 機器系列"

Azure 中 **Cloud Volumes ONTAP** 的 **VNet** 安全性

Cloud Volumes ONTAP 9.18.1 及更高版本在 Azure 單可用區和多可用區中的部署支援 Azure 虛擬網路（VNet）加密，作為其分層安全性策略的一部分，用於保護傳輸中的資料。Cloud Volumes ONTAP 利用 Azure 原生資料封包傳輸層安全性（DTLS）協定來保護 ONTAP 節點、管理介面和其他 Azure 服務之間的通訊，防止攔截和未經授權的存取。這種網路級加密與 ONTAP 內建的儲存和靜態資料保護機制相輔相成，為您的資料提供端對端的安全保障。

"Azure VNet 加密的網路"

2026 年 2 月 12 日

Azure 中對 **Ebdsv5** 和 **E104ids_v5 VM** 的支援

從 Cloud Volumes ONTAP 9.18.1 開始，您可以部署 Ebdsv5 和 E104ids_v5 VM，用於單節點和高可用性（HA）部署和升級。

Azure 虛擬機器 Eb 系列中的 Ebdsv5 VM 針對更高的遠端儲存效能進行了最佳化。您可以將這些 VM 用於記憶體密集型和 I/O 密集型的企業級工作負載，例如關聯式資料庫、記憶體內分析和其他要求嚴格的關鍵業務應用程式。

E104ids_v5 是一個獨立的 VM 執行個體，可協助您更妥善地處理排程的維護時段。與 E80ids_v4 相比，它提供更高的磁碟輸送量和 IOPS，以及更佳的整體網路效能。

"Azure 中Cloud Volumes ONTAP支援的配置"

"Azure 文件：Edsv5 大小系列"

2026 年 2 月 10 日

Cloud Volumes ONTAP 9.18.1 GA

現在您可以使用 NetApp Console 在 AWS、Azure 和 Google Cloud 中部署和管理 Cloud Volumes ONTAP 9.18.1 的正式版（GA）。

"了解有關此版本Cloud Volumes ONTAP的更多信息"。

2026 年 2 月 9 日

支援 Google Cloud Infrastructure Manager

Cloud Volumes ONTAP 9.16.1 及更高版本現在支援使用 "Google Cloud Infrastructure Manager"（IM）而非 "Cloud Deployment Manager"（DM）來部署 Google Cloud 中的新部署。Google 將在不久的將來棄用 Deployment Manager 作為基礎架構服務，轉而使用更進階的基礎架構管理器。

自 2026 年 2 月 9 日起，Cloud Volumes ONTAP 使用 Infrastructure Manager 進行新的和現有的部署。此表為您說明了一些工作流程：

情境	行動	代理程式的新 **API**	代理程式的新權限	適用於 **Cloud Volumes ONTAP** 的全新 **Google Cloud API**	文件資源
現有代理程式和現有 Cloud Volumes ONTAP 部署	為現有代理程式新增新的 API 和權限，並轉換現有的 Cloud Volumes ONTAP 系統。	• Cloud Infrastructure Manager API • 雲端配額 API	Console 版本的所有權限如下： • "2025 年 12 月 8 日" • "2026 年 2 月 09 日"	https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1	"為 Google Cloud Infrastructure Manager 設定現有的 Cloud Volumes ONTAP 部署"

情境	行動	代理程式的新 **API**	代理程式的新權限	適用於 **Cloud Volumes ONTAP** 的全新 **Google Cloud API**	文件資源
現有代理程式和新的 Cloud Volumes ONTAP 部署	為現有代理程式新增新的 API 和權限，並部署新的 Cloud Volumes ONTAP 系統。	• Cloud Infrastructure Manager API • 雲端配額 API	Console 版本的所有權限如下： • "2025 年 12 月 8 日" • "2026 年 2 月 09 日"	新部署的所有步驟	"開始在 Google Cloud 中使用 Cloud Volumes ONTAP"
新代理程式和新部署	建立新代理並部署新的 Cloud Volumes ONTAP 系統。				• "從 Google Cloud 建立 Console 代理" • "開始在 Google Cloud 中使用 Cloud Volumes ONTAP"

現在，您可以部署 Cloud Volumes ONTAP 以自動使用 Infrastructure Manager，或執行轉換工具將 Deployment Manager 中的現有部署切換到 Infrastructure Manager。轉換過程只需一次，之後您的系統將開始使用 Infrastructure Manager。有關執行轉換工具的說明，請參閱 "為 Google Cloud Infrastructure Manager 設定現有的 Cloud Volumes ONTAP 部署"。

使用 Infrastructure Manager 的 Cloud Volumes ONTAP 系統會使用 Google Cloud Storage 儲存桶來儲存資料和記錄，這些儲存桶位於首次部署的區域中，用於儲存部署記錄，這些記錄可供後續部署重複使用。這些儲存桶可能會產生額外費用，但請勿編輯或刪除儲存桶及其內容：

- `gs://netapp-cvo-infrastructure-manager-<project id>`：用於新的 Cloud Volumes ONTAP

部署的 ONTAP 版本和 SVM Terraform 範本。在此內， `dm-to-im-convert` 儲存桶包含 Cloud Volumes ONTAP Terraform 檔案。

- `<gcp project number>-<region>-blueprint-config`：用於儲存 Google Cloud Terraform 工件。

相關連結

- "開始在 Google Cloud 中使用 Cloud Volumes ONTAP"
- "NetApp Console Agent 4.2.0 發行說明"
- "Google Cloud Infrastructure Manager 所需的權限"

2026年1月12日

Cloud Volumes ONTAP的首選計費方式

現在您可以選擇首選的計費方式來計算您的Cloud Volumes ONTAP使用量和超額費用。自 2025 年 6 月 25 日起，自帶許可證 (BYOL) 授權模式將不再提供， NetApp已在NetApp Console的「授權和訂閱」部分中添加了首選的計費方式。您可以選擇使用年度市場訂閱進行計費和超額費用結算，或選擇現有的 BYOL 模式作為首選方案。這樣，您可以靈活選擇最適合您組織財務策略和使用模式的充電方式。

"計費偏好和超額費用"。

2025年12月10日

提升 **Azure** 中 **Premium SSD v2** 磁碟效能的能力

現在，您可以透過修改 IOPS 和吞吐量參數來提高 Azure 中 Premium SSD v2 託管磁碟的效能。利用此功能，您可以根據工作負載需求最佳化系統的儲存效能。

"在 Azure 中管理Cloud Volumes ONTAP的 Premium SSD v2 磁碟效能"。

Essentials 授權超額收費簡化

對於Cloud Volumes ONTAP市場年度合約/私有報價，Essentials 授權的超額使用運算現在與自帶授權 (BYOL) 套餐保持一致。此前，超出部分按基本套餐的每小時市場價格計費。現在，如果您的市場年度合約包含多個 Essentials 套餐， NetApp Console會將 Essentials 套餐的超額費用計入您訂閱中價格較高的 Essentials 套餐的可用容量。這簡化了 Essentials 套餐的超額費用計算，並確保從 BYOL 授權模式平穩過渡到訂閱模式。

"Essentials許可證超額費用如何收取"

支援 **Azure Edsv6** 尺寸系列

從Cloud Volumes ONTAP 9.17.1 開始，您可以透過NetApp Console為新的Cloud Volumes ONTAP執行個體部署 Azure Edsv6 系列虛擬機器。 Cloud Volumes ONTAP 9.17.1 及更高版本將僅支援新部署的第二代虛擬機器。這些第二代機器與最新技術相容，例如統一可擴充韌體介面 (UEFI)、Azure Boost 系統和 NVMe。它們非常適合記憶體密集系統和需要快速本地儲存的應用，例如資料庫伺服器和分析引擎。

"Azure 中Cloud Volumes ONTAP支援的配置"

2025年11月10日

增強的 **NVMe-TCP** 支持

先前，在 NVMe-TCP 上部署Cloud Volumes ONTAP實例時，您必須在部署之前手動取得和套用 NVMe 授權。透過此更新， Cloud Volumes ONTAP現在會在部署期間自動安裝所需的 NVMe 許可證，從而簡化設定流程。

對於缺少許可證的現有 NVMe-TCP 部署， Cloud Volumes ONTAP會自動套用授權。您必須重新啟動系統才能使許可證生效。

更多資訊請參見 "Cloud Volumes ONTAP支援的客戶端協定：NVMe-TCP"。

2025年10月17日

Azure 中的**Cloud Volumes ONTAP**現已僅限於最新支援版本

現在，透過NetApp Console在 Azure 中部署和升級Cloud Volumes ONTAP僅限於最新支援的版本。這確保了與 Microsoft 支援的最新一代硬體的兼容性，並提供最新的功能和安全性增強功能。控制台將提示您升級到支援的版本。

更多詳細信息，請參閱：

- 部署： "Cloud Volumes ONTAP部署支援的ONTAP版本"
- 升級： "Azure 支援的升級路徑"

2025年10月6日

BlueXP現在是**NetApp Console**

NetApp Console建立在增強和重組的BlueXP基礎之上，可在企業級內部和雲端環境中集中管理NetApp儲存和NetApp Data Services，提供即時洞察、更快的工作流程和簡化的管理，並且高度安全且合規。

有關更改的詳細信息，請參閱 "NetApp Console發行說明"。

簡化 **AWS** 中的**Cloud Volumes ONTAP**部署

現在，您可以使用快速部署方法在 AWS 中部署Cloud Volumes ONTAP，適用於單一節點和高可用性 (HA) 設定。與進階方法相比，此簡化流程減少了步驟數，在單一頁面上自動設定預設值，並最大限度地減少了導航，使部署更快、更容易。

有關更多信息，請參閱 "使用快速部署在 AWS 中部署Cloud Volumes ONTAP" 。

2025年9月4日

Cloud Volumes ONTAP 9.17.1 RC

現在您可以使用BlueXP在 Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.17.1 的候選版本 1。但此版本尚不支援在AWS中部署和升級。

"了解有關此版本Cloud Volumes ONTAP的更多信息"。

2025年8月11日

優化許可證的可用性終止

從 2025 年 8 月 11 日開始， Cloud Volumes ONTAP Optimized 授權將被棄用，並且將不再可在 Azure 和 Google Cloud 市場中以即用即付 (PAYGO) 訂閱的方式購買或續訂。如果您擁有現有的包含優化許可證的年度合同，則可以繼續使用該許可證，直到合約結束。當您的優化授權到期時，您可以選擇BlueXP中的Cloud Volumes ONTAP Essentials 或 Professional 授權。

但是，可以透過 API 新增或更新優化許可證。

有關許可包的信息，請參閱 "Cloud Volumes ONTAP許可"。

有關切換到不同充電方式的信息，請參閱 "管理基於容量的許可"。

2025年7月14日

支援透明代理

除了現有的明確代理連線之外， BlueXP現在還支援透明代理伺服器。建立或修改BlueXP連接器時，您可以設定透明代理伺服器來安全地管理往返Cloud Volumes ONTAP 的網路流量。

有關在Cloud Volumes ONTAP中使用代理伺服器的更多信息，請參閱：

- "用於支援 AWS 中的連接器代理程式的網路配置"
- "用於支援 Azure 中的連接器代理程式的網路配置"
- "用於支援 Google Cloud 中的連接器代理程式的網路配置"

Azure 中的**Cloud Volumes ONTAP**支援新的 **VM** 類型

從Cloud Volumes ONTAP 9.13.1 開始，L8s_v3 作為 Azure 單一和多個可用區域中的 VM 類型受到支持，適用於新的和現有的高可用性 (HA) 對部署。

有關詳細信息，請參閱https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html["Azure 中支援的配置"^] 。

2025年6月25日

Cloud Volumes ONTAP的 **BYOL** 授權可用性受限

自 2025 年 6 月 25 日起， NetApp已限制Cloud Volumes ONTAP的自帶授權 (BYOL) 授權模式。此限制適用於 AWS、Azure 和 Google Cloud 中的所有客戶和Cloud Volumes ONTAP部署。唯一的例外是美國公共部門客戶和中國區域部署。

NetApp支援和服務將持續到您的 BYOL 合約到期，但已過期的授權將無法續約或延長。 BYOL許可證到期後，您必須將其替換為透過雲端市場訂閱購買的基於容量的授權。透過超大規模市場購買的基於容量的授權模式可以簡化授權體驗並帶來更大的業務優勢。請聯絡您的NetApp客戶團隊或客戶成功代表，討論您的轉換方案。

欲了解更多信息，請參閱此客戶公報： "CPC-00661： Cloud Volumes ONTAP BYOL 政策變更" 。

2025年5月29日

為Cloud Volumes ONTAP 9.15.1 啟用私有模式部署

現在您可以在 AWS、Azure 和 Google Cloud 中以私有模式部署Cloud Volumes ONTAP 9.15.1。 Cloud Volumes ONTAP 9.15.1 的單節點和高可用性 (HA) 部署均啟用私有模式。

有關私有模式部署的更多信息，請參閱https://docs.netapp.com/us-en/bluexp-setup-admin/concept-modes.html#restricted-mode["了解BlueXP部署模式"^]。

2025年5月12日

在BlueXP中發現透過 Azure 市場進行的部署

BlueXP現在能夠發現透過 Azure 市場直接部署的Cloud Volumes ONTAP系統。這意味著您現在可以在BlueXP中將這些系統新增和管理為工作環境，就像其他Cloud Volumes ONTAP系統一樣。

"從 Azure 市場部署Cloud Volumes ONTAP"

2025年4月16日

Azure 支援的新區域

現在您可以在下列區域的 Azure 中的單一和多個可用區域中部署Cloud Volumes ONTAP 9.12.1 GA 及更高版本。這包括對單節點和高可用性 (HA) 部署的支援。

- 西班牙中部
- 墨西哥中央

有關所有地區的列表，請參閱 "Azure 下的全球區域地圖"。

2025年4月14日

透過 Google Cloud 中的 API 自動建立儲存虛擬機

現在您可以使用BlueXP API 在 Google Cloud 中自動建立儲存虛擬機器。您一直在Cloud Volumes ONTAP高可用性 (HA) 配置中使用此功能，現在您也可以在單節點部署中使用它。透過使用BlueXP API，您可以在 Google Cloud 環境中輕鬆建立、重新命名和刪除其他資料服務儲存虛擬機，而無需手動配置所需的網路介面、LIF 和管理 LIF。這種自動化簡化了管理儲存虛擬機器的過程。

"在 Google Cloud 中管理Cloud Volumes ONTAP的資料服務儲存虛擬機"

2025年4月3日

AWS 中Cloud Volumes ONTAP 9.13.1 對中國區域的支持

現在您可以在中國區域的 AWS 中部署Cloud Volumes ONTAP 9.13.1。這包括對單節點和高可用性 (HA) 部署的支援。僅支援直接從NetApp購買的授權。

有關區域可用性，請參閱 "Cloud Volumes ONTAP的全球區域地圖"。

2025年3月28日

為Cloud Volumes ONTAP 9.14.1 啟用私有模式部署

現在您可以在 AWS、Azure 和 Google Cloud 中以私有模式部署Cloud Volumes ONTAP 9.14.1。 Cloud Volumes ONTAP 9.14.1 的單節點和高可用性 (HA) 部署均啟用私有模式。

有關私有模式部署的更多信息，請參閱https://docs.netapp.com/us-en/bluexp-setup-admin/concept-modes.html#restricted-mode["了解BlueXP部署模式"^]。

2025年3月12日

Azure 中支援多可用區域部署的新區域

以下區域現在支援 Azure 中適用於Cloud Volumes ONTAP 9.12.1 GA 及更高版本的 HA 多可用區域部署：

- 美國中部
- US Gov Virginia（美國政府地區 - 維吉尼亞州）

有關所有地區的列表，請參閱 "Azure 下的全球區域地圖"。

2025年3月10日

透過 Azure 中的 API 自動建立儲存虛擬機

現在您可以使用BlueXP API 為 Azure 中的Cloud Volumes ONTAP建立、重新命名和刪除其他資料服務儲存虛擬機器。如果您需要使用儲存虛擬機器進行管理，則使用 API 可以自動執行儲存虛擬機器的建立過程，包括所需網路介面、LIF 和管理 LIF 的配置。

"在 Azure 中管理Cloud Volumes ONTAP的資料服務儲存虛擬機"

2025年3月6日

Cloud Volumes ONTAP 9.16.1 正式版

現在您可以使用BlueXP在 Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.16.1 通用可用性版本。但此版本尚不支援在AWS中部署和升級。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

2025年3月3日

Azure 對紐西蘭北部地區的支持

Azure 現已支援紐西蘭北部地區的Cloud Volumes ONTAP 9.12.1 GA 及更高版本的單節點和高可用性 (HA) 配置。請注意，此區域不支援 Lsv3 實例類型。

有關所有受支援區域的列表，請參閱 "Azure 下的全球區域地圖"。

2025年2月18日

介紹 **Azure** 市場直接部署

現在您可以利用 Azure 市場直接部署功能，直接從 Azure 市場輕鬆快速地部署Cloud Volumes ONTAP 。使用這種簡化的方法，您可以在您的環境中探索Cloud Volumes ONTAP的核心功能和功能，而無需設定BlueXP Connector 或滿足透過BlueXP部署Cloud Volumes ONTAP所需的其他入職標準。

- "了解 Azure 中的Cloud Volumes ONTAP部署選項"
- "從 Azure 市場部署Cloud Volumes ONTAP"

2025年2月10日

已啟用使用者身份驗證，可從**BlueXP**存取系統管理員

身為BlueXP管理員，您現在可以為從BlueXP存取ONTAP系統管理員的ONTAP使用者啟動身分驗證。您可以透過編輯BlueXP連接器設定來啟用此選項。此選項適用於標準模式和私人模式。

"使用系統管理員管理Cloud Volumes ONTAP" 。

BlueXP Advanced View 重新命名為 **System Manager**

透過ONTAP系統管理員從BlueXP對Cloud Volumes ONTAP進行進階管理的選項已從 **Advanced View** 重新命名為 **System Manager**。

"使用系統管理員管理Cloud Volumes ONTAP" 。

引入使用**BlueXP digital wallet**管理許可證的更簡單方法

現在，您可以透過使用BlueXP digital wallet中改進的導航點來體驗簡化的Cloud Volumes ONTAP授權管理：

- 透過*管理>Licenses and subscriptions>概述/直接許可證*選項卡輕鬆存取您的Cloud Volumes ONTAP許可證資訊。
- 按一下「概覽」標籤中 Cloud Volume ONTAP面板上的「檢視」以全面了解基於容量的授權。此高級視圖提供有關您的許可證和訂閱的詳細資訊。
- 如果您喜歡先前的介面，您可以按一下「切換到舊視圖」按鈕按類型查看許可證詳細資訊並修改許可證的收費方式。

"管理基於容量的許可證" 。

2024年12月9日

已更新 **Azure** 支援的虛擬機器列表，以符合最佳實踐

在 Azure 中部署Cloud Volumes ONTAP的新執行個體時， BlueXP上不再可選擇 DS_v2 和 Es_v3 機器系列。這些系列將僅在較舊的現有系統中保留和支援。從 9.12.1 版本開始，Azure 僅支援Cloud Volumes ONTAP的新部署。我們建議您切換到 Es_v4 或任何其他與Cloud Volumes ONTAP 9.12.1 及更高版本相容的系列。但是，DS_v2 和 Es_v3 系列機器將可用於透過 API 進行的新部署。

"Azure 中支援的配置"

2024年11月11日

基於節點的許可證的可用性終止

NetApp已計劃終止提供 (EOA) 和終止支援 (EOS) Cloud Volumes ONTAP基於節點的授權。從 2024 年 11 月 11 日起，基於節點的許可證的有限可用性已終止。基於節點的授權支援將於 2024 年 12 月 31 日結束。在基於節點的許可證 EOA 之後，您應該使用BlueXP許可證轉換工具過渡到基於容量的許可證。

對於年度或長期承諾， NetApp建議您在 EOA 日期或授權到期日之前聯絡您的NetApp代表，以確保過渡的先決條件到位。如果您沒有Cloud Volumes ONTAP節點的長期合同，並且根據按需付費 (PAYGO) 訂閱運行您的系統，那麼在 EOS 日期之前規劃您的轉換非常重要。對於長期合約和 PAYGO 訂閱，您都可以使用BlueXP授權轉換工具進行無縫轉換。

"基於節點的許可證的可用性終止" "將Cloud Volumes ONTAP基於節點的許可證轉換為基於容量的許可證"

從**BlueXP**中刪除基於節點的部署

使用基於節點的許可證部署Cloud Volumes ONTAP系統的選項在BlueXP上已棄用。除少數特殊情況外，您不能對任何雲端提供者的Cloud Volumes ONTAP部署使用基於節點的授權。

NetApp認識到符合合約義務和營運需求的以下獨特授權要求，並將在這些情況下繼續支援基於節點的授權：

- 美國公共部門客戶
- 私有模式下的部署
- AWS 中國區Cloud Volumes ONTAP部署
- 如果您擁有有效、未過期的按節點自帶授權（BYOL 授權）

"基於節點的許可證的可用性終止"

在 **Azure Blob** 儲存體上為**Cloud Volumes ONTAP**資料新增冷層

BlueXP現在可讓您選擇冷層來儲存 Azure Blob 儲存體上的非活動容量層資料。在現有的熱層和冷層中添加冷層可為您提供更實惠的儲存選項並提高成本效率。

"Azure 中的資料分層"

限制 **Azure** 儲存帳戶公共存取的選項

現在您可以選擇限制對 Azure 中Cloud Volumes ONTAP系統的儲存帳戶的公共存取。透過停用訪問，您可以保護您的私人 IP 位址不被洩露，即使在同一個 VNet 內，也需要遵守您組織的安全策略。此選項也會停用Cloud Volumes ONTAP系統的資料分層，並且適用於單節點和高可用性對。

"安全群組規則" 。

部署**Cloud Volumes ONTAP**後啟用 **WORM**

現在，您可以使用BlueXP在現有的Cloud Volumes ONTAP系統上啟動一次寫入、多次讀取 (WORM) 儲存。此功能為您提供了在工作環境中啟用 WORM 的靈活性，即使在建立期間未啟用 WORM。一旦啟用，您就無法停用 WORM。

"在Cloud Volumes ONTAP工作環境中啟用 WORM"

2024年10月25日

已更新 **Google Cloud** 支援的虛擬機器列表，以符合最佳實踐

在 Google Cloud 中部署Cloud Volumes ONTAP的新執行個體時， BlueXP上不再可選擇 n1 系列機器。n1 系列機器將保留，並且僅在較舊的現有系統中支援。從 9.8 版本開始，Google Cloud 才支援Cloud Volumes ONTAP的新部署。我們建議您切換到與Cloud Volumes ONTAP 9.8 及更高版本相容的 n2 系列機器類型。然而，n1 系列機器將可用於透過 API 執行的新部署。

"Google Cloud 中支援的配置" 。

私有模式下對 **Amazon Web Services** 的本機區域支持

BlueXP現在支援私有模式下的Cloud Volumes ONTAP高可用性 (HA) 部署的 AWS 本地區域。先前僅限於標準模式的支援現已擴展到包括私人模式。

在受限模式下使用BlueXP時不支援 AWS 本地區域。

有關具有 HA 部署的 AWS 本地區域的更多信息，請參閱"AWS 本地區域"。

2024年10月7日

增強用戶升級版本選擇的體驗

從此版本開始，當您嘗試使用BlueXP通知升級Cloud Volumes ONTAP，您將收到有關使用預設、最新和相容版本的指導。此外，現在您可以選擇與您的Cloud Volumes ONTAP實例相容的最新補丁或主要版本，或手動輸入要升級的版本。

"升級Cloud Volumes ONTAP軟體"

2024年9月9日

WORM 和 **ARP** 功能不再收費

WORM（一次寫入多次讀取）和 ARP（自主勒索軟體保護）的內建資料保護和安全功能將透過Cloud Volumes ONTAP許可證免費提供。新的定價模式適用於 AWS、Azure 和 Google Cloud 的新舊 BYOL 和 PAYGO/市場訂閱。基於容量和基於節點的許可證都將包含所有配置的 ARP 和 WORM，包括單節點和高可用性 (HA) 對，無需額外費用。

簡化的定價為您帶來以下好處：

- 目前包含 WORM 和 ARP 的帳戶將不再對這些功能收取費用。今後，您的帳單將只收取容量使用費，就像此次變更之前一樣。 WORM 和 ARP 將不再包含在您未來的帳單中。
- 如果您目前的帳戶不包含這些功能，現在可以免費選擇 WORM 和 ARP。
- 所有針對新帳戶的Cloud Volumes ONTAP產品均不收取 WORM 和 ARP 費用。

了解有關這些功能的更多資訊：

- "為Cloud Volumes ONTAP啟用NetApp勒索軟體防護解決方案"

- "WORM儲存"

2024年8月23日

AWS 現已支援加拿大西部地區

AWS 現已支援加拿大西部地區的Cloud Volumes ONTAP 9.12.1 GA 及更高版本。

有關所有地區的列表，請參閱 "AWS 下的全球區域地圖"。

2024年8月22日

Cloud Volumes ONTAP 9.15.1 正式版

BlueXP現在可以在 AWS、Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.15.1 通用可用性版本。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

2024年8月8日

Edge Cache 授權包已棄用

Edge Cache 基於容量的授權包將不再適用於Cloud Volumes ONTAP的未來部署。但是，您可以使用 API 來實作此功能。

Azure 中快閃記憶體快取的最低版本支持

在 Azure 中設定 Flash Cache 所需的最低Cloud Volumes ONTAP版本是 9.13.1 GA。您只能使用ONTAP 9.13.1 GA 及更高版本在 Azure 中的Cloud Volumes ONTAP系統上部署 Flash Cache。

有關支援的配置，請參閱 "Azure 中支援的配置"。

市場訂閱的免費試用已棄用

雲端供應商市場中按使用量付費訂閱的 30 天自動免費試用或評估授權將不再在Cloud Volumes ONTAP中提供。任何類型的市場訂閱（PAYGO 或年度合約）的收費將從首次使用時激活，沒有任何免費試用期。

2024年6月10日

Cloud Volumes ONTAP 9.15.0

BlueXP現在可以在 AWS、Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.15.0。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

2024年5月17日

Amazon Web Services 本地區域支持

Cloud Volumes ONTAP HA 部署現已支援 AWS 本地區域。 AWS 本地區域是一種基礎設施部署，其中儲存、運算、資料庫和其他精選 AWS 服務位於大城市和工業區附近。

> 在標準模式下使用BlueXP時支援 AWS 本地區域。目前，在受限模式或私有模式下使用BlueXP時不支援 AWS 本地區域。

有關具有 HA 部署的 AWS 本地區域的更多信息，請參閱 "AWS 本地區域"。

2024年4月23日

Azure 中支援多可用區域部署的新區域

以下區域現在支援 Azure 中適用於Cloud Volumes ONTAP 9.12.1 GA 及更高版本的 HA 多可用區域部署：

- 德國中西部
- 波蘭中部
- 美國西部 3
- 以色列中心
- 義大利北部
- 加拿大中部

有關所有地區的列表，請參閱 "Azure 下的全球區域地圖"。

Google Cloud 現已支援約翰尼斯堡地區

約翰尼斯堡地區(`africa-south1`Google Cloud 的Cloud Volumes ONTAP 9.12.1 GA 及更高版本現已支援區域。

有關所有地區的列表，請參閱 "Google Cloud 下的全球區域地圖"。

不再支援磁碟區模板和標籤

您無法再從範本建立磁碟區或編輯磁碟區的標籤。這些操作與BlueXP修復服務相關，但該服務已不再可用。

2024年3月8日

Amazon Instant Metadata Service v2 支持

在 AWS 中， Cloud Volumes ONTAP、Mediator 和 Connector 現在支援 Amazon Instant Metadata Service v2 (IMDSv2) 的所有功能。 IMDSv2 提供了增強的針對漏洞的保護。之前僅支援 IMDSv1。

如果您的安全性原則需要，您可以將 EC2 執行個體設定為使用 IMDSv2。有關說明，請參閱 "用於管理現有連接器的BlueXP設定和管理文檔"。

2024年3月5日

Cloud Volumes ONTAP 9.14.1 正式版

BlueXP現在可以在 AWS、Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.14.1 通用可用性版本。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

2024年2月2日

Azure 中對 **Edv5** 系列 **VM** 的支持

從 9.14.1 版本開始， Cloud Volumes ONTAP現在支援以下 Edv5 系列虛擬機器。

- E4ds_v5
- E8ds_v5
- E20s_v5
- E32ds_v5
- E48ds_v5
- E64ds_v5

"Azure 中支援的配置"

2024年1月16日

BlueXP中的補丁版本

BlueXP中僅提供針對Cloud Volumes ONTAP最新三個版本的補丁版本。

"升級Cloud Volumes ONTAP"

2024年1月8日

適用於 **Azure** 多可用區域的新 **VM**

從Cloud Volumes ONTAP 9.13.1 開始，以下 VM 類型支援 Azure 多個可用區域，用於新的和現有的高可用性對部署：

- L16s_v3
- L32s_v3
- L48s_v3
- L64s_v3

"Azure 中支援的配置"

2023年12月6日

Cloud Volumes ONTAP 9.14.1 RC1

BlueXP現在可以在 AWS、Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.14.1。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

FlexVol volume最大限制為 300 TiB

現在，您可以使用 System Manager 和ONTAP CLI（從Cloud Volumes ONTAP 9.12.1 P2 和 9.13.0 P2 開始）以及在BlueXP （從Cloud Volumes ONTAP 9.13.1 開始）中建立最大大小為 300 TiB 的FlexVol volume。

- "AWS 中的儲存限制"
- "Azure 中的儲存限制"
- "Google Cloud 中的儲存限制"

2023年12月5日

引入了以下變化。

Azure 中的新區域支持

單一可用區域區域支持

以下區域現在支援 Azure 中適用於Cloud Volumes ONTAP 9.12.1 GA 及更高版本的高可用性單可用區部署：

- 特拉維夫
- 米蘭

多可用區域支持

以下區域現在支援 Azure 中適用於Cloud Volumes ONTAP 9.12.1 GA 及更高版本的高可用性多可用區部署：

- 印度中部
- 挪威東部
- 瑞士北部
- 南非北部
- 阿拉伯聯合大公國北部

有關所有地區的列表，請參閱 "Azure 下的全球區域地圖"。

2023年11月10日

連接器 3.9.35 版本引入了以下更改。

Google Cloud 現已支援柏林地區

Google Cloud for Cloud Volumes ONTAP 9.12.1 GA 及更高版本現已支援柏林地區。

有關所有地區的列表，請參閱 "Google Cloud 下的全球區域地圖"。

2023年11月8日

連接器 3.9.35 版本引入了以下更改。

AWS 現已支援特拉維夫地區

AWS 現已支援特拉維夫地區的Cloud Volumes ONTAP 9.12.1 GA 及更高版本。

有關所有地區的列表，請參閱 "AWS 下的全球區域地圖"。

2023年11月1日

連接器 3.9.34 版本引入了以下更改。

Google Cloud 現已支援沙烏地阿拉伯地區

Google Cloud for Cloud Volumes ONTAP和 Connector for Cloud Volumes ONTAP 9.12.1 GA 及更高版本現已支援沙烏地阿拉伯地區。

有關所有地區的列表，請參閱 "Google Cloud 下的全球區域地圖"。

2023年10月23日

連接器 3.9.34 版本引入了以下更改。

Azure 中支援 **HA** 多可用區部署的新區域

Azure 中的下列區域現在支援Cloud Volumes ONTAP 9.12.1 GA 及更高版本的高可用性多可用區部署：

- 澳洲東部
- 東亞
- 法國中部
- 北歐
- 卡達中央
- 瑞典中央
- 西歐
- 美國西部 2

有關支援多個可用區的所有區域的列表，請參閱 "Azure 下的全球區域地圖"。

2023年10月6日

連接器 3.9.34 版本引入了以下更改。

Cloud Volumes ONTAP 9.14.0

BlueXP現在可以在 AWS、Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.14.0 通用可用性版

本。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

2023年9月10日

連接器 3.9.33 版本引入了以下更改。

Azure 中對 Lsv3 系列 VM 的支持

從 9.13.1 版本開始，Azure 中的Cloud Volumes ONTAP現在支援 L48s_v3 和 L64s_v3 實例類型，用於在單一和多個可用區域中具有共用託管磁碟的單節點和高可用性對部署。這些實例類型支援 Flash Cache。

"查看 Azure 中Cloud Volumes ONTAP支援的配置" "查看 Azure 中Cloud Volumes ONTAP的儲存限制"

2023年7月30日

連接器 3.9.32 版本引入了以下更改。

Google Cloud 中的 Flash Cache 和高寫入速度支持

可在 Google Cloud for Cloud Volumes ONTAP 9.13.1 及更高版本中單獨啟用快閃記憶體和高寫入速度。所有受支援的實例類型均具有高寫入速度。以下實例類型支援 Flash Cache：

- n2-標準-16
- n2-標準-32
- n2-標準-48
- n2-標準-64

您可以在單節點和高可用性對部署中單獨或一起使用這些功能。

"在 Google Cloud 啟動Cloud Volumes ONTAP"

使用情況報告增強功能

現在可以對使用報告中顯示的資訊進行各種改進。以下是使用情況報告的增強功能：

- TiB 單位現在包含在列名中。
- 現在包含一個用於序號的新「節點」欄位。
- 儲存虛擬機器使用情況報告下現在包含一個新的「工作負載類型」欄位。
- 工作環境名稱現在包含在儲存虛擬機器和磁碟區使用報告中。
- 卷類型“文件”現在標記為“主（讀/寫）”。
- 卷類型“輔助”現在標記為“輔助 (DP)”。

有關使用情況報告的更多信息，請參閱 "下載使用情況報告"。

2023年7月26日

連接器 3.9.31 版本引入了以下更改。

Cloud Volumes ONTAP 9.13.1 正式版

BlueXP現在可以在 AWS、Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.13.1 通用可用性版本。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

2023年7月2日

連接器 3.9.31 版本引入了以下更改。

支援 Azure 中的 HA 多可用區域部署

Azure 中的日本東部和韓國中部現在支援Cloud Volumes ONTAP 9.12.1 GA 及更高版本的 HA 多可用區域部署。

有關支援多個可用區的所有區域的列表，請參閱 "Azure 下的全球區域地圖"。

自主勒索軟體防護支持

Cloud Volumes ONTAP現已支援自主勒索軟體防護 (ARP)。 Cloud Volumes ONTAP版本 9.12.1 及更高版本提供 ARP 支援。

要了解有關 ARP 與Cloud Volumes ONTAP 的更多信息，請參閱 "自主勒索軟體防護"。

2023年6月26日

連接器 3.9.30 版本引入了以下更改。

Cloud Volumes ONTAP 9.13.1 RC1

BlueXP現在可以在 AWS、Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.13.1。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

2023年6月4日

連接器 3.9.30 版本引入了以下更改。

Cloud Volumes ONTAP升級版本選擇器更新

透過升級Cloud Volumes ONTAP頁面，您現在可以選擇升級到最新可用的Cloud Volumes ONTAP版本或舊版本。

要了解有關透過BlueXP升級Cloud Volumes ONTAP 的更多信息，請參閱 "升級Cloud Volumes ONTAP"。

2023年5月7日

連接器 3.9.29 版本引入了以下更改。

Google Cloud 現已支持卡達地區

Google Cloud for Cloud Volumes ONTAP和 Connector for Cloud Volumes ONTAP 9.12.1 GA 及更高版本現已支援卡達地區。

Azure 現已支援瑞典中部地區

Azure 現已支援瑞典中部地區的Cloud Volumes ONTAP以及Cloud Volumes ONTAP 9.12.1 GA 及更高版本的連接器。

支援 **Azure** 澳洲東部的 **HA** 多可用性區域部署

Azure 中的澳洲東部區域現在支援Cloud Volumes ONTAP 9.12.1 GA 及更高版本的 HA 多可用區域部署。

充電使用情況明細

現在，您可以了解訂閱基於容量的授權時需要支付的費用。可以從BlueXP中的數位錢包下載以下類型的使用情況報告。使用情況報告提供您的訂閱的容量詳細信息，並告訴您如何為Cloud Volumes ONTAP訂閱中的資源付費。可下載的報告可以輕鬆地與他人分享。

- Cloud Volumes ONTAP軟體包使用情況
- 進階用法
- 儲存虛擬機器使用情況
- 卷使用情況

有關更多信息，請參閱 "管理基於容量的許可證" 。

現在，無需訂閱市場即可存取**BlueXP**並顯示通知

現在，只要您在沒有市場訂閱的情況下存取BlueXP中的Cloud Volumes ONTAP，就會顯示一則通知。通知指出“此工作環境的市場訂閱必須符合Cloud Volumes ONTAP條款和條件。”

AWS IAM 策略中為 **HA** 中介器新增了新權限

這些新的 AWS 權限已新增至Cloud Volumes ONTAP高可用性 (HA) 環境中 HA 中介器的 IAM 策略：

- sts：AssumeRole
- ec2:描述子網

2023年4月4日

對 **AWS** 中國區域的支持

從Cloud Volumes ONTAP 9.12.1 GA 開始，AWS 現在支援中國地區，如下所示。

- 支援單節點系統。
- 支援直接從NetApp購買的授權。

有關區域可用性，請參閱 "Cloud Volumes ONTAP的全球區域地圖"。

2023年4月3日

連接器 3.9.28 版本引入了以下更改。

Google Cloud 現已支援都靈地區

Google Cloud for Cloud Volumes ONTAP和 Connector for Cloud Volumes ONTAP 9.12.1 GA 及更高版本現已支援都靈地區。

BlueXP digital wallet增強功能

BlueXP digital wallet現在顯示您透過市場私人優惠購買的許可容量。

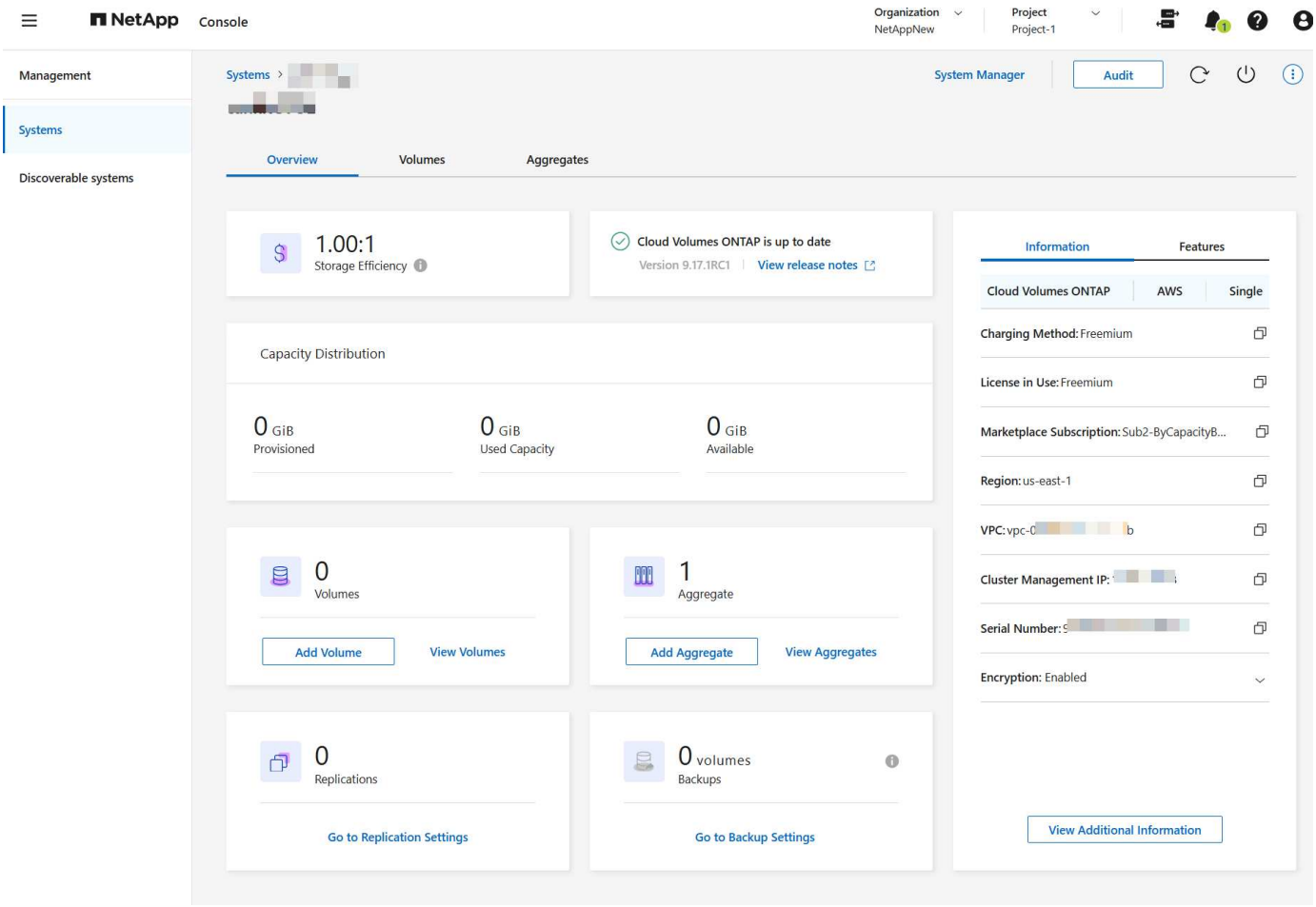
"了解如何查看帳戶中已消耗的容量" 。

支援在卷宗創建期間進行註釋

此版本可讓您在使用 API 建立Cloud Volumes ONTAP FlexGroup磁碟區或FlexVol volume時發表評論。

BlueXP使用者介面針對Cloud Volumes ONTAP概覽、磁碟區和聚合頁面進行了重新設計

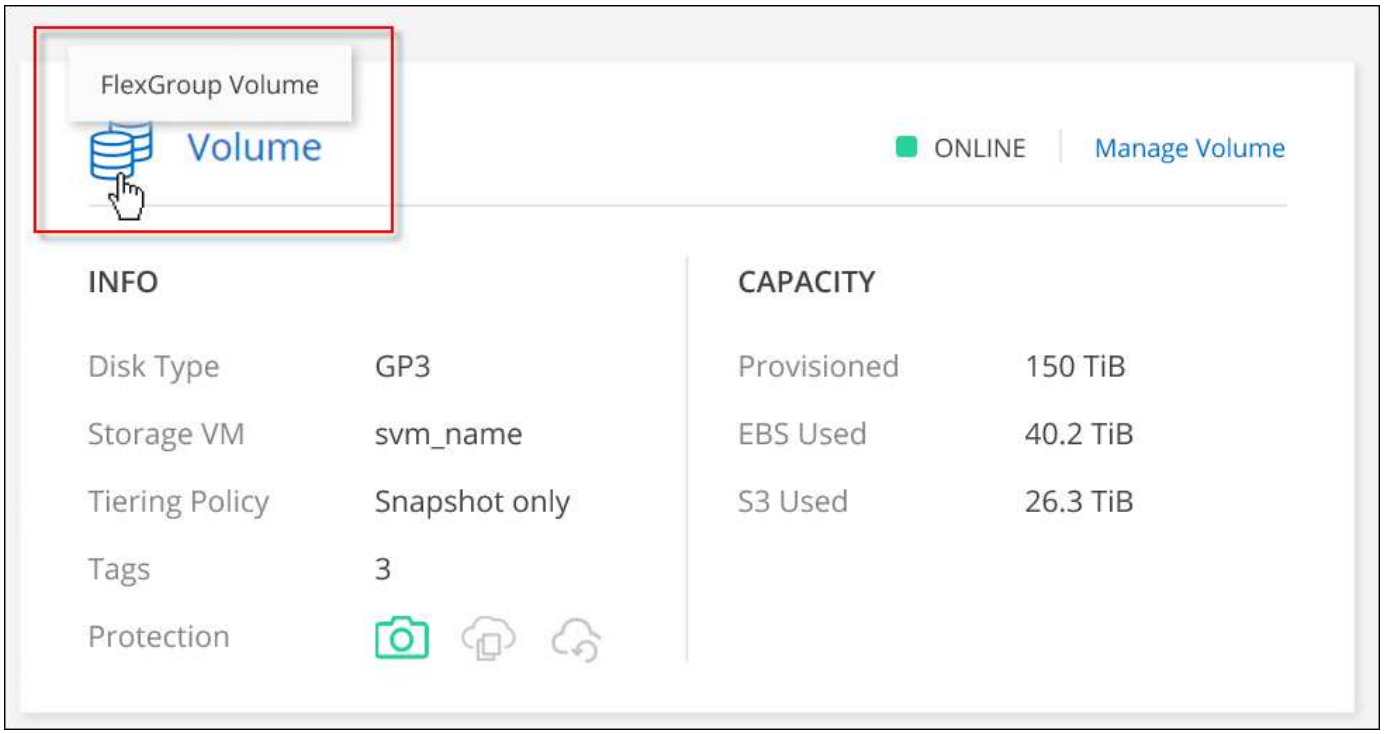
BlueXP現在重新設計了Cloud Volumes ONTAP概覽、磁碟區和聚合頁面的使用者介面。基於圖塊的設計在每個圖塊中呈現更全面的訊息，以獲得更好的使用者體驗。



可透過**Cloud Volumes ONTAP**查看**FlexGroup Volumes**

現在可以透過BlueXP中重新設計的磁碟區磁貼來檢視透過ONTAP System Manager 或ONTAP CLI 直接建立的FlexGroup磁碟區。與FlexVol磁碟區提供的資訊相同， BlueXP透過專用磁碟區圖塊提供已建立的FlexGroup磁碟區的詳細資訊。

目前，您只能查看BlueXP下的現有FlexGroup磁碟區。 BlueXP中創建FlexGroup卷的功能尚不可用，但計劃在未來版本中提供。



"了解有關查看已建立的FlexGroup區的更多資訊。"

2023年3月13日

Azure 對中國區域的支持

現在，中國北方 3 區域支援在 Azure 中單節點部署Cloud Volumes ONTAP 9.12.1 GA 和 9.13.0 GA。這些地區僅支援直接從NetApp購買的授權（BYOL 授權）。

僅 9.12.1 GA 和 9.13.0 GA 支援在中國區域全新部署Cloud Volumes ONTAP 。您可以將這些版本升級到Cloud Volumes ONTAP的更高修補程式和版本。如果您想在中國地區部署更高版本的Cloud Volumes ONTAP ，請聯絡NetApp支援。

有關區域可用性，請參閱 "Cloud Volumes ONTAP的全球區域地圖"。

2023年3月5日

連接器 3.9.27 版本引入了以下更改。

Cloud Volumes ONTAP 9.13.0

BlueXP現在可以在 AWS、Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.13.0。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

Azure 中的 **16 TiB** 和 **32 TiB** 支持

Cloud Volumes ONTAP現在支援 16 TiB 和 32 TiB 磁碟大小，用於在 Azure 中的託管磁碟上執行的高可用性部署。

詳細了解 "Azure 中支援的磁碟大小"。

MTEKM許可證

多租用戶加密金鑰管理 (MTEKM) 許可證現在包含在執行 9.12.1 GA 或更高版本的新舊Cloud Volumes ONTAP 系統中。

多租戶外部金鑰管理使單一儲存虛擬機器 (SVM) 能夠在使用NetApp磁碟區加密時透過 KMIP 伺服器維護自己的金鑰。

"了解如何使用NetApp加密解決方案加密磁碟區" 。

支援無網路環境

現在，任何與網路完全隔離的雲端環境都支援Cloud Volumes ONTAP 。這些環境僅支援基於節點的授權（BYOL）。不支援基於容量的許可。首先，手動安裝 Connector 軟體，登入 Connector 上執行的BlueXP控制台，將您的 BYOL 授權新增至BlueXP digital wallet，然後部署Cloud Volumes ONTAP。

- "在沒有網路存取的位置安裝連接器"
- "存取連接器上的BlueXP控制台"
- "新增未分配的許可證"

Google Cloud 中的 **Flash Cache** 和高寫入速度

現在， Cloud Volumes ONTAP 9.13.0 版本的選定實例可以支援快閃記憶體、高寫入速度和 8,896 位元組的高最大傳輸單元 (MTU)。

詳細了解 "Google Cloud 授權支援的配置"。

2023年2月5日

連接器 3.9.26 版本引入了以下更改。

在 **AWS** 中建立置放群組

現在可以使用新的配置設定來透過 AWS HA 單可用區 (AZ) 部署建立放置組。現在您可以選擇繞過失敗的放置群組建立並允許 AWS HA 單可用區部署成功完成。

有關如何配置置放群組建立設定的詳細信息，請參閱 "為 AWS HA 單可用區配置放置群組建立"。

私有 **DNS** 區域配置更新

現在可以使用新的配置設置，以便您在使用 Azure Private Links 時避免在私有 DNS 區域和虛擬網路之間建立連結。預設情況下啟用創建。

"向BlueXP提供有關 Azure 私人 DNS 的詳細信息"

WORM儲存與資料分層

現在，在建立Cloud Volumes ONTAP 9.8 系統或更高版本時，您可以同時啟用資料分層和 WORM 儲存。使用 WORM 儲存啟用資料分層可讓您將資料分層到雲端中的物件儲存。

"了解 WORM 儲存。"

2023年1月1日

連接器 3.9.25 版本引入了以下更改。

Google Cloud 中提供的授權包

Google Cloud Marketplace 中為Cloud Volumes ONTAP提供最佳化和基於 Edge Cache 容量的授權包，可作為即用即付產品或年度合約使用。

參考 "Cloud Volumes ONTAP許可"。

Cloud Volumes ONTAP的預設配置

多租用戶加密金鑰管理 (MTEKM) 授權不再包含在新的Cloud Volumes ONTAP部署中。

有關隨Cloud Volumes ONTAP自動安裝的ONTAP功能許可證的更多信息，請參閱 "Cloud Volumes ONTAP的預設配置"。

2022年12月15日

Cloud Volumes ONTAP 9.12.0

BlueXP現在可以在 AWS 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.12.0。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

2022年12月8日

Cloud Volumes ONTAP 9.12.1

BlueXP現在可以部署和管理Cloud Volumes ONTAP 9.12.1，其中包括對新功能和額外雲端提供者區域的支援。

"了解此版本Cloud Volumes ONTAP中包含的新功能"

2022年12月4日

連接器 3.9.24 版本引入了以下更改。

WORM + 雲端備份現在可在Cloud Volumes ONTAP建立期間使用

現在可以在Cloud Volumes ONTAP建立過程中啟動一次寫入、多次讀取 (WORM) 和雲端備份功能。

Google Cloud 現已支援以色列地區

Google Cloud for Cloud Volumes ONTAP和 Connector for Cloud Volumes ONTAP 9.11.1 P3 及更高版本現已支援以色列地區。

2022年11月15日

連接器 3.9.23 版本引入了以下更改。

Google Cloud 中的ONTAP S3 許可證

現在，在 Google Cloud Platform 中執行 9.12.1 或更高版本的新版和現有Cloud Volumes ONTAP系統均包含ONTAP S3 授權。

"ONTAP文件：了解如何設定和管理 S3 物件儲存服務"

2022年11月6日

連接器 3.9.23 版本引入了以下更改。

在 Azure 中移動資源組

現在，您可以將工作環境從相同 Azure 訂閱中的一個資源群組移至 Azure 中的另一個資源群組。

有關更多信息，請參閱 "移動資源組" 。

NDMP 副本認證

NDMP-copy 現已通過認證，可與 Cloud Volume ONTAP一起使用。

有關如何配置和使用 NDMP 的信息，請參閱 "ONTAP文件：NDMP 設定概述"。

Azure 的託管磁碟加密支援

已新增新的 Azure 權限，現在允許您在建立時加密所有託管磁碟。

有關此新功能的更多信息，請參閱 "設定Cloud Volumes ONTAP以在 Azure 中使用客戶管理的金鑰"。

2022年9月18日

連接器 3.9.22 版本引入了以下更改。

數位錢包增強功能

- 數位錢包現在顯示優化 I/O 許可包的摘要以及您帳戶中Cloud Volumes ONTAP系統的預先配置 WORM 容量。

  這些詳細資訊可以幫助您更了解收費方式以及是否需要購買額外的容量。

  "了解如何查看帳戶中已消耗的容量" 。

- 現在您可以從一種充電方式變更為優化充電方式。

  "了解如何更改充電方式" 。

優化成本和性能

現在您可以直接從 Canvas 優化Cloud Volumes ONTAP系統的成本和效能。

選擇工作環境後，您可以選擇「最佳化成本和效能」選項來變更Cloud Volumes ONTAP的實例類型。選擇較小規模的實例可以幫助您降低成本，而更改為較大規模的實例可以幫助您優化效能。

[選擇Cloud Volumes ONTAP系統後，可從 Canvas 取得「最佳化成本和效能」選項的螢幕截圖。]

AutoSupport通知

如果Cloud Volumes ONTAP系統無法傳送AutoSupport訊息， BlueXP現在將產生通知。通知中包含一個鏈接，您可以使用該鏈接來解決網絡問題。

2022年7月31日

連接器 3.9.21 版本引入了以下更改。

MTEKM許可證

多租用戶加密金鑰管理 (MTEKM) 許可證現在包含在執行 9.11.1 或更高版本的新和現有Cloud Volumes ONTAP系統中。

多租戶外部金鑰管理使單一儲存虛擬機器 (SVM) 能夠在使用NetApp磁碟區加密時透過 KMIP 伺服器維護自己的金鑰。

"了解如何使用NetApp加密解決方案加密磁碟區" 。

代理伺服器

如果沒有可用的出站網路連線來傳送AutoSupport訊息， BlueXP現在會自動設定您的Cloud Volumes ONTAP系統以使用連接器作為代理伺服器。

AutoSupport主動監控系統的健康狀況並向NetApp技術支援發送訊息。

唯一的要求是確保連接器的安全群組允許透過連接埠 3128 進行入站連接。部署連接器後，您需要開啟此連接埠。

更改充電方式

現在您可以變更使用基於容量的許可的Cloud Volumes ONTAP系統的收費方法。例如，如果您使用 Essentials 套件部署了Cloud Volumes ONTAP系統，則可以在業務需求變更時將其變更為 Professional 套件。此功能可透過數位錢包取得。

"了解如何更改充電方式" 。

安全群組增強

當您建立Cloud Volumes ONTAP工作環境時，使用者介面現在允許您選擇是否希望預先定義安全群組僅允許所選網路內的流量（建議）或所有網路內的流量。

[螢幕截圖顯示了選擇安全群組時工作環境精靈中可用的「允許內部流量」選項。]

2022年7月18日

Azure 中的新授權包

當您透過 Azure 市場訂閱付款時，Azure 中的Cloud Volumes ONTAP可以使用兩個新的基於容量的授權包：

- 優化：分別支付配置容量和 I/O 操作的費用
- **Edge Cache**：許可 "Cloud Volumes 邊緣緩存"

"了解有關這些許可包的更多信息" 。

2022年7月3日

連接器 3.9.20 版本引入了以下更改。

數位錢包

數位錢包現在顯示您帳戶中消耗的總容量以及許可證包消耗的容量。這可以幫助您了解收費方式以及是否需要購買額外的容量。

[顯示基於容量的許可證的數位錢包頁面的螢幕截圖。該頁面概述了您帳戶中已消耗的容量，然後按許可包細分了已消耗的容量。]

彈性卷增強

現在，從使用者介面建立Cloud Volumes ONTAP工作環境時， BlueXP支援 Amazon EBS Elastic Volumes 功能。使用 gp3 或 io1 磁碟時，彈性磁碟區功能預設為啟用。您可以根據您的儲存需求選擇初始容量，並在部署Cloud Volumes ONTAP後進行修改。

"了解有關 AWS 彈性卷支援的更多信息" 。

AWS 中的ONTAP S3 許可證

現在，在 AWS 中執行 9.11.0 或更高版本的新版本和現有Cloud Volumes ONTAP系統都包含ONTAP S3 授權。

"ONTAP文件：了解如何設定和管理 S3 物件儲存服務"

新的 Azure 雲端區域支持

從 9.10.1 版本開始，Azure West US 3 區域現在支援Cloud Volumes ONTAP 。

"查看Cloud Volumes ONTAP支援區域的完整列表"

Azure 中的ONTAP S3 許可證

現在，在 Azure 中執行 9.9.1 或更高版本的新版和現有Cloud Volumes ONTAP系統均包含ONTAP S3 授權。

"ONTAP文件：了解如何設定和管理 S3 物件儲存服務"

2022年6月7日

連接器 3.9.19 版本引入了以下更改。

Cloud Volumes ONTAP 9.11.1

BlueXP現在可以部署和管理Cloud Volumes ONTAP 9.11.1，其中包括對新功能和額外雲端提供者區域的支援。

"了解此版本Cloud Volumes ONTAP中包含的新功能"

新的高級視圖

如果您需要對Cloud Volumes ONTAP執行高階管理，則可以使用ONTAP System Manager（它是ONTAP系統提供的管理介面）來執行此操作。我們已將系統管理器介面直接包含在BlueXP中，讓您無需離開BlueXP即可進行高階管理。

此進階視圖可作為Cloud Volumes ONTAP 9.10.0 及更高版本的預覽版使用。我們計劃在即將發布的版本中完善這種體驗並增加增強功能。請使用產品內聊天向我們發送回饋。

"了解有關高級視圖的更多信息" 。

支援 **Amazon EBS** 彈性卷

透過Cloud Volumes ONTAP聚合支援 Amazon EBS Elastic Volumes 功能可提供更好的效能和額外的容量，同時使BlueXP能夠根據需要自動增加底層磁碟容量。

從 *new* Cloud Volumes ONTAP 9.11.0 系統以及 gp3 和 io1 EBS 磁碟類型開始，可以支援彈性磁碟區。

"了解有關彈性卷支持的更多信息" 。

請注意，對彈性磁碟區的支援需要為連接器授予新的 AWS 權限：

```
"ec2:DescribeVolumesModifications",
"ec2:ModifyVolume",
```

確保為您新增至BlueXP 的每組 AWS 憑證提供這些權限。 "查看最新的 AWS 連接器策略" 。

支援在共用 **AWS** 子網路中部署 **HA** 對

Cloud Volumes ONTAP 9.11.1 包含對 AWS VPC 共享的支援。此版本的連接器可讓您在使用 API 時在 AWS 共用子網路中部署 HA 對。

"了解如何在共享子網路中部署 HA 對" 。

使用服務端點時網路存取受限

當使用 VNet 服務端點在Cloud Volumes ONTAP和儲存帳戶之間建立連線時， BlueXP現在會限制網路存取。如果您停用 Azure Private Link 連接， BlueXP將使用服務端點。

"了解有關 Azure Private Link 與Cloud Volumes ONTAP連接的更多信息" 。

支援在 **Google Cloud** 中建立儲存虛擬機

從 9.11.1 版本開始，Google Cloud 中的Cloud Volumes ONTAP現在支援多個儲存虛擬機器。從此版本的連接器開始， BlueXP可讓您使用 API 在 Google Cloud 中的Cloud Volumes ONTAP HA 對上建立儲存虛擬機器。

若要支援建立儲存虛擬機，需要為連接器授予新的 Google Cloud 權限：

```
- compute.instanceGroups.get
- compute.addresses.get
```

請注意、您必須使用 ONTAP CLI 或 System Manager 在單節點系統上建立儲存 VM。

- "詳細了解 Google Cloud 中的儲存虛擬機器限制"
- "了解如何在 Google Cloud 中為Cloud Volumes ONTAP建立資料服務儲存虛擬機"

2022年5月2日

連接器 3.9.18 版本引入了以下更改。

Cloud Volumes ONTAP 9.11.0

BlueXP現在可以部署和管理Cloud Volumes ONTAP 9.11.0。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

增強調解員升級

當BlueXP升級 HA 對的中介器時，它會在刪除啟動磁碟之前驗證是否有新的中介器映像可用。此變更可確保升級過程不成功時中介仍可繼續成功運作。

K8s 選項卡已刪除

K8s 選項卡在先前的版本中已被棄用，現在已被刪除。

Azure 年度合約

現在可以透過年度合約在 Azure 中使用 Essentials 和 Professional 套件。您可以聯絡NetApp銷售代表購買年度合約。該合約在 Azure 市場中以私人優惠形式提供。

NetApp與您分享私人優惠後，您可以在建立工作環境期間從 Azure 市場訂閱時選擇年度方案。

"了解有關許可的更多信息" 。

S3 Glacier 即時檢索

現在您可以將分層資料儲存在 Amazon Simple Storage Service（Amazon S3）Glacier Instant Retrieval 儲存類別中。

"了解如何變更分層資料的儲存類別" 。

連接器所需的新 **AWS** 權限

在單一可用區 (AZ) 中部署 HA 對時，現在需要下列權限來建立 AWS 分佈置放群組：

```
"ec2:DescribePlacementGroups",
"iam:GetRolePolicy",
```

現在需要這些權限來優化BlueXP建立放置群組的方式。

確保為您新增至BlueXP 的每組 AWS 憑證提供這些權限。 "查看最新的 AWS 連接器策略" 。

新的 **Google Cloud** 區域支持

從 9.10.1 版本開始，以下 Google Cloud 區域現在支援Cloud Volumes ONTAP ：

- 德里 (asia-south2)
- 墨爾本 (australia-southeast2)
- 米蘭 (europe-west8) - 僅限單節點
- 聖地牙哥 (southamerica-west1) - 僅限單一節點

"查看Cloud Volumes ONTAP支援區域的完整列表"

Google Cloud 支援 **n2-standard-16**

從 9.10.1 版本開始，Google Cloud 中的Cloud Volumes ONTAP現在支援 n2-standard-16 機器類型。

"查看 Google Cloud 中Cloud Volumes ONTAP支援的配置"

Google Cloud 防火牆政策的增強功能

- 當您在 Google Cloud 中建立Cloud Volumes ONTAP HA 對時， BlueXP現在將顯示 VPC 中所有現有的防火牆策略。

  以前， BlueXP不會顯示 VPC-1、VPC-2 或 VPC-3 中沒有目標標籤的任何政策。

- 在 Google Cloud 中建立 Cloud Volumes ONTAP 單節點系統時，現在可以選擇預先定義的防火牆原則是僅允許選定 VPC 內的流量（建議）還是允許所有 VPC 內的流量。

Google Cloud 服務帳戶的增強功能

當您選擇與Cloud Volumes ONTAP一起使用的 Google Cloud 服務帳戶時， BlueXP現在會顯示與每個服務帳戶關聯的電子郵件地址。查看電子郵件地址可以更容易區分同名的服務帳戶。

[服務帳戶欄位的螢幕截圖]

2022年4月3日

系統管理員連結已刪除

我們刪除了先前在Cloud Volumes ONTAP工作環境中可用的系統管理器連結。

您仍可透過在與Cloud Volumes ONTAP系統連線的 Web 瀏覽器中輸入叢集管理 IP 位址來連線至系統管理員。 "了解有關連接到系統管理器的更多信息" 。

WORM儲存收費

現在，優惠特價已經過期，您現在需要為使用 WORM 儲存付費。根據 WORM 卷的總配置容量按小時收費。這適用於新的和現有的Cloud Volumes ONTAP系統。

"了解 WORM 儲存的定價" 。

2022年2月27日

連接器 3.9.16 版本引入了以下更改。

重新設計的捲嚮導

我們最近推出的建立新磁碟區精靈現在可在從「進階分配」選項在特定聚合上建立磁碟區時使用。

"了解如何在特定聚合上建立卷" 。

2022年2月9日

市場更新

- 現在，所有雲端供應商市場均提供 Essentials 套餐和 Professional 套餐。

  這些按容量收費的方法使您能夠按小時付費或直接從雲端提供者購買年度合約。您仍然可以選擇直接從NetApp購買按容量許可證。

  如果您在雲端市場中已有訂閱，那麼您也會自動訂閱這些新產品。部署新的Cloud Volumes ONTAP工作環境時，您可以選擇按容量收費。

  如果您是新客戶， BlueXP會在您建立新的工作環境時提示您訂閱。

- 所有雲端供應商市場的按節點許可均已棄用，並且不再適用於新訂戶。這包括年度合約和小時訂閱（探索、標準和高級）。

  此收費方式仍適用於擁有有效訂閱的現有客戶。

"了解有關Cloud Volumes ONTAP許可選項的更多信息" 。

2022年2月6日

交換未分配的許可證

如果您有未指派的基於節點的Cloud Volumes ONTAP許可證且尚未使用，您現在可以將其轉換為 Cloud Backup 許可證、Cloud Data Sense 許可證或 Cloud Tiering 許可證來交換該許可證。

此操作將撤銷Cloud Volumes ONTAP許可證，並為該服務建立具有相同到期日的等值美元許可證。

"了解如何交換未分配的基於節點的許可證" 。

2022年1月30日

連接器 3.9.15 版本引入了以下更改。

重新設計的授權選擇

我們重新設計了建立新的Cloud Volumes ONTAP工作環境時的許可選擇畫面。這些變化凸顯了 2021 年 7 月推出的按容量收費方法，並支援透過雲端供應商市場推出的即將推出的產品。

數位錢包更新

我們透過將Cloud Volumes ONTAP許可證整合到一個選項卡中來更新*數位錢包*。

2022年1月2日

連接器 3.9.14 版本引入了以下更改。

支援其他 **Azure VM** 類型

從 9.10.1 版本開始， Cloud Volumes ONTAP現在支援 Microsoft Azure 中的以下 VM 類型：

- E4ds_v4
- E8ds_v4
- E32ds_v4
- E48ds_v4

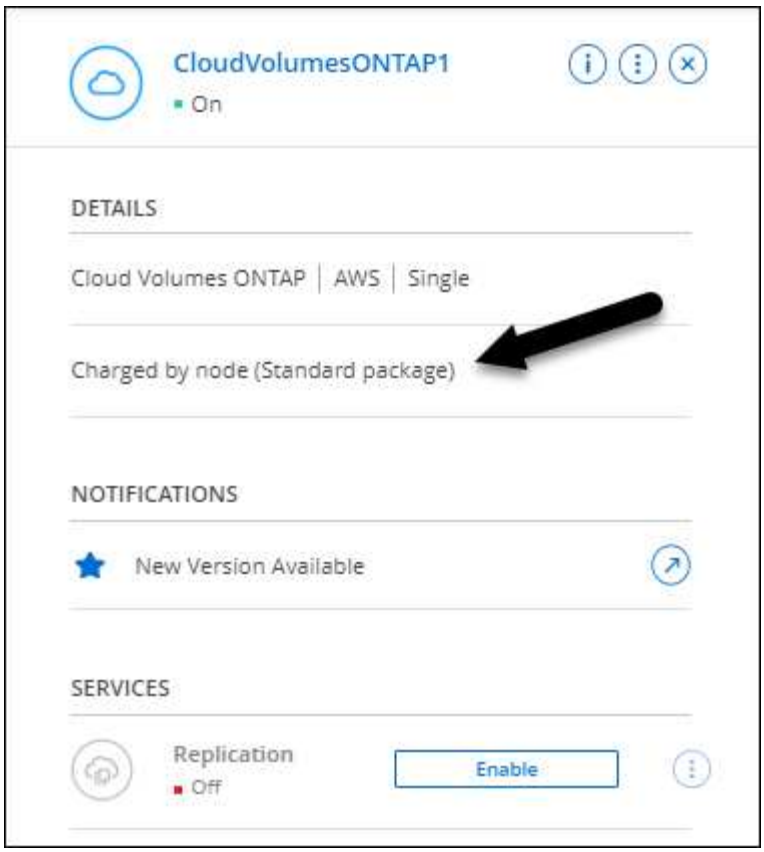
前往 "Cloud Volumes ONTAP發行說明"有關支援的配置的更多詳細資訊。

FlexClone收費更新

如果你使用 "基於容量的許可證"對於Cloud Volumes ONTAP，您不再需要為FlexClone磁碟區所使用的容量付費。

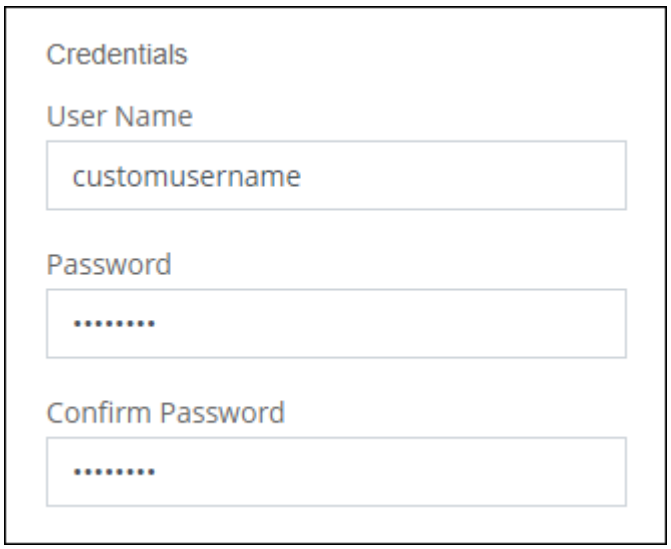
充電方式現已顯示

BlueXP現在在 Canvas 的右側面板中顯示每個Cloud Volumes ONTAP工作環境的收費方式。



選擇你的用戶名

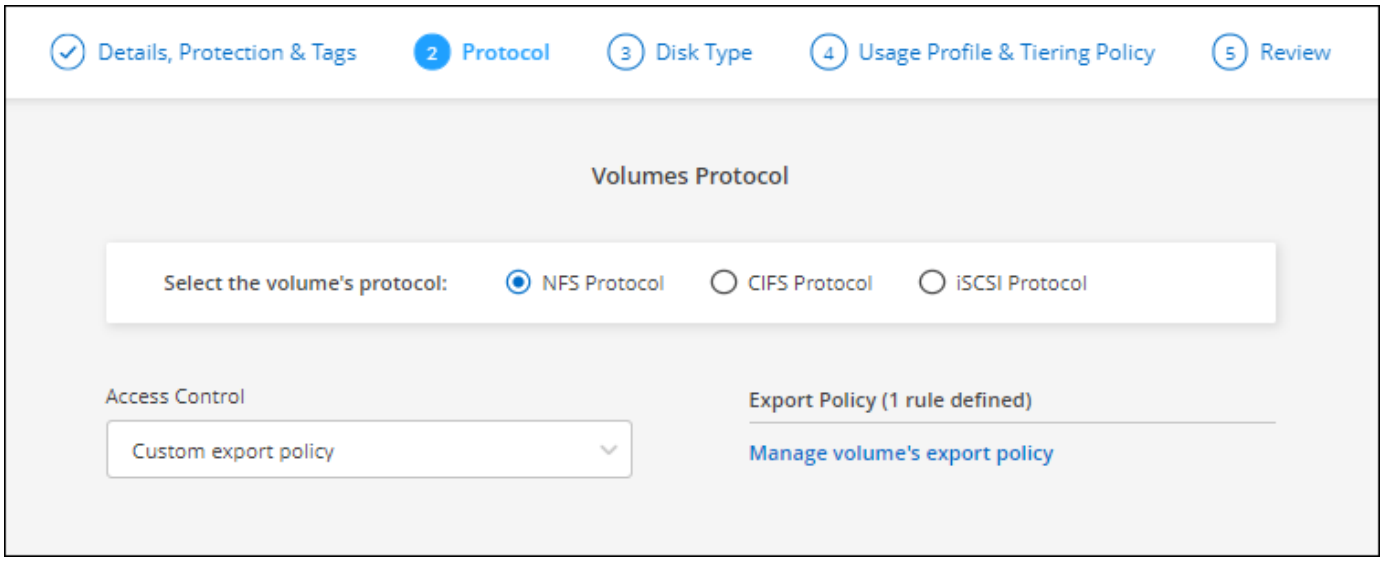
當您建立Cloud Volumes ONTAP工作環境時，現在可以選擇輸入您的首選使用者名，而不是預設的管理員使用者名稱。



磁碟區建立增強功能

我們對卷宗創建做了一些增強：

- 我們重新設計了建立磁碟區精靈，以便於使用。
- 現在您可以為 NFS 選擇自訂匯出策略。



2021年11月28日

連接器 3.9.13 版本引入了以下更改。

Cloud Volumes ONTAP 9.10.1

BlueXP現在可以部署和管理Cloud Volumes ONTAP 9.10.1。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

NetApp Keystone訂閱

現在您可以使用Keystone訂閱來支付Cloud Volumes ONTAP HA 對的費用。

Keystone訂閱是一種按需付費的訂閱式服務，為那些喜歡 OpEx 消費模式而非前期資本支出或租賃的用戶提供無縫的混合雲端體驗。

您可以從BlueXP部署的所有新版本的Cloud Volumes ONTAP都支援Keystone訂閱。

- "了解有關NetApp Keystone訂閱的更多信息" 。
- "了解如何在BlueXP中開始使用Keystone訂閱" 。

新的 **AWS** 區域支持

Cloud Volumes ONTAP現已在 AWS 亞太地區（大阪）區域（ap-northeast-3）獲得支援。

連接埠減少

Azure 中的 Cloud Volumes ONTAP 系統（包括單節點系統和 HA 配對）不再開放連接埠 8023 和 49000。

此變更適用於從 Connector 3.9.13 版本開始的_new_ Cloud Volumes ONTAP系統。

2021年10月4日

連接器 3.9.11 版本引入了以下更改。

Cloud Volumes ONTAP 9.10.0

BlueXP現在可以部署和管理Cloud Volumes ONTAP 9.10.0。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

減少部署時間

當啟用正常寫入速度時，我們減少了在 Microsoft Azure 或 Google Cloud 中部署Cloud Volumes ONTAP工作環境所需的時間。現在部署時間平均縮短了 3-4 分鐘。

2021年9月2日

連接器 3.9.10 版本引入了以下更改。

Azure 中的客戶管理加密金鑰

使用以下方式在 Azure 中的Cloud Volumes ONTAP上自動加密數據 "Azure 儲存服務加密"使用 Microsoft 管理的金鑰。但現在您可以透過完成以下步驟來使用您自己的客戶管理的加密金鑰：

1. 從 Azure 建立一個金鑰保管庫，然後在該保管庫中產生一個金鑰。
2. 從BlueXP中，使用 API 建立使用金鑰的Cloud Volumes ONTAP工作環境。

"了解有關這些步驟的更多信息" 。

2021年7月7日

連接器 3.9.8 版本引入了以下更改。

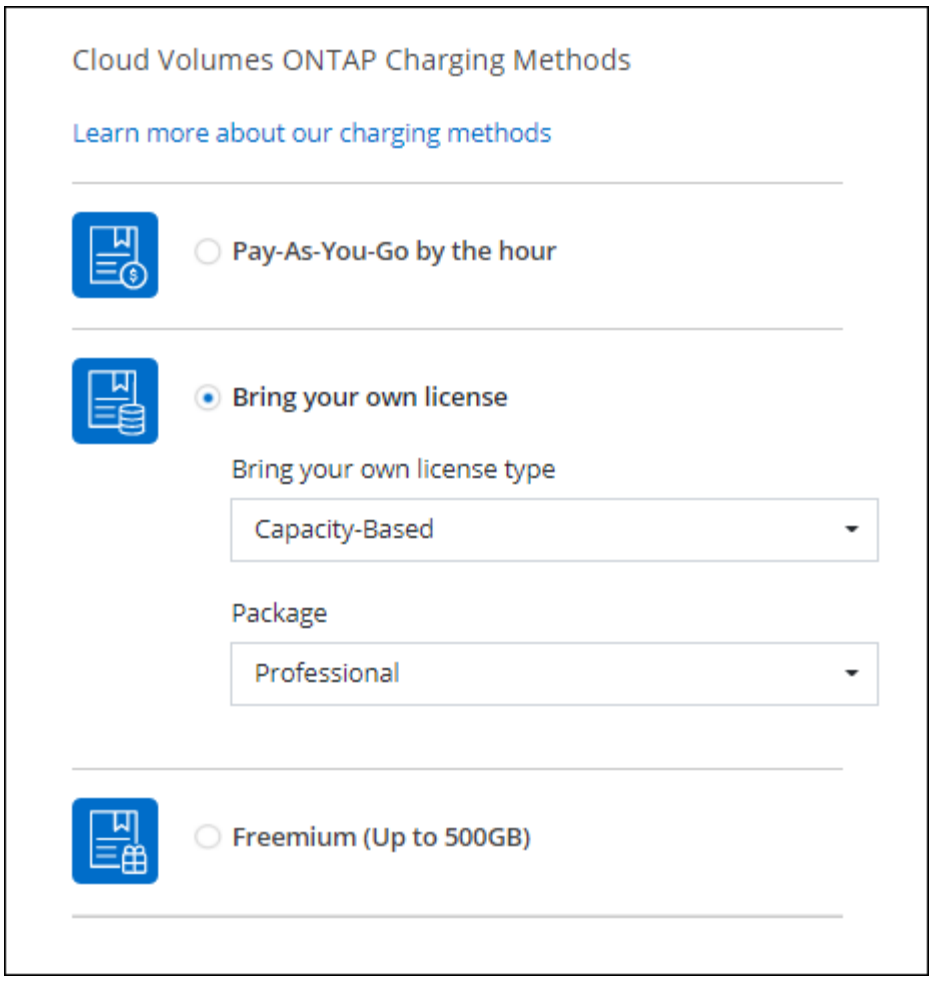
新的充電方式

Cloud Volumes ONTAP有新的計費方式。

- 基於容量的 **BYOL**：基於容量的許可證可讓您按 TiB 容量支付Cloud Volumes ONTAP費用。該許可證與您的NetApp帳戶相關聯，只要您的許可證提供足夠的容量，您就可以建立多個Cloud Volumes ONTAP系統。基於容量的許可以包的形式提供，可以是_Essentials_ 或_Professional_。
- 免費加值服務：免費加值服務可讓您免費使用NetApp的所有Cloud Volumes ONTAP功能（仍需支付雲端供應商費用）。每個系統的配置容量限制為 500 GiB，並且沒有支援合約。您最多可以擁有 10 個免費增值系統。

  "了解有關這些許可選項的更多信息" 。

  以下是您可以選擇的充電方法的範例：



WORM 儲存可供一般使用

一次寫入，多次讀取 (WORM) 儲存不再處於預覽階段，現在可以透過Cloud Volumes ONTAP供一般使用。 "了解有關 WORM 存儲的更多信息" 。

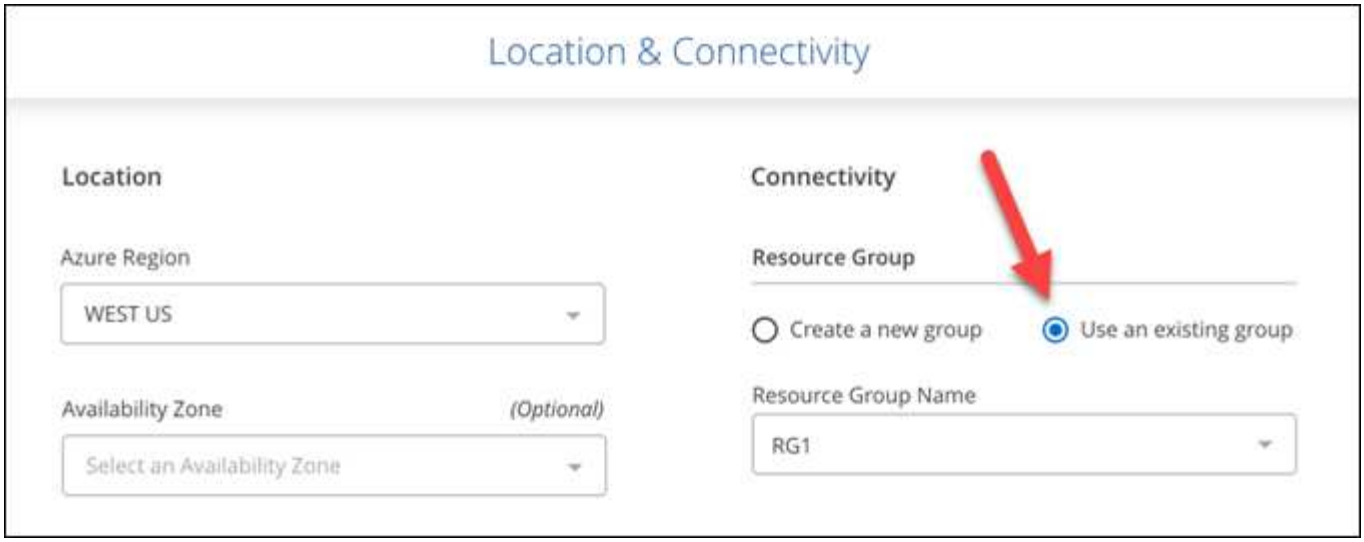
AWS 中對 **m5dn.24xlarge** 的支持

從 9.9.1 版本開始， Cloud Volumes ONTAP現在支援 m5dn.24xlarge 執行個體類型，並具有以下收費方式：PAYGO Premium、自帶授權 (BYOL) 和 Freemium。

"查看 AWS 中Cloud Volumes ONTAP支援的配置" 。

選擇現有的 **Azure** 資源群組

在 Azure 中建立Cloud Volumes ONTAP系統時，現在可以選擇為 VM 及其相關資源選擇現有資源組。



如果部署失敗或刪除，下列權限可讓BlueXP從資源組中刪除Cloud Volumes ONTAP資源：

```
"Microsoft.Network/privateEndpoints/delete",
"Microsoft.Compute/availabilitySets/delete",
```

確保提供這些權限給新增至BlueXP 的每組 Azure 憑證。 "查看 Azure 的最新連接器策略" 。

Azure 現已停用 **Blob** 公用存取

作為安全增強功能， BlueXP現在在為Cloud Volumes ONTAP建立儲存帳戶時停用 **Blob** 公共存取。

Azure Private Link 增強功能

預設情況下， BlueXP現在在新的Cloud Volumes ONTAP系統的啟動診斷儲存帳戶上啟用 Azure Private Link 連線。

這意味著Cloud Volumes ONTAP的所有儲存帳戶現在都將使用私有連結。

"了解有關使用 Azure Private Link 和Cloud Volumes ONTAP 的更多信息" 。

Google Cloud 中的平衡持久性磁碟

從 9.9.1 版本開始， Cloud Volumes ONTAP現在支援平衡持久性磁碟 (pd-balanced)。

這些 SSD 透過提供較低的每 GiB IOPS 來平衡效能和成本。

Google Cloud 不再支援 **custom-4-16384**

新的Cloud Volumes ONTAP系統不再支援 custom-4-16384 機器類型。

如果您現有的系統正在此機器類型上運行，您可以繼續使用它，但我們建議切換到 n2-standard-4 機器類型。

"查看 Google Cloud 中Cloud Volumes ONTAP支援的配置"。

2021年5月30日

連接器 3.9.7 版本引入了以下更改。

AWS 中的新專業套餐

新的專業套餐可讓您使用 AWS Marketplace 的年度合約捆綁Cloud Volumes ONTAP和Cloud Backup Service。按 TiB 付款。此訂閱不允許您備份本機資料。

如果您選擇此付款方式，您可以透過 EBS 磁碟和分層到 S3 物件儲存（單節點或 HA）為每個Cloud Volumes ONTAP系統配置最多 2 PiB。

前往 "AWS Marketplace 頁面"查看定價詳情並前往 "Cloud Volumes ONTAP發行說明"了解有關此許可選項的更多資訊。

AWS 中 **EBS** 磁碟區上的標籤

BlueXP現在在建立新的Cloud Volumes ONTAP工作環境時會為 EBS 磁碟區新增標籤。這些標籤是在部署Cloud Volumes ONTAP之後建立的。

如果您的組織使用服務控制策略 (SCP) 來管理權限，則此變更會有所幫助。

自動分層策略的最短冷卻期

如果您使用自動分層策略在磁碟區上啟用了資料分層，現在可以使用 API 調整最短冷卻期。

"了解如何調整最短冷卻時間。"

增強自訂導出策略

當您建立新的 NFS 磁碟區時， BlueXP現在會按升序顯示自訂匯出策略，讓您更容易找到所需的匯出策略。

刪除舊的雲端快照

BlueXP現在會刪除在部署Cloud Volumes ONTAP系統時以及每次關閉電源時建立的根和啟動磁碟的舊雲端快照。根捲和啟動磁碟區僅保留最近的兩個快照。

此增強功能透過刪除不再需要的快照來幫助降低雲端提供者的成本。

請注意，連接器需要新的權限才能刪除 Azure 快照。 "查看 Azure 的最新連接器策略" 。

```
"Microsoft.Compute/snapshots/delete"
```

2021年5月24日

Cloud Volumes ONTAP 9.9.1

BlueXP現在可以部署和管理Cloud Volumes ONTAP 9.9.1。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

2021年4月11日

連接器 3.9.5 版本引入了以下更改。

邏輯空間報告

BlueXP現在可以在其為Cloud Volumes ONTAP建立的初始儲存 VM 上啟用邏輯空間報告。

當邏輯報告空間時， ONTAP會報告磁碟區空間，以便儲存效率功能節省的所有實體空間也被報告為已使用。

AWS 中對 **gp3** 磁碟的支持

從 9.7 版本開始， Cloud Volumes ONTAP現在支援_通用 SSD (gp3)_ 磁碟。 gp3 磁碟是成本最低的 SSD，可在廣泛的工作負載中平衡成本和效能。

"在 AWS 中調整系統大小" 。

AWS 不再支援冷 **HDD** 磁碟

Cloud Volumes ONTAP不再支援 Cold HDD (sc1) 磁碟。

Azure 儲存體帳戶的 **TLS 1.2**

當BlueXP在 Azure 中為Cloud Volumes ONTAP建立儲存帳戶時，該儲存帳戶的 TLS 版本現在為 1.2 版。

2021年3月8日

連接器 3.9.4 版本引入了以下更改。

Cloud Volumes ONTAP 9.9.0

BlueXP現在可以部署和管理Cloud Volumes ONTAP 9.9.0。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

支援 **AWS C2S** 環境

現在您可以在 AWS 商業雲端服務 (C2S) 環境中部署Cloud Volumes ONTAP 9.8。

"在 AWS Secret Cloud 或 AWS Top Secret Cloud 中部署Cloud Volumes ONTAP" 。

使用客戶管理的 **CMK** 進行 **AWS** 加密

BlueXP始終允許您使用 AWS 金鑰管理服務 (KMS) 加密Cloud Volumes ONTAP資料。從Cloud Volumes ONTAP 9.9.0 開始，如果您選擇客戶管理的 CMK，則 EBS 磁碟上的資料和分層到 S3 的資料都會加密。以前，只有 EBS 資料會加密。

請注意，您需要為Cloud Volumes ONTAP IAM 角色提供使用 CMK 的存取權限。

"了解有關使用Cloud Volumes ONTAP設定 AWS KMS 的更多信息" 。

對 **Azure DoD** 的支持

您現在可以在 Azure 國防部 (DoD) 影響等級 6 (IL6) 中部署Cloud Volumes ONTAP 9.8。

Google Cloud 中的 **IP** 位址減少

我們減少了 Google Cloud 中Cloud Volumes ONTAP 9.8 及更高版本所需的 IP 位址數量。預設情況下，需要的 IP 位址少一個（我們將群集間 LIF 與節點管理 LIF 統一起來）。您也可以選擇在使用 API 時跳過建立 SVM 管理 LIF，這將減少對額外 IP 位址的需求。

"詳細了解 Google Cloud 中的 IP 位址要求"。

Google Cloud 中的共享 **VPC** 支持

在 Google Cloud 中部署Cloud Volumes ONTAP HA 對時，您現在可以為 VPC-1、VPC-2 和 VPC-3 選擇共用 VPC。以前，只有 VPC-0 可以成為共用 VPC。 Cloud Volumes ONTAP 9.8 及更高版本支援此變更。

"詳細了解 Google Cloud 網路需求"。

2021年1月4日

連接器 3.9.2 版本引入了以下更改。

AWS Outposts

幾個月前，我們宣布Cloud Volumes ONTAP已獲得 Amazon Web Services (AWS) Outposts Ready 認證。今天，我們很高興地宣布，我們已經透過 AWS Outposts 驗證了BlueXP和Cloud Volumes ONTAP 。

如果您有 AWS Outpost，則可以透過在工作環境精靈中選擇 Outpost VPC 在該 Outpost 中部署Cloud Volumes ONTAP 。體驗與駐留在 AWS 中的任何其他 VPC 相同。請注意，您需要先在 AWS Outpost 中部署連接器。

需要指出的是，存在一些限制：

- 目前僅支援單節點Cloud Volumes ONTAP系統
- 可與Cloud Volumes ONTAP一起使用的 EC2 執行個體僅限於 Outpost 中可用的執行個體
- 目前僅支援通用 SSD（gp2）

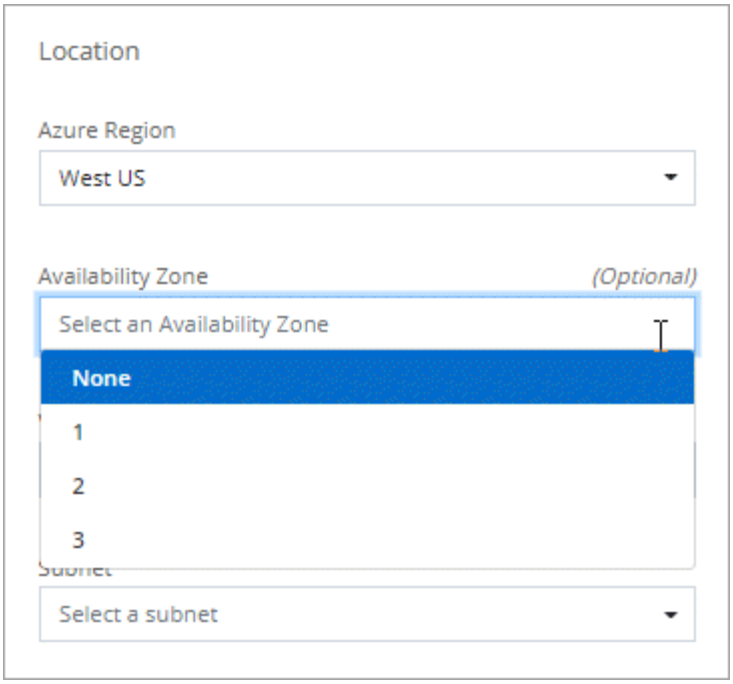
支援的 **Azure** 區域中的 **Ultra SSD VNVRAM**

當您在單節點系統中使用 E32s_v3 VM 類型時，Cloud Volumes ONTAP 現在可以使用 Ultra SSD 作為 VNVRAM "在任何受支援的 Azure 區域中"。

VNVRAM 提供更好的寫入效能。

在 **Azure** 中選擇一個可用性區域

現在您可以選擇要部署單節點Cloud Volumes ONTAP系統的可用區域。如果您不選擇 AZ， BlueXP將為您選擇一個。



Google Cloud 中的更大磁碟

Cloud Volumes ONTAP 現在支援 Google Cloud 中的 64 TB 磁碟。

由於 Google Cloud 限制，僅使用磁碟的最大系統容量仍為 256 TB。

Google Cloud 中的新機器類型

Cloud Volumes ONTAP現在支援以下機器類型：

- n2-standard-4 附有 Explore 授權和 BYOL
- n2-standard-8 具有標準授權和 BYOL
- 具有 Premium 許可證和 BYOL 的 n2-standard-32

2020年11月3日

連接器 3.9.0 版本引入了以下變更。

適用於**Cloud Volumes ONTAP** 的**Azure Private Link**

預設情況下， BlueXP現在啟用Cloud Volumes ONTAP及其關聯儲存帳戶之間的 Azure Private Link 連線。專用連結可保護 Azure 中端點之間的連線。

- "了解有關 Azure Private Links 的更多信息"
- "了解有關使用 Azure Private Link 和Cloud Volumes ONTAP 的更多信息"

已知限制

已知限制標識了該產品的此版本不支援或無法與其正確互通的平台、裝置或功能。仔細審

查這些限制。

這些限制特定於NetApp Console中的Cloud Volumes ONTAP管理。若要查看Cloud Volumes ONTAP軟體本身的限制， "前往Cloud Volumes ONTAP發行說明" 。

控制台不支援創建**FlexGroup**卷

雖然Cloud Volumes ONTAP支援FlexGroup卷，但控制台目前不支援建立FlexGroup卷。如果您從ONTAP系統管理員或ONTAP CLI 建立FlexGroup卷，則應將控制台中的容量管理模式設為 `Manual`。 `Automatic`模式可能無法與FlexGroup磁碟區正常搭配使用。

我們計劃在未來的版本中提供在控制台中建立FlexGroup磁碟區的功能。

控制台不支援帶有**Cloud Volumes ONTAP** 的**S3**

雖然 Cloud Volumes ONTAP 支援 S3 作為橫向擴充儲存選項，但 Console 不提供任何此功能的管理功能。使用 CLI 是從 Cloud Volumes ONTAP 設定 S3 用戶端存取的最佳實踐做法。如需詳細資訊，請參閱 "ONTAP S3 組態電源指南"。

"深入瞭解 Cloud Volumes ONTAP 對 ONTAP S3 和其他用戶端通訊協定的支援"。

控制台不支援儲存虛擬機器的災難復原

控制台不提供儲存虛擬機器 (SVM) 災難復原的任何設定或編排支援。您必須使用ONTAP系統管理員或ONTAP CLI。

"了解有關 SVM 災難復原的更多信息" 。

Cloud Volumes ONTAP發行說明

Cloud Volumes ONTAP的發行說明提供了特定於版本的資訊。版本中的新功能、支援的配置、儲存限制以及任何可能影響產品功能的已知限製或問題。

"轉至Cloud Volumes ONTAP發行說明"

開始

了解Cloud Volumes ONTAP

Cloud Volumes ONTAP可讓您最佳化雲端儲存成本和效能，同時增強資料保護、安全性和合規性。

Cloud Volumes ONTAP是一款純軟體儲存設備，可在雲端運行ONTAP資料管理軟體。它提供具有以下主要功能的企業級儲存：

- 儲存效率

  利用內建資料重複資料刪除、資料壓縮、精簡配置和複製來最大限度地降低儲存成本。

- 高可用性

  確保雲端環境故障時企業的可靠性和持續運作。

- 資料保護

  Cloud Volumes ONTAP利用 NetApp 業界領先的複製技術SnapMirror將本機資料複製到雲端，以便輕鬆取得可用於多種用例的輔助副本。

  Cloud Volumes ONTAP也與NetApp Backup and Recovery集成，提供備份和復原功能，以保護和長期存檔您的雲端資料。

  "了解有關備份和恢復的更多信息"

- 資料分層

  按需在高效能和低效能儲存池之間切換，無需使應用程式離線。

- 應用程式一致性

  使用NetApp SnapCenter確保NetApp Snapshot 副本的一致性。

  "了解有關SnapCenter的更多信息"

- 資料安全

  Cloud Volumes ONTAP支援資料加密並提供防毒和勒索軟體的保護。

- 隱私合規控制

  與NetApp Data Classification整合可協助您了解資料環境並識別敏感資料。

  "了解有關數據分類的更多信息"

Cloud Volumes ONTAP中包含ONTAP功能的授權。

"查看支援的Cloud Volumes ONTAP配置"

"了解有關Cloud Volumes ONTAP 的更多信息"

Cloud Volumes ONTAP部署支援的ONTAP版本

當您新增Cloud Volumes ONTAP系統時， NetApp Console可讓您從多個不同的ONTAP版本中進行選擇。

此處列出的 Cloud Volumes ONTAP 版本以外的版本無法用於新部署。此處版本中的修補程式或通用（正式發行）版本代表可用於部署的基礎版本。有關可用修補程式的詳細資訊，請參閱各版本的 "版本化發行說明"。

有關升級的資訊，請參閱 "支援的升級路徑"。

AWS

單節點

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

HA 對

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1

- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

Azure

單節點

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

HA 對

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

Google雲

單節點

- 9.18.1
- 9.17.1 P1
- 9.16.1

- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

HA 對

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

開始使用 **Amazon Web Services**

AWS 中的**Cloud Volumes ONTAP**快速入門

只需幾個步驟即可開始在 AWS 中使用Cloud Volumes ONTAP 。

1 建立控制台代理

如果你沒有 "控制台代理"但是，您需要建立一個。 "了解如何在 AWS 中建立控制台代理" 。

請注意，如果您想在沒有網路存取的子網路中部署Cloud Volumes ONTAP ，則需要手動安裝控制台代理程式並存取在該控制台代理程式上執行的NetApp Console使用者介面。 "了解如何在沒有網路存取的地方手動安裝控制台代理" 。

2 規劃您的配置

控制台提供符合您的工作負載要求的預先配置包，或者您可以建立自己的配置。如果您選擇自己的配置，您應該了解可用的選項。"了解更多" 。

3 設定網路

1. 確保您的 VPC 和子網路將支援控制台代理和Cloud Volumes ONTAP之間的連線。
2. 為NetApp AutoSupport啟用從目標 VPC 的出站網際網路存取。

   如果您在沒有網路存取的位置部署Cloud Volumes ONTAP，則不需要執行此步驟。
3. 設定到 Amazon Simple Storage Service（Amazon S3）服務的 VPC 端點。

   如果您想將冷資料從Cloud Volumes ONTAP到低成本物件存儲，則需要 VPC 端點。

"了解有關網絡要求的更多信息" 。

4 設定 **AWS KMS**

如果您想將 Amazon 加密與Cloud Volumes ONTAP結合使用，則需要確保有有效的客戶主金鑰 (CMK)。您還需要透過新增以_金鑰使用者_身分向控制台代理提供權限的 IAM 角色來修改每個 CMK 的金鑰策略。"了解更多" 。

5 使用控制台啟動**Cloud Volumes ONTAP**

按一下“新增系統”，選擇您想要部署的系統類型，然後完成精靈中的步驟。"閱讀逐步說明" 。

相關連結

- "為 AWS 建立控制台代理"
- "從 AWS Marketplace 建立控制台代理"
- "在本機安裝並設定控制台代理"
- "控制台代理的 AWS 權限"

在 **AWS** 中規劃您的**Cloud Volumes ONTAP**配置

在 AWS 中部署Cloud Volumes ONTAP時，您可以選擇符合您的工作負載需求的預先配置

系統，也可以建立自己的設定。如果您選擇自己的配置，您應該了解可用的選項。

選擇**Cloud Volumes ONTAP**許可證

Cloud Volumes ONTAP有多種授權選項。每個選項都可以讓您選擇符合您需求的消費模式。

- "了解Cloud Volumes ONTAP的授權選項"
- "了解如何設定許可"

選擇支援的區域

大多數 AWS 區域都支援Cloud Volumes ONTAP 。 "查看支援區域的完整列表" 。

必須先啟用較新的 AWS 區域，然後才能在這些區域中建立和管理資源。 "AWS 文件：了解如何啟用區域" 。

選擇受支援的本地區域

選擇本地區域是可選的。包括新加坡在內的一些 AWS 本地區域支援Cloud Volumes ONTAP 。 AWS 中的Cloud Volumes ONTAP僅支援單一可用區域中的高可用性 (HA) 模式。不支援單節點部署。

> Cloud Volumes ONTAP不支援 AWS 本地區域中的資料分層和雲端分層。此外，不支援具有未符合Cloud Volumes ONTAP資格的實例的本地區域。例如邁阿密，它不能用作本地區域，因為它只有不受支援且不合格的 Gen6 實例。

"AWS 文件：查看本地區域的完整列表" 。必須先啟用本地區域，然後才能在這些區域中建立和管理資源。

"AWS 文件：AWS 本機區域入門" 。

選擇支援的實例

Cloud Volumes ONTAP支援多種執行個體類型，具體取決於您選擇的授權類型。

"AWS 中Cloud Volumes ONTAP支援的配置"

了解儲存限制

Cloud Volumes ONTAP系統的原始容量限制與許可證相關。額外的限制會影響聚合和磁碟區的大小。在規劃配置時您應該注意這些限制。

"AWS 中Cloud Volumes ONTAP的儲存限制"

在 **AWS** 中調整系統大小

調整Cloud Volumes ONTAP系統的大小可以幫助您滿足效能和容量要求。選擇實例類型、磁碟類型和磁碟大小時，您應該注意幾個關鍵點：

實例類型

- 將您的工作負載要求與每個 EC2 執行個體類型的最大吞吐量和 IOPS 相符。
- 如果多個使用者同時向系統寫入數據，請選擇具有足夠 CPU 來管理請求的執行個體類型。

- 如果您有一個主要用於讀取的應用程序，那麼請選擇具有足夠 RAM 的系統。
  - "AWS 文件：Amazon EC2 執行個體類型"
  - "AWS 文件：Amazon EBS 優化實例"

EBS 磁碟類型

從高層次來看，EBS 磁碟類型之間的差異如下。要了解有關 EBS 磁碟用例的更多信息，請參閱 "AWS 文件：EBS 磁碟區類型"。

- 通用 *SSD (gp3)* 磁碟是成本最低的 SSD，可在廣泛的工作負載中平衡成本和效能。效能以 IOPS 和吞吐量來定義。 Cloud Cloud Volumes ONTAP 9.7 及更高版本支援 gp3 磁碟。

  當您選擇 gp3 磁碟時， NetApp Console會填入預設 IOPS 和吞吐量值，這些值會根據所選磁碟大小提供與 gp2 磁碟相當的效能。您可以增加這些值以更高的成本獲得更好的效能，但我們不支援較低的值，因為這會導致效能下降。簡而言之，堅持預設值或增加它們。不要降低它們。 "AWS 文件：了解有關 gp3 磁碟及其效能的更多信息" 。

  請注意， Cloud Volumes ONTAP支援具有 gp3 磁碟的 Amazon EBS Elastic Volumes 功能。"了解有關彈性卷支持的更多信息" 。

- 通用 *SSD (gp2)* 磁碟可在廣泛的工作負載中平衡成本和效能。性能以 IOPS 來定義。
- *Provisioned IOPS SSD (io1)* 磁碟適用於需要以較高成本獲得最高效能的關鍵應用程式。

  請注意， Cloud Volumes ONTAP支援具有 io1 磁碟的 Amazon EBS Elastic Volumes 功能。"了解有關彈性卷支持的更多信息" 。

- 吞吐量最佳化 *HDD (st1)* 磁碟適用於需要以較低價格實現快速、一致吞吐量的頻繁存取的工作負載。

> ⓘ 如果您的 Cloud Volumes ONTAP 系統位於 AWS Local Zone，則不支援將資料分層儲存到 Amazon Simple Storage Service（Amazon S3），因為在 Local Zone 之外存取 Amazon S3 儲存貯體會造成更高的延遲，並影響 Cloud Volumes ONTAP 活動。

EBS 磁碟大小

如果您選擇的配置不支援"Amazon EBS 彈性卷功能"，那麼您需要在啟動Cloud Volumes ONTAP系統時選擇初始磁碟大小。之後，您可以"讓控制台為您管理系統容量"，但如果你想"自己創建聚合"，請注意以下事項：

- 聚合中的所有磁碟必須具有相同的大小。
- EBS 磁碟的效能與磁碟大小相關。此大小決定了 SSD 磁碟的基線 IOPS 和最大突發持續時間以及 HDD 磁碟的基線和突發吞吐量。
- 最終，您應該選擇能夠提供您所需的_持續效能_的磁碟大小。
- 即使您確實選擇了更大的磁碟（例如，六個 4 TiB 磁碟），您可能無法獲得所有的 IOPS，因為 EC2 執行個體可能會達到其頻寬限制。

  有關 EBS 磁碟效能的更多詳細信息，請參閱 "AWS 文件：EBS 磁碟區類型"。

  如上所述，支援 Amazon EBS Elastic Volumes 功能的Cloud Volumes ONTAP配置不支援選擇磁碟大小。"了解有關彈性卷支持的更多信息" 。

查看預設系統磁碟

除了用戶資料的儲存之外，控制台還購買了Cloud Volumes ONTAP系統資料（啟動資料、根資料、核心資料和NVRAM）的雲端儲存。出於規劃目的，在部署Cloud Volumes ONTAP之前查看這些詳細資訊可能會有所幫助。

"查看 AWS 中Cloud Volumes ONTAP系統資料的預設磁碟" 。

控制台代理還需要係統磁碟。 "查看控制台代理預設配置的詳細信息" 。

準備在 **AWS Outpost** 中部署**Cloud Volumes ONTAP**

如果您有 AWS Outpost，則可以透過在部署過程中選擇 Outpost VPC 在該 Outpost 中部署Cloud Volumes ONTAP 。體驗與駐留在 AWS 中的任何其他 VPC 相同。請注意，您需要先在 AWS Outpost 中部署控制台代理程式。

需要指出的是，存在一些限制：

- 目前僅支援單節點Cloud Volumes ONTAP系統
- 可與Cloud Volumes ONTAP一起使用的 EC2 執行個體僅限於 Outpost 中可用的執行個體
- 目前僅支援通用 SSD（gp2）

收集網路資訊

在 AWS 中啟動Cloud Volumes ONTAP時，您需要指定有關 VPC 網路的詳細資訊。您可以使用工作表從管理員收集資訊。

單一可用區中的單一節點或 **HA** 對

AWS 資訊	你的價值
地區	
專有網絡	
子網	
安全群組（如果使用您自己的）	

多個可用區中的 **HA** 對

AWS 資訊	你的價值
地區	
專有網絡	
安全群組（如果使用您自己的）	
節點 1 可用區	
節點 1 子網	
節點 2 可用區	

AWS 資訊	你的價值
節點 2 子網	
中介可用區域	
調解器子網	
中介者的金鑰對	
叢集管理口浮動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

控制台可讓您選擇Cloud Volumes ONTAP的寫入速度設定。在選擇寫入速度之前，您應該了解正常設定和高設定之間的差異以及使用高寫入速度時的風險和建議。"了解有關寫入速度的更多信息" 。

選擇卷使用情況設定檔

ONTAP包含多種儲存效率功能，可減少您所需的總儲存量。在控制台中建立磁碟區時，您可以選擇啟用這些功能的設定檔或停用這些功能的設定檔。您應該了解有關這些功能的更多信息，以幫助您決定使用哪個配置文件。

NetApp儲存效率功能有以下優勢：

精簡配置

向主機或使用者提供比實體儲存池中實際擁有的更多的邏輯儲存。不是預先分配儲存空間，而是在寫入資料時動態地將儲存空間分配給每個磁碟區。

重複資料刪除

透過定位相同的資料塊並將其替換為對單一共享區塊的引用來提高效率。該技術透過消除駐留在同一磁碟區中的冗餘資料區塊來減少儲存容量需求。

壓縮

透過壓縮主儲存、輔助儲存和歸檔儲存磁碟區內的資料來減少儲存資料所需的實體容量。

設定網路

為Cloud Volumes ONTAP設定 AWS 網路

NetApp Console負責設定Cloud Volumes ONTAP的網路元件，例如 IP 位址、網路遮罩和路由。您需要確保可以存取外部網路、有足夠的私人 IP 位址、有正確的連線等等。

一般要求

確保您已滿足 AWS 中的以下要求。

Cloud Volumes ONTAP節點的出站互聯網訪問

Cloud Volumes ONTAP系統需要出站網際網路存取才能存取外部端點以實現各種功能。如果這些端點在具有嚴格安全要求的環境中被阻止， Cloud Volumes ONTAP將無法正常運作。

控制台代理程式會聯絡多個端點以進行日常操作。有關所用端點的信息，請參閱 "查看從控制台代理聯繫的端點" 和 "準備好使用控制台的網絡"。

Cloud Volumes ONTAP端點

Cloud Volumes ONTAP使用這些端點與各種服務進行通訊。

端點	適用於	目的	部署模式	端點不可用時的影響
\ https://netapp-cloud-account.auth0.com	驗證	用於控制台中的身份驗證。	標準和限制模式。	用戶身份驗證失敗，以下服務仍然不可用： • Cloud Volumes ONTAP服務 • ONTAP服務 • 協定和代理服務
\ https://api.bluexp.netapp.com/tenancy	租賃	用於從控制台檢索Cloud Volumes ONTAP資源以授權資源和使用者。	標準和限制模式。	Cloud Volumes ONTAP資源和使用者未獲得授權。
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	用於將AutoSupport遙測資料傳送給NetApp支援。	標準和限制模式。	AutoSupport資訊仍未送達。
AWS 服務的確切商業端點（後綴為 `amazonaws.com`）取決於您使用的 AWS 區域。請參閱 "AWS 文件了解詳細信息"。	• 雲形成 • 彈性運算雲（EC2） • 身分和存取管理(IAM) • 金鑰管理服務（KMS） • 安全性令牌服務(STS) • Amazon Simple Storage Service（S3）	與 AWS 服務通訊。	標準和私人模式。	Cloud Volumes ONTAP無法與 AWS 服務通訊以在 AWS 中執行特定操作。

端點	適用於	目的	部署模式	端點不可用時的影響
AWS 服務的特定政府端點取決於您使用的 AWS 區域。端點後綴為 `amazonaws.com` 和 `c2s.ic.gov`。參考 "AWS 開發工具包"和 "AWS 文件"了解更多。	• 雲形成 • 彈性運算雲（EC2） • 身分和存取管理 (IAM) • 金鑰管理服務（KMS） • 安全性令牌服務 (STS) • 簡單儲存服務（S3）	與 AWS 服務通訊。	限制模式。	Cloud Volumes ONTAP無法與 AWS 服務通訊以在 AWS 中執行特定操作。

HA 中介器的出站互聯網訪問

HA 中介執行個體必須具有與 AWS EC2 服務的出站連接，以便它可以協助儲存故障轉移。為了提供連接，您可以新增公用 IP 位址、指定代理伺服器或使用手動選項。

手動選項可以是 NAT 閘道或從目標子網路到 AWS EC2 服務的介面 VPC 端點。有關 VPC 終端節點的詳細信息，請參閱 "AWS 文件：介面 VPC 終端節點 (AWS PrivateLink)"。

NetApp Console代理程式的網路代理程式配置

您可以使用NetApp Console代理程式的代理伺服器設定來啟用來自Cloud Volumes ONTAP 的外部網路存取。控制台支援兩種類型的代理：

- 明確代理：來自Cloud Volumes ONTAP 的出站流量使用在控制台代理的代理配置期間指定的代理伺服器的 HTTP 位址。管理員可能還配置了使用者憑證和根 CA 憑證以進行額外的身份驗證。Cloud Volumes ONTAP 顯式代理程式有可用的根 CA 證書，請確保使用 "ONTAP CLI：安全性憑證安裝"命令。
- 透明代理：網路配置為透過控制台代理的代理程式自動路由來自Cloud Volumes ONTAP 的出站流量。設定透明代理時，管理員只需要提供用於從Cloud Volumes ONTAP進行連接的根 CA 證書，而不是代理伺服器的 HTTP 位址。確保使用以下方式取得相同的根 CA 憑證並將其上傳到您的Cloud Volumes ONTAP系統 "ONTAP CLI：安全性憑證安裝"命令。

有關配置代理伺服器的信息，請參閱 "配置控制台代理以使用代理伺服器"。

私人 **IP** 位址

控制台會自動為Cloud Volumes ONTAP指派所需數量的私人 IP 位址。您需要確保您的網路有足夠的可用私人 IP 位址。

Console 為 Cloud Volumes ONTAP 分配的 LIF 數量取決於您部署的是單節點系統還是 HA 配對。LIF 是與實體連接埠關聯的 IP 位址。

單節點系統的 **IP** 位址

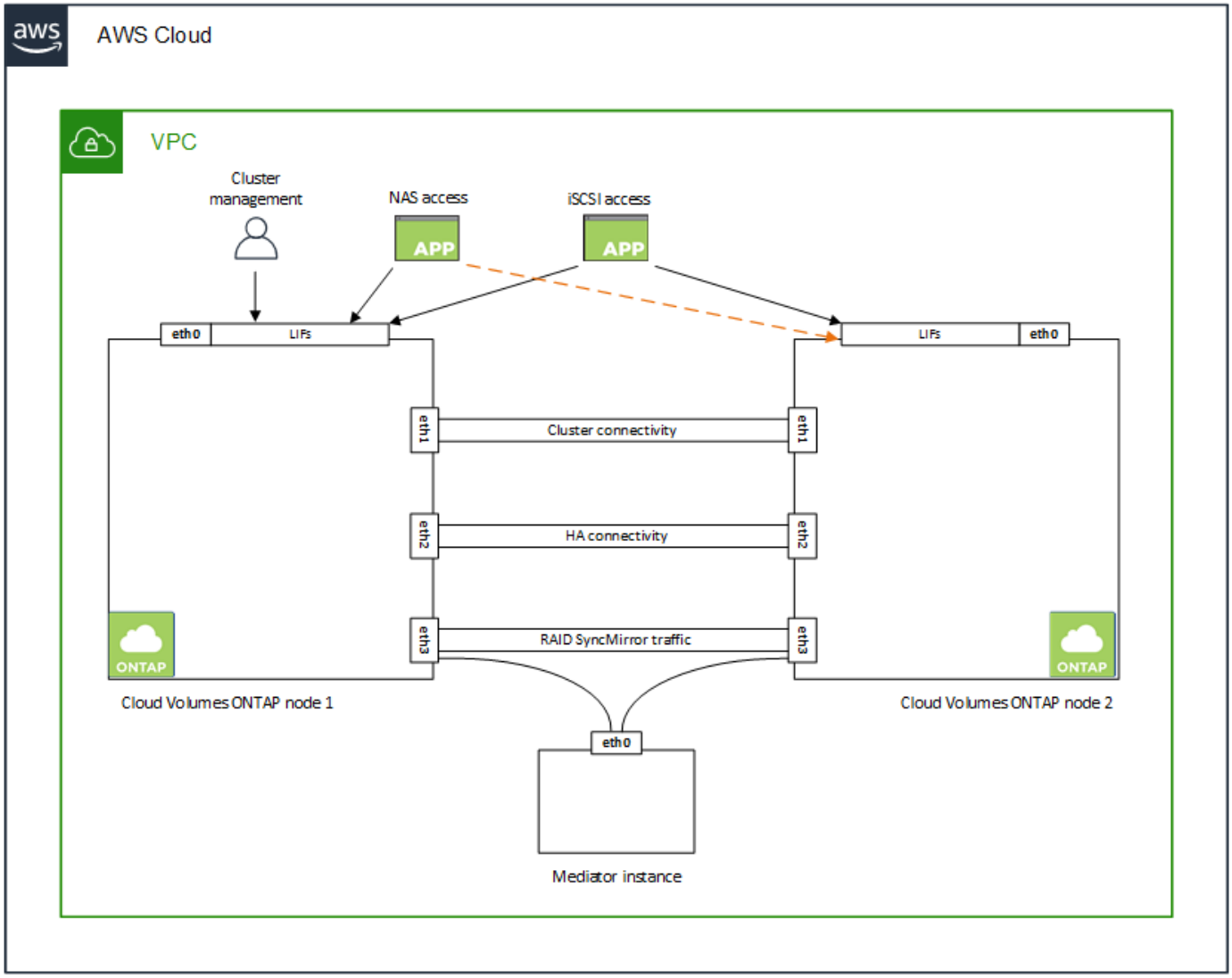
NetApp Console 為單節點系統指派 6 個 IP 位址。

下表提供了與每個私人 IP 位址關聯的 LIF 的詳細資訊。

雷射誘導螢光	目的
叢集管理	整個集群（HA 對）的行政管理。
節點管理	節點的行政管理。
集群間	跨叢集通訊、備份和複製。
NAS數據	透過 NAS 協定進行客戶端存取。
iSCSI 數據	透過 iSCSI 協定進行客戶端存取。系統也將其用於其他重要的網路工作流程。此 LIF 是必需的，不應刪除。
儲存虛擬機器管理	儲存虛擬機器管理 LIF 與S SnapCenter等管理工具一起使用。

HA 對的 **IP** 位址

HA 配對需要的 IP 位址比單節點系統多。這些 IP 位址分佈在不同的乙太網路介面上，如下圖所示：



HA 對所需的私人 IP 位址數量取決於您選擇的部署模型。在單一 AWS 可用區 (AZ) 中部署的 HA 對需要 15 個私人 IP 位址，而在多個 AZ 中部署的 HA 對需要 13 個私人 IP 位址。

下表提供了與每個私人 IP 位址關聯的 LIF 的詳細資訊。

雷射誘導螢光	介面	節點	目的
叢集管理	eth0	節點 1	整個集群（HA 對）的行政管理。
節點管理	eth0	節點 1 和節點 2	節點的行政管理。
集群間	eth0	節點 1 和節點 2	跨叢集通訊、備份和複製。
NAS數據	eth0	節點 1	透過 NAS 協定進行客戶端存取。
iSCSI 數據	eth0	節點 1 和節點 2	透過 iSCSI 協定進行客戶端存取。系統也將其用於其他重要的網路工作流程。這些 LIF 是必需的，不應刪除。
集群連接	eth1	節點 1 和節點 2	使節點能夠相互通訊並在叢集內移動資料。
HA 連接	eth2	節點 1 和節點 2	發生故障轉移時兩個節點之間的通訊。
RSM iSCSI 流量	eth3	節點 1 和節點 2	RAID SyncMirror iSCSI 流量，以及兩個Cloud Volumes ONTAP節點和中介之間的通訊。
調解員	eth0	調解員	節點和中介之間的通訊通道，用於協助儲存接管和歸還過程。

雷射誘導螢光	介面	節點	目的
節點管理	eth0	節點 1 和節點 2	節點的行政管理。
集群間	eth0	節點 1 和節點 2	跨叢集通訊、備份和複製。
iSCSI 數據	eth0	節點 1 和節點 2	透過 iSCSI 協定進行客戶端存取。這些 LIF 還管理節點之間浮動 IP 位址的遷移。這些 LIF 是必需的，不應刪除。
集群連接	eth1	節點 1 和節點 2	使節點能夠相互通訊並在叢集內移動資料。
HA 連接	eth2	節點 1 和節點 2	發生故障轉移時兩個節點之間的通訊。
RSM iSCSI 流量	eth3	節點 1 和節點 2	RAID SyncMirror iSCSI 流量，以及兩個Cloud Volumes ONTAP節點和中介之間的通訊。
調解員	eth0	調解員	節點和中介之間的通訊通道，用於協助儲存接管和歸還過程。

當部署在多個可用區時，多個 LIF 與"浮動IP位址"，這不計入 AWS 私有 IP 限制。

安全群組

您不需要建立安全性群組，因為控制台會為您完成此操作。如果您需要使用自己的，請參閱"安全群組規則"。

正在尋找有關控制台代理的資訊？ "查看控制台代理程式的安全性群組規則"

資料分層連接

如果您想要將 EBS 用作效能層，將 Amazon S3 用作容量層，則必須確保 Cloud Volumes ONTAP 與 S3 建立連線。提供此連線的最佳方法是建立指向 S3 服務的 VPC 端點。有關說明，請參閱 "AWS 文件：建立網關終端節點"。

建立 VPC 端點時，請確保選擇與Cloud Volumes ONTAP實例相對應的區域、VPC 和路由表。您還必須修改安全群組以新增允許流量到 S3 端點的出站 HTTPS 規則。否則， Cloud Volumes ONTAP無法連線到 S3 服務。

如果您遇到任何問題，請參閱 "AWS Support 知識中心：為什麼我無法使用閘道 VPC 終端節點連接到 S3 儲存桶？"

與**ONTAP**系統的連接

要在 AWS 中的Cloud Volumes ONTAP系統和其他網路中的ONTAP系統之間複製數據，您必須在 AWS VPC 和其他網路（例如您的公司網路）之間建立 VPN 連線。有關說明，請參閱 "AWS 文件：設定 AWS VPN 連接"。

CIFS 的 **DNS** 和 **Active Directory**

如果您想要設定 CIFS 存儲，則必須在 AWS 中設定 DNS 和 Active Directory，或將您的本機設定擴展到 AWS。

DNS 伺服器必須為 Active Directory 環境提供名稱解析服務。您可以設定 DHCP 選項集以使用預設 EC2 DNS 伺服器，該伺服器不能是 Active Directory 環境使用的 DNS 伺服器。

有關說明，請參閱 "AWS 文件：AWS 雲端上的 Active Directory 網域服務：快速入門參考部署"。

VPC共享

從 9.11.1 版本開始，AWS 透過 VPC 共享支援Cloud Volumes ONTAP HA 對。 VPC 共用可讓您的組織與其他 AWS 帳戶共用子網路。若要使用此配置，您必須設定您的 AWS 環境，然後使用 API 部署 HA 對。

"了解如何在共享子網路中部署 HA 對" 。

多可用區中 **HA** 對的要求

額外的 AWS 網路需求適用於使用多個可用區 (AZ) 的Cloud Volumes ONTAP HA 設定。在啟動 HA 對之前，您應該查看這些要求，因為在新增Cloud Volumes ONTAP系統時必須在控制台中輸入網路詳細資訊。

要了解 HA 對的工作原理，請參閱"高可用性對"。

可用區域

此 HA 部署模型使用多個 AZ 來確保資料的高可用性。您應該為每個Cloud Volumes ONTAP實例和中介實例使用專用 AZ，這為 HA 對之間提供了通訊通道。

每個可用區都應該有一個子網路。

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

多個可用區中的 HA 配置使用浮動 IP 位址，如果發生故障，這些位址會在節點之間遷移。它們無法從 VPC 外部本地訪問，除非您"設定 AWS 中繼網關"。

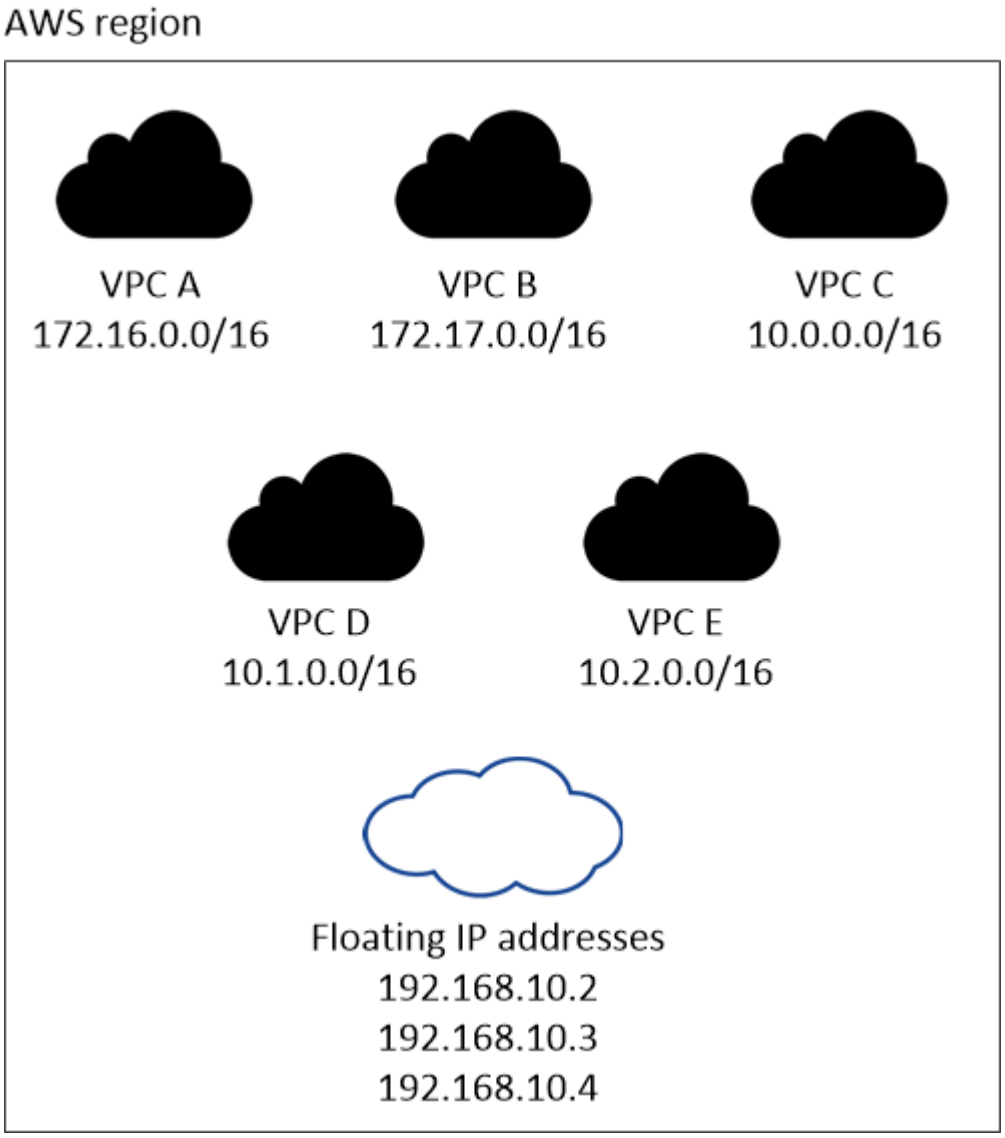
一個浮動 IP 位址用於叢集管理，一個用於節點 1 上的 NFS/CIFS 數據，一個用於節點 2 上的 NFS/CIFS 資料。用於 SVM 管理的第四個浮動 IP 位址是可選的。

如果您將SnapDrive for Windows 或SnapCenter與 HA 對一起使用，則 SVM 管理 LIF 需要浮動 IP 位址。

新增Cloud Volumes ONTAP HA 系統時，需要輸入浮動 IP 位址。控制台在啟動系統時將 IP 位址指派給 HA 對。

浮動 IP 位址必須位於您部署 HA 配置的 AWS 區域中的所有 VPC 的 CIDR 區塊之外。將浮動 IP 位址視為您所在區域的 VPC 以外的邏輯子網路。

以下範例顯示了浮動 IP 位址與 AWS 區域中的 VPC 之間的關係。雖然浮動 IP 位址位於所有 VPC 的 CIDR 區塊之外，但它們可以透過路由表路由到子網路。



控制台會自動建立靜態 IP 位址，用於 iSCSI 存取和來自 VPC 外部用戶端的 NAS 存取。您不需要滿足這些類型的 IP 位址的任何要求。

中轉網關，用於從 **VPC** 外部啟用浮動 **IP** 訪問

如果需要的話，"設定 AWS 中繼網關"允許從 HA 對所在的 VPC 外部存取 HA 對的浮動 IP 位址。

路由表

指定浮動 IP 位址後，系統會提示您選擇應包含浮動 IP 位址路由的路由表。這使得客戶端可以存取 HA 對。

如果您的 VPC 中的子網路只有一個路由表（主路由表），則控制台會自動將浮動 IP 位址新增至該路由表。如果您有多個路由表，則在啟動 HA 對時選擇正確的路由表非常重要。否則，某些用戶端可能無法存取Cloud Volumes ONTAP。

例如，您可能有兩個與不同路由表關聯的子網路。如果您選擇路由表 A，而不是路由表 B，則與路由表 A 關聯的子網路中的用戶端可以存取 HA 對，但與路由表 B 關聯的子網路中的用戶端則不能存取。

有關路由表的更多信息，請參閱 "AWS 文件：路由表"。

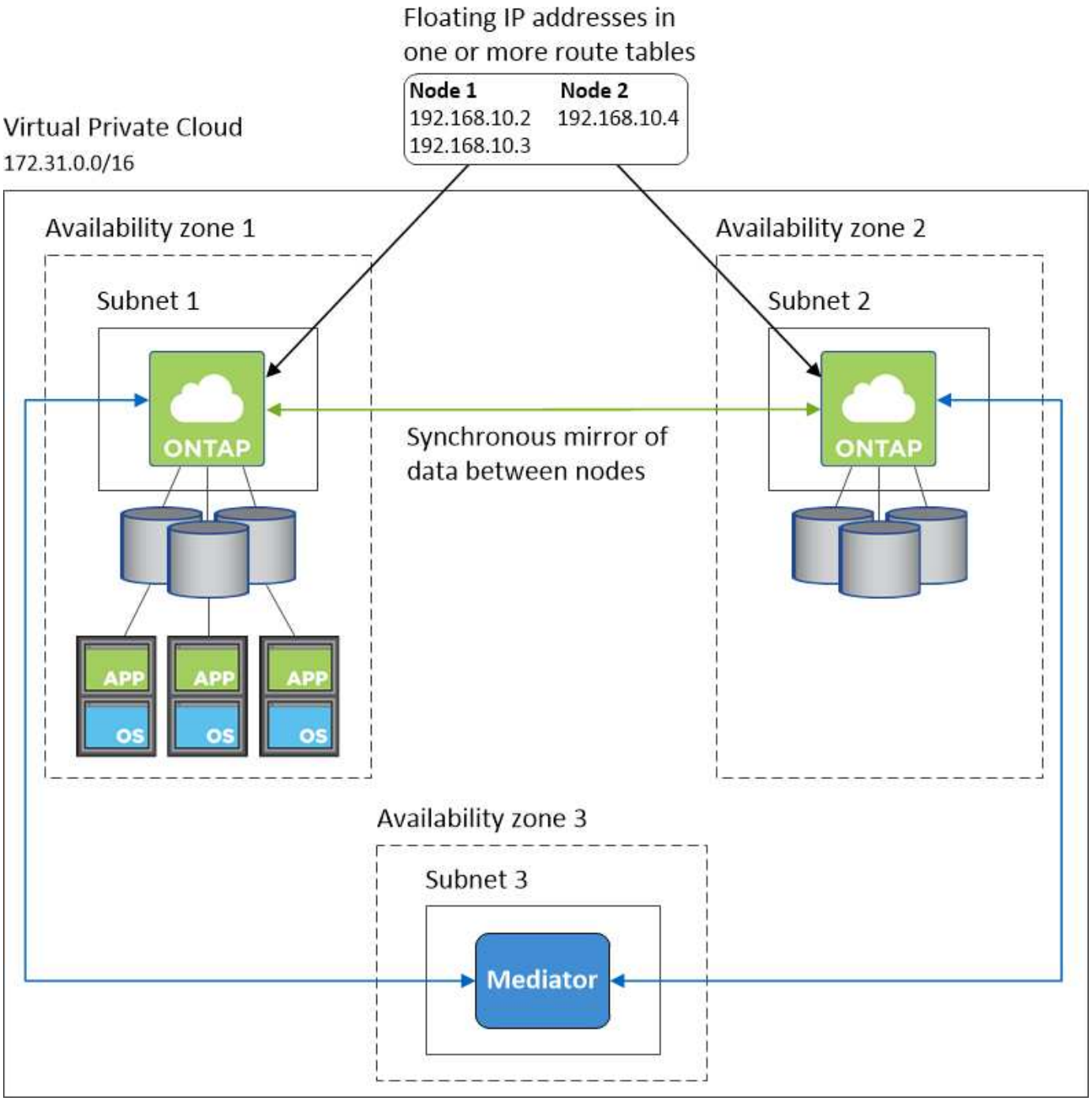
連接到**NetApp**管理工具

若要將NetApp管理工具與多個 AZ 中的 HA 設定一起使用，您有兩種連線選項：

1. 在不同的 VPC 中部署NetApp管理工具，並"設定 AWS 中繼網關"。網關允許從 VPC 外部存取叢集管理介面的浮動 IP 位址。
2. 在同一 VPC 中部署NetApp管理工具，並使用與 NAS 用戶端類似的路由配置。

HA 設定範例

下圖說明了多個可用區中的 HA 對特有的網路元件：三個可用區、三個子網路、浮動 IP 位址和一個路由表。



控制台代理的要求

如果您尚未建立控制台代理，則應查看網路需求。

- "查看控制台代理程式的網路要求"
- "AWS 中的安全群組規則"

相關主題

- "驗證Cloud Volumes ONTAP 的AutoSupport設置"
- "了解ONTAP內部端口" 。

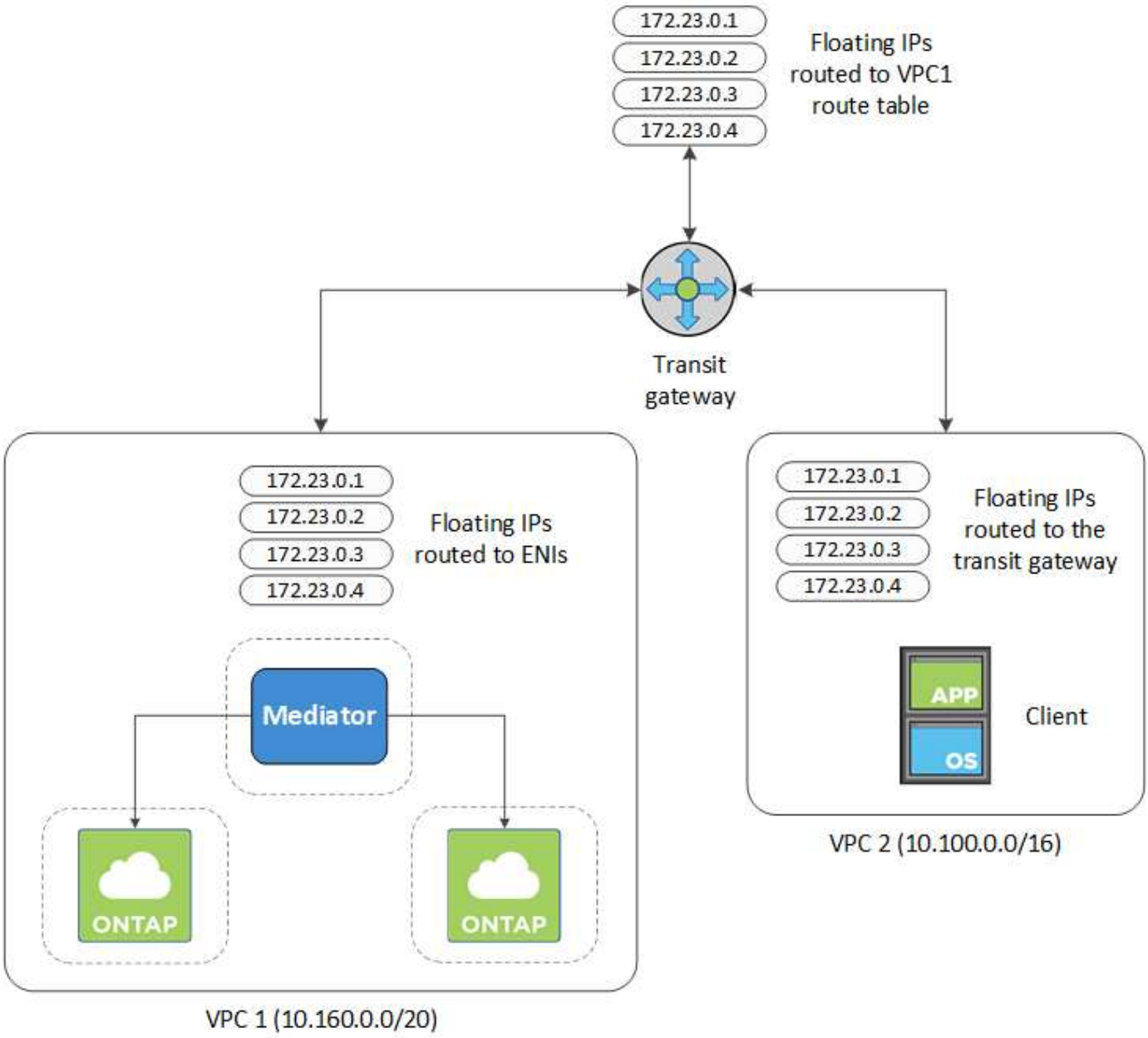
設定 AWS 中轉網關以允許存取 HA 對的"浮動IP位址"來自 HA 對所在的 VPC 外部。

當Cloud Volumes ONTAP HA 設定分佈在多個 AWS 可用區時，需要浮動 IP 位址才能從 VPC 內部存取 NAS 資料。當發生故障時，這些浮動 IP 位址可以在節點之間遷移，但它們無法從 VPC 外部進行本機存取。單獨的私人 IP 位址提供從 VPC 外部的資料訪問，但它們不提供自動故障轉移。

叢集管理介面和可選的 SVM 管理 LIF 也需要浮動 IP 位址。

如果您設定了 AWS 傳輸網關，則可以從 HA 對所在的 VPC 外部存取浮動 IP 位址。這意味著 VPC 以外的 NAS 用戶端和NetApp管理工具可以存取浮動 IP。

下面是一個顯示透過中轉網關連接的兩個 VPC 的範例。 HA 系統位於一個 VPC 中，而客戶端位於另一個 VPC 中。然後，您可以使用浮動 IP 位址在用戶端上安裝 NAS 磁碟區。

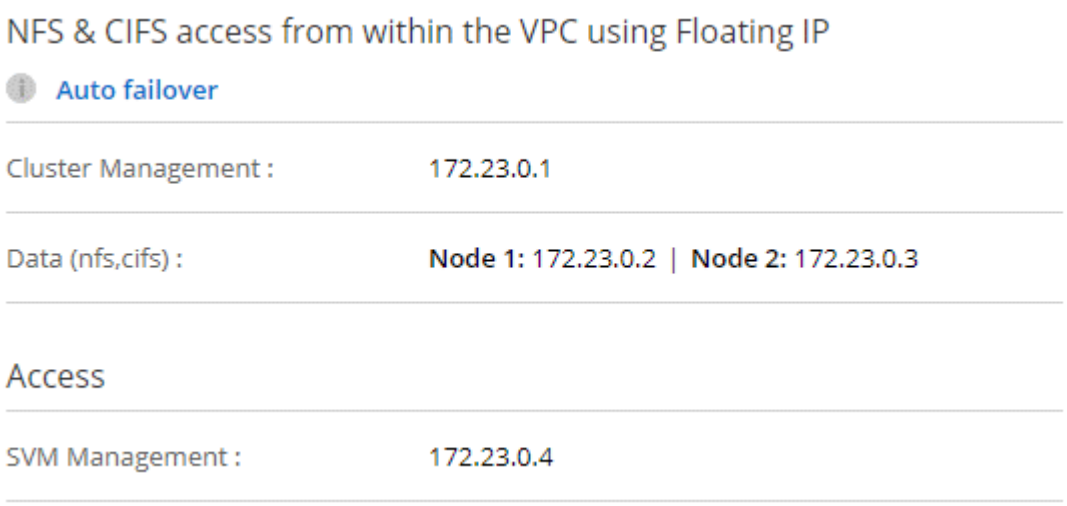


以下步驟說明如何設定類似的配置。

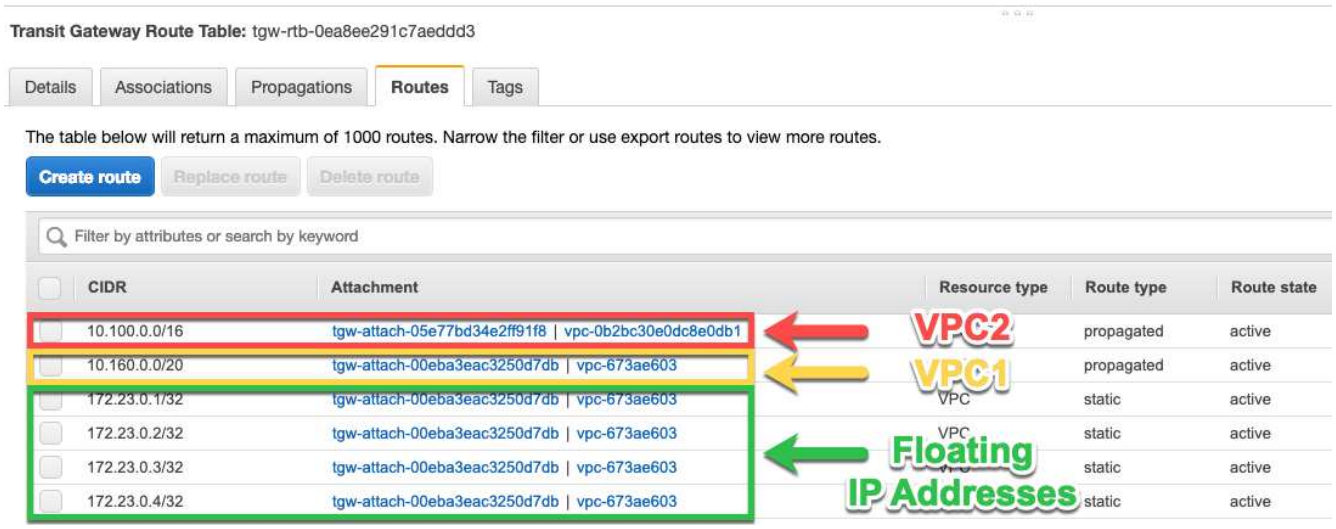
步驟

1. "建立中轉網關並將 VPC 附加到該網關" 。
2. 將 VPC 與傳輸網關路由表關聯。
   a. 在 **VPC** 服務中，按一下 **Transit Gateway Route Tables**。
   b. 選擇路由表。
   c. 按一下*關聯*，然後選擇*建立關聯*。
   d. 選擇要關聯的附件（VPC），然後按一下*建立關聯*。
3. 透過指定 HA 對的浮動 IP 位址在傳輸網關的路由表中建立路由。

   您可以在NetApp Console的系統資訊頁面上找到浮動 IP 位址。以下是一個例子：



   以下範例圖顯示了中轉網關的路由表。它包括到兩個 VPC 的 CIDR 區塊的路由和Cloud Volumes ONTAP使用的四個浮動 IP 位址。

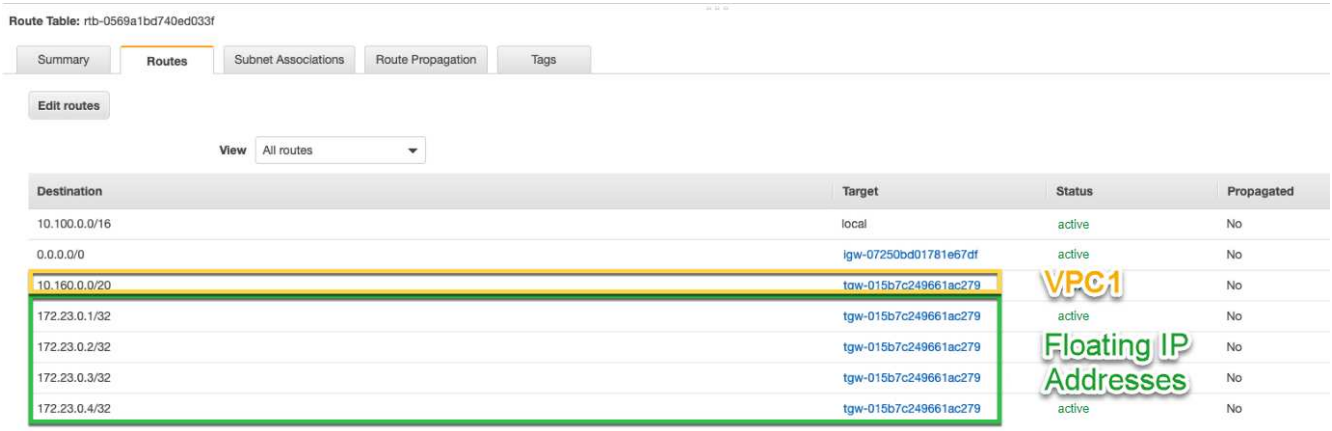


4. 修改需要存取浮動IP位址的VPC的路由表。

a. 為浮動IP位址新增路由條目。

b. 將路由條目新增至 HA 對所在 VPC 的 CIDR 區塊。

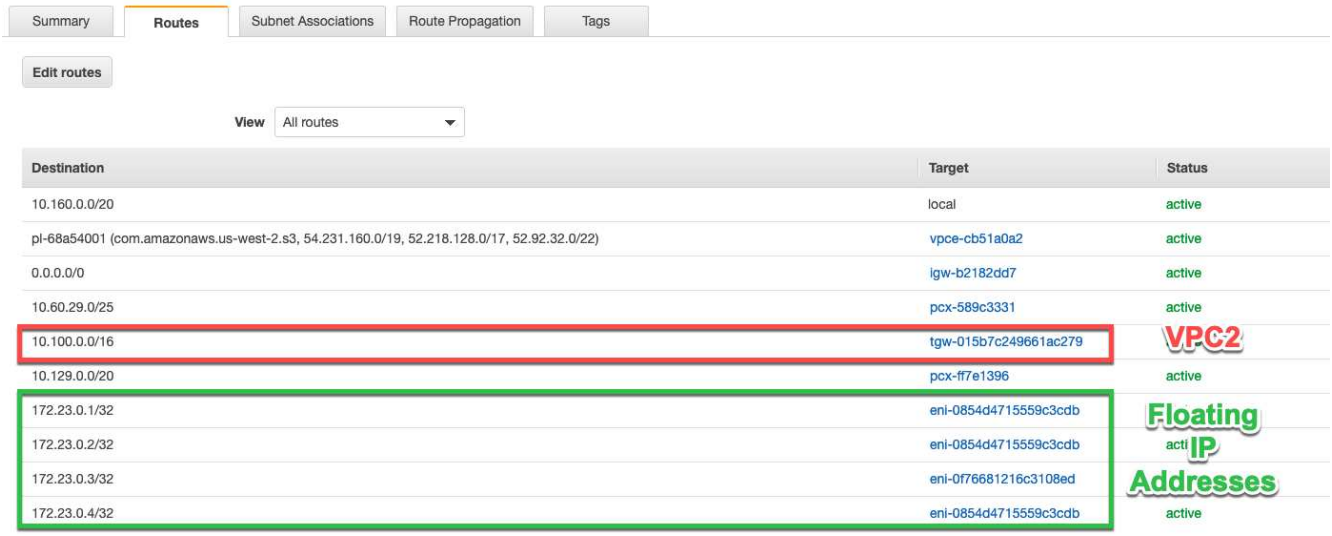
下面的範例圖顯示了 VPC 2 的路由表，其中包含到 VPC 1 的路由和浮動 IP 位址。



5. 透過在需要存取浮動 IP 位址的 VPC 中新增路由來修改 HA 對的 VPC 的路由表。

這一步很重要，因為它完成了 VPC 之間的路由。

以下範例影像顯示了 VPC 1 的路由表。它包括到浮動 IP 位址和客戶端所在的 VPC 2 的路由。控制台在部署 HA 對時會自動將浮動 IP 新增至路由表。



6. 將安全性群組設定更新為 VPC 的所有流量。

a. 在虛擬私有雲下，點選*子網路*。

b. 按一下「路由表」選項卡，為 HA 對的其中一個浮動 IP 位址選擇所需的環境。

c. 按一下“安全性群組”。

d. 選擇*編輯入站規則*。

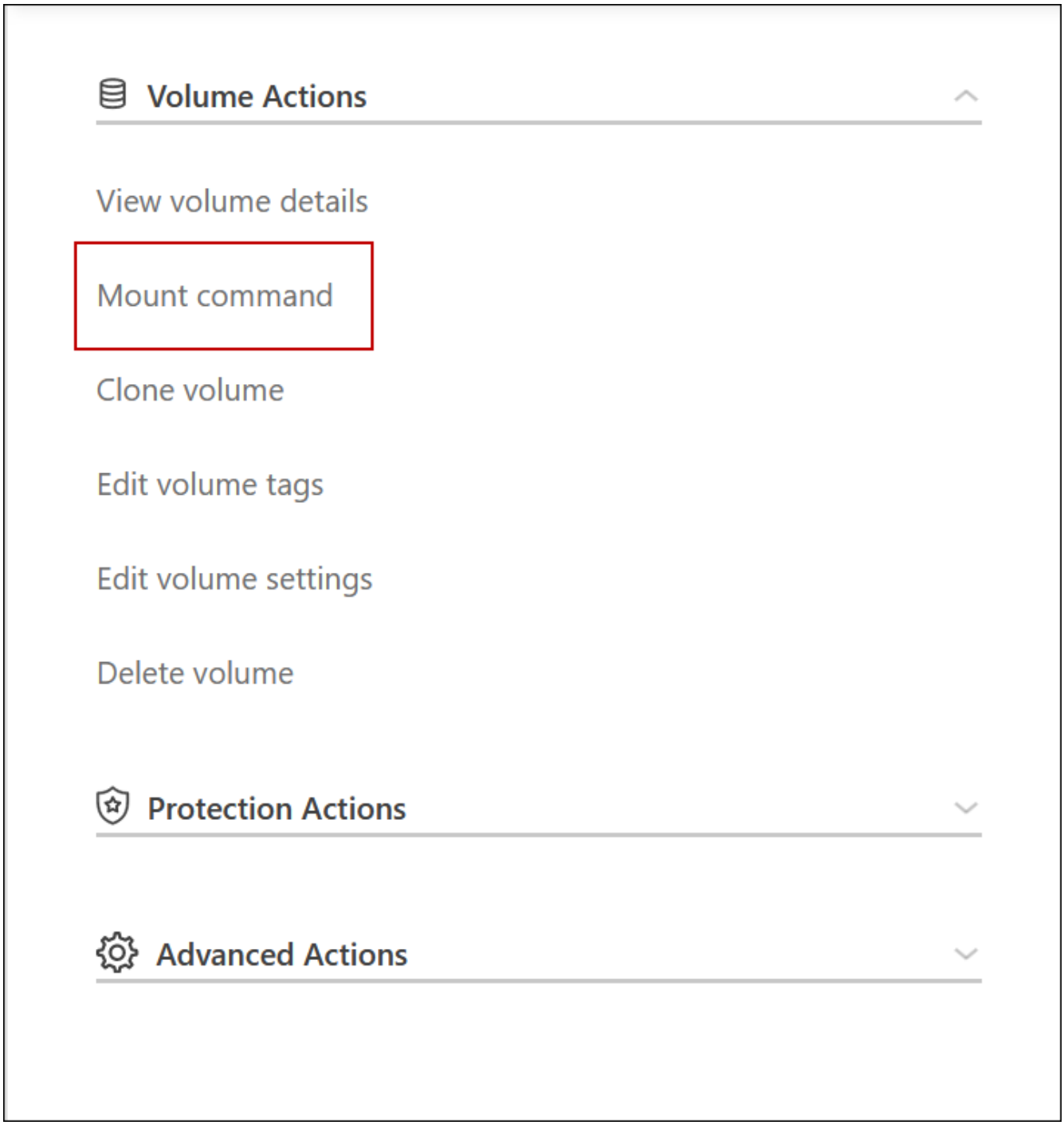
e. 按一下“新增規則”。

f. 在類型下，選擇*所有流量*，然後選擇 VPC IP 位址。

g. 按一下“儲存規則”以套用變更。

7. 使用浮動 IP 位址將磁碟區掛載到客戶端。

   您可以透過控制台中「管理磁碟區」面板下的「**Mount Command**」選項在控制台中找到正確的 IP 位址。



8. 如果您正在掛載 NFS 卷，請設定匯出策略以符合用戶端 VPC 的子網路。

   "了解如何編輯卷" 。

相關連結

- "AWS 中的高可用性對"
- "AWS 中Cloud Volumes ONTAP的網路需求"

在 **AWS** 共用子網路中部署**Cloud Volumes ONTAP HA** 對

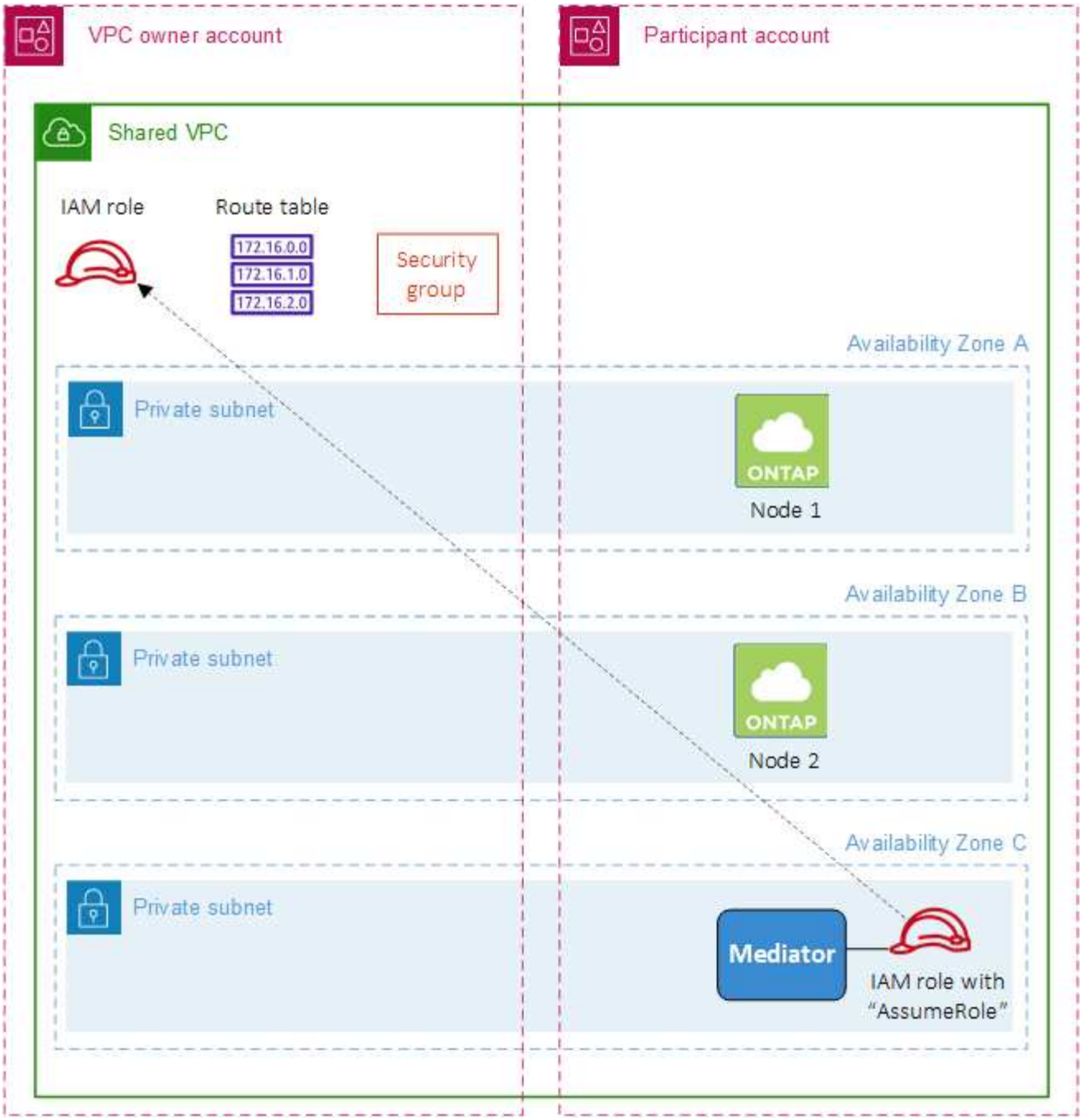
從 9.11.1 版本開始，AWS 透過 VPC 共享支援Cloud Volumes ONTAP HA 對。 VPC 共用可讓您的組織與其他 AWS 帳戶共用子網路。若要使用此配置，您必須設定您的 AWS 環境，然後使用 API 部署 HA 對。

和 "VPC共享"， Cloud Volumes ONTAP HA 配置分佈在兩個帳戶中：

- VPC 擁有者帳戶，擁有網路（VPC、子網路、路由表和Cloud Volumes ONTAP安全群組）
- 參與者帳戶，其中 EC2 執行個體部署在共用子網路中（這包括兩個 HA 節點和中介者）

對於跨多個可用區部署的Cloud Volumes ONTAP HA 配置，HA 中介需要特定權限才能寫入 VPC 擁有者帳戶中的路由表。您需要透過設定調解員可以承擔的 IAM 角色來提供這些權限。

下圖顯示了此部署所涉及的元件：



請依照下列步驟所述，您需要與參與者帳戶共用子網，然後在 VPC 擁有者帳戶中建立 IAM 角色和安全性群組。

當您建立Cloud Volumes ONTAP系統時， NetApp Console會自動建立 IAM 角色並將其附加到中介器。此角色承擔您在 VPC 擁有者帳戶中建立的 IAM 角色，以便對與 HA 對關聯的路由表進行變更。

步驟

1. 與參與者帳戶共用 VPC 所有者帳戶中的子網路。

   此步驟是在共用子網路中部署 HA 對所必需的。

   "AWS 文件：共享子網"

2. 在 VPC 擁有者帳戶中，為Cloud Volumes ONTAP建立一個安全群組。

"請參閱Cloud Volumes ONTAP的安全群組規則" 。請注意，您不需要為 HA 中介建立安全群組。控制台會為您完成該操作。

3. 在 VPC 擁有者帳戶中，建立一個包含下列權限的 IAM 角色：

```
Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
```

4. 使用 API 建立新的Cloud Volumes ONTAP系統。

   請注意，您必須指定以下欄位：

   - “安全群組 ID”

     「securityGroupId」欄位應指定您在 VPC 所有者帳戶中建立的安全性群組（請參閱上面的步驟 2）。

   - “haParams”物件中的“assumeRoleArn”

     「assumeRoleArn」欄位應包含您在 VPC 擁有者帳戶中建立的 IAM 角色的 ARN（請參閱上面的步驟 3）。

     例如：

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

+
"了解Cloud Volumes ONTAP API"

在 **AWS** 單可用區中為**Cloud Volumes ONTAP HA** 對配置放置組建立

如果放置組建立失敗，AWS 單可用區 (AZ) 中的Cloud Volumes ONTAP高可用性 (HA) 部署可能會失敗並回溯。如果Cloud Volumes ONTAP節點和中介實例不可用，則放置群組的建立也會失敗，部署會回滾。為了避免這種情況，您可以修改配置，以便即使放置組建立失敗也能完成部署。

繞過回滾程序後， Cloud Volumes ONTAP部署程序已成功完成，並通知您放置群組建立未完成。

步驟

1. 使用 SSH 連線到NetApp Console代理主機並登入。
2. 導航至 `/opt/application/netapp/cloudmanager/docker_occm/data`。
3. 編輯 `app.conf`透過改變 `rollback-on-placement-group-failure`參數 `false`。此參數的預設值是 `true`。

```
{
    "occm" : {
        "aws" : {
            "rollback-on-placement-group-failure" : false
        }
    }
}
```

4. 儲存檔案並登出控制台代理程式。您不需要重新啟動控制台代理。

Cloud Volumes ONTAP的 **AWS** 安全群組入站和出站規則

NetApp Console建立 AWS 安全性群組，其中包含Cloud Volumes ONTAP成功運作所需的入站和出站規則。您可能希望參考連接埠以進行測試，或者您喜歡使用自己的安全群組。

Cloud Volumes ONTAP規則

Cloud Volumes ONTAP的安全群組需要入站和出站規則。

入站規則

新增Cloud Volumes ONTAP系統並選擇預先定義安全性群組時，您可以選擇允許下列其中的流量：

- 僅限選定的 **VPC**：入站流量的來源是Cloud Volumes ONTAP系統的 VPC 子網路範圍和控制台代理程式所在的 VPC 子網路範圍。這是推薦的選項。
- 所有 **VPC**：入站流量的來源是 0.0.0.0/0 IP 範圍。

協定	港口	目的
所有 ICMP	全部	對執行個體執行 ping 操作
HTTP	80	使用叢集管理 LIF 的 IP 位址透過 HTTP 存取ONTAP System Manager Web 控制台
HTTPS	443	使用叢集管理 LIF 的 IP 位址與控制台代理程式建立連線並透過 HTTPS 存取ONTAP System Manager Web 控制台
SSH	22	透過 SSH 存取叢集管理 LIF 或節點管理 LIF 的 IP 位址
TCP	111	NFS 的遠端過程調用
TCP	139	CIFS 的 NetBIOS 服務會話
TCP	161-162	簡單網路管理協議

協定	港口	目的
TCP	445	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
TCP	635	NFS 掛載
TCP	749	Kerberos
TCP	2049	NFS 伺服器守護程式
TCP	3260	透過 iSCSI 資料 LIF 進行 iSCSI 訪問
TCP	4045	NFS 鎖守護程式
TCP	4046	NFS 網路狀態監視器
TCP	10000	使用 NDMP 備份
TCP	11104	SnapMirror群集間通訊會話的管理
TCP	11105	使用集群間 LIF 進行SnapMirror資料傳輸
UDP	111	NFS 的遠端過程調用
UDP	161-162	簡單網路管理協議
UDP	635	NFS 掛載
UDP	2049	NFS 伺服器守護程式
UDP	4045	NFS 鎖守護程式
UDP	4046	NFS 網路狀態監視器
UDP	4049	NFS rquotad 協議

出站規則

Cloud Volumes ONTAP的預設安全群組開啟所有出站流量。如果可以接受，請遵循基本的出站規則。如果您需要更嚴格的規則，請使用進階出站規則。

基本出站規則

Cloud Volumes ONTAP的預設安全群組包括以下出站規則。

協定	港口	目的
所有 ICMP	全部	所有出站流量
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高級出站規則

如果您需要對出站流量製定嚴格的規則，則可以使用下列資訊僅開啟Cloud Volumes ONTAP出站通訊所需的連接埠。

來源是Cloud Volumes ONTAP系統上的介面（IP 位址）。

服務	協定	港口	來源	目的地	目的
活動目錄	TCP	88	節點管理 LIF	Active Directory 林	Kerberos V 驗證
	UDP	137	節點管理 LIF	Active Directory 林	NetBIOS 名稱服務
	UDP	138	節點管理 LIF	Active Directory 林	NetBIOS 資料封包服務
	TCP	139	節點管理 LIF	Active Directory 林	NetBIOS 服務會話
	TCP 和 UDP	389	節點管理 LIF	Active Directory 林	LDAP
	TCP	445	節點管理 LIF	Active Directory 林	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
	TCP	464	節點管理 LIF	Active Directory 林	Kerberos V 更改和設定密碼（SET_CHANGE）
	UDP	464	節點管理 LIF	Active Directory 林	Kerberos 金鑰管理
	TCP	749	節點管理 LIF	Active Directory 林	Kerberos V 更改和設定密碼（RPCSEC_GSS）
	TCP	88	資料 LIF（NFS、CIFS、iSCSI）	Active Directory 林	Kerberos V 驗證
	UDP	137	資料 LIF（NFS、CIFS）	Active Directory 林	NetBIOS 名稱服務
	UDP	138	資料 LIF（NFS、CIFS）	Active Directory 林	NetBIOS 資料封包服務
	TCP	139	資料 LIF（NFS、CIFS）	Active Directory 林	NetBIOS 服務會話
	TCP 和 UDP	389	資料 LIF（NFS、CIFS）	Active Directory 林	LDAP
	TCP	445	資料 LIF（NFS、CIFS）	Active Directory 林	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
	TCP	464	資料 LIF（NFS、CIFS）	Active Directory 林	Kerberos V 更改和設定密碼（SET_CHANGE）
	UDP	464	資料 LIF（NFS、CIFS）	Active Directory 林	Kerberos 金鑰管理
	TCP	749	資料 LIF（NFS、CIFS）	Active Directory 林	Kerberos V 更改和設定密碼（RPCSEC_GSS）
AutoSupport	HTTPS	443	節點管理 LIF	mysupport.netapp.com	AutoSupport （預設為 HTTPS）
	HTTP	80	節點管理 LIF	mysupport.netapp.com	AutoSupport （僅當傳輸協定從 HTTPS 變更為 HTTP 時）
	TCP	3128	節點管理 LIF	控制台代理	如果出站網路連線不可用，則透過控制台代理上的代理伺服器傳送AutoSupport訊息

服務	協定	港口	來源	目的地	目的
備份到S3	TCP	5010	集群間 LIF	備份端點或還原端點	備份到 S3 功能的備份和還原作業
簇	所有流量	所有流量	一個節點上的所有 LIF	另一個節點上的所有 LIF	群集間通訊（僅限Cloud Volumes ONTAP HA）
	TCP	3000	節點管理 LIF	HA介導者	ZAPI 呼叫（僅限Cloud Volumes ONTAP HA）
	ICMP	1	節點管理 LIF	HA介導者	保持活動狀態（僅限Cloud Volumes ONTAP HA）
配置備份	HTTP	80	節點管理 LIF	http://<控制台代理 IP 位址>/occm/offboxconfig	將配置備份傳送到控制台代理程式。"ONTAP文檔"
DHCP	UDP	68	節點管理 LIF	DHCP	DHCP 用戶端首次設定
DHCP服務	UDP	67	節點管理 LIF	DHCP	DHCP 伺服器
DNS	UDP	53	節點管理 LIF 和資料 LIF（NFS、CIFS）	DNS	DNS
NDMP	TCP	18600–18699	節點管理 LIF	目標伺服器	NDMP 拷貝
SMTP	TCP	25	節點管理 LIF	郵件伺服器	SMTP 警報，可用於AutoSupport
SNMP	TCP	161	節點管理 LIF	監控伺服器	透過 SNMP 陷阱進行監控
	UDP	161	節點管理 LIF	監控伺服器	透過 SNMP 陷阱進行監控
	TCP	162	節點管理 LIF	監控伺服器	透過 SNMP 陷阱進行監控
	UDP	162	節點管理 LIF	監控伺服器	透過 SNMP 陷阱進行監控
SnapMirror	TCP	11104	集群間 LIF	ONTAP叢集間 LIF	SnapMirror群集間通訊會話的管理
	TCP	11105	集群間 LIF	ONTAP叢集間 LIF	SnapMirror資料傳輸
系統日誌	UDP	514	節點管理 LIF	Syslog伺服器	Syslog 轉送訊息

HA 調解器外部安全群組的規則

Cloud Volumes ONTAP HA 中介的預先定義外部安全群組包括以下入站和出站規則。

入站規則

HA 中介的預定義安全群組包括以下入站規則。

協定	港口	來源	目的
TCP	3000	控制台代理的 CIDR	透過控制台代理存取 RESTful API

出站規則

HA 中介的預定義安全群組開啟所有出站流量。如果可以接受，請遵循基本的出站規則。如果您需要更嚴格的規則，請使用進階出站規則。

基本出站規則

HA 中介的預定義安全群組包括以下出站規則。

協定	港口	目的
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高級出站規則

如果您需要對出站流量製定嚴格的規則，則可以使用以下資訊僅開啟 HA 中介器出站通訊所需的連接埠。

協定	港口	目的地	目的
HTTP	80	AWS EC2 執行個體上的控制台代理程式的 IP 位址	下載中介器的升級版本
HTTPS	443	ec2.amazonaws.com	協助儲存故障轉移
UDP	53	ec2.amazonaws.com	協助儲存故障轉移

您可以建立從目標子網路到 AWS EC2 服務的介面 VPC 端點，而不是開啟連接埠 443 和 53。

HA 設定內部安全群組的規則

Cloud Volumes ONTAP HA 設定的預先定義內部安全性群組包括以下規則。此安全群組支援 HA 節點之間以及中介器和節點之間的通訊。

控制台始終建立此安全性群組。您沒有選擇使用自己的。

入站規則

預定義安全性群組包括以下入站規則。

協定	港口	目的
所有流量	全部	HA 中介器與 HA 節點之間的通信

出站規則

預定義安全性群組包括以下出站規則。

協定	港口	目的
所有流量	全部	HA 中介器與 HA 節點之間的通信

"查看控制台代理程式的安全性群組規則"

設定Cloud Volumes ONTAP以在 AWS 中使用客戶管理的金鑰

如果您想要將 Amazon 加密與Cloud Volumes ONTAP一起使用，則需要設定 AWS 金鑰管理服務 (KMS)。

步驟

1. 確保存在有效的客戶主金鑰 (CMK)。

   CMK 可以是 AWS 管理的 CMK 或客戶管理的 CMK。它可以與NetApp Console和Cloud Volumes ONTAP位於同一個 AWS 帳戶中，也可以位於不同的 AWS 帳戶中。

   "AWS 文件：客戶主金鑰 (CMK)"

2. 透過新增以_金鑰使用者_身分向控制台提供權限的 IAM 角色來修改每個 CMK 的金鑰策略。

   將身分識別和存取管理 (IAM) 角色新增為關鍵用戶，可授予控制台使用 CMK 與Cloud Volumes ONTAP 的權限。

   "AWS 文件：編輯金鑰"

3. 如果 CMK 位於不同的 AWS 帳戶中，請完成下列步驟：

   a. 從 CMK 所在的帳戶進入 KMS 控制台。

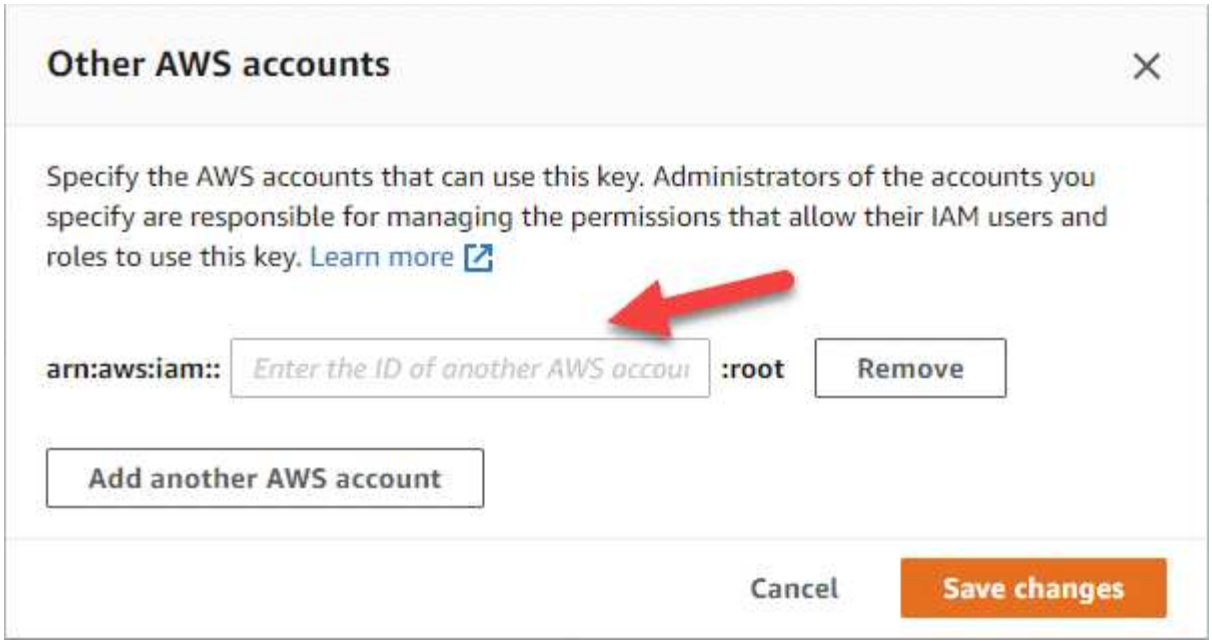
   b. 選擇鍵。

   c. 在「常規配置」窗格中，複製金鑰的 ARN。

      建立Cloud Volumes ONTAP系統時，您需要向控制台提供 ARN。

   d. 在 其他 **AWS** 帳戶 窗格中，新增為控制台提供權限的 AWS 帳戶。

      通常，這是部署控制台的帳戶。如果 AWS 中未安裝控制台，請使用您向控制台提供 AWS 存取金鑰的帳戶。



e. 現在切換到為控制台提供權限的 AWS 帳戶並開啟 IAM 控制台。

f. 建立包含下面列出的權限的 IAM 策略。

g. 將政策附加到向控制台提供權限的 IAM 角色或 IAM 使用者。

以下政策提供控制台使用來自外部 AWS 帳戶的 CMK 所需的權限。請務必修改「資源」部分中的區域和帳戶 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
                }
            }
        }
    ]
}
```

+
有關此過程的更多詳細信息，請參閱 "AWS 文件：允許其他帳戶中的使用者使用 KMS 金鑰"。

4. 如果您使用的是客戶管理的 CMK，請透過將Cloud Volumes ONTAP IAM 角色新增為_密鑰使用者_來修改 CMK 的密鑰原則。

   如果您在 Cloud Volumes ONTAP 上啟用了資料分層，並且想要加密儲存在 Amazon Simple Storage

Service（Amazon S3）儲存貯體中的資料，則需要執行此步驟。

您需要在部署Cloud Volumes ONTAP之後執行此步驟，因為 IAM 角色是在建立Cloud Volumes ONTAP系統時建立的。 （當然，您可以選擇使用現有的Cloud Volumes ONTAP IAM 角色，因此可以先執行此步驟。）

"AWS 文件：編輯金鑰"

為Cloud Volumes ONTAP節點設定 AWS IAM 角色

必須將具有所需權限的 AWS 身分和存取管理 (IAM) 角色附加到每個Cloud Volumes ONTAP節點。對於 HA 調解員也是如此。最簡單的方法是讓NetApp Console為您建立 IAM 角色，但您也可以使用自己的角色。

此任務是可選的。建立Cloud Volumes ONTAP系統時，預設選項是讓控制台為您建立 IAM 角色。如果您企業的安全政策要求您自行建立 IAM 角色，請依照下列步驟操作。

AWS Secret Cloud 需要提供您自己的 IAM 角色。"了解如何在 C2S 中部署Cloud Volumes ONTAP" 。

步驟

1. 前往 AWS IAM 主控台。
2. 建立包含下列權限的 IAM 原則：
    - Cloud Volumes ONTAP節點的基本策略

標準區域

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud（美國）區域

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-us-gov:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

絕密地區

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

秘密區域

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

- Cloud Volumes ONTAP節點的備份策略

  如果您打算將NetApp Backup and Recovery與Cloud Volumes ONTAP系統一起使用，則節點的 IAM 角色必須包含下方顯示的第二個原則。

標準區域

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud（美國）區域

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

絕密地區

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

秘密區域

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- HA介導者

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses",
                "sts:AssumeRole",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

3. 建立一個 IAM 角色並將您建立的策略附加到該角色。

結果

現在，您擁有可以在建立新的Cloud Volumes ONTAP系統時選擇的 IAM 角色。

更多資訊

- "AWS 文件：建立 IAM 原則"
- "AWS 文件：建立 IAM 角色"

在 AWS 中設定Cloud Volumes ONTAP許可

在您決定要與Cloud Volumes ONTAP一起使用哪種授權選項後，需要執行幾個步驟才能在建立新系統時選擇該授權選項。

免費增值

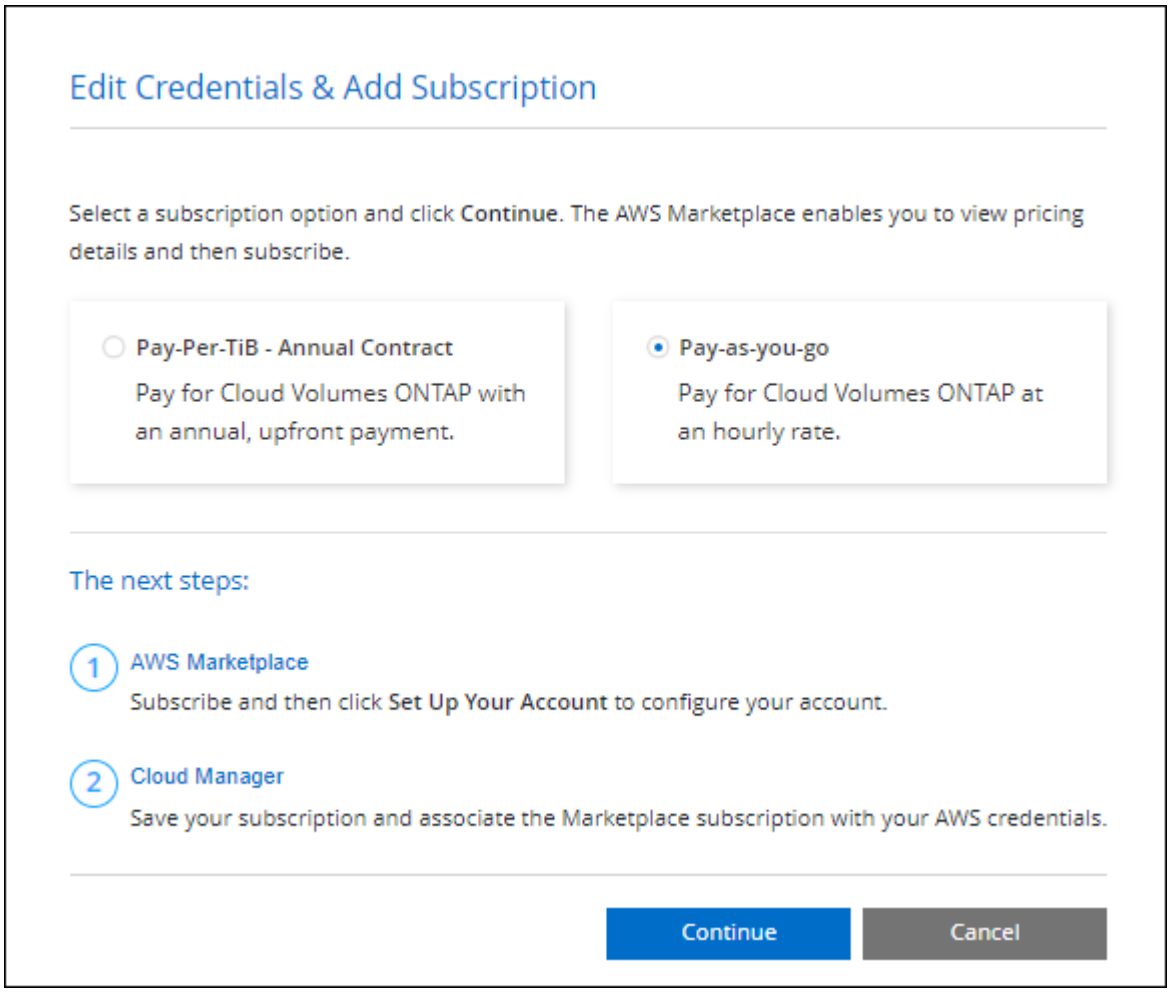
選擇免費加值服務，免費使用Cloud Volumes ONTAP，最高可提供 500 GiB 的設定容量。"了解有關免費增值服務的更多信息" 。

步驟

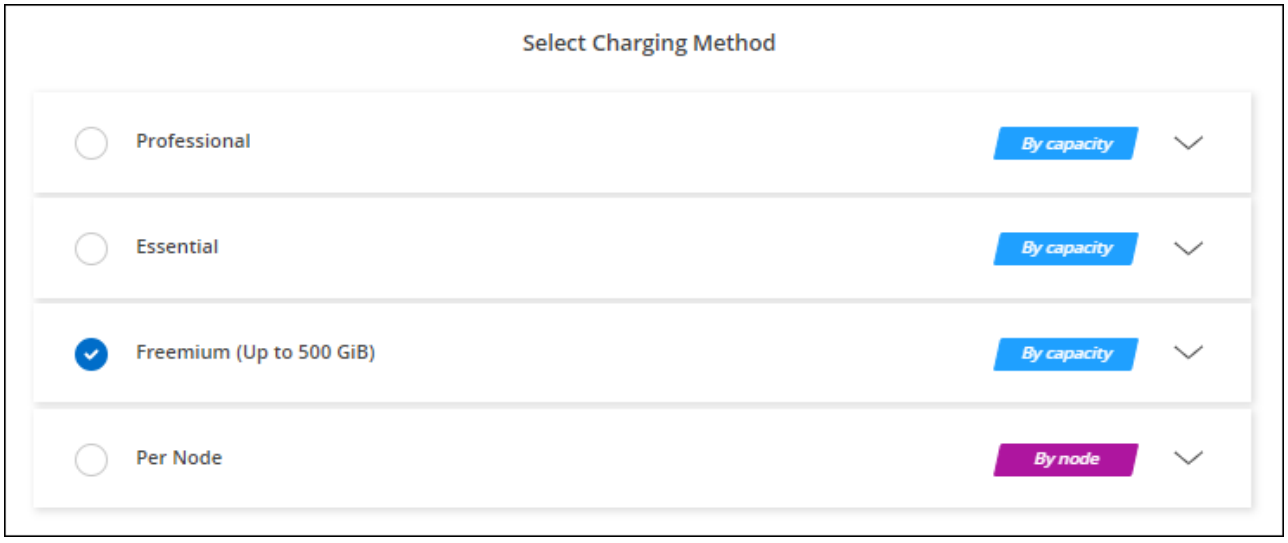
1. 從NetApp Console的左側導覽功能表中，選擇「儲存」>「管理」 。
2. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。
    a. 在“詳細資料和憑證”頁面上，按一下“編輯憑證”>“新增訂閱”，然後依照指示訂閱 AWS Marketplace 中的

即用即付服務。

除非您超過 500 GiB 的預配置容量，否則您無需透過市場訂閱付費，此時系統將自動轉換為"基本套餐"。



a. 返回控制台後，到達收費方式頁面時選擇「免費增值」。



"查看在 AWS 中啟動Cloud Volumes ONTAP 的逐步說明"。

基於容量的許可證

基於容量的許可使您能夠按 TiB 容量支付Cloud Volumes ONTAP費用。基於容量的許可以_包_的形式提供：Essentials 包或 Professional 包。

Essentials 和 Professional 套餐提供以下幾種消費模式或購買選項：

- 從NetApp購買的授權（自帶授權 (BYOL)）
- AWS Marketplace 的按小時付費 (PAYGO) 訂閱
- 來自 AWS Marketplace 的年度合約

"了解有關基於容量的許可的更多信息" 。

以下部分介紹如何開始使用每種消費模型。

BYOL

透過從NetApp購買授權 (BYOL) 進行預付款，以便在任何雲端供應商部署Cloud Volumes ONTAP系統。

已限制 BYOL 授權的購買、延期和續約。有關更多信息，請參閱 "Cloud Volumes ONTAP的 BYOL 授權可用性受限" 。

步驟

1. "聯絡NetApp銷售人員以取得許可證"
2. "將您的NetApp支援網站帳戶新增至控制台"

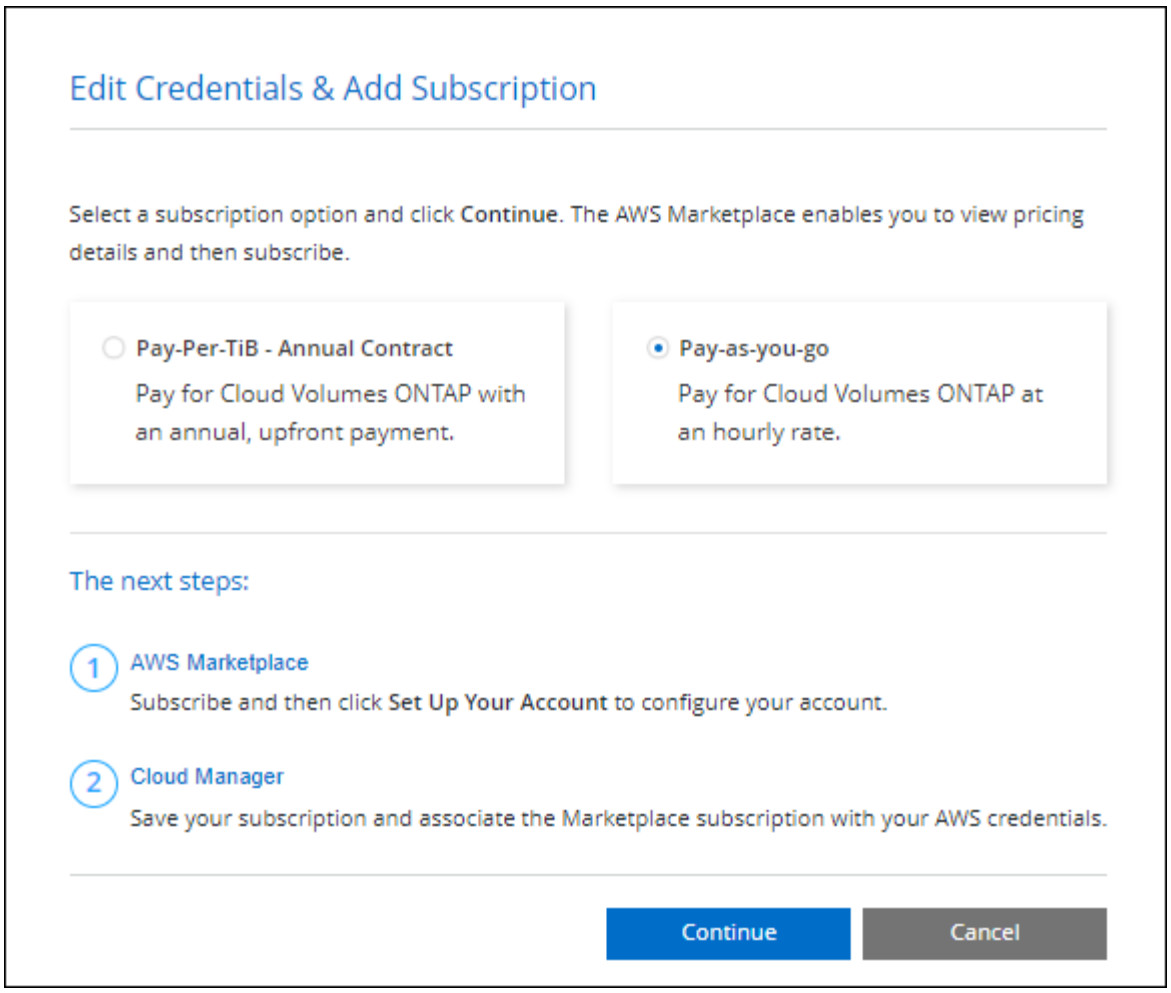
   控制台會自動查詢 NetApp 的授權服務，以取得與您的NetApp支援網站帳戶相關的授權的詳細資訊。如果沒有錯誤，控制台會自動將許可證新增至控制台。

   您必須先從控制台取得許可證，然後才能與Cloud Volumes ONTAP一起使用。如果需要的話，你可以"手動將許可證新增至控制台"。

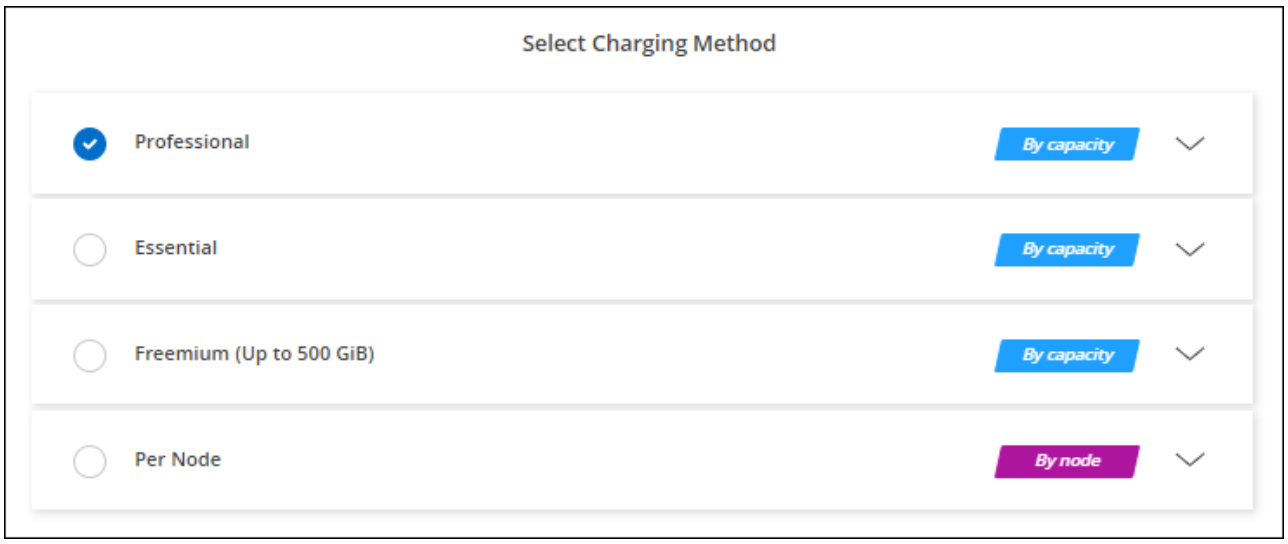
3. 在控制台的「系統」頁面上，按一下「新增系統」並依照步驟操作。

   a. 在“詳細資料和憑證”頁面上，按一下“編輯憑證”>“新增訂閱”，然後依照指示訂閱 AWS Marketplace 中的即用即付服務。

      總是會先向您從NetApp購買的許可證收費，但如果您超出許可容量或許可證期限到期，則會按照市場上的小時費率向您收費。



a. 返回控制台後，在到達收費方式頁面時選擇基於容量的套餐。



"查看在 AWS 中啟動Cloud Volumes ONTAP 的逐步說明" 。

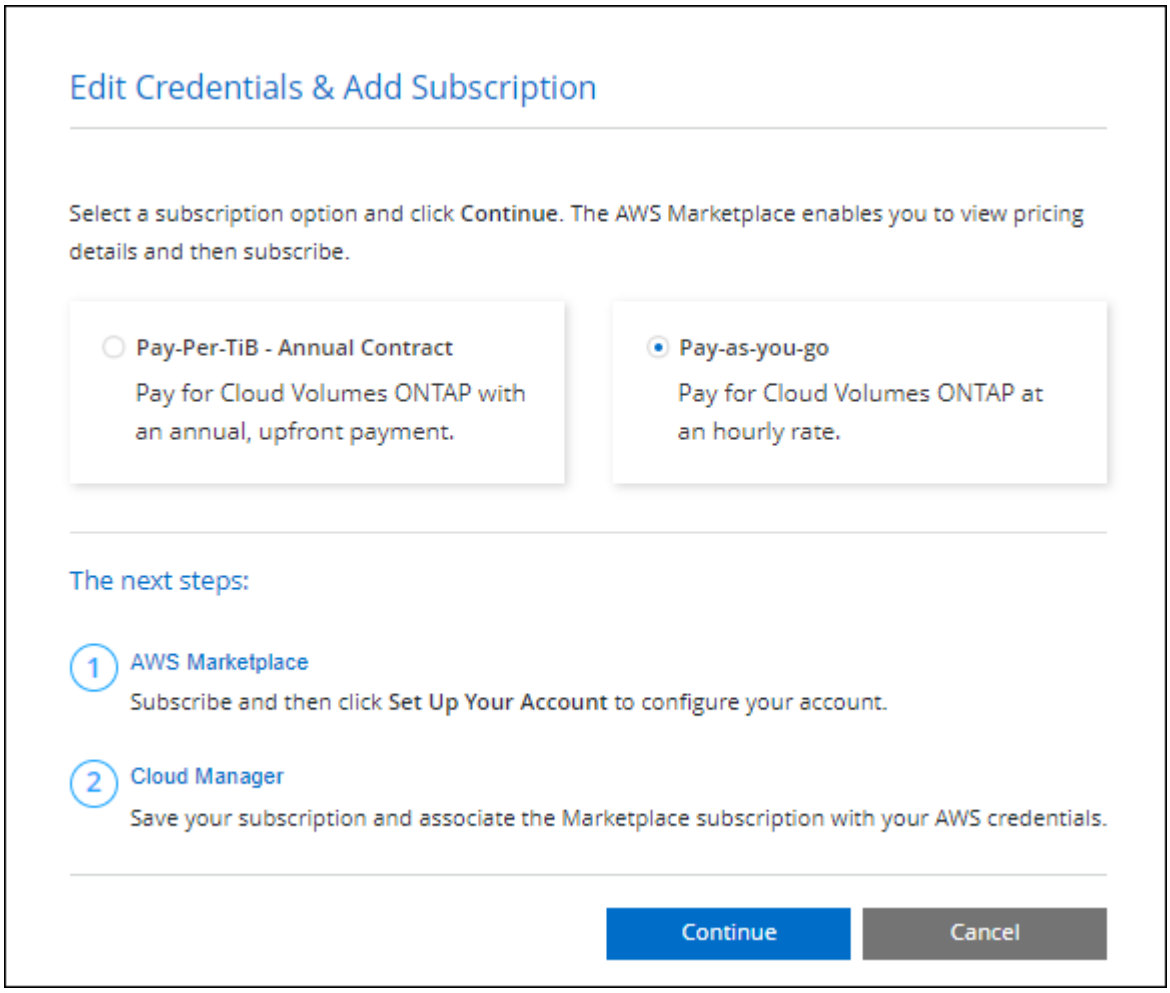
PAYGO 訂閱

透過訂閱雲端供應商市場提供的服務按小時付費。

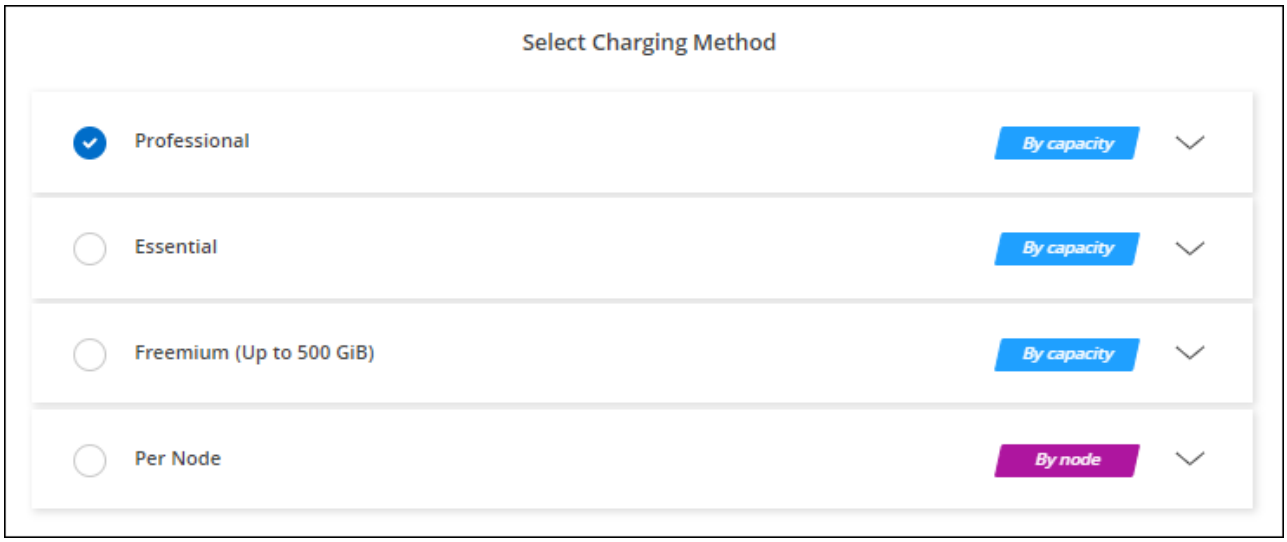
當您建立Cloud Volumes ONTAP系統時，控制台會提示您訂閱 AWS Marketplace 中提供的協定。然後將該訂閱與系統關聯以進行收費。您可以使用相同的訂閱來取得其他Cloud Volumes ONTAP系統。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。
   a. 在“詳細資訊和憑證”頁面上，按一下“編輯憑證”>“新增訂閱”，然後依照指示訂閱 AWS Marketplace 中的即用即付服務



   b. 返回控制台後，在到達收費方式頁面時選擇基於容量的套餐。



"查看在 AWS 中啟動Cloud Volumes ONTAP 的逐步說明" 。

您可以從「設定」>「憑證」頁面管理與您的 AWS 帳戶關聯的 AWS Marketplace 訂閱。 "了解如何管理您的 AWS 帳戶和訂閱"

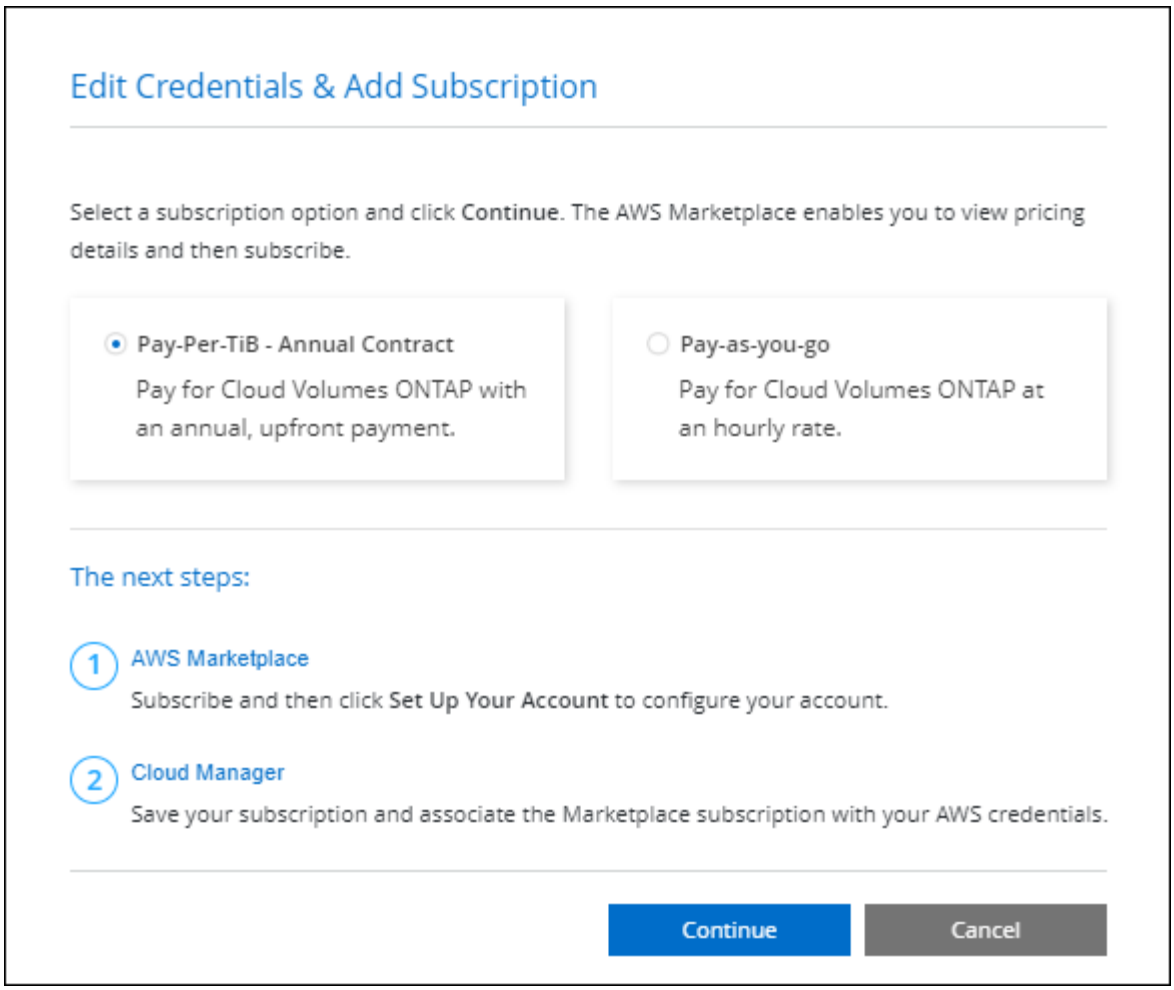
年度合約

從雲端提供者的市場購買年度合同，按年付款。

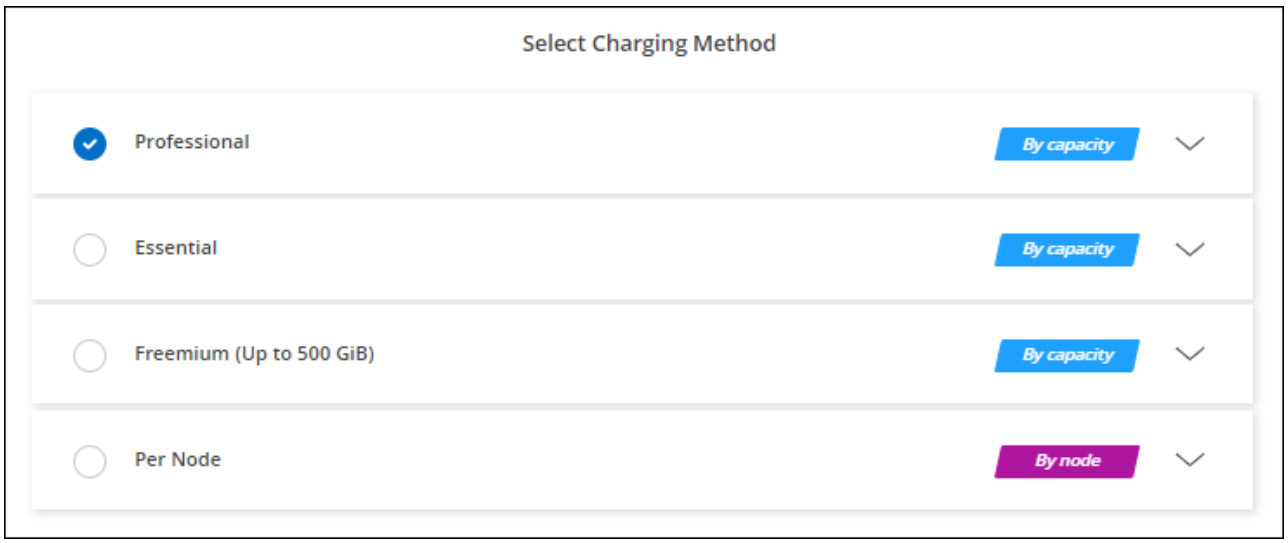
與按小時訂閱類似，控制台會提示您訂閱 AWS Marketplace 中提供的年度合約。

步驟

1. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。
   a. 在*詳細資訊和憑證*頁面上，按一下*編輯憑證 > 新增訂閱*，然後依照指示在 AWS Marketplace 中訂閱年度合約。



b. 返回控制台後，在到達收費方式頁面時選擇基於容量的套餐。



"查看在 AWS 中啟動Cloud Volumes ONTAP 的逐步說明" 。

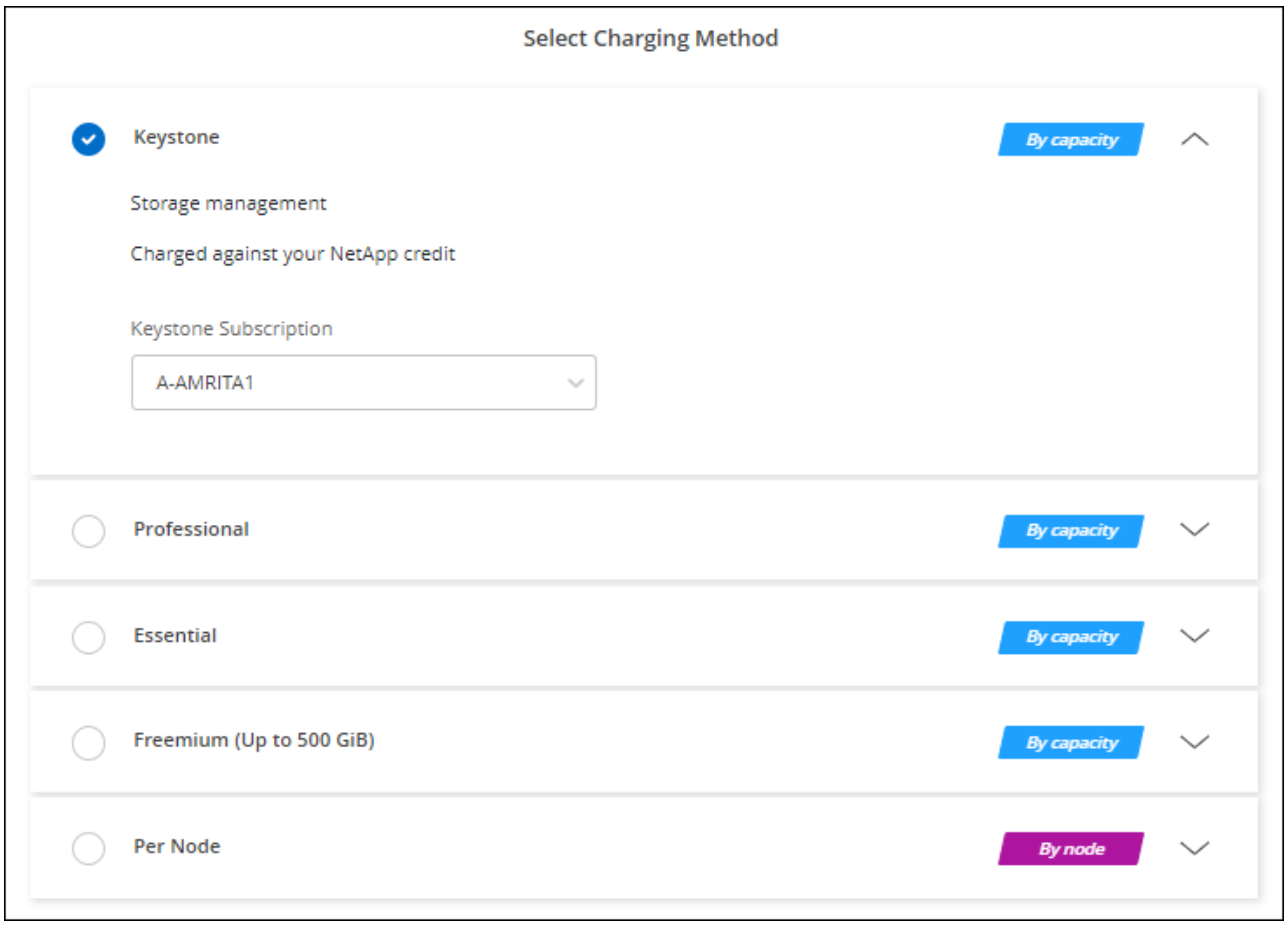
Keystone訂閱

Keystone訂閱是一種按需付費的訂閱式服務。"了解有關NetApp Keystone訂閱的更多信息" 。

步驟

1. 如果您尚未訂閱， "聯絡NetApp"
2. 聯絡NetApp 為您的使用者帳號授權一個或多個Keystone訂閱。
3. NetApp授權您的帳戶後，"連結您的訂閱以用於Cloud Volumes ONTAP" 。
4. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。

    a. 當提示選擇充電方式時，選擇Keystone Subscription 充電方式。



"查看在 AWS 中啟動Cloud Volumes ONTAP 的逐步說明" 。

基於節點的許可證

基於節點的許可證是Cloud Volumes ONTAP的上一代許可證。基於節點的授權可以從NetApp (BYOL) 購買，並且僅在特定情況下才可以續訂授權。有關信息，請參閱：

- "基於節點的許可證的可用性終止"
- "基於節點的許可證的可用性終止"
- "將基於節點的許可證轉換為基於容量的許可證"

使用快速部署在 **AWS** 中部署**Cloud Volumes ONTAP**

您可以使用快速部署方法在 AWS 中部署Cloud Volumes ONTAP，適用於單一節點和高可用性 (HA) 設定。與先進的方法相比，這種簡化的流程減少了部署步驟。它還透過在單一頁面上自動設定預設值並最小化導航來提供更清晰的工作流程。

開始之前

您需要以下內容才能從NetApp Console在 AWS 中新增Cloud Volumes ONTAP系統。

- 已啟動並正在執行的控制台代理程式。
  - 你應該有一個 "與您的專案或工作區關聯的控制台代理"。
  - "您應該準備好讓控制台代理程式始終處於運行狀態" 。
- 了解您想要使用的配置。

  您應該已經做好準備，選擇配置並從管理員處獲取 AWS 網路資訊。有關詳細信息，請參閱"規劃您的Cloud Volumes ONTAP配置"。
- 了解設定Cloud Volumes ONTAP許可所需的條件。

  "了解如何設定許可" 。
- CIFS 設定的 DNS 和 Active Directory。

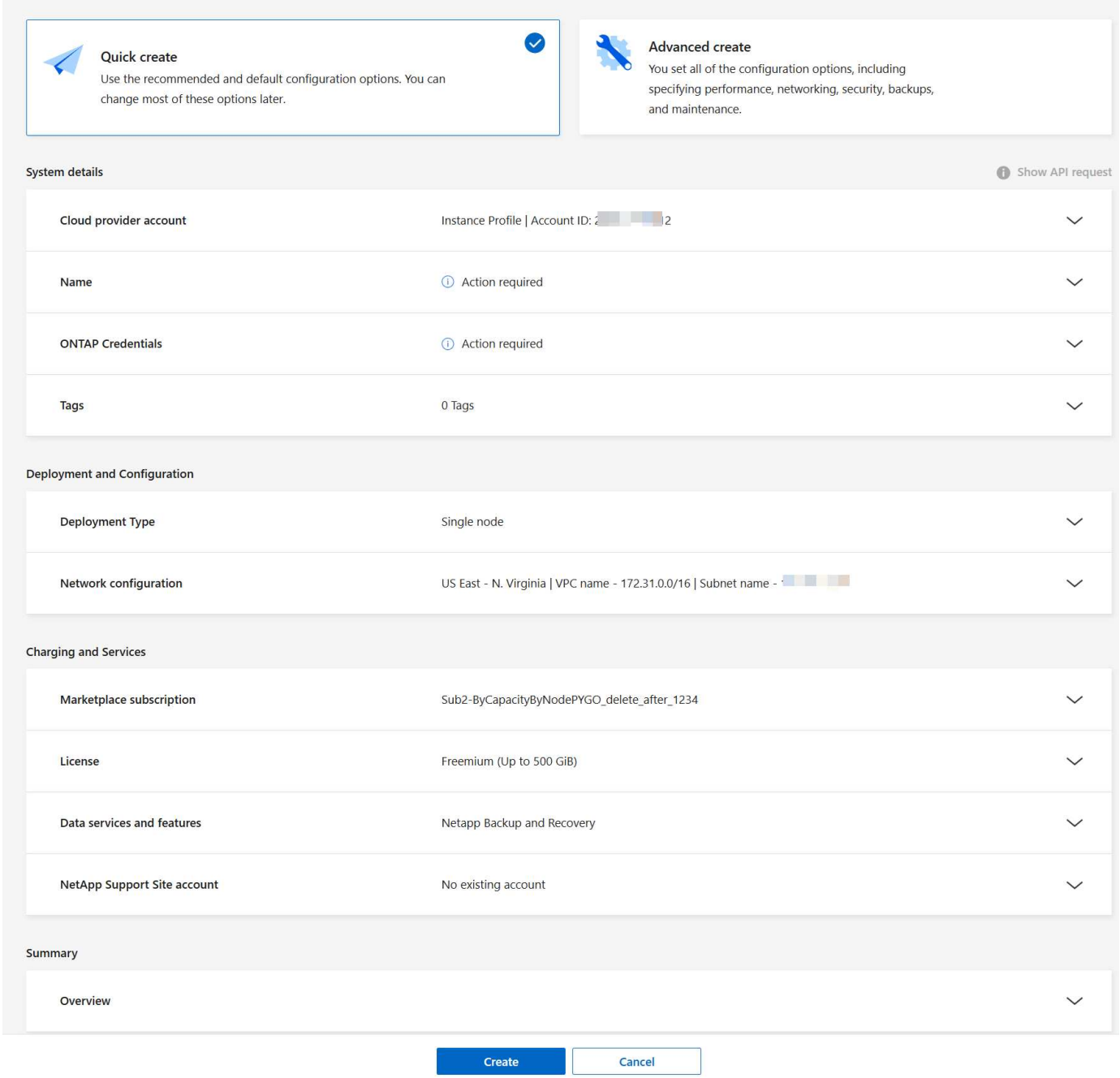
  有關詳細信息，請參閱"AWS 中Cloud Volumes ONTAP的網路需求"。

關於此任務

建立Cloud Volumes ONTAP系統後， NetApp Console會立即在指定的 VPC 中啟動測試實例以驗證連線性。如果成功，控制台會立即終止實例，然後開始部署系統。如果控制台無法驗證連接，則系統建立失敗。測試實例可以是 `t2.nano`（對於預設 VPC 租賃）或 `m3.medium`（適用於專用 VPC 租賃）。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在 Canvas 頁面上，按一下 新增系統 並依照指示進行操作。
3. 選擇 **Amazon Web Services** > * Cloud Volumes ONTAP* > 新增。預設選擇*快速建立*選項。



系統詳細信息

1. 雲端提供者帳戶：帳戶詳細資料將根據您選擇的控制台代理自動填入。如果您有多個帳戶，請選擇要使用的帳戶。如果控制台代理程式不可用，系統將提示您 "建立控制台代理"。
2. 名稱：系統名稱。控制台使用系統（叢集）名稱來命名Cloud Volumes ONTAP系統和 Amazon EC2 執行個體。如果您選擇該選項，它也會使用該名稱作為預先定義安全性群組的前綴。
3. * ONTAP憑證* 這些是Cloud Volumes ONTAP叢集管理員帳戶的憑證。您可以使用這些憑證透過ONTAP System Manager 或ONTAP CLI 連線到Cloud Volumes ONTAP 。您可以保留預設的_admin_用戶名，也可以將其變更為自訂使用者名稱。
4. 標籤 AWS 標籤是您的 AWS 資源的元資料。控制台將標籤新增至Cloud Volumes ONTAP實例以及與該執行個體關聯的每個 AWS 資源。建立Cloud Volumes ONTAP系統時，您可以從使用者介面新增最多 15 個標籤，然後可以在建立後新增更多標籤。請注意，在建立系統時，API 不會將您限制為四個標籤。有關標籤的信息，請參閱 "AWS 文件：標記您的 Amazon EC2 資源"。

部署和配置

1. 部署類型：選擇您想要使用的部署類型，單一節點、單一可用區 (AZ) 中的高可用性 (HA) 或多個 AZ 中的 HA。
2. 網路設定：輸入您在 "AWS 工作表"。
   a. **AWS** 區域：預設選擇關聯雲端帳戶的、擁有子網路資源的 VPC 所在區域。
   b. **VPC**：輸入具有子網路的 AWS 區域的 VPC。如果沒有子網，則選擇 VPC 的預設值。
   c. 子網路：您只能為 VPC 選擇一個子網，以用於單節點部署或單 AZ 中的 HA 部署。

高可用性

如果您選擇了 HA 配置，請輸入以下資訊：

單可用區高可用性

1. 調解器存取：指定調解器存取資訊。調解器是一個單獨的實例，用於監控 HA 對的健康狀況並在發生故障時提供仲裁。提供金鑰對名稱以使中介執行個體能夠連線到 AWS EC2 服務，並選擇連線方法。

多個可用區中的高可用性

1. 可用區域和中介：選擇每個節點的可用區域 (AZ) 以及要部署Cloud Volumes ONTAP HA 對的中介和對應子網路。
2. 浮動 **IP**：如果您選擇多個 AZ，請為 NFS 和 CIFS 服務以及叢集和 SVM 管理指定浮動 IP 位址。 IP 位址必須位於該區域內所有 VPC 的 CIDR 區塊之外。有關更多詳細信息，請參閱"多個可用區中Cloud Volumes ONTAP HA 的 AWS 網路需求"。
3. 調解器存取：指定調解器存取資訊。調解器是一個單獨的實例，用於監控 HA 對的健康狀況並在發生故障時提供仲裁。提供金鑰對名稱以使中介執行個體能夠連線到 AWS EC2 服務，並選擇連線方法。
4. 路由表：如果您選擇了多個 AZ，請選擇包含到浮動 IP 位址的路由的路由表。如果您有多個路由表，則選擇正確的路由表非常重要。否則，某些用戶端可能無法存取Cloud Volumes ONTAP HA 對。有關路由表的更多信息，請參閱 "AWS 文件：路由表"。

充電和服務

1. 市場訂閱：選擇您想要與此Cloud Volumes ONTAP系統一起使用的 AWS 市場訂閱。
2. 許可證：選擇您想要與此Cloud Volumes ONTAP系統一起使用的許可證類型。您可以從專業版、基本版和高級版授權中進行選擇。有關不同許可證的信息，請參閱"了解Cloud Volumes ONTAP許可證"。
3. 資料服務與功能：啟用服務或停用您不想與Cloud Volumes ONTAP一起使用的服務。
   - "了解有關NetApp分類的更多信息"
   - "了解有關NetApp Backup and Recovery的更多信息"
   - "了解Cloud Volumes ONTAP上的 WORM 存儲"

     如果您想利用 WORM 和資料分層，則必須停用備份和還原並部署版本 9.8 或更高版本的Cloud Volumes ONTAP系統。

   - * NetApp支援網站帳戶*：如果您有多個帳戶，請選擇要使用的帳戶。

總結

檢查或編輯您輸入的詳細信息，然後點擊*建立*。

部署程序完成後，請勿修改 AWS 雲端入口網站中系統產生的Cloud Volumes ONTAP配置，尤其是系統標籤。對這些配置所做的任何變更都可能導致意外行為或資料遺失。

相關連結

- "規劃您的Cloud Volumes ONTAP配置"
- "使用進階部署在 AWS 中部署Cloud Volumes ONTAP"

在 AWS 中啟動Cloud Volumes ONTAP

您可以在單一系統設定中啟動Cloud Volumes ONTAP ，也可以在 AWS 中以 HA 對的形式啟動 Cloud Volumes ONTAP。此方法提供了進階部署體驗，與快速部署方法相比，它提供了更多的配置選項和靈活性。

開始之前

開始之前您需要以下內容。

- 已啟動並正在執行的控制台代理程式。
  - 你應該有一個 "與您的系統關聯的控制台代理"。
  - "您應該準備好讓控制台代理程式始終處於運行狀態" 。
- 了解您想要使用的配置。

  您應該已經做好準備，選擇配置並從管理員處獲取 AWS 網路資訊。有關詳細信息，請參閱"規劃您的Cloud Volumes ONTAP配置"。
- 了解設定Cloud Volumes ONTAP許可所需的條件。

  "了解如何設定許可" 。
- CIFS 設定的 DNS 和 Active Directory。

  有關詳細信息，請參閱"AWS 中Cloud Volumes ONTAP的網路需求"。

在 AWS 中啟動單節點Cloud Volumes ONTAP系統

如果您想要在 AWS 中啟動Cloud Volumes ONTAP ，則需要在NetApp Console中建立新系統。

關於此任務

建立系統後，控制台會立即在指定的 VPC 中啟動測試執行個體以驗證連線性。如果成功，控制台將立即終止實例，然後開始部署Cloud Volumes ONTAP系統。如果無法驗證連接，系統建立將失敗。測試實例可以是 `t2.nano`（對於預設 VPC 租賃）或 `m3.medium`（適用於專用 VPC 租賃）。

步驟

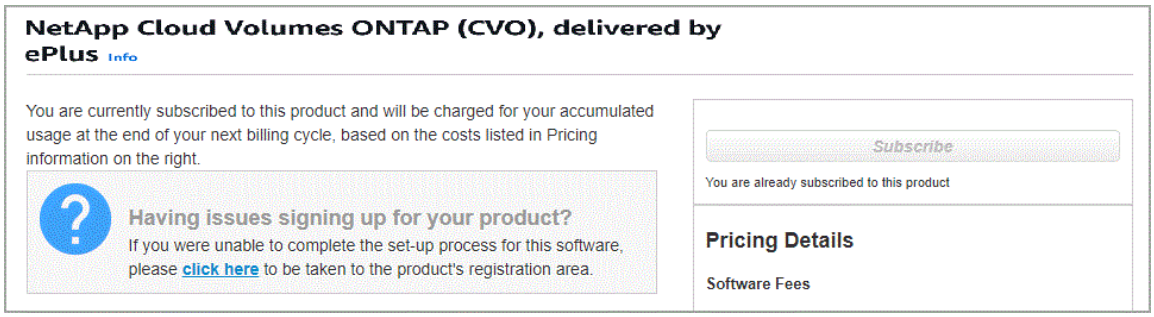
1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，點擊*新增系統*並依照指示操作。

3. 選擇 **Amazon Web Services** 和 * Cloud Volumes ONTAP Single Node*。
4. 選擇*進階建立*。由於預設選擇了*快速建立*模式，您可能會看到一條有關預設值的訊息。按一下“繼續”。
5. 如果出現提示， "建立控制台代理" 。
6. 詳細資料和憑證：可選擇變更 AWS 憑證和訂閱，輸入系統名稱，根據需要新增標籤，然後輸入密碼。

   此頁面中的某些欄位是不言自明的。下表描述了您可能需要指導的欄位：

場地	描述
系統名稱	控制台使用系統名稱來命名Cloud Volumes ONTAP系統和 Amazon EC2 執行個體。如果您選擇該選項，它也會使用該名稱作為預先定義安全性群組的前綴。
添加標籤	AWS 標籤是您的 AWS 資源的元資料。控制台將標籤新增至Cloud Volumes ONTAP實例以及與該執行個體關聯的每個 AWS 資源。建立系統時，您可以從使用者介面新增多達四個標籤，然後可以在建立系統後新增更多標籤。請注意，在建立系統時，API 不會將您限制為四個標籤。有關標籤的信息，請參閱 "AWS 文件：標記您的 Amazon EC2 資源"。
使用者名稱和密碼	這些是Cloud Volumes ONTAP叢集管理員帳戶的憑證。您可以使用這些憑證透過ONTAP System Manager 或ONTAP CLI 連線到Cloud Volumes ONTAP 。保留預設的_admin_使用者名稱或將其變更為自訂使用者名稱。
編輯憑證	選擇與您要部署此系統的帳戶關聯的 AWS 憑證。您也可以將 AWS 市場訂閱與此Cloud Volumes ONTAP系統關聯起來使用。點擊「新增訂閱」將所選憑證與新的 AWS 市場訂閱關聯。訂閱可以是年度合同，也可以是按小時付費的Cloud Volumes ONTAP 。https://docs.netapp.com/us-en/bluexp-setup-admin/task-adding-aws-accounts.html["了解如何在NetApp Console新增其他 AWS 憑證"^] 。

如果多個 IAM 使用者在同一個 AWS 帳戶中工作，則每個使用者都需要訂閱。第一個用戶訂閱後，AWS 市場會通知後續用戶他們已經訂閱，如下圖所示。當 AWS 帳戶有訂閱時，每個 IAM 使用者都需要將自己與該訂閱關聯起來。如果您看到下面顯示的訊息，請點擊「點擊這裡」連結前往控制台網站並完成該過
程。



7. 服務：啟用服務啟用或停用您不想與Cloud Volumes ONTAP一起使用的單一服務。
   - "了解有關NetApp Data Classification的更多信息"
   - "了解有關NetApp Backup and Recovery的更多信息"

如果您想使用 WORM 和資料分層，則必須停用備份和還原並部署版本 9.8 或更高版本的Cloud Volumes ONTAP系統。

8. 位置和連接：輸入您在 "AWS 工作表"。

   下表描述了您可能需要指導的欄位：

場地	描述
專有網絡	如果您有 AWS Outpost，則可以透過選擇 Outpost VPC 在該 Outpost 中部署單節點Cloud Volumes ONTAP系統。體驗與駐留在 AWS 中的任何其他 VPC 相同。
產生的安全群組	如果您讓控制台為您產生安全性群組，則需要選擇如何允許流量： • 如果您選擇*僅限選定的 VPC*，則入站流量的來源是選定 VPC 的子網路範圍和控制台代理程式所在 VPC 的子網路範圍。這是推薦的選項。 • 如果您選擇*所有 VPC*，則入站流量的來源為 0.0.0.0/0 IP 範圍。
使用現有的安全群組	如果您使用現有的防火牆策略，請確保它包含所需的規則。"了解Cloud Volumes ONTAP的防火牆規則" 。

9. 資料加密：選擇無資料加密或 AWS 管理加密。

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

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

   "了解如何為Cloud Volumes ONTAP設定 AWS KMS" 。

   "了解有關受支援的加密技術的更多信息" 。

10. 收費方式和 **NSS** 帳戶：指定您想要在此系統中使用的收費選項，然後指定NetApp支援網站帳戶。
    - "了解Cloud Volumes ONTAP的授權選項" 。
    - "了解如何設定許可" 。
11. * Cloud Volumes ONTAP配置*（僅限年度 AWS 市場合約）：查看預設配置並點擊*繼續*或點擊*更改配置*以選擇您自己的配置。

    如果保留預設配置，則只需要指定一個卷，然後審核並批准該配置。

12. 預先配置套件：選擇其中一個套件以快速啟動Cloud Volumes ONTAP，或點擊*變更配置*以選擇您自己的配置。

    如果您選擇其中一個包，那麼您只需要指定一個卷，然後審核並批准配置。

13. **IAM** 角色：最好保留預設選項，讓控制台為您建立角色。

    如果您希望使用自己的政策，則必須滿足"Cloud Volumes ONTAP節點的策略需求"。

14. 許可：根據需要變更Cloud Volumes ONTAP版本並選擇實例類型和實例租賃。

如果所選版本有較新的候選版本、通用版本或修補程式版本，則控制台在建立系統時會將系統更新至該版本。例如，如果您選擇Cloud Volumes ONTAP 9.13.1 且 9.13.1 P4 可用，則會發生更新。更新不會從一個版本發生到另一個版本 - 例如，從 9.13 到 9.14。

15. 底層儲存資源：選擇磁碟類型，配置底層存儲，並選擇是否保持資料分層啟用。

    請注意以下事項：

    - 磁碟類型適用於初始磁碟區（和聚合）。您可以為後續磁碟區（和聚合）選擇不同的磁碟類型。
    - 如果您選擇 gp3 或 io1 磁碟，控制台將使用 AWS 中的彈性磁碟區功能根據需要自動增加底層儲存磁碟容量。您可以根據您的儲存需求選擇初始容量，並在部署Cloud Volumes ONTAP後進行修改。"了解有關 AWS 彈性卷支援的更多信息" 。
    - 如果您選擇 gp2 或 st1 磁碟，則可以為初始聚合中的所有磁碟以及使用簡單設定選項時控制台建立的任何其他聚合選擇磁碟大小。您可以使用進階分配選項建立使用不同磁碟大小的聚合。
    - 您可以在建立或編輯磁碟區時選擇特定的磁碟區分層策略。
    - 如果您停用資料分層，則可以在後續聚合上啟用它。

      "了解資料分層的工作原理" 。

16. 寫入速度與 **WORM**：

    a. 如有需要，請選擇*正常*或*高*寫入速度。

       "了解有關寫入速度的更多信息" 。

    b. 如果需要，請啟動一次寫入、多次讀取 (WORM) 儲存。

       如果為Cloud Volumes ONTAP 9.7 及更低版本啟用了資料分層，則無法啟用 WORM。啟用 WORM 和分層後，恢復或降級到Cloud Volumes ONTAP 9.8 的操作將被阻止。

    "了解有關 WORM 存儲的更多信息" 。

    a. 如果您啟動 WORM 存儲，請選擇保留期限。

17. 建立磁碟區：輸入新磁碟區的詳細資料或點選*跳過*。

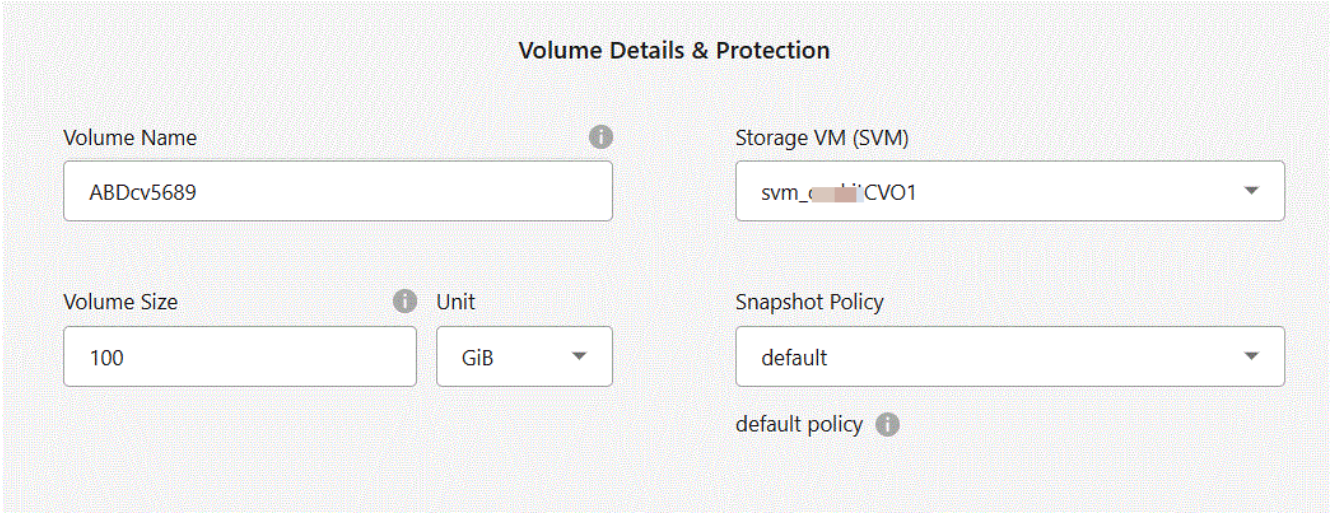
    "了解支援的客戶端協定和版本" 。

    此頁面中的某些欄位是不言自明的。下表描述了您可能需要指導的欄位：

場地	描述
尺寸	您可以輸入的最大大小很大程度上取決於您是否啟用精簡配置，這使您能夠建立比目前可用的實體儲存更大的磁碟區。
存取控制（僅適用於 NFS）	導出策略定義了子網路中可以存取磁碟區的用戶端。預設情況下，控制台輸入一個提供對子網路中所有實例的存取權限的值。
權限和使用者/群組（僅適用於 CIFS）	這些欄位可讓您控制使用者和群組對共用的存取等級（也稱為存取控制清單或 ACL）。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。如果指定網域 Windows 使用者名，則必須使用網域\使用者名稱格式包含使用者的網域。

場地	描述
快照策略	Snapshot 副本策略指定自動建立的NetApp Snapshot 副本的頻率和數量。NetApp Snapshot 副本是時間點檔案系統映像，它不會影響效能並且只需要最少的儲存空間。您可以選擇預設策略或無策略。對於瞬態數據，您可能會選擇無：例如，對於 Microsoft SQL Server，請選擇 tempdb。
進階選項（僅適用於 NFS）	為磁碟區選擇一個 NFS 版本：NFSv3 或 NFSv4。
啟動器群組和 IQN（僅適用於 iSCSI）	iSCSI 儲存目標稱為 LUN（邏輯單元），並以標準區塊裝置呈現給主機。啟動器群組是 iSCSI 主機節點名稱表，用於控制哪些啟動器可以存取哪些 LUN。iSCSI 目標透過標準乙太網路網路適配器 (NIC)、具有軟體啟動器的 TCP 卸載引擎 (TOE) 卡、融合網路適配器 (CNA) 或專用主機匯流排適配器 (HBA) 連接到網絡，並透過 iSCSI 限定名稱 (IQN) 進行識別。當您建立 iSCSI 磁碟區時，控制台會自動為您建立 LUN。我們透過為每個磁碟區建立一個 LUN 來簡化操作，因此無需進行任何管理。建立磁碟區後，"使用 IQN 從主機連線到 LUN" 。

下圖顯示了磁碟區建立精靈的第一頁：



18. **CIFS** 設定：如果您選擇 CIFS 協議，請設定 CIFS 伺服器。

場地	描述
DNS 主 IP 位址和輔助 IP 位址	為 CIFS 伺服器提供名稱解析的 DNS 伺服器的 IP 位址。所列的 DNS 伺服器必須包含定位 CIFS 伺服器將加入的網域的 Active Directory LDAP 伺服器和網域控制站所需的服務位置記錄 (SRV)。
要加入的 Active Directory 網域	您希望 CIFS 伺服器加入的 Active Directory (AD) 網域的 FQDN。
授權加入網域的憑證	具有足夠權限將電腦新增至 AD 網域內指定組織單位 (OU) 的 Windows 帳戶的名稱和密碼。
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 網域內與 CIFS 伺服器關聯的組織單位。預設值為 CN=Computers。如果將 AWS Managed Microsoft AD 配置為Cloud Volumes ONTAP 的AD 伺服器，則應在此欄位中輸入 **OU=Computers,OU=corp**。

場地	描述
DNS 網域	Cloud Volumes ONTAP儲存虛擬機器 (SVM) 的 DNS 網域。大多數情況下，該域與 AD 域相同。
NTP 伺服器	選擇「使用 Active Directory 網域」以使用 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，那麼您應該使用 API。請參閱 "NetApp Console自動化文檔"了解詳情。請注意，只有在建立 CIFS 伺服器時才能設定 NTP 伺服器。建立 CIFS 伺服器後，它不可配置。

19. 使用情況設定檔、磁碟類型和分層原則：選擇是否要啟用儲存效率功能，並在需要時編輯磁碟區分層策略。

    更多信息，請參閱"了解卷使用情況"，"資料分層概述" ， 和 "KB：CVO 支援哪些內嵌儲存效率功能？"

20. 審核並批准：審核並確認您的選擇。
    a. 查看有關配置的詳細資訊。
    b. 按一下「更多資訊」以查看有關支援和控制台將購買的 AWS 資源的詳細資訊。
    c. 選取*我明白…*複選框。
    d. 按一下“開始”。

結果

控制台啟動Cloud Volumes ONTAP實例。您可以在*審核*頁面上追蹤進度。

如果您在啟動Cloud Volumes ONTAP實例時遇到任何問題，請查看失敗訊息。您也可以選擇系統並點擊*重新建立環境*。

如需更多協助，請訪問 "NetApp Cloud Volumes ONTAP支持"。

部署程序完成後，請勿修改 AWS 雲端入口網站中系統產生的Cloud Volumes ONTAP配置，尤其是系統標籤。對這些配置所做的任何變更都可能導致意外行為或資料遺失。

完成後

- 如果您配置了 CIFS 共享，請授予使用者或群組對檔案和資料夾的權限，並驗證這些使用者是否可以存取共用並建立檔案。
- 如果要將配額套用於卷，請使用ONTAP系統管理員或ONTAP CLI。

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

在 **AWS** 中啟動**Cloud Volumes ONTAP HA** 對

如果您想要在 AWS 中啟動Cloud Volumes ONTAP HA 對，則需要在控制台中建立 HA 系統。

限制

目前，AWS Outposts 不支援 HA 對。

關於此任務

建立Cloud Volumes ONTAP系統後，控制台會立即在指定的 VPC 中啟動測試實例以驗證連線性。如果成功，控制台將立即終止實例，然後開始部署Cloud Volumes ONTAP系統。如果無法驗證連接，系統建立將失敗。測試

實例可以是 `t2.nano`（對於預設 VPC 租賃）或 `m3.medium`（適用於專用 VPC 租賃）。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，按一下*新增系統*並依照指示操作。
3. 選擇 **Amazon Web Services** 和 * Cloud Volumes ONTAP HA*。

   一些 AWS 本地區域可用。

   您必須先啟用本機區域並在 AWS 帳戶的本機區域中建立子網，然後才能使用 AWS 本地區域。按照*選擇加入 AWS 本機區域*和*將您的 Amazon VPC 擴展到本機區域*中的步驟操作"AWS 教學課程「開始使用 AWS 本地區域部署低延遲應用程式"。

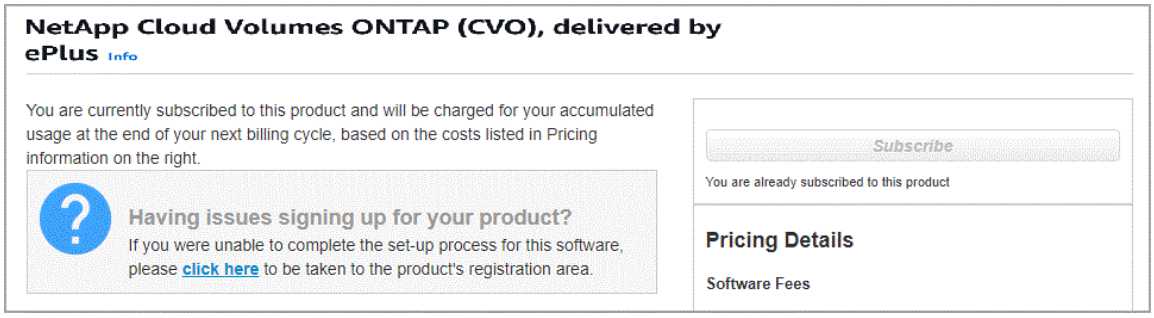
   如果您執行的是控制台代理 3.9.36 或更低版本，則需要新增 `DescribeAvailabilityZones`AWS EC2 控制台中 AWS 角色的權限。

4. 詳細資料和憑證：可選擇變更 AWS 憑證和訂閱，輸入系統名稱，根據需要新增標籤，然後輸入密碼。

   此頁面中的某些欄位是不言自明的。下表描述了您可能需要指導的欄位：

場地	描述
系統名稱	控制台使用系統名稱來命名Cloud Volumes ONTAP系統和 Amazon EC2 執行個體。如果您選擇該選項，它也會使用該名稱作為預先定義安全性群組的前綴。
添加標籤	AWS 標籤是您的 AWS 資源的元資料。控制台將標籤新增至Cloud Volumes ONTAP實例以及與該執行個體關聯的每個 AWS 資源。建立系統時，您可以從使用者介面新增多達四個標籤，然後可以在建立系統後新增更多標籤。請注意，在建立系統時，API 不會將您限制為四個標籤。有關標籤的信息，請參閱 "AWS 文件：標記您的 Amazon EC2 資源"。
使用者名稱和密碼	這些是Cloud Volumes ONTAP叢集管理員帳戶的憑證。您可以使用這些憑證透過ONTAP System Manager 或ONTAP CLI 連線到Cloud Volumes ONTAP 。保留預設的_admin_使用者名稱或將其變更為自訂使用者名稱。
編輯憑證	選擇要用於此Cloud Volumes ONTAP系統的 AWS 憑證和市場訂閱。點擊「新增訂閱」將所選憑證與新的 AWS 市場訂閱關聯。訂閱可以是年度合同，也可以是按小時付費的Cloud Volumes ONTAP 。如果您直接從NetApp購買了授權（自帶授權 (BYOL)），則無需 AWS 訂閱。 NetApp已限制 BYOL 授權的購買、延期和續約。有關更多信息，請參閱 "Cloud Volumes ONTAP的 BYOL 授權可用性受限" 。https://docs.netapp.com/us-en/bluexp-setup-admin/task-adding-aws-accounts.html["了解如何在控制台中新增其他 AWS 憑證"^] 。

如果多個 IAM 使用者在同一個 AWS 帳戶中工作，則每個使用者都需要訂閱。第一個用戶訂閱後，AWS 市場會通知後續用戶他們已經訂閱，如下圖所示。當 AWS 帳戶有訂閱時，每個 IAM 使用者都需要將自己與該訂閱關聯起來。如果您看到下面顯示的訊息，請點擊「點擊這裡」連結前往控制台網站並完成該過
程。



5. 服務：啟用服務啟用或停用您不想在此Cloud Volumes ONTAP系統中使用的單一服務。
   - "了解有關NetApp Data Classification的更多信息"
   - "了解有關備份和恢復的更多信息"

   如果您想使用 WORM 和資料分層，則必須停用備份和還原並部署版本 9.8 或更高版本的Cloud Volumes ONTAP系統。

6. **HA** 部署模型：選擇 HA 配置。

   有關部署模型的概述，請參閱"適用於 AWS 的Cloud Volumes ONTAP HA"。

7. 位置和連線（單一可用區 (AZ)）或*區域和 VPC*（多個 AZ）：輸入您在 AWS 工作表中記錄的網路資訊。

   下表描述了您可能需要指導的欄位：

場地	描述
產生的安全群組	如果您讓控制台為您產生安全性群組，則需要選擇如何允許流量： • 如果您選擇*僅限選定的 VPC*，則入站流量的來源是選定 VPC 的子網路範圍和控制台代理程式所在 VPC 的子網路範圍。這是推薦的選項。 • 如果您選擇*所有 VPC*，則入站流量的來源為 0.0.0.0/0 IP 範圍。
使用現有的安全群組	如果您使用現有的防火牆策略，請確保它包含所需的規則。"了解Cloud Volumes ONTAP的防火牆規則" 。

8. 連線和 **SSH** 驗證：選擇 HA 對和中介的連線方法。
9. 浮動 **IP**：如果您選擇多個 AZ，請指定浮動 IP 位址。

   IP 位址必須位於該區域內所有 VPC 的 CIDR 區塊之外。有關更多詳細信息，請參閱"多個可用區中Cloud Volumes ONTAP HA 的 AWS 網路需求"。

10. 路由表：如果您選擇了多個 AZ，請選擇應包含到浮動 IP 位址的路由的路由表。

    如果您有多個路由表，那麼選擇正確的路由表非常重要。否則，某些用戶端可能無法存取Cloud Volumes

ONTAP HA 對。有關路由表的更多信息，請參閱 "AWS 文件：路由表"。

11. 資料加密：選擇無資料加密或 AWS 管理加密。

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

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

    "了解如何為Cloud Volumes ONTAP設定 AWS KMS" 。

    "了解有關受支援的加密技術的更多信息" 。

12. 收費方式和 **NSS** 帳戶：指定您想要在此系統中使用的收費選項，然後指定NetApp支援網站帳戶。
    - "了解Cloud Volumes ONTAP的授權選項" 。
    - "了解如何設定許可" 。
13. * Cloud Volumes ONTAP配置*（僅限年度 AWS Marketplace 合約）：查看預設配置並點擊*繼續*或點擊*更改配置*以選擇您自己的配置。

    如果保留預設配置，則只需要指定一個卷，然後審核並批准該配置。

14. 預先配置套件（按小時或僅限 BYOL）：選擇其中一個套件以快速啟動Cloud Volumes ONTAP，或點擊*變更配置*以選擇您自己的配置。

    如果您選擇其中一個包，那麼您只需要指定一個卷，然後審核並批准配置。

15. **IAM** 角色：最好保留預設選項，讓控制台為您建立角色。

    如果您希望使用自己的政策，則必須滿足"Cloud Volumes ONTAP節點和 HA 調解器的策略需求"。

16. 許可：根據需要變更Cloud Volumes ONTAP版本並選擇實例類型和實例租賃。

    如果所選版本有較新的候選版本、通用版本或修補程式版本，則控制台在建立系統時會將系統更新至該版本。例如，如果您選擇Cloud Volumes ONTAP 9.13.1 且 9.13.1 P4 可用，則會發生更新。更新不會從一個版本發生到另一個版本 - 例如，從 9.13 到 9.14。

17. 底層儲存資源：選擇磁碟類型，配置底層存儲，並選擇是否保持資料分層啟用。

    請注意以下事項：

    - 磁碟類型適用於初始磁碟區（和聚合）。您可以為後續磁碟區（和聚合）選擇不同的磁碟類型。
    - 如果您選擇 gp3 或 io1 磁碟，控制台將使用 AWS 中的彈性磁碟區功能根據需要自動增加底層儲存磁碟容量。您可以根據您的儲存需求選擇初始容量，並在部署Cloud Volumes ONTAP後進行修改。"了解有關 AWS 彈性卷支援的更多信息" 。
    - 如果您選擇 gp2 或 st1 磁碟，則可以為初始聚合中的所有磁碟以及使用簡單設定選項時控制台建立的任何其他聚合選擇磁碟大小。您可以使用進階分配選項建立使用不同磁碟大小的聚合。
    - 您可以在建立或編輯磁碟區時選擇特定的磁碟區分層策略。
    - 如果您停用資料分層，則可以在後續聚合上啟用它。

"了解資料分層的工作原理" 。

18. 寫入速度與 **WORM**：

    a. 如有需要，請選擇*正常*或*高*寫入速度。

       "了解有關寫入速度的更多信息" 。

    b. 如果需要，請啟動一次寫入、多次讀取 (WORM) 儲存。

       如果為Cloud Volumes ONTAP 9.7 及更低版本啟用了資料分層，則無法啟用 WORM。啟用 WORM 和分層後，恢復或降級到Cloud Volumes ONTAP 9.8 的操作將被阻止。

    "了解有關 WORM 存儲的更多信息" 。

    a. 如果您啟動 WORM 存儲，請選擇保留期限。

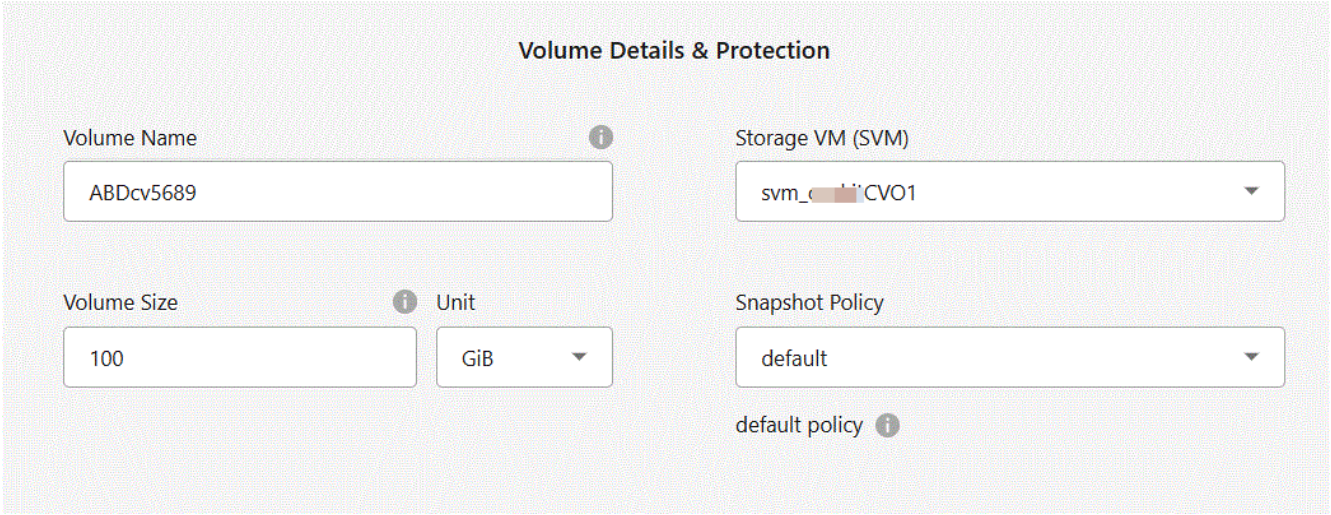
19. 建立磁碟區：輸入新磁碟區的詳細資料或點選*跳過*。

    "了解支援的客戶端協定和版本" 。

    此頁面中的某些欄位是不言自明的。下表描述了您可能需要指導的欄位：

場地	描述
尺寸	您可以輸入的最大大小很大程度上取決於您是否啟用精簡配置，這使您能夠建立比目前可用的實體儲存更大的磁碟區。
存取控制（僅適用於 NFS）	導出策略定義了子網路中可以存取磁碟區的用戶端。預設情況下，控制台輸入一個提供對子網路中所有實例的存取權限的值。
權限和使用者/群組（僅適用於 CIFS）	這些欄位可讓您控制使用者和群組對共用的存取等級（也稱為存取控制清單或 ACL）。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。如果指定網域 Windows 使用者名，則必須使用網域\使用者名稱格式包含使用者的網域。
快照策略	Snapshot 副本策略指定自動建立的NetApp Snapshot 副本的頻率和數量。NetApp Snapshot 副本是時間點檔案系統映像，它不會影響效能並且只需要最少的儲存空間。您可以選擇預設策略或無策略。對於瞬態數據，您可能會選擇無：例如，對於 Microsoft SQL Server，請選擇 tempdb。
進階選項（僅適用於 NFS）	為磁碟區選擇一個 NFS 版本：NFSv3 或 NFSv4。
啟動器群組和 IQN（僅適用於 iSCSI）	iSCSI 儲存目標稱為 LUN（邏輯單元），並以標準區塊裝置呈現給主機。啟動器群組是 iSCSI 主機節點名稱表，用於控制哪些啟動器可以存取哪些 LUN。iSCSI 目標透過標準乙太網路網路適配器 (NIC)、具有軟體啟動器的 TCP 卸載引擎 (TOE) 卡、融合網路適配器 (CNA) 或專用主機匯流排適配器 (HBA) 連接到網絡，並透過 iSCSI 限定名稱 (IQN) 進行識別。當您建立 iSCSI 磁碟區時，控制台會自動為您建立 LUN。我們透過為每個磁碟區建立一個 LUN 來簡化操作，因此無需進行任何管理。建立磁碟區後，"使用 IQN 從主機連線到 LUN" 。

    下圖顯示了磁碟區建立精靈的第一頁：



20. **CIFS** 設定：如果您選擇了 CIFS 協議，請設定 CIFS 伺服器。

場地	描述
DNS 主 IP 位址和輔助 IP 位址	為 CIFS 伺服器提供名稱解析的 DNS 伺服器的 IP 位址。所列的 DNS 伺服器必須包含定位 CIFS 伺服器將加入的網域的 Active Directory LDAP 伺服器和網域控制站所需的服務位置記錄 (SRV)。
要加入的 Active Directory 網域	您希望 CIFS 伺服器加入的 Active Directory (AD) 網域的 FQDN。
授權加入網域的憑證	具有足夠權限將電腦新增至 AD 網域內指定組織單位 (OU) 的 Windows 帳戶的名稱和密碼。
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 網域內與 CIFS 伺服器關聯的組織單位。預設值為 CN=Computers。如果將 AWS Managed Microsoft AD 配置為Cloud Volumes ONTAP 的AD 伺服器，則應在此欄位中輸入 **OU=Computers,OU=corp**。
DNS 網域	Cloud Volumes ONTAP儲存虛擬機器 (SVM) 的 DNS 網域。大多數情況下，該域與 AD 域相同。
NTP 伺服器	選擇「使用 Active Directory 網域」以使用 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，那麼您應該使用 API。請參閱 "NetApp Console自動化文檔"了解詳情。請注意，只有在建立 CIFS 伺服器時才能設定 NTP 伺服器。建立 CIFS 伺服器後，它不可配置。

21. 使用情況設定檔、磁碟類型和分層原則：選擇是否要啟用儲存效率功能，並在需要時編輯磁碟區分層策略。

    更多信息，請參閱"選擇卷使用情況設定檔"和"資料分層概述"。

22. 審核並批准：審核並確認您的選擇。
    a. 查看有關配置的詳細資訊。
    b. 按一下「更多資訊」以查看有關支援和控制台將購買的 AWS 資源的詳細資訊。
    c. 選取*我明白...*複選框。
    d. 按一下“開始”。

結果

控制台啟動Cloud Volumes ONTAP HA 對。您可以在*審核*頁面上追蹤進度。

如果您在啟動 HA 對時遇到任何問題，請查看失敗訊息。您也可以選擇系統並點擊重新建立環境。

如需更多協助，請訪問 "NetApp Cloud Volumes ONTAP支持"。

完成後

- 如果您配置了 CIFS 共享，請授予使用者或群組對檔案和資料夾的權限，並驗證這些使用者是否可以存取共用並建立檔案。
- 如果要將配額套用於卷，請使用ONTAP系統管理員或ONTAP CLI。

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

  部署程序完成後，請勿修改 AWS 雲端入口網站中系統產生的Cloud Volumes ONTAP配置，尤其是系統標籤。對這些配置所做的任何變更都可能導致意外行為或資料遺失。

相關連結

- "規劃您的Cloud Volumes ONTAP配置"
- "使用快速部署在 AWS 中部署Cloud Volumes ONTAP"

在 **AWS Secret Cloud** 或 **AWS Top Secret Cloud** 中部署**Cloud Volumes ONTAP**

與標準 AWS 區域NetApp Console，您可以在"AWS 秘密雲"並且在"AWS 頂級機密雲"部署Cloud Volumes ONTAP，為您的雲端儲存提供企業級功能。 AWS Secret Cloud 和 Top Secret Cloud 是特定於美國情報界的封閉區域；本頁的說明僅適用於 AWS Secret Cloud 和 Top Secret Cloud 區域使用者。

開始之前

在開始之前，請先查看 AWS Secret Cloud 和 Top Secret Cloud 中支援的版本，並了解控制台中的私有模式。

- 查看 AWS Secret Cloud 和 Top Secret Cloud 中支援的以下版本：
  - Cloud Volumes ONTAP 9.12.1 P2
  - 控制台代理版本 3.9.32

    需要控制台代理程式才能在 AWS 中部署和管理Cloud Volumes ONTAP 。您將從安裝在控制台代理實例上的軟體登入控制台。 AWS Secret Cloud 和 Top Secret Cloud 不支援控制台的 SaaS 網站。
- 了解私人模式

  在 AWS Secret Cloud 和 Top Secret Cloud 中，控制台以_私有模式_運作。在私人模式下，控制台與 SaaS 圖層沒有連線。您可以透過可以存取控制台代理的本機基於 Web 的應用程式來存取控制台。

  要了解有關隱私模式工作原理的更多信息，請參閱"控制台中的私有部署模式"。

步驟 1：設定網絡

設定您的 AWS 網絡，以便Cloud Volumes ONTAP可以正常運作。

步驟

1. 選擇要啟動控制台代理實例和Cloud Volumes ONTAP實例的 VPC 和子網路。
2. 確保您的 VPC 和子網路將支援控制台代理和Cloud Volumes ONTAP之間的連線。
3. 設定到 Amazon Simple Storage Service（Amazon S3）服務的 VPC 端點。

   如果您想將冷資料從Cloud Volumes ONTAP到低成本物件存儲，則需要 VPC 端點。

步驟 2：設定權限

設定 IAM 策略和角色，為控制台代理程式和Cloud Volumes ONTAP提供在 AWS Secret Cloud 或 Top Secret Cloud 中執行操作所需的權限。

您需要針對以下各項制定 IAM 策略和 IAM 角色：

- 控制台代理實例
- Cloud Volumes ONTAP實例
- 對於 HA 對， Cloud Volumes ONTAP HA 中介實例（如果您要部署 HA 對）

步驟

1. 前往 AWS IAM 控制台並點擊 政策。
2. 為控制台代理實例建立策略。

> 您建立這些策略來支援 AWS 環境中的 S3 儲存桶。稍後建立儲存桶時，請確保儲存桶名稱以 `fabric-pool-`。此要求適用於 AWS Secret Cloud 和 Top Secret Cloud 區域。

秘密區域

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
```

```
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
```

```
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

絕密地區

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
```

```
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
```

```
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
```

```
        ]
}
```

3. 為Cloud Volumes ONTAP建立策略。

秘密區域

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

絕密地區

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

對於 HA 對，如果您打算部署Cloud Volumes ONTAP HA 對，請為 HA 中介建立策略。

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

4. 建立角色類型為 Amazon EC2 的 IAM 角色並附加您在前面步驟中建立的政策。

   創建角色：

   與政策類似，您應該為控制台代理設定一個 IAM 角色，為Cloud Volumes ONTAP節點設定一個 IAM 角色。對於 HA 對：與政策類似，您應該為控制台代理設定一個 IAM 角色，為Cloud Volumes ONTAP節點設定一個 IAM 角色，為 HA 中介設定一個 IAM 角色（如果您想要部署 HA 對）。

   選擇角色：

   啟動控制台代理實例時，必須選擇控制台代理 IAM 角色。當您從控制台建立Cloud Volumes ONTAP系統時，您可以選擇Cloud Volumes ONTAP的 IAM 角色。對於 HA 對，您可以在建立Cloud Volumes ONTAP系統時選擇Cloud Volumes ONTAP和 HA 中介的 IAM 角色。

步驟 3：設定 AWS KMS

如果您想要將 Amazon 加密與Cloud Volumes ONTAP結合使用，請確保符合 AWS 金鑰管理服務 (KMS) 的要求。

步驟

1. 確保您的帳戶或其他 AWS 帳戶中存在有效的客戶主金鑰 (CMK)。

   CMK 可以是 AWS 管理的 CMK 或客戶管理的 CMK。

2. 如果 CMK 位於與您計劃部署Cloud Volumes ONTAP 的帳戶不同的 AWS 帳戶中，則需要取得該金鑰的 ARN。

   建立Cloud Volumes ONTAP系統時，您需要向控制台提供 ARN。

3. 將執行個體的 IAM 角色新增至 CMK 的金鑰使用者清單。

這授予控制台使用 CMK 和Cloud Volumes ONTAP 的權限。

步驟 4：安裝控制台代理程式並設定控制台

在開始使用控制台在 AWS 中部署Cloud Volumes ONTAP之前，您必須安裝並設定控制台代理。它使控制台能夠管理公有Cloud Volumes ONTAP）內的資源和流程。

步驟

1. 取得由憑證授權單位 (CA) 簽署的、採用隱私增強郵件 (PEM) Base-64 編碼 X.509 格式的根憑證。請查閱您所在組織的政策和程序以取得證書。

   對於 AWS Secret Cloud 區域，您應該上傳 `NSS Root CA 2`證書，對於 Top Secret Cloud，`Amazon Root CA 4`證書。確保僅上傳這些憑證而不是整個鏈。證書鏈檔案很大，上傳可能會失敗。如果您有其他證書，您可以稍後上傳，如下一步所述。

   您需要在設定過程中上傳證書。控制台透過 HTTPS 向 AWS 發送請求時使用受信任的憑證。

2. 啟動控制台代理實例：
   a. 前往控制台的 AWS Intelligence Community Marketplace 頁面。
   b. 在「自訂啟動」標籤上，選擇從 EC2 控制台啟動執行個體的選項。
   c. 依照提示配置實例。

      配置實例時請注意以下事項：

      - 我們推薦 t3.xlarge。
      - 您必須選擇在設定權限時建立的 IAM 角色。
      - 您應該保留預設儲存選項。
      - 控制台代理程式所需的連線方法如下：SSH、HTTP 和 HTTPS。
3. 從與實例有連接的主機設定控制台：
   a. 開啟網頁瀏覽器並輸入 https://ipaddress其中 ipaddress 是安裝控制台代理程式的 Linux 主機的 IP 位址。
   b. 指定用於連接 AWS 服務的代理伺服器。
   c. 上傳您在步驟 1 中獲得的憑證。
   d. 依照提示設定新系統。
      - 系統詳細資料：輸入控制台代理的名稱和您的公司名稱。
      - 建立管理員使用者：為系統建立管理員使用者。

        該用戶帳戶在系統本機運行。無法透過控制台連線到 auth0 服務。

      - 審核：審核詳細信息，接受許可協議，然後選擇*設定*。
   e. 若要完成 CA 簽章憑證的安裝，請從 EC2 控制台重新啟動控制台代理程式執行個體。
4. 控制台代理重新啟動後，使用您在安裝精靈中建立的管理員使用者帳號登入。

步驟 **5**：（可選）安裝私有模式憑證

對於 AWS Secret Cloud 和 Top Secret Cloud 區域，此步驟是可選的，並且僅當您除了上一步中安裝的根憑證之外還有其他憑證時才需要執行此步驟。

步驟

1. 列出現有安裝的證書。
   a. 若要收集 occm 容器 docker id（標識名稱“ds-occm-1”），請執行以下命令：

   ```
   docker ps
   ```

   b. 若要進入 occm 容器，請執行下列命令：

   ```
   docker exec -it <docker-id> /bin/sh
   ```

   c. 若要從「TRUST_STORE_PASSWORD」環境變數收集密碼，請執行以下命令：

   ```
   env
   ```

   d. 若要列出信任庫中所有已安裝的證書，請執行以下命令並使用上一個步驟收集的密碼：

   ```
   keytool -list -v -keystore occm.truststore
   ```

2. 新增證書。
   a. 若要收集 occm 容器 docker id（標識名稱“ds-occm-1”），請執行以下命令：

   ```
   docker ps
   ```

   b. 若要進入 occm 容器，請執行下列命令：

   ```
   docker exec -it <docker-id> /bin/sh
   ```

   將新的證書文件保存在裡面。

   c. 若要從「TRUST_STORE_PASSWORD」環境變數收集密碼，請執行以下命令：

   ```
   env
   ```

   d. 若要將憑證新增至信任庫，請執行以下命令並使用上一個步驟中的密碼：

```
keytool -import -alias <alias-name> -file <certificate-file-name>
-keystore occm.truststore
```

e. 若要檢查憑證是否已安裝，請執行以下命令：

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

f. 若要退出 occm 容器，請執行下列命令：

```
exit
```

g. 若要重設 occm 容器，請執行下列命令：

```
docker restart <docker-id>
```

步驟 **6**：向控制台新增許可證

如果您從NetApp購買了許可證，則需要將其新增至控制台，以便在建立新的Cloud Volumes ONTAP系統時選擇該許可證。在將這些許可證與新的Cloud Volumes ONTAP系統關聯之前，它們將保持未指派狀態。

步驟

1. 從左側導覽選單中，選擇*Licenses and subscriptions*。
2. 在 * Cloud Volumes ONTAP* 面板上，選擇 檢視。
3. 在 * Cloud Volumes ONTAP* 標籤上，選擇 許可證**>**基於節點的許可證。
4. 按一下“未分配”。
5. 按一下「新增未指派的許可證」。
6. 輸入許可證的序號或上傳許可證文件。
7. 如果您還沒有許可證文件，則需要從 netapp.com 手動上傳許可證文件。
   a. 前往"NetApp許可證文件產生器"並使用您的NetApp支援網站憑證登入。
   b. 輸入您的密碼，選擇您的產品，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*。
   c. 選擇您是否希望透過電子郵件或直接下載接收 serialnumber.NLF JSON 檔案。
8. 按一下「新增許可證」。

結果

控制台會將許可證新增為未指派狀態，直到您將其與新的Cloud Volumes ONTAP系統關聯。您可以在左側導覽功能表的 **Licenses and subscriptions> Cloud Volumes ONTAP >** 檢視 **>** 授權 下看到授權。

步驟 7：從控制台啟動Cloud Volumes ONTAP

您可以透過在控制台中建立新系統來在 AWS Secret Cloud 和 Top Secret Cloud 中啟動Cloud Volumes ONTAP個體。

開始之前

對於 HA 對，需要金鑰對來啟用對 HA 中介的基於金鑰的 SSH 驗證。

步驟

1. 在「系統」頁面上，按一下「新增系統」。
2. 在「建立」下，選擇Cloud Volumes ONTAP。

   對於 HA：在 建立 下，選擇Cloud Volumes ONTAP或Cloud Volumes ONTAP HA。

3. 完成精靈中的步驟以啟動Cloud Volumes ONTAP系統。

> 透過精靈進行選擇時，請不要選擇*服務*下的*資料感知與合規性*和*備份到雲端*。在*預先配置套件*下，僅選擇*變更配置*，並確保您沒有選擇任何其他選項。 AWS Secret Cloud 和 Top Secret Cloud 區域不支援預先設定包，如果選擇，您的部署將會失敗。

在多個可用區中部署**Cloud Volumes ONTAP HA** 的注意事項

完成 HA 對嚮導時請注意以下事項。

- 在多個可用區 (AZ) 中部署Cloud Volumes ONTAP HA 時，您應該設定一個傳輸閘道。有關說明，請參閱"設定 AWS 中繼網關"。
- 由於發佈時 AWS Top Secret Cloud 中只有兩個可用可用區，因此請如下部署配置：
  - 節點 1：可用區 A
  - 節點 2：可用區 B
  - 調解員：可用區域 A 或 B

在單節點和 **HA** 節點中部署**Cloud Volumes ONTAP** 的注意事項

完成精靈時請注意以下事項：

- 您應該保留預設選項以使用產生的安全性群組。

  預先定義的安全性群組包含Cloud Volumes ONTAP成功運作所需的規則。如果您有使用自己的需求，可以參考下面的安全群組部分。

- 您必須選擇在準備 AWS 環境時所建立的 IAM 角色。
- 底層 AWS 磁碟類型適用於初始Cloud Volumes ONTAP磁碟區。

  您可以為後續磁碟區選擇不同的磁碟類型。

- AWS 磁碟的效能與磁碟大小相關。

  您應該選擇能夠提供所需持續效能的磁碟大小。有關 EBS 效能的更多詳細信息，請參閱 AWS 文件。

- 磁碟大小是系統上所有磁碟的預設大小。

  如果您稍後需要不同的大小，則可以使用進階分配選項來建立使用特定大小磁碟的聚合。

結果

Cloud Volumes ONTAP已啟動。您可以在*審計*頁面追蹤進度。

步驟 **8**：安裝資料分層的安全性證書

您需要手動安裝安全性憑證才能在 AWS Secret Cloud 和 Top Secret Cloud 區域中啟用資料分層。

開始之前

1. 建立 S3 儲存桶。

   確保儲存桶名稱帶有前綴 `fabric-pool-.`例如 `fabric-pool-testbucket`。

2. 保留您安裝的根證書 `step 4`便利。

步驟

1. 複製您安裝的根證書中的文本 `step 4`。
2. 使用 CLI 安全地連線到Cloud Volumes ONTAP系統。
3. 安裝根證書。您可能需要按 `ENTER`多次鍵入：

```
security certificate install -type server-ca -cert-name <certificate-
name>
```

4. 出現提示時，輸入複製的整個文本，包括 `----- BEGIN CERTIFICATE -----`到 `----- END CERTIFICATE -----`。
5. 保留 CA 簽署的數位憑證的副本以供日後參考。
6. 保留 CA 名稱和憑證序號。
7. 為 AWS Secret Cloud 和 Top Secret Cloud 區域配置物件儲存： `set -privilege advanced -confirmations off`
8. 運行此命令來配置物件儲存。

   所有 Amazon 資源名稱 (ARN) 應以 `-iso-b`， 例如 `arn:aws-iso-b`。例如，如果資源需要具有區域的 ARN，對於 Top Secret Cloud，請使用以下命名約定 `us-iso-b`對於 `-server`旗幟。對於 `AWS Secret Cloud`，使用 `us-iso-b-1`。

```
storage aggregate object-store config create -object-store-name
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl
-enabled true -port 443
```

9. 驗證物件儲存是否已成功建立： `storage aggregate object-store show -instance`
10. 將物件存儲附加到聚合。對於每個新的聚合體都應重複此操作： `storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>`

開始使用 Microsoft Azure

了解 Azure 中的Cloud Volumes ONTAP部署選項

NetApp提供了兩種在 Azure 上部署Cloud Volumes ONTAP 的選項。 Cloud Volumes ONTAP傳統上依賴NetApp Console進行部署和編排。從Cloud Volumes ONTAP 9.16.1 開始，您可以利用 Azure 市場直接部署，這是一個簡化的過程，可以存取有限但仍然強大的Cloud Volumes ONTAP功能和選項。

當您直接從 Azure 市場部署Cloud Volumes ONTAP時，您無需設定控制台代理程式或符合透過控制台部署Cloud Volumes ONTAP所需的其他安全性和入職標準。從 Azure 市場，您只需點擊幾下即可快速部署Cloud Volumes ONTAP ，並在您的環境中探索其核心特性和功能。

在 Azure 市集完成部署後，您可以在控制台中發現這些系統。發現後，您可以將它們作為Cloud Volumes ONTAP系統進行管理，並利用所有控制台功能。請參閱"在控制台中發現已部署的系統" 。

以下是兩個選項之間的功能比較。請注意，透過 Azure 市場部署的獨立執行個體的功能在控制台中被發現時會發生變化。

	Azure 市場	**NetApp Console**
入職訓練	更短、更簡單，直接部署所需的準備工作最少	更長的入職流程，包括控制台代理的安裝
支援的虛擬機器 **(VM)** 類型	Eds_v5 和 Ls_v3 實例類型	全方位的 VM 類型。https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html["Azure 中支援的配置"^]
執照	免費許可證	任何基於容量的許可證。"Cloud Volumes ONTAP許可"
* NetApp支援*	不包括	根據許可證類型可用
容量	最多 500 GiB	可透過配置擴展
部署模型	單可用區（AZ）高可用（HA）模式部署	所有支援的配置，包括單節點和 HA 模式、單 AZ 和多 AZ 部署
支援的磁碟類型	高級 SSD v2 託管磁碟	更廣泛的支持。"Cloud Volumes ONTAP的預設配置"
寫入速度（快速寫入模式）	不支援	根據您的配置，支援。"了解Cloud Volumes ONTAP中的寫入速度" 。
編排功能	無法使用	根據許可證類型，可透過NetApp Console取得

	Azure 市場	NetApp Console
支援的儲存虛擬機器數量	每個部署一個	根據您的配置，多個儲存虛擬機器。"支援的儲存虛擬機器數量"
更改實例類型	不支援	支援
* FabricPool分層*	不支援	支援

相關連結

- Azure 市場直接部署："從 Azure 市場部署Cloud Volumes ONTAP"
- 透過控制台部署："Azure 中的Cloud Volumes ONTAP快速入門"
- "NetApp Console文檔"

NetApp Console入門

Azure 中的Cloud Volumes ONTAP快速入門

只需幾個步驟即可開始使用Cloud Volumes ONTAP for Azure。


建立控制台代理

如果你沒有 "控制台代理"但是，您需要建立一個。 "了解如何在 Azure 中建立控制台代理"

請注意，如果您想在沒有網路存取的子網路中部署Cloud Volumes ONTAP ，則需要手動安裝控制台代理程式並存取在該控制台代理程式上執行的NetApp Console。 "了解如何在沒有網路存取的地方手動安裝控制台代理"


規劃您的配置

控制台提供符合您的工作負載要求的預先配置包，或者您可以建立自己的配置。如果您選擇自己的配置，您應該了解可用的選項。有關信息，請參閱"在 Azure 中規劃您的Cloud Volumes ONTAP配置"。


設定網路

1. 確保您的 VNet 和子網路將支援控制台代理程式和Cloud Volumes ONTAP之間的連線。
2. 為NetApp AutoSupport啟用從目標 VPC 的出站網際網路存取。

   如果您在沒有網路存取的位置部署Cloud Volumes ONTAP，則不需要執行此步驟。

"了解有關網絡要求的更多信息" 。


啟動Cloud Volumes ONTAP

按一下“新增系統”，選擇您想要部署的系統類型，然後完成精靈中的步驟。"閱讀逐步說明" 。

相關連結

- "從控制台建立控制台代理"

- "從 Azure 市集建立控制台代理"
- "在 Linux 主機上安裝控制台代理軟體"
- "控制台如何處理權限"

在 **Azure** 中規劃您的**Cloud Volumes ONTAP**配置

在 Azure 中部署Cloud Volumes ONTAP時，您可以選擇符合您的工作負載需求的預先設定係統，也可以建立自己的設定。如果您選擇自己的配置，您應該了解可用的選項。

選擇**Cloud Volumes ONTAP**許可證

Cloud Volumes ONTAP有多種授權選項。每個選項都可以讓您選擇符合您需求的消費模式。

- "了解Cloud Volumes ONTAP的授權選項"
- "了解如何設定許可"

選擇支援的區域

大多數 Microsoft Azure 區域都支援Cloud Volumes ONTAP 。 "查看支援區域的完整列表" 。

選擇受支援的 **VM** 類型

Cloud Volumes ONTAP支援多種 VM 類型，視您選擇的授權類型而定。

"Azure 中Cloud Volumes ONTAP支援的配置"

了解儲存限制

Cloud Volumes ONTAP系統的原始容量限制與許可證相關。額外的限制會影響聚合和磁碟區的大小。在規劃配置時您應該注意這些限制。

"Azure 中Cloud Volumes ONTAP的儲存限制"

在 **Azure** 中調整系統大小

調整Cloud Volumes ONTAP系統的大小可以幫助您滿足效能和容量要求。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

查看受支援的虛擬機器類型 "Cloud Volumes ONTAP發行說明"然後查看有關每種受支援的 VM 類型的詳細資訊。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：記憶體最佳化虛擬機器大小"

Azure 磁碟類型（單節點系統）

為Cloud Volumes ONTAP建立磁碟區時，您需要選擇Cloud Volumes ONTAP用作磁碟的底層雲端儲存。

單節點系統可以使用下列類型的 Azure 託管磁碟：

- 進階 *SSD* 託管磁碟 以更高的成本為 I/O 密集型工作負載提供高效能。
- 與高級 SSD 託管磁碟相比，高級 *SSD v2* 託管磁碟 以更低的成本提供更高的效能和更低的延遲。
- _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 並且想要降低成本，那麼「標準 HDD 託管磁碟」是一個不錯的選擇。

有關這些磁碟用例的更多詳細信息，請參閱 "Microsoft Azure 文件：Azure 中有哪些磁碟類型？"。

具有 **HA** 對的 **Azure** 磁碟類型

HA 系統使用進階 SSD 共享託管磁碟，它們都以更高的成本為 I/O 密集型工作負載提供高效能。 9.12.1 版本之前建立的 HA 部署使用進階頁面 blob。

Azure 磁碟大小

啟動Cloud Volumes ONTAP實例時，您必須選擇聚合的預設磁碟大小。 NetApp Console將此磁碟大小用於初始聚合，以及使用簡單設定選項時建立的任何其他聚合。您可以透過以下方式建立使用不同於預設磁碟大小的聚合："使用進階分配選項" 。

聚合中的所有磁碟必須具有相同的大小。

選擇磁碟大小時，您應該考慮幾個因素。磁碟大小會影響您支付的儲存費用、您可以在聚合中建立的磁碟區的大小、 Cloud Volumes ONTAP可用的總容量以及儲存效能。

Azure Premium Storage 的效能與磁碟大小相關。更大的磁碟可提供更高的 IOPS 和吞吐量。例如，選擇 1 TiB 磁碟可以提供比 500 GiB 磁碟更好的效能，但成本更高。

標準儲存的磁碟大小之間沒有效能差異。您應該根據所需的容量來選擇磁碟大小。

請參閱 Azure 以了解按磁碟大小劃分的 IOPS 和吞吐量：

- "Microsoft Azure：託管磁碟定價"
- "Microsoft Azure：Page Blob 定價"

查看預設系統磁碟

除了用戶資料的儲存之外，控制台還購買了Cloud Volumes ONTAP系統資料（啟動資料、根資料、核心資料和NVRAM）的雲端儲存。出於規劃目的，在部署Cloud Volumes ONTAP之前查看這些詳細資訊可能會有所幫助。

"查看 Azure 中Cloud Volumes ONTAP系統資料的預設磁碟" 。

控制台代理還需要係統磁碟。 "查看控制台代理預設配置的詳細信息" 。

收集網路資訊

在 Azure 中部署Cloud Volumes ONTAP時，您需要指定有關虛擬網路的詳細資訊。您可以使用工作表從管理員收集資訊。

Azure 資訊	你的價值
地區	

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

選擇寫入速度

控制台可讓您選擇Cloud Volumes ONTAP的寫入速度設定。在選擇寫入速度之前，您應該了解正常設定和高設定之間的差異以及使用高寫入速度時的風險和建議。"了解有關寫入速度的更多信息" 。

選擇卷使用情況設定檔

ONTAP包含多種儲存效率功能，可減少您所需的總儲存量。在控制台中建立磁碟區時，您可以選擇啟用這些功能的設定檔或停用這些功能的設定檔。您應該了解有關這些功能的更多信息，以幫助您決定使用哪個配置文件。

NetApp儲存效率功能有以下優勢：

精簡配置

向主機或使用者提供比實體儲存池中實際擁有的更多的邏輯儲存。不是預先分配儲存空間，而是在寫入資料時動態地將儲存空間分配給每個磁碟區。

重複資料刪除

透過定位相同的資料塊並將其替換為對單一共享區塊的引用來提高效率。該技術透過消除駐留在同一磁碟區中的冗餘資料區塊來減少儲存容量需求。

壓縮

透過壓縮主儲存、輔助儲存和歸檔儲存磁碟區內的資料來減少儲存資料所需的實體容量。

為Cloud Volumes ONTAP設定 Azure 網路

NetApp Console負責設定Cloud Volumes ONTAP的網路元件，例如 IP 位址、網路遮罩和路由。您需要確保可以存取外部網路、有足夠的私人 IP 位址、有正確的連線等等。

Cloud Volumes ONTAP的要求

Azure 中必須符合下列網路需求。

出站互聯網訪問

Cloud Volumes ONTAP系統需要出站網際網路存取才能存取外部端點以實現各種功能。如果這些端點在具有嚴格安全要求的環境中被阻止， Cloud Volumes ONTAP將無法正常運作。

控制台代理也會聯絡多個端點以進行日常操作。有關端點的信息，請參閱 "查看從控制台代理聯繫的端點"和 "準備好使用控制台的網絡"。

Cloud Volumes ONTAP端點

Cloud Volumes ONTAP使用這些端點與各種服務進行通訊。

端點	適用於	目的	部署模式	不可用時的影響
\ https://netapp-cloud-account.auth0.com	驗證	用於控制台中的身份驗證。	標準和限制模式。	用戶身份驗證失敗，以下服務仍然不可用： • Cloud Volumes ONTAP服務 • ONTAP服務 • 協定和代理服務
https://vault.azure.net	金鑰保管庫	用於使用客戶管理金鑰 (CMK) 時從 Azure Key Vault 擷取客戶端金鑰。	標準、受限和私人模式。	Cloud Volumes ONTAP服務無法使用。
\ https://api.bluexp.netapp.com/tenancy	租賃	用於從控制台檢索Cloud Volumes ONTAP資源以授權資源和使用者。	標準和限制模式。	Cloud Volumes ONTAP資源和使用者未獲得授權。
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	用於將AutoSupport遙測資料傳送給NetApp支援。	標準和限制模式。	AutoSupport資訊仍未送達。
\ https://management.azure.com \ https://login.microsoftonline.com \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://core.windows.net	公共區域	與 Azure 服務通訊。	標準、受限和私人模式。	Cloud Volumes ONTAP無法與 Azure 服務通訊以對 Azure 中的控制台執行特定操作。
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	中國區	與 Azure 服務通訊。	標準、受限和私人模式。	Cloud Volumes ONTAP無法與 Azure 服務通訊以對 Azure 中的控制台執行特定操作。

端點	適用於	目的	部署模式	不可用時的影響
\ https://management.microsoftazure.de \ https://login.microsoftonline.de \ https://blob.core.cloudapi.de \ https://core.cloudapi.de	德國地區	與 Azure 服務通訊。	標準、受限和私人模式。	Cloud Volumes ONTAP無法與 Azure 服務通訊以對 Azure 中的控制台執行特定操作。
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	政府區域	與 Azure 服務通訊。	標準、受限和私人模式。	Cloud Volumes ONTAP無法與 Azure 服務通訊以對 Azure 中的控制台執行特定操作。
\ https://management.azure.microsoft.scloud \ https://login.microsoftonline.microsoft.scloud \ https://blob.core.microsoft.scloud \ https://core.microsoft.scloud	政府國防部區	與 Azure 服務通訊。	標準、受限和私人模式。	Cloud Volumes ONTAP無法與 Azure 服務通訊以對 Azure 中的控制台執行特定操作。

NetApp Console代理程式的網路代理程式配置

您可以使用NetApp Console代理程式的代理伺服器設定來啟用來自Cloud Volumes ONTAP 的外部網路存取。控制台支援兩種類型的代理：

- 明確代理：來自Cloud Volumes ONTAP 的出站流量使用在控制台代理的代理配置期間指定的代理伺服器的 HTTP 位址。管理員可能還配置了使用者憑證和根 CA 憑證以進行額外的身份驗證。Cloud Volumes ONTAP 顯式代理程式有可用的根 CA 證書，請確保使用 "ONTAP CLI：安全性憑證安裝"命令。
- 透明代理：網路配置為透過控制台代理的代理程式自動路由來自Cloud Volumes ONTAP 的出站流量。設定透明代理時，管理員只需要提供用於從Cloud Volumes ONTAP進行連接的根 CA 證書，而不是代理伺服器的 HTTP 位址。確保使用以下方式取得相同的根 CA 憑證並將其上傳到您的Cloud Volumes ONTAP系統 "ONTAP CLI：安全性憑證安裝"命令。

有關配置代理伺服器的信息，請參閱 "配置控制台代理以使用代理伺服器"。

IP 位址

控制台會自動為 Azure 中的Cloud Volumes ONTAP指派所需數量的私有 IP 位址。您需要確保您的網路有足夠的可用私人 IP 位址。

分配給 Cloud Volumes ONTAP 的 LIF 數量取決於您部署的是單節點系統還是 HA 配對。LIF 是與實體連接埠相關聯的 IP 位址。管理工具（例如 SnapCenter）需要 SVM 管理 LIF。

> iSCSI LIF 透過 iSCSI 協定提供用戶端訪問，並被系統用於其他重要的網路工作流程。這些 LIF 是必需的，不應刪除。

單節點系統的 **IP** 位址

Console 會為單節點系統指派 5 或 6 個 IP 位址：

- 叢集管理IP
- 節點管理IP
- SnapMirror的群集間 IP
- NFS/CIFS IP
- iSCSI IP

> iSCSI IP 透過 iSCSI 協定提供客戶端存取。系統也將其用於其他重要的網路工作流程。此 LIF 是必需的，不應刪除。

- SVM 管理（可選 - 預設未配置）

HA 對的 **IP** 位址

控制台在部署期間將 IP 位址指派給 4 個 NIC（每個節點）。

請注意，NetApp Console 會在 HA 配對上建立 SVM 管理 LIF，但不會在 Azure 中的單節點系統上建立。

NIC0

- 節點管理IP
- 群集間 IP
- iSCSI IP

> iSCSI IP 透過 iSCSI 協定提供客戶端存取。系統也將其用於其他重要的網路工作流程。此 LIF 是必需的，不應刪除。

NIC1

- 叢集網路IP

NIC2

- 叢集互連 IP (HA IC)

NIC3

- Pageblob NIC IP（磁碟存取）

NIC3 僅適用於使用頁 Blob 儲存的 HA 部署。

上述 IP 位址在故障轉移事件中不會遷移。

此外，還配置了 4 個前端 IP（FIP）以在故障轉移事件時進行遷移。這些前端 IP 位於負載平衡器中。

- 叢集管理IP
- NodeA 資料 IP (NFS/CIFS)
- NodeB資料IP（NFS/CIFS）
- SVM 管理 IP

與 **Azure** 服務的安全連線

預設情況下，控制台啟用 Azure 專用鏈接，用於Cloud Volumes ONTAP和 Azure 頁 Blob 儲存帳戶之間的連接。

在大多數情況下，您無需執行任何操作 - 控制台會為您管理 Azure 專用連結。但是如果您使用 Azure 私人 DNS，則需要編輯設定檔。您還應該了解 Azure 中控制台代理程式的位置需求。

如果您的業務需要，您也可以停用專用連結連線。如果停用該鏈接，控制台會將Cloud Volumes ONTAP配置為使用服務端點。

"了解有關將 Azure Private Links 或服務端點與Cloud Volumes ONTAP結合使用的更多信息" 。

Azure VNet 加密的網路

Cloud Volumes ONTAP 支援 "Azure Virtual Network（VNet）加密"加密 VNet 內或對等 VNet 之間的 VM 對 VM 流量。此功能在 Azure VNet 層配置，與 Cloud Volumes ONTAP 拓撲（單節點或 HA）無關。

您只需確保虛擬機器網路卡已啟用加速網路，並在啟用功能之前查看 Azure VNet 加密需求和限制。您不應修改 NetApp 託管負載平衡器物件。

"Azure 文件：VNet 加密與 Accelerated Networking"。

與其他**ONTAP**系統的連接

要在 Azure 中的Cloud Volumes ONTAP系統和其他網路中的ONTAP系統之間複製數據，您必須在 Azure VNet 和其他網路（例如您的公司網路）之間建立 VPN 連線。

有關說明，請參閱 "Microsoft Azure 文件：在 Azure 入口網站中建立網站到網站連接"。

HA 互連埠

Cloud Volumes ONTAP HA 對包含 HA 互連，這使得每個節點能夠持續檢查其夥伴節點是否正常運行，並為對方的非揮發性記憶體鏡像日誌資料。 HA 互連使用 TCP 連接埠 10006 進行通訊。

預設情況下，HA 互連 LIF 之間的通訊是開放的，且此連接埠沒有安全群組規則。但是，如果您在 HA 互連 LIF 之間建立防火牆，則需要確保 TCP 流量對連接埠 10006 開放，以便 HA 對可以正常運作。

Azure 資源組中只有一個 HA 對

您必須為在 Azure 中部署的每個Cloud Volumes ONTAP HA 對使用一個專用資源群組。一個資源組中僅支援一個 HA 對。

如果您嘗試在 Azure 資源組中部署第二個Cloud Volumes ONTAP HA 對，控制台會遇到連線問題。

安全群組規則

控制台建立 Azure 安全性群組，其中包含Cloud Volumes ONTAP成功執行的入站和出站規則。 "查看控制台代理程式的安全性群組規則" 。

Cloud Volumes ONTAP的 Azure 安全性群組需要開啟適當的連接埠以進行節點之間的內部通訊。 "了解ONTAP內部端口" 。

我們不建議修改預先定義的安全性群組或使用自訂安全群組。但是，如果必須這樣做，請注意，部署過程要求Cloud Volumes ONTAP系統在自己的子網路內擁有完全存取權限。部署完成後，如果決定修改網路安全群組，請確保保持叢集連接埠和 HA 網路連接埠開放。這確保了Cloud Volumes ONTAP叢集內的無縫通訊（節點之間的任意通訊）。

單節點系統的入站規則

新增Cloud Volumes ONTAP系統並選擇預先定義安全性群組時，您可以選擇允許下列其中的流量：

- 僅限選定的 **VNet**：入站流量的來源是Cloud Volumes ONTAP系統的 VNet 子網路範圍和控制台代理程式所在的 VNet 子網路範圍。這是推薦的選項。
- 所有 **VNets**：入站流量的來源是 0.0.0.0/0 IP 範圍。
- 已停用：此選項限制對您的儲存帳戶的公共網路訪問，並停用Cloud Volumes ONTAP系統的資料分層。如果由於安全法規和政策，您的私人 IP 位址即使在同一個 VNet 內也不應該暴露，那麼建議使用此選項。

優先權和名稱	連接埠和協定	來源和目的地	描述
1000 入站_ssh	22 TCP	任意到任意	透過 SSH 存取叢集管理 LIF 或節點管理 LIF 的 IP 位址
1001 入站 http	80 TCP	任意到任意	使用叢集管理 LIF 的 IP 位址透過 HTTP 存取ONTAP System Manager Web 控制台
1002 inbound_111_tcp	111 TCP	任意到任意	NFS 的遠端過程調用
1003 inbound_111_udp	111 UDP	任意到任意	NFS 的遠端過程調用
1004 inbound_139	139 TCP	任意到任意	CIFS 的 NetBIOS 服務會話
1005 入站_161-162 _tcp	161-162 TCP	任意到任意	簡單網路管理協議
1006 入站_161-162 _udp	161-162 UDP	任意到任意	簡單網路管理協議

優先權和名稱	連接埠和協定	來源和目的地	描述
1007 inbound_443	443 TCP	任意到任意	使用叢集管理 LIF 的 IP 位址與控制台代理程式建立連線並透過 HTTPS 存取ONTAP System Manager Web 控制台
1008 inbound_445	445 TCP	任意到任意	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
1009 inbound_635_tcp	635 TCP	任意到任意	NFS 掛載
1010 inbound_635_udp	635 UDP	任意到任意	NFS 掛載
1011 inbound_749	749 TCP	任意到任意	Kerberos
1012 inbound_2049_tcp	2049 TCP	任意到任意	NFS 伺服器守護程式
1013 inbound_2049_udp	2049 UDP	任意到任意	NFS 伺服器守護程式
1014 inbound_3260	3260 TCP	任意到任意	透過 iSCSI 資料 LIF 進行 iSCSI 訪問
1015 入站_4045-4046_tcp	4045-4046 TCP	任意到任意	NFS 鎖定守護程式和網路狀態監視器
1016 入站_4045-4046_udp	4045-4046 UDP	任意到任意	NFS 鎖定守護程式和網路狀態監視器
1017 inbound_10000	10000 TCP	任意到任意	使用 NDMP 備份
1018 入站_11104-11105	11104-11105 TCP	任意到任意	SnapMirror資料傳輸
3000 入站拒絕 _所有_tcp	任意連接埠 TCP	任意到任意	阻止所有其他 TCP 入站流量
3001 入站拒絕 _所有 udp	任意連接埠 UDP	任意到任意	阻止所有其他 UDP 入站流量
65000 允許 VnetInBound	任意連接埠任意協定	虛擬網路到虛擬網絡	來自 VNet 內部的入站流量
65001 允許 Azure 負載平衡器入站	任意連接埠任意協定	AzureLoadBalancer 到任意	來自 Azure 標準負載平衡器的資料流量
65500 拒絕所有入站	任意連接埠任意協定	任意到任意	阻止所有其他入站流量

HA 系統的入站規則

新增Cloud Volumes ONTAP系統並選擇預先定義安全性群組時，您可以選擇允許下列其中的流量：

- 僅限選定的 **VNet**：入站流量的來源是Cloud Volumes ONTAP系統的 VNet 子網路範圍和控制台代理程式所在的 VNet 子網路範圍。這是推薦的選項。
- 所有 **VNets**：入站流量的來源是 0.0.0.0/0 IP 範圍。

HA 系統的入站規則比單節點系統少，因為入站資料流量會經過 Azure Standard Load Balancer。因此，來自 Load Balancer 的流量應該保持開放狀態，如「AllowAzureLoadBalancerInBound」規則所示。

- 已停用：此選項限制對您的儲存帳戶的公共網路訪問，並停用Cloud Volumes ONTAP系統的資料分層。如果由於安全法規和政策，您的私人 IP 位址即使在同一個 VNet 內也不應該暴露，那麼建議使用此選項。

優先權和名稱	連接埠和協定	來源和目的地	描述
100 inbound_443	443 任何協議	任意到任意	使用叢集管理 LIF 的 IP 位址與控制台代理程式建立連線並透過 HTTPS 存取ONTAP System Manager Web 控制台
101 inbound_111_tcp	111 任何協議	任意到任意	NFS 的遠端過程調用
102 inbound_2049_tcp	2049 任何協議	任意到任意	NFS 伺服器守護程式
111 入站_ssh	22 任何協議	任意到任意	透過 SSH 存取叢集管理 LIF 或節點管理 LIF 的 IP 位址
121 inbound_53	53 任何協議	任意到任意	DNS 和 CIFS
65000 允許 VnetInBound	任意連接埠任意協定	虛擬網路到虛擬網絡	來自 VNet 內部的入站流量
65001 允許 Azure 負載平衡器入站	任意連接埠任意協定	AzureLoadBalancer 到任意	來自 Azure 標準負載平衡器的資料流量
65500 拒絕所有入站	任意連接埠任意協定	任意到任意	阻止所有其他入站流量

出站規則

Cloud Volumes ONTAP的預設安全群組開啟所有出站流量。如果可以接受，請遵循基本的出站規則。如果您需要更嚴格的規則，請使用進階出站規則。

基本出站規則

Cloud Volumes ONTAP的預設安全群組包括以下出站規則。

港口	協定	目的
全部	所有 TCP	所有出站流量
全部	所有 UDP	所有出站流量

高級出站規則

如果您需要對出站流量製定嚴格的規則，則可以使用下列資訊僅開啟Cloud Volumes ONTAP出站通訊所需的連接埠。

來源是Cloud Volumes ONTAP系統上的介面（IP 位址）。

服務	港口	協定	來源	目的地	目的
活動目錄	88	TCP	節點管理 LIF	Active Directory 林	Kerberos V 驗證
	137	UDP	節點管理 LIF	Active Directory 林	NetBIOS 名稱服務
	138	UDP	節點管理 LIF	Active Directory 林	NetBIOS 資料封包服務
	139	TCP	節點管理 LIF	Active Directory 林	NetBIOS 服務會話
	389	TCP 和 UDP	節點管理 LIF	Active Directory 林	LDAP
	445	TCP	節點管理 LIF	Active Directory 林	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
	464	TCP	節點管理 LIF	Active Directory 林	Kerberos V 更改和設定密碼（SET_CHANGE）
	464	UDP	節點管理 LIF	Active Directory 林	Kerberos 金鑰管理
	749	TCP	節點管理 LIF	Active Directory 林	Kerberos V 更改和設定密碼（RPCSEC_GSS）
	88	TCP	資料 LIF（NFS、CIFS、iSCSI）	Active Directory 林	Kerberos V 驗證
	137	UDP	資料 LIF（NFS、CIFS）	Active Directory 林	NetBIOS 名稱服務
	138	UDP	資料 LIF（NFS、CIFS）	Active Directory 林	NetBIOS 資料封包服務
	139	TCP	資料 LIF（NFS、CIFS）	Active Directory 林	NetBIOS 服務會話
	389	TCP 和 UDP	資料 LIF（NFS、CIFS）	Active Directory 林	LDAP
	445	TCP	資料 LIF（NFS、CIFS）	Active Directory 林	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
	464	TCP	資料 LIF（NFS、CIFS）	Active Directory 林	Kerberos V 更改和設定密碼（SET_CHANGE）
	464	UDP	資料 LIF（NFS、CIFS）	Active Directory 林	Kerberos 金鑰管理
	749	TCP	資料 LIF（NFS、CIFS）	Active Directory 林	Kerberos V 更改和設定密碼（RPCSEC_GSS）
AutoSupport	HTTPS	443	節點管理 LIF	mysupport.netapp.com	AutoSupport （預設為 HTTPS）
	HTTP	80	節點管理 LIF	mysupport.netapp.com	AutoSupport （僅當傳輸協定從 HTTPS 變更為 HTTP 時）
	TCP	3128	節點管理 LIF	控制台代理	如果出站網路連線不可用，則透過控制台代理上的代理伺服器傳送AutoSupport訊息

服務	港口	協定	來源	目的地	目的
配置備份	HTTP	80	節點管理 LIF	http://<控制台代理 IP 位址>/occm/offboxconfig	將配置備份傳送到控制台代理程式。"ONTAP文檔" 。
DHCP	68	UDP	節點管理 LIF	DHCP	DHCP 用戶端首次設定
DHCP服務	67	UDP	節點管理 LIF	DHCP	DHCP 伺服器
DNS	53	UDP	節點管理 LIF 和資料 LIF（NFS、CIFS）	DNS	DNS
NDMP	18600–18699	TCP	節點管理 LIF	目標伺服器	NDMP 拷貝
SMTP	25	TCP	節點管理 LIF	郵件伺服器	SMTP 警報，可用於AutoSupport
SNMP	161	TCP	節點管理 LIF	監控伺服器	透過 SNMP 陷阱進行監控
	161	UDP	節點管理 LIF	監控伺服器	透過 SNMP 陷阱進行監控
	162	TCP	節點管理 LIF	監控伺服器	透過 SNMP 陷阱進行監控
	162	UDP	節點管理 LIF	監控伺服器	透過 SNMP 陷阱進行監控
SnapMirror	11104	TCP	集群間 LIF	ONTAP叢集間 LIF	SnapMirror群集間通訊會話的管理
	11105	TCP	集群間 LIF	ONTAP叢集間 LIF	SnapMirror資料傳輸
系統日誌	514	UDP	節點管理 LIF	Syslog伺服器	Syslog 轉送訊息

控制台代理的要求

如果您尚未建立控制台代理，您也應該查看控制台代理的網路需求。

- "查看控制台代理程式的網路要求"
- "Azure 中的安全性群組規則"

相關主題

- "驗證Cloud Volumes ONTAP 的AutoSupport設置"
- "了解ONTAP內部端口" 。

設定**Cloud Volumes ONTAP**以在 **Azure** 中使用客戶管理的金鑰

使用具有 Microsoft 管理金鑰的 Azure 儲存服務加密，資料會在 Azure 中的Cloud Volumes ONTAP上自動加密。但是您可以按照本頁上的步驟使用您自己的加密金鑰。

資料加密概述

Cloud Volumes ONTAP資料在 Azure 中自動使用 "Azure 儲存服務加密"。預設實作使用 Microsoft 管理的金鑰。無需設定。

如果您想將客戶管理的金鑰與Cloud Volumes ONTAP一起使用，則需要完成以下步驟：

1. 從 Azure 建立一個金鑰保管庫，然後在該保管庫中產生一個金鑰。
2. 從NetApp Console，使用 API 建立使用金鑰的Cloud Volumes ONTAP系統。

資料如何加密

控制台使用磁碟加密集，從而可以透過託管磁碟而不是頁面 blob 來管理加密金鑰。任何新的資料磁碟也使用相同的磁碟加密集。較低版本將使用 Microsoft 管理的金鑰，而不是客戶管理的金鑰。

建立配置為使用客戶管理金鑰的Cloud Volumes ONTAP系統後， Cloud Volumes ONTAP資料將如下加密。

Cloud Volumes ONTAP配置	用於密鑰加密的系統磁碟	用於密鑰加密的資料磁碟
單節點	• 引導 • 核 • NVRAM	• 根 • 數據
具有頁面 Blob 的 Azure HA 單可用性區域	• 引導 • 核 • NVRAM	沒有任何
具有共用託管磁碟的 Azure HA 單可用性區域	• 引導 • 核 • NVRAM	• 根 • 數據
具有共用託管磁碟的 Azure HA 多個可用性區域	• 引導 • 核 • NVRAM	• 根 • 數據

Cloud Volumes ONTAP的所有 Azure 儲存帳戶均使用客戶管理的金鑰加密。如果您想在建立儲存帳戶期間對其進行加密，則必須在Cloud Volumes ONTAP建立請求中建立並提供資源的 ID。這適用於所有類型的部署。如果您不提供，儲存帳戶仍將被加密，但控制台首先使用 Microsoft 管理的金鑰加密建立儲存帳戶，然後更新儲存帳戶以使用客戶管理的金鑰。

Cloud Volumes ONTAP中的金鑰輪換

配置加密金鑰時，必須使用 Azure 入口網站來設定並啟用自動金鑰輪替。建立並啟用新版本的加密金鑰可確保Cloud Volumes ONTAP可以自動偵測並使用最新的金鑰版本進行加密，確保您的資料保持安全而無需人工幹預。

有關配置金鑰和設定金鑰輪換的信息，請參閱以下 Microsoft Azure 文件主題：

- "在 Azure Key Vault 中配置加密金鑰自動輪換"
- "Azure PowerShell - 啟用客戶管理的金鑰"

配置金鑰後，請確保已選擇 "啟用自動旋轉"，以便Cloud Volumes ONTAP可以在先前的金鑰過期時使用新的金鑰。如果您未在 Azure 入口網站上啟用此選項， Cloud Volumes ONTAP將無法自動偵測新金鑰，這可能會導致儲存設定問題。

建立使用者分配的託管標識

您可以選擇建立稱為使用者指派的託管識別碼的資源。這樣做可以讓您在建立Cloud Volumes ONTAP系統時加密您的儲存帳戶。我們建議在建立金鑰保管庫和產生金鑰之前建立此資源。

此資源具有以下 ID： `userassignedidentity` 。

步驟

1. 在 Azure 中，前往 Azure 服務並選擇 託管識別。
2. 按一下“建立”。
3. 提供以下詳細資訊：
   - 訂閱：選擇訂閱。我們建議選擇與控制台代理的訂閱相同的訂閱。
   - 資源組：使用現有資源組或建立新的資源組。
   - 區域：可選，選擇與控制台代理相同的區域。
   - 名稱：輸入資源的名稱。
4. （可選）新增標籤。
5. 按一下“建立”。

建立金鑰保管庫並產生金鑰

金鑰保管庫必須位於您計劃建立Cloud Volumes ONTAP系統的相同 Azure 訂閱和區域中。

如果你建立了使用者分配的託管標識，在建立金鑰保管庫時，也應該為金鑰保管庫建立存取策略。

步驟

1. "在 Azure 訂閱中建立金鑰保管庫" 。

   請注意密鑰保管庫的以下要求：

   - 密鑰保管庫必須與Cloud Volumes ONTAP系統位於同一區域。
   - 應啟用以下選項：
     - 軟刪除（此選項預設為啟用，但不能停用）
     - 清除保護
     - **Azure Disk Encryption** 磁碟區加密（適用於單節點系統、多個區域中的 HA 配對以及 HA 單一 AZ 部署）

       使用 Azure 客戶管理加密金鑰的前提是為金鑰保管庫啟用 Azure 磁碟加密。
   - 如果建立了使用者指派的託管標識，則應啟用下列選項：
     - 保險庫存取保單

2. 如果選擇了“保管庫存取原則”，請按一下“建立”為金鑰保管庫建立存取原則。如果沒有，請跳至步驟 3。
   a. 選擇以下權限：
      - 得到
      - 清單
      - 解密
      - 加密
      - 解開密鑰
      - 包裝鍵
      - 核實
      - 符號
   b. 選擇使用者指派的託管標識（資源）作為主體。
   c. 審查並建立存取策略。
3. "在金鑰保管庫中產生金鑰" 。

   請注意密鑰的以下要求：

   - 金鑰類型必須是*RSA*。
   - 建議的 RSA 金鑰大小為 **2048**，但也支援其他大小。

建立使用加密金鑰的系統

建立金鑰保管庫並產生加密金鑰後，您可以建立配置為使用該金鑰的新Cloud Volumes ONTAP系統。這些步驟透過使用 API 來支援。

所需權限

如果您想要將客戶管理的金鑰與單節點Cloud Volumes ONTAP系統一起使用，請確保控制台代理具有下列權限：

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"查看最新的權限列表"

步驟

1. 使用下列 API 呼叫取得 Azure 訂閱中的金鑰保管庫清單。

   對於 HA 對： `GET /azure/ha/metadata/vaults`

對於單節點： `GET /azure/vsa/metadata/vaults`

記下*名稱*和*資源組*。您需要在下一個步驟中指定這些值。

"了解有關此 API 呼叫的更多信息" 。

2. 使用以下 API 呼叫取得保管庫中的金鑰清單。

對於 HA 對： `GET /azure/ha/metadata/keys-vault`

對於單節點： `GET /azure/vsa/metadata/keys-vault`

記下*keyName*。您需要在下一個步驟中指定該值（以及保險庫名稱）。

"了解有關此 API 呼叫的更多信息" 。

3. 使用下列 API 呼叫建立Cloud Volumes ONTAP系統。

a. 對於 HA 對：

`POST /azure/ha/working-environments`

請求主體必須包含以下欄位：

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

包括 `"userAssignedIdentity": " userAssignedIdentityId"`如果您建立此資源是為了用於儲存帳戶加密，則欄位。

"了解有關此 API 呼叫的更多信息" 。

b. 對於單節點系統：

`POST /azure/vsa/working-environments`

請求主體必須包含以下欄位：

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

包括 `"userAssignedIdentity": " userAssignedIdentityId"`如果您建立此資源是為了用於儲存帳戶加密，則欄位。

"了解有關此 API 呼叫的更多信息" 。

結果

您有一個新的Cloud Volumes ONTAP系統，該系統配置為使用客戶管理的金鑰進行資料加密。

在 **Azure** 中設定**Cloud Volumes ONTAP**許可

在您決定要與Cloud Volumes ONTAP一起使用哪種授權選項後，需要執行幾個步驟才能在建立新系統時選擇該授權選項。

免費增值

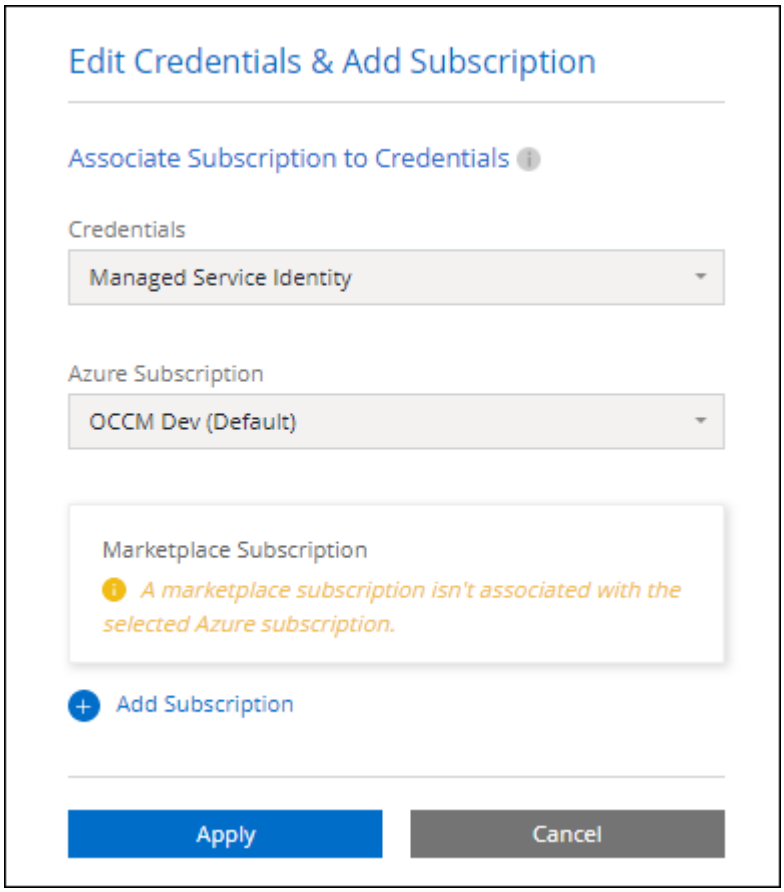
選擇免費加值服務，免費使用Cloud Volumes ONTAP，最高可提供 500 GiB 的設定容量。"了解有關免費增值服務的更多信息" 。

步驟

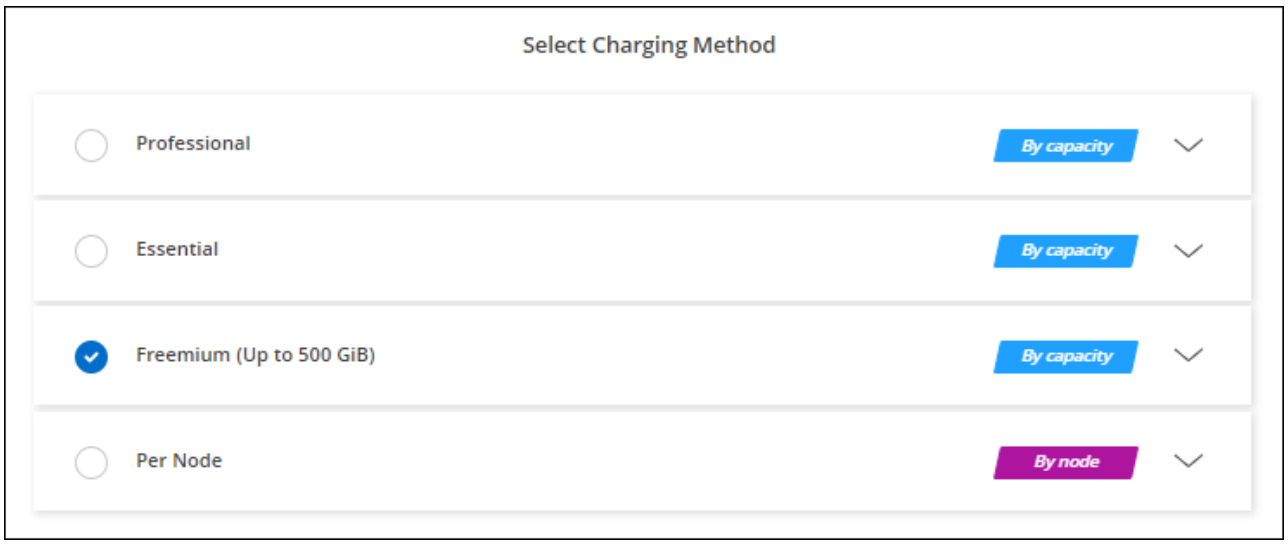
1. 從NetApp Console的左側導覽功能表中，選擇「儲存」>「管理」 。
2. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。

    a. 在“詳細資訊和憑證”頁面上，按一下“編輯憑證”>“新增訂閱”，然後依照指示訂閱 Azure 市集中的即用即付產品。

    除非您超過 500 GiB 的預配置容量，否則您無需透過市場訂閱付費，此時系統將自動轉換為"基本套餐" 。



a. 返回控制台後，到達收費方式頁面時選擇「免費增值」。



"查看在 Azure 中啟動Cloud Volumes ONTAP 的逐步說明" 。

基於容量的許可證

基於容量的許可使您能夠按 TiB 容量支付Cloud Volumes ONTAP費用。基於容量的許可以_包_的形式提供：Essentials 包或 Professional 包。

Essentials 和 Professional 套餐提供以下幾種消費模式或購買選項：

- 從NetApp購買的授權（自帶授權 (BYOL)）
- Azure 市場提供的按小時付費 (PAYGO) 訂閱
- 年度合約

"了解有關基於容量的許可的更多信息" 。

以下部分介紹如何開始使用每種消費模型。

BYOL

透過從NetApp購買授權 (BYOL) 進行預付款，以便在任何雲端供應商部署Cloud Volumes ONTAP系統。

已限制 BYOL 授權的購買、延期和續約。有關更多信息，請參閱 "Cloud Volumes ONTAP的 BYOL 授權可用性受限" 。

步驟

1. "聯絡NetApp銷售人員以取得許可證"
2. "將您的NetApp支援網站帳戶新增至控制台"

   控制台會自動查詢 NetApp 的授權服務，以取得與您的NetApp支援網站帳戶相關的授權的詳細資訊。如果沒有錯誤，控制台會自動將許可證新增至控制台。

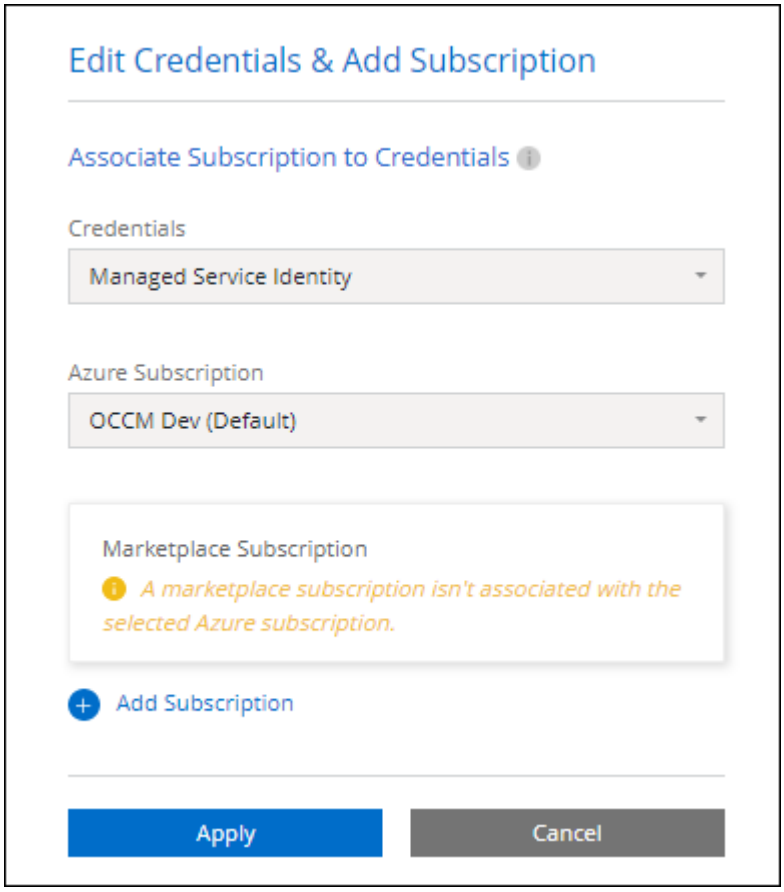
   您必須先從控制台取得許可證，然後才能與Cloud Volumes ONTAP一起使用。如果需要的話，你可以"手動

將許可證新增至控制台"。

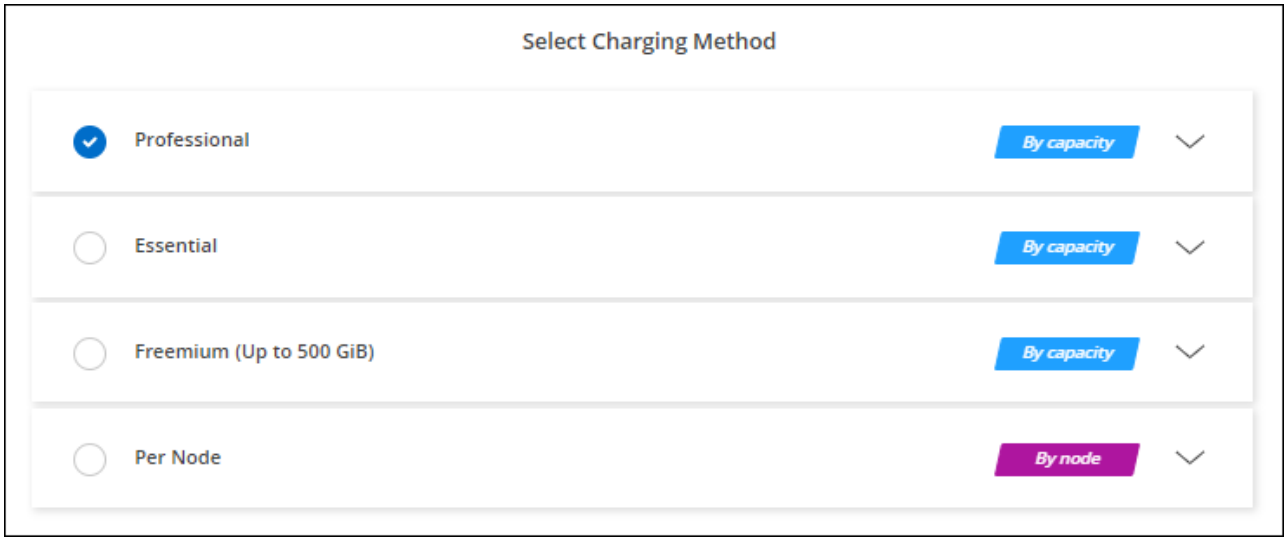
3. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。

   a. 在“詳細資訊和憑證”頁面上，按一下“編輯憑證”>“新增訂閱”，然後依照指示訂閱 Azure 市集中的即用即付產品。

      總是會先向您從NetApp購買的許可證收費，但如果您超出許可容量或許可證期限到期，則會按照市場上的小時費率向您收費。



   a. 返回控制台後，在到達收費方式頁面時選擇基於容量的套餐。



"查看在 Azure 中啟動Cloud Volumes ONTAP 的逐步說明" 。

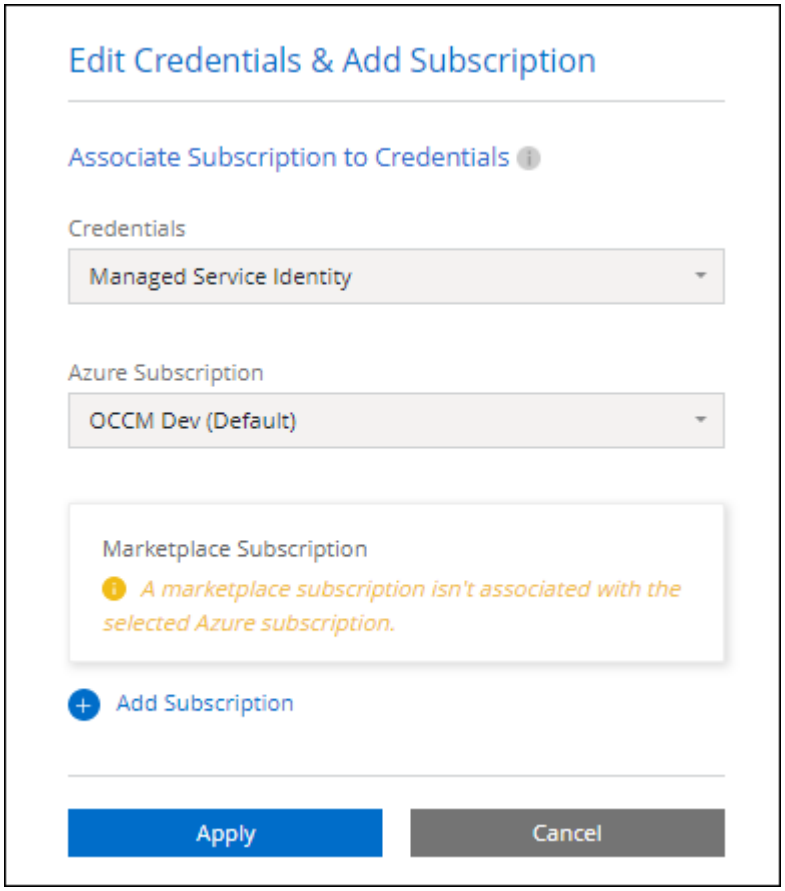
PAYGO 訂閱

透過訂閱雲端供應商市場提供的服務按小時付費。

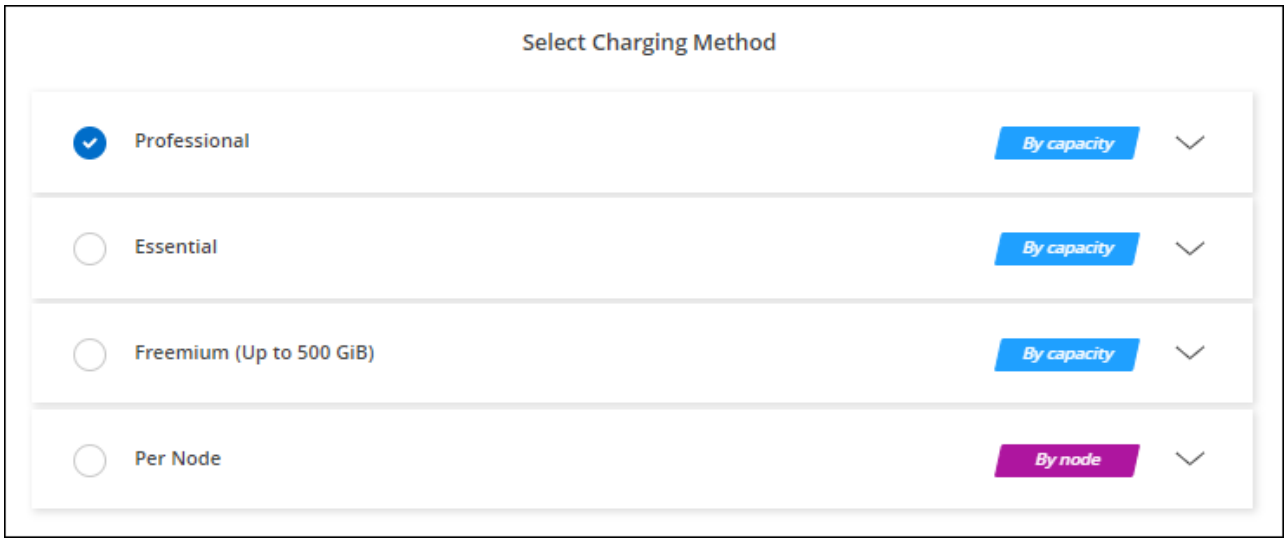
當您建立Cloud Volumes ONTAP系統時，控制台會提示您訂閱 Azure 市場中提供的協定。然後將該訂閱與系統關聯以進行收費。您可以將同一訂閱用於其他系統。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。
   a. 在“詳細資訊和憑證”頁面上，按一下“編輯憑證”>“新增訂閱”，然後依照指示訂閱 Azure 市集中的即用即付產品。



   b. 返回控制台後，在到達收費方式頁面時選擇基於容量的套餐。



"查看在 Azure 中啟動Cloud Volumes ONTAP 的逐步說明" 。

您可以從「設定」>「憑證」頁面管理與您的 Azure 帳戶相關聯的 Azure 市集訂閱。 "了解如何管理 Azure 帳戶和訂閱"

年度合約

透過購買年度合約每年支付Cloud Volumes ONTAP 的費用。

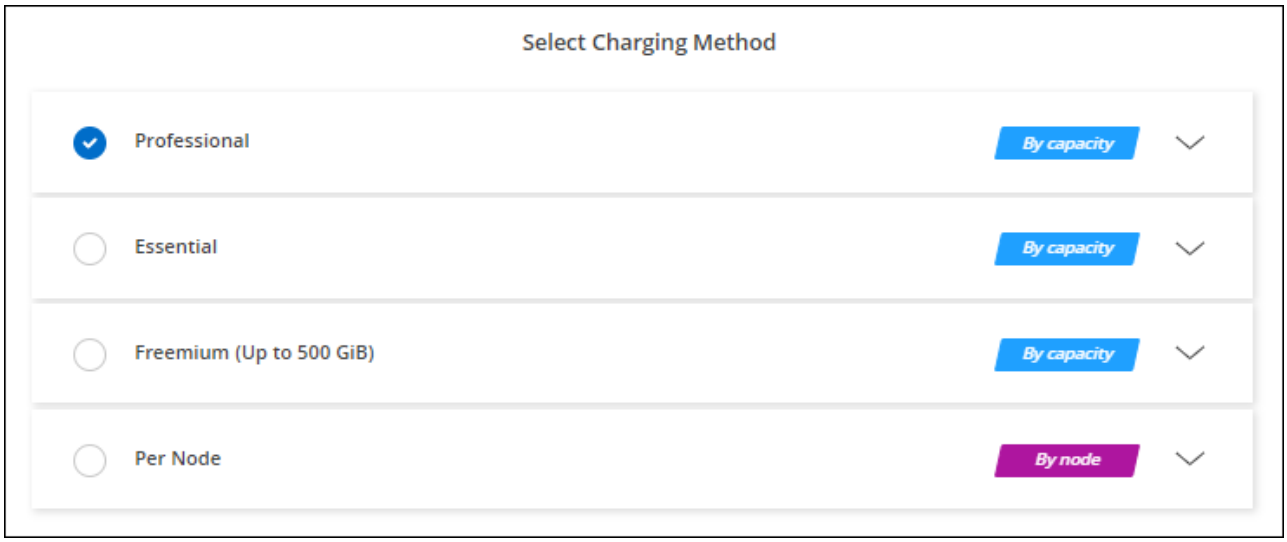
步驟

1. 聯絡您的NetApp銷售代表購買年度合約。

   該合約在 Azure 市場中以私人優惠的形式提供。

   NetApp與您分享私人優惠後，您可以在系統建立期間從 Azure 市場訂閱時選擇年度方案。

2. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。
   a. 在「詳細資料和憑證」頁面上，按一下「編輯憑證」>「新增訂閱」>「繼續」。
   b. 在 Azure 入口網站中，選擇與您的 Azure 帳戶共用的年度計劃，然後按一下「訂閱」。
   c. 返回控制台後，在到達收費方式頁面時選擇基於容量的套餐。



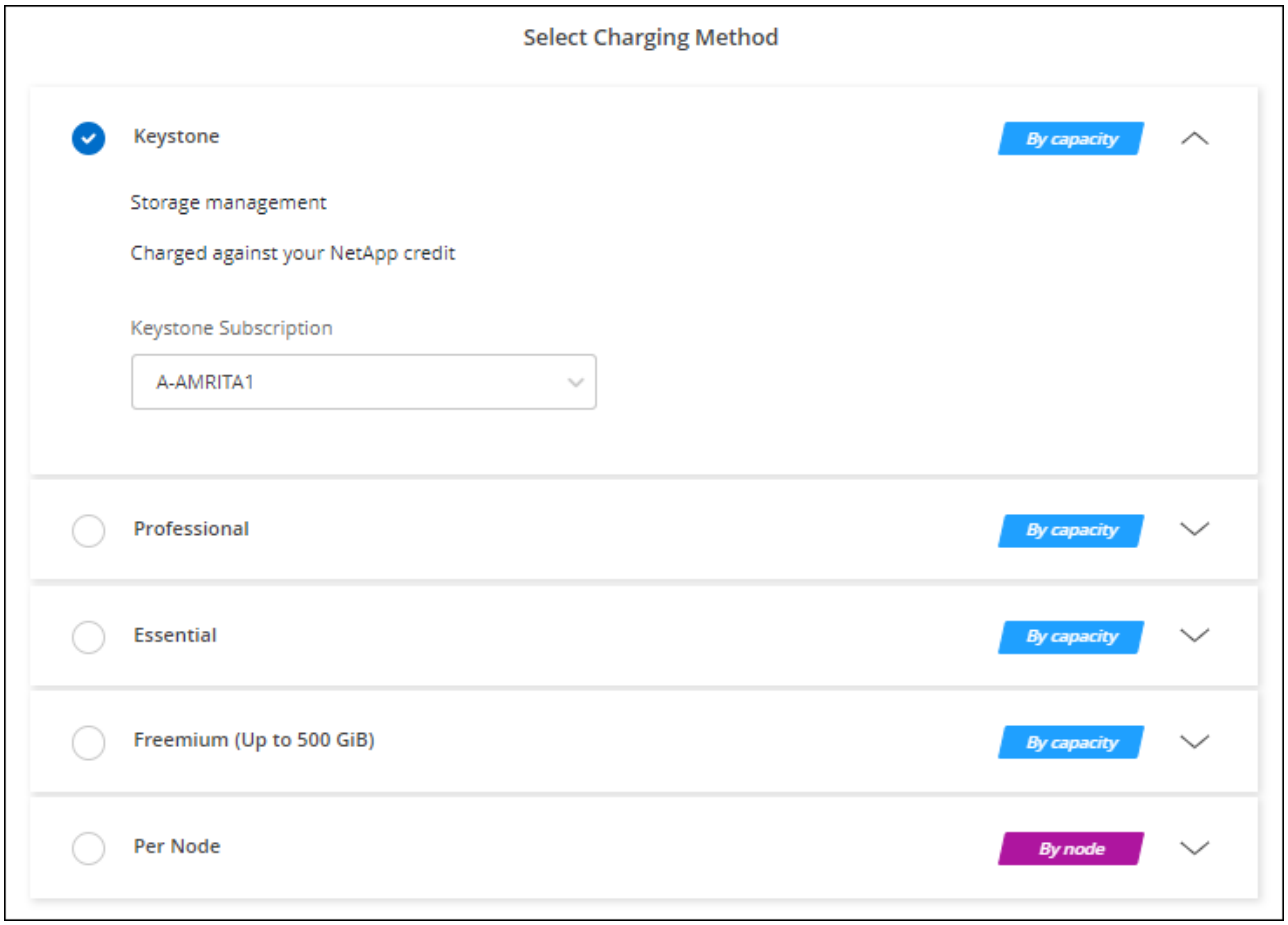
"查看在 Azure 中啟動Cloud Volumes ONTAP 的逐步說明" 。

Keystone訂閱

Keystone訂閱是一種按需付費的訂閱式服務。"了解有關NetApp Keystone訂閱的更多信息" 。

步驟

1. 如果您尚未訂閱， "聯絡NetApp"
2. 聯絡NetApp 以在控制台中授權您的使用者帳戶擁有一個或多個Keystone訂閱。
3. NetApp授權您的帳戶後，"連結您的訂閱以用於Cloud Volumes ONTAP" 。
4. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。
    a. 當提示選擇充電方式時，選擇Keystone Subscription 充電方式。



"查看在 Azure 中啟動Cloud Volumes ONTAP 的逐步說明" 。

基於節點的許可證

基於節點的許可證是Cloud Volumes ONTAP的上一代許可證。基於節點的授權可以從NetApp (BYOL) 購買，並且僅在特定情況下才可以續訂授權。有關信息，請參閱：

- "基於節點的許可證的可用性終止"
- "基於節點的許可證的可用性終止"
- "將基於節點的許可證轉換為基於容量的許可證"

在 **Azure** 中為**Cloud Volumes ONTAP**啟用高可用性模式

您應該啟用 Microsoft Azure 的高可用性（HA）模式，以減少計劃外故障轉移時間，並為 Cloud Volumes ONTAP 啟用 NFSv4 支援。啟用此模式後，您的 Cloud Volumes ONTAP HA 節點在 CIFS 和 NFSv4 用戶端發生計劃外故障轉移時，可以實現較低的復原時間目標（RTO）（60 秒）。

從Cloud Volumes ONTAP 9.10.1 開始，我們減少了在 Microsoft Azure 中執行的Cloud Volumes ONTAP HA 對的非計畫性故障轉移時間，並增加了對 NFSv4 的支援。若要讓這些增強功能可用於Cloud Volumes ONTAP，您需要在 Azure 訂閱上啟用高可用性功能。

關於此任務

NetApp Console 會在需要於 Azure 訂閱啟用此功能時提示您這些詳細資訊。請注意以下事項：

- 您的Cloud Volumes ONTAP HA 對的高可用性沒有問題。此 Azure 功能與ONTAP協同工作，以減少用戶端觀察到的因計劃外故障轉移事件而導致的 NFS 協定應用程式中斷時間。
- 啟用此功能不會對Cloud Volumes ONTAP HA 造成破壞。
- 在您的 Azure 訂閱上啟用此功能不會為其他虛擬機器帶來問題。
- Cloud Volumes ONTAP在 CIFS 和 NFS 用戶端上的叢集和 SVM 管理 LIF 故障轉移期間使用內部 Azure 負載平衡器。
- 啟用 HA 模式後，控制台每 12 小時掃描一次系統以更新內部 Azure 負載平衡器規則。

步驟

擁有 *Owner* 權限的 Azure 使用者可以透過 Azure CLI 啟用該功能。

1. "從 Azure 入口網站存取 Azure Cloud Shell"
2. 註冊高可用性模式功能：

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. （可選）驗證該功能現在是否已註冊：

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

Azure CLI 應傳回類似以下內容的結果：

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

相關連結

1. "Microsoft Azure 文件：高可用性連接埠概述"

2. "Microsoft Azure 說明文件：開始使用 Azure CLI"

在 **Azure** 中為**Cloud Volumes ONTAP**啟用 **VMOrchestratorZonalMultiFD**

若要在本機冗餘儲存 (LRS) 單一可用區 (AZ) 中部署 VM 實例，您應該啟動 Microsoft `Microsoft.Compute/VMOrchestratorZonalMultiFD`您的訂閱功能。在高可用性 (HA) 模式下，此功能有助於在相同可用區域內的不同故障域中部署節點。

除非您啟動此功能，否則不會發生區域部署，且先前的 LRS 非區域部署將生效。

有關在單一可用區域中部署虛擬機器的信息，請參閱"Azure 中的高可用性對"。

以具有「所有者」權限的使用者身分執行下列步驟：

步驟

1. 從 Azure 入口網站存取 Azure Cloud Shell。欲了解更多信息，請參閱 "Microsoft Azure 文件：Azure Cloud Shell 入門"。
2. 註冊 `Microsoft.Compute/VMOrchestratorZonalMultiFD`透過執行以下命令來啟用此功能：

```
az 帳號設定 -s <Azure_subscription_name_or_ID> az 功能註冊 --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
```

3. 驗證註冊狀態及輸出範例：

```
az feature show -n VMOrchestratorZonalMultiFD --namespace Microsoft.Compute { “id” ：“/subscriptions/<ID>/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestratorZonalMultiFD”，“Compname”：” “state”：“Registered” }，“type” ：“Microsoft.Features/providers/features” }
```

在 **Azure** 中啟動**Cloud Volumes ONTAP**

您可以透過在 NetApp Console 中建立 Cloud Volumes ONTAP 系統，在 Azure 中啟動單節點系統或 HA 配對。

開始之前

開始之前您需要以下內容。

- 已啟動並正在執行的控制台代理程式。
  - 你應該有一個 "與您的系統關聯的控制台代理"。
  - "您應該準備好讓控制台代理程式始終處於運行狀態" 。
- 了解您想要使用的配置。

  您應該有一個配置計劃，並且從管理員那裡獲得必要的 Azure 網路詳細資訊。有關詳細信息，請參閱"規劃您的Cloud Volumes ONTAP配置" 。

- 了解設定Cloud Volumes ONTAP許可所需的條件。

  "了解如何設定許可" 。

關於此任務

當控制台在 Azure 中建立Cloud Volumes ONTAP系統時，它會建立多個 Azure 對象，例如資源群組、網路介面和儲存帳戶。您可以在精靈結束時查看資源摘要。

> 資料遺失的可能性
>
> 最佳做法是為每個Cloud Volumes ONTAP系統使用新的專用資源群組。
>
> 由於資料遺失的風險，不建議在現有的共用資源組中部署Cloud Volumes ONTAP 。雖然控制台可以在部署失敗或刪除的情況下從共用資源群組中刪除Cloud Volumes ONTAP資源，但 Azure 使用者可能會意外從共用資源群組中刪除Cloud Volumes ONTAP資源。

在 **Azure** 中啟動單節點**Cloud Volumes ONTAP**系統

如果要在 Azure 中啟動單節點 Cloud Volumes ONTAP 系統，則需要在 Console 中建立單節點系統。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，點擊*新增系統*並依照指示操作。
3. 選擇位置：選擇*Microsoft Azure*和* Cloud Volumes ONTAP單一節點*。
4. 如果出現提示， "建立控制台代理" 。
5. 詳細資料和憑證：可選擇變更 Azure 憑證和訂閱，指定群集名稱，根據需要新增標籤，然後指定憑證。

   下表描述了您可能需要指導的欄位：

場地	描述
系統名稱	控制台使用系統名稱來命名Cloud Volumes ONTAP系統和 Azure 虛擬機器。如果您選擇該選項，它也會使用該名稱作為預先定義安全性群組的前綴。
資源組標籤	標籤是 Azure 資源的元資料。當您在此欄位中輸入標籤時，控制台會將它們新增至與Cloud Volumes ONTAP系統關聯的資源群組。建立系統時，您可以從使用者介面新增多達四個標籤，然後可以在建立系統後新增更多標籤。請注意，在建立系統時，API 不會將您限制為四個標籤。有關標籤的信息，請參閱 "Microsoft Azure 文件：使用標籤來組織您的 Azure 資源"。
使用者名稱和密碼	這些是Cloud Volumes ONTAP叢集管理員帳戶的憑證。您可以使用這些憑證透過ONTAP System Manager 或ONTAP CLI 連線到Cloud Volumes ONTAP 。保留預設的_admin_使用者名稱或將其變更為自訂使用者名稱。
編輯憑證	您可以選擇不同的 Azure 憑證和不同的 Azure 訂閱來與此Cloud Volumes ONTAP系統一起使用。您需要將 Azure 市場訂閱與選定的 Azure 訂閱關聯，以便部署即用即付的Cloud Volumes ONTAP系統。 "了解如何新增憑證" 。

6. 服務：啟用或停用您想要或不想與Cloud Volumes ONTAP一起使用的單一服務。

   。"了解有關NetApp Data Classification的更多信息"

- "了解有關NetApp Backup and Recovery的更多信息"

如果您想使用 WORM 和資料分層，則必須停用備份和還原並部署版本 9.8 或更高版本的Cloud Volumes ONTAP系統。

7. 位置：選擇區域、可用區域、VNet 和子網，然後選取核取方塊以確認控制台代理程式和目標位置之間的網路連線。

對於中國區域，僅Cloud Volumes ONTAP 9.12.1 GA 和 9.13.0 GA 支援單節點部署。您可以將這些版本升級到Cloud Volumes ONTAP的更高補丁和版本，如下所示"Azure 中支援"。如果您想在中國地區部署更高版本的Cloud Volumes ONTAP ，請聯絡NetApp支援。中國地區僅支援直接從NetApp購買的許可證，不提供市場訂閱。

8. 連線：選擇新的或現有的資源群組，然後選擇是否使用預先定義的安全群組或使用您自己的安全群組。

下表描述了您可能需要指導的欄位：

場地	描述
資源組	為Cloud Volumes ONTAP建立新的資源組或使用現有的資源組。最佳做法是為Cloud Volumes ONTAP使用新的專用資源群組。雖然可以在現有的共享資源組中部署Cloud Volumes ONTAP ，但由於資料遺失的風險，因此不建議這樣做。請參閱上面的警告以了解更多詳細資訊。 如果您使用的 Azure 帳戶具有 "所需權限"，如果部署失敗或刪除，控制台會從資源群組中刪除Cloud Volumes ONTAP資源。
產生的安全群組	如果您讓控制台為您產生安全性群組，則需要選擇如何允許流量： • 如果選擇*僅限選取的 VNet*，則入站流量的來源為選取 VNet 的子網路範圍和控制台代理程式所在的 VNet 的子網路範圍。這是推薦的選項。 • 如果選擇“所有 **VNets**”，則入站流量的來源為 0.0.0.0/0 IP 範圍。
使用現有的	如果您選擇現有的安全性群組，則它必須符合Cloud Volumes ONTAP要求。"查看預設安全群組" 。

9. 收費方式和 **NSS** 帳戶：指定您想要在此系統中使用的收費選項，然後指定NetApp支援網站帳戶。
   - "了解Cloud Volumes ONTAP的授權選項" 。
   - "了解如何設定許可" 。
10. 預先配置套件：選擇其中一個套件來快速部署Cloud Volumes ONTAP系統，或點擊*建立我自己的設定*。

如果您選擇其中一個套餐，您只需指定一個卷，然後審核並批准配置。

11. 許可：如果需要，請變更Cloud Volumes ONTAP版本，並選擇虛擬機器類型。

如果所選版本有較新的候選版本、通用版本或修補程式版本，則BlueXP會在建立工作環境時將系統更新至該版本。例如，如果您選擇Cloud Volumes ONTAP 9.16.1 P3 並且 9.16.1 P4 可用，則會發生更新。更新不會從一個版本發生到另一個版本 - 例如，從 9.15 到 9.16。

12. 從 **Azure** 市集訂閱：如果控制台無法啟用Cloud Volumes ONTAP的程式部署，您將看到此頁面。請依照螢幕上所列的步驟操作。請參閱 "以程式設計方式部署 Marketplace 產品"了解更多。
13. 底層儲存資源：選擇初始聚合的設定：磁碟類型、每個磁碟的大小以及是否應啟用資料分層到 Blob 儲存。

    請注意以下事項：

    - 如果在 VNet 中停用了對您的儲存帳戶的公共訪問，則您無法在Cloud Volumes ONTAP系統中啟用資料分層。有關信息，請參閱"安全群組規則"。
    - 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聚合中的所有磁碟以及使用簡單配置選項時控制台建立的任何其他聚合。您可以使用進階分配選項建立使用不同磁碟大小的聚合。

      有關選擇磁碟類型和大小的協助，請參閱"在 Azure 中調整系統大小"。
    - 您可以在建立或編輯磁碟區時選擇特定的磁碟區分層策略。
    - 如果您停用資料分層，則可以在後續聚合上啟用它。

      "了解有關數據分層的更多信息" 。
14. 寫入速度與 **WORM**：

    a. 如有需要，請選擇*正常*或*高*寫入速度。

       "了解有關寫入速度的更多信息" 。

    b. 如果需要，請啟動一次寫入、多次讀取 (WORM) 儲存。

       此選項僅適用於某些 VM 類型。若要了解支援的 VM 類型，請參閱"HA 對許可證支援的配置"。

       如果為Cloud Volumes ONTAP 9.7 及更低版本啟用了資料分層，則無法啟用 WORM。啟用 WORM 和分層後，恢復或降級到Cloud Volumes ONTAP 9.8 的操作將被阻止。

    "了解有關 WORM 存儲的更多信息" 。

    a. 如果您啟動 WORM 存儲，請選擇保留期限。
15. 建立磁碟區：輸入新磁碟區的詳細資料或點選*跳過*。

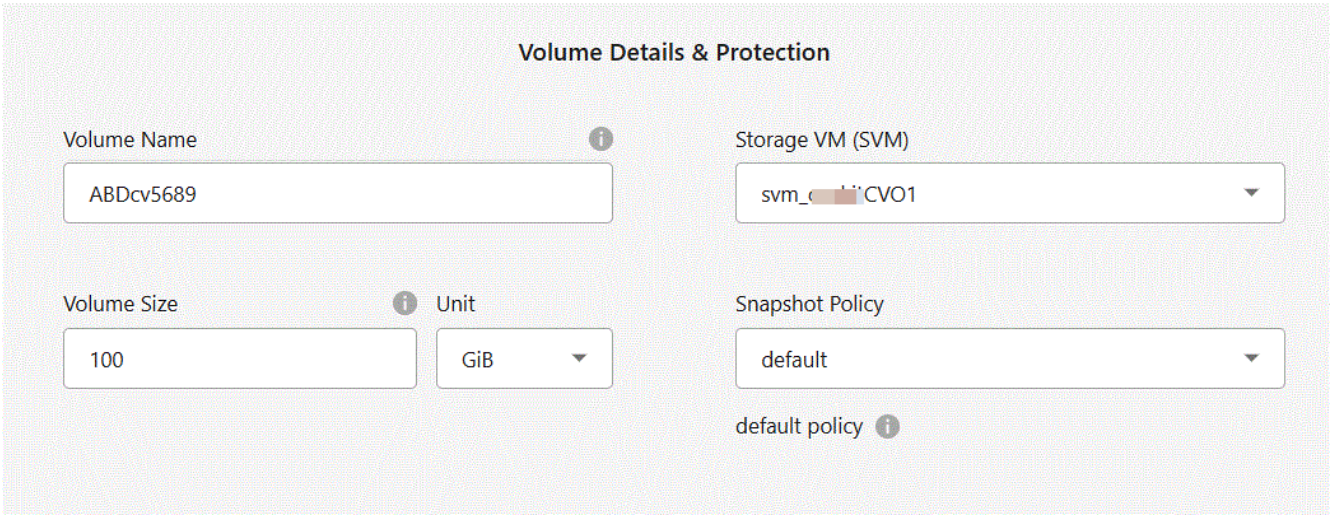
    "了解支援的客戶端協定和版本" 。

    此頁面中的某些欄位是不言自明的。下表描述了您可能需要指導的欄位：

場地	描述
尺寸	您可以輸入的最大大小很大程度上取決於您是否啟用精簡配置，這使您能夠建立比目前可用的實體儲存更大的磁碟區。
存取控制（僅適用於 NFS）	導出策略定義了子網路中可以存取磁碟區的用戶端。預設情況下，控制台輸入一個提供對子網路中所有實例的存取權限的值。

場地	描述
權限和使用者/群組（僅適用於 CIFS）	這些欄位可讓您控制使用者和群組對共用的存取等級（也稱為存取控制清單或 ACL）。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。如果指定網域 Windows 使用者名，則必須使用網域\使用者名稱格式包含使用者的網域。
快照策略	Snapshot 副本策略指定自動建立的NetApp Snapshot 副本的頻率和數量。NetApp Snapshot 副本是時間點檔案系統映像，它不會影響效能並且只需要最少的儲存空間。您可以選擇預設策略或無策略。對於瞬態數據，您可能會選擇無：例如，對於 Microsoft SQL Server，請選擇 tempdb。
進階選項（僅適用於 NFS）	為磁碟區選擇一個 NFS 版本：NFSv3 或 NFSv4。
啟動器群組和 IQN（僅適用於 iSCSI）	iSCSI 儲存目標稱為 LUN（邏輯單元），並以標準區塊裝置呈現給主機。啟動器群組是 iSCSI 主機節點名稱表，用於控制哪些啟動器可以存取哪些 LUN。iSCSI 目標透過標準乙太網路網路適配器 (NIC)、具有軟體啟動器的 TCP 卸載引擎 (TOE) 卡、融合網路適配器 (CNA) 或專用主機匯流排適配器 (HBA) 連接到網絡，並透過 iSCSI 限定名稱 (IQN) 進行識別。當您建立 iSCSI 磁碟區時，控制台會自動為您建立 LUN。我們透過為每個磁碟區建立一個 LUN 來簡化操作，因此無需進行任何管理。建立磁碟區後，"使用 IQN 從主機連線到 LUN" 。

下圖顯示了磁碟區建立精靈的第一頁：



16. **CIFS** 設定：如果您選擇 CIFS 協議，請設定 CIFS 伺服器。

場地	描述
DNS 主 IP 位址和輔助 IP 位址	為 CIFS 伺服器提供名稱解析的 DNS 伺服器的 IP 位址。所列的 DNS 伺服器必須包含定位 CIFS 伺服器將加入的網域的 Active Directory LDAP 伺服器和網域控制站所需的服務位置記錄 (SRV)。
要加入的 Active Directory 網域	您希望 CIFS 伺服器加入的 Active Directory (AD) 網域的 FQDN。
授權加入網域的憑證	具有足夠權限將電腦新增至 AD 網域內指定組織單位 (OU) 的 Windows 帳戶的名稱和密碼。
CIFS 伺服器 NetBIOS 名稱	AD 網域中唯一的 CIFS 伺服器名稱。

場地	描述
組織單位	AD 網域內與 CIFS 伺服器關聯的組織單位。預設值為 CN=Computers。若要將 Azure AD 網域服務設定為Cloud Volumes ONTAP 的AD 伺服器，您應該在此欄位中輸入 **OU=AADDC Computers** 或 **OU=AADDC Users** 。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 文件：在 Azure AD 網域服務託管網域中建立組織單位 (OU)"^]
DNS 網域	Cloud Volumes ONTAP儲存虛擬機器 (SVM) 的 DNS 網域。大多數情況下，該域與 AD 域相同。
NTP 伺服器	選擇「使用 Active Directory 網域」以使用 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，那麼您應該使用 API。請參閱 "NetApp Console自動化文檔"了解詳情。請注意，只有在建立 CIFS 伺服器時才能設定 NTP 伺服器。建立 CIFS 伺服器後，它不可配置。

17. 使用情況設定檔、磁碟類型和分層策略：選擇是否要啟用儲存效率功能並變更磁碟區分層策略（如果需要）。

    更多信息，請參閱"了解卷使用情況"和"資料分層概述"。

18. 審核並批准：審核並確認您的選擇。
    a. 查看有關配置的詳細資訊。
    b. 按一下「更多資訊」以查看有關支援和控制台將購買的 Azure 資源的詳細資訊。
    c. 選取*我明白…*複選框。
    d. 按一下“開始”。

結果

控制台部署Cloud Volumes ONTAP系統。您可以在審核頁面上追蹤進度。

如果您在部署Cloud Volumes ONTAP系統時遇到任何問題，請查看失敗訊息。您也可以選擇系統並點擊*重新建立環境*。

如需更多協助，請訪問 "NetApp Cloud Volumes ONTAP支持"。

部署程序完成後，請勿修改 Azure 入口網站中系統產生的Cloud Volumes ONTAP配置，尤其是系統標籤。對這些配置所做的任何變更都可能導致意外行為或資料遺失。

完成後

- 如果您配置了 CIFS 共享，請授予使用者或群組對檔案和資料夾的權限，並驗證這些使用者是否可以存取共用並建立檔案。
- 如果要將配額套用於卷，請使用ONTAP系統管理員或ONTAP CLI。

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

在 **Azure** 中啟動**Cloud Volumes ONTAP HA** 對

如果您想在 Azure 中啟動Cloud Volumes ONTAP HA 對，則需要在控制台中建立 HA 系統。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，點擊*新增系統*並依照指示操作。
3. 如果出現提示， "建立控制台代理" 。
4. 詳細資料和憑證：可選擇變更 Azure 憑證和訂閱，指定群集名稱，根據需要新增標籤，然後指定憑證。

   下表描述了您可能需要指導的欄位：

場地	描述
系統名稱	控制台使用系統名稱來命名Cloud Volumes ONTAP系統和 Azure 虛擬機器。如果您選擇該選項，它也會使用該名稱作為預先定義安全性群組的前綴。
資源組標籤	標籤是 Azure 資源的元資料。當您在此欄位中輸入標籤時，控制台會將它們新增至與Cloud Volumes ONTAP系統關聯的資源群組。建立系統時，您可以從使用者介面新增多達四個標籤，然後可以在建立系統後新增更多標籤。請注意，在建立系統時，API 不會將您限制為四個標籤。有關標籤的信息，請參閱 "Microsoft Azure 文件：使用標籤來組織您的 Azure 資源"。
使用者名稱和密碼	這些是Cloud Volumes ONTAP叢集管理員帳戶的憑證。您可以使用這些憑證透過ONTAP System Manager 或ONTAP CLI 連線到Cloud Volumes ONTAP 。保留預設的_admin_使用者名稱或將其變更為自訂使用者名稱。
編輯憑證	您可以選擇不同的 Azure 憑證和不同的 Azure 訂閱來與此Cloud Volumes ONTAP系統一起使用。您需要將 Azure 市場訂閱與選定的 Azure 訂閱關聯，以便部署即用即付的Cloud Volumes ONTAP系統。 "了解如何新增憑證" 。

5. 服務：根據您是否要將各個服務與Cloud Volumes ONTAP一起使用來啟用或停用它們。
   - "了解有關NetApp Data Classification的更多信息"
   - "了解有關NetApp Backup and Recovery的更多信息"

   如果您想使用 WORM 和資料分層，則必須停用備份和還原並部署版本 9.8 或更高版本的Cloud Volumes ONTAP系統。

6. **HA**部署模型：
   a. 選擇*單一可用區*或*多個可用區*。
      - 對於單一可用區域，請選擇 Azure 區域、可用區域、VNet 和子網路。

        從Cloud Volumes ONTAP 9.15.1 開始，您可以在 Azure 中的單一可用區域 (AZ) 中以 HA 模式部署虛擬機器 (VM) 執行個體。您需要選擇支援此部署的區域和地理。如果區域或地理不支援區域部署，則遵循先前LRS的非區域部署模式。若要了解共享託管磁碟支援的配置，請參閱"具有共享託管磁碟的 HA 單可用區域配置"。

      - 對於多個可用區域，請選擇區域、VNet、子網路、節點 1 的區域以及節點 2 的區域。
   b. 選取*我已驗證網路連線…*複選框。
7. 連線：選擇新的或現有的資源群組，然後選擇是否使用預先定義的安全群組或使用您自己的安全群組。

   下表描述了您可能需要指導的欄位：

場地	描述
資源組	為Cloud Volumes ONTAP建立新的資源組或使用現有的資源組。最佳做法是為Cloud Volumes ONTAP使用新的專用資源群組。雖然可以在現有的共享資源組中部署Cloud Volumes ONTAP ，但由於資料遺失的風險，因此不建議這樣做。請參閱上面的警告以了解更多詳細資訊。 您必須為在 Azure 中部署的每個Cloud Volumes ONTAP HA 對使用專用資源群組。一個資源組中僅支援一個 HA 對。如果您嘗試在 Azure 資源組中部署第二個Cloud Volumes ONTAP HA 對，控制台會遇到連線問題。 如果您使用的 Azure 帳戶具有 "所需權限"，如果部署失敗或刪除，控制台會從資源群組中刪除Cloud Volumes ONTAP資源。
產生的安全群組	如果您讓控制台為您產生安全性群組，則需要選擇如何允許流量： • 如果選擇*僅限選取的 VNet*，則入站流量的來源為選取 VNet 的子網路範圍和控制台代理程式所在的 VNet 的子網路範圍。這是推薦的選項。 • 如果選擇“所有 **VNets**”，則入站流量的來源為 0.0.0.0/0 IP 範圍。
使用現有的	如果您選擇現有的安全性群組，則它必須符合Cloud Volumes ONTAP要求。"查看預設安全群組" 。

8. 收費方式和 **NSS** 帳戶：指定您想要在此系統中使用的收費選項，然後指定NetApp支援網站帳戶。
   - "了解Cloud Volumes ONTAP的授權選項" 。
   - "了解如何設定許可" 。
9. 預先配置套件：選擇其中一個套件來快速部署Cloud Volumes ONTAP系統，或點擊*變更配置*。

   如果您選擇其中一個套餐，您只需指定一個卷，然後審核並批准配置。
10. 許可：根據需要變更Cloud Volumes ONTAP版本並選擇虛擬機器類型。

    如果所選版本有較新的候選版本、通用版本或修補程式版本，則控制台在建立系統時會將其更新至該版本。例如，如果您選擇Cloud Volumes ONTAP 9.13.1 且 9.13.1 P4 可用，則會發生更新。更新不會從一個版本發生到另一個版本 — 例如，從 9.13 到 9.14。
11. 從 **Azure** 市集訂閱：如果控制台無法啟用Cloud Volumes ONTAP的程式部署，請依照下列步驟操作。
12. 底層儲存資源：選擇初始聚合的設定：磁碟類型、每個磁碟的大小以及是否應啟用資料分層到 Blob 儲存。

    請注意以下事項：
    - 磁碟大小適用於初始聚合中的所有磁碟以及使用簡單配置選項時控制台建立的任何其他聚合。您可以使用進階分配選項建立使用不同磁碟大小的聚合。

      有關選擇磁碟大小的協助，請參閱"在 Azure 中調整系統大小"。
    - 如果在 VNet 中停用了對您的儲存帳戶的公共訪問，則您無法在Cloud Volumes ONTAP系統中啟用資料分層。有關信息，請參閱"安全群組規則"。

- 您可以在建立或編輯磁碟區時選擇特定的磁碟區分層策略。
- 如果您停用資料分層，則可以在後續聚合上啟用它。

  "了解有關數據分層的更多信息" 。

- 從Cloud Volumes ONTAP 9.15.0P1 開始，Azure 頁面 blob 不再支援新的高可用性對部署。如果您目前在現有的高可用性對部署中使用 Azure 頁 Blob，則可以移轉到 Edsv4 系列 VM 和 Edsv5 系列 VM 中較新的 VM 執行個體類型。

  "詳細了解 Azure 中支援的配置" 。

13. 寫入速度與 **WORM**：

    a. 如有需要，請選擇*正常*或*高*寫入速度。

       "了解有關寫入速度的更多信息" 。

    b. 如果需要，請啟動一次寫入、多次讀取 (WORM) 儲存。

       此選項僅適用於某些 VM 類型。若要了解支援的 VM 類型，請參閱"HA 對許可證支援的配置"。

       如果為Cloud Volumes ONTAP 9.7 及更低版本啟用了資料分層，則無法啟用 WORM。啟用 WORM 和分層後，恢復或降級到Cloud Volumes ONTAP 9.8 的操作將被阻止。

    "了解有關 WORM 存儲的更多信息" 。

    a. 如果您啟動 WORM 存儲，請選擇保留期限。

14. 與儲存和 **WORM** 的安全通訊：選擇是否啟用與 Azure 儲存帳戶的 HTTPS 連接，並啟動一次寫入、多次讀取 (WORM) 儲存（如果需要）。

    HTTPS 連線從Cloud Volumes ONTAP 9.7 HA 對到 Azure 頁面 blob 儲存帳戶。請注意，啟用此選項可能會影響寫入效能。建立系統後，您無法變更設定。

    "了解有關 WORM 存儲的更多信息" 。

    如果啟用了資料分層，則無法啟用 WORM。

    "了解有關 WORM 存儲的更多信息" 。

15. 建立磁碟區：輸入新磁碟區的詳細資料或點選*跳過*。

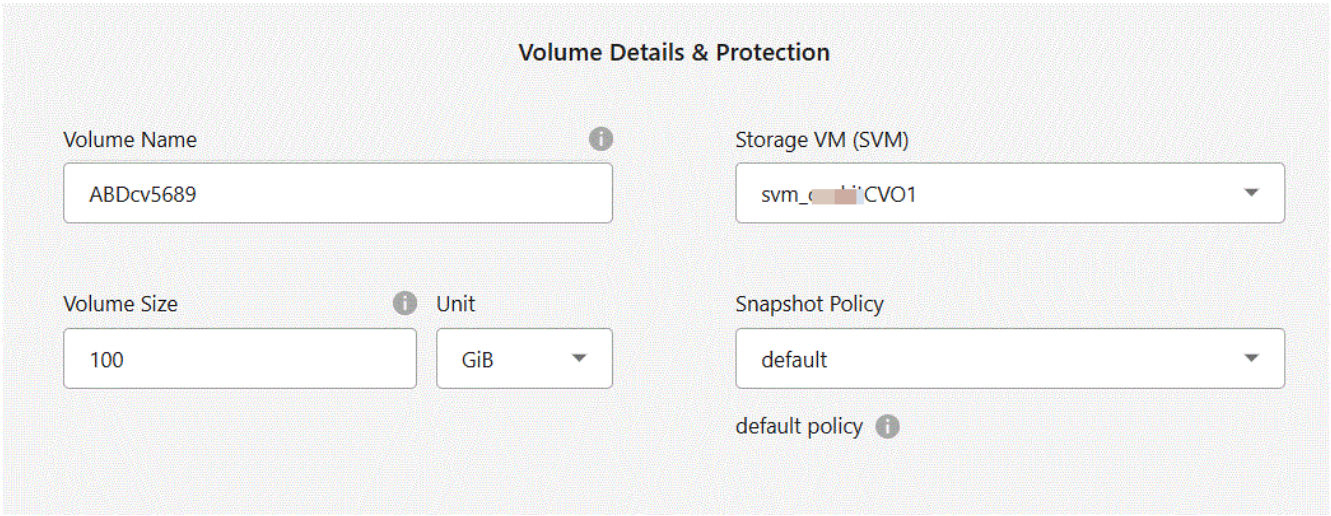
    "了解支援的客戶端協定和版本" 。

    此頁面中的某些欄位是不言自明的。下表描述了您可能需要指導的欄位：

場地	描述
尺寸	您可以輸入的最大大小很大程度上取決於您是否啟用精簡配置，這使您能夠建立比目前可用的實體儲存更大的磁碟區。
存取控制（僅適用於 NFS）	導出策略定義了子網路中可以存取磁碟區的用戶端。預設情況下，控制台輸入一個提供對子網路中所有實例的存取權限的值。

場地	描述
權限和使用者/群組（僅適用於 CIFS）	這些欄位可讓您控制使用者和群組對共用的存取等級（也稱為存取控制清單或 ACL）。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。如果指定網域 Windows 使用者名，則必須使用網域\使用者名稱格式包含使用者的網域。
快照策略	Snapshot 副本策略指定自動建立的NetApp Snapshot 副本的頻率和數量。NetApp Snapshot 副本是時間點檔案系統映像，它不會影響效能並且只需要最少的儲存空間。您可以選擇預設策略或無策略。對於瞬態數據，您可能會選擇無：例如，對於 Microsoft SQL Server，請選擇 tempdb。
進階選項（僅適用於 NFS）	為磁碟區選擇一個 NFS 版本：NFSv3 或 NFSv4。
啟動器群組和 IQN（僅適用於 iSCSI）	iSCSI 儲存目標稱為 LUN（邏輯單元），並以標準區塊裝置呈現給主機。啟動器群組是 iSCSI 主機節點名稱表，用於控制哪些啟動器可以存取哪些 LUN。iSCSI 目標透過標準乙太網路網路適配器 (NIC)、具有軟體啟動器的 TCP 卸載引擎 (TOE) 卡、融合網路適配器 (CNA) 或專用主機匯流排適配器 (HBA) 連接到網絡，並透過 iSCSI 限定名稱 (IQN) 進行識別。當您建立 iSCSI 磁碟區時，控制台會自動為您建立 LUN。我們透過為每個磁碟區建立一個 LUN 來簡化操作，因此無需進行任何管理。建立磁碟區後，"使用 IQN 從主機連線到 LUN" 。

下圖顯示了磁碟區建立精靈的第一頁：



16. **CIFS** 設定：如果您選擇 CIFS 協議，請設定 CIFS 伺服器。

場地	描述
DNS 主 IP 位址和輔助 IP 位址	為 CIFS 伺服器提供名稱解析的 DNS 伺服器的 IP 位址。所列的 DNS 伺服器必須包含定位 CIFS 伺服器將加入的網域的 Active Directory LDAP 伺服器和網域控制站所需的服務位置記錄 (SRV)。
要加入的 Active Directory 網域	您希望 CIFS 伺服器加入的 Active Directory (AD) 網域的 FQDN。
授權加入網域的憑證	具有足夠權限將電腦新增至 AD 網域內指定組織單位 (OU) 的 Windows 帳戶的名稱和密碼。
CIFS 伺服器 NetBIOS 名稱	AD 網域中唯一的 CIFS 伺服器名稱。

場地	描述
組織單位	AD 網域內與 CIFS 伺服器關聯的組織單位。預設值為 CN=Computers。若要將 Azure AD 網域服務設定為Cloud Volumes ONTAP 的AD 伺服器，您應該在此欄位中輸入 **OU=AADDC Computers** 或 **OU=AADDC Users** 。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 文件：在 Azure AD 網域服務託管網域中建立組織單位 (OU)"^]
DNS 網域	Cloud Volumes ONTAP儲存虛擬機器 (SVM) 的 DNS 網域。大多數情況下，該域與 AD 域相同。
NTP 伺服器	選擇「使用 Active Directory 網域」以使用 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，那麼您應該使用 API。請參閱 "NetApp Console自動化文檔"了解詳情。請注意，只有在建立 CIFS 伺服器時才能設定 NTP 伺服器。建立 CIFS 伺服器後，它不可配置。

17. 使用情況設定檔、磁碟類型和分層策略：選擇是否要啟用儲存效率功能並變更磁碟區分層策略（如果需要）。

    更多信息，請參閱"選擇卷使用情況設定檔"，"資料分層概述" ， 和 "KB：CVO 支援哪些內嵌儲存效率功能？"

18. 審核並批准：審核並確認您的選擇。

    a. 查看有關配置的詳細資訊。

    b. 按一下「更多資訊」以查看有關支援和控制台將購買的 Azure 資源的詳細資訊。

    c. 選取*我明白…*複選框。

    d. 按一下“開始”。

結果

控制台部署Cloud Volumes ONTAP系統。您可以在審核頁面上追蹤進度。

如果您在部署Cloud Volumes ONTAP系統時遇到任何問題，請查看失敗訊息。您也可以選擇系統並點擊*重新建立環境*。

如需更多協助，請訪問 "NetApp Cloud Volumes ONTAP支持"。

完成後

- 如果您配置了 CIFS 共享，請授予使用者或群組對檔案和資料夾的權限，並驗證這些使用者是否可以存取共用並建立檔案。
- 如果要將配額套用於卷，請使用ONTAP系統管理員或ONTAP CLI。

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

部署程序完成後，請勿修改 Azure 入口網站中系統產生的Cloud Volumes ONTAP配置，尤其是系統標籤。對這些配置所做的任何變更都可能導致意外行為或資料遺失。

相關連結

*"在 Azure 中規劃Cloud Volumes ONTAP配置" *"從 Azure 市場在 Azure 中部署Cloud Volumes ONTAP"

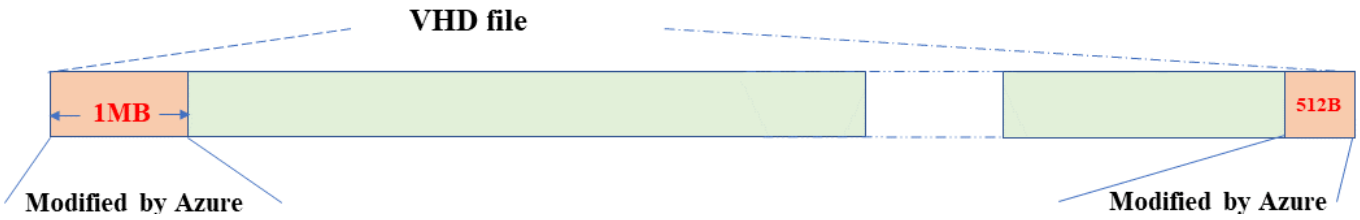
針對**Cloud Volumes ONTAP** 的**Azure** 市場映像驗證

Azure 映像驗證符合增強的NetApp安全要求。驗證圖像檔案是一個簡單的過程。但是，Azure 映像簽署驗證需要特別注意 Azure VHD 映像文件，因為它在 Azure 市場中已更改。

Cloud Volumes ONTAP 9.15.0 及更高版本支援 Azure 映像驗證。

Azure 對已發布 **VHD** 檔案的更改

VHD 檔案開頭的 1 MB（1048576 位元組）和結尾的 512 位元組已被 Azure 修改。 NetApp對剩餘的 VHD 檔案進行簽署。



在範例中，VHD 檔案為 10GB。 NetApp簽署的部分標示為綠色（10 GB - 1 MB - 512 位元組）。

相關連結

- "頁面錯誤部落格：如何使用 OpenSSL 進行簽署和驗證"
- "使用 Azure Marketplace 映像為 Azure Stack Edge Pro GPU 建立 VM 映像 | Microsoft Learn"
- "使用 Azure CLI 將託管磁碟匯出/複製到儲存帳戶 | Microsoft Learn"
- "Azure Cloud Shell 快速入門 - Bash | Microsoft Learn"
- "如何安裝 Azure CLI | Microsoft Learn"
- "az 儲存 blob 副本 | Microsoft Learn"
- "使用 Azure CLISign in— 登入與驗證 | Microsoft Learn"

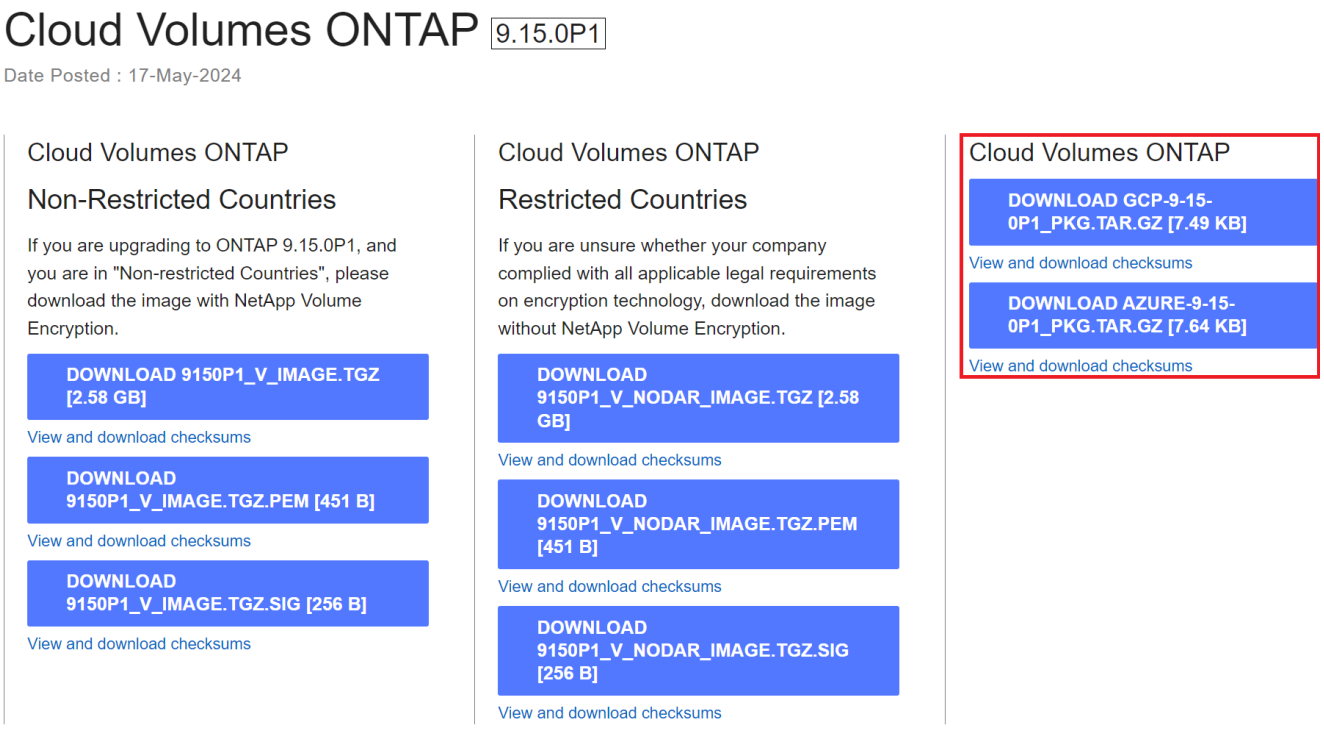
下載適用於**Cloud Volumes ONTAP** 的**Azure** 映像文件

您可以從 "NetApp支援站點"。

tar.gz 檔案包含圖像簽名驗證所需的檔案。除了 *tar.gz* 檔案之外，您還應該下載圖像的 *checksum* 檔案。校驗和檔案包含 `md5`和 `sha256`*tar.gz* 檔案的校驗和。

步驟

1. 前往 "NetApp支援網站上的Cloud Volumes ONTAP產品頁面"並從*下載*部分下載所需的軟體版本。
2. 在Cloud Volumes ONTAP下載頁面上，按一下 Azure 映像檔的下載檔案並下載 *tar.gz* 檔案。



3. 在 Linux 上，運行 `md5sum AZURE-<version>_PKG.TAR.GZ`。

   在 macOS 上，運行 `sha256sum AZURE-<version>_PKG.TAR.GZ`。

4. 驗證 `md5sum`和 `sha256sum`值與下載的 Azure 映像中的值相符。
5. 在 Linux 和 macOS 上，使用以下命令提取 *tar.gz* 文件 `tar -xzf`命令。

   解壓縮後的 *tar.gz* 檔案包含摘要（*.sig*）檔案、公鑰憑證（*.pem*）檔案和鏈憑證（*.pem*）檔案。

   提取 **tar.gz** 檔案後的範例輸出：

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
```

從 **Azure** 市場匯出**Cloud Volumes ONTAP**的 **VHD** 映像

一旦 VHD 映像發佈到 Azure 雲端，它就不再由NetApp管理。相反，已發布的圖像被放置在 Azure 市場上。當映像在 Azure 市場上暫存和發佈時，Azure 會修改 VHD 開頭的 1 MB 和結尾的 512 位元組。要驗證VHD檔案的簽名，需要從Azure市場匯出Azure修改後的VHD鏡像。

開始之前

確保您的系統上安裝了 Azure CLI，或可以透過 Azure 入口網站使用 Azure Cloud Shell。有關如何安裝 Azure CLI 的詳細信息，請參閱 "Microsoft 文件：如何安裝 Azure CLI"。

步驟

1. 使用 *version_readme* 檔案的內容將系統上的Cloud Volumes ONTAP版本對應到 Azure 市場映像版本。Cloud Volumes ONTAP版本由 `buildname`Azure 市場鏡像版本表示為 `version`在版本映射中。

   在下列範例中， Cloud Volumes ONTAP版本 `9.15.0P1`對應到 `Azure` 市場映像版本 `9150.01000024.05090105`。此 Azure 市場鏡像版本稍後用於設定鏡像 URN。

   ```
   [
    "buildname": "9.15.0P1",
       "publisher": "netapp",
        "version": "9150.01000024.05090105"

   ]
   ```

2. 確定要建立虛擬機器的區域。區域名稱用作 `locName`設定市場影像的 URN 時的變數。若要列出可用區域，請執行以下命令：

   ```
   az account list-locations -o table
   ```

   在此表中，區域名稱出現在 `Name`場地。

   ```
   $ az account list-locations -o table
   DisplayName               Name                 RegionalDisplayName
   ------------------------  -------------------
   -------------------------------------
   East US                   eastus               (US) East US
   East US 2                 eastus2              (US) East US 2
   South Central US          southcentralus       (US) South Central US
   ...
   ```

3. 查看下表中對應Cloud Volumes ONTAP版本和 VM 部署類型的 SKU 名稱。 SKU 名稱用作 `skuName`設定市場影像的 URN 時的變數。

   例如，所有採用Cloud Volumes ONTAP 9.15.0 的單節點部署都應使用 `ontap_cloud_byol`作為 SKU 名稱。

* Cloud Volumes ONTAP版本*	透過虛擬機器部署	**SKU** 名稱
9.17.1 及更高版本	Azure 市場	ontap_cloud_direct_gen2
9.17.1 及更高版本	NetApp Console	ontap_cloud_gen2
9.16.1	Azure 市場	ontap_cloud_direct
9.16.1	主機	ontap_cloud

9.15.1	主機	ontap_cloud
9.15.0	控制台，單節點部署	ontap_cloud_byol
9.15.0	控制台、高可用性 (HA) 部署	ontap_cloud_byol_ha

4. 對應ONTAP版本和 Azure 市場映像後，使用 Azure Cloud Shell 或 Azure CLI 從 Azure 市場匯出 VHD 檔案。

使用 **Linux** 上的 **Azure Cloud Shell** 匯出 **VHD** 文件

從 Azure Cloud Shell，將市場映像匯出至 VHD 檔案（例如，*9150.01000024.05090105.vhd*），然後下載到本機 Linux 系統。執行下列步驟從 Azure 市場取得 VHD 映像。

步驟

1. 設定市場圖像的 URN 和其他參數。 URN 格式為 `<publisher>:<offer>:<sku>:<version>`。或者，您可以列出NetApp市場圖像來確認正確的圖像版本。

```
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...
```

2. 從市場映像建立一個具有匹配映像版本的新託管磁碟：

```
PS /home/user1> $diskName = "9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = "fnf1"
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
$urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
--access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas
```

3. 將 VHD 檔案從託管磁碟匯出到 Azure 儲存體。建立具有適當存取等級的容器。在這個例子中，我們使用了一個名為 `vm-images`和 `Container`訪問級別。從 Azure 入口網站取得儲存帳戶存取金鑰：儲存帳戶 **>** ***examplesaname*** **>** 存取金鑰 **>** ***key1*** **>** ***key*** **>** 顯示 **>** ***<copy>***

```
PS /home/user1> $storageAccountName = “examplesaname”
PS /home/user1> $containerName = “vm-images”
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = “9150.01000024.05090105.vhd”
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState –Container $containerName
–Context $destContext -Blob $destBlobName
```

4. 將產生的映像下載到您的 Linux 系統。使用 `wget`下載VHD檔案的指令：

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

URL 遵循標準格式。為了實現自動化，您可以獲得如下所示的 URL 字串。或者，您可以使用 Azure CLI `az`命令來取得 URL。範例 URL：https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

5. 清理託管磁碟

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

使用 **Linux** 上的 **Azure CLI** 匯出 **VHD** 文件

使用本機 Linux 系統的 Azure CLI 將市場映像匯出到 VHD 檔案。

步驟

1. 登入 Azure CLI 並列出市場圖像：

```
% az login --use-device-code
```

2. 要登錄，請使用網頁瀏覽器開啟頁面 https://microsoft.com/devicelogin並輸入驗證碼。

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...
```

3. 從具有匹配映像版本的市場映像建立新的託管磁碟。

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxx"
```

為了使流程自動化，需要從標準輸出中提取 SAS。請參閱相應文件以獲取指導。

4. 從託管磁碟匯出 VHD 檔案。

   a. 建立具有適當存取等級的容器。在此範例中，名為 `vm-images`和 `Container`使用訪問級別。

   b. 從 Azure 入口網站取得儲存帳戶存取金鑰：儲存帳戶 **> *examplesaname* >** 存取金鑰 **> *key1* > *key* >** 顯示 **> *<copy>***

      您也可以使用 `az`此步驟的命令。

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS --destination
-container $containerName --account-name $storageAccountName --account
-key $storageAccountKey --destination-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. 檢查 blob 副本的狀態。

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. 將生成的映像下載到您的 Linux 伺服器。

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

URL 遵循標準格式。為了實現自動化，您可以獲得如下所示的 URL 字串。或者，您可以使用 Azure CLI `az`命令來取得 URL。範例 URL：https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

7. 清理託管磁碟

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

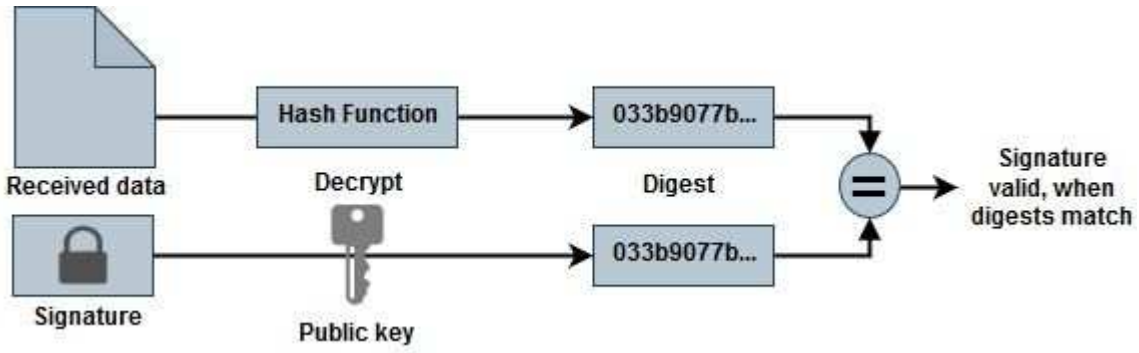
驗證文件簽名

針對**Cloud Volumes ONTAP** 的**Azure** 市場映像簽章驗證

Azure 映像驗證過程透過剝離 VHD 檔案的開頭 1 MB 和結尾 512 位元組，然後套用雜湊函數來產生摘要檔案。為了匹配簽章程序，使用_sha256_進行雜湊。

文件簽章驗證工作流程摘要

以下是文件簽章驗證工作流程的概述。



- 從 "NetApp支援站點"並提取摘要（.sig）文件、公鑰證書（.pem）文件和鏈證書（.pem）文件。請參閱"下載 Azure 映像摘要文件"了解更多。
- 信任鏈的驗證。
- 從公鑰憑證（.pem）中提取公鑰（.pub）。
- 使用提取的公鑰解密摘要檔案。
- 將結果與從圖像檔案中刪除開頭 1 MB 和結尾 512 位元組後建立的臨時檔案的新生成的摘要進行比較。此步驟透過使用 OpenSSL 命令列工具執行。 OpenSSL CLI 工具會在檔案比對成功或失敗時顯示對應的訊息。

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

在 Linux 上驗證匯出的 VHD 檔案簽章包括驗證信任鏈、編輯檔案和驗證簽章。

步驟

1. 從下載 Azure 映像檔 "NetApp支援站點"並提取摘要（.sig）文件、公鑰證書（.pem）文件和鏈證書（.pem）文件。

   參考 "下載 Azure 映像摘要文件"了解更多。

2. 驗證信任鏈。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. 刪除 VHD 檔案開頭的 1 MB（1,048,576 位元組）和結尾的 512 位元組。使用時 `tail`， 這 `-c +K`選項從檔案的第 `K` 個位元組產生位元組。因此，它將 `1048577` 傳遞給 `tail -c`。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. 使用 OpenSSL 從憑證中提取公鑰，並使用簽署檔案和公鑰驗證剝離的檔案（sign.tmp）。

   命令提示字元根據驗證顯示指示成功或失敗的訊息。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. 清理工作區。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

驗證 **macOS** 上**Cloud Volumes ONTAP**的 **Azure** 市場映像簽名

在 Linux 上驗證匯出的 VHD 檔案簽章包括驗證信任鏈、編輯檔案和驗證簽章。

步驟

1. 從下載 Azure 映像檔 "NetApp支援站點"並提取摘要（.sig）文件、公鑰證書（.pem）文件和鏈證書（.pem）文件。

   參考 "下載 Azure 映像摘要文件"了解更多。

2. 驗證信任鏈。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. 刪除 VHD 檔案開頭的 1MB（1,048,576 位元組）和結尾的 512 位元組。使用時 `tail`， 這 `-c +K`選項從檔案的第 `K` 個位元組產生位元組。因此，它將 `1048577` 傳遞給 `tail -c`。請注意，在 macOS 上，tail 指令可能需要大約十分鐘才能完成。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. 使用 OpenSSL 從憑證中提取公鑰，並使用簽署檔案和公鑰驗證剝離的檔案（sign.tmp）。命令提示字元根據驗證顯示指示成功或失敗的訊息。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. 清理工作區。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

從 **Azure** 市場部署**Cloud Volumes ONTAP**

您可以使用 Azure 市場直接部署來快速輕鬆地部署Cloud Volumes ONTAP。從 Azure 市場，您只需點擊幾下即可快速部署Cloud Volumes ONTAP ，並在您的環境中探索其核心特性和功能。

有關該產品的更多信息，請參閱"了解NetApp Console和市場中的Cloud Volumes ONTAP產品"。

關於此任務

使用 Azure 市場直接部署部署的Cloud Volumes ONTAP系統具有這些屬性。請注意，透過 Azure 市場部署的獨立實例的功能在NetApp Console中被發現時會發生變化。

- 最新的Cloud Volumes ONTAP版本（9.16.1 或更高版本）。
- Cloud Volumes ONTAP的免費許可證，限制為 500 GiB 的配置容量。此許可證不包括NetApp支持，且沒有到期日期。
- 兩個節點在單一可用區 (AZ) 中以高可用性 (HA) 模式配置，並配置預設序號。儲存虛擬機器（儲存 VM）部署在"靈活的編排模式"。
- 預設創建的實例的聚合。
- 預置容量為 500 GiB 的高級 SSD v2 託管磁碟，以及根磁碟和資料磁碟。
- 部署了一個資料儲存虛擬機，具有 NFS、CIFS、iSCSI 和 NVMe/TCP 資料服務。您不能新增任何額外的資料儲存虛擬機器。
- 為 NFS、CIFS (SMB)、iSCSI、自主勒索軟體防護 (ARP)、 SnapLock和SnapMirror安裝授權。
- "ONTAP溫度敏感儲存效率 (TSSE)"、磁碟區加密和外部金鑰管理預設啟用。
- 不支援以下功能：
  - FabricPool分層
  - 更改儲存虛擬機器類型
  - 快速寫入模式

開始之前

- 確保您擁有有效的 Azure 市場訂閱。
- 確保您滿足"單一可用區內的高可用性部署"在 Azure 中。請參閱"為Cloud Volumes ONTAP設定 Azure 網路"。
- 您需要指派以下 Azure 角色之一才能部署Cloud Volumes ONTAP：
  - 這 `contributor`具有預設權限的角色。欲了解更多信息，請參閱 "Microsoft Azure 文件：Azure 內建角色"。
  - 具有以下權限的自訂 RBAC 角色。欲了解更多信息，請參閱 "Azure 文件：Azure 自訂角色"。

“權限”：[{“操作”：[“Microsoft.AAD/register/action”
，“Microsoft.Resources/subscriptions/resourceGroups/write”
，“Microsoft.Network/loadBalancers/write”，“Microsoft.ClassicCompute/virtualMachin es/write”
，“Microsoft.Compute/capacityReservationGroups/deploy/action”
，“Microsoft.ClassicCompute/virtualMachines/networkInterfaces/associatedNetworkSecurityGrou ps/write”，“Microsoft.Ne twork/networkInterfaces/write”
，“Microsoft.Compute/virtualMachines/write”
，“Microsoft.Compute/virtualMachines/extensions/write”
，“Microsoft.Resources/deployments/validate/action”，“Micr osoft.Resources/subscriptions/resourceGroups/read”，“Microsoft.Network/virtualNetworks/write”
，“Microsoft.Network/virtualNetworks/read”，“Microsoft.Network/networkSecurityGroups/write”，“Microsoft.Network/networkSecurityGroups/read”、“Microsoft.Compute/disks/write”、“Microsoft.C ompute/virtualMachineScaleSets/write”、“Microsoft.Resources/deployment s/write
」、「Microsoft.Network/virtualNetworks/subnets/read」、「Microsoft.Network/virtualNetworks/s ubnets/write」]、「notActions」：[]、「dataActions」：[]、「notDataActions」：[] }]

如果您已將資源提供者「Microsoft.storage」註冊到您的訂閱，那麼您不需要`Microsoft.AAD/register/action`允許。欲了解更多信息，請參閱 "Azure 文件：Azure 儲存權限"。

步驟

1. 從 Azure 市場網站搜尋NetApp產品。
2. 選擇* NetApp Cloud Volumes ONTAP direct*。
3. 按一下「建立」以啟動部署精靈。
4. 選擇一個計劃。 *計劃*清單通常顯示Cloud Volumes ONTAP的最新版本。
5. 在「基本資訊」標籤中，提供以下詳細資訊：
   - 訂閱：選擇訂閱。部署將與訂閱號掛鉤。
   - 資源組：使用現有資源組或建立新的資源組。資源組有助於在Cloud Volumes ONTAP系統的單一群組內分配所有資源，例如磁碟和儲存虛擬機器。
   - 區域：選擇支援在單一 AZ 中部署 Azure HA 的區域。您只會看到清單中可用的區域。
   - 大小：為支援的 Premium SSD v2 託管磁碟選擇儲存 VM 大小。
   - 區域：為您選擇的地區選擇一個區域。
   - 管理者密碼：設定密碼。部署完成後，您可以使用此管理員密碼登入系統。
   - 確認密碼：再次輸入相同的密碼確認。
     - 在「網路」標籤中，新增虛擬網路和子網，或從清單中選擇它們。

       為了遵守 Microsoft Azure 限制，您應該在設定新的虛擬網路時建立一個新的子網路。同樣，如果您選擇現有網絡，則應選擇現有子網路。

     - 若要選擇預先定義的網路安全群組，請選擇「是」。選擇「否」以指派具有必要流量規則的預先定義 Azure 網路安全性群組。有關詳細信息，請參閱"Azure 的安全性群組規則" 。
     - 在「進階」標籤中確認是否已設定此部署所需的兩個 Azure 功能。參考"為Cloud Volumes ONTAP單

可用區部署啟用 Azure 功能"和"在 Azure 中為Cloud Volumes ONTAP啟用高可用性模式"。

- 您可以在*標籤*標籤中為資源或資源群組定義名稱和值對。
- 在「**Review + create**」標籤中，查看詳細資訊並開始部署。

完成後

選擇通知圖示即可查看部署進度。部署Cloud Volumes ONTAP後，您可以查看列出的可供操作的儲存虛擬機器。

一旦可以訪問，請使用ONTAP系統管理員或ONTAP CLI 透過您設定的管理員憑證登入儲存虛擬機器。此後，您可以建立磁碟區、LUN 或共用並開始利用Cloud Volumes ONTAP的儲存功能。

解決部署問題

直接透過 Azure 市場部署的Cloud Volumes ONTAP系統不包括NetApp的支援。如果部署過程中出現任何問題，您可以獨立排除故障並解決。

步驟

1. 在 Azure 市場網站上，前往 啟動診斷 **>** 序列日誌。
2. 下載並調查串行日誌。
3. 請參閱產品文件和知識庫 (KB) 文章以進行故障排除。
   - "Azure 市場文檔"
   - "NetApp文檔"
   - "NetApp知識庫文章"

在控制台中發現已部署的系統

您可以發現使用 Azure 市場直接部署部署的Cloud Volumes ONTAP系統，並在控制台中的 系統 頁面上進行管理。控制台代理程式發現系統、新增系統並套用必要的許可證，並為這些系統解鎖控制台的全部功能。保留具有 PSSD v2 託管磁碟的單一 AZ 中的原始 HA 配置，並且系統註冊到與原始部署相同的 Azure 訂閱和資源群組。

關於此任務

在發現使用 Azure 市場直接部署部署的Cloud Volumes ONTAP系統時，控制台代理將執行下列任務：

- 將發現系統的免費許可證替換為常規的基於容量的許可證"免費增值許可證"。
- 保留已部署系統的現有功能，並新增控制台的附加功能，例如資料保護、資料管理和安全功能。
- 使用 NFS、CIFS (SMB)、iSCSI、ARP、 SnapLock和SnapMirror的新ONTAP授權取代節點上已安裝的授權。
- 將通用節點序號轉換為唯一序號。
- 根據需要為資源分配新的系統標籤。
- 將實例的動態 IP 位址轉換為靜態 IP 位址。
- 啟用以下功能"FabricPool分層"，"AutoSupport" ， 和"一次寫入多次讀取"（WORM）儲存。您可以在需要時從控制台啟動這些功能。
- 將實例註冊到用於發現它們的 NSS 帳戶。
- 啟用容量管理功能"自動和手動模式"對於已發現的系統。

開始之前

確保在 Azure 市場上部署已完成。只有當部署完成且可供發現時，控制台代理才能發現系統。

步驟

在控制台中，您可以按照標準程序來發現現有系統。請參閱"將現有的Cloud Volumes ONTAP系統新增至控制台"。

> 在發現過程中，您可能會看到失敗訊息，但您可以忽略它們，直到發現過程完成。在發現期間，請勿修改 Azure 市場入口網站中系統產生的Cloud Volumes ONTAP配置，尤其是系統標籤。對這些配置所做的任何變更都可能導致意外的系統行為。

完成後

發現完成後，您可以在控制台的「系統」頁面上查看列出的系統。您可以執行各種管理任務，例如"擴大總量"，"添加卷"，"配置額外的儲存虛擬機"， 和"更改實例類型"。

相關連結

有關建立儲存的更多信息，請參閱ONTAP文件：

- "為 NFS 建立卷"
- "為 iSCSI 建立 LUN"
- "為 CIFS 建立共享"

開始使用 Google Cloud

Google Cloud 中的Cloud Volumes ONTAP快速入門

只需幾個步驟即可在 Google Cloud 中開始使用Cloud Volumes ONTAP 。


建立控制台代理

如果你沒有 "控制台代理"但是，你需要創建一個。 "了解如何在 Google Cloud 中建立控制台代理"

請注意，如果您想在沒有網路存取的子網路中部署Cloud Volumes ONTAP ，則需要手動安裝控制台代理程式並存取在該控制台代理程式上執行的NetApp Console。 "了解如何在沒有網路存取的地方手動安裝控制台代理"


規劃您的配置

控制台提供符合您的工作負載要求的預先配置包，或者您可以建立自己的配置。如果您選擇自己的配置，您應該了解可用的選項。

"了解有關規劃配置的更多信息"。


設定網路

1. 確保您的 VPC 和子網路將支援控制台代理和Cloud Volumes ONTAP之間的連線。

2. 如果您打算啟用資料分層， "為私有 Google 存取權設定Cloud Volumes ONTAP子網路" 。
3. 如果您正在部署 HA 對，請確保您有四個 VPC，每個 VPC 都有自己的子網路。
4. 如果您使用共用 VPC，請向控制台代理服務帳戶提供_計算網路使用者_角色。
5. 為NetApp AutoSupport啟用從目標 VPC 的出站網際網路存取。

   如果您在沒有網路存取的位置部署Cloud Volumes ONTAP，則不需要執行此步驟。

"了解有關網絡要求的更多信息" 。

4 設定服務帳戶

Cloud Volumes ONTAP需要 Google Cloud 服務帳戶來實現兩個目的。第一個是當你啟用"資料分層"將冷資料分層到 Google Cloud 中的低成本物件儲存。第二個是當你啟用 "NetApp Backup and Recovery"將磁碟區備份到低成本的物件儲存。

您可以設定一個服務帳戶並將其用於兩種用途。服務帳戶必須具有*儲存管理員*角色。

"閱讀逐步說明" 。

5 啟用 **Google Cloud API**

"在您的專案中啟用 Google Cloud API". "這些 API"，您可能已經在建立 Console 代理時啟用了它們，這些是在 Google Cloud 中部署 Cloud Volumes ONTAP 所必需的。

6 使用控制台啟動**Cloud Volumes ONTAP**

按一下“新增系統”，選擇您想要部署的系統類型，然後完成精靈中的步驟。"閱讀逐步說明" 。

相關連結

- "建立控制台代理"
- "在 Linux 主機上安裝控制台代理軟體"
- "控制台代理的 Google Cloud 權限"

在 **Google Cloud** 中規劃您的**Cloud Volumes ONTAP**配置

在 Google Cloud 中部署Cloud Volumes ONTAP時，您可以選擇符合您的工作負載需求的預先設定係統，也可以建立自己的設定。如果您選擇自己的配置，您應該了解可用的選項。

選擇**Cloud Volumes ONTAP**許可證

Cloud Volumes ONTAP有多種授權選項。每個選項都可以讓您選擇符合您需求的消費模式。

- "了解Cloud Volumes ONTAP的授權選項"
- "了解如何設定許可"

選擇支援的區域

大多數 Google Cloud 區域支援Cloud Volumes ONTAP 。 "查看支援區域的完整列表" 。

選擇支援的機器類型

Cloud Volumes ONTAP支援多種機器類型，具體取決於您選擇的授權類型。

"Google Cloud 中 Cloud Volumes ONTAP 支援的組態"

了解儲存限制

Cloud Volumes ONTAP系統的原始容量限制與許可證相關。額外的限制會影響聚合和磁碟區的大小。在規劃配置時您應該注意這些限制。

"Google Cloud 中 Cloud Volumes ONTAP 的儲存限制"

在 **Google Cloud** 中調整系統大小

調整Cloud Volumes ONTAP系統的大小可以幫助您滿足效能和容量要求。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

請查看支援的機器類型。 "Cloud Volumes ONTAP發行說明"然後查看谷歌提供的關於每種受支援機器類型的詳細資訊。將您的工作負載需求與機器類型的 vCPU 和記憶體數量相符。請注意，每個 CPU 核心都會提高網路效能。

請參閱以下內容以了解更多詳細資訊：

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

磁碟類型

為Cloud Volumes ONTAP建立磁碟區時，您需要選擇Cloud Volumes ONTAP用於磁碟的底層雲端儲存。磁碟類型可以是以下任一種：

- 區域 *SSD* 持久性磁碟：SSD 持久性磁碟最適合需要高隨機 IOPS 率的工作負載。
- 區域平衡持久性磁碟：這些 SSD 透過提供每 GB 較低的 IOPS 來平衡效能和成本。
- 區域標準持久磁碟：標準持久磁碟經濟實惠，可處理順序讀取/寫入作業。

  如欲了解更多詳情，請參閱 "Google Cloud 文件：區域持久性磁碟（標準和 SSD）"。

磁碟大小

部署Cloud Volumes ONTAP系統時，您需要選擇初始磁碟大小。之後，您可以讓NetApp Console為您管理系統的容量，但如果您想自行建立聚合，請注意以下事項：

- 聚合中的所有磁碟必須具有相同的大小。
- 確定所需的空間，同時考慮性能。

- 持久磁碟的效能會隨著磁碟大小和系統可用的 vCPU 數量自動擴展。

  請參閱以下內容以了解更多詳細資訊：

  - "Google Cloud 文件：區域持久性磁碟（標準和 SSD）"
  - "Google Cloud 文件：最佳化持久磁碟和本機 SSD 效能"

查看預設系統磁碟

除了用戶資料的儲存之外，控制台還購買了Cloud Volumes ONTAP系統資料（啟動資料、根資料、核心資料和NVRAM）的雲端儲存。出於規劃目的，在部署Cloud Volumes ONTAP之前查看這些詳細資訊可能會有所幫助。

- "查看 Google Cloud 中Cloud Volumes ONTAP系統資料的預設磁碟" 。
- "Google Cloud 文件：雲端配額概述"

  Google Cloud Compute Engine 對資源使用實施配額，因此您應確保在部署Cloud Volumes ONTAP之前尚未達到限制。

控制台代理還需要係統磁碟。 "查看控制台代理預設配置的詳細信息" 。

收集網路資訊

在 Google Cloud 中部署 Cloud Volumes ONTAP 時，您需要指定虛擬網路的詳細資訊。您可以使用工作表從管理員收集這些資訊。

單節點系統的網路資訊

Google Cloud 資訊	你的價值
地區	
區	
VPC 網路	
子網	
防火牆策略（如果使用您自己的）	

多個區域中 **HA** 對的網路資訊

Google Cloud 資訊	你的價值
地區	
節點 1 的區域	
節點 2 的區域	
調解員區域	
VPC-0 和子網	

Google Cloud 資訊	你的價值
VPC-1 和子網	
VPC-2 和子網	
VPC-3 和子網	
防火牆策略（如果使用您自己的）	

單一區域中 **HA** 對的網路資訊

Google Cloud 資訊	你的價值
地區	
區	
VPC-0 和子網	
VPC-1 和子網	
VPC-2 和子網	
VPC-3 和子網	
防火牆策略（如果使用您自己的）	

選擇寫入速度

控制台可讓您選擇Cloud Volumes ONTAP的寫入速度設置，但 Google Cloud 中的高可用性 (HA) 對除外。在選擇寫入速度之前，您應該了解正常設定和高設定之間的差異以及使用高寫入速度時的風險和建議。"了解有關寫入速度的更多信息" 。

選擇卷使用情況設定檔

ONTAP包含多種儲存效率功能，可減少您所需的總儲存量。在控制台中建立磁碟區時，您可以選擇啟用這些功能的設定檔或停用這些功能的設定檔。您應該了解有關這些功能的更多信息，以幫助您決定使用哪個配置文件。

NetApp儲存效率功能有以下優勢：

精簡配置

向主機或使用者提供比實體儲存池中實際擁有的更多的邏輯儲存。不是預先分配儲存空間，而是在寫入資料時動態地將儲存空間分配給每個磁碟區。

重複資料刪除

透過定位相同的資料塊並將其替換為對單一共享區塊的引用來提高效率。該技術透過消除駐留在同一磁碟區中的冗餘資料區塊來減少儲存容量需求。

壓縮

透過壓縮主儲存、輔助儲存和歸檔儲存磁碟區內的資料來減少儲存資料所需的實體容量。

為Cloud Volumes ONTAP設定 Google Cloud 網路

NetApp Console負責設定Cloud Volumes ONTAP的網路元件，例如 IP 位址、網路遮罩和路由。您需要確保可以存取外部網路、有足夠的私人 IP 位址、有正確的連線等等。

如果你想部署 HA 對，你應該"了解 HA 對在 Google Cloud 中的工作原理"。

Cloud Volumes ONTAP的要求

Google Cloud 必須滿足以下要求。

單節點系統的特定要求

如果要部署單節點系統、請確保您的網路符合下列要求。

一個 VPC

單節點系統需要一個虛擬私有雲（VPC）。

私人 IP 位址

對於 Google Cloud 中的單節點系統，Console 會將私人 IP 位址指派給下列各項：

- 節點
- 簇
- 儲存虛擬機
- 數據 NAS LIF
- 資料 iSCSI LIF

如果您使用 API 部署Cloud Volumes ONTAP並指定下列標誌，則可以跳過建立儲存虛擬機器 (SVM) 管理 LIF：

```
skipSvmManagementLif: true
```

LIF 是與實體連接埠關聯的 IP 位址。 SnapCenter等管理工具需要儲存虛擬機器 (SVM) 來管理 LIF。

HA 對的特定要求

如果要部署 HA 對，請確保您的網路符合以下要求。

一個或多個區域

您可以透過在多個區域或單一區域中部署 HA 配置來確保資料的高可用性。建立 HA 對時，控制台會提示您選擇多個區域或單一區域。

- 多區域（建議）

  跨三個區域部署 HA 配置可確保當一個區域內發生故障時資料仍然可用。請注意，與使用單一區域相比，寫入效能略低，但差異很小。

- 單區

  在單一區域中部署時， Cloud Volumes ONTAP HA 配置使用分散放置策略。此策略可確保 HA 配置免受區域內單點故障的影響，而無需使用單獨的區域來實現故障隔離。

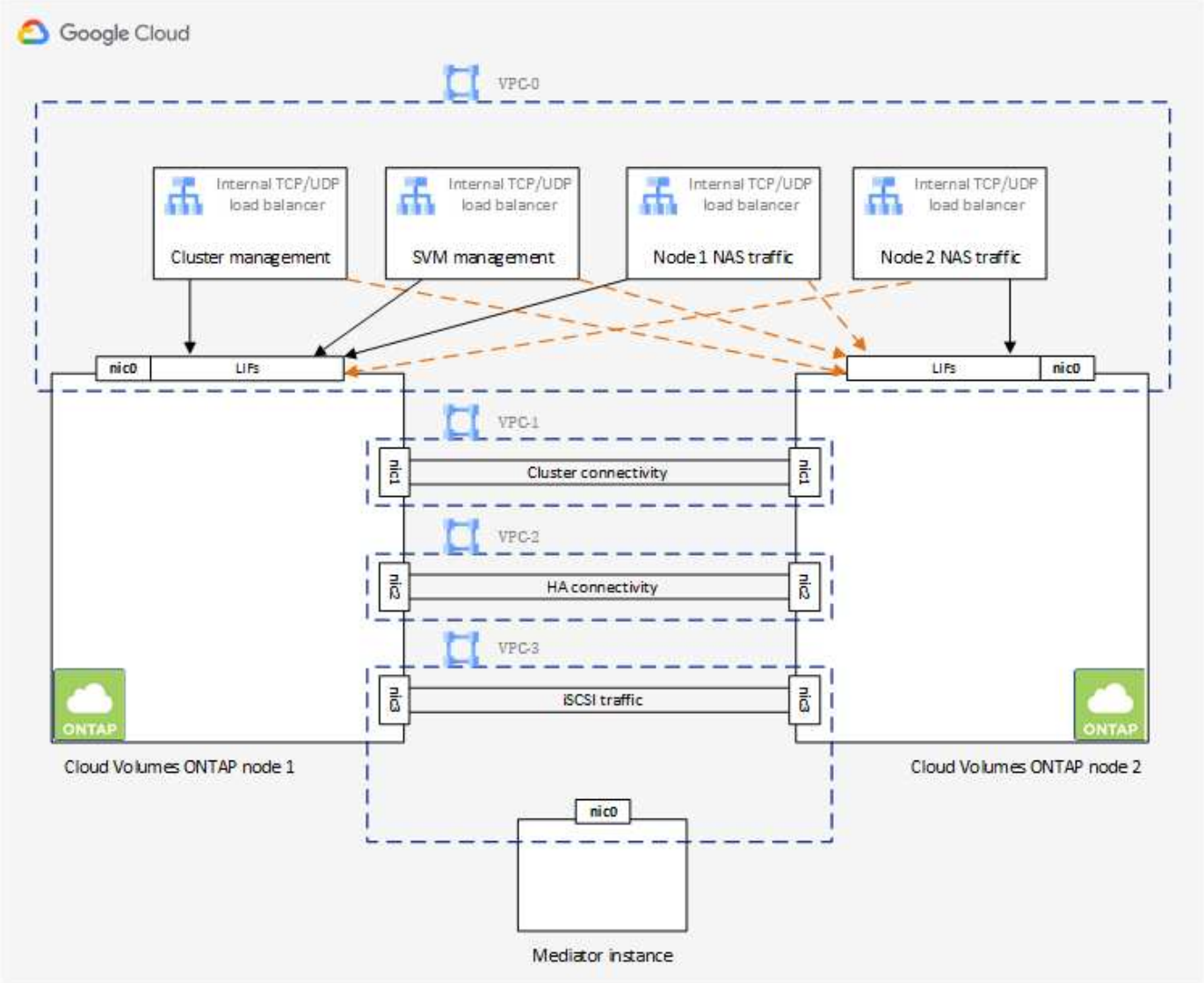
  這種部署模型確實降低了您的成本，因為區域之間沒有資料流出費用。

四個虛擬私有雲

HA 配置需要四個虛擬私有雲 (VPC)。需要四個 VPC，因為 Google Cloud 要求每個網路介面位於單獨的 VPC 網路中。

建立 HA 對時，控制台會提示您選擇四個 VPC：

- VPC-0 用於資料和節點的入站連接
- VPC-1、VPC-2 和 VPC-3 用於節點和 HA 中介之間的內部通信



子網

每個 VPC 都需要一個私有子網路。

如果將控制台代理程式放置在 VPC-0 中，則需要在子網路上啟用私人 Google 存取權限以存取 API 並啟用資料分層。

這些 VPC 中的子網路必須具有不同的 CIDR 範圍。它們不能有重疊的 CIDR 範圍。

私人 **IP** 位址

控制台會自動為 Google Cloud 中的Cloud Volumes ONTAP指派所需數量的私有 IP 位址。您需要確保您的網路有足夠的可用私有位址。

分配給 Cloud Volumes ONTAP 的 LIF 數量取決於您部署的是單節點系統還是 HA 配對。LIF 是與實體連接埠相關聯的 IP 位址。管理工具（例如 SnapCenter）需要 SVM 管理 LIF。

- 單節點 Console 會為單節點系統指派 4 個 IP 位址：
  - 節點管理 LIF
  - 集群管理 LIF
  - iSCSI 資料 LIF

    iSCSI LIF 透過 iSCSI 協定提供用戶端訪問，並被系統用於其他重要的網路工作流程。這些 LIF 是必需的，不應刪除。

  - NAS LIF

    如果您使用 API 部署Cloud Volumes ONTAP並指定下列標誌，則可以跳過建立儲存虛擬機器 (SVM) 管理 LIF：

```
skipSvmManagementLif: true
```

- **HA** 對 控制台為 HA 對分配 12-13 個 IP 位址：
  - 2 個節點管理 LIF (e0a)
  - 1 集群管理 LIF (e0a)
  - 2 個 iSCSI LIF (e0a)

    iSCSI LIF 透過 iSCSI 協定提供用戶端訪問，並被系統用於其他重要的網路工作流程。這些 LIF 是必需的，不應刪除。

  - 1 或 2 個 NAS LIF (e0a)
  - 2 個集群 LIF (e0b)
  - 2 個 HA 互連 IP 位址 (e0c)
  - 2 個 RSM iSCSI IP 位址（e0d）

    如果您使用 API 部署Cloud Volumes ONTAP並指定下列標誌，則可以跳過建立儲存虛擬機器 (SVM) 管

理 LIF：

```
skipSvmManagementLif: true
```

內部負載平衡器

控制台建立四個 Google Cloud 內部負載平衡器（TCP/UDP），用於管理傳入Cloud Volumes ONTAP HA 對的流量。您無需進行任何設定。我們將其列為一項要求只是為了告知您網路流量並減輕任何安全問題。

一個負載平衡器用於叢集管理，一個用於儲存虛擬機器 (SVM) 管理，一個用於到節點 1 的 NAS 流量，最後一個用於到節點 2 的 NAS 流量。

每個負載平衡器的設定如下：

- 一個共享的私人 IP 位址
- 一次全球健康檢查

  預設情況下，健康檢查使用的連接埠為63001、63002、63003。

- 一個區域 TCP 後端服務
- 一個區域 UDP 後端服務
- 一條 TCP 轉送規則
- 一條 UDP 轉送規則
- 全域存取已禁用

  儘管預設情況下會停用全域訪問，但支援在部署後啟用它。我們禁用它是因為跨區域流量會有明顯更高的延遲。我們希望確保您不會因為意外的跨區域坐騎而產生負面體驗。啟用此選項是為了滿足您的業務需求。

共享 **VPC**

Google Cloud 共享 VPC 和獨立 VPC 皆支援Cloud Volumes ONTAP和控制台代理。

對於單節點系統，VPC 可以是共用 VPC 或獨立 VPC。

對於 HA 對，需要四個 VPC。每個 VPC 可以是共享的，也可以是獨立的。例如，VPC-0 可以是共用 VPC，而 VPC-1、VPC-2 和 VPC-3 可以是獨立 VPC。

共用 VPC 可讓您跨多個專案配置和集中管理虛擬網路。您可以在_主機專案_中設定共用 VPC 網絡，並在_服務項目_中部署控制台代理程式和Cloud Volumes ONTAP虛擬機器實例。

"Google Cloud 文件：共享 VPC 概覽" 。

"查看控制台代理部署中涵蓋的所需共用 VPC 權限"

VPC 中的資料包鏡像

"資料包鏡像"必須在部署Cloud Volumes ONTAP的 Google Cloud 子網路中停用。

Cloud Volumes ONTAP系統需要出站網際網路存取才能存取外部端點以實現各種功能。如果這些端點在具有嚴格安全要求的環境中被阻止， Cloud Volumes ONTAP將無法正常運作。

控制台代理也會聯絡多個端點以進行日常操作。有關端點的信息，請參閱 "查看從控制台代理聯繫的端點"和 "準備好使用控制台的網絡"。

Cloud Volumes ONTAP端點

Cloud Volumes ONTAP使用這些端點與各種服務進行通訊。

端點	適用於	目的	部署模式	端點不可用時的影響
\ https://netapp-cloud-account.auth0.com	驗證	用於控制台中的身份驗證。	標準和限制模式。	用戶身份驗證失敗，以下服務仍然不可用： • Cloud Volumes ONTAP服務 • ONTAP服務 • 協定和代理服務
\ https://api.bluexp.netapp.com/tenancy	租賃	用於從控制台檢索Cloud Volumes ONTAP資源以授權資源和使用者。	標準和限制模式。	Cloud Volumes ONTAP資源和使用者未獲得授權。
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	用於將AutoSupport遙測資料傳送給NetApp支援。	標準和限制模式。	AutoSupport資訊仍未送達。

端點	適用於	目的	部署模式	端點不可用時的影響
https://cloudbuild.googleapis.com/v1（僅適用於私有模式部署）https://cloudkms.googleapis.com/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://compute.googleapis.com/compute/v1 https://www.googleapis.com/compute/beta https://www.googleapis.com/compute/v1/projects/ https://www.googleapis.com/deploymentmanager/v2/projects https://www.googleapis.com/storage/v1 https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1 https://iam.googleapis.com/v1 https://storage.googleapis.com/storage/v1	Google Cloud（商業用途）。	與 Google Cloud 服務通訊。	標準、受限和私人模式。	Cloud Volumes ONTAP無法與 Google Cloud 服務通訊以對 Google Cloud 中的控制台執行特定操作。

與其他網路中的**ONTAP**系統的連接

要在 Google Cloud 中的Cloud Volumes ONTAP系統和其他網路中的ONTAP系統之間複製數據，您必須在 VPC 和其他網路（例如您的公司網路）之間建立 VPN 連線。

"Google Cloud 文件：Cloud VPN 概覽" 。

防火牆規則

控制台建立 Google Cloud 防火牆規則，其中包含Cloud Volumes ONTAP成功運作所需的入站和出站規則。您可能希望參考連接埠以進行測試，或者您喜歡使用自己的防火牆規則。

Cloud Volumes ONTAP的防火牆規則需要入站和出站規則。如果您正在部署 HA 配置，這些是 VPC-0 中Cloud Volumes ONTAP的防火牆規則。

請注意，HA 配置需要兩組防火牆規則：

- 針對 VPC-0 中的 HA 組件的一組規則。這些規則允許對Cloud Volumes ONTAP進行資料存取。
- 針對 VPC-1、VPC-2 和 VPC-3 中的 HA 組件的另一組規則。這些規則對於 HA 組件之間的入站和出站通訊開放。了解更多 。

正在尋找有關控制台代理的資訊？ "查看控制台代理的防火牆規則"

入站規則

新增Cloud Volumes ONTAP系統時，您可以在部署期間選擇預先定義防火牆策略的來源篩選器：

- 僅限選定的 **VPC**：入站流量的來源過濾器是Cloud Volumes ONTAP系統的 VPC 子網路範圍和控制台代理程式所在的 VPC 子網路範圍。這是推薦的選項。
- 所有 **VPC**：入站流量的來源過濾器是 0.0.0.0/0 IP 範圍。

如果您使用自己的防火牆策略，請確保新增所有需要與Cloud Volumes ONTAP通訊的網絡，同時也要確保新增兩個位址範圍以允許內部 Google 負載平衡器正常運作。這些位址是 130.211.0.0/22 和 35.191.0.0/16。欲了解更多信息，請參閱 "Google Cloud 文件：負載平衡器防火牆規則"。

協定	港口	目的
所有 ICMP	全部	對執行個體執行 ping 操作
HTTP	80	使用叢集管理 LIF 的 IP 位址透過 HTTP 存取ONTAP System Manager Web 控制台
HTTPS	443	使用叢集管理 LIF 的 IP 位址與控制台代理程式建立連線並透過 HTTPS 存取ONTAP System Manager Web 控制台
SSH	22	透過 SSH 存取叢集管理 LIF 或節點管理 LIF 的 IP 位址
TCP	111	NFS 的遠端過程調用
TCP	139	CIFS 的 NetBIOS 服務會話
TCP	161-162	簡單網路管理協議
TCP	445	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
TCP	635	NFS 掛載
TCP	749	Kerberos
TCP	2049	NFS 伺服器守護程式
TCP	3260	透過 iSCSI 資料 LIF 進行 iSCSI 訪問
TCP	4045	NFS 鎖守護程式
TCP	4046	NFS 網路狀態監視器
TCP	10000	使用 NDMP 備份
TCP	11104	SnapMirror群集間通訊會話的管理
TCP	11105	使用集群間 LIF 進行SnapMirror資料傳輸
TCP	63001-63050	負載平衡探測端口以確定哪個節點是健康的（僅 HA 對需要）

協定	港口	目的
UDP	111	NFS 的遠端過程調用
UDP	161-162	簡單網路管理協議
UDP	635	NFS 掛載
UDP	2049	NFS 伺服器守護程式
UDP	4045	NFS 鎖守護程式
UDP	4046	NFS 網路狀態監視器
UDP	4049	NFS rquotad 協議

出站規則

Cloud Volumes ONTAP的預設安全群組開啟所有出站流量。如果可以接受，請遵循基本的出站規則。如果您需要更嚴格的規則，請使用進階出站規則。

基本出站規則

Cloud Volumes ONTAP的預設安全群組包括以下出站規則。

協定	港口	目的
所有 ICMP	全部	所有出站流量
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高級出站規則

如果您需要對出站流量製定嚴格的規則，則可以使用下列資訊僅開啟Cloud Volumes ONTAP出站通訊所需的連接埠。 Cloud Volumes ONTAP叢集使用下列連接埠來調節節點流量。

來源是Cloud Volumes ONTAP系統的介面（IP 位址）。

服務	協定	港口	來源	目的地	目的
活動目錄	TCP	88	節點管理 LIF	Active Directory 林	Kerberos V 驗證
	UDP	137	節點管理 LIF	Active Directory 林	NetBIOS 名稱服務
	UDP	138	節點管理 LIF	Active Directory 林	NetBIOS 資料封包服務
	TCP	139	節點管理 LIF	Active Directory 林	NetBIOS 服務會話
	TCP 和 UDP	389	節點管理 LIF	Active Directory 林	LDAP
	TCP	445	節點管理 LIF	Active Directory 林	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
	TCP	464	節點管理 LIF	Active Directory 林	Kerberos V 更改和設定密碼（SET_CHANGE）
	UDP	464	節點管理 LIF	Active Directory 林	Kerberos 金鑰管理
	TCP	749	節點管理 LIF	Active Directory 林	Kerberos V 更改和設定密碼（RPCSEC_GSS）
	TCP	88	資料 LIF（NFS、CIFS、iSCSI）	Active Directory 林	Kerberos V 驗證
	UDP	137	資料 LIF（NFS、CIFS）	Active Directory 林	NetBIOS 名稱服務
	UDP	138	資料 LIF（NFS、CIFS）	Active Directory 林	NetBIOS 資料封包服務
	TCP	139	資料 LIF（NFS、CIFS）	Active Directory 林	NetBIOS 服務會話
	TCP 和 UDP	389	資料 LIF（NFS、CIFS）	Active Directory 林	LDAP
	TCP	445	資料 LIF（NFS、CIFS）	Active Directory 林	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
	TCP	464	資料 LIF（NFS、CIFS）	Active Directory 林	Kerberos V 更改和設定密碼（SET_CHANGE）
	UDP	464	資料 LIF（NFS、CIFS）	Active Directory 林	Kerberos 金鑰管理
	TCP	749	資料 LIF（NFS、CIFS）	Active Directory 林	Kerberos V 更改和設定密碼（RPCSEC_GSS）
AutoSupport	HTTPS	443	節點管理 LIF	mysupport.netapp.com	AutoSupport （預設為 HTTPS）
	HTTP	80	節點管理 LIF	mysupport.netapp.com	AutoSupport （僅當傳輸協定從 HTTPS 變更為 HTTP 時）
	TCP	3128	節點管理 LIF	控制台代理	如果出站網路連線不可用，則透過控制台代理上的代理伺服器傳送AutoSupport訊息

服務	協定	港口	來源	目的地	目的
配置備份	HTTP	80	節點管理 LIF	http://<控制台代理 IP 位址>/occm/offboxconfig	將配置備份傳送到控制台代理程式。"ONTAP文檔"
DHCP	UDP	68	節點管理 LIF	DHCP	DHCP 用戶端首次設定
DHCP服務	UDP	67	節點管理 LIF	DHCP	DHCP 伺服器
DNS	UDP	53	節點管理 LIF 和資料 LIF（NFS、CIFS）	DNS	DNS
NDMP	TCP	18600–18699	節點管理 LIF	目標伺服器	NDMP 拷貝
SMTP	TCP	25	節點管理 LIF	郵件伺服器	SMTP 警報，可用於AutoSupport
SNMP	TCP	161	節點管理 LIF	監控伺服器	透過 SNMP 陷阱進行監控
	UDP	161	節點管理 LIF	監控伺服器	透過 SNMP 陷阱進行監控
	TCP	162	節點管理 LIF	監控伺服器	透過 SNMP 陷阱進行監控
	UDP	162	節點管理 LIF	監控伺服器	透過 SNMP 陷阱進行監控
SnapMirror	TCP	11104	集群間 LIF	ONTAP叢集間 LIF	SnapMirror群集間通訊會話的管理
	TCP	11105	集群間 LIF	ONTAP叢集間 LIF	SnapMirror資料傳輸
系統日誌	UDP	514	節點管理 LIF	Syslog伺服器	Syslog 轉送訊息

VPC-1、**VPC-2** 和 **VPC-3** 的規則

在 Google Cloud 中，HA 配置部署在四個 VPC 中。 VPC-0 中的 HA 設定所需的防火牆規則是以上所列的Cloud Volumes ONTAP。

同時，為 VPC-1、VPC-2 和 VPC-3 中的執行個體所建立的預定義防火牆規則支援透過所有協定和連接埠進行入站通訊。這些規則支援 HA 節點之間的通訊。

從 HA 節點到 HA 中介的通訊透過連接埠 3260（iSCSI）進行。

> 為了讓新的 Google Cloud HA 對部署實現較高的寫入速度，VPC-1、VPC-2 和 VPC-3 需要至少 8,896 位元組的最大傳輸單元 (MTU)。如果您選擇將現有的 VPC-1、VPC-2 和 VPC-3 升級到 8,896 位元組的 MTU，則必須在設定過程中關閉使用這些 VPC 的所有現有 HA 系統。

私有模式部署的 **Infrastructure Manager** 組態

如果您想要以私有模式部署 Cloud Volumes ONTAP 9.16.1 或更高版本，則需要進行一些設定變更，以便 Cloud Volumes ONTAP 可以使用 Google Cloud Infrastructure Manager 作為部署服務，而不是 Google 最終將棄用的 Deployment Manager。

開始之前

- 請確保您的 Cloud Volumes ONTAP 系統版本為 9.16.1 或更高版本。如果不是，請升級您的系統。有關說明，請參閱 "升級Cloud Volumes ONTAP"。
- 請確保已啟用 Google Cloud API。請參閱 "啟用 Google Cloud API"。
- 請確保已啟用 Cloud Build API。請參閱 "在此處啟用 Cloud Build API"。
- 確認 Console 代理程式的服務帳戶擁有所有標準權限。此外，請確保該服務帳戶擁有 `cloudbuild.workerpools.get`和 `cloudbuild.workerpools.list`權限。請參閱 "控制台代理的 Google Cloud 權限"。

步驟

1. 使用此配置在與 Cloud Volumes ONTAP 部署相同的區域中建立私有工作池。有關建立私有工作池的資訊，請參閱 "Google Cloud 文件：建立和管理私有資源池"和 "Google Cloud Build 定價"。

   工作池必須具有以下配置：

   - 機器類型：e2-medium
   - 磁碟大小：100 GB
   - 指派外部 IP：False
   - 網路：預設或專用網路。
   - 已配置子網路以存取 "Google API"。請執行以下步驟以確保子網路可以存取 Google API：
     i. 請確保已為子網路啟用「Private Google Access」。
     ii. 前往 **VPC Network** 層級 **> Private Service Access** 標籤 **> Allocated IP ranges for services**。
     iii. 選擇 **Allocate IP range** 並為與 Google Compute Service 的私有連線分配內部 IP 範圍。
     iv. 在 **Private connection to services** 中，選擇 **Create Connection**。
     v. 選擇 **Connected service producer = Google Cloud Platform**。
     vi. 為上一個步驟中建立的私人連線 IP 範圍指派配置。
2. 部署此工作池並保持其運行，以進行 Cloud Volumes ONTAP 管理。Google Cloud 使用此工作池在隔離環境中執行所有 Terraform 操作。
3. 以私有模式部署 Cloud Volumes ONTAP 時，請在 **GCP Worker Pool** 欄位中選擇此工作池的名稱。請參閱 "在 Google Cloud 啟動Cloud Volumes ONTAP" 以取得相關說明。

控制台代理的要求

如果您尚未建立控制台代理，則應查看網路需求。

- "查看控制台代理程式的網路要求"
- "Google Cloud 中的防火牆規則"

支援控制台代理的網路配置

您可以使用為控制台代理程式設定的代理伺服器來啟用來自Cloud Volumes ONTAP存取。控制台支援兩種類型的代理：

- 明確代理：來自Cloud Volumes ONTAP 的出站流量使用控制台代理代理程式設定期間指定的代理伺服器的 HTTP 位址。控制台代理管理員可能還配置了使用者憑證和根 CA 憑證以進行額外的驗證。Cloud Volumes

ONTAP顯式代理程式有可用的根 CA 證書，請確保使用 "ONTAP CLI：安全性憑證安裝"命令。

- 透明代理：網路配置為透過控制台代理代理程式自動路由來自Cloud Volumes ONTAP 的出站流量。設定透明代理程式時，控制台代理程式管理員僅需要提供用於從Cloud Volumes ONTAP進行連接的根 CA 證書，而不是代理伺服器的 HTTP 位址。確保使用以下方式取得相同的根 CA 憑證並將其上傳到您的Cloud Volumes ONTAP系統 "ONTAP CLI：安全性憑證安裝"命令。

有關為控制台代理程式配置代理伺服器的信息，請參閱 "配置控制台代理以使用代理伺服器"。

在 **Google Cloud** 中為**Cloud Volumes ONTAP**設定網路標籤

在控制台代理程式的透明代理程式配置期間，管理員會為 Google Cloud 新增網路標籤。您需要取得並手動新增Cloud Volumes ONTAP配置的相同網路標籤。此標籤對於代理伺服器正常運作是必要的。

1. 在 Google Cloud Console 中、找到您的 Cloud Volumes ONTAP 系統。
2. 前往*詳細資料>網路>網路標籤*。
3. 新增用於控制台代理的標籤並儲存配置。

相關主題

- "驗證Cloud Volumes ONTAP 的AutoSupport設置"
- "了解ONTAP內部端口" 。

設定 **VPC** 服務控制以在 **Google Cloud** 中部署**Cloud Volumes ONTAP**

當選擇使用 VPC 服務控制鎖定您的 Google Cloud 環境時，您應該了解NetApp Console和Cloud Volumes ONTAP如何與 Google Cloud API 交互，以及如何配置您的服務邊界以部署控制台和Cloud Volumes ONTAP。

VPC 服務控制使您能夠控制對受信任邊界之外的 Google 管理服務的訪問，阻止來自不受信任位置的資料訪問，並降低未經授權的資料傳輸風險。 "詳細了解 Google Cloud VPC 服務控制" 。

NetApp服務如何與 **VPC** 服務控制進行通訊

控制台直接與 Google Cloud API 通訊。這可以從 Google Cloud 外部的外部 IP 位址觸發（例如，來自 api.services.cloud.netapp.com），也可以從 Google Cloud 內部指派給控制台代理程式的內部位址觸發。

根據控制台代理程式的部署方式，您的服務邊界可能需要做出某些例外。

圖片

Cloud Volumes ONTAP 和 Console 都使用來自 Google Cloud 內由 NetApp 管理的專案中的映像。如果您的組織有政策阻止使用非組織內部託管的映像，這可能會影響 Console 代理程式和 Cloud Volumes ONTAP 的部署。

您可以使用手動安裝方法手動部署控制台代理，但Cloud Volumes ONTAP也需要從NetApp專案中擷取映像。您必須提供允許清單才能部署控制台代理程式和Cloud Volumes ONTAP。

部署控制台代理

部署控制台代理程式的使用者需要能夠引用 projectId 為 *netapp-cloudmanager* 且專案編號為 *14190056516* 中所託管的映像。

- 控制台服務帳戶需要引用服務項目中託管在 projectId *netapp-cloudmanager* 中的映像和項目編號 *14190056516*。
- 預設 Google API 服務代理程式的服務帳戶需要引用服務項目中 projectId *netapp-cloudmanager* 和項目編號 *14190056516* 中託管的圖片。

下面定義了使用 VPC 服務控制拉取這些影像所需的規則範例。

VPC 服務控制邊界策略

策略允許對 VPC Service Controls 規則集設定例外。有關策略的更多資訊，請造訪 "Google Cloud VPC Service Controls 政策文件"。

若要設定控制台所需的策略，請導覽至您組織內的 VPC 服務控制邊界並新增下列策略。這些欄位應與 VPC 服務控制策略頁面中給出的選項相符。也要注意，*所有*規則都是必需的，並且規則集中應該使用*OR*參數。

入口規則

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

或者

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

或者

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

出口規則

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

上面列出的項目編號是NetApp用於儲存控制台代理程式和Cloud Volumes ONTAP 的圖像的專案 *netapp-cloudmanager*。

為Cloud Volumes ONTAP建立 Google Cloud 服務帳號

Cloud Volumes ONTAP需要 Google Cloud 服務帳戶來實現兩個目的。第一個是當你啟用"資料分層"將冷資料分層到 Google Cloud 中的低成本物件儲存。第二個是當你啟用"NetApp Backup and Recovery"將磁碟區備份到低成本的物件儲存。

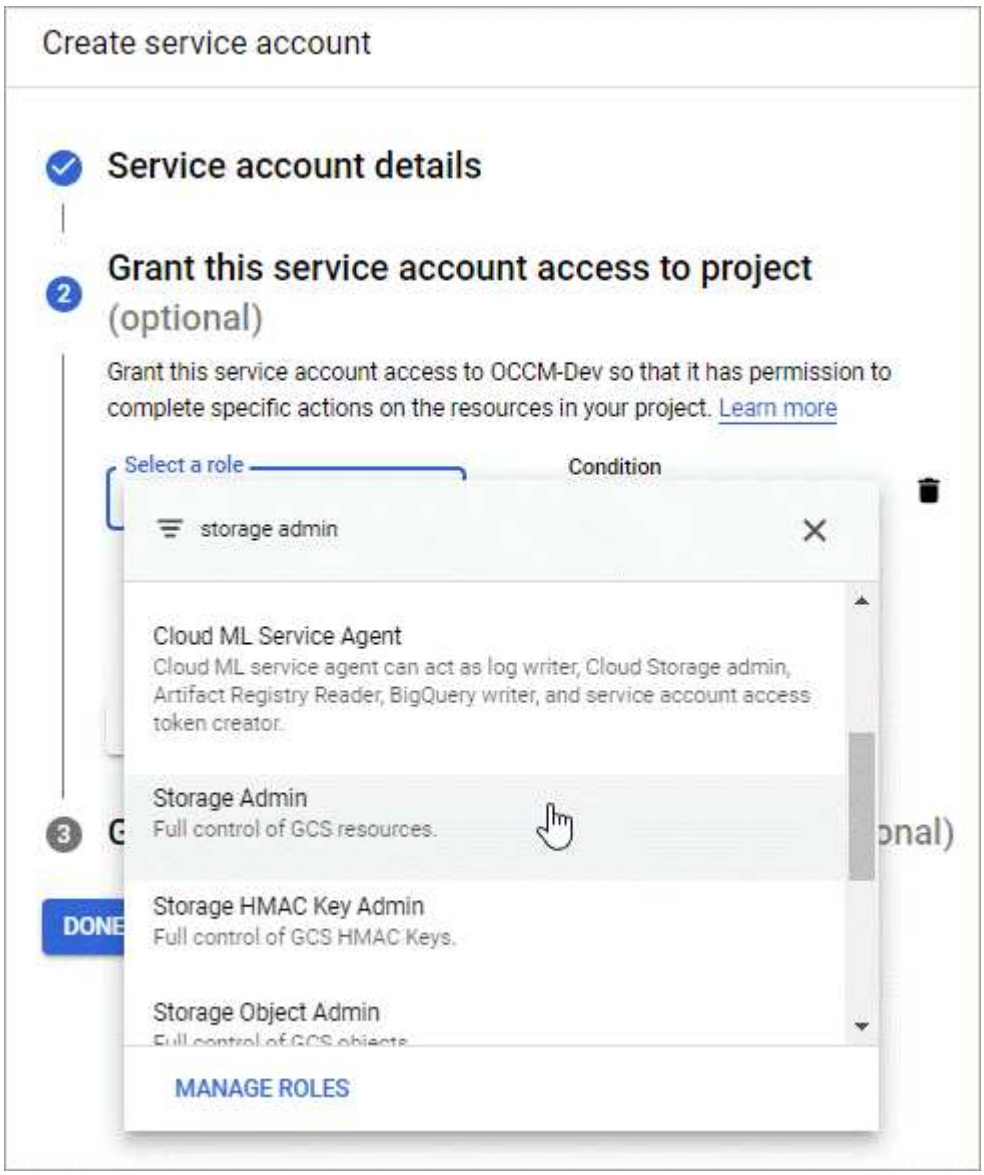
Cloud Volumes ONTAP使用服務帳戶來存取和管理一個用於分層資料的儲存桶以及另一個用於備份的儲存桶。

您可以設定一個服務帳戶並將其用於兩種用途。服務帳戶必須具有*儲存管理員*角色。

步驟

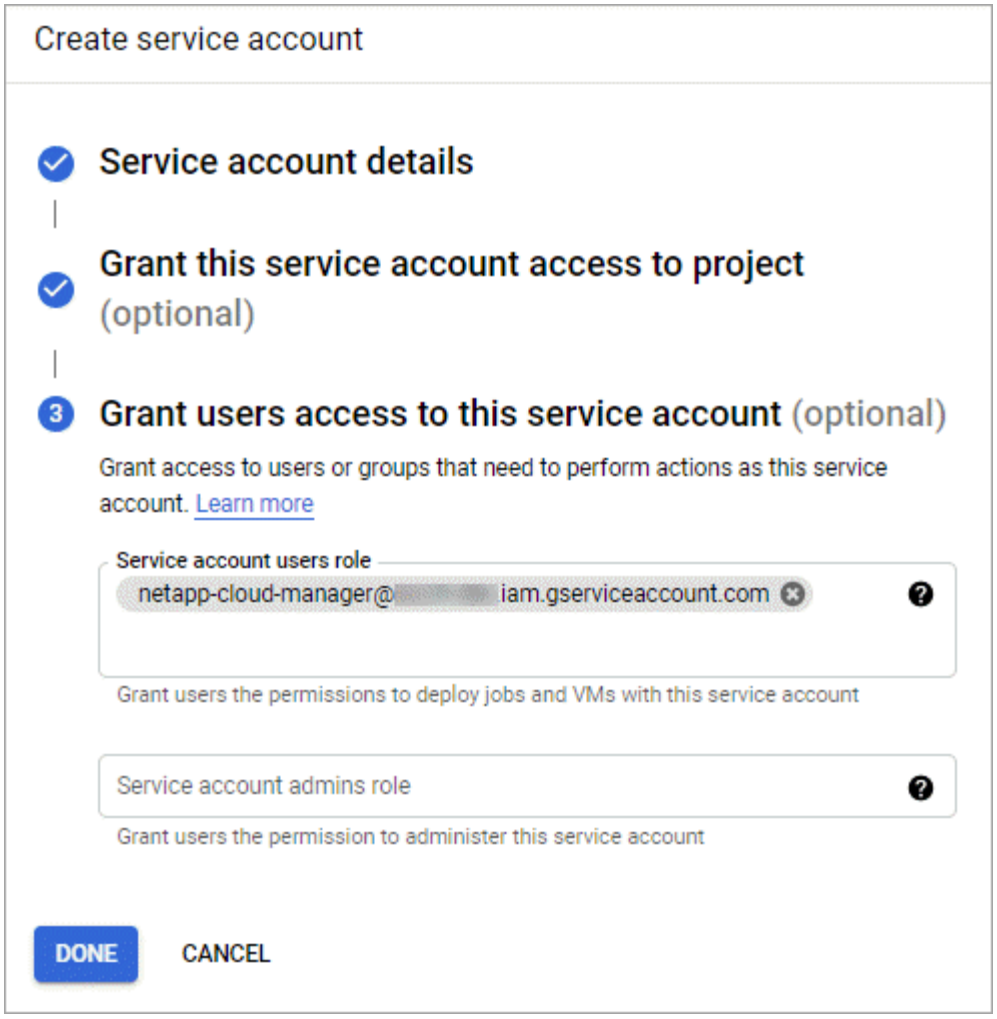
1. 在 Google Cloud Console 中 "前往服務帳戶頁面"。
2. 選擇您的項目。
3. 點擊*建立服務帳戶*並提供所需資訊。
    a. 服務帳戶詳細資料：輸入名稱和描述。

b. 授予此服務帳戶存取項目的權限：選擇*儲存管理員*角色。



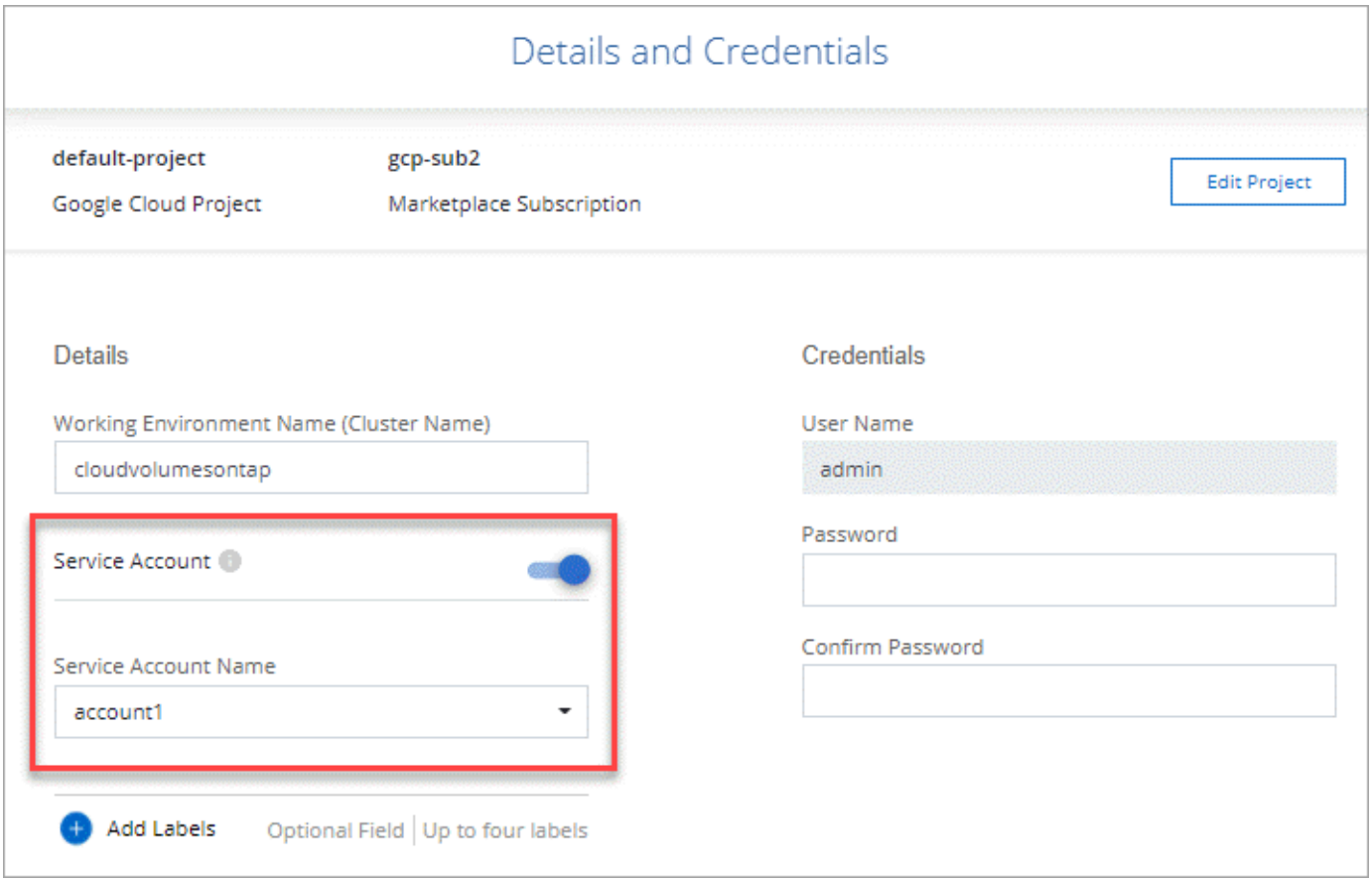
c. 授予使用者存取此服務帳戶的權限：將控制台代理服務帳戶作為_服務帳戶使用者_新增至此新服務帳戶。

此步驟僅對於資料分層是必需的。備份和還原不需要它。



下一步是什麼？

稍後建立Cloud Volumes ONTAP系統時，您需要選擇服務帳戶。



將客戶管理的加密金鑰與Cloud Volumes ONTAP結合使用

雖然 Google Cloud Storage 總是會在將資料寫入磁碟之前加密，但您可以使用 API 建立使用_客戶管理加密金鑰_的Cloud Volumes ONTAP系統。這些是您使用雲端金鑰管理服務在 GCP 中產生和管理的金鑰。

步驟

1. 確保控制台代理服務帳戶在儲存金鑰的項目中具有專案層級的正確權限。

   權限已在以下文件中提供： "預設的服務帳戶權限"但如果您使用其他項目來管理雲端金鑰服務，則可能無法套用此功能。

   權限如下：

   ```
   - cloudkms.cryptoKeyVersions.useToEncrypt
   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.list
   ```

2. 確保 "Google Compute Engine 服務代理"對金鑰具有 Cloud KMS 加密器/解密器權限。

   服務帳戶的名稱使用以下格式：「service-[service_project_number]@compute-system.iam.gserviceaccount.com」。

"Google Cloud 文件：將 IAM 與 Cloud KMS 結合使用 - 授予資源角色"

3. 透過呼叫 get 指令來取得金鑰的“id” `/gcp/vsa/metadata/gcp-encryption-keys` API 呼叫或透過在 GCP 控制台中的鍵上選擇「複製資源名稱」。
4. 如果使用客戶管理的加密金鑰並將資料分層到物件存儲， NetApp Console會嘗試使用用於加密持久磁碟的相同金鑰。但您首先需要啟用 Google Cloud Storage 儲存桶才能使用金鑰：

   a. 請依照下列步驟尋找 Google Cloud Storage 服務代理 "Google Cloud 文件：取得雲端儲存服務代理"。

   b. 導覽至加密金鑰並為 Google Cloud Storage 服務代理程式指派 Cloud KMS Encrypter/Decrypter 權限。

   有關詳細信息，請參閱 "Google Cloud 文件：使用客戶管理的加密金鑰"

5. 建立系統時，請在 API 請求中使用「gcpEncryption」參數。

   例子

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-
1/cryptoKeys/generatedkey1"
  }
```

請參閱 "NetApp Console自動化文檔"有關使用“GcpEncryption”參數的更多詳細資訊。

在 Google Cloud 中設定Cloud Volumes ONTAP許可

在您決定要與Cloud Volumes ONTAP一起使用哪種授權選項後，需要執行幾個步驟才能在建立新系統時選擇該授權選項。

免費增值

選擇免費加值服務，免費使用Cloud Volumes ONTAP，最高可提供 500 GiB 的設定容量。"了解有關免費增值服務的更多信息" 。

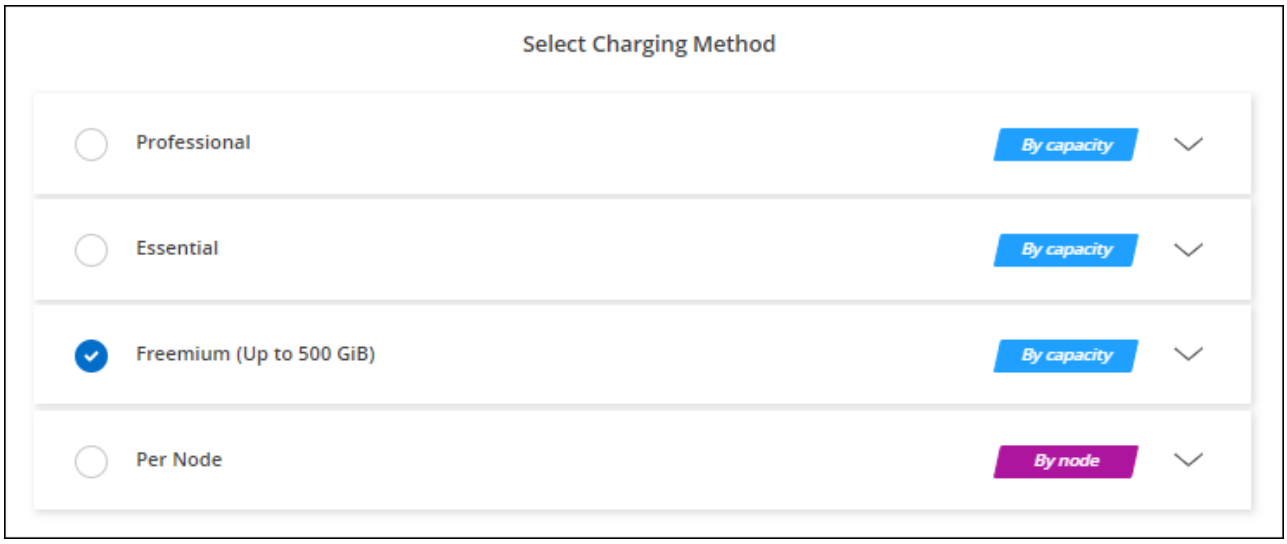
步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在「系統」頁面上，按一下「新增系統」並依照NetApp Console中的步驟進行操作。

   a. 在*詳細資訊和憑證*頁面上，按一下*編輯憑證>新增訂閱*，然後依照指示訂閱 Google Cloud Marketplace 中的即用即付產品。

   除非您超過 500 GiB 的預配置容量，否則您無需透過市場訂閱付費，此時系統將自動轉換為"基本套餐"。

   b. 返回控制台後，到達收費方式頁面時選擇「免費增值」。



"查看在 Google Cloud 中啟動Cloud Volumes ONTAP 的逐步說明" 。

基於容量的許可證

基於容量的許可使您能夠按 TiB 容量支付Cloud Volumes ONTAP費用。基於容量的許可以_包_的形式提供：Essentials 或 Professional 包。

Essentials 和 Professional 套餐提供以下幾種消費模式或購買選項：

- 從NetApp購買的授權（自帶授權 (BYOL)）
- Google Cloud Marketplace 的按小時付費 (PAYGO) 訂閱
- 年度合約

"了解有關基於容量的許可的更多信息" 。

以下部分介紹如何開始使用每種消費模型。

BYOL

透過從NetApp購買授權 (BYOL) 進行預付款，以便在任何雲端供應商部署Cloud Volumes ONTAP系統。

已限制 BYOL 授權的購買、延期和續約。有關更多信息，請參閱 "Cloud Volumes ONTAP的 BYOL 授權可用性受限" 。

步驟

1. "聯絡NetApp銷售人員以取得許可證"
2. "將您的NetApp支援網站帳號新增至NetApp Console"

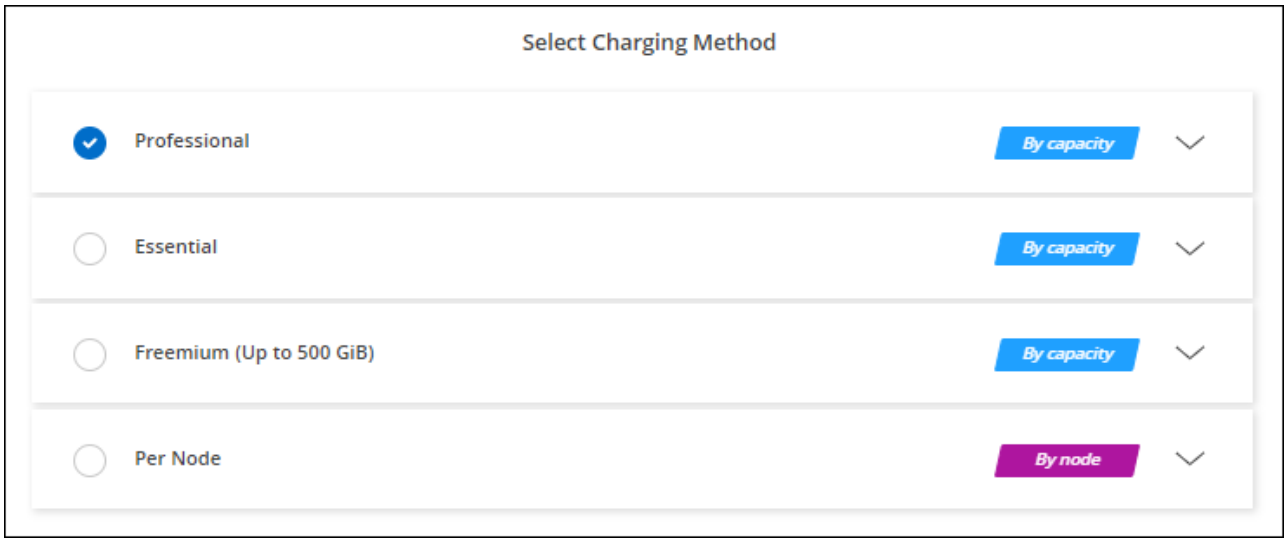
   控制台會自動查詢 NetApp 的授權服務，以取得與您的NetApp支援網站帳戶相關的授權的詳細資訊。如果沒有錯誤，控制台將新增許可證。

   您必須先從控制台取得許可證，然後才能與Cloud Volumes ONTAP一起使用。如果需要的話，你可以"手動將許可證新增至控制台"。

3. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。
   a. 在*詳細資訊和憑證*頁面上，按一下*編輯憑證>新增訂閱*，然後依照指示訂閱 Google Cloud Marketplace 中的即用即付產品。

      總是會先向您從NetApp購買的許可證收費，但如果您超出許可容量或許可證期限到期，則會按照市場上的小時費率向您收費。

   b. 返回控制台後，在到達收費方式頁面時選擇基於容量的套餐。



"查看在 Google Cloud 中啟動Cloud Volumes ONTAP 的逐步說明" 。

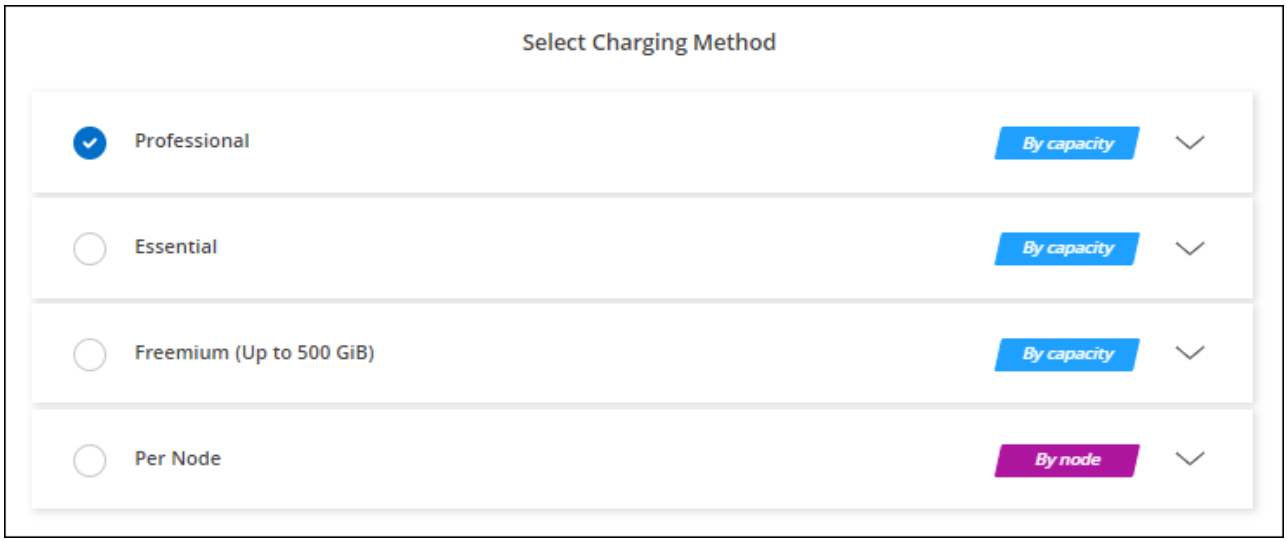
PAYGO 訂閱

透過訂閱雲端供應商市場提供的服務按小時付費。

當您建立Cloud Volumes ONTAP系統時，控制台會提示您訂閱 Google Cloud Marketplace 中提供的協定。然後將該訂閱與系統關聯以進行收費。您可以將同一訂閱用於其他系統。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。
   a. 在*詳細資訊和憑證*頁面上，按一下*編輯憑證>新增訂閱*，然後依照指示訂閱 Google Cloud Marketplace 中的即用即付產品。
   b. 返回控制台後，在到達收費方式頁面時選擇基於容量的套餐。



"查看在 Google Cloud 中啟動Cloud Volumes ONTAP 的逐步說明" 。

您可以從「設定」>「憑證」頁面管理與您的帳戶相關的 Google Cloud Marketplace 訂閱。 "了解如何管理您的 Google Cloud 憑證和訂閱"

年度合約

透過購買年度合約每年支付Cloud Volumes ONTAP 的費用。

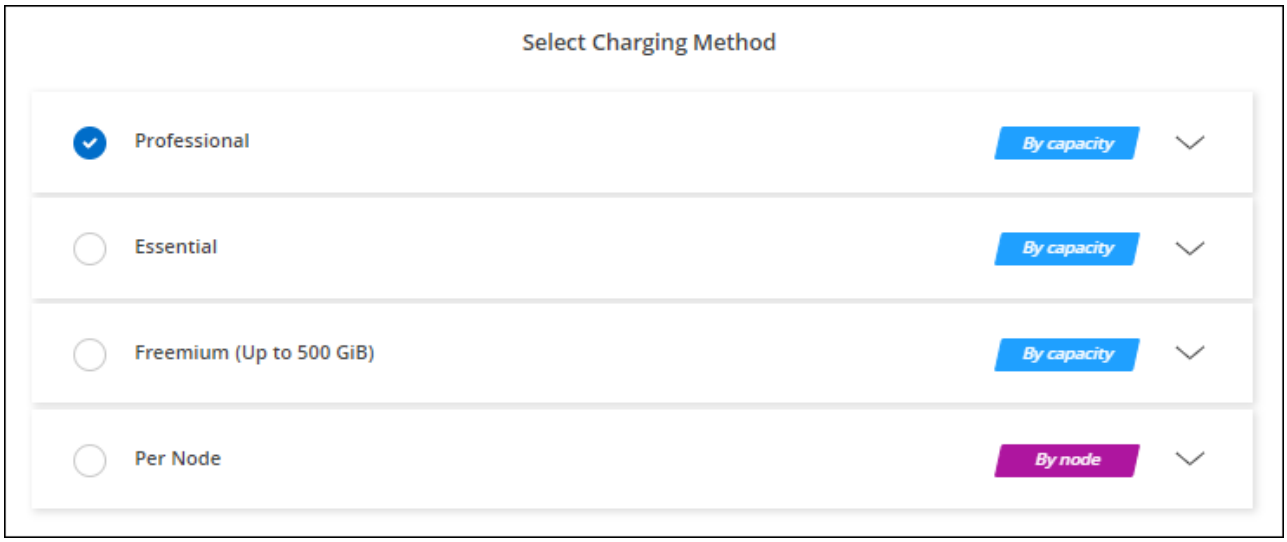
步驟

1. 聯絡您的NetApp銷售代表購買年度合約。

   該合約在 Google Cloud Marketplace 中以私人優惠形式提供。

   NetApp與您分享私人優惠後，您可以在系統建立期間從 Google Cloud Marketplace 訂閱時選擇年度方案。

2. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。
   a. 在*詳細資訊和憑證*頁面上，按一下*編輯憑證>新增訂閱*，然後依照指示在 Google Cloud Marketplace 中訂閱年度方案。
   b. 在 Google Cloud 中，選擇與您的帳戶共享的年度計劃，然後按一下*訂閱*。
   c. 返回控制台後，在到達收費方式頁面時選擇基於容量的套餐。



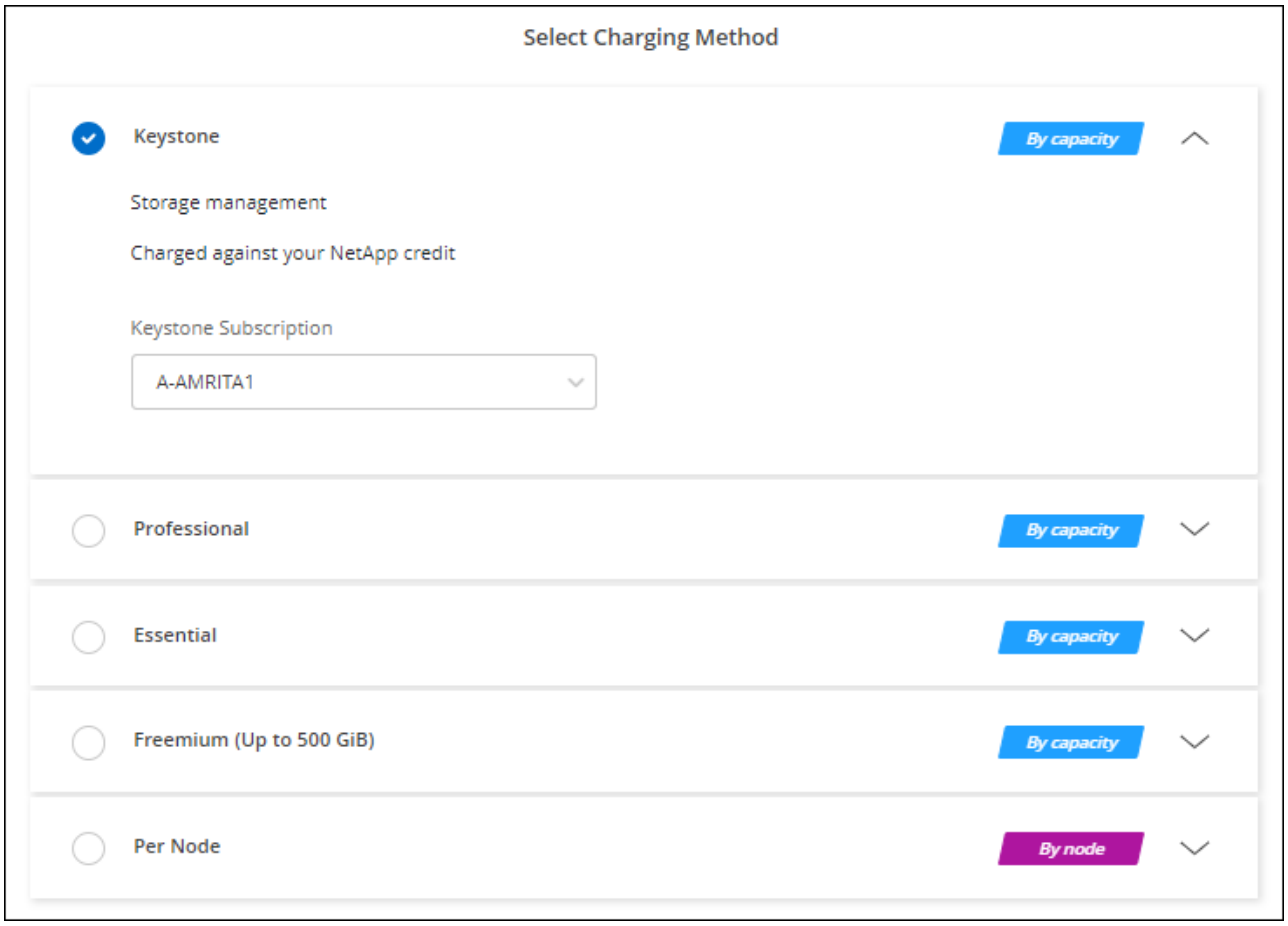
"查看在 Google Cloud 中啟動Cloud Volumes ONTAP 的逐步說明" 。

Keystone訂閱

Keystone訂閱是一種按需付費的訂閱式服務。"了解有關NetApp Keystone訂閱的更多信息" 。

步驟

1. 如果您尚未訂閱， "聯絡NetApp"
2. 聯絡NetApp 授權您的控制台使用者帳號擁有一個或多個Keystone訂閱。
3. NetApp授權您的帳戶後，"連結您的訂閱以用於Cloud Volumes ONTAP" 。
4. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。
    a. 當提示選擇充電方式時，選擇Keystone Subscription 充電方式。



"查看在 Google Cloud 中啟動Cloud Volumes ONTAP 的逐步說明" 。

基於節點的許可證

基於節點的許可證是Cloud Volumes ONTAP的上一代許可證。基於節點的授權可以從NetApp (BYOL) 購買，並且僅在特定情況下才可以續訂授權。有關信息，請參閱：

- "基於節點的許可證的可用性終止"
- "基於節點的許可證的可用性終止"
- "將基於節點的許可證轉換為基於容量的許可證"

在 Google Cloud 啟動Cloud Volumes ONTAP

您可以在單一節點設定中啟動Cloud Volumes ONTAP ，也可以在 Google Cloud 中以 HA 對的形式啟動 Cloud Volumes ONTAP。

開始之前

開始之前您需要以下內容。

- 已啟動並執行的 NetApp Console 代理程式。
  - 你應該有一個 "與您的系統關聯的控制台代理"。

- "您應該準備好讓控制台代理程式始終處於運行狀態" 。
- 與控制台代理程式關聯的服務帳戶 "應該具有所需的權限"

- 了解您想要使用的配置。

  您應該已經做好準備，選擇配置並從管理員處獲取 Google Cloud 網路資訊。有關詳細信息，請參閱"規劃您的Cloud Volumes ONTAP配置"。

- 了解設定Cloud Volumes ONTAP許可所需的條件。

  "了解如何設定許可" 。

- Google Cloud API 應該 "在您的專案中啟用"：
  - 雲端部署管理器 V2 API
  - 雲端日誌 API
  - 雲端資源管理器 API
  - 計算引擎 API
  - 身分識別和存取管理 (IAM) API

在 **Google Cloud** 啟動單節點系統

在NetApp Console中建立一個系統以在 Google Cloud 中啟動Cloud Volumes ONTAP 。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，點擊*新增系統*並依照指示操作。
3. 選擇位置：選擇*Google Cloud*和* Cloud Volumes ONTAP*。
4. 如果出現提示， "建立控制台代理" 。
5. 詳細資料和憑證：選擇一個項目，指定一個群集名稱，可選地選擇一個服務帳戶，可選地新增標籤，然後指定憑證。

   下表描述了您可能需要指導的欄位：

場地	描述
系統名稱	控制台使用系統名稱來命名Cloud Volumes ONTAP系統和 Google Cloud VM 執行個體。如果您選擇該選項，它也會使用該名稱作為預先定義安全性群組的前綴。
服務帳戶名稱	如果你打算使用"資料分層"或者 "NetApp Backup and Recovery"使用Cloud Volumes ONTAP，則需要啟用*服務帳戶*並選擇具有預先定義儲存管理員角色的服務帳戶。"了解如何建立服務帳號" 。
添加標籤	標籤是您的 Google Cloud 資源的元資料。控制台將標籤新增至Cloud Volumes ONTAP系統以及與該系統關聯的 Google Cloud 資源。建立系統時，您可以從使用者介面新增多達四個標籤，然後可以在建立系統後新增更多標籤。請注意，在建立系統時，API 不會將您限制為四個標籤。有關標籤的信息，請參閱 "Google Cloud 文件：標記資源"。

場地	描述
使用者名稱和密碼	這些是Cloud Volumes ONTAP叢集管理員帳戶的憑證。您可以使用這些憑證透過ONTAP System Manager 或ONTAP CLI 連線到Cloud Volumes ONTAP 。保留預設的_admin_使用者名稱或將其變更為自訂使用者名稱。
編輯項目	選擇您希望Cloud Volumes ONTAP駐留的項目。預設項目是控制台所在的項目。 如果下拉清單中沒有顯示其他專案，則表示您尚未將服務帳戶與其他專案建立關聯。請前往 Google Cloud Console，開啟 IAM 服務，然後選擇專案。將服務帳戶與您用於 Console 的角色新增至該專案。您需要為每個專案重複此步驟。 這是您為控制台設定的服務帳戶，"如本頁所述" 。 按一下「新增訂閱」將選定的憑證與訂閱關聯。 若要建立按使用量付費的Cloud Volumes ONTAP系統，您需要從 Google Cloud 市場選擇與Cloud Volumes ONTAP訂閱相關聯的 Google Cloud 專案。參考 "將市場訂閱與 Google Cloud 憑證關聯"。

6. 服務：選擇您想要在此系統上使用的服務。為了選擇備份和恢復，或使用NetApp Cloud Tiering，您必須在步驟 3 中指定服務帳戶。

   如果您想使用 WORM 和資料分層，則必須停用備份和還原並部署版本 9.8 或更高版本的Cloud Volumes ONTAP系統。

7. 位置與連線：選擇系統所在的 Google Cloud 區域和區域、選擇防火牆原則，並確認與 Google Cloud 儲存設備的網路連線以進行資料分層。

   下表描述了您可能需要指導的欄位：

場地	描述
連線驗證	若要將冷資料分層至 Google Cloud Storage 儲存桶，必須為Cloud Volumes ONTAP所在的子網路設定私人 Google Access。有關說明，請參閱 "Google Cloud 文件：配置私有 Google 存取權限"。
產生的防火牆策略	如果您讓控制台為您產生防火牆策略，則需要選擇如何允許流量： • 如果您選擇*僅限選定的 VPC*，則入站流量的來源過濾器是選定 VPC 的子網路範圍和控制台代理程式所在 VPC 的子網路範圍。這是推薦的選項。 • 如果您選擇*所有 VPC*，則入站流量的來源過濾器是 0.0.0.0/0 IP 範圍。
使用現有的防火牆策略	如果您使用現有的防火牆策略，請確保它包含所需的規則："了解Cloud Volumes ONTAP的防火牆規則"

8. 收費方式與 **NSS** 帳戶：指定您想要在此系統中使用的收費選項，然後指定NetApp支援網站帳號：
   - "了解Cloud Volumes ONTAP的授權選項"
   - "了解如何設定許可"

9. 預先配置套件：選擇其中一個套件以快速部署 Cloud Volumes ONTAP 系統，或按一下*建立我自己的組態*。預先配置套件會因所選的 Cloud Volumes ONTAP 版本而異。例如，對於 Cloud Volumes ONTAP 9.18.1 及更新版本，NetApp Console 會顯示包含 C3 VM 的套件，包括 Hyperdisk Balanced 磁碟。您可以根據工作負載需求修改組態，例如 IOPS 和處理量參數。

   如果您選擇其中一個套餐，您只需指定一個卷，然後審核並批准配置。

10. 許可：根據需要變更Cloud Volumes ONTAP版本並選擇機器類型。

    如果所選版本有較新的候選版本、通用版本或修補程式版本，則控制台在建立系統時會將其更新至該版本。例如，如果您選擇Cloud Volumes ONTAP 9.13.1 且 9.13.1 P4 可用，則會發生更新。更新不會從一個版本發生到另一個版本 — 例如，從 9.13 到 9.14。

11. 底層儲存資源：選擇初始聚合的設定：磁碟類型和每個磁碟的大小。

    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聚合中的所有磁碟以及使用簡單配置選項時控制台建立的任何其他聚合。您可以使用進階分配選項建立使用不同磁碟大小的聚合。

    有關選擇磁碟類型和大小的協助，請參閱"在 Google Cloud 中調整系統大小"。

12. 快閃記憶體快取、寫入速度和 **WORM**：

    a. 如有需要，請啟用 **Flash Cache** 或選擇 **Normal** 或 **High** 寫入速度。

       了解更多關於 "快閃記憶體"和"寫入速度"的信息。

       透過*高*寫入速度選項可實現高寫入速度和更高的 8,896 位元組最大傳輸單元 (MTU)。此外，8,896 的更高 MTU 要求選擇 VPC-1、VPC-2 和 VPC-3 進行部署。有關 VPC-1、VPC-2 和 VPC-3 的更多信息，請參閱 "VPC-1、VPC-2 和 VPC-3 的規則"。

    b. 如果需要，請啟動一次寫入、多次讀取 (WORM) 儲存。

       如果為Cloud Volumes ONTAP 9.7 及更低版本啟用了資料分層，則無法啟用 WORM。啟用 WORM 和分層後，恢復或降級到Cloud Volumes ONTAP 9.8 的操作將被阻止。

    "了解有關 WORM 存儲的更多信息" 。

    a. 如果您啟動 WORM 存儲，請選擇保留期限。

13. **Google Cloud Platform** 中的資料分層：選擇是否在初始聚合上啟用資料分層，為分層資料選擇儲存類，然後選擇具有預先定義儲存管理員角色的服務帳戶（ Cloud Volumes ONTAP 9.7 或更高版本所需），或選擇 Google Cloud 帳戶（ Cloud Volumes ONTAP 9.6 所需）。

    請注意以下事項：

    - 控制台在Cloud Volumes ONTAP實例上設定服務帳戶。此服務帳戶提供將資料分層至 Google Cloud Storage 儲存桶的權限。請確保將控制台代理服務帳戶新增為分層服務帳戶的用戶，否則，您無法從控制台中選擇它。
    - 如需新增 Google Cloud 帳戶的協助，請參閱 "使用 9.6 設定和新增 Google Cloud 帳戶以進行資料分層"。

- 您可以在建立或編輯磁碟區時選擇特定的磁碟區分層策略。
- 如果停用資料分層、則可以在後續 Aggregate 上啟用、但您需要關閉系統、並從 Google Cloud Console 新增服務帳戶。

  "了解有關數據分層的更多信息" 。

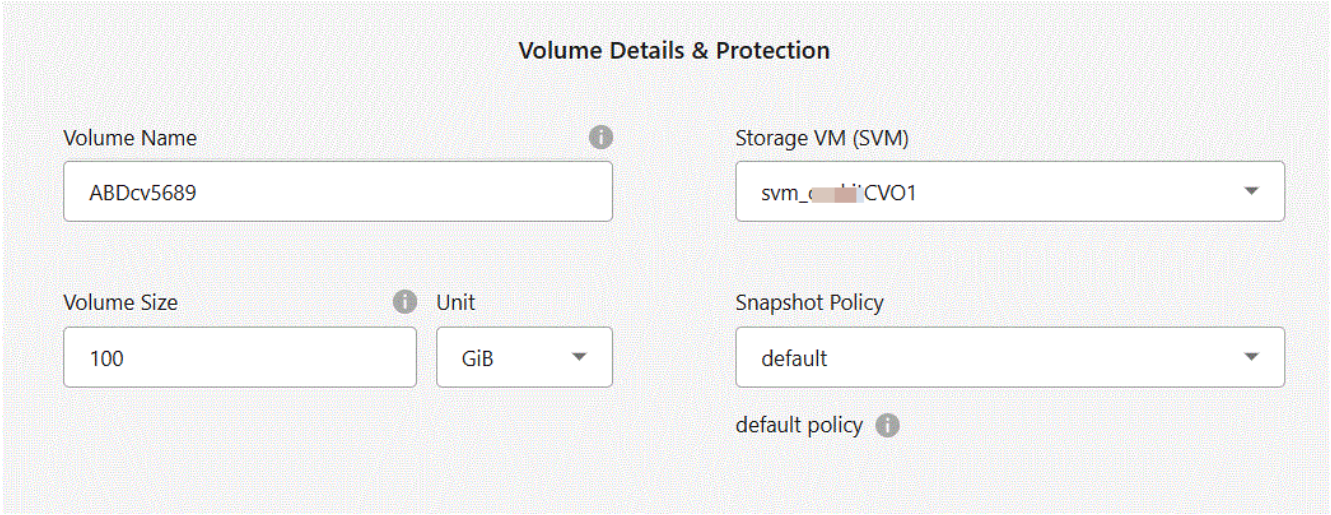
14. 建立磁碟區：輸入新磁碟區的詳細資料或點選*跳過*。

    "了解支援的客戶端協定和版本" 。

    此頁面中的某些欄位是不言自明的。下表描述了您可能需要指導的欄位：

場地	描述
尺寸	您可以輸入的最大大小很大程度上取決於您是否啟用精簡配置，這使您能夠建立比目前可用的實體儲存更大的磁碟區。
存取控制（僅適用於 NFS）	導出策略定義了子網路中可以存取磁碟區的用戶端。預設情況下，控制台輸入一個提供對子網路中所有實例的存取權限的值。
權限和使用者/群組（僅適用於 CIFS）	這些欄位可讓您控制使用者和群組對共用的存取等級（也稱為存取控制清單或 ACL）。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。如果指定網域 Windows 使用者名，則必須使用網域\使用者名稱格式包含使用者的網域。
快照策略	Snapshot 副本策略指定自動建立的NetApp Snapshot 副本的頻率和數量。NetApp Snapshot 副本是時間點檔案系統映像，它不會影響效能並且只需要最少的儲存空間。您可以選擇預設策略或無策略。對於瞬態數據，您可能會選擇無：例如，對於 Microsoft SQL Server，請選擇 tempdb。
進階選項（僅適用於 NFS）	為磁碟區選擇一個 NFS 版本：NFSv3 或 NFSv4。
啟動器群組和 IQN（僅適用於 iSCSI）	iSCSI 儲存目標稱為 LUN（邏輯單元），並以標準區塊裝置呈現給主機。啟動器群組是 iSCSI 主機節點名稱表，用於控制哪些啟動器可以存取哪些 LUN。iSCSI 目標透過標準乙太網路網路適配器 (NIC)、具有軟體啟動器的 TCP 卸載引擎 (TOE) 卡、融合網路適配器 (CNA) 或專用主機匯流排適配器 (HBA) 連接到網絡，並透過 iSCSI 限定名稱 (IQN) 進行識別。當您建立 iSCSI 磁碟區時，控制台會自動為您建立 LUN。我們透過為每個磁碟區建立一個 LUN 來簡化操作，因此無需進行任何管理。建立磁碟區後，"使用 IQN 從主機連線到 LUN" 。

    下圖顯示了磁碟區建立精靈的第一頁：



15. **CIFS** 設定：如果您選擇 CIFS 協議，請設定 CIFS 伺服器。

場地	描述
DNS 主 IP 位址和輔助 IP 位址	為 CIFS 伺服器提供名稱解析的 DNS 伺服器的 IP 位址。所列的 DNS 伺服器必須包含定位 CIFS 伺服器將加入的網域的 Active Directory LDAP 伺服器和網域控制站所需的服務位置記錄 (SRV)。如果您正在設定 Google 管理的 Active Directory，則預設可以使用 169.254.169.254 IP 位址存取 AD。
要加入的 Active Directory 網域	您希望 CIFS 伺服器加入的 Active Directory (AD) 網域的 FQDN。
授權加入網域的憑證	具有足夠權限將電腦新增至 AD 網域內指定組織單位 (OU) 的 Windows 帳戶的名稱和密碼。
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 網域內與 CIFS 伺服器關聯的組織單位。預設值為 CN=Computers。若要將 Google Managed Microsoft AD 設定為Cloud Volumes ONTAP的 AD 伺服器，請在此欄位中輸入 **OU=Computers,OU=Cloud** 。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud 文件：Google Managed Microsoft AD 中的組織單位"^]
DNS 網域	Cloud Volumes ONTAP儲存虛擬機器 (SVM) 的 DNS 網域。大多數情況下，該域與 AD 域相同。
NTP 伺服器	選擇「使用 Active Directory 網域」以使用 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，那麼您應該使用 API。欲了解更多信息，請參閱 "NetApp Console自動化文檔"了解詳情。請注意，只有在建立 CIFS 伺服器時才能設定 NTP 伺服器。建立 CIFS 伺服器後，它不可配置。

16. 使用情況設定檔、磁碟類型和分層策略：選擇是否要啟用儲存效率功能並變更磁碟區分層策略（如果需要）。

    更多信息，請參閱"選擇卷使用情況設定檔"，"資料分層概述" ， 和 "KB：CVO 支援哪些內嵌儲存效率功能？"

17. 審核並批准：審核並確認您的選擇。

a. 查看有關配置的詳細資訊。

b. 點擊*更多資訊*查看有關支援和控制台將購買的 Google Cloud 資源的詳細資訊。

c. 選取*我明白…*複選框。

d. 按一下“開始”。

結果

控制台部署Cloud Volumes ONTAP系統。您可以在*審核*頁面上追蹤進度。

如果您在部署Cloud Volumes ONTAP系統時遇到任何問題，請查看失敗訊息。您也可以選擇系統並點擊*重新建立環境*。

如需更多協助，請訪問 "NetApp Cloud Volumes ONTAP支持"。

完成後

- 如果您配置了 CIFS 共享，請授予使用者或群組對檔案和資料夾的權限，並驗證這些使用者是否可以存取共用並建立檔案。
- 如果要將配額套用於卷，請使用ONTAP系統管理員或ONTAP CLI。

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

部署程序完成後，請勿在 Google Cloud 入口網站中修改系統產生的 Cloud Volumes ONTAP 配置，例如系統標記和 Google Cloud 資源中設定的標籤。對這些配置進行任何更改都可能導致意外行為或資料遺失。

在 **Google Cloud** 中啟動 **HA** 對

在控制台中建立一個系統以在 Google Cloud 中啟動Cloud Volumes ONTAP 。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，按一下*儲存>系統*並按照提示進行操作。
3. 選擇位置：選擇*Google Cloud*和* Cloud Volumes ONTAP HA*。
4. 詳細資料和憑證：選擇一個項目，指定一個群集名稱，可選地選擇一個服務帳戶，可選地新增標籤，然後指定憑證。

   下表描述了您可能需要指導的欄位：

場地	描述
系統名稱	控制台使用系統名稱來命名Cloud Volumes ONTAP系統和 Google Cloud VM 執行個體。如果您選擇該選項，它也會使用該名稱作為預先定義安全性群組的前綴。
服務帳戶名稱	如果您打算使用"NetApp Cloud Tiering"或者 "備份和復原"服務，您需要啟用*服務帳戶*開關，然後選擇具有預先定義儲存管理員角色的服務帳戶。

場地	描述
添加標籤	標籤是您的 Google Cloud 資源的元資料。控制台將標籤新增至Cloud Volumes ONTAP系統以及與該系統關聯的 Google Cloud 資源。建立系統時，您可以從使用者介面新增多達四個標籤，然後可以在建立系統後新增更多標籤。請注意，在建立系統時，API 不會將您限制為四個標籤。有關標籤的信息，請參閱 "Google Cloud 文件：標記資源"。
使用者名稱和密碼	這些是Cloud Volumes ONTAP叢集管理員帳戶的憑證。您可以使用這些憑證透過ONTAP System Manager 或ONTAP CLI 連線到Cloud Volumes ONTAP 。保留預設的_admin_使用者名稱或將其變更為自訂使用者名稱。
編輯項目	選擇您希望 Cloud Volumes ONTAP 所在的專案。 如果下拉清單中沒有顯示其他專案，則表示您尚未將服務帳戶與其他專案建立關聯。請前往 Google Cloud Console，開啟 IAM 服務，然後選擇專案。將服務帳戶與您用於 Console 的角色新增至該專案。您需要為每個專案重複此步驟。 這是您為控制台設定的服務帳戶，"如本頁所述" 。 按一下「新增訂閱」將選定的憑證與訂閱關聯。 若要建立按使用量付費的Cloud Volumes ONTAP系統，您需要從 Google Cloud Marketplace 中選擇與Cloud Volumes ONTAP訂閱相關聯的 Google Cloud 專案。參考 "將市場訂閱與 Google Cloud 憑證關聯"。

5. 服務：選擇您想要在此系統上使用的服務。若要選擇備份和恢復，或使用NetApp Cloud Tiering，您必須在步驟 3 中指定服務帳戶。

   如果您想使用 WORM 和資料分層，則必須停用備份和還原並部署版本 9.8 或更高版本的Cloud Volumes ONTAP系統。

6. **HA** 部署模型：為 HA 配置選擇多個區域（建議）或單一區域。然後選擇區域和分區。

   "了解有關 HA 部署模型的更多信息" 。

7. 連線性：為 HA 設定選擇四個不同的 VPC，每個 VPC 中選擇一個子網，然後選擇一個防火牆策略。

   "了解有關網絡要求的更多信息" 。

   下表描述了您可能需要指導的欄位：

場地	描述
產生的策略	如果您讓控制台為您產生防火牆策略，則需要選擇如何允許流量： • 如果您選擇*僅限選定的 VPC*，則入站流量的來源過濾器是選定 VPC 的子網路範圍和控制台代理程式所在 VPC 的子網路範圍。這是推薦的選項。 • 如果您選擇*所有 VPC*，則入站流量的來源過濾器是 0.0.0.0/0 IP 範圍。

場地	描述
使用現有的	如果您使用現有的防火牆策略，請確保它包含所需的規則。"了解Cloud Volumes ONTAP的防火牆規則" 。

8. 收費方式和 **NSS** 帳戶：指定您想要在此系統中使用的收費選項，然後指定NetApp支援網站帳戶。
   - "了解Cloud Volumes ONTAP的授權選項" 。
   - "了解如何設定許可" 。
9. 預先配置套件：選擇其中一個套件來快速部署Cloud Volumes ONTAP系統，或點擊*建立我自己的設定*。

   如果您選擇其中一個套餐，您只需指定一個卷，然後審核並批准配置。
10. 許可：根據需要變更Cloud Volumes ONTAP版本並選擇機器類型。

    如果所選版本有較新的候選版本、通用版本或修補程式版本，則控制台在建立系統時會將其更新至該版本。例如，如果您選擇Cloud Volumes ONTAP 9.13.1 且 9.13.1 P4 可用，則會發生更新。更新不會從一個版本發生到另一個版本 - 例如，從 9.13 到 9.14。
11. 底層儲存資源：選擇初始聚合的設定：磁碟類型和每個磁碟的大小。

    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聚合中的所有磁碟以及使用簡單配置選項時控制台建立的任何其他聚合。您可以使用進階分配選項建立使用不同磁碟大小的聚合。

    有關選擇磁碟類型和大小的協助，請參閱"在 Google Cloud 中調整系統大小"。
12. 快閃記憶體快取、寫入速度和 **WORM**：
    a. 如有需要，請啟用 **Flash Cache** 或選擇 **Normal** 或 **High** 寫入速度。

       了解更多關於 "快閃記憶體"和"寫入速度"的信息。

       透過 n2-standard-16、n2-standard-32、n2-standard-48 和 n2-standard-64 實例類型的高 寫入速度選項，可以獲得高寫入速度和更高的 8,896 位元組的最大傳輸單元 (MTU)。此外，8,896 的更高 MTU 要求選擇 VPC-1、VPC-2 和 VPC-3 進行部署。高寫入速度和 8,896 的 MTU 取決於功能，無法在配置的實例中單獨停用。有關 VPC-1、VPC-2 和 VPC-3 的更多信息，請參閱 "VPC-1、VPC-2 和 VPC-3 的規則"。

    b. 如果需要，請啟動一次寫入、多次讀取 (WORM) 儲存。

       如果為Cloud Volumes ONTAP 9.7 及更低版本啟用了資料分層，則無法啟用 WORM。啟用 WORM 和分層後，恢復或降級到Cloud Volumes ONTAP 9.8 的操作將被阻止。

    "了解有關 WORM 存儲的更多信息" 。

    a. 如果您啟動 WORM 存儲，請選擇保留期限。
13. **Google Cloud** 中的資料分層：選擇是否在初始聚合上啟用資料分層，為分層資料選擇儲存類，然後選擇具有預先定義儲存管理員角色的服務帳戶。

請注意以下事項：

- 控制台在Cloud Volumes ONTAP實例上設定服務帳戶。此服務帳戶提供將資料分層至 Google Cloud Storage 儲存桶的權限。請確保將控制台代理服務帳戶新增為分層服務帳戶的用戶，否則，您無法從控制台中選擇它。
- 您可以在建立或編輯磁碟區時選擇特定的磁碟區分層策略。
- 如果停用資料分層、則可以在後續 Aggregate 上啟用、但您需要關閉系統、並從 Google Cloud Console 新增服務帳戶。

  "了解有關數據分層的更多信息" 。

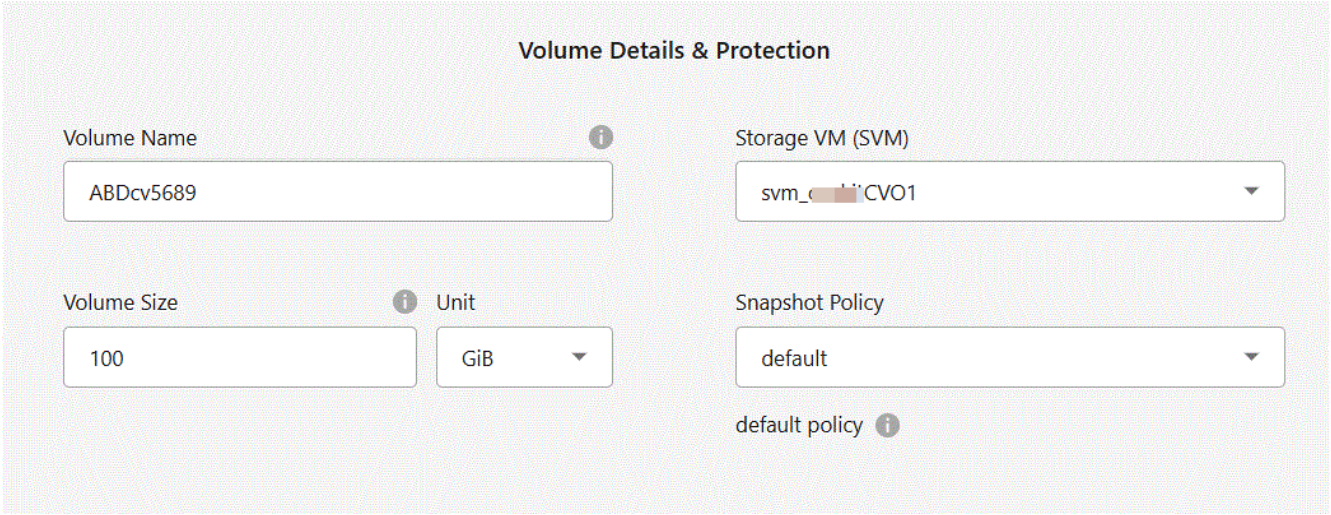
14. 建立磁碟區：輸入新磁碟區的詳細資料或點選*跳過*。

    "了解支援的客戶端協定和版本" 。

    此頁面中的某些欄位是不言自明的。下表描述了您可能需要指導的欄位：

場地	描述
尺寸	您可以輸入的最大大小很大程度上取決於您是否啟用精簡配置，這使您能夠建立比目前可用的實體儲存更大的磁碟區。
存取控制（僅適用於 NFS）	導出策略定義了子網路中可以存取磁碟區的用戶端。預設情況下，控制台輸入一個提供對子網路中所有實例的存取權限的值。
權限和使用者/群組（僅適用於 CIFS）	這些欄位可讓您控制使用者和群組對共用的存取等級（也稱為存取控制清單或 ACL）。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。如果指定網域 Windows 使用者名，則必須使用網域\使用者名稱格式包含使用者的網域。
快照策略	Snapshot 副本策略指定自動建立的NetApp Snapshot 副本的頻率和數量。NetApp Snapshot 副本是時間點檔案系統映像，它不會影響效能並且只需要最少的儲存空間。您可以選擇預設策略或無策略。對於瞬態數據，您可能會選擇無：例如，對於 Microsoft SQL Server，請選擇 tempdb。
進階選項（僅適用於 NFS）	為磁碟區選擇一個 NFS 版本：NFSv3 或 NFSv4。
啟動器群組和 IQN（僅適用於 iSCSI）	iSCSI 儲存目標稱為 LUN（邏輯單元），並以標準區塊裝置呈現給主機。啟動器群組是 iSCSI 主機節點名稱表，用於控制哪些啟動器可以存取哪些 LUN。iSCSI 目標透過標準乙太網路網路適配器 (NIC)、具有軟體啟動器的 TCP 卸載引擎 (TOE) 卡、融合網路適配器 (CNA) 或專用主機匯流排適配器 (HBA) 連接到網絡，並透過 iSCSI 限定名稱 (IQN) 進行識別。當您建立 iSCSI 磁碟區時，控制台會自動為您建立 LUN。我們透過為每個磁碟區建立一個 LUN 來簡化操作，因此無需進行任何管理。建立磁碟區後，"使用 IQN 從主機連線到 LUN" 。

    下圖顯示了磁碟區建立精靈的第一頁：



15. **CIFS** 設定：如果您選擇 CIFS 協議，請設定 CIFS 伺服器。

場地	描述
DNS 主 IP 位址和輔助 IP 位址	為 CIFS 伺服器提供名稱解析的 DNS 伺服器的 IP 位址。所列的 DNS 伺服器必須包含定位 CIFS 伺服器將加入的網域的 Active Directory LDAP 伺服器和網域控制站所需的服務位置記錄 (SRV)。如果您正在設定 Google 管理的 Active Directory，則預設可以使用 169.254.169.254 IP 位址存取 AD。
要加入的 Active Directory 網域	您希望 CIFS 伺服器加入的 Active Directory (AD) 網域的 FQDN。
授權加入網域的憑證	具有足夠權限將電腦新增至 AD 網域內指定組織單位 (OU) 的 Windows 帳戶的名稱和密碼。
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 網域內與 CIFS 伺服器關聯的組織單位。預設值為 CN=Computers。若要將 Google Managed Microsoft AD 設定為Cloud Volumes ONTAP的 AD 伺服器，請在此欄位中輸入 **OU=Computers,OU=Cloud** 。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud 文件：Google Managed Microsoft AD 中的組織單位"^]
DNS 網域	Cloud Volumes ONTAP儲存虛擬機器 (SVM) 的 DNS 網域。大多數情況下，該域與 AD 域相同。
NTP 伺服器	選擇「使用 Active Directory 網域」以使用 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，那麼您應該使用 API。請參閱 "NetApp Console自動化文檔"了解詳情。請注意，只有在建立 CIFS 伺服器時才能設定 NTP 伺服器。建立 CIFS 伺服器後，它不可配置。

16. 使用情況設定檔、磁碟類型和分層策略：選擇是否要啟用儲存效率功能並變更磁碟區分層策略（如果需要）。

    更多信息，請參閱"選擇卷使用情況設定檔"，"資料分層概述" ， 和 "KB：CVO 支援哪些內嵌儲存效率功能？"

17. 審核並批准：審核並確認您的選擇。

a. 查看有關配置的詳細資訊。

b. 點擊*更多資訊*查看有關支援和控制台將購買的 Google Cloud 資源的詳細資訊。

c. 選取*我明白…*複選框。

d. 按一下“開始”。

結果

控制台部署Cloud Volumes ONTAP系統。您可以在*審核*頁面上追蹤進度。

如果您在部署Cloud Volumes ONTAP系統時遇到任何問題，請查看失敗訊息。您也可以選擇系統並點擊*重新建立環境*。

如需更多協助，請訪問 "NetApp Cloud Volumes ONTAP支持"。

完成後

- 如果您配置了 CIFS 共享，請授予使用者或群組對檔案和資料夾的權限，並驗證這些使用者是否可以存取共用並建立檔案。
- 如果要將配額套用於卷，請使用ONTAP系統管理員或ONTAP CLI。

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

部署程序完成後，請勿在 Google Cloud 入口網站中修改系統產生的 Cloud Volumes ONTAP 配置，例如系統標記和 Google Cloud 資源中設定的標籤。對這些配置進行任何更改都可能導致意外行為或資料遺失。

相關連結

- "在 Google Cloud 規劃Cloud Volumes ONTAP配置"

Google Cloud Platform 圖像驗證

了解如何在Cloud Volumes ONTAP中驗證 Google Cloud 映像

Google Cloud 映像驗證符合增強的NetApp安全要求。已經對生成圖像的腳本進行了更改，以便使用專門為此任務生成的私鑰對圖像進行簽署。您可以使用 Google Cloud 的簽章摘要和公用憑證來驗證 Google Cloud 映像的完整性，該憑證可透過以下方式下載 "國家安全局"針對特定版本。

Cloud Volumes ONTAP軟體版本 9.13.0 或更高版本支援 Google Cloud 映像驗證。

將 Google Cloud 映像轉換為Cloud Volumes ONTAP 的原始格式

用於部署新實例、升級或在現有映像中使用的映像將透過以下方式與客戶端共用 "NetApp 支援站點 (NSS)"。已簽署的摘要和憑證可透過 NSS 入口網站下載。確保您下載的摘要和憑證與NetApp支援共享的影像對應的正確版本。例如，9.13.0 影像將具有 9.13.0 簽名摘要和 NSS 上可用的憑證。

為什麼需要這一步？

無法直接下載 Google Cloud 的圖片。為了根據簽署的摘要和證書驗證圖像，您需要有一個機制來比較兩個檔案並下載圖像。為此，您必須將圖像匯出/轉換為 disk.raw 格式，並將結果保存在 Google Cloud 的儲存桶中。在此過程中，disk.raw 檔案被壓縮並壓縮。

使用者/服務帳戶需要權限才能執行以下操作：

- 存取 Google 儲存桶
- 寫入 Google 儲存桶
- 建立雲端建置作業（在匯出過程中使用）
- 存取所需圖像
- 建立匯出影像任務

若要驗證映像，必須將其轉換為 disk.raw 格式，然後下載。

使用 **Google Cloud** 命令列匯出 **Google Cloud** 鏡像

將影像匯出到雲端儲存的首選方法是使用 "gcloud compute images export 指令"。此命令獲取提供的圖像並將其轉換為 disk.raw 文件，該文件會被 tarred 和 gzip 壓縮。產生的檔案保存在目標URL，然後可以下載進行驗證。

使用者/帳戶必須具有存取和寫入所需儲存桶、匯出映像和雲端建置（Google 用於匯出映像）的權限才能執行此操作。

使用 **gcloud** 匯出 **Google Cloud** 鏡像

點擊顯示

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

解壓縮壓縮檔

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

有關如何透過 Google Cloud 匯出圖像的更多信息，請參閱 "Google Cloud 文件：匯出影像"。

影像簽名驗證

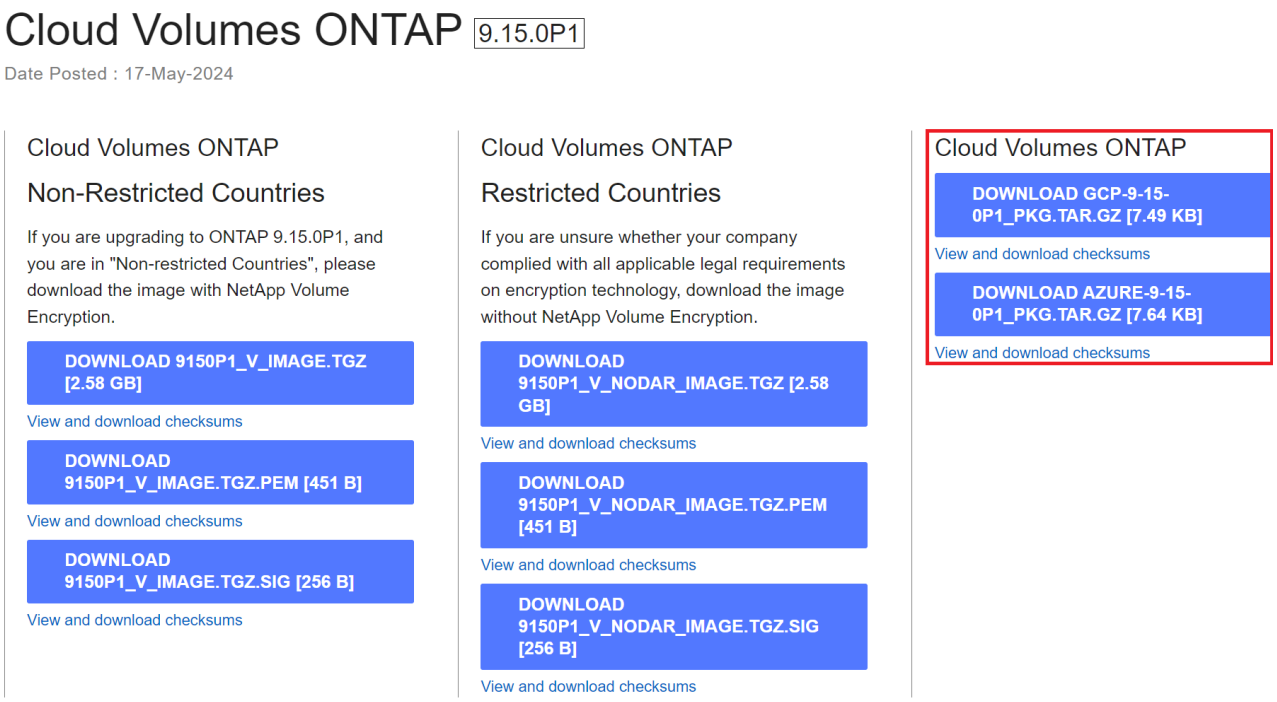
Cloud Volumes ONTAP的 Google Cloud 映像簽章驗證

若要驗證匯出的 Google Cloud 簽章映像，您必須從 NSS 下載映像摘要檔案以驗證 disk.raw 檔案和摘要檔案內容。

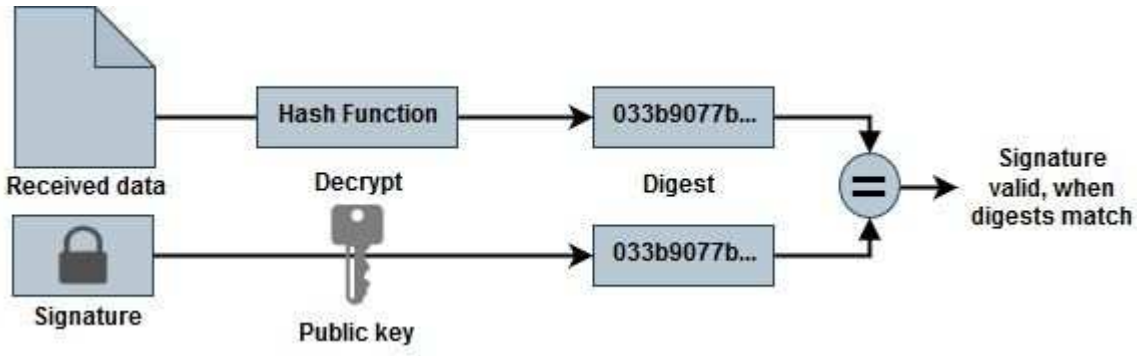
簽名影像驗證工作流程摘要

以下是 Google Cloud 簽名影像驗證工作流程的概述。

- 從 "國家安全局"，下載包含以下文件的 Google Cloud 檔案：
  - 簽名摘要（.sig）
  - 包含公鑰的憑證（.pem）
  - 憑證鏈（.pem）



- 下載轉換後的 disk.raw 文件
- 使用證書鏈驗證證書
- 使用包含公鑰的憑證驗證簽署的摘要
  - 使用公鑰解密簽署的摘要，以提取映像檔的摘要
  - 建立下載的 disk.raw 檔案的摘要
  - 比較兩個摘要文件進行驗證



使用 **OpenSSL** 驗證**Cloud Volumes ONTAP**的 **Google Cloud** 映像 **disk.raw** 文件

您可以透過以下方式驗證 Google Cloud 下載的 disk.raw 檔案與摘要檔案內容 "國家安全局"使用 OpenSSL。

用於驗證映像的 OpenSSL 命令與 Linux、macOS 和 Windows 機器相容。

步驟

1. 使用 OpenSSL 驗證憑證。

點擊顯示

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
          e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
          22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
          38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
          fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
          bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. 將下載的 disk.raw 檔案、簽名和憑證放在一個目錄中。
3. 使用 OpenSSL 從憑證中提取公鑰。
4. 使用提取的公鑰解密簽名並驗證下載的 disk.raw 檔案的內容。

點擊顯示

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```

使用Cloud Volumes ONTAP

許可證管理

管理Cloud Volumes ONTAP基於容量的許可

從NetApp Console管理基於容量的許可證，以確保您的NetApp帳戶具有足夠的容量用於您的Cloud Volumes ONTAP系統。

_基於容量的許可證_使您能夠按 TiB 容量支付Cloud Volumes ONTAP 的費用。

您可以從NetApp Console管理基於容量的Cloud Volumes ONTAP許可證。

> 雖然控制台中管理的產品和服務的實際使用情況和計量始終以 GiB 和 TiB 計算，但 GB/GiB 和 TB/TiB 這兩個術語可互換使用。這反映在雲端市場清單、報價、清單描述和其他支援文件中

"了解有關Cloud Volumes ONTAP許可證的更多信息" 。

如何將許可證新增至NetApp Console

從NetApp銷售代表處購買許可證後， NetApp將向您發送一封電子郵件，其中包含序號和其他許可詳細資訊。

同時，控制台會自動查詢 NetApp 的授權服務，以取得與您的NetApp支援網站帳戶相關的授權的詳細資訊。如果沒有錯誤，它會添加許可證。

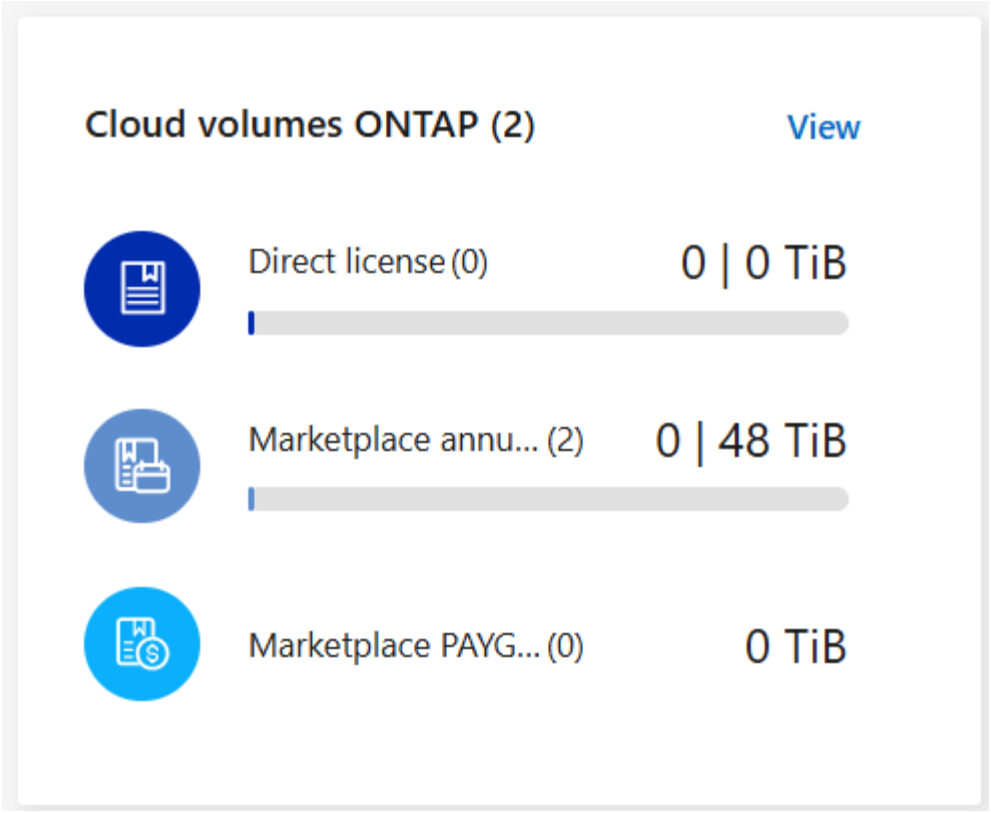
如果控制台無法新增許可證，則需要手動新增它們。例如，如果控制台代理安裝在沒有網路存取的位置，則您需要自行新增許可證。 "了解如何將購買的許可證新增至您的帳戶" 。

查看您帳戶中已消耗的容量

控制台顯示您帳戶中消耗的總容量以及按許可包消耗的容量。這可以幫助您了解收費方式以及是否需要購買額外的容量。

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」 。
2. 在「概覽」標籤上， Cloud Volumes ONTAP圖塊顯示為您的帳戶配置的目前容量。



- _直接許可證_是您的NetApp帳戶中所有Cloud Volumes ONTAP系統的總配置容量。收費基於每個磁碟區的配置大小，而不考慮磁碟區內的本機、已使用、儲存或有效空間。
- _年度合約_是您從NetApp購買的總授權容量（自帶授權 (BYOL) 或市場合約）。
- *PAYGO* 是使用雲端市場訂閱的總配置容量。只有當消耗的容量高於授權容量或控制台中沒有可用的 BYOL 授權時，才使用 PAYGO 收費。

3. 選擇「檢視」以查看每個許可證包所消耗的容量。
4. 選擇「許可證」標籤查看您購買的每個包許可證的詳細資訊。

   為了更了解 Essentials 套件所顯示的容量，您應該熟悉充電的工作原理。 "了解 Essentials 套餐的收費" 。

5. 選擇「訂閱」標籤來查看按許可證消費模式消耗的容量。此選項卡包括 PAYGO 和年度合約許可證。

   您只會看到與您目前正在查看的組織相關的訂閱。

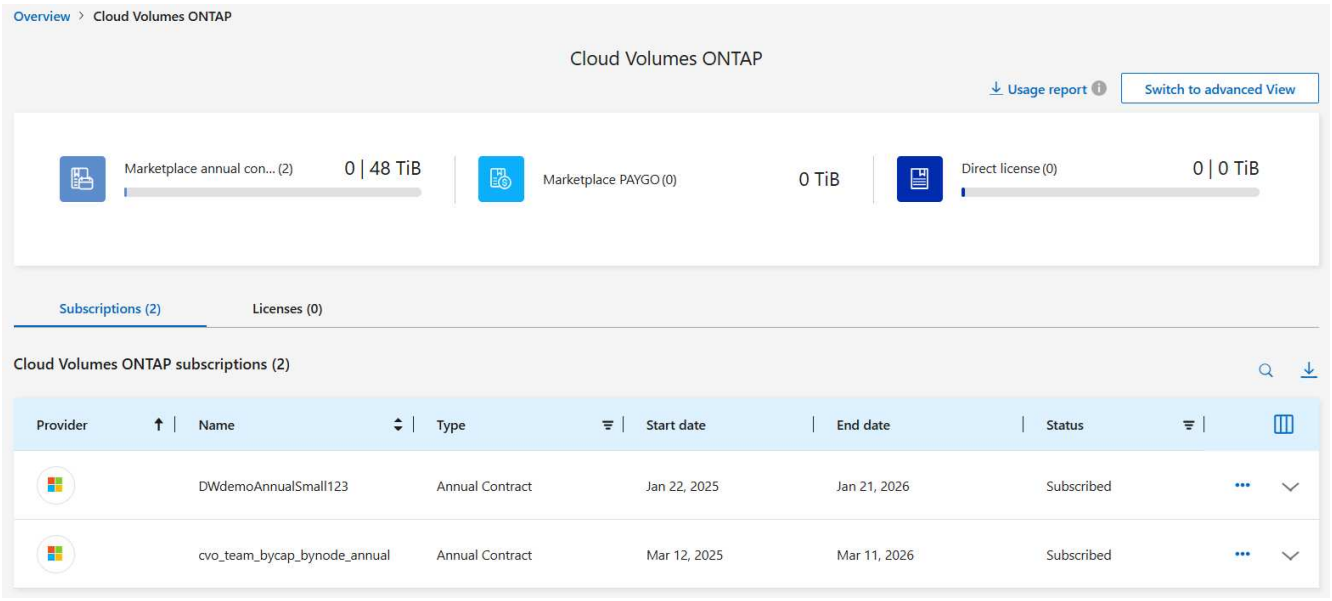
6. 當您查看有關訂閱的資訊時，您可以與表中的詳細資訊進行互動。展開一行可以查看更多詳細資訊。
   - 選擇 選擇表中顯示的列。請注意，「期限」和「自動續訂」欄預設不會出現。自動續約列僅顯示 Azure 合約的續約資訊。

查看包裹詳情

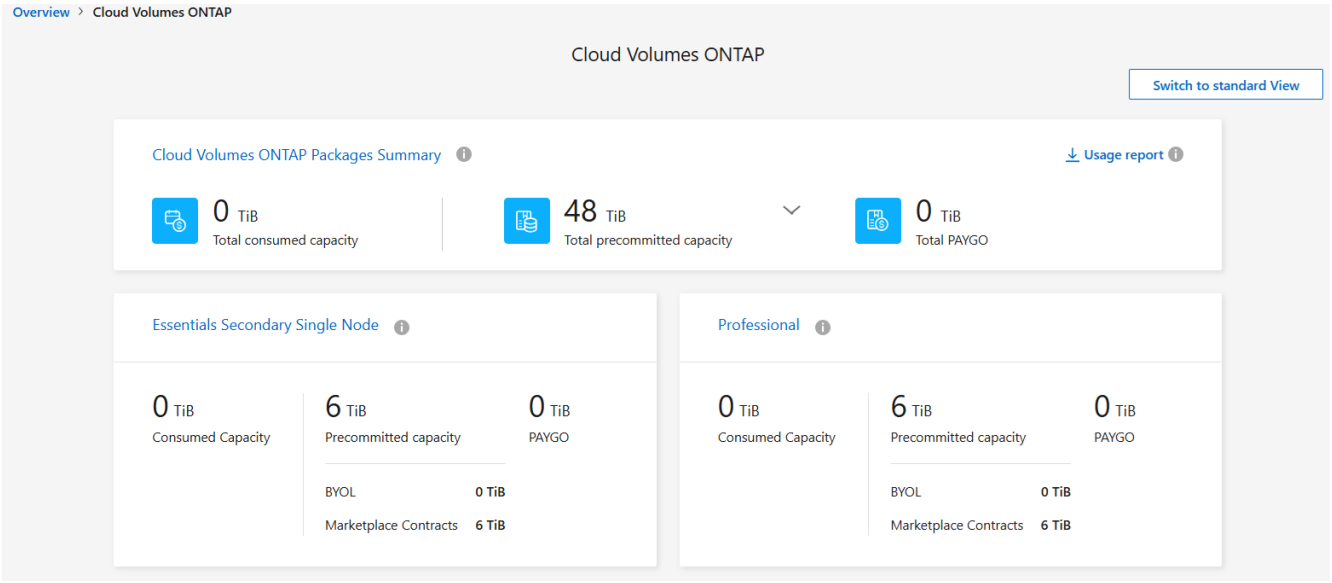
您可以透過在Cloud Volumes ONTAP頁面上切換到傳統模式來查看每個套件使用的容量的詳細資訊。

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」 。
2. 在「概覽」標籤上， Cloud Volumes ONTAP圖塊顯示為您的帳戶配置的目前容量。
3. 選擇「檢視」以查看每個授權包的配置容量。

4. 選擇*切換到進階視圖*。



5. 查看您想要查看的包裹的詳細資訊。



改變充電方式

基於容量的許可以_包_的形式提供。建立Cloud Volumes ONTAP系統時，您可以根據業務需求從多個授權包中進行選擇。如果您在建立系統後需求發生變化，您可以隨時更改套餐。例如，您可以從 Essentials 套件變更為 Professional 套件。

"了解有關基於容量的許可包的更多信息" 。

關於此任務

- 更改收費方式不會影響您是透過從NetApp (BYOL) 購買的授權或透過雲端提供者的市場即用即付 (PAYGO) 訂閱進行收費。

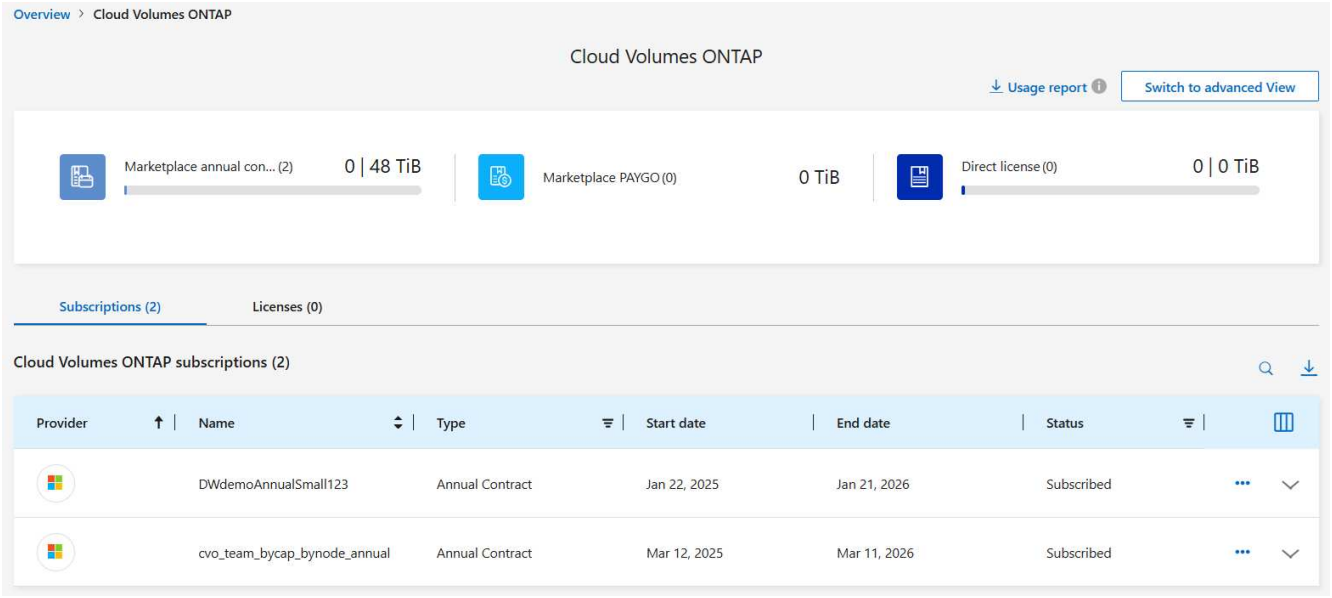
  控制台總是會先嘗試根據許可證收費。如果沒有許可證，則會根據市場訂閱收費。您不必將 BYOL 訂閱轉換

為市場訂閱，反之亦然。

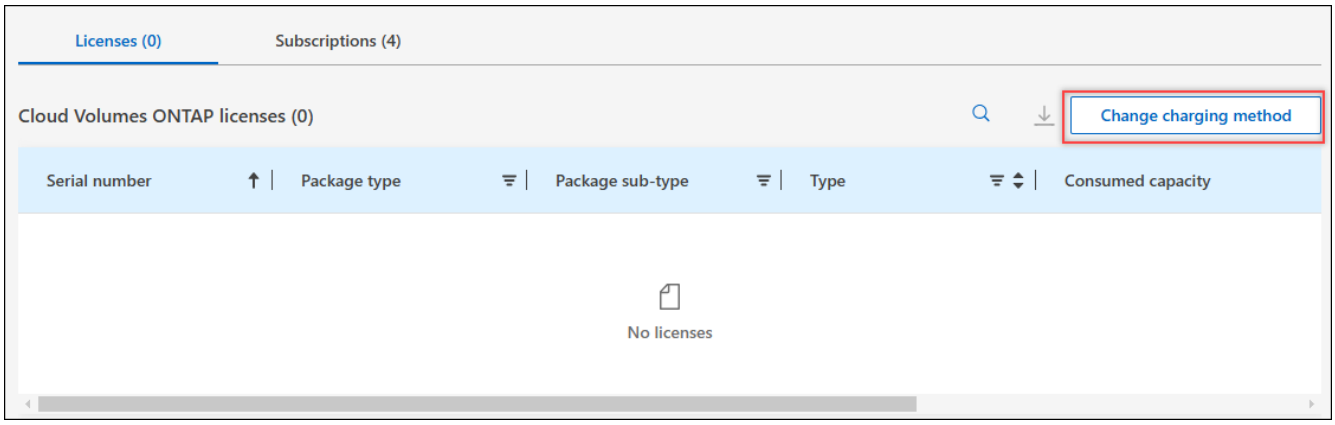
- 如果您擁有來自雲端提供者市場的私人優惠或合同，則更改為合同中未包含的收費方式將導致對 BYOL（如果您從NetApp購買了許可證）或 PAYGO 收費。

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」 。
2. 選擇“概覽”標籤。
3. 在Cloud Volumes ONTAP圖塊上，選擇 檢視。
4. 選擇*切換到進階視圖*。



5. 向下捲動到*基於容量的許可證*表並選擇*更改收費方式*。



6. 在*變更收費方式*彈出視窗中，選擇Cloud Volumes ONTAP系統，選擇新的收費方式，然後確認您了解變更套餐類型將影響服務費用。
7. 選擇*更改充電方式*。

下載使用情況報告

您可以從控制台下載四份使用量報告。這些使用情況報告提供您的訂閱的容量詳細信息，並告訴您如何為Cloud Volumes ONTAP訂閱中的資源付費。可下載的報告會擷取某個時間點的數據，並且可以輕鬆地與他人分享。

以下報告可供下載。顯示的容量值以 TiB 為單位。

- 進階用法：此報告包含以下資訊：
  - 總消耗容量
  - 預先承諾的總容量
  - 總 BYOL 容量
  - 市場合約總容量
  - PAYGO 總容量
- * Cloud Volumes ONTAP軟體包使用情況*：此報告包含每個軟體包的以下資訊：
  - 總消耗容量
  - 預先承諾的總容量
  - 總 BYOL 容量
  - 市場合約總容量
  - PAYGO 總容量
- 儲存虛擬機器使用情況：此報告顯示收費容量在Cloud Volumes ONTAP系統和儲存虛擬機器 (SVM) 之間的分配。此資訊僅在報告中提供。它包含以下資訊：
  - 系統 ID 和名稱（顯示為 UUID）
  - 雲端
  - NetApp帳號 ID
  - 系統配置
  - SVM 名稱
  - 預配置容量
  - 充電容量匯總
  - 市集計費條款
  - Cloud Volumes ONTAP軟體套件或功能
  - 收費 SaaS 市集訂閱名稱
  - 收費 SaaS 市集訂閱 ID

- 工作負載類型

- 磁碟區使用情況：此報表顯示Cloud Volumes ONTAP系統中如何依磁碟區細分收費容量。控制台中的任何螢幕上均不顯示此資訊。它包括以下資訊：
  - 系統 ID 和名稱（顯示為 UUID）
  - SVN 名稱
  - 卷 ID
  - 卷類型
  - 卷配置容量

    FlexClone磁碟區不包含在此報表中，因為這些類型的磁碟區不會產生費用。

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」。
2. 在*概覽*標籤上，從Cloud Volumes ONTAP圖塊中選擇*檢視*。
3. 選擇*使用情況報告*。

   使用情況報告下載。

4. 開啟下載的檔案以存取報告。

透過NetApp Console管理Cloud Volumes ONTAP 的Keystone訂閱

透過啟用與Cloud Volumes ONTAP一起使用的訂閱並要求變更訂閱服務等級的承諾容量，在NetApp Console中管理您的Keystone訂閱。請求服務等級的額外容量可為Cloud Volumes ONTAP系統提供更多儲存空間。

NetApp Keystone是一種靈活的隨選付費訂閱服務，可為喜歡 OpEx 而非 CapEx 或租賃的客戶提供混合雲體驗。

"了解有關Keystone的更多信息"

授權您的帳戶

您需要先聯絡NetApp授權您的控制台帳號使用Keystone訂閱，然後才能在控制台中使用和管理Keystone訂閱。

步驟

1. 從NetApp Console選單中，選擇「管理 >Licenses and subscriptions」。
2. 選擇* Keystone訂閱*。
3. 如果您看到「歡迎使用NetApp Keystone」頁面，請向頁面上列出的地址發送電子郵件。

   NetApp代表將透過授權您的帳戶存取訂閱來處理您的要求。

4. 返回“Keystone訂閱”選項卡查看您的訂閱。

連結訂閱

在NetApp授權您的帳戶後，您可以連結Keystone訂閱以用於Cloud Volumes ONTAP。此操作使用戶能夠選擇訂閱作為新Cloud Volumes ONTAP系統的收費方式。

步驟

1. 從NetApp Console選單中，選擇「管理 >Licenses and subscriptions」。
2. 選擇* Keystone訂閱*。
3. 對於您想要連結的訂閱，請點擊 ••• 並選擇*連結*。

結果

訂閱現已連結至您的控制台組織或帳戶，並可在建立Cloud Volumes ONTAP工作環境時進行選擇。

請求更多或更少的承諾容量

如果您想要變更訂閱服務等級的承諾容量，您可以直接從控制台向NetApp傳送請求。請求服務等級的額外容量可為Cloud Volumes ONTAP系統提供更多儲存空間。

步驟

1. 從NetApp Console選單中，選擇「管理 >Licenses and subscriptions」。
2. 選擇* Keystone訂閱*。
3. 對於要調整容量的訂閱，請按一下 ••• 並選擇*查看詳細資訊和編輯*。
4. 輸入一個或多個訂閱所請求的承諾容量。
5. 向下滾動，輸入請求的任何其他詳細信息，然後點擊“提交”。

結果

您的請求將在 NetApp 系統中建立一張票以供處理。

監控使用情況

Digital Advisor儀表板可讓您監控Keystone訂閱使用情況並產生報告。

"了解有關監控訂閱使用情況的更多信息"

取消訂閱鏈接

如果您不再想將Keystone訂閱與控制台一起使用，您可以取消訂閱連結。請注意，您只能取消連結未附加至現有Cloud Volumes ONTAP訂閱的訂閱。

步驟

1. 從NetApp Console選單中，選擇「管理 >Licenses and subscriptions」。
2. 選擇* Keystone*。
3. 對於要取消連結的訂閱，點擊 ••• 並選擇*取消連結*。

結果

該訂閱已與您的控制台組織或帳戶取消鏈接，並且在創建Cloud Volumes ONTAP工作環境時不再可供選擇。

管理Cloud Volumes ONTAP 的基於節點的許可

在NetApp Console中管理基於節點的許可證，以確保每個Cloud Volumes ONTAP系統都具有所需容量的有效許可證。

_基於節點的許可證_是上一代許可證模型（不適用於新客戶）：

- 從NetApp購買自帶授權 (BYOL)
- 從雲端供應商的市場購買按小時付費 (PAYGO) 訂閱

您可以從NetApp Console管理基於節點的Cloud Volumes ONTAP許可證。

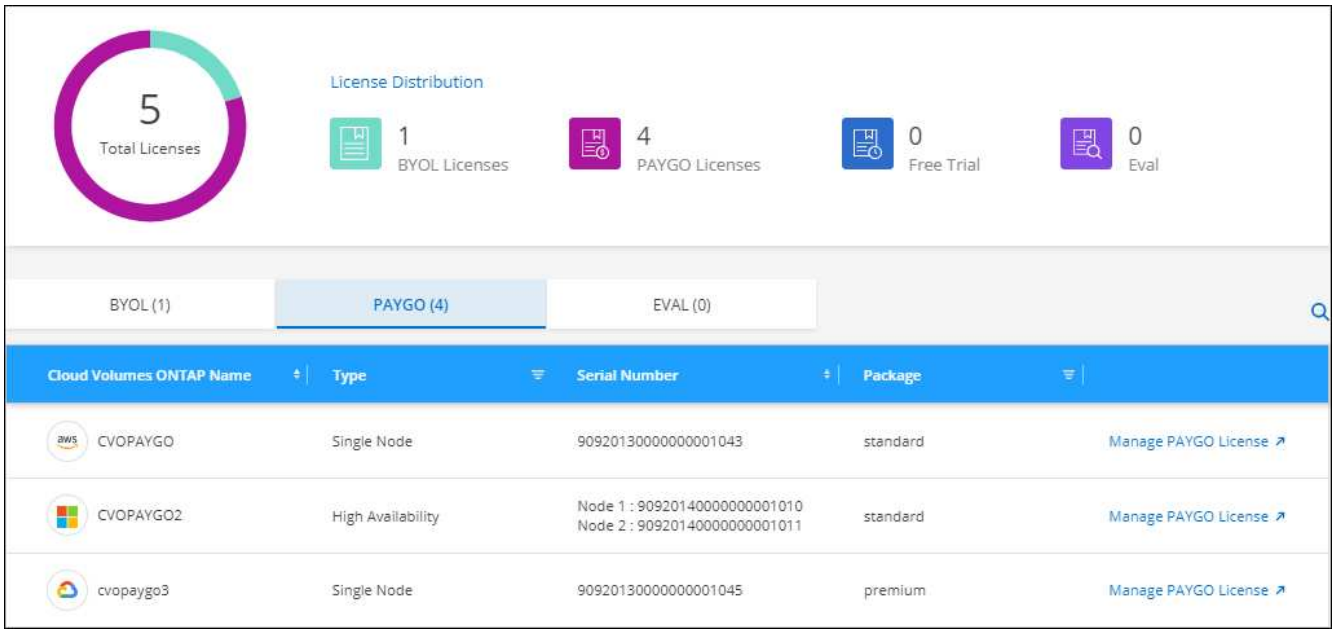
"了解有關Cloud Volumes ONTAP許可證的更多信息" 。

管理 PAYGO 許可證

Licenses and subscriptions選單，您可以查看有關每個 PAYGO Cloud Volumes ONTAP系統的詳細信息，包括序號和 PAYGO 許可證類型。

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」 。
2. 選擇“概覽”標籤。
3. 在Cloud Volumes ONTAP圖塊上，選擇 檢視。
4. 從下拉式選單中選擇*基於節點的授權*。
5. 點擊*PAYGO*。
6. 在表格中查看有關每個 PAYGO 許可證的詳細資訊。



7. 如果需要，請按一下*管理 PAYGO 授權*來變更 PAYGO 授權或變更執行個體類型。

管理 BYOL 許可證

透過新增和刪除系統許可證和額外容量許可證來管理您直接從NetApp購買的許可證。

已限制 BYOL 授權的購買、延期和續約。有關更多信息，請參閱 "Cloud Volumes ONTAP的 BYOL 授權可用性受限" 。

新增未分配的許可證

將基於節點的許可證新增至控制台，以便您在建立新的Cloud Volumes ONTAP系統時可以選擇該許可證。控制台將這些許可證標識為_未分配_。

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」 。
2. 選擇“概覽”標籤。
3. 在Cloud Volumes ONTAP圖塊上，選擇 檢視。
4. 從下拉式選單中選擇*基於節點的授權*。
5. 按一下“未分配”。
6. 按一下「新增未指派的許可證」 。
7. 輸入許可證的序號或上傳許可證文件。

   如果您還沒有許可證文件，請參閱下面的部分。

8. 按一下「新增許可證」 。

結果

控制台新增許可證。在您將許可證與新的Cloud Volumes ONTAP系統關聯之前，該許可證將被標識為未指派。此後，許可證將移至「Licenses and subscriptions」中的「BYOL」標籤。

交換未分配的基於節點的許可證

如果您有未指派的基於節點的Cloud Volumes ONTAP許可證且尚未使用，則可以將其轉換為NetApp Backup and Recovery許可證、 NetApp Data Classification許可證或NetApp Cloud Tiering許可證來交換該許可證。

交換許可證將撤銷Cloud Volumes ONTAP許可證並為該服務建立等值美元的許可證：

- Cloud Volumes ONTAP HA 對的授權轉換為 51 TiB 直接許可證
- Cloud Volumes ONTAP單節點授權轉換為 32 TiB 直接許可證

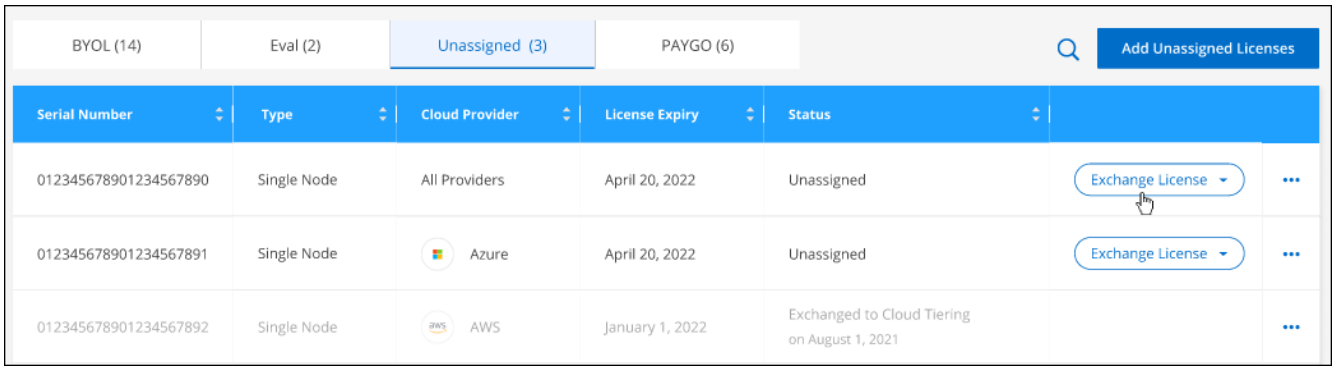
轉換後的許可證的到期日與Cloud Volumes ONTAP許可證相同。

"查看如何交換基於節點的許可證的演練。"

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」 。
2. 選擇“概覽”標籤。

3. 在Cloud Volumes ONTAP圖塊上，選擇 檢視。
4. 從下拉式選單中選擇*基於節點的授權*。
5. 按一下“未分配”。
6. 按一下「交換許可證」。



7. 選擇您想要交換許可證的服務。
8. 如果出現提示，請為 HA 對選擇一個額外的許可證。
9. 閱讀法律同意並點擊*同意*。

結果

控制台將未指派的許可證轉換為您選擇的服務。您可以在「資料服務許可證」標籤中查看新的許可證。

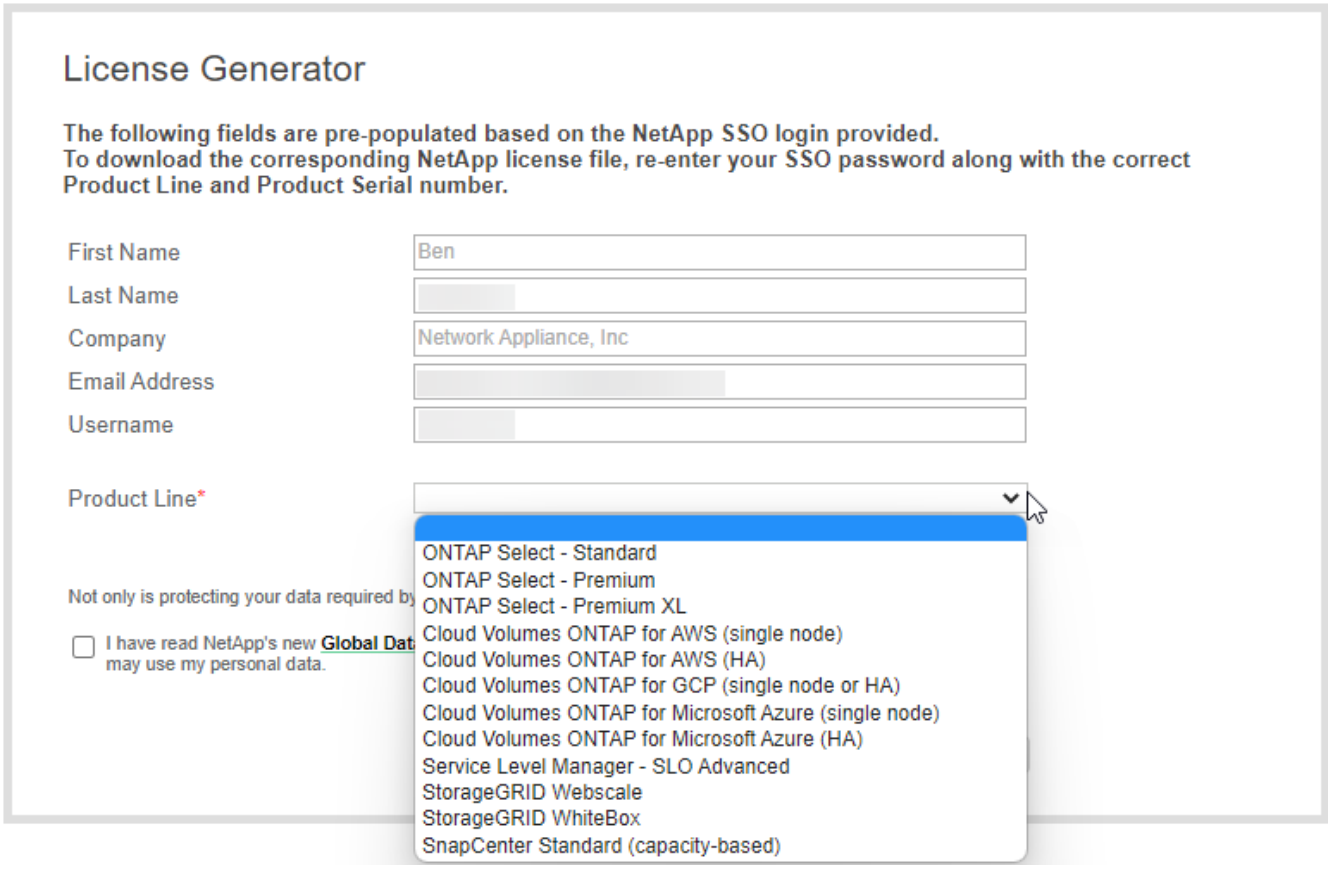
取得系統許可證文件

在大多數情況下，控制台可以使用您的NetApp支援網站帳戶自動取得您的授權文件。但如果不能，那麼您將需要手動上傳許可證文件。如果您沒有許可證文件，您可以從 netapp.com 取得。

步驟

1. 前往 "NetApp許可證文件產生器"並使用您的NetApp支援網站憑證登入。
2. 輸入您的密碼，選擇您的產品，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*。

   例子



3. 選擇您是否希望透過電子郵件或直接下載接收 serialnumber.NLF JSON 檔案。

更新系統許可證

當您透過聯絡NetApp代表續訂 BYOL 訂閱時，控制台會自動從NetApp取得新授權並將其安裝在Cloud Volumes ONTAP系統上。如果控制台無法透過安全的網路連線存取許可證文件，您可以自行取得該文件，然後手動上傳該文件。

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」。
2. 選擇“概覽”標籤。
3. 在Cloud Volumes ONTAP圖塊上，選擇 檢視。
4. 從下拉式選單中選擇*基於節點的授權*。
5. 在 **BYOL** 標籤中，展開Cloud Volumes ONTAP系統的詳細資訊。
6. 點擊系統許可證旁邊的操作選單，然後選擇*更新許可證*。
7. 上傳許可證文件（如果您有 HA 對，則上傳多個文件）。
8. 按一下「更新許可證」。

結果

控制台更新Cloud Volumes ONTAP系統上的許可證。

您可以為Cloud Volumes ONTAP BYOL 系統購買額外的容量許可證，以分配超過 BYOL 系統許可證提供的 368 TiB 的容量。例如，您可以購買一個額外的許可證容量，為Cloud Volumes ONTAP分配最多 736 TiB 的容量。或者您可以購買三個額外的容量許可證以獲得高達 1.4 PiB。

您可以為單節點系統或 HA 配對購買的授權數量沒有限制。

新增容量許可證

透過控制台右下角的聊天圖示聯絡我們，購買額外容量許可證。購買許可證後，您可以將其套用至Cloud Volumes ONTAP系統。

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」。
2. 選擇“概覽”標籤。
3. 在Cloud Volumes ONTAP圖塊上，選擇 檢視。
4. 從下拉式選單中選擇*基於節點的授權*。
5. 在 **BYOL** 標籤中，展開Cloud Volumes ONTAP系統的詳細資訊。
6. 按一下「新增容量許可證」。
7. 輸入序號或上傳許可證文件（如果您有 HA 對，則上傳文件）。
8. 按一下「新增容量許可證」。

更新容量許可證

如果您延長了額外容量許可證的期限，則需要在控制台中更新許可證。

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」。
2. 選擇“概覽”標籤。
3. 在Cloud Volumes ONTAP圖塊上，選擇 檢視。
4. 從下拉式選單中選擇*基於節點的授權*。
5. 在 **BYOL** 標籤中，展開Cloud Volumes ONTAP系統的詳細資訊。
6. 按一下容量許可證旁的操作選單，然後選擇*更新許可證*。
7. 上傳許可證文件（如果您有 HA 對，則上傳多個文件）。
8. 按一下「更新許可證」。

刪除容量許可證

如果額外容量許可證已過期且不再使用，那麼您可以隨時將其刪除。

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」。

2. 選擇“概覽”標籤。
3. 在Cloud Volumes ONTAP圖塊上，選擇 檢視。
4. 從下拉式選單中選擇*基於節點的授權*。
5. 在 **BYOL** 標籤中，展開Cloud Volumes ONTAP系統的詳細資訊。
6. 點擊容量許可證旁邊的操作選單，然後選擇*刪除許可證*。
7. 按一下“刪除”。

PAYGO 與 **BYOL** 之間的變化

不支援將系統從 PAYGO 按節點授權轉換為 BYOL 按節點授權（反之亦然）。如果您想在按使用量付費訂閱和 BYOL 訂閱之間切換，那麼您需要部署一個新系統並將資料從現有系統複製到新系統。

步驟

1. 建立一個新的Cloud Volumes ONTAP系統。
2. 對於需要複製的每個卷，在系統之間設定一次性資料複製。

   "了解如何在系統之間複製數據"

3. 透過刪除原始系統來終止不再需要的Cloud Volumes ONTAP系統。

   "了解如何刪除Cloud Volumes ONTAP系統" 。

相關連結

關聯："基於節點的許可證的可用性終止" "將基於節點的許可證轉換為基於容量的許可證"

捲和 LUN 管理

在Cloud Volumes ONTAP系統上建立FlexVol volume

如果在啟動初始Cloud Volumes ONTAP系統後需要更多存儲，您可以從NetApp Console為 NFS、CIFS 或 iSCSI 建立新的FlexVol磁碟區。

您可以透過多種方式建立新磁碟區：

- 指定新磁碟區的詳細信息，並讓控制台為您處理底層資料聚合。了解更多
- 在您選擇的資料聚合上建立磁碟區。了解更多
- 在 HA 配置中的第二個節點上建立磁碟區。了解更多

開始之前

關於卷配置的一些注意事項：

- 當您建立 iSCSI 磁碟區時，控制台會自動為您建立 LUN。我們透過為每個磁碟區建立一個 LUN 來簡化操作，因此無需進行任何管理。建立磁碟區後，"使用 IQN 從主機連線到 LUN" 。
- 您可以從ONTAP系統管理員或ONTAP CLI 建立其他 LUN。

- 如果您想在 AWS 中使用 CIFS，則必須設定 DNS 和 Active Directory。有關詳細信息，請參閱"Cloud Volumes ONTAP for AWS 的網路需求"。
- 如果您的Cloud Volumes ONTAP配置支援 Amazon EBS 彈性磁碟區功能，您可能需要"詳細了解建立磁碟區時發生的情況"。

創建卷

建立磁碟區最常見的方法是指定所需的磁碟區類型，然後讓控制台為您處理磁碟指派。但您也可以選擇要在其上建立磁碟區的特定聚合。

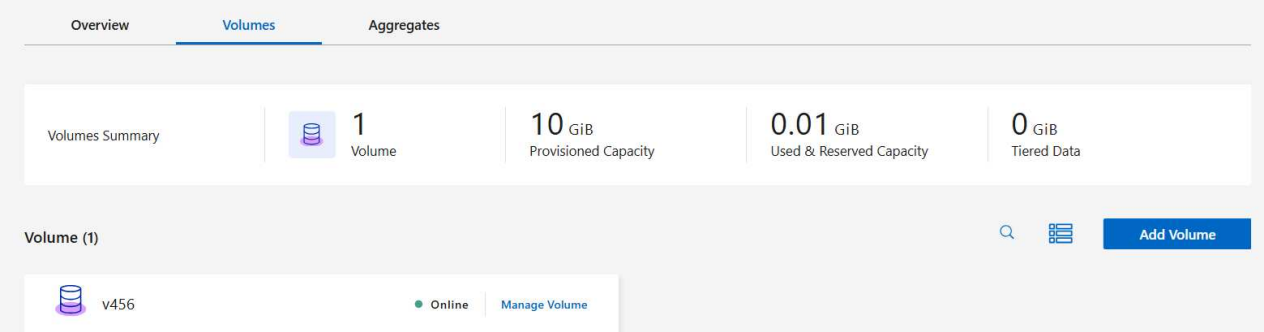
步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在 **Systems** 頁面上，雙擊要在其上設定FlexVol volume的Cloud Volumes ONTAP系統的名稱。

   您可以透過讓控制台為您處理磁碟分配來建立捲，或為磁碟區選擇特定的聚合。只有當您對Cloud Volumes ONTAP系統上的資料聚合有充分了解時，才建議選擇特定的聚合。

任何聚合

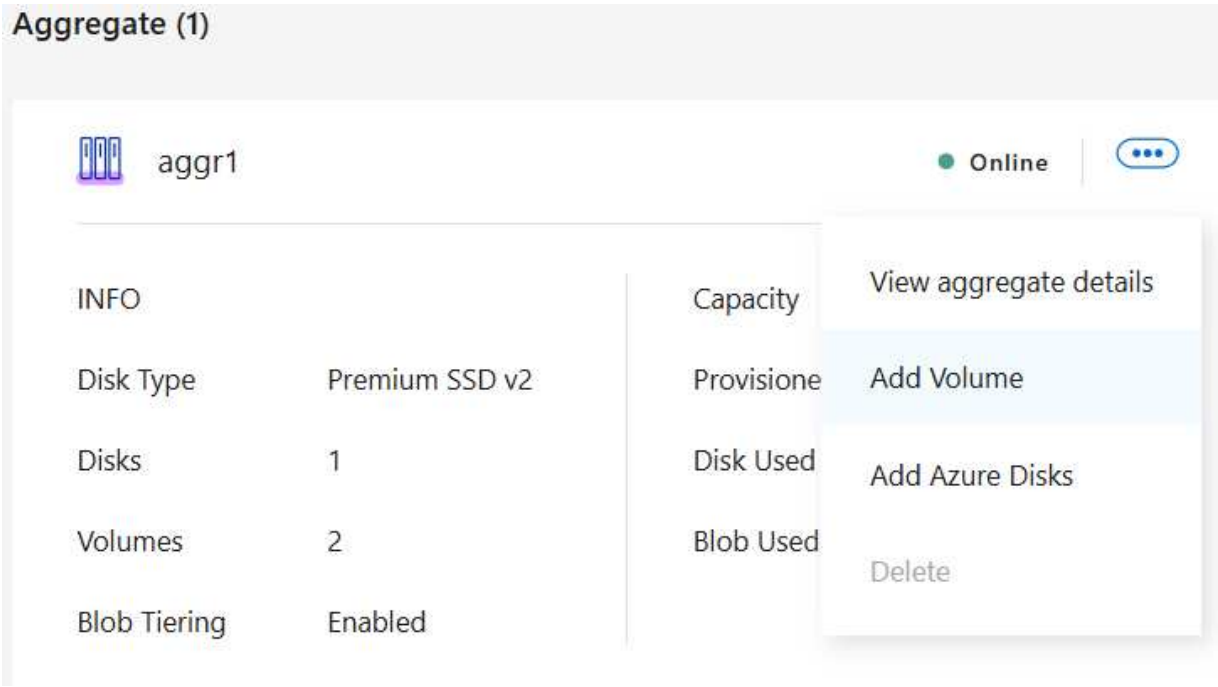
選擇“卷”選項卡，然後按一下“新增卷”



特定骨材

a. 在*聚合*選項卡上，轉到所需的聚合並點擊 ••• 圖示.

b. 選擇*新增卷*



3. 請依照精靈中的步驟建立磁碟區。

a. 詳細資訊、保護和標籤：輸入有關磁碟區的基本詳細資訊並選擇快照策略。

此頁面上的某些欄位是不言自明的。以下列表描述了您可能需要指導的欄位：

場地	描述
卷名	您可以為新磁碟區輸入的可識別名稱。
卷大小	您可以輸入的最大大小很大程度上取決於您是否啟用精簡配置，這使您能夠建立比目前可用的實體儲存更大的磁碟區。

場地	描述
儲存虛擬機器 (SVM)	儲存虛擬機是在ONTAP內運作的虛擬機，可為您的用戶端提供儲存和資料服務。您可能知道這是 SVM 或 vserver。 Cloud Volumes ONTAP預設配置一個儲存虛擬機，但某些配置支援額外的儲存虛擬機。您可以為新磁碟區指定儲存虛擬機器。
快照策略	Snapshot 副本策略指定自動建立的NetApp Snapshot 副本的頻率和數量。NetApp Snapshot 副本是時間點檔案系統映像，它不會影響效能並且只需要最少的儲存空間。您可以選擇預設策略或無策略。對於瞬態數據，您可能會選擇無：例如，對於 Microsoft SQL Server，請選擇 tempdb。

b. 協定：為磁碟區選擇一個協定（NFS、CIFS 或 iSCSI），然後提供所需的資訊。

   如果您選擇 CIFS 但尚未設定伺服器，則按一下「下一步」後控制台會提示您設定 CIFS 連線。

   "了解支援的客戶端協定和版本" 。

   以下部分描述了您可能需要指導的欄位。這些描述是按照協議組織的。

NFS

存取控制

選擇自訂匯出策略以使磁碟區可供客戶端使用。

出口政策

定義子網路中可以存取磁碟區的客戶端。預設情況下，控制台輸入一個提供對子網路中所有實例的存取權限的值。

CIFS

權限和使用者/群組

使您能夠控制使用者和群組對 SMB 共用的存取等級（也稱為存取控制清單或 ACL）。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。如果指定網域 Windows 使用者名，則必須使用網域\使用者名稱格式包含使用者的網域。

DNS 主 **IP** 位址和輔助 **IP** 位址

為 CIFS 伺服器提供名稱解析的 DNS 伺服器的 IP 位址。所列的 DNS 伺服器必須包含定位 CIFS 伺服器將加入的網域的 Active Directory LDAP 伺服器和網域控制站所需的服務位置記錄 (SRV)。

如果您正在設定 Google 管理的 Active Directory，則預設可以使用 169.254.169.254 IP 位址存取 AD。

要加入的 **Active Directory** 網域

您希望 CIFS 伺服器加入的 Active Directory (AD) 網域的 FQDN。

授權加入網域的憑證

具有足夠權限將電腦新增至 AD 網域內指定組織單位 (OU) 的 Windows 帳戶的名稱和密碼。

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 網域內與 CIFS 伺服器關聯的組織單位。預設值為 CN=Computers。

- 若要將 AWS Managed Microsoft AD 設定為Cloud Volumes ONTAP 的AD 伺服器，請在此欄位中輸入 **OU=Computers,OU=corp**。
- 若要將 Azure AD 網域服務設定為Cloud Volumes ONTAP 的AD 伺服器，請在此欄位中輸入 **OU=AADDC Computers** 或 **OU=AADDC Users**。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 文件：在 Azure AD 網域服務託管網域中建立組織單位 (OU)"^]
- 若要將 Google Managed Microsoft AD 設定為Cloud Volumes ONTAP的 AD 伺服器，請在此欄位中輸入 **OU=Computers,OU=Cloud**。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud 文件：Google Managed Microsoft AD 中的組織單位"^]

DNS 網域

Cloud Volumes ONTAP儲存虛擬機器 (SVM) 的 DNS 網域。大多數情況下，該域與 AD 域相同。

NTP 伺服器

選擇「使用 Active Directory 網域」以使用 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，那麼您應該使用 API。欲了解更多信息，請參閱 "NetApp Console自動化文檔"。

請注意，只有在建立 CIFS 伺服器時才能設定 NTP 伺服器。建立 CIFS 伺服器後，它不可配置。

iSCSI

邏輯單元號

iSCSI 儲存目標稱為 LUN（邏輯單元），並以標準區塊裝置呈現給主機。當您建立 iSCSI 磁碟區時，控制台會自動為您建立 LUN。我們透過為每個磁碟區建立一個 LUN 來簡化操作，因此無需進行任何管理。建立磁碟區後，"使用 IQN 從主機連線到 LUN" 。

發起者群組

啟動器群組 (igroup) 指定哪些主機可以存取儲存系統上的指定 LUN

主機啟動器 **(IQN)**

iSCSI 目標透過標準乙太網路網路適配器 (NIC)、具有軟體啟動器的 TCP 卸載引擎 (TOE) 卡、融合網路適配器 (CNA) 或專用主機匯流排適配器 (HBA) 連接到網絡，並透過 iSCSI 限定名稱 (IQN) 進行識別。

a. 磁碟類型：根據您的效能需求和成本要求為磁碟區選擇底層磁碟類型。

   - "在 AWS 中調整系統規模"
     - "在 Azure 中調整系統大小"
     - "在 Google Cloud 中調整系統規模"

4. 使用設定檔和分層策略：選擇是否啟用或停用磁碟區上的儲存效率功能，然後選擇"卷分層策略"。

   ONTAP包含多種儲存效率功能，可減少您所需的總儲存量。 NetApp儲存效率功能有以下優勢：

   精簡配置

   向主機或使用者提供比實體儲存池中實際擁有的更多的邏輯儲存。不是預先分配儲存空間，而是在寫入資料時動態地將儲存空間分配給每個磁碟區。

   重複資料刪除

   透過定位相同的資料塊並將其替換為對單一共享區塊的引用來提高效率。該技術透過消除駐留在同一磁碟區中的冗餘資料區塊來減少儲存容量需求。

   壓縮

   透過壓縮主儲存、輔助儲存和歸檔儲存磁碟區內的資料來減少儲存資料所需的實體容量。

5. 審核：審核有關卷的詳細信息，然後按一下*新增*。

結果

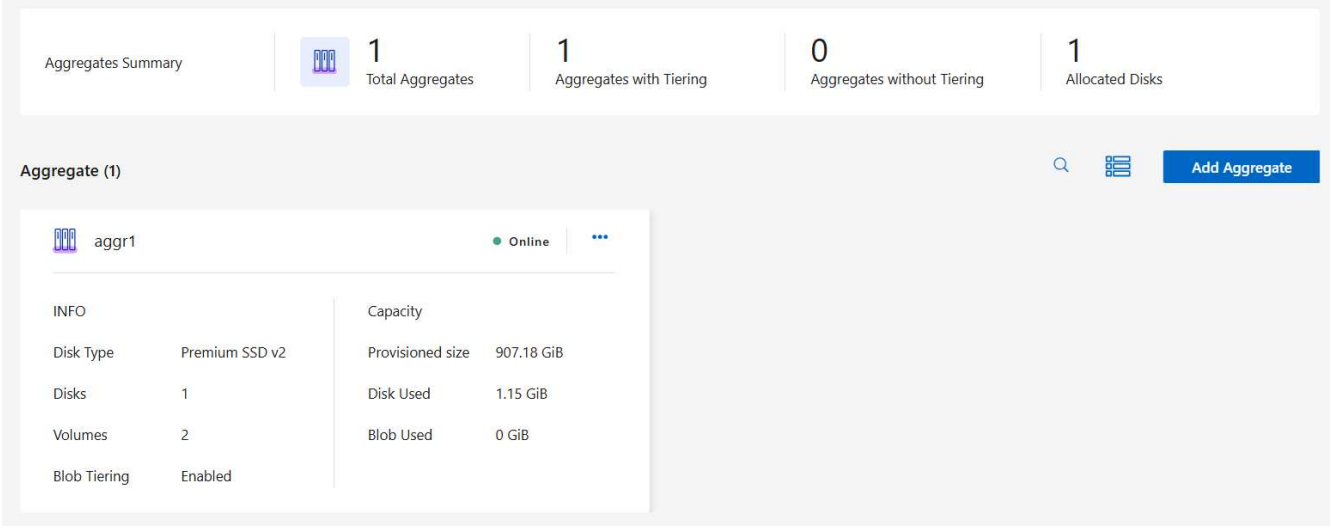
控制台在Cloud Volumes ONTAP系統上建立磁碟區。

在 HA 配置中的第二個節點上建立卷

預設情況下，控制台在 HA 配置中的第一個節點上建立磁碟區。如果您需要主動-主動配置，其中兩個節點都向客戶端提供數據，則必須在第二個節點上建立聚合和磁碟區。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在「系統」頁面上，雙擊要管理聚合的Cloud Volumes ONTAP系統的名稱。
3. 在“聚合”標籤上，按一下“新增聚合”，然後建立聚合。



4. 對於主節點，選擇 HA 對中的第二個節點。
5. 控制台建立聚合後，選擇它，然後按一下*建立磁碟區*。
6. 輸入新卷的詳細信息，然後按一下“建立”。

結果

控制台在 HA 對中的第二個節點上建立磁碟區。

對於在多個 AWS 可用區中部署的 HA 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。

建立磁碟區後

如果您配置了 CIFS 共享，請授予使用者或群組對檔案和資料夾的權限，並驗證這些使用者是否可以存取共用並建立檔案。

如果要將配額應用於卷，則必須使用ONTAP系統管理員或ONTAP CLI。配額可讓您限製或追蹤使用者、群組或 qtree 使用的磁碟空間和檔案數量。

管理Cloud Volumes ONTAP系統上的捲

您可以在NetApp Console中管理磁碟區和 CIFS 伺服器。您也可以移動磁碟區以避免容量問題。

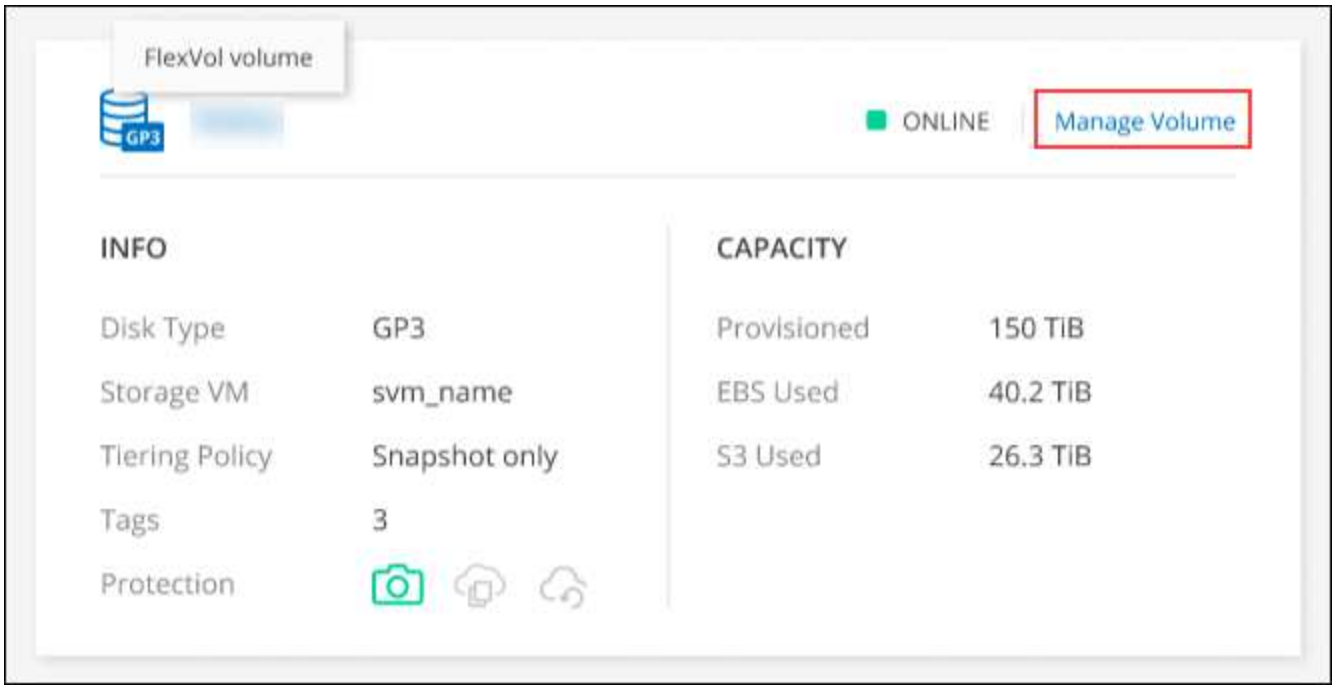
您可以在NetApp Console標準視圖中管理卷，也可以透過控制台中包含的ONTAP系統管理器來管理卷，以進行高級捲管理。標準視圖提供了一組有限的選項來修改您的捲。系統管理器提供高階管理，例如複製、調整大小、更改反勒索軟體、分析、保護和活動追蹤的設定以及跨層移動磁碟區。有關信息，請參閱"使用系統管理員管理Cloud Volumes ONTAP"。

管理磁碟區

透過使用控制台的標準視圖，您可以根據儲存需求管理磁碟區。您可以檢視、編輯、複製、還原和刪除磁碟區。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，雙擊要管理磁碟區的Cloud Volumes ONTAP系統。
3. 選擇“卷”選項卡。



4. 在所需的捲圖塊上，按一下*管理磁碟區*。

任務	行動
查看有關卷的信息	在「管理磁碟區」面板的「磁碟區操作」下，按一下「檢視磁碟區詳細資料」。
取得NFS掛載命令	a. 在「管理磁碟區」面板的「磁碟區操作」下，按一下「安裝指令」。 b. 按一下“複製”。

任務	行動
複製卷	a. 在「管理磁碟區」面板的「磁碟區操作」下，按一下「複製磁碟區」。 b. 根據需要修改克隆名稱，然後按一下“克隆”。 此過程會建立一個FlexClone磁碟區。 FlexClone磁碟區是可寫入的、時間點副本，它節省空間，因為它只使用少量空間來儲存元數據，並且僅在更改或新增資料時才消耗額外的空間。 要了解有關FlexClone卷的更多信息，請參閱 "ONTAP 9 邏輯儲存管理指南"。
編輯卷（限讀寫卷）	a. 在“管理磁碟區”面板的“磁碟區操作”下，按一下“編輯磁碟區設定” b. 修改磁碟區的快照策略、NFS 協定版本、NFS 存取控制清單（匯出策略）或共用權限，然後按一下*套用*。 如果您需要自訂 Snapshot 策略，則可以使用ONTAP System Manager 建立它們。
刪除卷	a. 在「管理磁碟區」面板的「磁碟區操作」下，按一下「刪除磁碟區」。 b. 在「刪除磁碟區」視窗下，輸入要刪除的磁碟區的名稱。 c. 再次點選“刪除”進行確認。
按需建立 Snapshot 副本	a. 在「管理磁碟區」面板的「保護操作」下，按一下「建立 Snapshot 副本」。 b. 如果需要，請變更名稱，然後按一下“建立”。
將資料從 Snapshot 副本還原到新卷	a. 在「管理磁碟區」面板的「保護操作」下，按一下「從 Snapshot 副本還原」。 b. 選擇一個 Snapshot 副本，輸入新磁碟區的名稱，然後按一下「復原」。
更改底層磁碟類型	a. 在「管理磁碟區」面板的「進階操作」下，按一下「變更磁碟類型」。 b. 選擇磁碟類型，然後按一下“變更”。 控制台將磁碟區移至使用所選磁碟類型的現有聚合，或為該磁碟區建立新的聚合。

任務	行動
更改分層策略	a. 在「管理磁碟區」面板的「進階操作」下，按一下「變更分層策略」。 b. 選擇不同的策略並點擊*更改*。 控制台將磁碟區移至使用具有分層功能的所選磁碟類型的現有聚合，或為該磁碟區建立新的聚合。
刪除卷	a. 選擇一個卷，然後按一下“刪除”。 b. 在對話方塊中輸入磁碟區的名稱。 c. 再次點選“刪除”進行確認。

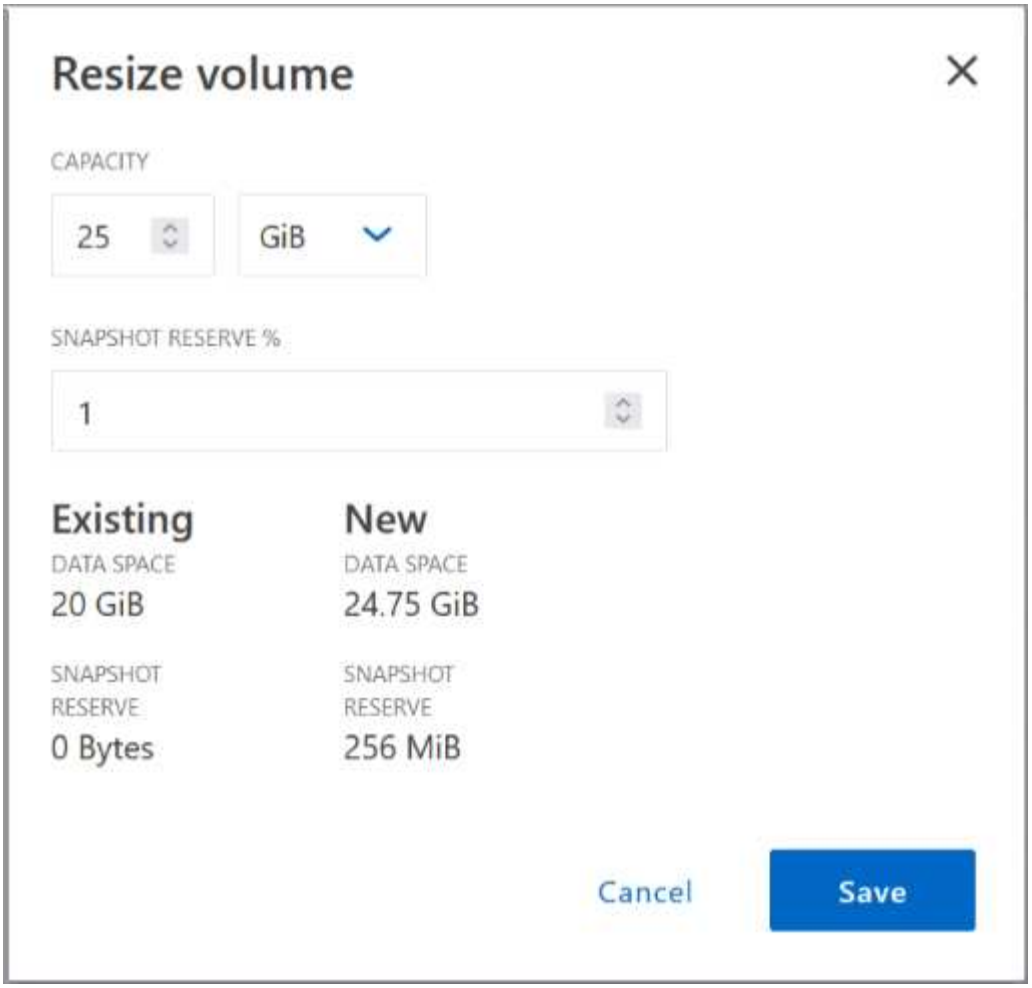
調整磁碟區大小

預設情況下，當磁碟區空間不足時，它會自動增長到最大大小。預設值為 1,000，這表示磁碟區可以增長到其大小的 11 倍。該值可以在控制台代理的設定中配置。

如果您需要調整磁碟區大小，您可以從控制台中的ONTAP系統管理員進行操作。

步驟

1. 按一下系統管理員視圖以透過ONTAP系統管理員調整磁碟區大小。請參閱"如何開始" 。
2. 從左側導覽選單中，選擇“儲存”>“磁碟區”。
3. 從磁碟區清單中，確定應調整大小的磁碟區。
4. 點選選項圖標 。
5. 選擇*調整大小*。
6. 在*調整磁碟區大小*畫面上，根據需要編輯容量和快照預留百分比。您可以將現有的可用空間與修改後的容量進行比較。
7. 點選“儲存”。



調整磁碟區大小時，請務必考慮系統的容量限制。前往 "Cloud Volumes ONTAP發行說明"了解更多。

修改 **CIFS** 伺服器

如果您變更 DNS 伺服器或 Active Directory 網域，則需要修改Cloud Volumes ONTAP中的 CIFS 伺服器，以便它可以繼續為用戶端提供儲存服務。

步驟

1. 從Cloud Volumes ONTAP系統的 **Overview** 標籤中，按一下右側面板下的 **Feature** 標籤。
2. 在 CIFS 設定欄位下，按一下 鉛筆圖示 以顯示 CIFS 設定視窗。
3. 指定 CIFS 伺服器的設定：

任務	行動
選擇儲存虛擬機器 (SVM)	選擇 Cloud Volume ONTAP儲存虛擬機器 (SVM) 顯示其配置的 CIFS 資訊。
要加入的 Active Directory 網域	您希望 CIFS 伺服器加入的 Active Directory (AD) 網域的 FQDN。
授權加入網域的憑證	具有足夠權限將電腦新增至 AD 網域內指定組織單位 (OU) 的 Windows 帳戶的名稱和密碼。

任務	行動
DNS 主 IP 位址和輔助 IP 位址	為 CIFS 伺服器提供名稱解析的 DNS 伺服器的 IP 位址。所列的 DNS 伺服器必須包含定位 Active Directory LDAP 伺服器和 CIFS 伺服器將加入的網域的網域控制站所需的服務位置記錄 (SRV)。 ifdef::gcp[] 如果您正在設定 Google Managed Active Directory，則預設可以使用 169.254.169.254 IP 位址存取 AD。 endif::gcp[]
DNS 網域	Cloud Volumes ONTAP儲存虛擬機器 (SVM) 的 DNS 網域。大多數情況下，該域與 AD 域相同。
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 網域內與 CIFS 伺服器關聯的組織單位。預設值為 CN=Computers。 • 若要將 AWS Managed Microsoft AD 設定為Cloud Volumes ONTAP 的AD 伺服器，請在此欄位中輸入 **OU=Computers,OU=corp**。 • 若要將 Azure AD 網域服務設定為Cloud Volumes ONTAP 的AD 伺服器，請在此欄位中輸入 **OU=AADDC Computers** 或 **OU=AADDC Users**。"Azure 文件：在 Azure AD 網域服務託管網域中建立組織單位 (OU)" • 若要將 Google Managed Microsoft AD 設定為Cloud Volumes ONTAP 的 AD 伺服器，請在此欄位中輸入 **OU=Computers,OU=Cloud** 。"Google Cloud 文件：Google Managed Microsoft AD 中的組織單位"

4. 點選“設定”。

結果

Cloud Volumes ONTAP使用變更來更新 CIFS 伺服器。

移動磁碟區

移動磁碟區以提高容量利用率、提高效能並滿足服務等級協定。

您可以在ONTAP系統管理員中移動卷，方法是選擇磁碟區和目標聚合、啟動卷移動操作以及選擇性地監控卷移動作業。使用系統管理員時，磁碟區移動操作會自動完成。

步驟

1. 使用ONTAP系統管理員或ONTAP CLI 將磁碟區移至聚合。

   在大多數情況下，您可以使用系統管理員來移動磁碟區。

   有關說明，請參閱"ONTAP 9 捲移動快速指南"。

當控制台顯示「需要操作」訊息時移動卷

控制台可能會顯示「需要採取行動」訊息，表示需要移動磁碟區以避免容量問題，但您需要自行解決問題。如果發生這種情況，您需要確定如何修正問題，然後移動一個或多個磁碟區。

當聚合已達到 90% 的使用容量時，控制台會顯示這些「需要操作」訊息。如果啟用了資料分層，則當聚合已達到 80% 的已使用容量時會顯示訊息。預設情況下，保留 10% 的可用空間用於資料分層。"了解有關數據分層的可用空間比率的更多信息" 。

步驟

1. [確定如何修正容量問題] 。
2. 根據您的分析，移動卷以避免容量問題：
   - [將磁碟區移至另一個系統以避免容量問題] 。
   - [將磁碟區移至另一個聚合以避免容量問題] 。

確定如何修正容量問題

如果控制台無法提供移動磁碟區以避免容量問題的建議，則必須確定需要移動的磁碟區以及是否應將它們移至同一系統上的另一個聚合或另一個系統。

步驟

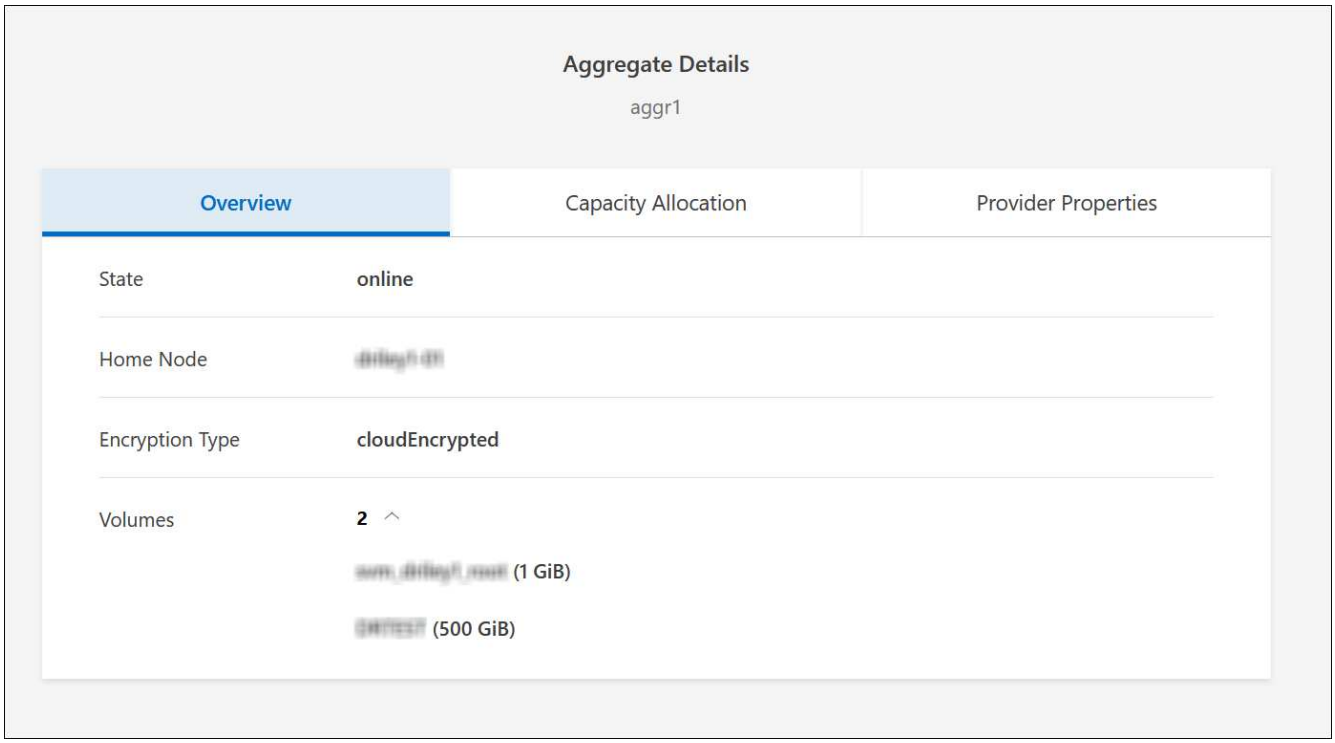
1. 查看“需要操作”訊息中的高級信息，以確定已達到其容量限制的聚合。

   例如，進階資訊應該顯示類似以下內容：聚合 aggr1 已達到其容量限制。

2. 確定要移出聚合的一個或多個磁碟區：

   a. 在Cloud Volumes ONTAP系統中，按一下 **Aggregates tab**。
   b. 在聚合圖塊上，按一下 圖標，然後點擊*查看匯總詳情*。
   c. 在「聚合詳細資料」畫面的「概述」標籤下，檢視每個磁碟區的大小並選擇要移出聚合的一個或多個磁碟區。

      您應該選擇足夠大的磁碟區來釋放聚合中的空間，以避免將來出現額外的容量問題。



3. 如果系統尚未達到磁碟限制，則應將磁碟區移至現有聚合或同一系統上的新聚合。

   有關信息，請參閱將磁碟區移至另一個聚合以避免容量問題。

4. 如果系統已達到磁碟限制，請執行下列操作之一：
   a. 刪除所有未使用的磁碟區。
   b. 重新排列磁碟區以釋放聚合上的空間。

      有關信息，請參閱將磁碟區移至另一個聚合以避免容量問題。

   c. 將兩個或多個磁碟區移動到另一個有空間的系統。

      有關信息，請參閱將磁碟區移至另一個聚合以避免容量問題。

將磁碟區移至另一個系統以避免容量問題

您可以將一個或多個磁碟區移至另一個Cloud Volumes ONTAP系統以避免容量問題。如果系統達到其磁碟限制，您可能需要執行此操作。

關於此任務

您可以按照此任務中的步驟來修正以下「需要操作」訊息：

> 移動磁碟區對於避免容量問題是必要的；但是，控制台無法為您執行此操作，因為系統已達到磁碟限制。

步驟

1. 確定具有可用容量的Cloud Volumes ONTAP系統，或部署新系統。

2. 將來源系統拖曳到目標系統以執行磁碟區的一次性資料複製。

   有關信息，請參閱"在系統之間複製數據"。

3. 前往「複製狀態」頁面，然後中斷SnapMirror關係，將複製的磁碟區從資料保護磁碟區轉換為讀取/寫入磁碟區。

   有關信息，請參閱"管理資料複製計劃和關係"。

4. 配置資料存取的磁碟區。

   有關配置資料存取目標磁碟區的信息，請參閱"ONTAP 9 卷災難復原快速指南"。

5. 刪除原始磁碟區。

   有關信息，請參閱"管理磁碟區"。

將磁碟區移至另一個聚合以避免容量問題

您可以將一個或多個磁碟區移至另一個聚合以避免容量問題。

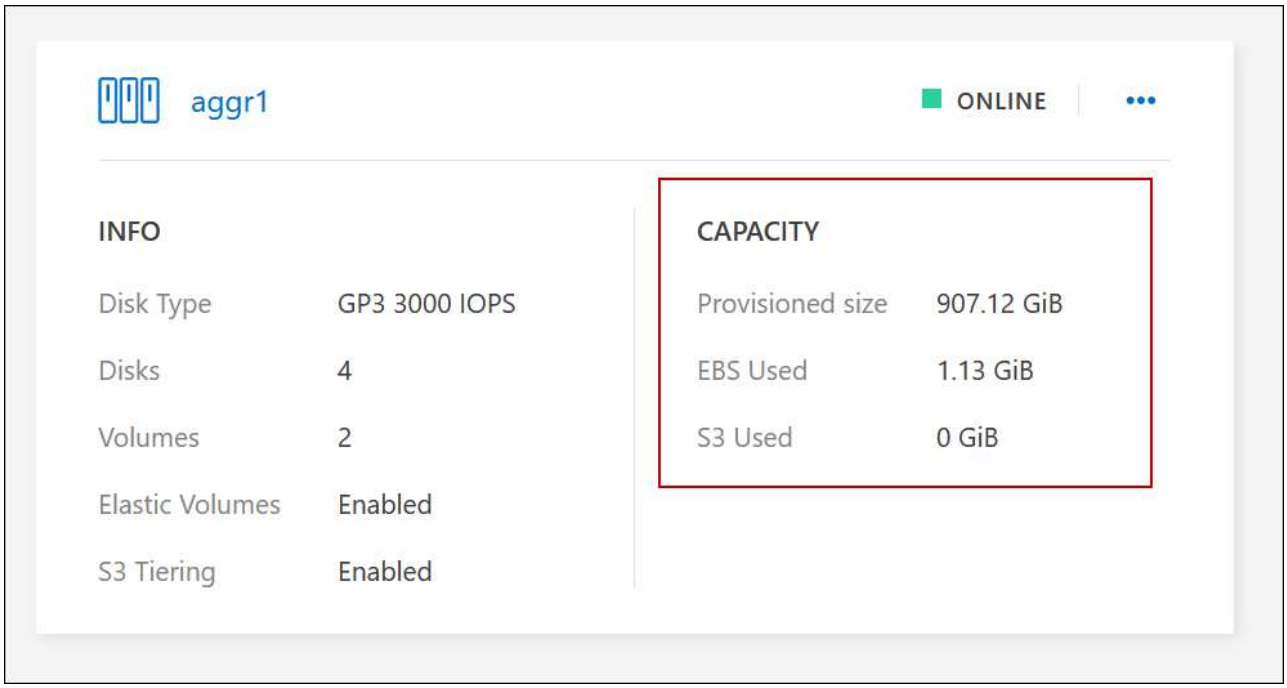
關於此任務

您可以按照此任務中的步驟來修正以下「需要操作」訊息：

> 需要移動兩個或更多磁碟區以避免容量問題；但是，控制台無法為您執行此操作。

步驟

1. 驗證現有聚合是否具有可供您需要移動的磁碟區所使用的容量：
   a. 在Cloud Volumes ONTAP系統上，按一下 **Aggregates tab**。
   b. 在所需的聚合圖塊上，按一下 ••• 圖標，然後*查看聚合詳細資訊*以查看可用容量（預先配置大小減去已使用聚合容量）。



2. 如果需要，將磁碟新增至現有聚合：
   a. 選擇聚合，然後按一下•••圖示 > 新增磁碟。
   b. 選擇要新增的磁碟數量，然後按一下「新增」。
3. 如果沒有可用容量的聚合，則建立一個新的聚合。

   有關信息，請參閱"建立聚合"。
4. 使用ONTAP系統管理員或ONTAP CLI 將磁碟區移至聚合。
5. 在大多數情況下，您可以使用系統管理員來移動磁碟區。

   有關說明，請參閱"ONTAP 9 捲移動快速指南"。

交易量變動執行緩慢的原因

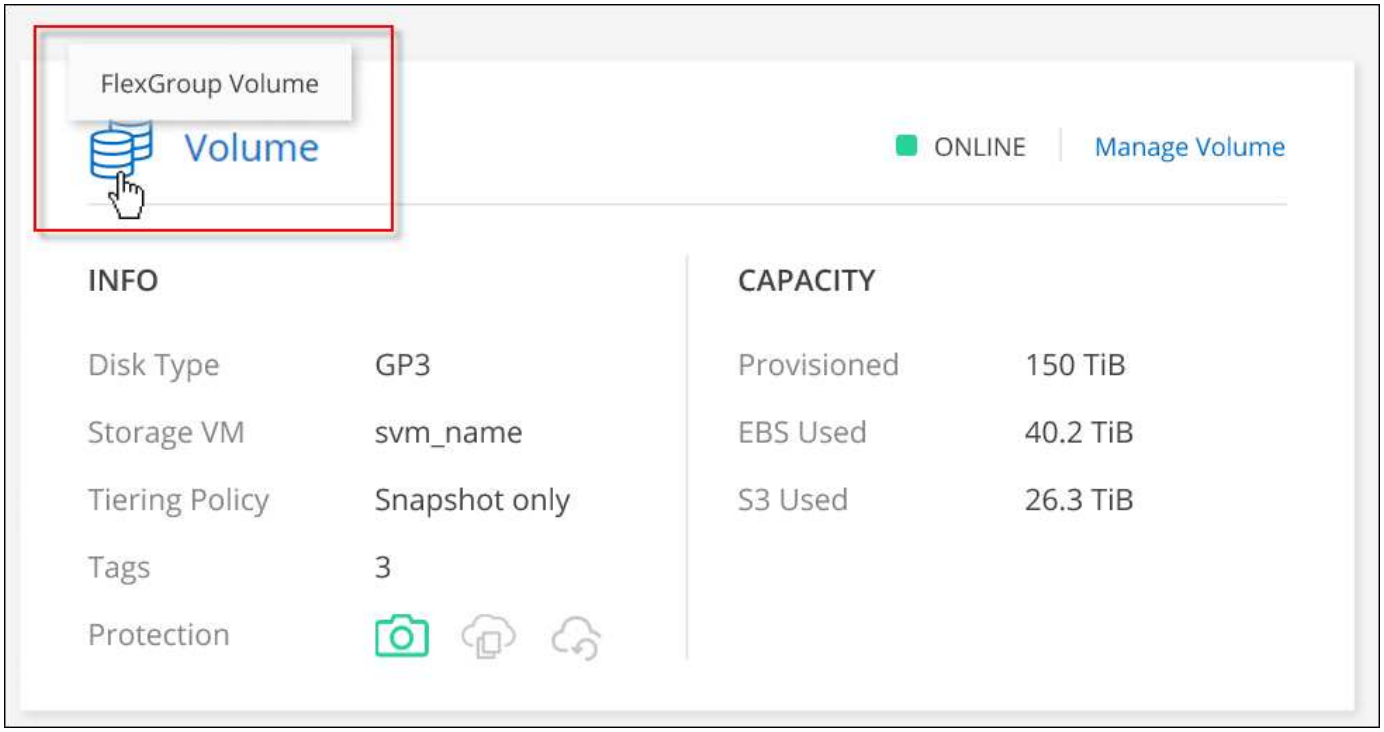
如果Cloud Volumes ONTAP符合以下任何條件，則行動磁碟區所需的時間可能會比您預期的要長：

- 該卷是一個克隆。
- 該卷是克隆的父親卷。
- 來源聚合或目標聚合具有單一吞吐量最佳化 HDD (st1) 磁碟。
- 其中一個聚合使用了較舊的物件命名方案。兩個聚合必須使用相同的名稱格式。

  如果在 9.4 或更早版本中的聚合上啟用了資料分層，則使用較舊的命名方案。
- 來源聚合和目標聚合上的加密設定不匹配，或正在進行重新金鑰。
- 在磁碟區移動時指定了 *-tiering-policy* 選項來變更分層原則。
- 在磁碟區移動時指定了 *-generate-destination-key* 選項。

查看FlexGroup卷

您可以直接透過控制台中的「磁碟區」標籤檢視透過ONTAP System Manager 或ONTAP CLI 建立的FlexGroup區。您可以透過專用的 **Volumes** 圖塊查看 FleGroup 卷的詳細信息，並透過圖示的懸停文字識別每個FlexGroup卷組。此外，您可以透過磁碟區樣式列識別和排序磁碟區清單視圖下的FlexGroup磁碟區。



目前，您只能在控制台下方查看現有的FlexGroup磁碟區。您無法在控制台中建立FlexGroup磁碟區。

將非活動Cloud Volumes ONTAP資料分層到低成本物件存儲

您可以透過將用於熱資料的 SSD 或 HDD 效能層與用於非活動資料的物件儲存容量層結合來降低Cloud Volumes ONTAP的儲存成本。資料分層由FabricPool技術提供支援。有關進階概述，請參閱"資料分層概述"。

要設定資料分層，您需要執行以下操作：

1. 選擇支援的配置

大多數配置都受支援。如果您擁有執行最新版本的Cloud Volumes ONTAP系統，那麼您就可以開始了。"了解更多" 。

2. 確保**Cloud Volumes ONTAP**與物件儲存之間的連接

- 對於 AWS，您需要一個指向 Amazon Simple Storage Service （Amazon S3）的 VPC 終端節點。了解更多.
- 對於 Azure，只要NetApp Console具有所需的權限，您就不需要執行任何操作。了解更多 。

- 對於 Google Cloud，您需要設定私人 Google Access 子網路並設定服務帳戶。了解更多 。

3 確保您已啟用分層聚合

應在聚合上啟用資料分層，以便在磁碟區上啟用它。您應該了解新捲和現有捲的要求。了解更多 。

4 建立、修改或複製磁碟區時選擇分層策略

當您建立、修改或複製磁碟區時， NetApp Console會提示您選擇分層策略。

- "來自讀寫卷的層次數據"
- "來自資料保護卷的分層數據"

> 資料分層不需要什麼？
>
> - 您不需要安裝功能授權來啟用資料分層。
> - 您不需要為容量層建立物件儲存。控制台會為您完成該操作。
> - 您不需要在系統層級啟用資料分層。
>
> 控制台在創建系統時為冷數據創建對象存儲，只要沒有連線或權限問題 。之後，您只需要在磁碟區上啟用資料分層（在某些情況下，在聚合體上 ）。

支援資料分層的配置

您可以在使用特定配置和功能時啟用資料分層。

AWS 支援

- 從Cloud Volumes ONTAP 9.2 開始，AWS 支援資料分層。
- 性能層可以是通用 SSD（gp3 或 gp2）或預先配置 IOPS SSD（io1）。

> 使用吞吐量最佳化 HDD (st1) 時，我們不建議將資料分層到物件儲存。

- 非活動資料分層儲存到 Amazon S3 儲存桶。不支援分層到其他提供者。

Azure 中的支持

- Azure 支援資料分層，如下所示：
  - 版本 9.4 適用於單節點系統
  - 9.6 版，配備 HA 對
- 效能層可以是高級 SSD 託管磁碟、標準 SSD 託管磁碟或標準 HDD 託管磁碟。
- 非活動資料分層到 Microsoft Azure Blob。不支援分層到其他提供者。

Google Cloud 支援

- 從Cloud Volumes ONTAP 9.6 開始，Google Cloud 支援資料分層。
- 效能層可以是 SSD 持久性磁碟、平衡持久性磁碟或標準持久性磁碟。
- 非活動資料分層儲存到 Google Cloud Storage。不支援分層到其他提供者。

功能互通性

- 資料分層由加密技術支援。
- 必須在磁碟區上啟用精簡配置。

要求

根據您的雲端供應商，必須設定某些連線和權限，以便Cloud Volumes ONTAP可以將冷資料分層到物件儲存。

將冷資料分層至 Amazon S3 的要求

確保 Cloud Volumes ONTAP 已連線至 Amazon S3。提供此連線的最佳方法是建立指向 S3 服務的 VPC 端點。有關說明，請參閱 "AWS 文件：建立網關終端節點"。

建立 VPC 端點時，請確保選擇與Cloud Volumes ONTAP實例相對應的區域、VPC 和路由表。您還必須修改安全群組以新增允許流量到 S3 端點的出站 HTTPS 規則。否則， Cloud Volumes ONTAP無法連線到 S3 服務。

如果您遇到任何問題，請參閱 "AWS Support 知識中心：為什麼我無法使用閘道 VPC 終端節點連接到 S3 儲存桶？"。

將冷資料分層到 Azure Blob 儲存體的需求

只要控制台具有所需的權限，您就不需要在效能層和容量層之間建立連線。如果控制台代理程式的自訂角色具有下列權限，則控制台將為您啟用 VNet 服務終端：

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

自訂角色預設包含權限。 "查看控制台代理程式的 Azure 權限"

將冷資料分層到 Google Cloud Storage 儲存桶的要求

- 必須為Cloud Volumes ONTAP所在的子網路設定私有 Google Access。有關說明，請參閱 "Google Cloud 文件：配置私有 Google 存取權限"。
- 必須將服務帳戶附加到Cloud Volumes ONTAP。

  "了解如何設定此服務帳號" 。

  建立Cloud Volumes ONTAP系統時，系統會提示您選擇此服務帳戶。

  如果在部署過程中未選擇服務帳號，則需要關閉 Cloud Volumes ONTAP，前往 Google Cloud Console，然後將服務帳號附加到 Cloud Volumes ONTAP 執行個體。之後，您可以按照下一節中的說明啟用資料分層。

- 若要使用客戶管理的加密金鑰加密儲存桶，請啟用 Google Cloud 儲存桶以使用該金鑰。

  "了解如何將客戶管理的加密金鑰與Cloud Volumes ONTAP結合使用" 。

實現要求後啟用資料分層

只要沒有連線或權限問題，控制台就會在建立系統時為冷資料建立物件儲存。如果您在建立系統之後才實現上面列出的要求，那麼您將需要透過 API 或ONTAP系統管理員手動啟用分層，從而建立物件儲存。

透過控制台啟用分層的功能將在未來的Cloud Volumes ONTAP版本中提供。

確保在聚合上啟用分層

必須在聚合上啟用資料分層才能在磁碟區上啟用資料分層。您應該了解新捲和現有捲的要求。

- 新卷

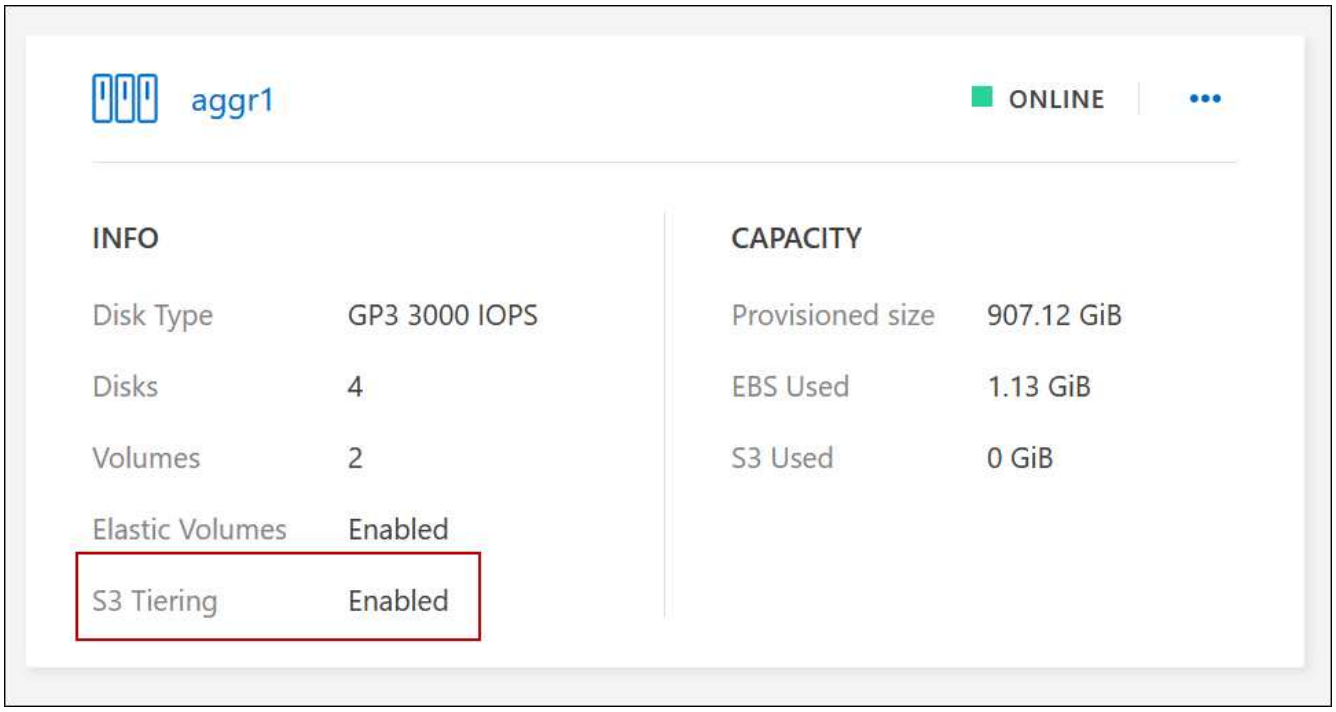
  如果您在新磁碟區上啟用資料分層，則無需擔心在聚合上啟用資料分層。控制台在已啟用分層的現有聚合上建立卷，或者如果尚不存在啟用資料分層的聚合，則為該磁碟區建立新的聚合。

- 現有捲

  若要在現有磁碟區上啟用資料分層，請確保在底層聚合上啟用它。如果現有聚合上未啟用資料分層，則需要使用ONTAP系統管理器將現有聚合附加到物件儲存。

確認聚合上是否啟用了分層的步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 開啟Cloud Volumes ONTAP系統。
3. 選擇“聚合”標籤並檢查聚合上是否啟用或停用分層。



在聚合上啟用分層的步驟

1. 在ONTAP系統管理員中，按一下「儲存」>「層級」。
2. 點擊聚合的操作選單並選擇*附加雲層*。
3. 選擇要附加的雲層，然後按一下「儲存」。

下一步是什麼？

現在您可以在新磁碟區和現有磁碟區上啟用資料分層，如下一節所述。

來自讀寫卷的層次數據

Cloud Volumes ONTAP可以將讀寫磁碟區上的非活動資料分層到經濟高效的物件儲存中，從而釋放效能層以儲存熱資料。

步驟

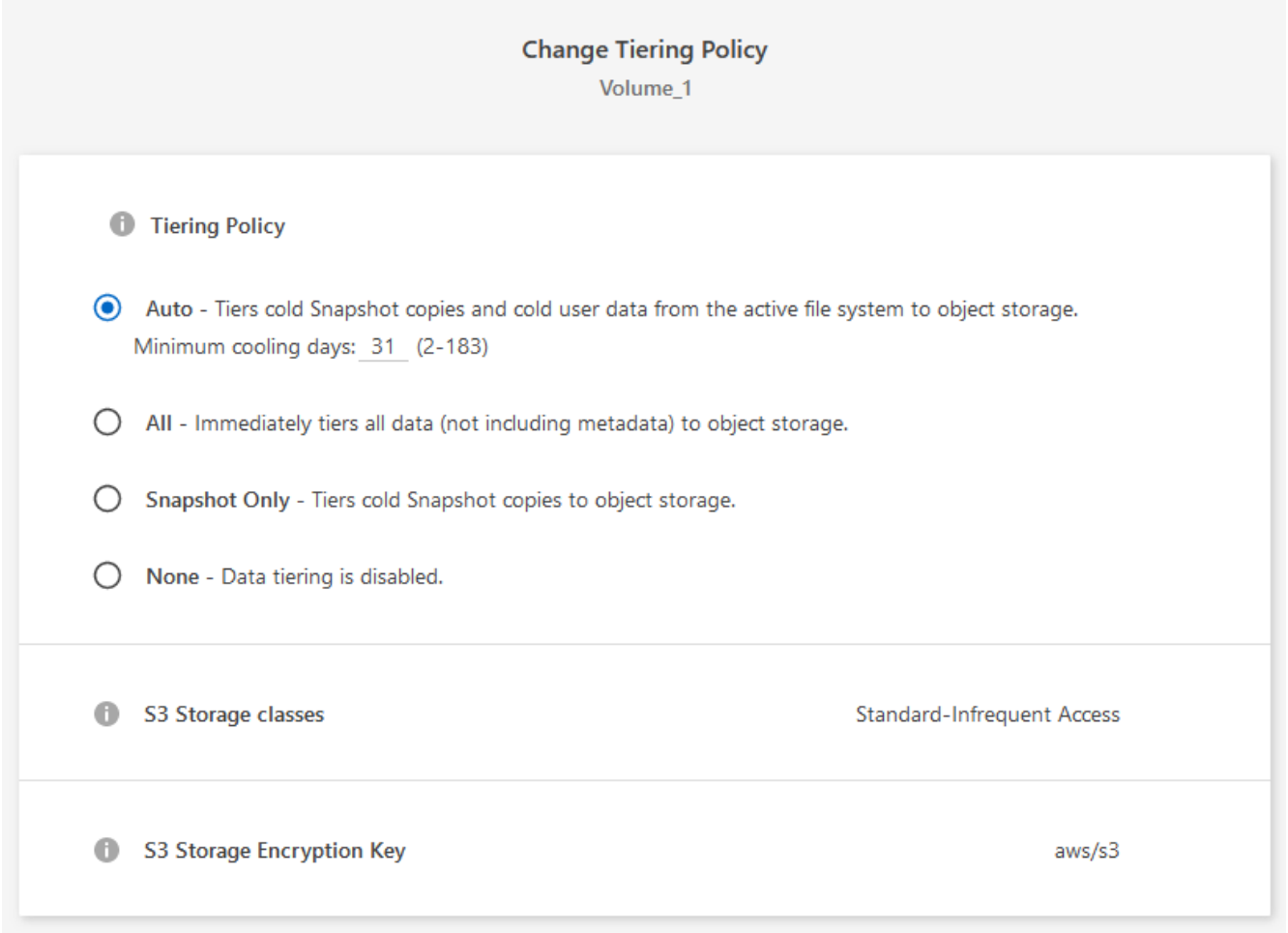
1. 在系統下的*Volumes*標籤中，建立一個新磁碟區或變更現有磁碟區的圖層：

任務	行動
建立新磁碟區	按一下“新增磁碟區”。
修改現有捲	選擇所需的磁碟區圖區塊，按一下「管理磁碟區」以存取「管理磁碟區」右側面板，然後按一下右側面板下的「進階操作」和「變更分層原則」。

2. 選擇分層策略。

   有關這些政策的描述，請參閱"資料分層概述"。

   例子



如果尚不存在啟用資料分層的聚合，則控制台將為磁碟區建立一個新的聚合。

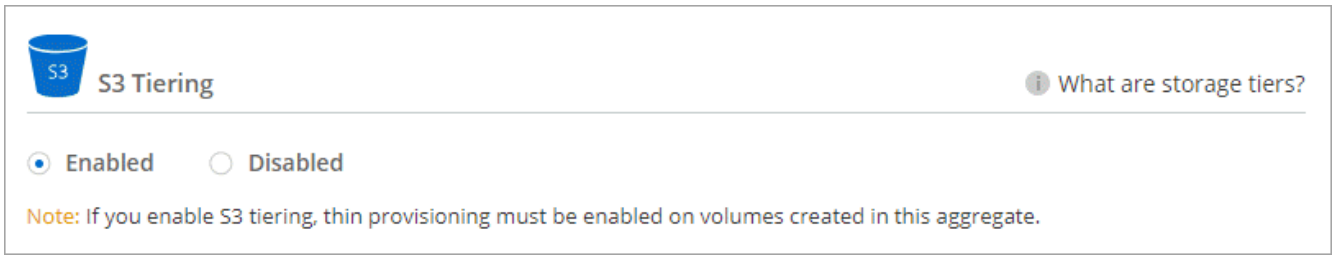
來自資料保護卷的分層數據

Cloud Volumes ONTAP可以將資料從資料保護磁碟區分層到容量層。如果啟動目標卷，資料在讀取時會逐漸移動到效能層。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在 系統 頁面上，選擇包含來源磁碟區的Cloud Volumes ONTAP系統，然後將其拖曳到要將磁碟區複製到的系統。
3. 依照提示操作，直到到達分層頁面並啟用資料分層到物件儲存。

   例子



有關複製資料的協助，請參閱 "將數據複製到雲端或從雲端複製數據"。

變更分層資料的儲存類別

部署Cloud Volumes ONTAP後，您可以透過變更 30 天未存取的非活動資料的儲存類別來降低儲存成本。如果您確實存取數據，則存取成本會更高，因此在更改儲存類別之前必須考慮到這一點。

分層資料的儲存類別是系統範圍的，而不是每個磁碟區的。

有關受支援的儲存類別的信息，請參閱"資料分層概述"。

步驟

1. 在Cloud Volumes ONTAP系統上，按一下選單圖標，然後按一下 儲存類別 或 **Blob** 儲存分層。
2. 選擇一個儲存類，然後按一下*儲存*。

變更資料分層的可用空間比率

資料分層的可用空間比率定義了將資料分層到物件儲存時Cloud Volumes ONTAP SSD/HDD 上需要多少可用空間。預設設定是 10% 的可用空間，但您可以根據需要調整設定。

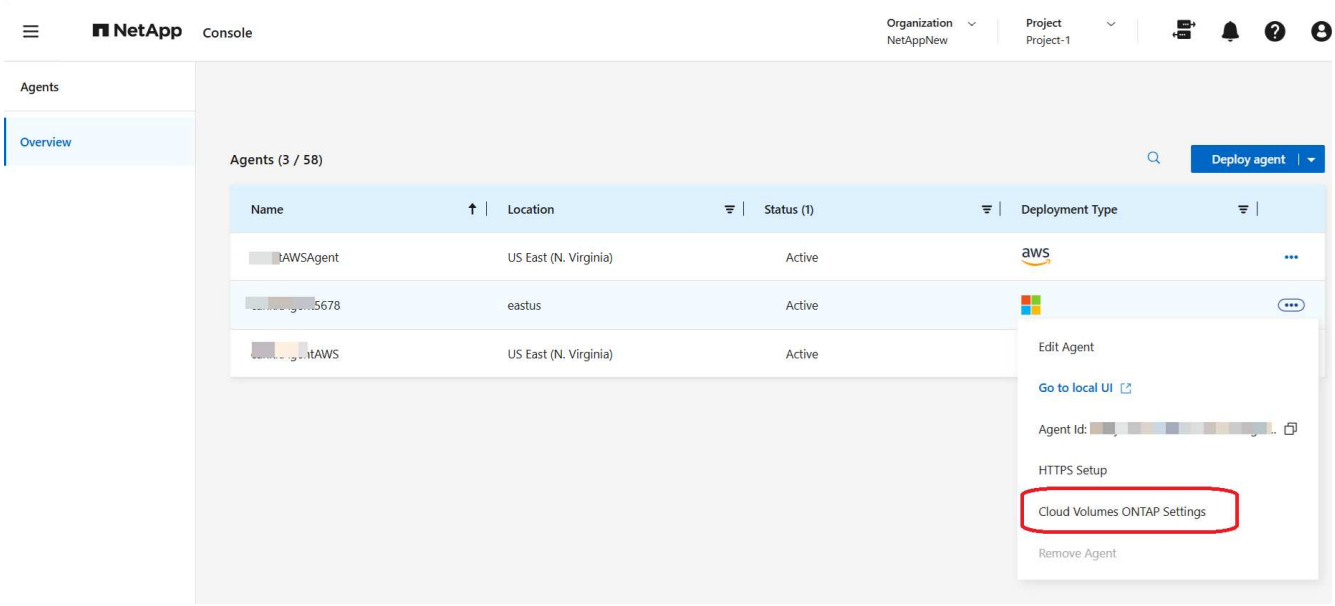
例如，您可以選擇少於 10% 的可用空間，以確保您利用所購買的容量。當需要額外容量時，控制台可以為您購買額外的磁碟（直到達到聚合的磁碟限制）。

如果沒有足夠的空間，那麼Cloud Volumes ONTAP就無法移動數據，而且您可能會遇到效能下降的情況。任何改變都應謹慎進行。如果您不確定，請聯絡NetApp支援尋求指導。

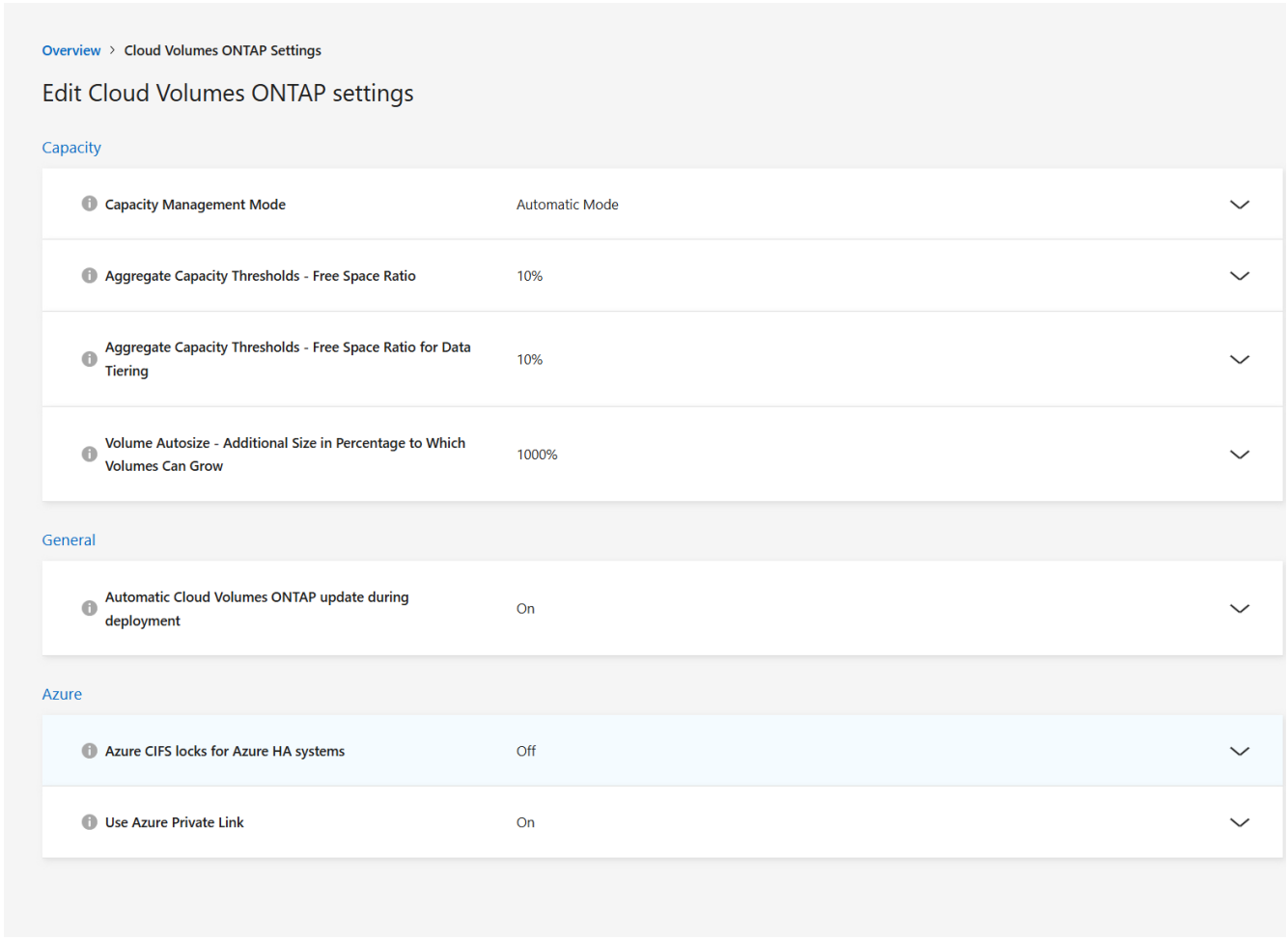
此比率對於災難復原場景很重要，因為當從物件儲存讀取資料時， Cloud Volumes ONTAP會將資料移至 SSD/HDD 以提供更好的效能。如果沒有足夠的空間，那麼Cloud Volumes ONTAP就無法移動資料。在更改比例時請考慮到這一點，以便滿足您的業務需求。

步驟

1. 從左側導覽窗格前往*管理>代理*。
2. 點選 ••• 管理Cloud Volumes ONTAP系統的控制台代理的圖示。
3. 選擇* Cloud Volumes ONTAP設定*。



4. 在「容量」下，按一下「聚合容量閾值 - 資料分層的可用空間比率」。



5. 根據您的要求更改可用空間比例，然後按一下「儲存」。

更改自動分層策略的冷卻期

如果您使用自動分層策略在Cloud Volumes ONTAP磁碟區上啟用了資料分層，則可以根據業務需求調整預設冷卻期。僅使用ONTAP CLI 和 API 支援此操作。

冷卻期是指磁碟區中的使用者資料在被視為「冷」並移動到物件儲存之前必須保持不活動的天數。

自動分層策略的預設冷卻期為 31 天。您可以如下變更冷卻時間：

- 9.8 或更高版本：2 天至 183 天
- 9.7 或更早版本：2 天至 63 天

步

1. 建立磁碟區或修改現有磁碟區時，請在 API 請求中使用 *minimumCoolingDays* 參數。

在系統退役時刪除 **S3** 儲存桶

當您退役環境時，您可以刪除包含來自Cloud Volumes ONTAP系統的分層資料的 S3 儲存桶。

只有在滿足以下條件時，您才可以刪除 S3 儲存桶：

- Cloud Volume ONTAP系統已從控制台中刪除。
- 所有物件都從儲存桶中刪除，並且 S3 儲存桶為空。

當您退役Cloud Volumes ONTAP系統時，為該環境建立的 S3 儲存桶不會自動刪除。相反，它保持孤立狀態以防止任何意外的資料遺失。您可以刪除儲存桶中的對象，然後移除 S3 儲存桶本身，或保留它以供日後使用。參考 "ONTAP CLI：vserver object-store-server bucket 刪除"。

從主機系統連接到**Cloud Volumes ONTAP**上的 **LUN**

當您建立 iSCSI 磁碟區時， NetApp Console會自動為您建立 LUN。我們透過為每個磁碟區建立一個 LUN 來簡化操作，因此無需進行任何管理。建立磁碟區後，使用 IQN 從主機連線到 LUN。

請注意以下事項：

- 控制台的自動容量管理不適用於 LUN。當它建立 LUN 時，它會停用自動增長功能。
- 您可以從ONTAP系統管理員或ONTAP CLI 建立其他 LUN。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，雙擊要管理磁碟區的Cloud Volumes ONTAP系統。
3. 在系統中，選擇*Volumes*選項卡。
4. 前往所需的磁碟區圖區塊，然後選擇*管理磁碟區*以存取右側的管理磁碟區面板。
5. 按一下*目標 iQN*。
6. 按一下*複製*以複製 iQN 名稱。

7. 建立從主機到 LUN 的 iSCSI 連線。
    - "適用於 Red Hat Enterprise Linux 的ONTAP 9 iSCSI 快速設定：啟動與目標的 iSCSI 會話"
    - "適用於 Windows 的ONTAP 9 iSCSI 快速設定：啟動與目標的 iSCSI 會話"
    - "ONTAP SAN 主機配置"

使用Cloud Volumes ONTAP系統上的FlexCache磁碟區加速資料存取

FlexCache卷是一種儲存卷，用於快取從原始（或來源）卷讀取的 SMB 和 NFS 資料。隨後讀取快取資料可以加快對該資料的存取速度。

您可以使用FlexCache磁碟區來加快資料存取速度或卸載存取量大的磁碟區的流量。 FlexCache磁碟區有助於提高效能，特別是當用戶端需要重複存取相同資料時，因為可以直接提供資料而無需存取原始磁碟區。 FlexCache卷非常適合讀取密集的系統工作負載。

NetApp Console提供FlexCache磁碟區的管理"NetApp Volume Caching"。

您也可以使用ONTAP CLI 或ONTAP系統管理器來建立和管理FlexCache磁碟區：

- "FlexCache卷實現更快資料存取電源指南"
- "在 System Manager 中建立FlexCache卷"

當來源加密時使用FlexCache

在原始磁碟區已加密的Cloud Volumes ONTAP系統上設定FlexCache時，需要執行額外的步驟，以確保FlexCache磁碟區可以正確存取和快取加密資料。

開始之前

1. 加密設定：確保來源磁碟區完全加密且可操作。對於Cloud Volumes ONTAP系統，這涉及與特定於雲端的金鑰管理服務整合。

對於 AWS，這通常表示使用 AWS 金鑰管理服務 (KMS)。有關信息，請參閱"使用 AWS Key Management Service 管理金鑰"。

對於 Azure，您需要為NetApp磁碟區加密 (NVE) 設定 Azure Key Vault。有關信息，請參閱"使用 Azure Key Vault 管理金鑰"。

對於 Google Cloud，它是 Google Cloud Key Management Service。有關信息，請參閱"使用 Google 的雲端金鑰管理服務管理金鑰"。

1. 金鑰管理服務：在建立FlexCache區之前，請先確認金鑰管理服務是否在Cloud Volumes ONTAP系統上正確設定。此配置對於FlexCache磁碟區解密來自原始磁碟區的資料至關重要。
2. 許可：確認有效的FlexCache許可證可用並在Cloud Volumes ONTAP系統上啟動。
3. * ONTAP版本*：確保您的Cloud Volumes ONTAP系統的ONTAP版本支援帶有加密磁碟區的FlexCache 。參考最新 "ONTAP發行說明"或相容性矩陣以獲取更多資訊。
4. 網路配置：確保網路配置允許原始磁碟區和FlexCache磁碟區之間的無縫通訊。這包括雲端環境中的正確路由和 DNS 解析。

步驟

使用加密來源磁碟區在Cloud Volumes ONTAP系統上建立FlexCache磁碟區。有關詳細步驟和其他注意事項，請參閱以下部分：

- "FlexCache卷實現更快資料存取電源指南"
- "在 System Manager 中建立FlexCache卷"

聚合管理

為Cloud Volumes ONTAP系統建立聚合

您可以自行建立聚合，也可以讓NetApp Console在建立磁碟區時為您建立聚合。自行建立聚合的好處是您可以選擇底層磁碟大小，從而可以根據所需的容量或效能調整聚合的大小。

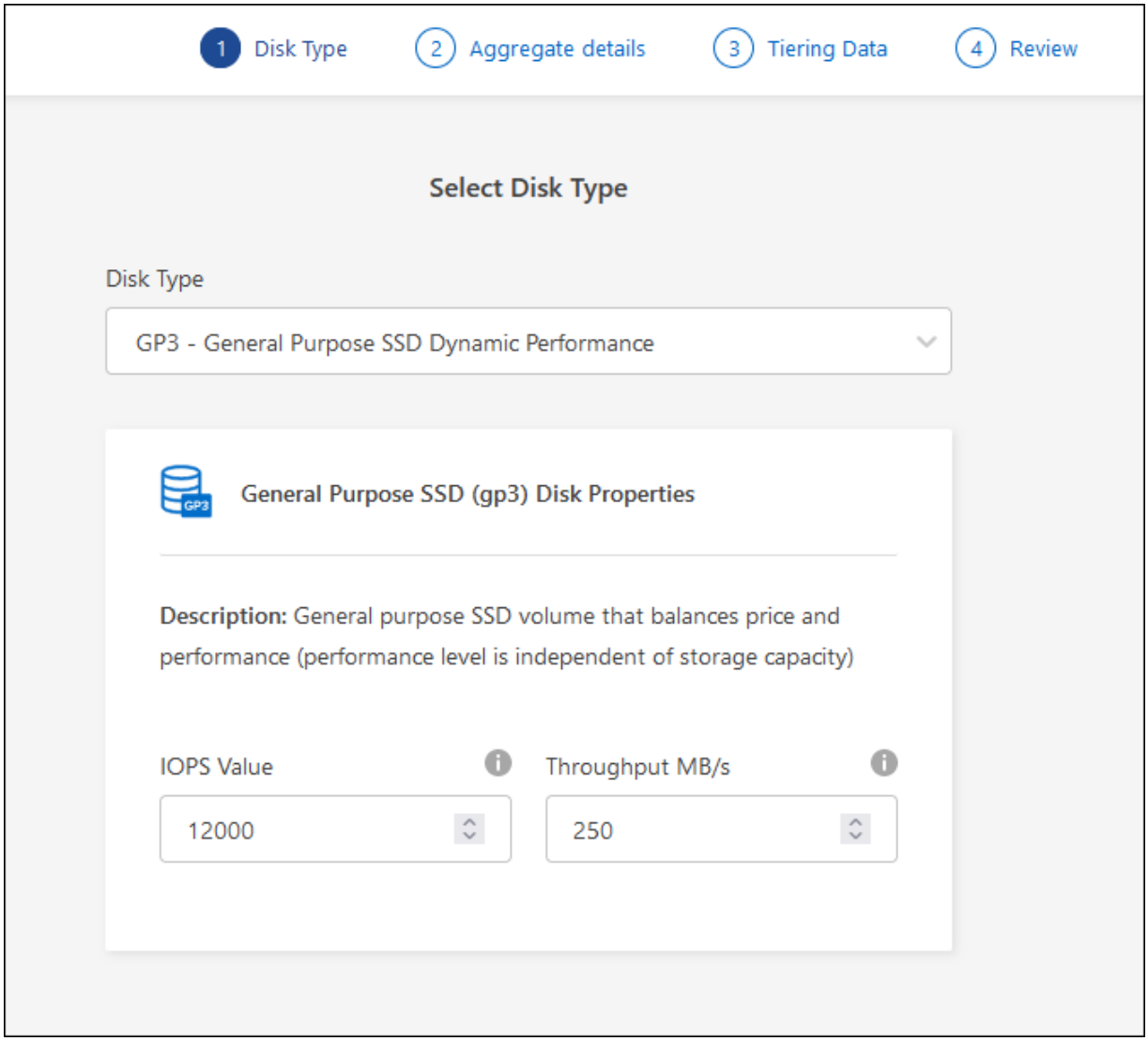
必須直接從控制台建立和刪除所有磁碟和聚合。您不應從其他管理工具執行這些操作。這樣做會影響系統穩定性，妨礙將來添加磁碟的能力，並可能產生冗餘的雲端供應商費用。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在「系統」頁面上，雙擊要管理聚合的Cloud Volumes ONTAP系統的名稱。
3. 在“聚合”標籤上，按一下“新增聚合”，然後指定聚合的詳細資訊。

AWS

- 如果系統提示您選擇磁碟類型和磁碟大小，請參閱"在 AWS 中規劃您的Cloud Volumes ONTAP配置"。
- 如果提示您輸入聚合的容量大小，表示您正在支援 Amazon EBS 彈性磁碟區功能的配置上建立聚合。以下螢幕截圖顯示了由 gp3 磁碟組成的新聚合的範例。



"了解有關彈性卷支持的更多信息"。

Azure

有關磁碟類型和磁碟大小的協助，請參閱"在 Azure 中規劃您的Cloud Volumes ONTAP配置"。

Google雲

有關磁碟類型和磁碟大小的協助，請參閱"在 Google Cloud 中規劃您的Cloud Volumes ONTAP配置"。

4. 按一下“新增”，然後按一下“核准並購買”。

管理Cloud Volumes ONTAP叢集的聚合

透過新增磁碟、查看有關聚合的資訊以及刪除聚合來自行管理聚合。

必須直接從NetApp Console建立和刪除所有磁碟和聚合。您不應從其他管理工具執行這些操作。這樣做會影響系統穩定性，妨礙將來添加磁碟的能力，並可能產生冗餘的雲端供應商費用。

開始之前

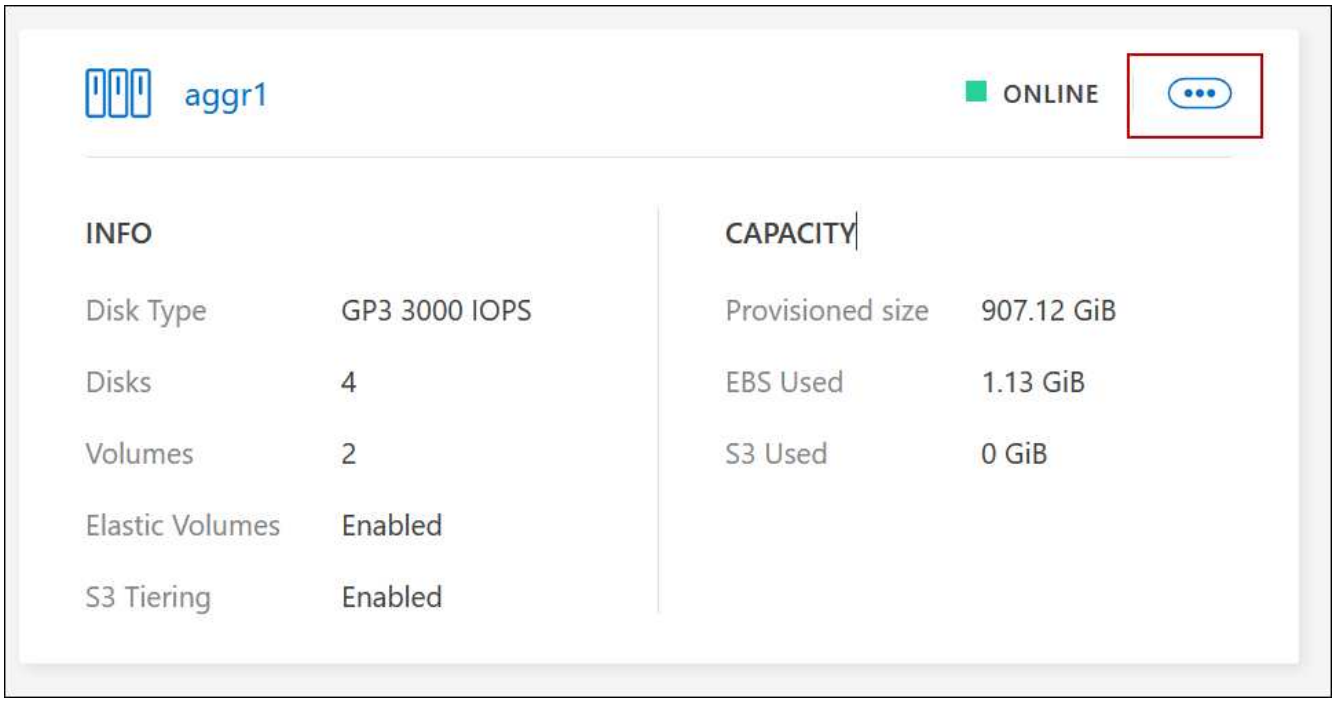
如果要刪除聚合，則必須先刪除聚合中的磁碟區。

關於此任務

如果聚合空間不足，您可以使用ONTAP系統管理員將磁碟區移至另一個聚合。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在「系統」頁面上，雙擊要管理聚合的Cloud Volumes ONTAP系統。
3. 從系統詳細資料中，按一下「聚合」標籤。
4. 對於所需的聚合，按一下 ••• 管理操作的圖示。



5. 透過可用選項管理您的聚合 ••• 菜單。

若要將磁碟新增至聚合，聚合中的所有磁碟必須具有相同的大小。

對於 AWS，您可以增加支援 Amazon EBS 彈性磁碟區的聚合的容量。

1. 根據 ••• 在選單上，點選*增加容量*。
2. 輸入您想要新增的額外容量，然後按一下*增加*。

請注意，您必須將聚合的容量增加至少 256 GiB 或聚合大小的 10%。例如，如果您有 1.77 TiB 聚合，則 10% 就是 181 GiB。這低於 256 GiB，因此聚合的大小必須增加 256 GiB 的最小值。

在控制台代理上管理Cloud Volumes ONTAP聚合容量

每個控制台代理程式都有設定來決定如何管理Cloud Volumes ONTAP的聚合容量。

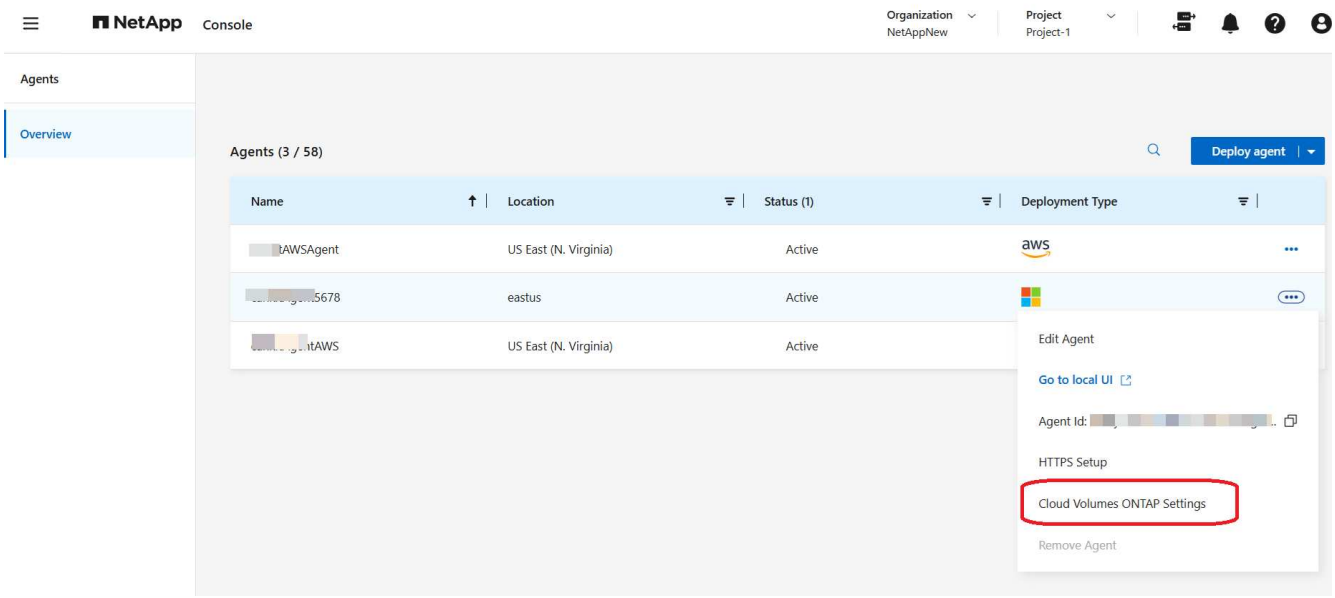
這些設定會影響控制台代理程式管理的所有Cloud Volumes ONTAP系統。如果您有另一個控制台代理，則可以進行不同的配置。

所需權限

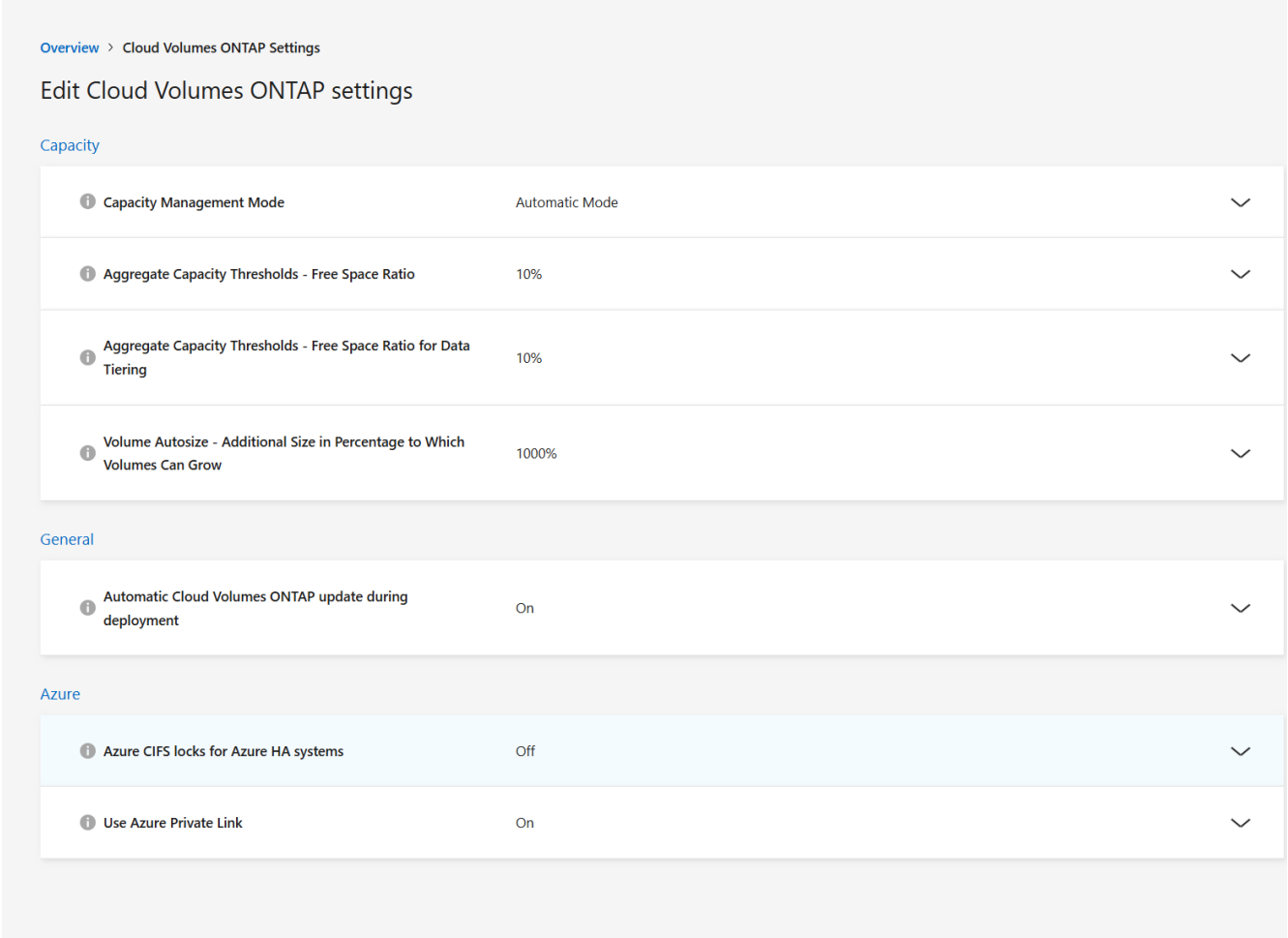
您需要NetApp Console的組織或帳號管理員權限才能修改Cloud Volumes ONTAP設定。

步驟

1. 從左側導覽窗格前往*管理>代理*。
2. 點選 ••• 管理Cloud Volumes ONTAP系統的控制台代理的圖示。
3. 選擇* Cloud Volumes ONTAP設定*。



4. 在「容量」下，修改以下任意設定：



容量管理模式

選擇控制台是否應通知您儲存容量決策，或是否應自動為您管理容量需求。

"了解容量管理模式的工作原理" 。

總容量門檻 - 可用空間比率

此比率是容量管理決策中的關鍵參數，無論您處於自動或手動容量管理模式，了解其影響都至關重要。建議根據您的特定儲存需求和預期成長來設定此閾值，以維持資源利用率和成本之間的平衡。

在手動模式下，如果聚合上的可用空間比率低於指定的閾值，則會觸發通知，提醒您應採取措施解決低可用空間比率問題。監控這些通知並手動管理總容量以避免服務中斷並確保最佳效能非常重要。

可用空間比率計算如下：（聚合容量 - 聚合上的總使用容量）/聚合容量

參考"自動容量管理"現在了解容量在Cloud Volumes ONTAP中自動管理。

聚合容量閾值 - 資料分層的可用空間比率

定義將資料分層到容量層（物件儲存）時效能層（磁碟）上需要多少可用空間。

此比率對於災難復原場景很重要。當從容量層讀取資料時， Cloud Volumes ONTAP會將資料移至效能層以提供更好的效能。如果沒有足夠的空間，那麼Cloud Volumes ONTAP就無法移動資料。

5. 點選“儲存”。

在 Azure 中管理磁碟效能

在 Azure 中管理Cloud Volumes ONTAP的 Premium SSD v2 磁碟效能

您可以透過設定 Premium SSD v2 磁碟的 IOPS 和吞吐量參數來最佳化 Azure 中的Cloud Volumes ONTAP效能。此功能僅在Cloud Volumes ONTAP已部署 Azure Premium SSD v2 磁碟類型時可用，在初始部署期間無法使用。透過提升效能，您可以充分利用 Azure Premium SSD v2 磁碟的靈活性和高效能功能。

Premium SSD v2 磁碟支援需要快速、可靠性能、低延遲、高 IOPS 和高吞吐量的工作負載。透過調整 IOPS 和吞吐量設置，您可以自訂部署中聚合的效能。有關 Premium SSD v2 磁碟的更多信息，請參閱 "部署進階 SSD v2 磁碟"。

使用 API 實作修改 Premium SSD v2 磁碟設定的自動化流程。有關執行Cloud Volumes ONTAP API 呼叫的信息，請參閱 "您的第一次 API 呼叫"。

關於此任務

- 此功能適用於 Azure 單一可用性區域中的Cloud Volumes ONTAP部署。
- 更改磁碟設定會統一改變 RAID 群組或聚合的效能。為了確保整個叢集效能的一致性，叢集中所有磁碟的效能都調整到同一水平。
- 這些變更僅影響單一聚合體，不會影響群組內的其他聚合體。
- 在NetApp Console中部署Cloud Volumes ONTAP或進行容量最佳化時自動配置的高級 SSD v2 磁碟，或透過 API 新增的高級 SSD v2 磁碟，均可進行修改。
- 不支援磁碟調整大小（更改磁碟容量）。

開始之前

在配置 Premium SSD v2 磁碟的 IOPS 和吞吐量參數之前，請注意以下幾點：

- 請確保您僅選擇了進階 SSD v2 資料磁碟。 Premium SSD v1 磁碟或根磁碟和啟動磁碟不符合此變更條件。
- 使用Cloud Volumes ONTAP在部署期間建立的預先配置基線設定作為對應磁碟大小的最小 IOPS 和吞吐量值。這些基準設定與 Premium SSD v1 的效能特點相符。
- 將 IOPS 和吞吐量值設定為等於或高於磁碟大小的最低基準值。例如，對於 1TB 的磁碟大小，將最小 IOPS 值設為 5,000，將最小吞吐量值設為 200 MBps。您可以設定高於這些最小值的值，但不能低於這些最小值。
- 在支援的 Premium SSD v2 範圍內配置值：IOPS 在 3000 到 80000 之間，吞吐量在 125 到 1200 MBps 之間。
- 請確保您的 Premium SSD v2 磁碟大小在 Azure Cloud Volumes ONTAP支援的 500GB 到 32TB 範圍內。請注意，這些大小限制與 Azure 為進階 SSD v2 磁碟提供的最小值和最大值不同。

步驟

- 使用下列 API 呼叫來變更 IOPS 和吞吐量的屬性值：

  在 24 小時內，您最多可以呼叫此 API 四次。

```
PUT /azure/vsa/aggregates/{workingEnvironmentId}/{aggregateName}
```

在請求主體中包含以下參數：

```
{
  "aggregateName": "aggr_name",
  "iops": "modified_iops_value",
  "throughput": "modified_throughput_value",
  "workingEnvironmentId": "we_id"
}
```

完成後

API 回傳回應表示操作成功後，請在 Azure 入口網站中檢查Cloud Volumes ONTAP系統的磁碟詳細信息，以驗證修改後的參數。

相關資訊

- "準備使用 API"
- "Cloud Volumes ONTAP工作流程"
- "取得所需的標識符"
- "使用 REST API 存取Cloud Volumes ONTAP"
- "在可用性集中將 Premium SSD v2 與虛擬機器一起使用"

在 **Azure Cloud Volumes ONTAP**中變更進階 **SSD** 磁碟的效能層級

您可以使用 Azure 入口網站升級 Azure Cloud Volumes ONTAP高階 SSD 託管磁碟的效能層級。這是一個手動過程，涉及將每個高級 SSD 磁碟的磁碟層級變更為更高效能的層級。更改NVRAM磁碟的效能層級可以透過提供更高的 IOPS 和吞吐量能力來幫助緩解效能瓶頸並提高Cloud Volumes ONTAP系統的效率。

請務必與NetApp支援團隊合作，確定您環境中遇到的瓶頸是由於NVRAM磁碟引起的，升級該層級可以解決該問題。

關於此任務

- 預設情況下，Azure 中的Cloud Volumes ONTAP在 P20 層部署高階 SSD 磁碟作為NVRAM 。P20 層級提供平衡的效能，適合大多數工作負載。但是，如果您的工作負載需要更高的效能，您可以將NVRAM磁碟升級到更高的級別，例如 P30。

  目前，您只能透過 Azure 入口網站將NVRAM磁碟從 P20 層升級至 P30 層。

- 您無需更改磁碟大小。容量仍然是 512 GB。此操作只會改變磁碟的效能等級。

開始之前

- 仔細評估是否有必要進行此項更改，因為將NVRAM磁碟升級到更高效能等級會產生額外的成本。
- 您的Cloud Volumes ONTAP版本必須為 9.11.1 或更高版本。對於較低版本，您可以升級到 9.11.1 或更高版本，或向NetApp支援部門提出功能策略變更請求 (FPVR)。

步驟

此場景假設有兩個節點 `node01` 和 `node02` 在Cloud Volumes ONTAP高可用性 (HA) 部署中。使用 Azure 入口網站升級層級。

1. 運行此命令以進行 `node1` 活動節點。手動故障轉移 `node02`。

   ```
   storage failover takeover -ofnode <Node02>
   ```

2. Sign inAzure 入口網站。
3. 接管完成後，請前往虛擬機器實例。 `node02`然後點擊“停止”按鈕將其關閉。
4. 導航至資源組 `node02` 從磁碟清單中選擇NVRAM磁碟以變更層級。
5. 選擇*尺寸+性能*。
6. 在「效能等級」下拉式選單中，選擇 `P30 - 5000 IOPS, 200MB/s`。
7. 選擇*調整大小*。
8. 打開 `node02` 實例。
9. 檢查 Azure 序列控制台，直到看到以下訊息： `waiting for giveback`。
10. 執行此命令即可回饋 `node02`：

    ```
    storage failover giveback -ofnode <Node02>
    ```

11. 重複這些步驟 `node01` 製作 `node02` 接管 `node01`這樣您就可以升級NVRAM磁碟層。 `node01`。

完成後

當您啟動兩個節點後，請在 Azure 入口網站中檢查Cloud Volumes ONTAP系統的磁碟詳細信息，以驗證修改後的參數。

相關資訊

- Azure 文件： "無需停機即可更改性能等級"
- 支援團隊知識庫： "如何在 Azure CVO 升級NVRAM磁碟的效能層"
- "升級Cloud Volumes ONTAP軟體版本"

儲存虛擬機器管理

管理Cloud Volumes ONTAP 的儲存虛擬機

儲存虛擬機是在ONTAP內運作的虛擬機，可為您的用戶端提供儲存和資料服務。您可能知道這是一個_SVM_或_vserver_。 Cloud Volumes ONTAP預設配置一個儲存虛擬機，但某些配置支援額外的儲存虛擬機。

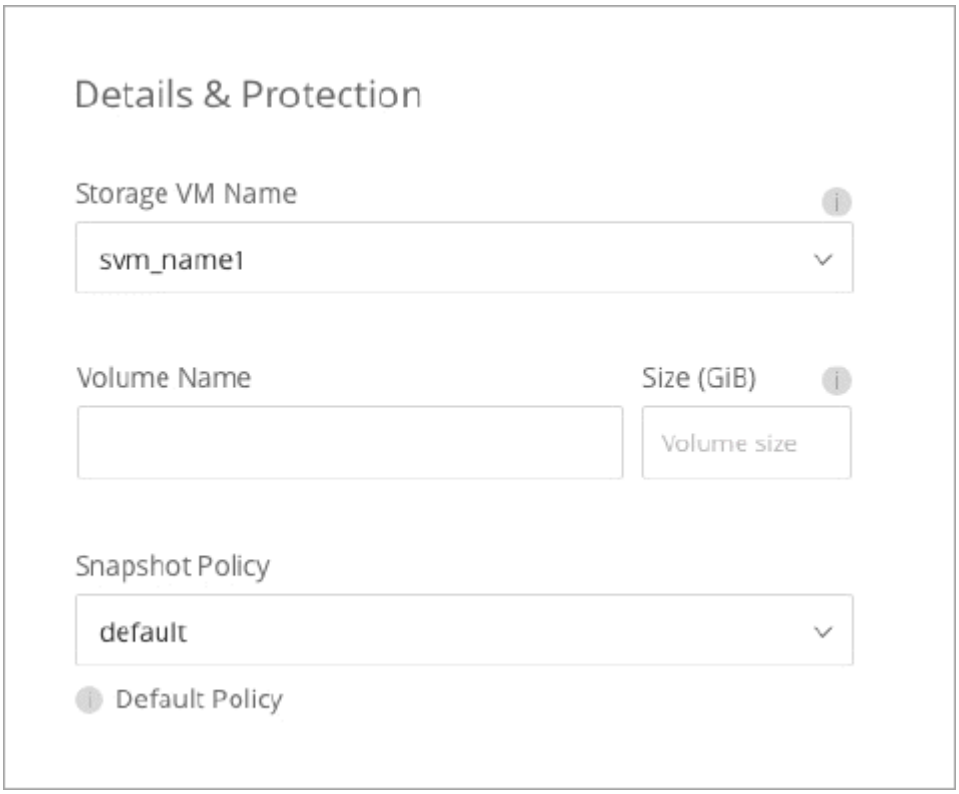
支援的儲存虛擬機器數量

特定配置支援多個儲存虛擬機器。前往 "Cloud Volumes ONTAP發行說明"驗證您的Cloud Volumes ONTAP版本支援的儲存虛擬機器數量。

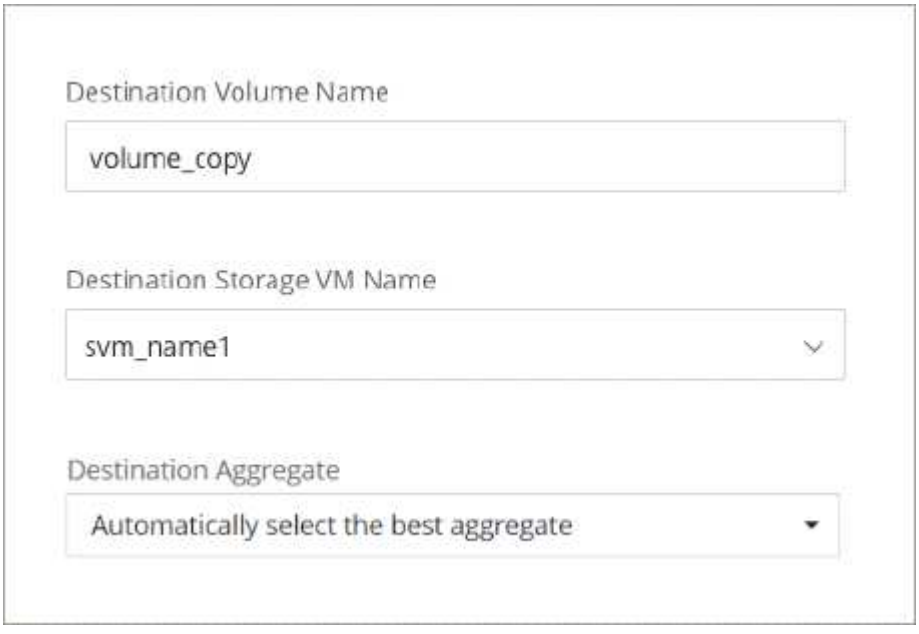
使用多個儲存虛擬機

NetApp Console支援您從ONTAP系統管理員或ONTAP CLI 建立的任何其他儲存虛擬機器。

例如，下圖顯示如何在建立磁碟區時選擇儲存虛擬機器。



下圖顯示了將磁碟區複製到另一個系統時如何選擇儲存虛擬機器。



修改預設儲存虛擬機器的名稱

控制台會自動命名其為Cloud Volumes ONTAP所建立的單一儲存虛擬機器。如果您有嚴格的命名標準，則可以

從ONTAP系統管理員、 ONTAP CLI 或 API 修改儲存虛擬機器的名稱。例如，您可能希望該名稱與ONTAP叢集的儲存虛擬機器的命名方式相符。

管理 **AWS** 中**Cloud Volumes ONTAP**的資料服務儲存虛擬機

儲存虛擬機是在ONTAP內運作的虛擬機，可為您的用戶端提供儲存和資料服務。您可能知道這是一個_SVM_或_vserver_。 Cloud Volumes ONTAP預設配置一個儲存虛擬機，但某些配置支援額外的儲存虛擬機。

若要建立額外的資料服務儲存虛擬機，您需要在 AWS 中指派 IP 位址，然後根據您的Cloud Volumes ONTAP設定執行ONTAP命令。

支援的儲存虛擬機器數量

從 9.7 版本開始，特定的Cloud Volumes ONTAP配置支援多個儲存虛擬機器。前往 "Cloud Volumes ONTAP發行說明"驗證您的Cloud Volumes ONTAP版本支援的儲存虛擬機器數量。

所有其他Cloud Volumes ONTAP配置都支援一個資料服務儲存虛擬機器和一個用於災難復原的目標儲存虛擬機器。如果來源儲存虛擬機器發生中斷，您可以啟動目標儲存虛擬機器進行資料存取。

驗證配置的限制

每個 EC2 執行個體支援每個網路介面的最大私有 IPv4 位址數量。在 AWS 中為新的儲存虛擬機器指派 IP 位址之前，您需要驗證限制。

步驟

1. 去 "Cloud Volumes ONTAP發行說明中的儲存限制部分"。
2. 確定您的執行個體類型每個介面的最大 IP 位址數。
3. 記下這個號碼，因為在下一節中分配 AWS 中的 IP 位址時需要它。

在 **AWS** 中分配 **IP** 位址

在為新的儲存虛擬機器建立 LIF 之前，必須將私人 IPv4 位址指派給 AWS 中的連接埠 e0a。

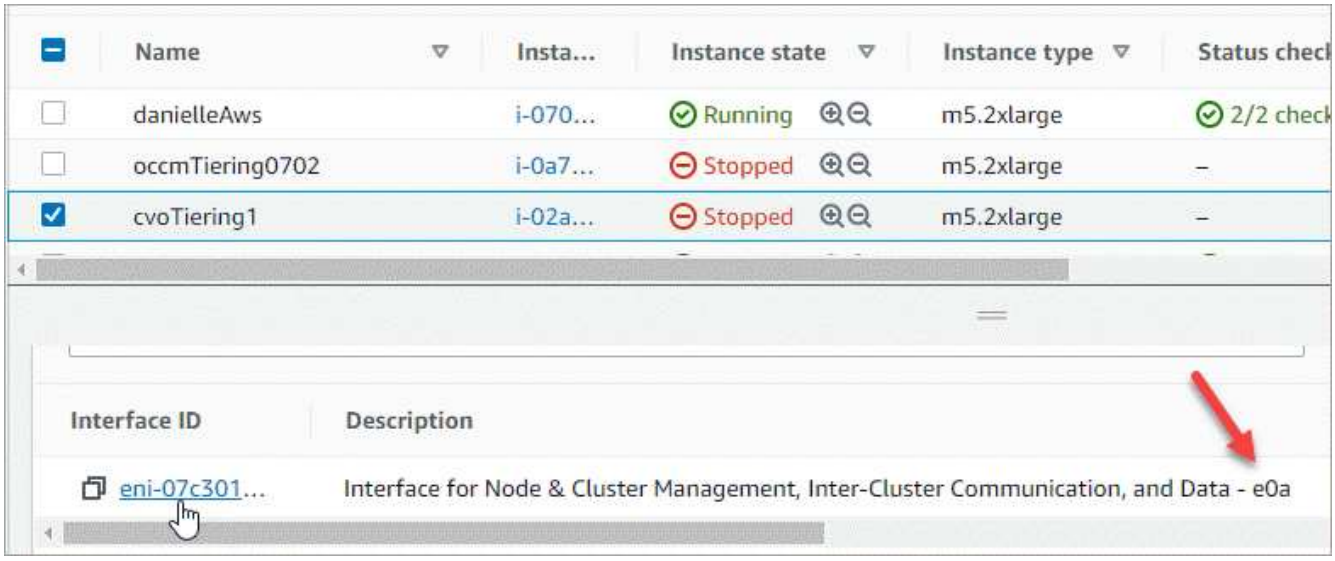
請注意，儲存虛擬機器的選用管理 LIF 需要在單節點系統和單一可用區（AZ）中的高可用性（HA）對上指派私人 IP 位址。此管理 LIF 提供與管理工具（例如 SnapCenter）的連結。

步驟

1. 登入AWS並開啟EC2服務。
2. 選擇Cloud Volumes ONTAP實例並點選 網路。

   如果您要在 HA 對上建立儲存虛擬機，請選擇節點 1。

3. 向下捲動至*網路介面*並點選連接埠 e0a 的*介面 ID*。



4. 選擇網路介面並點選*操作>管理 IP 位址*。
5. 展開 e0a 的 IP 位址清單。
6. 驗證 IP 位址：
   a. 計算已指派的 IP 位址數量，以確認連接埠是否有空間容納額外的 IP。

      您應該已經在本頁的上一節中確定了每個介面支援的最大 IP 位址數量。

   b. 可選：前往Cloud Volumes ONTAP的ONTAP CLI 並執行 **network interface show** 以確認每個 IP 位址都在使用中。

      如果 IP 位址未使用，那麼您可以將其與新的儲存 VM 一起使用。

7. 返回 AWS 控制台，按一下「指派新 IP 位址」以根據新儲存 VM 所需的數量指派其他 IP 位址。
   - 單節點系統：需要一個未使用的次要私有 IP。

     如果您想在儲存虛擬機器上建立管理 LIF，則需要選購的輔助私人 IP。

   - 單一 AZ 中的 HA 對：節點 1 上需要一個未使用的輔助私有 IP。

     如果您想在儲存虛擬機器上建立管理 LIF，則需要選購的輔助私人 IP。

   - 多個可用區中的 HA 對：每個節點都需要一個未使用的輔助私有 IP。
8. 如果您要在單一 AZ 中的 HA 對上指派 IP 位址，請啟用*允許重新指派輔助私有 IPv4 位址*。
9. 點選“儲存”。
10. 如果您在多個可用區中有一個 HA 對，則需要對節點 2 重複這些步驟。

在單節點系統上建立儲存 **VM**

這些步驟會在單節點系統上建立新的儲存 VM。建立 NAS LIF 需要一個私有 IP 位址，如果您要建立管理 LIF，則需要另一個選用的私有 IP 位址。

步驟

1. 建立儲存虛擬機器和到儲存虛擬機器的路由。

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. 建立 NAS LIF。

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node
```

其中 *private_ip_x* 是 e0a 上未使用的輔助私有 IP。

3. 可選：建立儲存虛擬機器管理 LIF。

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

其中 *private_ip_y* 是 e0a 上另一個未使用的輔助私有 IP。

4. 將一個或多個聚合分配給儲存虛擬機器。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

此步驟是必需的，因為新的儲存虛擬機器需要存取至少一個聚合，然後您才能在儲存虛擬機器上建立磁碟區。

在單一可用區內的 **HA** 對上建立儲存虛擬機

這些步驟在單一 AZ 中的 HA 對上建立一個新的儲存虛擬機器。建立 NAS LIF 需要一個私人 IP 位址，如果要建立管理 LIF，則需要另一個可選的私人 IP 位址。

這兩個 LIF 都分配在節點 1 上。如果發生故障，私人 IP 位址可以在節點之間移動。

步驟

1. 建立儲存虛擬機器和到儲存虛擬機器的路由。

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. 在節點 1 上建立 NAS LIF。

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

其中 *private_ip_x* 是 cvo-node1 的 e0a 上未使用的輔助私有 IP。在接管的情況下，該 IP 位址可以重新定位到 cvo-node2 的 e0a，因為服務策略 default-data-files 表示 IP 可以遷移到合作夥伴節點。

3. 選用：在節點 1 上建立儲存虛擬機器管理 LIF。

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

其中 *private_ip_y* 是 e0a 上另一個未使用的輔助私有 IP。

4. 將一個或多個聚合分配給儲存虛擬機器。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

此步驟是必需的，因為新的儲存虛擬機器需要存取至少一個聚合，然後您才能在儲存虛擬機器上建立磁碟區。

5. 如果您使用的是Cloud Volumes ONTAP 9.11.1 或更高版本，請修改儲存虛擬機器的網路服務策略。

需要修改服務，因為它可以確保Cloud Volumes ONTAP可以使用 iSCSI LIF 進行出站管理連線。

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

在多個可用區的 **HA** 對上建立儲存虛擬機

這些步驟在多個 AZ 中的 HA 對上建立一個新的儲存虛擬機器。

對於 NAS LIF 來說，浮動 IP 位址是必需的，而對於管理 LIF 來說，浮動 IP 位址是可選的。這些浮動 IP 位址不需要您在 AWS 中指派私有 IP。相反，浮動 IP 會在 AWS 路由表中自動配置為指向相同 VPC 中特定節點的 ENI。

為了使浮動 IP 與ONTAP一起運作，必須在每個節點上的每個儲存虛擬機器上配置一個私人 IP 位址。這反映在以下步驟中，其中在節點 1 和節點 2 上建立 iSCSI LIF。

步驟

1. 建立儲存虛擬機器和到儲存虛擬機器的路由。

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. 在節點 1 上建立 NAS LIF。

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

   - 浮動 IP 位址必須位於您部署 HA 配置的 AWS 區域中的所有 VPC 的 CIDR 區塊之外。 192.168.209.27 是一個範例浮動 IP 位址。"了解有關選擇浮動 IP 位址的更多信息" 。
   - `-service-policy default-data-files`表示 IP 可以遷移到夥伴節點。

3. 選用：在節點 1 上建立儲存虛擬機器管理 LIF。

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

4. 在節點 1 上建立 iSCSI LIF。

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmask nodei1Mask -lif
ip_node1_iscsi_2 -home-node cvo-node1
```

   - 此 iSCSI LIF 需要支援儲存虛擬機器中浮動 IP 的 LIF 遷移。它不必是 iSCSI LIF，但不能配置為在節點之間遷移。
   - `-service-policy default-data-block`表示IP位址不會在節點之間遷移。
   - *private_ip* 是 cvo_node1 的 eth0 (e0a) 上未使用的輔助私有 IP 位址。

5. 在節點 2 上建立 iSCSI LIF。

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif
ip_node2_iscsi_2 -home-node cvo-node2
```

   - 此 iSCSI LIF 需要支援儲存虛擬機器中浮動 IP 的 LIF 遷移。它不必是 iSCSI LIF，但不能配置為在節點

之間遷移。

- `-service-policy default-data-block`表示IP位址不會在節點之間遷移。
- *private_ip* 是 cvo_node2 的 eth0 (e0a) 上未使用的輔助私有 IP 位址。

6. 將一個或多個聚合分配給儲存虛擬機器。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

此步驟是必需的，因為新的儲存虛擬機器需要存取至少一個聚合，然後您才能在儲存虛擬機器上建立磁碟區。

7. 如果您使用的是Cloud Volumes ONTAP 9.11.1 或更高版本，請修改儲存虛擬機器的網路服務策略。

需要修改服務，因為它可以確保Cloud Volumes ONTAP可以使用 iSCSI LIF 進行出站管理連線。

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

在 Azure 中管理Cloud Volumes ONTAP的資料服務儲存虛擬機

儲存虛擬機是在ONTAP內運作的虛擬機，可為您的用戶端提供儲存和資料服務。您可能知道這是一個_SVM_或_vserver_。 Cloud Volumes ONTAP預設為儲存虛擬機，但您可以在 Azure 中執行Cloud Volumes ONTAP時建立其他儲存虛擬機器。

若要在 Azure 中建立和管理其他資料服務儲存虛擬機，您應該使用 API。這是因為 API 自動化了建立儲存虛擬機器和配置所需網路介面的過程。建立儲存虛擬機器時， NetApp Console會配置所需的 LIF 服務，以及儲存虛擬機器出站 SMB/CIFS 通訊所需的 iSCSI LIF。

有關執行Cloud Volumes ONTAP API 呼叫的信息，請參閱 "您的第一次 API 呼叫"。

支援的儲存虛擬機器數量

從Cloud Volumes ONTAP 9.9.0 開始，根據您的許可證，支援具有特定配置的多個儲存虛擬機器。請參閱 "Cloud Volumes ONTAP發行說明"驗證您的Cloud Volumes ONTAP版本支援的儲存虛擬機器數量。

9.9.0 之前的所有Cloud Volumes ONTAP版本都支援一個資料服務儲存虛擬機器和一個用於災難復原的目標儲存虛擬機器。如果來源儲存虛擬機器發生中斷，您可以啟動目標儲存虛擬機器進行資料存取。

建立儲存虛擬機

根據您的設定和授權類型，您可以透過 NetApp Console 的 API，在單一節點系統或高可用性（HA）組態中建立多個儲存 VM。

關於此任務

當您使用 API 建立儲存虛擬機器並配置所需的網路介面時，控制台也會修改 `default-data-files`透過從 NAS 資料 LIF 中刪除以下服務並將其新增至用於出站管理連線的 iSCSI 資料 LIF，可以在資料儲存虛擬機器上實施策略：

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

開始之前

控制台代理程式需要特定權限才能為Cloud Volumes ONTAP建立儲存虛擬機器。所需權限包含在 "NetApp提供的政策"。

單節點系統

使用下列 API 呼叫在單節點系統上建立儲存 VM。

```
POST /azure/vsa/working-environments/{workingEnvironmentId}/svm
```

在請求主體中包含以下參數：

```
{ "svmName": "myNewSvm1"
   "svmPassword": "optional, the API takes the cluster password if not
provided"
   "mgmtLif": "optional, to create an additional management LIF, if you
want to use the storage VM for management purposes"}
```

HA 對

使用以下 API 呼叫在 HA 對上建立儲存虛擬機器：

```
POST /azure/ha/working-environments/{workingEnvironmentId}/svm
```

在請求主體中包含以下參數：

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
   "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

管理單節點系統和 HA 配對上的儲存 VM

使用 API，您可以重新命名和刪除單節點和 HA 配置中的儲存虛擬機器。

開始之前

控制台代理程式需要特定權限來管理Cloud Volumes ONTAP 的儲存虛擬機器。所需權限包含在 "NetApp提供的政策"。

重新命名儲存虛擬機

若要重新命名儲存虛擬機，您應該提供現有儲存虛擬機和新儲存虛擬機的名稱作為參數。

步驟

- 使用下列 API 呼叫重新命名單節點系統上的儲存 VM：

  ```
  PUT /azure/vsa/working-environments/{workingEnvironmentId}/svm
  ```

  在請求主體中包含以下參數：

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

- 使用以下 API 呼叫重命名 HA 對上的儲存虛擬機器：

```
PUT /azure/ha/working-environments/{workingEnvironmentId}/svm
```

在請求主體中包含以下參數：

```
{
  "svmNewName": "NewSvmName",
  "svmName": "OldSvmName"
}
```

刪除儲存虛擬機

在單一節點或 HA 配置中，如果儲存虛擬機器沒有任何活動卷，則可以將其刪除。

步驟

- 使用以下 API 呼叫刪除單節點系統上的儲存 VM ：

  ```
  DELETE /azure/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
  ```

- 使用以下 API 呼叫刪除 HA 對上的儲存虛擬機器：

  ```
  DELETE /azure/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
  ```

相關資訊

- "準備使用 API"
- "Cloud Volumes ONTAP工作流程"
- "取得所需的標識符"
- "使用NetApp Console的 REST API"

在 Google Cloud 中管理Cloud Volumes ONTAP的資料服務儲存虛擬機

儲存虛擬機是在ONTAP內運作的虛擬機，可為您的用戶端提供儲存和資料服務。您可能知道這是一個_SVM_或_vserver_。 Cloud Volumes ONTAP預設配置一個儲存虛擬機，但某些配置支援額外的儲存虛擬機。

要在 Google Cloud 中建立和管理其他資料服務儲存虛擬機，您應該使用 API。這是因為 API 自動化了建立儲存虛擬機器和配置所需網路介面的過程。建立儲存虛擬機器時， NetApp Console會配置所需的 LIF 服務，以及儲存虛擬機器出站 SMB/CIFS 通訊所需的 iSCSI LIF。

有關執行Cloud Volumes ONTAP API 呼叫的信息，請參閱 "您的第一次 API 呼叫"。

支援的儲存虛擬機器數量

從Cloud Volumes ONTAP 9.11.1 開始，根據您的許可證，支援具有特定配置的多個儲存虛擬機器。請參閱 "Cloud Volumes ONTAP發行說明"驗證您的Cloud Volumes ONTAP版本支援的儲存虛擬機器數量。

9.11.1 之前的所有Cloud Volumes ONTAP版本都支援一個資料服務儲存虛擬機器和一個用於災難復原的目標儲

存虛擬機器。如果來源儲存虛擬機器發生中斷，您可以啟動目標儲存虛擬機器進行資料存取。

建立儲存虛擬機

根據您的組態和授權類型，您可以使用 API 在單節點系統或高可用性 （HA） 組態中建立多個儲存 VM。

關於此任務

當您使用 API 建立儲存虛擬機器並配置所需的網路介面時，控制台也會修改 `default-data-files`透過從 NAS 資料 LIF 中刪除以下服務並將其新增至用於出站管理連線的 iSCSI 資料 LIF，可以在資料儲存虛擬機器上實施策略：

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

開始之前

控制台代理程式需要特定權限才能為Cloud Volumes ONTAP HA 對建立儲存虛擬機器。所需的權限包含在... "NetApp提供的政策" 。

單節點系統

使用下列 API 呼叫在單節點系統上建立儲存 VM。

```
POST /gcp/vsa/working-environments/{workingEnvironmentId}/svm
```

在請求主體中包含以下參數：

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
   "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

HA 對

使用以下 API 呼叫在 HA 對上建立儲存虛擬機器：

```
POST /gcp/ha/working-environments/{workingEnvironmentId}/svm/
```

在請求主體中包含以下參數：

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
}
```

管理儲存虛擬機

使用 API，您可以重新命名和刪除單節點和 HA 配置中的儲存虛擬機器。

開始之前

控制台代理程式需要特定權限來管理Cloud Volumes ONTAP HA 對的儲存虛擬機器。所需的權限包含在... "NetApp提供的政策" 。

重新命名儲存虛擬機

若要重新命名儲存虛擬機，您應該提供現有儲存虛擬機和新儲存虛擬機的名稱作為參數。

步驟

- 使用下列 API 呼叫重新命名單節點系統上的儲存 VM：

  `PUT /gcp/vsa/working-environments/{workingEnvironmentId}/svm`

  在請求主體中包含以下參數：

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

- 使用以下 API 呼叫重命名 HA 對上的儲存虛擬機器：

  `PUT /gcp/ha/working-environments/{workingEnvironmentId}/svm`

  在請求主體中包含以下參數：

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

刪除儲存虛擬機

在單一節點或 HA 配置中，如果儲存虛擬機器沒有任何活動卷，則可以將其刪除。

步驟

- 使用以下 API 呼叫刪除單節點系統上的儲存 VM ：

```
DELETE /gcp/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
```

- 使用以下 API 呼叫刪除 HA 對上的儲存虛擬機器：

```
DELETE /gcp/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
```

相關資訊

- "準備使用 API"
- "Cloud Volumes ONTAP工作流程"
- "取得所需的標識符"
- "使用NetApp Console的 REST API"

為Cloud Volumes ONTAP設定儲存虛擬機器災難復原

NetApp Console不提供儲存虛擬機器 (SVM) 災難復原的設定或編排支援。若要執行這些任務，請使用ONTAP System Manager 或ONTAP CLI。

如果要在兩個 Cloud Volumes ONTAP 系統之間設定 SnapMirror SVM 複製，則複製必須在兩個 HA 配對系統或兩個單節點系統之間進行。您無法在 HA 配對系統和單節點系統之間設定 SnapMirror SVM 複製。

有關ONTAP CLI 說明，請參閱以下文件。

- "SVM 災難復原準備快速指南"
- "SVM 災難復原快速指南"

安全性和資料加密

使用NetApp加密解決方案加密Cloud Volumes ONTAP上的捲

Cloud Volumes ONTAP支援NetApp磁碟區加密 (NVE) 和NetApp聚合加密 (NAE)。 NVE 和 NAE 是基於軟體的解決方案，可實現符合 FIPS 140-2 標準的捲靜態資料加密。"了解有關這些加密解決方案的更多信息" 。

NVE 和 NAE 均由外部金鑰管理器支援。

如果def::aws[] endif::aws[] 如果def::azure[] endif::azure[] 如果def::gcp[] endif::gcp[] 如果def::aws[] endif::aws[] 如果def::azure[] endif::azure[] 如果你::gcp[] defendiffcp[]

使用 AWS 金鑰管理服務管理Cloud Volumes ONTAP加密金鑰

您可以使用"AWS 的金鑰管理服務 (KMS)"在 AWS 部署的應用程式中保護您的ONTAP加密金鑰。

可以使用 CLI 或ONTAP REST API 啟用 AWS KMS 的金鑰管理。

使用 KMS 時，請注意預設使用資料 SVM 的 LIF 與雲端金鑰管理端點進行通訊。節點管理網路用於與 AWS 的身份驗證服務進行通訊。如果叢集網路配置不正確，叢集將無法正確利用金鑰管理服務。

開始之前

- Cloud Volumes ONTAP必須運作 9.12.0 或更高版本
- 您必須已安裝磁碟區加密 (VE) 許可證，並且
- 您必須已安裝多租用戶加密金鑰管理 (MTEKM) 授權。
- 您必須是叢集或 SVM 管理員
- 您必須擁有有效的 AWS 訂閱

您只能為資料 SVM 配置金鑰。

配置

AWS

1. 您必須創建一個"授予"用於管理加密的 IAM 角色將使用的 AWS KMS 金鑰。 IAM 角色必須包含允許以下操作的策略：
   - `DescribeKey`
   - `Encrypt`
   - `Decrypt`若要建立贈款，請參閱"AWS 文件"。
2. "為適當的 IAM 角色新增策略。"政策應該支持 `DescribeKey`， `Encrypt` ，和 `Decrypt`營運.

Cloud Volumes ONTAP

1. 切換到您的Cloud Volumes ONTAP環境。
2. 切換到進階權限等級：
   `set -privilege advanced`
3. 啟用 AWS 金鑰管理員：
   `security key-manager external aws enable -vserver data_svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. 出現提示時，輸入金鑰。
5. 確認 AWS KMS 已正確配置：
   `security key-manager external aws show -vserver svm_name`

使用 **Azure Key Vault** 管理**Cloud Volumes ONTAP**加密金鑰

您可以使用 Azure Key Vault (AKV) 來保護 Azure 部署的應用程式中ONTAP加密金鑰。請參閱"Microsoft 文件"。

AKV 僅可用於保護資料 SVM 的NetApp磁碟區加密 (NVE) 金鑰。欲了解更多信息，請參閱"ONTAP文檔" 。

可以使用 CLI 或ONTAP REST API 啟用 AKV 金鑰管理。

使用 AKV 時，請注意預設使用資料 SVM LIF 與雲端金鑰管理端點通訊。節點管理網路用於與雲端提供者的身份驗證服務（login.microsoftonline.com）進行通訊。如果叢集網路配置不正確，叢集將無法正確利用金鑰管理服

務。

開始之前

- Cloud Volumes ONTAP必須運作 9.10.1 或更高版本
- 已安裝磁碟區加密 (VE) 授權（NetApp磁碟區加密許可證會自動安裝在每個在NetApp支援中註冊的Cloud Volumes ONTAP系統上）
- 您必須擁有多租戶加密金鑰管理 (MT_EK_MGMT) 許可證
- 您必須是叢集或 SVM 管理員
- 有效的 Azure 訂閱

限制

- AKV 只能在資料 SVM 上配置
- NAE 不能與 AKV 一起使用。 NAE 需要外部支援的 KMIP 伺服器。
- Cloud Volumes ONTAP節點每 15 分鐘輪詢一次 AKV，以確認可存取性和金鑰可用性。此輪詢週期是不可設定的，並且在輪詢嘗試連續四次失敗後（總共 1 小時），磁碟區將處於離線狀態。

配置過程

概述的步驟擷取如何向 Azure 註冊您的Cloud Volumes ONTAP配置以及如何建立 Azure Key Vault 和金鑰。如果您已經完成這些步驟，請確保您具有正確的配置設置，特別是在建立 Azure Key Vault，然後繼續Cloud Volumes ONTAP配置。

- Azure 應用程式註冊
- 建立 Azure 用戶端機密
- 建立 Azure Key Vault
- 建立加密金鑰
- 建立 Azure Active Directory 端點（僅限 HA）
- Cloud Volumes ONTAP配置

Azure 應用程式註冊

1. 您必須先在 Azure 訂閱中註冊您希望Cloud Volumes ONTAP用於存取 Azure Key Vault 的應用程式。在 Azure 入口網站中，選擇套用註冊。
2. 選擇新註冊。
3. 為您的應用程式提供名稱並選擇支援的應用程式類型。預設的單一租戶足以滿足 Azure Key Vault 的使用。選擇註冊。
4. 在 Azure 概覽視窗中，選擇已註冊的應用程式。將應用程式（客戶端）**ID**和目錄（租用戶）**ID**複製到安全位置。在稍後的註冊過程中將需要它們。

建立 **Azure** 用戶端機密

1. 在 Azure Key Vault 應用程式註冊的 Azure 入口網站中，選擇「憑證和機密」窗格。
2. 選擇新客戶端密鑰。為您的客戶端密鑰輸入一個有意義的名稱。 NetApp建議的有效期限為 24 個月；但是，您的特定雲端治理策略可能需要不同的設定。
3. 按一下新增以建立客戶端金鑰。複製值列中列出的秘密字串，並將其儲存在安全的位置，以便稍後使

用Cloud Volumes ONTAP配置。當您離開該頁面後，秘密值將不再顯示。

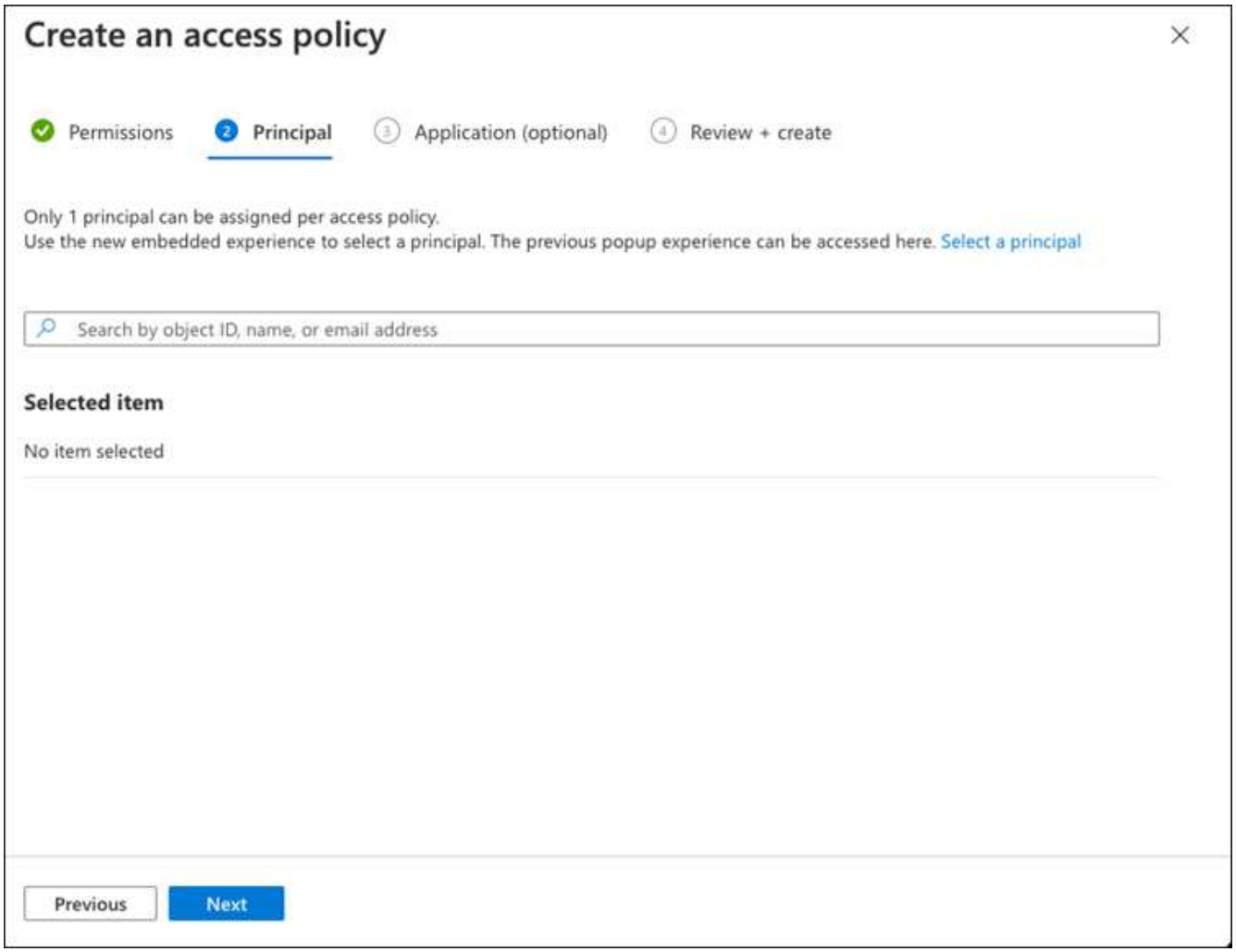
建立 **Azure Key Vault**

1. 如果您有現有的 Azure Key Vault，則可以將其連接到Cloud Volumes ONTAP配置；但是，您必須根據此過程中的設定調整存取原則。
2. 在 Azure 入口網站中，導覽至 **Key Vaults** 部分。
3. 點擊「+建立」並輸入所需信息，包括資源組、區域和定價層。此外，輸入保留已刪除保管庫的天數，並在金鑰保管庫上選擇啟用清除保護。
4. 選擇下一步來選擇存取策略。
5. 選擇以下選項：
   a. 在存取配置下，選擇**Vault** 訪問策略。
   b. 在資源存取下，選擇**Azure** 磁碟加密進行磁碟區加密。
6. 選擇“+建立”以新增存取策略。
7. 在從範本配置下，按一下下拉式選單，然後選擇金鑰、機密和憑證管理範本。
8. 選擇每個下拉權限選單（金鑰、秘密、憑證），然後在選單清單頂部選擇全選以選擇所有可用的權限。您應該：
   - 關鍵權限：已選擇 20 個
   - 秘密權限：已選擇 8 個
   - 憑證權限：已選擇 16 個


Create an access policy
1 Permissions
2 Principal
3 Application (optional)
4 Review + create
Configure from a template
Key, Secret, & Certificate Management
Key permissions
Key Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Cryptographic Operations
Select all
Decrypt
Encrypt
Unwrap Key
Wrap Key
Verify
Sign
Privileged Key Operations
Select all
Purge
Release
Rotation Policy Operations
Select all
Rotate
Get Rotation Policy
Set Rotation Policy
Secret permissions
Secret Management Operations
Select all
Get
List
Set
Delete
Recover
Backup
Restore
Privileged Secret Operations
Select all
Purge
Certificate permissions
Certificate Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Manage Contacts
Manage Certificate Authorities
Get Certificate Authorities
List Certificate Authorities
Set Certificate Authorities
Delete Certificate Authorities
Privileged Certificate Operations
Select all
Purge
Previous
Next

9. 按一下下一步，選擇您在 Azure 中建立的主體註冊應用程式Azure 應用程式註冊。選擇下一步。

   每個策略只能分配一個主體。



10. 按一下下一步兩次，直到到達審核並建立。然後，按一下建立。
11. 選擇下一步進入網路選項。
12. 選擇適當的網路存取方法或選擇所有網路和檢視 **+** 建立來建立金鑰保管庫。 （網路存取方法可能由治理策略或您的企業雲端安全團隊規定。）
13. 記錄金鑰保管庫 URI：在您建立的金鑰保管庫中，導覽至概覽功能表並從右側列複製**Vault URI**。您需要它來完成後面的步驟。

建立加密金鑰

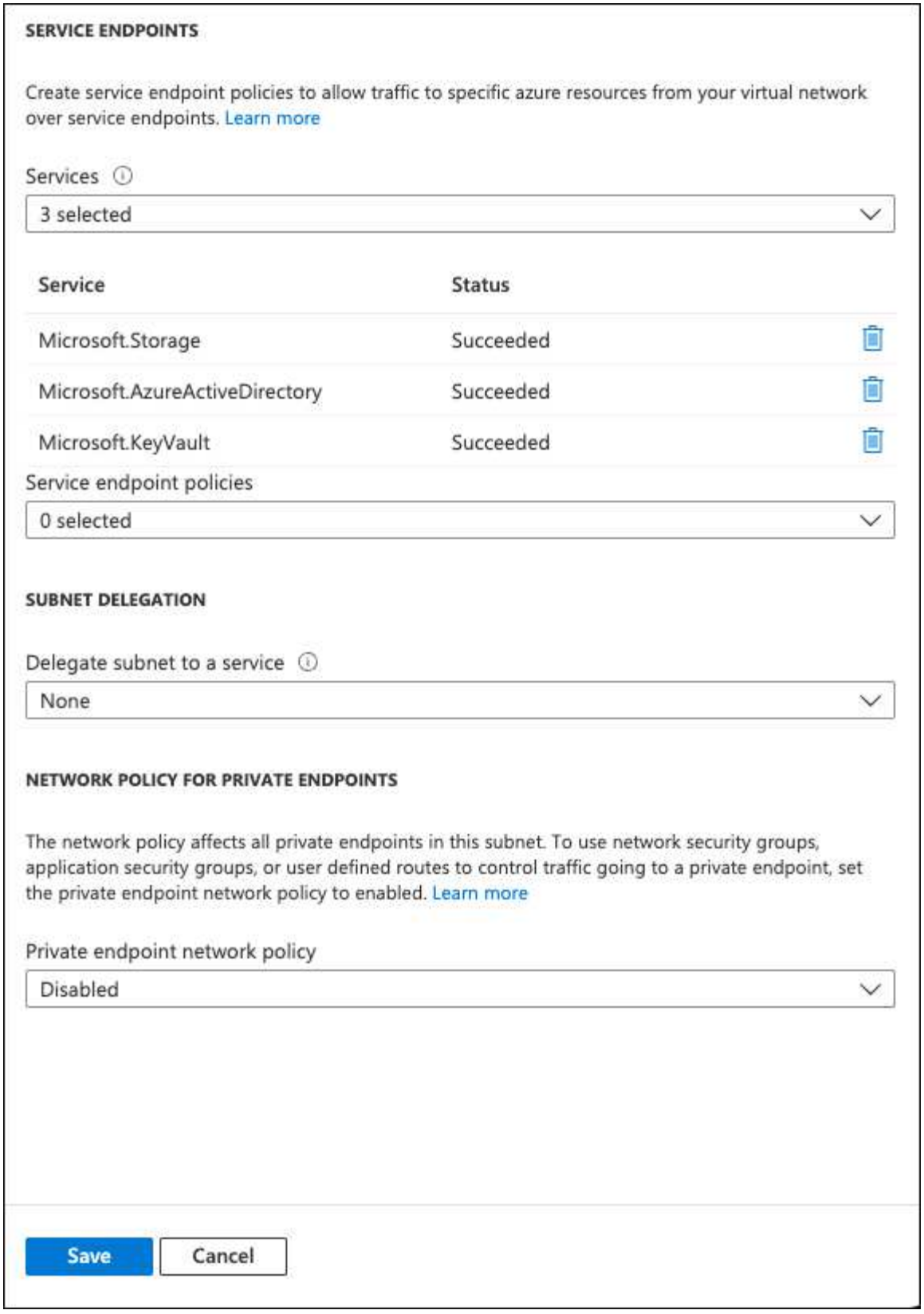
1. 在您為Cloud Volumes ONTAP建立的 Key Vault 選單中，導覽至 **Keys** 選項。
2. 選擇產生/導入來建立新金鑰。
3. 將預設選項設定為生成。
4. 提供以下資訊：
   - 加密金鑰名稱

- 金鑰類型：RSA
- RSA金鑰大小：2048
- 已啟用：是

5. 選擇建立來建立加密金鑰。
6. 返回**Keys**選單並選擇您剛剛建立的密鑰。
7. 選擇目前版本下的金鑰ID，查看金鑰屬性。
8. 找到密鑰標識符欄位。複製 URI，直到但不包括十六進位字串。

建立 **Azure Active Directory** 端點（僅限 **HA**）

1. 僅當您為 HA Cloud Volumes ONTAP系統設定 Azure Key Vault 時才需要此程序。
2. 在 Azure 入口網站中導覽至虛擬網路。
3. 選擇部署Cloud Volumes ONTAP系統的虛擬網絡，然後選擇頁面左側的子網選單。
4. 從清單中選擇Cloud Volumes ONTAP部署的子網路名稱。
5. 導航至服務端點標題。在下拉式選單中，選擇以下內容：
   - **Microsoft.AzureActiveDirectory**
   - **Microsoft.KeyVault**
   - **Microsoft.Storage**（可選）



6. 選擇儲存來捕獲您的設定。

Cloud Volumes ONTAP配置

1. 使用您首選的 SSH 用戶端連線到叢集管理 LIF。
2. 在ONTAP中進入進階權限模式：

```
set advanced -con off
```

3. 確定所需的資料 SVM 並驗證其 DNS 配置：
   `vserver services name-service dns show`

   a. 如果所需資料 SVM 的 DNS 項目存在且包含 Azure DNS 項目，則無需執行任何操作。如果沒有，請為資料 SVM 新增指向 Azure DNS、私人 DNS 或本機伺服器的 DNS 伺服器項目。這應該與叢集管理員 SVM 的條目相符：
      `vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`

   b. 驗證已為資料 SVM 建立 DNS 服務：
      `vserver services name-service dns show`

4. 使用應用程式註冊後儲存的用戶端 ID 和租用戶 ID 啟用 Azure Key Vault：
   `security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name key_vault_URI -key-id full_key_URI`

   這 `_full_key_URI`價值必須利用 `<https:// <key vault host name>/keys/<key label>`格式。

5. 成功啟用 Azure Key Vault 後，輸入 `client secret value`當出現提示時。

6. 檢查密鑰管理器的狀態：
   `security key-manager external azure check`輸出將如下所示：

```
::*> security key-manager external azure check

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
    Status: OK

Category: ekmip_server
    Status: OK

Category: kms_wrapped_key_status
    Status: UNKNOWN
    Details: No volumes created yet for the vserver. Wrapped KEK status
will be available after creating encrypted volumes.

3 entries were displayed.
```

如果 `service_reachability`狀態不是 `OK`，SVM 無法透過所有必要的連線和權限存取 Azure Key Vault 服務。確保您的 Azure 網路策略和路由不會阻止您的私人 vNet 到達 Azure Key Vault 公共終端點。如果確實如此，請考慮使用 Azure Private 端點從 vNet 內部存取 Key Vault。您可能還需要在 SVM 上新增靜態主機條目來解析端點的私人 IP 位址。

這 `kms_wrapped_key_status`將會報告 `UNKNOWN`在初始配置時。其狀態將變為 `OK`第一卷加密後。

7. 可選：建立測試卷以驗證 NVE 的功能。

   ```
   vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
   -state online -policy default
   ```

   如果配置正確， Cloud Volumes ONTAP將自動建立磁碟區並啟用磁碟區加密。

8. 確認卷已正確建立並加密。如果是的話， `-is-encrypted`參數將顯示為 `true`。
   ```
   vol show -vserver SVM_name -fields is-encrypted
   ```
9. 可選：如果要更新 Azure Key Vault 驗證憑證上的憑證，請使用下列命令：
   ```
   security key-manager external azure update-credentials -vserver v1
   -authentication-method certificate
   ```

相關連結

- "設定Cloud Volumes ONTAP以在 Azure 中使用客戶管理的金鑰"
- "Microsoft Azure 文件：關於 Azure Key Vault"
- "ONTAP指令參考指南"

使用 Google Cloud KMS 管理Cloud Volumes ONTAP加密金鑰

您可以使用"Google Cloud Platform 的金鑰管理服務（Cloud KMS）"在 Google Cloud Platform 部署的應用程式中保護您的Cloud Volumes ONTAP加密金鑰。

可以使用ONTAP CLI 或ONTAP REST API 啟用 Cloud KMS 的金鑰管理。

使用 Cloud KMS 時，請注意預設使用資料 SVM 的 LIF 與雲端金鑰管理端點進行通訊。節點管理網路用於與雲端提供者的身份驗證服務（oauth2.googleapis.com）進行通訊。如果叢集網路配置不正確，叢集將無法正確利用金鑰管理服務。

開始之前

- 您的系統應該執行Cloud Volumes ONTAP 9.10.1 或更高版本
- 您必須使用資料 SVM。 Cloud KMS 只能在資料 SVM 上配置。
- 您必須是叢集或 SVM 管理員
- 應在 SVM 上安裝磁碟區加密 (VE) 許可證
- 從Cloud Volumes ONTAP 9.12.1 GA 開始，也應安裝多租用戶加密金鑰管理 (MTEKM) 許可證
- 需要有效的 Google Cloud Platform 訂閱

配置

Google雲

1. 在您的 Google Cloud 環境中，"建立對稱 GCP 金鑰環和金鑰" 。
2. 為 Cloud KMS 金鑰和Cloud Volumes ONTAP服務帳戶指派自訂角色。
   a. 建立自訂角色：

```
gcloud iam roles create kmsCustomRole
    --project=<project_id>
    --title=<kms_custom_role_name>
    --description=<custom_role_description>

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersio
ns.list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVer
sions.useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,clou
dkms.locations.get,cloudkms.locations.list,resourcemanager.projects.g
et
    --stage=GA
```

b. 指派您建立的自訂角色：
`gcloud kms keys add-iam-policy-binding *key_name* --keyring *key_ring_name* --location *key_location* --member serviceAccount:_service_account_Name_ --role projects/*customer_project_id*/roles/kmsCustomRole`

> 如果您使用的是Cloud Volumes ONTAP 9.13.0 或更高版本，則無需建立自訂角色。您可以指派預定義的[cloudkms.cryptoKeyEncrypterDecrypter^] 角色。

3. 下載服務帳戶 JSON 金鑰：
`gcloud iam service-accounts keys create key-file --iam-account=*sa-name*@*project-id*.iam.gserviceaccount.com`

Cloud Volumes ONTAP

1. 使用您首選的 SSH 用戶端連線到叢集管理 LIF。
2. 切換到進階權限等級：
`set -privilege advanced`
3. 為資料 SVM 建立 DNS。
`dns create -domains c.<*project*>.internal -name-servers *server_address* -vserver *SVM_name*`
4. 建立 CMEK 條目：
`security key-manager external gcp enable -vserver *SVM_name* -project-id *project* -key-ring-name *key_ring_name* -key-ring-location *key_ring_location* -key-name *key_name*`
5. 出現提示時，請輸入您的 GCP 帳戶中的服務帳戶 JSON 金鑰。
6. 確認啟用流程成功：
`security key-manager external gcp check -vserver *svm_name*`
7. 可選：建立磁碟區來測試加密 `vol create *volume_name* -aggregate *aggregate* -vserver *vserver_name* -size 10G`

故障排除

如果需要進行故障排除，您可以在上面的最後兩個步驟中追蹤原始 REST API 日誌：

1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

為Cloud Volumes ONTAP啟用NetApp勒索軟體防護解決方案

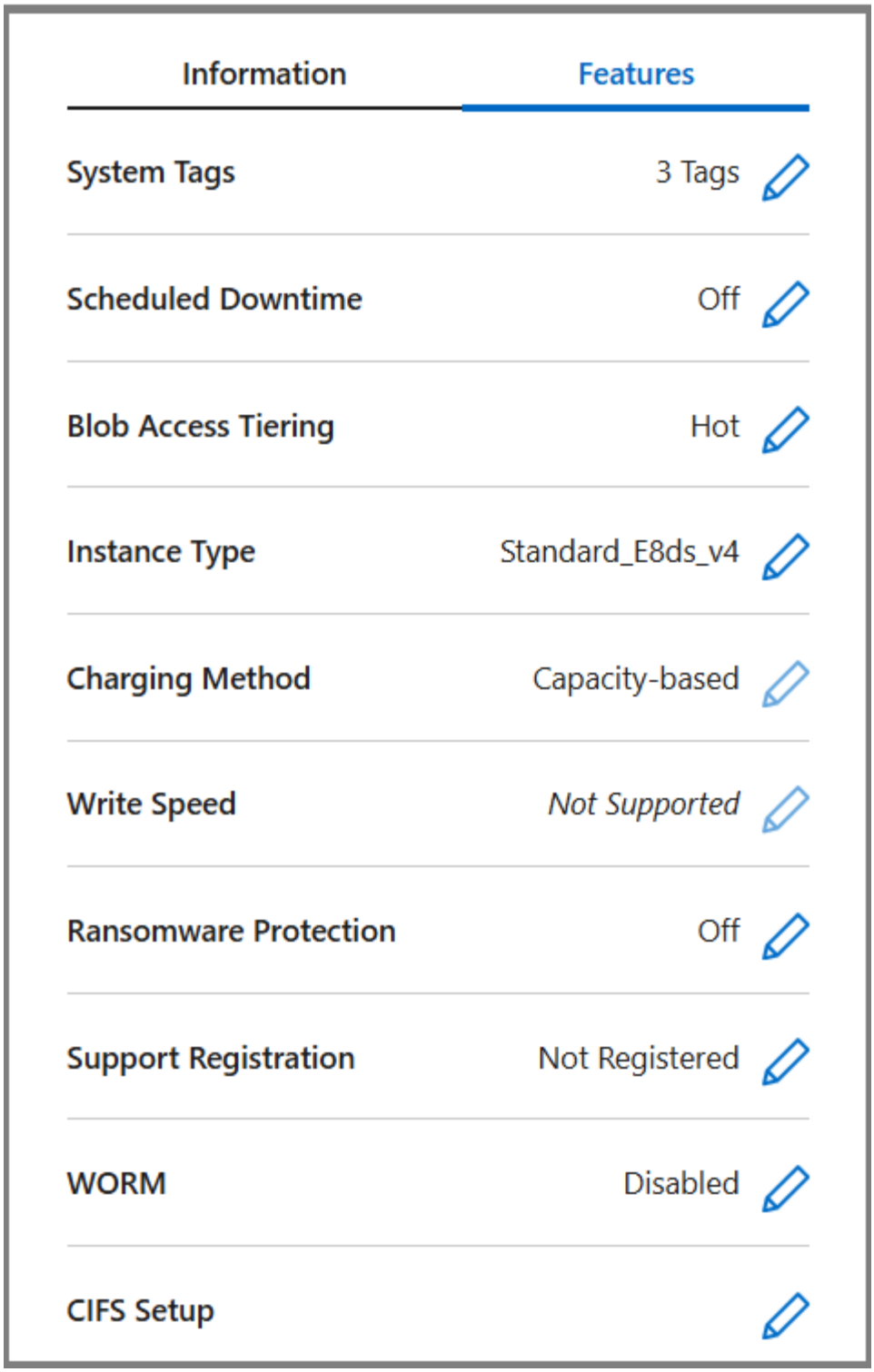
勒索軟體攻擊會浪費企業的時間、資源和聲譽。 NetApp Console可讓您實施兩種NetApp勒索軟體解決方案：針對共同勒索軟體檔案副檔名的防護和自主勒索軟體防護 (ARP)。這些解決方案為可見性、檢測和補救提供了有效的工具。

防禦常見勒索軟體檔案副檔名

控制台上的勒索軟體防護設定可讓您利用ONTAP FPolicy 功能來防禦常見的勒索軟體檔案擴充類型。

步驟

1. 在 **Systems** 頁面上，雙擊您配置為使用勒索軟體保護的Cloud Volumes ONTAP系統的名稱。
2. 在「概述」標籤上，按一下「功能」面板，然後按一下「勒索軟體防護」旁的鉛筆圖示。



3. 實施NetApp勒索軟體解決方案：

   a. 如果您的磁碟區未啟用快照策略，請按一下「啟動快照策略」。

      NetApp Snapshot 技術提供了業界最佳的勒索軟體補救解決方案。成功復原的關鍵是從未受感染的備份中復原。快照副本是唯讀的，可防止勒索軟體破壞。他們還可以提供創建單一文件副本或完整災難復原解決方案的圖像的粒度。

   b. 按一下「啟動 **FPolicy**」以啟用 ONTAP 的 FPolicy 解決方案，該解決方案可以根據檔案的副檔名阻止檔

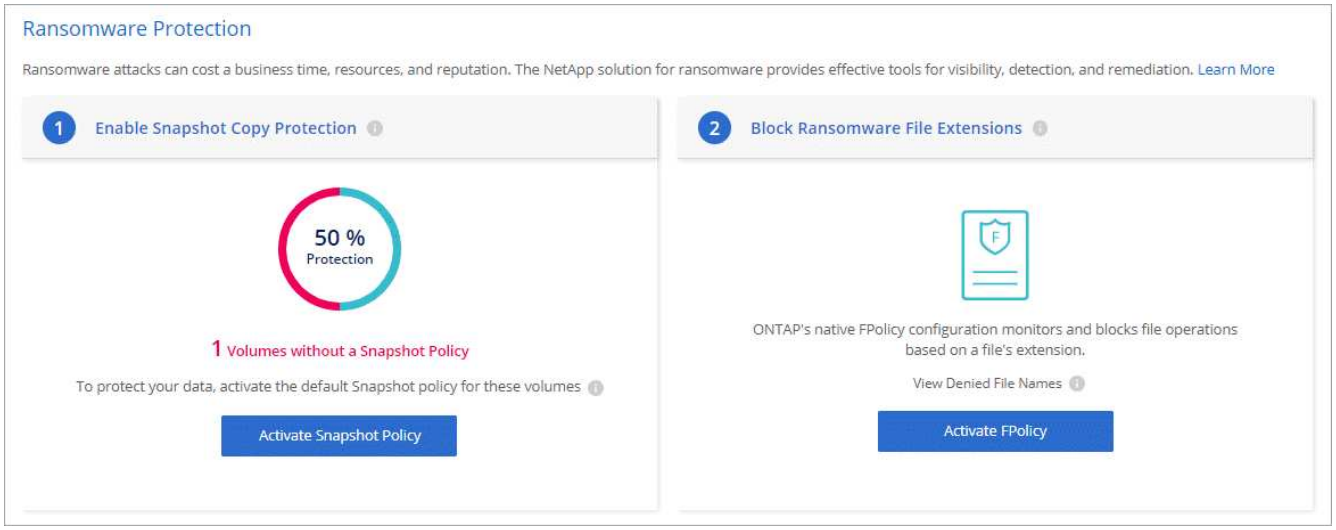
案操作。

此預防解決方案透過阻止常見的勒索軟體檔案類型來提高對勒索軟體攻擊的防護。

預設 FPolicy 範圍會封鎖具有下列副檔名的檔案：

micro、加密、鎖定、加密、crypt、crinf、r5a、XRNT、XTBL、R16M01D05、pzdc、好、哈哈！、OMG！ 、RDM、RRK、encryptedRS、crjoker、EnCiPhErEd、LeChiffre

當您在Cloud Volumes ONTAP上啟動 FPolicy 時，將會建立此範圍。此列表基於常見的勒索軟體檔案類型。您可以使用Cloud Volumes ONTAP CLI 中的 *vserver fpolicy policy scope* 指令自訂被封鎖的檔案副檔名。



自主勒索軟體防護

Cloud Volumes ONTAP支援自主勒索軟體防護 (ARP) 功能，可對工作負載進行分析，以主動偵測並警告可能表明勒索軟體攻擊的異常活動。

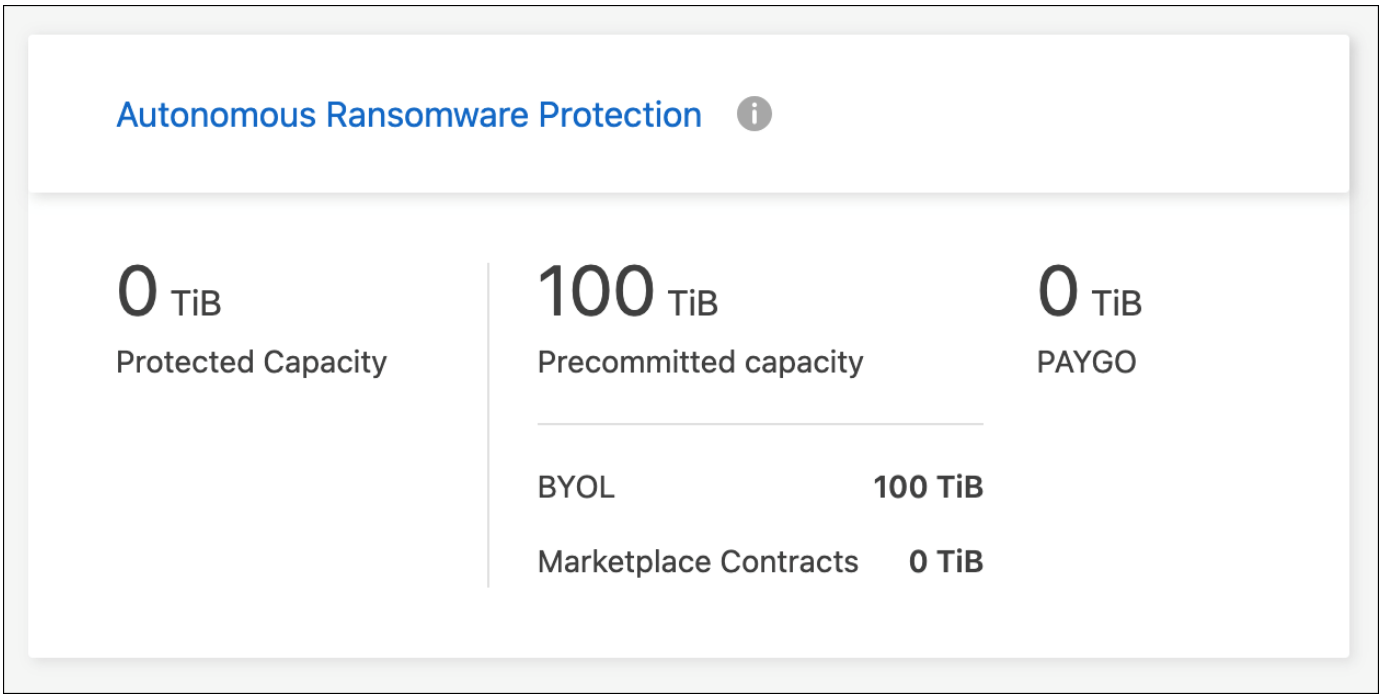
與透過以下方式提供的檔案副檔名保護分開 "勒索軟體防護設置"，ARP 功能使用工作負載分析根據偵測到的「異常活動」向使用者發出潛在攻擊警報。勒索軟體防護設定和 ARP 功能可以結合使用，以實現全面的勒索軟體防護。

ARP 功能可與自帶授權 (BYOL) 一起使用，且無需額外付費即可在市場訂閱您的授權。

啟用 ARP 的磁碟區具有指定狀態「學習模式」或「活動」 。

卷的 ARP 配置是透過ONTAP系統管理器和ONTAP CLI 執行的。

有關如何使用ONTAP System Manager 和ONTAP CLI 啟用 ARP 的更多信息，請參閱 "ONTAP文件：啟用自主勒索軟體防護"。



在Cloud Volumes ONTAP上建立 WORM 檔案的防篡改 Snapshot 副本

您可以在Cloud Volumes ONTAP系統上建立一次寫入、多次讀取 (WORM) 檔案的防篡改 Snapshot 副本，並在特定保留期內以未修改的形式保留快照。此功能由SnapLock技術提供支持，並提供了額外的資料保護和合規性層。

開始之前

確保用於建立 Snapshot 副本的磁碟區是SnapLock磁碟區。有關在卷上啟用SnapLock保護的信息，請參閱 "ONTAP文件：設定SnapLock"。

步驟

1. 從SnapLock磁碟區建立 Snapshot 副本。有關使用 CLI 或系統管理員建立 Snapshot 副本的信息，請參閱 "ONTAP文件：管理本機 Snapshot 副本概述"。

   Snapshot 副本繼承了磁碟區的 WORM 屬性，使其具有防篡改功能。底層的SnapLock技術可確保快照在指定的保留期結束之前受到保護，不會被編輯和刪除。

2. 如果需要編輯這些快照，您可以修改保留期。欲了解更多信息，請參閱 "ONTAP文檔：設定保留時間"。

> ⓘ 即使 Snapshot 副本在特定保留期內受到保護，叢集管理員也可以刪除來源磁碟區，因為Cloud Volumes ONTAP中的 WORM 儲存在「可信任儲存管理員」模型下執行。此外，受信任的雲端管理員可以透過操作雲端儲存資源來刪除WORM資料。

相關連結

- 有關 WORM 的更多信息，請參閱"了解Cloud Volumes ONTAP上的 WORM 存儲"。
- 有關SnapLock卷的充電信息，請參閱"Cloud Volumes ONTAP中的授權和計費"。

系統管理

升級Cloud Volumes ONTAP

從NetApp Console升級Cloud Volumes ONTAP以取得最新的功能和增強功能。在升級軟體之前，您應該準備好Cloud Volumes ONTAP系統。

升級概述

在開始Cloud Volumes ONTAP升級程序之前，您應該注意以下事項。

僅從控制台升級

您不應使用ONTAP系統管理員或ONTAP CLI 升級Cloud Volumes ONTAP ，而應僅使用控制台升級。否則可能會影響系統穩定性。

控制台提供了兩種升級Cloud Volumes ONTAP 的方法：

- 透過關注系統上出現的升級通知
- 透過將升級映像放置在 HTTPS 位置，然後向控制台提供 URL

支援的升級路徑

您可以升級到的 Cloud Volumes ONTAP 版本取決於您目前正在執行的版本。下表中每個發行版本的通用版本或修補程式版本代表可供升級的基本版本。有關可用修補程式的詳細資訊，請參閱每個發行版本的 "版本化發行說明"。

AWS 支援的升級路徑

目前版本	可直接升級到的版本
9.17.1 P1	9.18.1
9.16.1	9.17.1 P1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1

目前版本	可直接升級到的版本
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4
9.2	9.3
9.1	9.2
9.0	9.1
8.3	9.0

Azure 支援的升級路徑

目前版本	可直接升級到的版本
9.17.1 P1	9.18.1
9.16.1 P3	9.17.1 P1
9.15.1 P10	9.16.1 P3
9.14.1 P13	9.15.1 P10
9.13.1 P16	9.14.1 P13
9.12.1 P18	9.13.1 P16
9.11.1 P20	9.12.1 P18

如果您在 Azure 中擁有較低版本的Cloud Volumes ONTAP ，則必須先升級到下一個版本，然後按照支援的升級路徑達到目標版本。例如，如果您有Cloud Volumes ONTAP 9.7 P7，請遵循下列升級路徑：

- 9.7 P7 → 9.8 P18
- 9.8 P18 → 9.9.1 P15

- 9.9.1 P15 → 9.10.1 P12
- 9.10.1 P12 → 9.11.1 P20

Google Cloud 支援的升級路徑

目前版本	可直接升級到的版本
9.17.1 P1	9.18.1
9.16.1	9.17.1 P1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4
9.2	9.3
9.1	9.2

目前版本	可直接升級到的版本
9.0	9.1
8.3	9.0

請注意以下事項：

- Cloud Volumes ONTAP支援的升級路徑與本機ONTAP叢集支援的升級路徑不同。
- 如果您按照系統中出現的通知進行升級，控制台將提示您升級到遵循這些支援的升級路徑的版本。
- 如果透過將升級映像放置在 HTTPS 位置來進行升級，請務必遵循這些支援的升級路徑。
- 在某些情況下，您可能需要升級幾次才能達到目標版本。

  例如，如果您正在執行版本 9.8 並且想要升級到 9.10.1，則首先需要升級到版本 9.9.1，然後再升級到 9.10.1。

補丁版本

從 2024 年 1 月開始，僅當Cloud Volumes ONTAP的三個最新版本發布補丁時才可進行補丁升級。當 RC 或 GA 版本無法部署時，偶爾會有修補程式版本可供部署。

我們使用最新的 GA 版本來確定要在控制台中顯示的最新版本。例如，如果目前 GA 版本是 9.13.1，則控制台中會出現 9.11.1-9.13.1 的補丁。

對於補丁版本 9.11.1 或更低版本，您需要使用手動升級程序下載ONTAP映像。

作為補丁版本的一般規則，您可以從較低的補丁版本升級到相同或下一個Cloud Volumes ONTAP版本中的任何較高補丁版本。

以下是幾個例子：

- 9.13.0 → 9.13.1 P15
- 9.12.1 → 9.13.1 P2

恢復或降級

不支援將Cloud Volumes ONTAP還原或降級到先前的版本。

支援註冊

必須在NetApp支援處註冊Cloud Volumes ONTAP才能使用本頁所述的任何方法升級軟體。這適用於現收現付（PAYGO）和自備授權（BYOL）。你需要"手動註冊PAYGO系統"，而 BYOL 系統是預設註冊的。

未註冊支援的系統仍會在有新版本可用時收到控制台中出現的軟體更新通知。但您需要先註冊系統才能升級軟體。

HA 調解器的升級

控制台也會在Cloud Volumes ONTAP升級過程中根據需求更新中介實例。

使用 **c4**、**m4** 和 **r4 EC2** 執行個體類型在 **AWS** 中進行升級

Cloud Volumes ONTAP不再支援 c4、m4 和 r4 EC2 執行個體類型。您可以使用這些實例類型將現有部署升級到Cloud Volumes ONTAP版本 9.8-9.12.1。在升級之前，我們建議您更改實例類型。如果您無法變更實例類型，則需要啟用增強連網升級之前。閱讀以下部分以了解有關變更實例類型和啟用增強連網的詳細資訊。

在執行 9.13.0 及更高版本的Cloud Volumes ONTAP中，您無法使用 c4、m4 和 r4 EC2 執行個體類型進行升級。在這種情況下，您需要減少磁碟數量，然後更改實例類型或部署具有 c5、m5 和 r5 EC2 執行個體類型的新 HA 對配置並遷移資料。

更改實例類型

c4、m4 和 r4 EC2 執行個體類型允許每個節點擁有比 c5、m5 和 r5 EC2 執行個體類型更多的磁碟。如果您正在執行的 c4、m4 或 r4 EC2 執行個體每個節點的磁碟數低於 c5、m5 和 r5 執行個體每個節點的最大磁碟限額，則可以將 EC2 執行個體類型變更為 c5、m5 或 r5。

"檢查 EC2 執行個體的磁碟和分層限制" "變更Cloud Volumes ONTAP的 EC2 執行個體類型"

如果您無法變更實例類型，請依照[啟用增強連網]。

啟用增強連網

若要升級至Cloud Volumes ONTAP 9.8 及更高版本，您必須在執行 c4、m4 或 r4 實例類型的叢集上啟用_增強網路_。若要啟用 ENA，請參閱知識庫文章"如何在 AWS Cloud Volumes ONTAP執行個體上啟用 SR-IOV 或 ENA 等增強網絡"。

準備升級

在執行升級之前，您必須驗證系統已準備就緒並進行任何必要的配置變更。

- [規劃停機時間]
- [驗證自動交還是否仍然啟用]
- 暫停SnapMirror傳輸
- [驗證聚合是否在線]
- 驗證所有 LIF 是否位於主端口

規劃停機時間

升級單節點系統時，升級過程會使系統離線最多 25 分鐘，在此期間 I/O 會中斷。

在許多情況下，升級 HA 對不會造成中斷，且 I/O 也不會中斷。在此無中斷升級過程中，每個節點都會同步升級，以繼續為客戶端提供 I/O 服務。

面向會話的協定在升級過程中可能會對某些區域的用戶端和應用程式造成不利影響。有關詳細信息，請參閱"ONTAP文檔"

驗證自動交還是否仍然啟用

必須在Cloud Volumes ONTAP HA 對上啟用自動交還（這是預設）。如果不是，則操作將會失敗。

"ONTAP文件：用於設定自動交還的命令"

暫停SnapMirror傳輸

如果Cloud Volumes ONTAP系統具有活動的SnapMirror關係，最好在更新Cloud Volumes ONTAP軟體之前暫停傳輸。暫停傳輸可防止SnapMirror故障。您必須暫停從目標系統的傳輸。

儘管NetApp Backup and Recovery使用SnapMirror的實作來建立備份檔案（稱為SnapMirror Cloud），但在系統升級時無需暫停備份。

關於此任務

以下步驟介紹如何使用ONTAP System Manager 9.3 及更高版本。

步驟

1. 從目標系統登入系統管理員。

   您可以透過將 Web 瀏覽器指向叢集管理 LIF 的 IP 位址來登入系統管理員。您可以在Cloud Volumes ONTAP系統中找到 IP 位址。

   您從中存取控制台的電腦必須具有與Cloud Volumes ONTAP 的網路連線。例如，您可能需要從雲端供應商網路中的跳轉主機登入控制台。

2. 點選*保護>關係*。
3. 選擇關係並點選*操作>靜默*。

驗證聚合是否在線

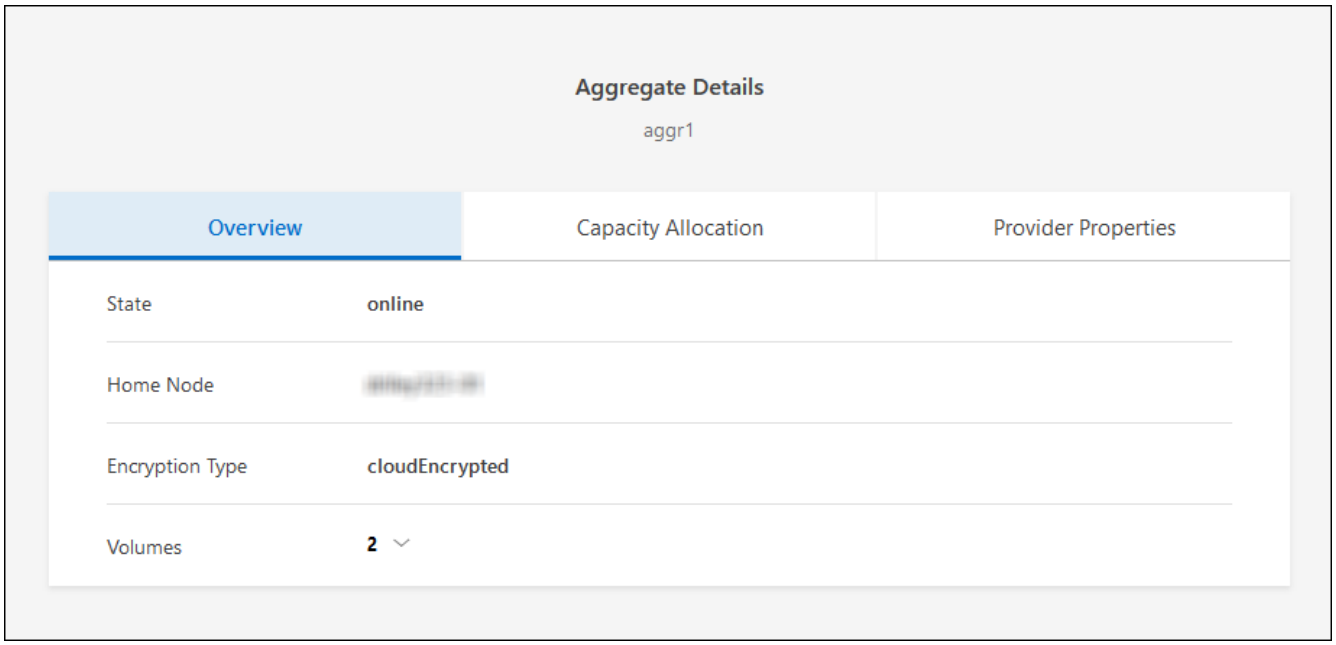
在更新軟體之前， Cloud Volumes ONTAP的聚合必須處於線上狀態。在大多數配置中，聚合應該處於線上狀態，但如果沒有，則應將其置於線上狀態。

關於此任務

以下步驟介紹如何使用ONTAP System Manager 9.3 及更高版本。

步驟

1. 在Cloud Volumes ONTAP系統上，按一下 **Aggregates** 標籤。
2. 在所需的聚合圖塊上，按一下 圖標，然後選擇*查看匯總詳情*。



3. 如果聚合處於離線狀態，請使用ONTAP系統管理員使聚合處於連線狀態：
   a. 按一下“儲存”>“聚合和磁碟”>“聚合”。
   b. 選擇聚合，然後按一下*更多操作>狀態>線上*。

驗證所有 **LIF** 是否位於主端口

升級前，所有 LIF 必須位於主連接埠上。請參閱ONTAP文檔"驗證所有 LIF 是否位於主端口"。

若發生升級失敗錯誤，請查閱知識庫 (KB) 文章"Cloud Volumes ONTAP升級失敗"。

升級Cloud Volumes ONTAP

當有新版本可供升級時，控制台會通知您。您可以從此通知開始升級程序。有關更多信息，請參閱[從控制台通知升級] 。

執行軟體升級的另一種方法是使用外部 URL 上的映像。如果控制台無法存取 S3 儲存桶來升級軟體或您獲得了補丁，則此選項很有用。有關更多信息，請參閱透過 URL 上的可用影像進行升級 。

從控制台通知升級

當有新版本的Cloud Volumes ONTAP Cloud Volumes ONTAP工作環境中顯示通知：

您必須擁有NetApp支援網站帳戶，然後才能透過通知升級Cloud Volumes ONTAP 。

您可以從此通知開始升級過程，該通知透過從 S3 儲存桶取得軟體映像、安裝映像，然後重新啟動系統來自動執行該過程。

開始之前

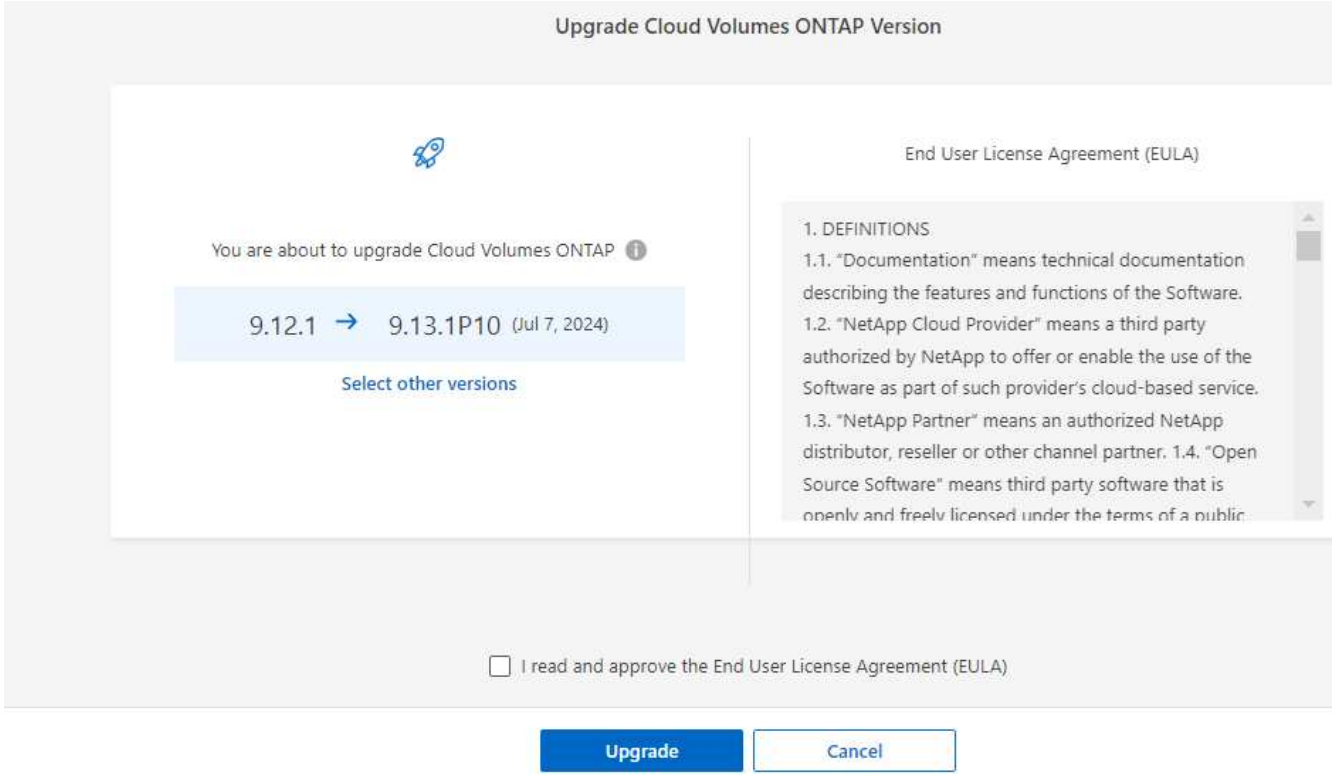
Cloud Volumes ONTAP系統上不得進行磁碟區或聚合建立等操作。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 選擇一個Cloud Volumes ONTAP系統。

   如果有新版本可用，概覽標籤中會出現通知：

3. 如果要升級已安裝的Cloud Volumes ONTAP版本，請按一下“立即升級！”預設情況下，您會看到最新的、相容的升級版本。

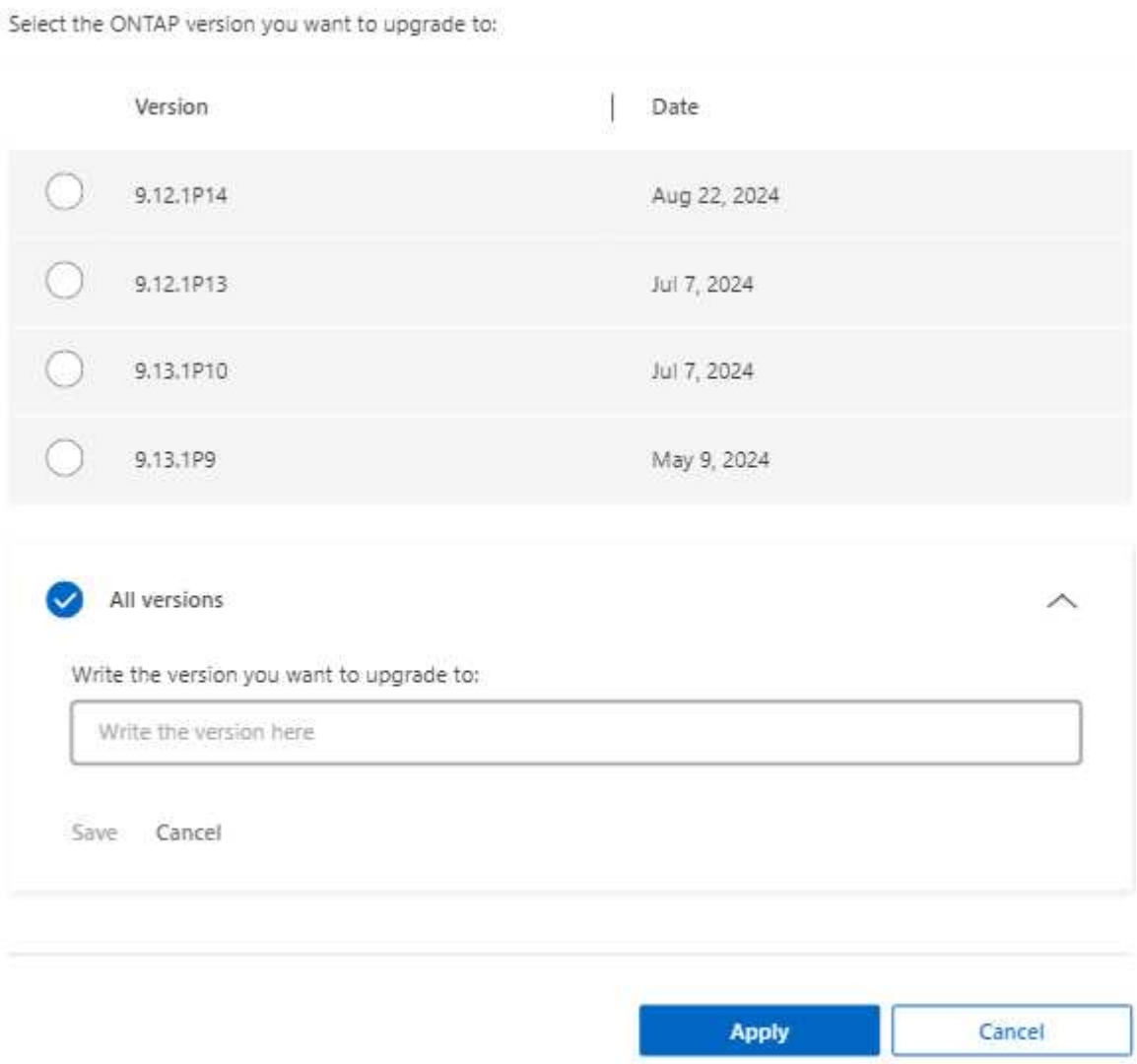


   若要升級到其他版本，請點選*選擇其他版本*。您會看到所列的最新Cloud Volumes ONTAP版本也與您系統上安裝的版本相容。例如，您的系統上安裝的版本是9.12.1P3，並且有以下相容版本可用：

   - 9.12.1P4 至 9.12.1P14
   - 9.13.1 和 9.13.1P1 您會看到 9.13.1P1 是升級的預設版本，而 9.12.1P13、9.13.1P14、9.13.1 和 9.13.1P1 是其他可用版本。

4. 或者，您可以按一下「所有版本」來輸入要升級到的另一個版本（例如，已安裝版本的下一個修補程式）。有關目前Cloud Volumes ONTAP版本的相容升級路徑，請參閱"支援的升級路徑"。

5. 按一下“儲存”，然後按一下“應用”



。

6. 在升級Cloud Volumes ONTAP頁面中，請閱讀 EULA，然後選擇 我已閱讀並同意 **EULA**。
7. 選擇*升級*。
8. 若要查看進度，請在Cloud Volumes ONTAP系統上選擇 **Audit**。

結果

控制台開始軟體升級。軟體更新完成後，您可以在系統上執行操作。

完成後

如果您暫停了SnapMirror傳輸，請使用系統管理員恢復傳輸。

透過 **URL** 上的可用影像進行升級

您可以將Cloud Volumes ONTAP軟體映像放在控制台代理程式或 HTTP 伺服器上，然後從控制台啟動軟體升級。如果控制台無法存取 S3 儲存桶來升級軟體，您可以使用此選項。

開始之前

- Cloud Volumes ONTAP系統上不得進行磁碟區或聚合建立等操作。

- 如果您使用 HTTPS 託管ONTAP映像，則升級可能會因缺少憑證而導致的 SSL 驗證問題而失敗。解決方法是產生並安裝 CA 簽署的證書，用於ONTAP和控制台之間的身份驗證。

  前往NetApp知識庫查看逐步說明：

  "NetApp KB：如何將控制台設定為 HTTPS 伺服器來託管升級映像"

步驟

1. 選用：設定可以託管Cloud Volumes ONTAP軟體映像的 HTTP 伺服器。

   如果您有與虛擬網路的 VPN 連接，則可以將Cloud Volumes ONTAP軟體映像放置在您自己網路中的 HTTP 伺服器上。否則，您必須將檔案放在雲端中的 HTTP 伺服器上。

2. 如果您對Cloud Volumes ONTAP使用自己的安全群組，請確保出站規則允許 HTTP 連接，以便Cloud Volumes ONTAP可以存取軟體映像。

   預先定義的Cloud Volumes ONTAP安全群組預設允許出站 HTTP 連線。

3. 從以下位置取得軟體映像 "NetApp支援站點"。
4. 將軟體映像複製到控制台代理或將提供該檔案的 HTTP 伺服器上的目錄中。

   有兩條路徑可用。正確的路徑取決於您的控制台代理版本。

   - `/opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/`
   - `/opt/application/netapp/cloudmanager/ontap/images/`
5. 在系統上，按一下 ••• 圖標，然後點擊*更新Cloud Volumes ONTAP*。
6. 在更新Cloud Volumes ONTAP版本頁面上，輸入 URL，然後按一下 變更圖片。

   如果您將軟體映像複製到上面顯示的路徑中的控制台代理，則需要輸入以下 URL：

   http://<Console_agent_private-IP-address>/ontap/images/<映像檔名>

   在 URL 中，**image-file-name** 必須遵循「cot.image.9.13.1P2.tgz」格式。

7. 按一下“繼續”進行確認。

結果

控制台開始軟體更新。軟體更新完成後，您就可以在系統上執行操作。

完成後

如果您暫停了SnapMirror傳輸，請使用系統管理員恢復傳輸。

修復使用 **Google Cloud NAT** 閘道時下載失敗的問題

控制台代理程式會自動下載Cloud Volumes ONTAP 的軟體更新。如果您的設定使用 Google Cloud NAT 網關，下載可能會失敗。您可以透過限制軟體映像劃分的部分數來解決此問題。您必須使用 API 來完成此步驟。

步

1. 向 `/occm/`config 提交 PUT 請求，並將以下 JSON 作為正文：

```
{
  "maxDownloadSessions": 32
}
```

maxDownloadSessions 的值可以是 1 或任何大於 1 的整數。如果值為1，則下載的影像不會被分割。

請注意，32 是一個範例值。您應該使用的值取決於您的 NAT 配置和您可以同時擁有的會話數。

"了解有關 /occm/config API 呼叫的更多信息" 。

註冊Cloud Volumes ONTAP即用即付系統

Cloud Volumes ONTAP即用即付 (PAYGO) 系統包含NetApp的支持，但您必須先透過向NetApp註冊系統來啟動支援。

需要向NetApp註冊 PAYGO 系統才能使用任何方法升級ONTAP軟體"本頁描述"。

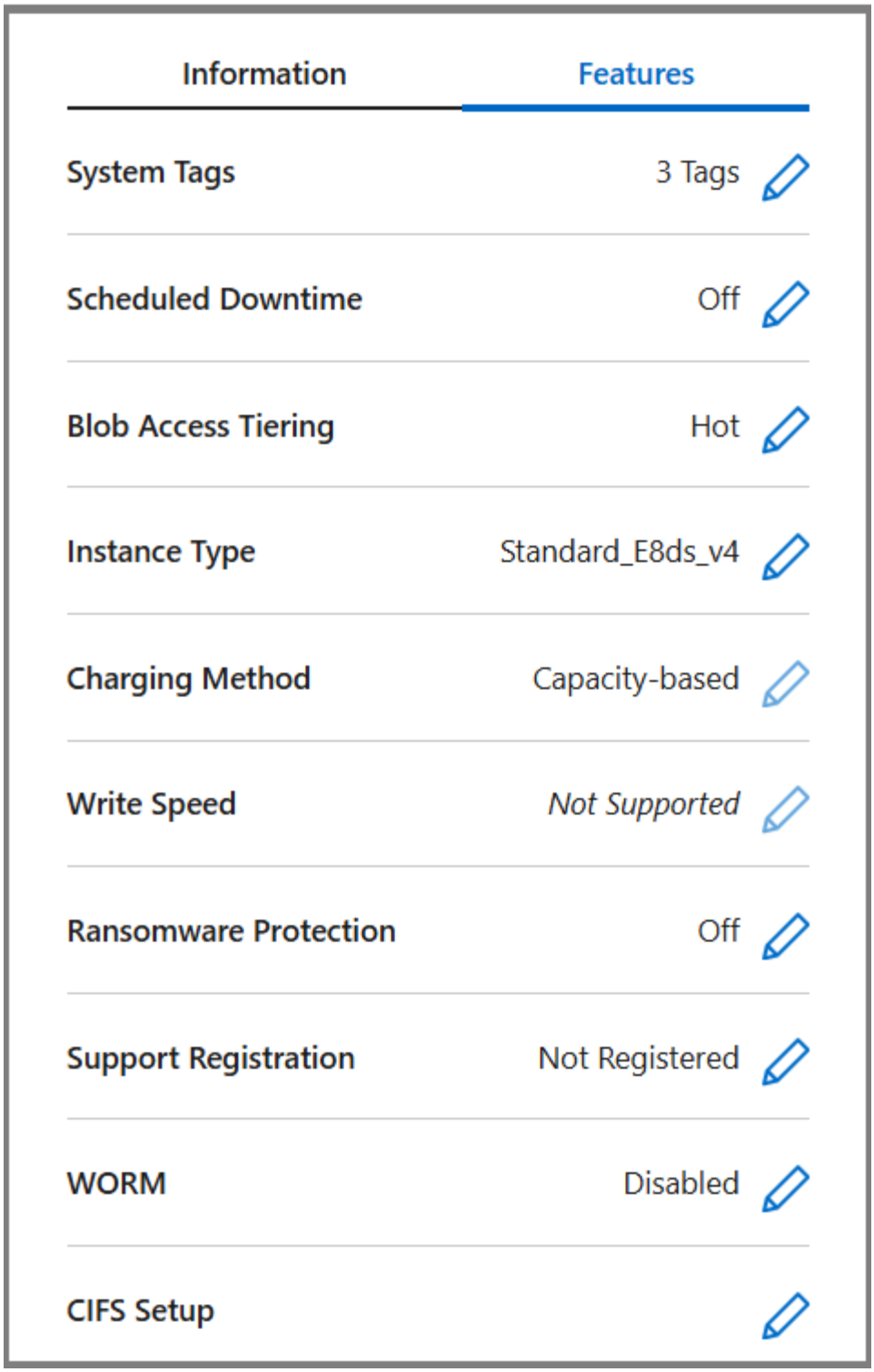
未註冊支援的系統仍會在有新版本可用時收到NetApp Console中顯示的軟體更新通知。但您需要先註冊系統才能升級軟體。

步驟

1. 如果您尚未將NetApp支援網站帳戶新增至控制台，請前往 帳戶設定 並立即新增。

   "了解如何新增NetApp支援網站帳戶" 。

2. 在「系統」頁面上，雙擊要註冊的系統的名稱。
3. 在「概述」標籤上，按一下「功能」面板，然後按一下「支援註冊」旁邊的鉛筆圖示。



4. 選擇NetApp支援網站帳號並點選「註冊」。

結果

該系統已在NetApp註冊。

將Cloud Volumes ONTAP基於節點的許可證轉換為基於容量的許可證

在基於節點的許可證的可用性終止 (EOA) 之後，您應該使用NetApp Console中的許可證轉

換工具過渡到基於容量的許可證。

對於年度或長期承諾， NetApp建議您在 EOA 日期（2024 年 11 月 11 日）或許可證到期日之前聯繫您的NetApp代表，以確保過渡的先決條件到位。如果您沒有Cloud Volumes ONTAP節點的長期合同，並且根據按需付費 (PAYGO) 訂閱運行您的系統，那麼在 2024 年 12 月 31 日支援終止 (EOS) 之前規劃您的轉換非常重要。在這兩種情況下，您都應確保您的系統符合要求，然後再使用NetApp Console中的許可證轉換工具實現無縫過渡。

有關 EOA 和 EOS 的信息，請參閱"基於節點的許可證的可用性終止"。

關於此任務

- 當您使用許可證轉換工具時，從基於節點到基於容量的許可模型的轉換是在現場線上進行的，從而無需進行任何資料遷移或配置額外的雲端資源。
- 它是一種無中斷操作，不會發生服務中斷或應用程式停機。
- Cloud Volumes ONTAP系統中的帳戶和應用程式資料保持不變。
- 轉換後，底層雲端資源不受影響。
- 許可證轉換工具支援所有部署類型，例如單節點、單可用區 (AZ) 中的高可用性 (HA)、多 AZ 中的 HA、自帶許可證 (BYOL) 和 PAYGO。
- 該工具支援所有基於節點的許可證作為來源，以及所有基於容量的許可證作為目標。例如，如果您擁有基於節點的 PAYGO 標準許可證，則可以將其轉換為透過市場購買的任何基於容量的許可證。 NetApp已限制 BYOL 授權的購買、延期和續約。有關更多信息，請參閱 "Cloud Volumes ONTAP的 BYOL 授權可用性受限" 。
- 所有雲端供應商、AWS、Azure 和 Google Cloud 都支援轉換。
- 轉換後，基於節點的許可證的序號將被基於容量的格式取代。這是轉換的一部分，並反映在您的NetApp支援網站 (NSS) 帳戶中。
- 當您過渡到基於容量的模型時，您的資料將繼續保留在與基於節點的許可相同的位置。這種方法保證了資料放置不會中斷，並在整個過渡過程中堅持資料主權原則。

開始之前

- 您應該擁有一個具有客戶存取權限或管理員存取權限的 NSS 帳戶。
- 您的 NSS 帳戶應使用您用於存取控制台的使用者憑證進行註冊。
- Cloud Volumes ONTAP系統應連結至具有客戶存取權限或管理員存取權限的 NSS 帳戶。
- 您應該擁有有效的基於容量的許可證，可以是 BYOL 許可證或市場訂閱。
- 您的帳戶中應該有基於容量的許可證。此授權可以是市場訂閱，也可以是控制台中 **Licenses and subscriptions** 下提供的 BYOL/私人優惠包。
- 在選擇目的地套餐之前，請先了解以下標準：
  - 如果帳戶具有基於容量的 BYOL 許可證，則所選目標包應與帳戶的 BYOL 基於容量的許可證保持一致：
    - 什麼時候 `Professional`被選為目標包，該帳戶應具有帶有專業包的 BYOL 許可證：
    - 什麼時候 `Essentials`被選為目標包，該帳戶應具有 Essentials 包的 BYOL 授權。
  - 如果目標套件與帳戶的 BYOL 授權可用性不一致，則表示基於容量的授權可能不包含所選套件。在這種情況下，我們將透過您的市場訂閱向您收費。
  - 如果沒有基於容量的 BYOL 授權而只有市場訂閱，則應確保所選包包含在基於容量的市場訂閱中。

- 如果您現有的基於容量的許可證中沒有足夠的容量，並且您有市場訂閱來對額外的容量使用收費，那麼您將透過市場訂閱為額外的容量付費。
- 如果您現有的基於容量的許可證中沒有足夠的容量，並且您沒有市場訂閱來收取額外容量使用的費用，則無法進行轉換。您應該添加市場訂閱來收取額外容量或將可用容量擴展到您目前的授權。
- 如果目標套件與帳戶的 BYOL 授權可用性不一致，且您現有的基於容量的授權中沒有足夠的容量，那麼您將透過市場訂閱付費。

如果任何一項要求未滿足，則許可證轉換不會發生。在特定情況下，許可證可能會轉換，但不能使用。點擊資訊圖示以識別問題並採取糾正措施。

步驟

1. 在「系統」頁面上，雙擊要修改許可證類型的系統的名稱。
2. 在「概述」標籤上，按一下「功能」面板。
3. 檢查*充電方式*旁邊的鉛筆圖示。如果您的系統的充電方式是 `Node Based`，可轉換為按容量充電。

   如果您的Cloud Volumes ONTAP系統已按容量收費，或任何要求未滿足，則該圖示將被停用。

4. 在*將基於節點的許可證轉換為基於容量的許可證*螢幕上，驗證系統名稱和來源許可證詳細資訊。
5. 選擇轉換現有許可證的目標包：
   - 必需品。預設值為 `Essentials`。
   - 專業的
6. 如果您擁有 BYOL 許可證，則可以在轉換完成後選取核取方塊以從控制台中刪除基於節點的許可證。如果轉換仍在進行中，選取此核取方塊將不會從控制台中刪除授權。此選項不適用於市場訂閱。
7. 選取核取方塊以確認您了解變更的含義，然後按一下「繼續」。

完成後

查看新的許可證序號並在控制台的*Licenses and subscriptions*選單中驗證變更。

不同超標量中的定價

有關定價的詳細信息，請訪問 "NetApp Console網站"。

有關特定超標量中的私人優惠的信息，請寫信至：

- AWS - awspo@netapp.com
- Azure - azurepo@netapp.com
- Google Cloud - gcppo@netapp.com

啟動並停止Cloud Volumes ONTAP系統

您可以從NetApp Console停止並啟動Cloud Volumes ONTAP來管理您的雲端運算成本。

安排**Cloud Volumes ONTAP**自動關閉

您可能想要在特定時間間隔內關閉Cloud Volumes ONTAP以降低運算成本。您無需手動執行此操作，而是可以將控制台配置為在特定時間自動關閉然後重新啟動系統。

關於此任務

- 當您計劃自動關閉Cloud Volumes ONTAP系統時，如果正在進行活動資料傳輸，控制台會延遲關閉。

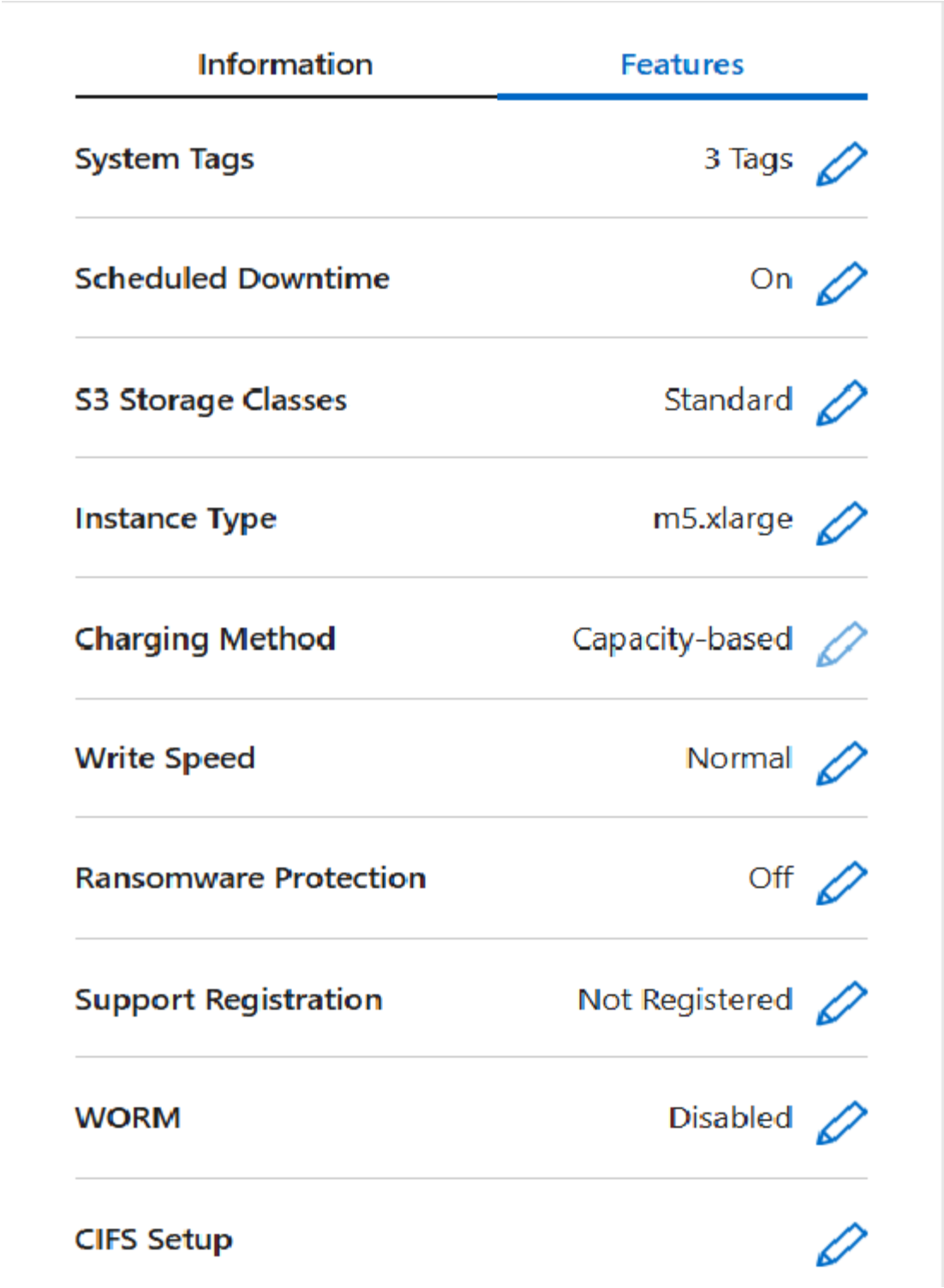
  傳輸完成後，系統將關閉。

- 此任務計劃會自動關閉 HA 對中的兩個節點。
- 透過排程關閉來關閉Cloud Volumes ONTAP時，不會建立啟動磁碟和根磁碟的快照。

  如下一節所述，只有在執行手動關機時才會自動建立快照。

步驟

1. 在*系統*頁面上，雙擊Cloud Volumes ONTAP系統。
2. 在「概覽」標籤上，按一下「功能」面板，然後按一下「規劃停機時間」旁的鉛筆圖示。



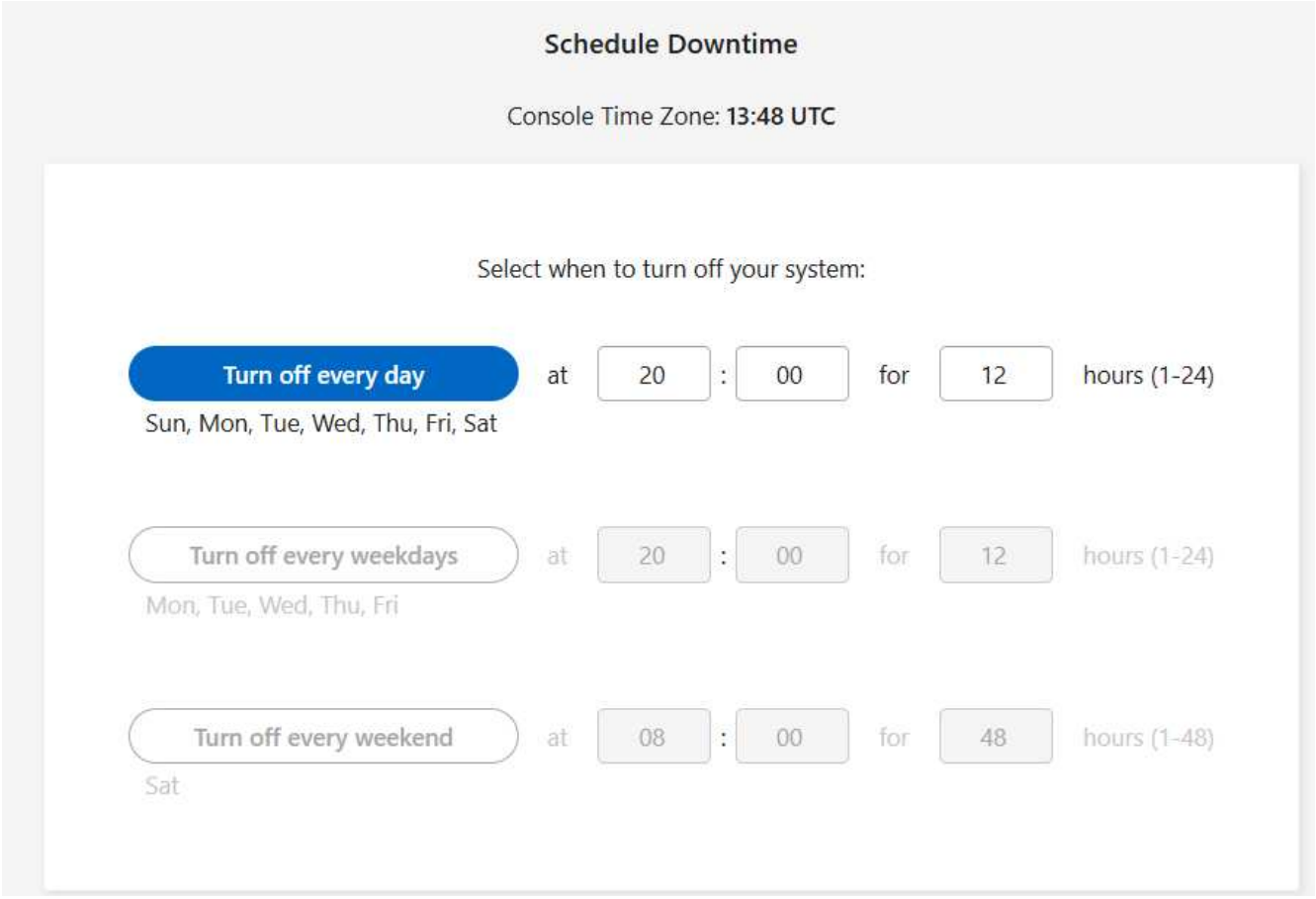
3. 指定關機計劃：

   a. 選擇是否每天、每個工作日、每個週末或這三個選項的任意組合關閉系統。

   b. 指定您想要關閉系統的時間以及關閉系統的時間長度。

      例子

      下圖顯示了一個時間表，指示控制台每週六晚上 20:00（晚上 8:00）關閉系統 12 小時。控制台每週一凌晨 12:00 重新啟動系統



4. 點選“儲存”。

結果

時間表已儲存。功能面板下對應的計劃停機時間行項目顯示「開啟」。

停止Cloud Volumes ONTAP

停止Cloud Volumes ONTAP可節省計算成本並建立根磁碟和啟動磁碟的快照，這有助於排除故障。

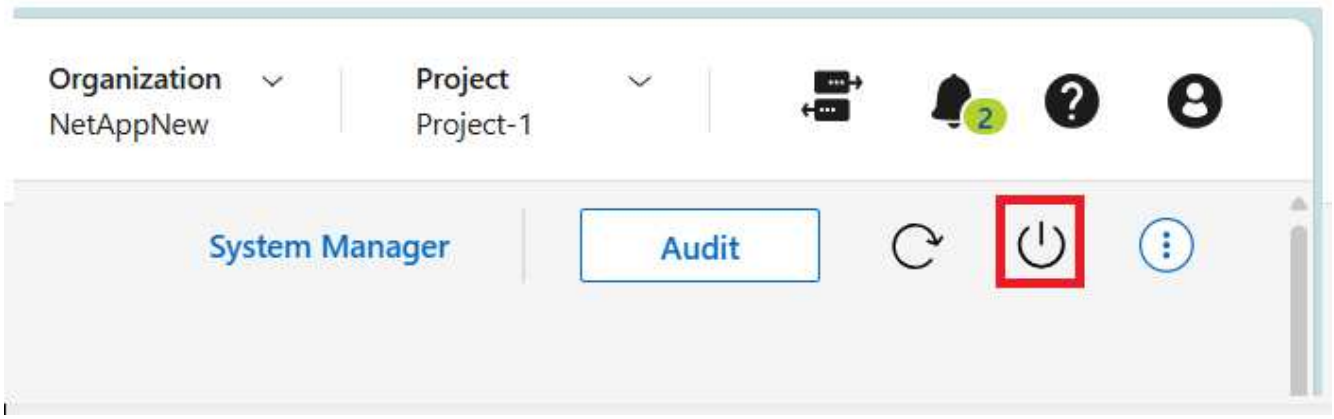
> 為了降低成本，控制台會定期刪除根和啟動磁碟的舊快照。根磁碟和啟動磁碟僅保留最近的兩個快照。

關於此任務

當您停止 HA 對時，控制台將關閉兩個節點。

步驟

1. 在系統中，按一下「關閉」圖示。



2. 保持建立快照的選項處於啟用狀態，因為快照可以啟用系統復原。
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*系統*頁面重新啟動系統。

   重新啟動時會自動建立快照。

使用 NTP 伺服器同步 Cloud Volumes ONTAP 系統時間

為 Cloud Volumes ONTAP 叢集設定網路時間協定（NTP）伺服器，可確保叢集時間與網路中的其他系統和外部伺服器的時間精確同步。將叢集時間與外部 NTP 伺服器同步有助於維護基礎架構的一致性。NetApp 預設情況下會為新 Cloud Volumes ONTAP 部署設定 NTP 伺服器。但是，如果現有 Cloud Volumes ONTAP 叢集未配置 NTP 伺服器，則必須設定 NTP 伺服器，以確保網路內外時間的精確同步。

您可以使用以下命令指定 NTP 伺服器：

- "NetApp ConsoleAPI"。
- ONTAP CLI 指令 "建立叢集時間服務 NTP 伺服器"。

如果您未設定 NTP 伺服器，可能會遇到服務中斷和時間同步不準確的情況。

相關連結

- 知識庫（KB）文章： "CVO叢集如何使用NTP？"
- "準備使用 API"
- "Cloud Volumes ONTAP工作流程"
- "取得所需的標識符"
- "使用NetApp Console的 REST API"

修改系統寫入速度

您可以在NetApp Console中為Cloud Volumes ONTAP選擇正常或高寫入速度。預設寫入速

度正常。如果您的工作負載需要快速寫入效能，您可以變更為高寫入速度。

所有類型的單節點系統和部分 HA 配對配置均支援高寫入速度。在 "Cloud Volumes ONTAP發行說明"中查看支援的配置

在更改寫入速度之前，您應該"了解正常設定和高設定之間的差異"。

關於此任務

- 確保磁碟區或聚合建立等操作尚未進行。
- 請注意，此變更將重新啟動Cloud Volumes ONTAP系統。這是一個破壞性的過程，需要整個系統停機。

步驟

1. 在*系統*頁面上，雙擊您配置寫入速度的系統的名稱。
2. 在「概述」標籤上，按一下「功能」面板，然後按一下「寫入速度」旁邊的鉛筆圖示。
3. 選擇*正常*或*高*。

   如果您選擇“高”，那麼您需要閱讀“我明白...”聲明並透過勾選方塊進行確認。

   從 9.13.0 版本開始，Google Cloud 中的Cloud Volumes ONTAP HA 對支援 高 寫入速度選項。

4. 按一下“儲存”，查看確認訊息，然後按一下“核准”。

變更Cloud Volumes ONTAP叢集管理員密碼

Cloud Volumes ONTAP包含一個叢集管理員帳戶。如果需要，您可以從NetApp Console變更此帳戶的密碼。

您不應透過ONTAP系統管理員或ONTAP CLI 變更管理員帳戶的密碼。密碼不會反映在控制台中。因此，控制台無法正確監控實例。

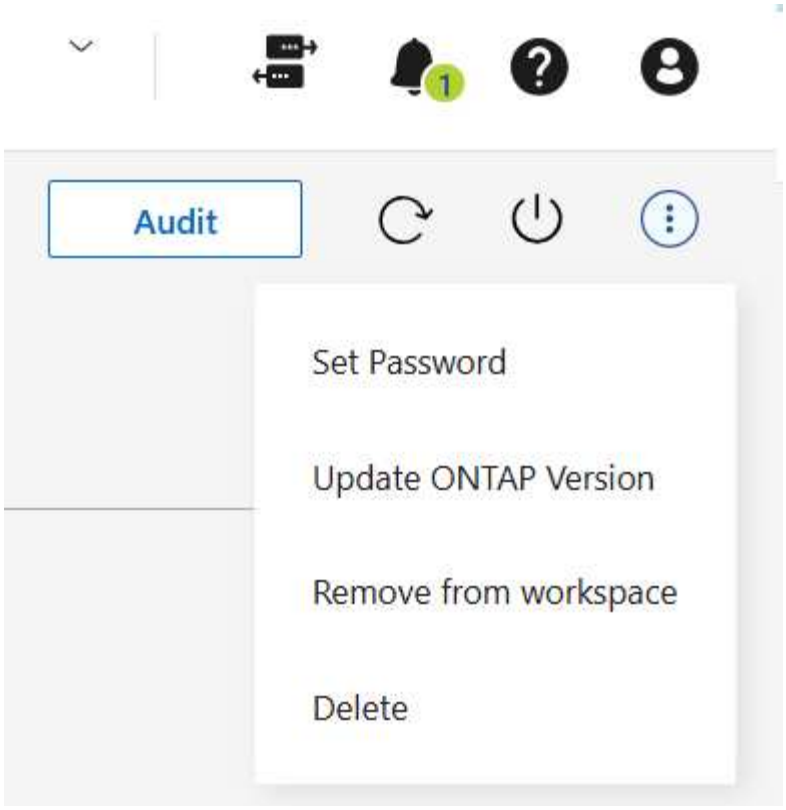
關於此任務

密碼必須遵守一些規則。新密碼：

- 不應包含該詞 `admin`
- 長度必須介於 8 到 50 個字元之間
- 必須至少包含一個英文字母和一個數字
- 不應包含以下特殊字元： `/ ( ) { } [ ] # : % " ? \`

步驟

1. 在*系統*頁面上，雙擊Cloud Volumes ONTAP系統的名稱。
2. 在控制台的右上角，按一下•••圖標，然後選擇*設定密碼*。



新增、移除或刪除系統

將現有的**Cloud Volumes ONTAP**系統新增至**NetApp Console**

您可以探索現有的 Cloud Volumes ONTAP 系統並將其新增至 NetApp Console 以進行集中管理。當您使用帳戶上線系統時，該系統會註冊到該帳戶。在具有多個帳戶或組織的環境中，您只能探索和管理已註冊到您的 Console 登入帳戶的系統。

在進行系統註冊時，請確保所有操作均在系統最初註冊的同一組織和帳戶內執行。例如，您可以將 Cloud Volumes ONTAP 系統遷移到新的 Console 代理，但遷移過程必須在同一組織內進行。

您無法探索、檢視或管理已註冊到其他帳戶或組織的系統。

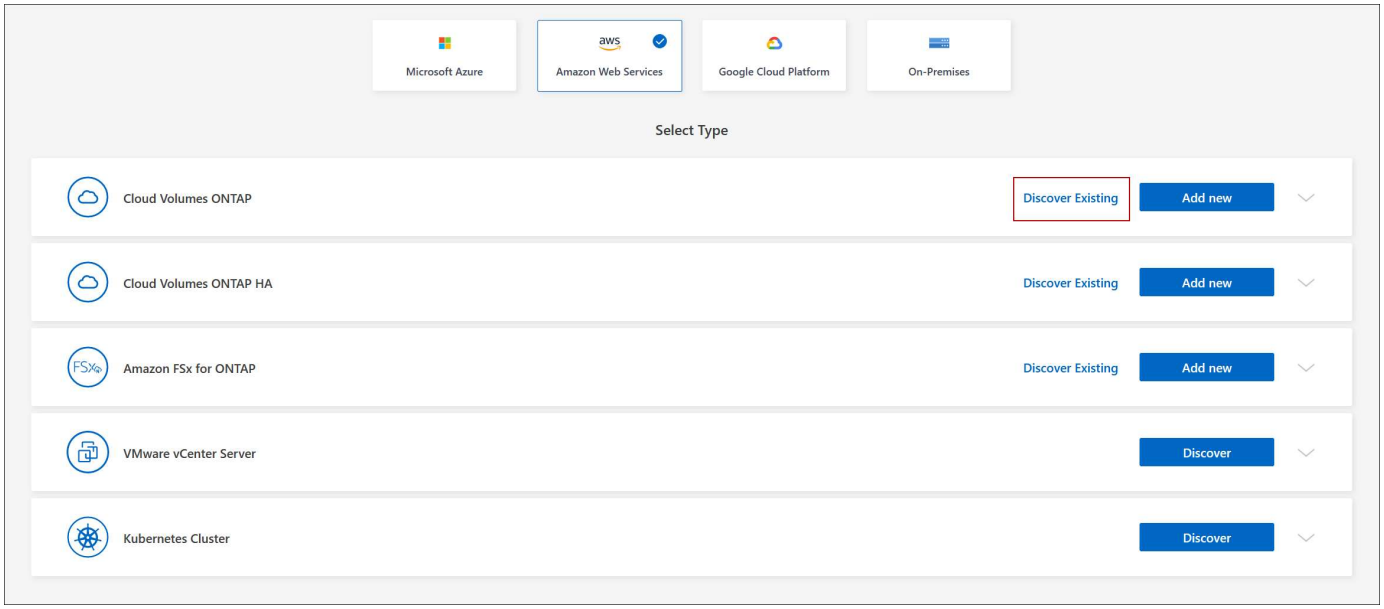
開始之前

您必須知道Cloud Volumes ONTAP管理員使用者帳號的密碼。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，按一下*新增系統*。
3. 選擇系統所在的雲端提供者。
4. 選擇要新增的Cloud Volumes ONTAP系統的類型。
5. 點擊連結即可發現現有系統。

+



1. 在「區域」頁面上，選擇一個區域。您可以看到在所選區域中運作的系統。

Cloud Volumes ONTAP系統在此頁面中以實例形式表示。從清單中，您可以只選擇使用目前帳戶註冊的那些執行個體。

2. 在「憑證」頁面上，輸入Cloud Volumes ONTAP管理員使用者的密碼，然後選擇「**Go**」。

結果

控制台將Cloud Volumes ONTAP系統新增至 系統 頁面。

從**NetApp Console**移除**Cloud Volumes ONTAP**系統

您可以刪除Cloud Volumes ONTAP系統以將其移至另一個系統或解決發現問題。

關於此任務

刪除Cloud Volumes ONTAP系統會將其從NetApp Console中移除。它不會刪除Cloud Volumes ONTAP系統。如果需要，您可以稍後重新發現該系統。

步驟

1. 在「系統」頁面上，雙擊要刪除的系統。
2. 在控制台的右上角，按一下 ••• 圖標，然後選擇*從工作區中刪除*。
3. 在*從工作區中刪除*視窗中，按一下*刪除*。

結果

控制台刪除系統。使用者可以隨時從*系統*頁面重新發現已刪除的系統。

從**NetApp Console**移除**Cloud Volumes ONTAP**系統

您應該始終從NetApp Console中刪除Cloud Volumes ONTAP系統，而不是從雲端提供者的應用程式中刪除。例如，如果您終止了雲端提供者授權的Cloud Volumes ONTAP實例，則您不能將該授權金鑰用於另一個實例。您必須從控制台中刪除Cloud Volumes ONTAP系統

才能釋放許可證。

當您刪除系統時，控制台會終止Cloud Volumes ONTAP實例並刪除磁碟和快照。

> 刪除系統時，不會刪除其他資源，例如NetApp Backup and Recovery管理的備份以及NetApp Data Classification的實例。您需要手動刪除它們。如果您不這樣做，那麼您將繼續為這些資源支付費用。

當控制台在您的雲端提供者中部署Cloud Volumes ONTAP時，它會對執行個體啟用終止保護。此選項有助於防止意外終止。

步驟

1. 如果您在系統上啟用了備份和還原功能，請確定是否仍然需要備份的數據，然後… "如有必要，刪除備份" 。

   備份和還原在設計上獨立於Cloud Volumes ONTAP 。當您刪除Cloud Volumes ONTAP系統時，備份和復原不會自動刪除備份，且 UI 中目前不支援在系統被刪除後刪除備份。

2. 如果您在此系統上啟用了資料分類，並且沒有其他系統使用此服務，那麼您需要刪除該服務的實例。

   "了解有關資料分類實例的更多信息" 。

3. 刪除Cloud Volumes ONTAP系統。
   a. 在「系統」頁面上，雙擊要刪除的Cloud Volumes ONTAP系統的名稱。
   b. 在控制台的右上角，按一下•••圖標，然後選擇*刪除*。
   c. 輸入要刪除的系統的名稱，然後按一下「刪除」。刪除系統可能需要最多五分鐘。

> 僅適用於Cloud Volumes ONTAP Professional 許可證，備份和復原是免費的。此免費福利不適用於已刪除的環境。如果Cloud Volumes ONTAP環境的備份副本保留在備份和復原實例中，則您將需要為備份副本付費，直到它們被刪除為止。

AWS 管理

修改 **AWS** 中**Cloud Volumes ONTAP**系統的 **EC2** 執行個體類型

在 AWS 中啟動Cloud Volumes ONTAP時，您可以從多個執行個體或類型中進行選擇。如果您確定實例類型太小或太大，無法滿足您的需求，您可以隨時變更實例類型。

關於此任務

- 必須在Cloud Volumes ONTAP HA 對上啟用自動交還（這是預設）。如果不是，則操作將會失敗。

  "ONTAP 9 文件：用於設定自動交還的命令"

- 變更執行個體類型可能會影響 AWS 服務費用。
- 此操作重新啟動Cloud Volumes ONTAP。

  對於單節點系統， I/O 會中斷。

  對於 HA 對來說，這種變化是無中斷的。 HA 對繼續提供數據。

NetApp Console透過啟動接管並等待返回來一次更改一個節點。 NetApp 的品質保證團隊在過程中對檔案的寫入和讀取進行了測試，並且沒有發現客戶端的任何問題。隨著連接的變化，在 I/O 層級觀察到一些重試，但應用層克服了 NFS/CIFS 連接的重新連接。

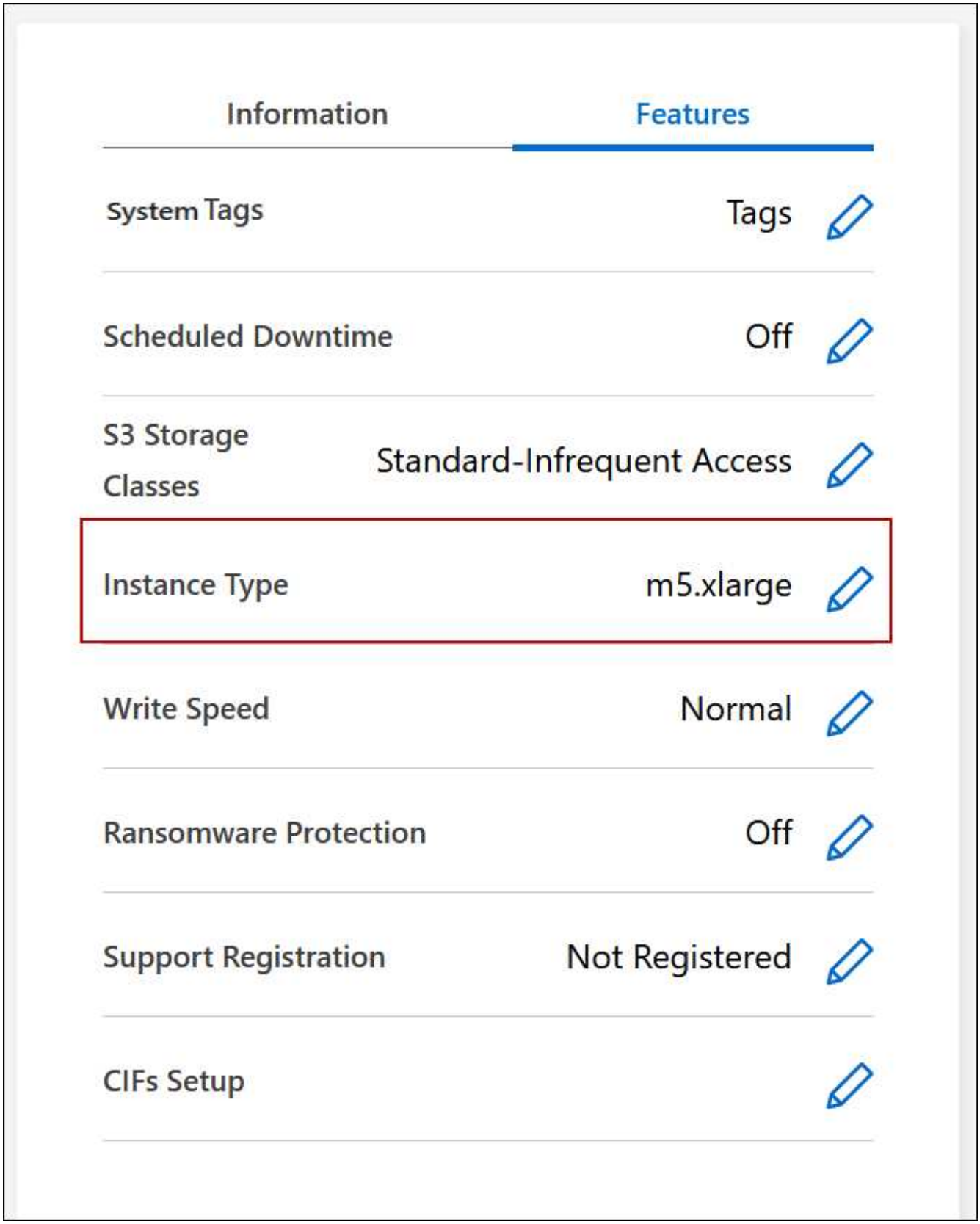
參考

有關 AWS 支援的實例類型列表，請參閱"支援的 EC2 實例"。

如果您無法將實例類型從 c4、m4 或 r4 實例變更為其他類型，請參閱知識庫文章"將 AWS Xen CVO 執行個體轉換為 Nitro (KVM)"。

步驟

1. 在*系統*頁面上，選擇系統。
2. 在概覽標籤上，按一下功能面板，然後按一下*實例類型*旁邊的鉛筆圖示。



如果您使用的是基於節點的即用即付 (PAYGO) 許可證，則可以透過點擊「許可證類型」旁邊的鉛筆圖示來選擇不同的許可證和實例類型。

3. 選擇實例類型，選取核取方塊以確認您了解變更的含義，然後按一下*變更*。

結果

Cloud Volumes ONTAP使用新設定重新啟動。

修改多個 **AWS AZ** 中的**Cloud Volumes ONTAP HA** 對的路由表

您可以修改 AWS 路由表，其中包含部署在多個 AWS 可用區 (AZ) 中的 HA 對的浮動 IP 位址的路由。如果新的 NFS 或 CIFS 用戶端需要存取 AWS 中的 HA 對，您可以這樣做。

步驟

1. 在*系統*頁面上，選擇系統。
2. 在概覽標籤上，按一下功能面板，然後按一下*路由表*旁的鉛筆圖示。
3. 修改所選路由表列表，然後按一下「儲存」。

結果

NetApp Console傳送 AWS 請求來修改路由表。

Azure 管理

變更**Cloud Volumes ONTAP**的 **Azure VM** 類型

在 Microsoft Azure 中啟動Cloud Volumes ONTAP時，您可以從多種 VM 類型中進行選擇。如果您確定虛擬機器類型太小或太大，無法滿足您的需求，您可以隨時變更虛擬機器類型。

關於此任務

- 必須在Cloud Volumes ONTAP HA 對上啟用自動交還（這是預設）。如果不是，則操作將會失敗。

  "ONTAP 9 文件：用於設定自動交還的命令"

- 變更 VM 類型可能會影響 Microsoft Azure 服務費用。
- 此操作重新啟動Cloud Volumes ONTAP。

  對於單節點系統， I/O 會中斷。

  對於 HA 對來說，這種變化是無中斷的。 HA 對繼續提供數據。

NetApp Console透過啟動接管並等待返回來一次更改一個節點。 NetApp 的品質保證團隊在過程中對檔案的寫入和讀取進行了測試，並且沒有發現客戶端的任何問題。隨著連接的變化，在 I/O 層級觀察到一些重試，但應用層克服了 NFS/CIFS 連接的重新連接。

步驟

1. 在*系統*頁面上，選擇系統。
2. 在「概述」標籤上，按一下「功能」面板，然後按一下「**VM** 類型」旁邊的鉛筆圖示。

   如果您使用的是基於節點的即用即付 (PAYGO) 許可證，則可以透過點擊「許可證類型」旁邊的鉛筆圖示來選擇不同的許可證和 VM 類型。

3. 選擇 VM 類型，選取核取方塊以確認您了解變更的含義，然後按一下「變更」。

結果

Cloud Volumes ONTAP使用新設定重新啟動。

覆寫 **Azure** 中**Cloud Volumes ONTAP HA** 對的 **CIFS** 鎖

組織或帳戶管理員可以在NetApp Console中啟用一項設置，以防止在 Azure 維護事件期間出現Cloud Volumes ONTAP儲存復原問題。啟用此設定後， Cloud Volumes ONTAP將否決 CIFS 鎖定並重設活動的 CIFS 會話。

關於此任務

Microsoft Azure 會安排其虛擬機器的定期維護事件。當Cloud Volumes ONTAP HA 對上發生維護事件時，HA 對會啟動儲存接管。如果在此維護事件期間有活動的 CIFS 會話，則 CIFS 檔案上的鎖定可能會阻止儲存復原。

如果啟用此設置， Cloud Volumes ONTAP將否決鎖定並重置活動的 CIFS 會話。因此，HA 對可以在這些維護事件期間完成儲存恢復。

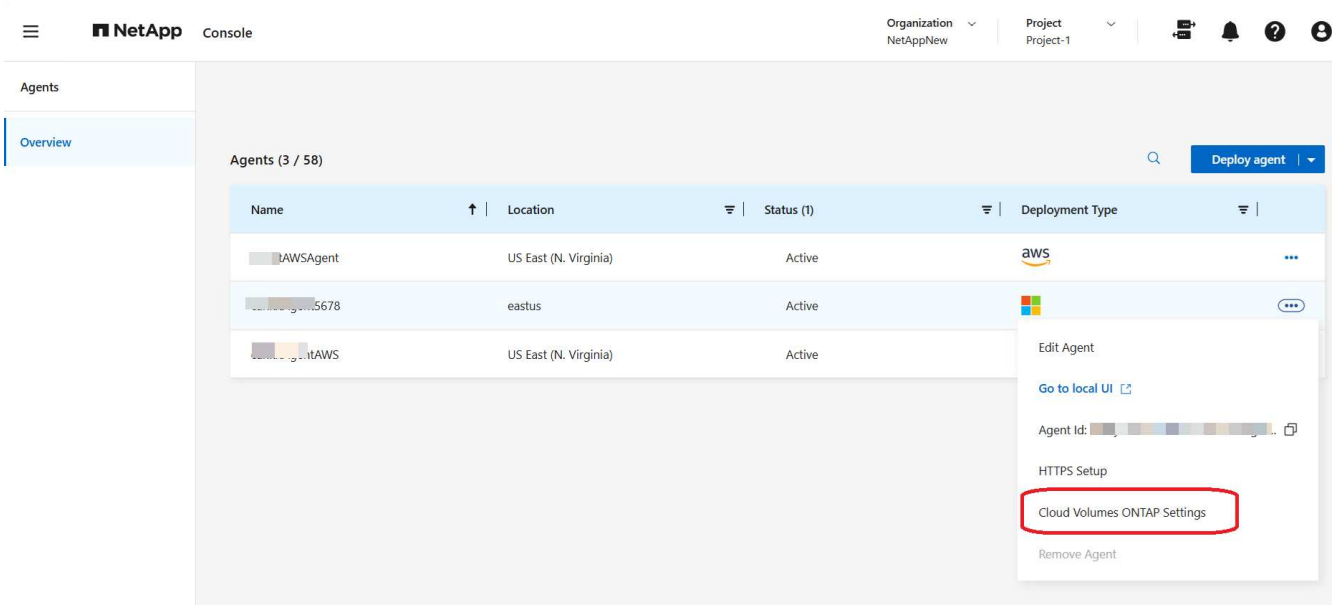
此過程可能會對 CIFS 用戶端造成破壞。 CIFS 用戶端未提交的資料可能會遺失。

開始之前

您需要先建立控制台代理，然後才能變更控制台設定。 "學習使用" 。

步驟

1. 從左側導覽窗格前往*管理>代理*。
2. 點選 ••• 管理Cloud Volumes ONTAP系統的控制台代理的圖示。
3. 選擇* Cloud Volumes ONTAP設定*。



4. 在「Azure」下，按一下「Azure HA 系統的 Azure CIFS 鎖定」。
5. 按一下複選框以啟用該功能，然後按一下“儲存”。

為Cloud Volumes ONTAP系統使用 Azure Private Link 或服務端點

Cloud Volumes ONTAP使用 Azure Private Link 連接到其關聯的儲存帳戶。如果需要，您可以停用 Azure Private Links 並改用服務端點。

概況

預設情況下， NetApp Console啟用 Azure Private Link 來建立Cloud Volumes ONTAP與其關聯儲存帳戶之間的連線。 Azure 專用連結可保護 Azure 中端點之間的連線並提供效能優勢。

如果需要，您可以將Cloud Volumes ONTAP設定為使用服務端點而不是 Azure Private Link。

無論採用哪種配置，控制台始終限制Cloud Volumes ONTAP和儲存帳戶之間的連接的網路存取。網路存取僅限於部署Cloud Volumes ONTAP 的VNet 和部署控制台代理程式的 VNet。

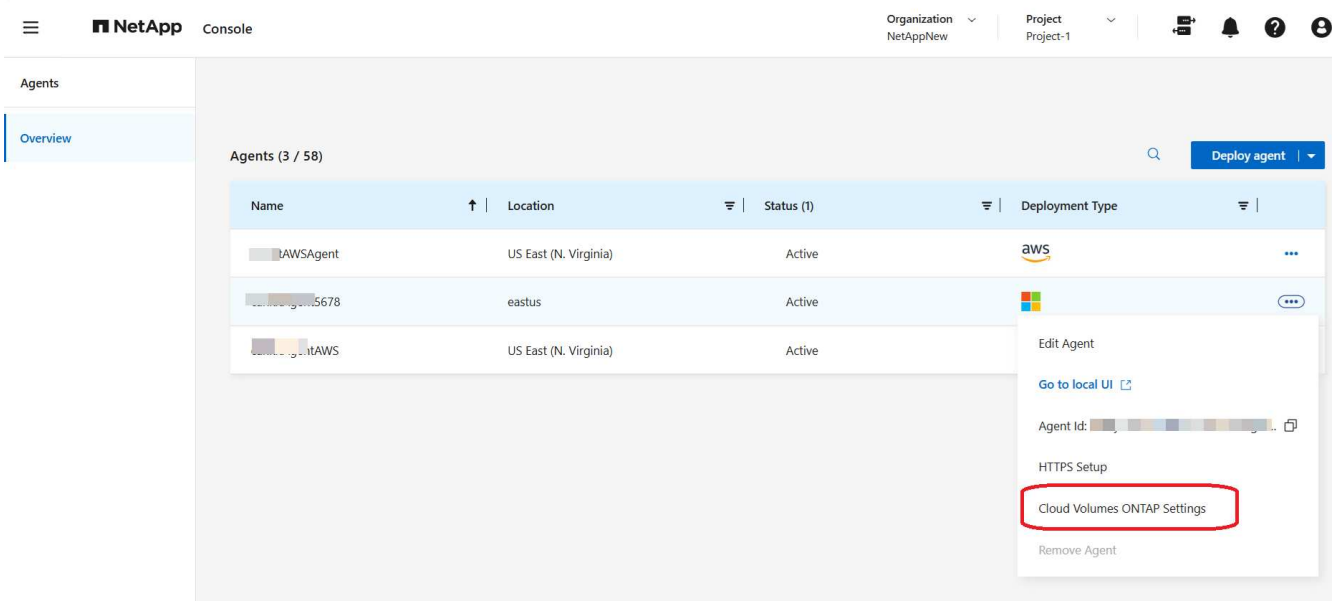
停用 Azure Private Links 並改用服務終點

如果您的業務需要，您可以在控制台中變更設置，以便將Cloud Volumes ONTAP配置為使用服務端點而不是 Azure Private Link。變更此設定適用於您建立的新Cloud Volumes ONTAP系統。服務端點僅支援"Azure 區域對"控制台代理程式和Cloud Volumes ONTAP VNet 之間。

控制台代理應部署在與其管理的Cloud Volumes ONTAP系統相同的 Azure 區域中，或部署在 "Azure 區域對"適用於Cloud Volumes ONTAP系統。

步驟

1. 從左側導覽窗格前往*管理>代理*。
2. 點選 ••• 管理Cloud Volumes ONTAP系統的控制台代理的圖示。
3. 選擇* Cloud Volumes ONTAP設定*。



4. 在「**Azure**」下，按一下「使用 **Azure** 專用連結」。
5. 取消選擇* Cloud Volumes ONTAP和儲存帳戶之間的專用連結連線*。
6. 點選“儲存”。

完成後

如果您停用了 Azure Private Links 且控制台代理程式使用代理伺服器，則必須啟用直接 API 流量。

"了解如何在控制台代理上啟用直接 API 流量"

使用 **Azure Private Links**

在大多數情況下，您無需執行任何操作即可設定與Cloud Volumes ONTAP 的Azure Private 連結。控制台為您管理 Azure 專用連結。但是如果您使用現有的 Azure 私人 DNS 區域，則需要編輯設定檔。

自訂 **DNS** 的要求

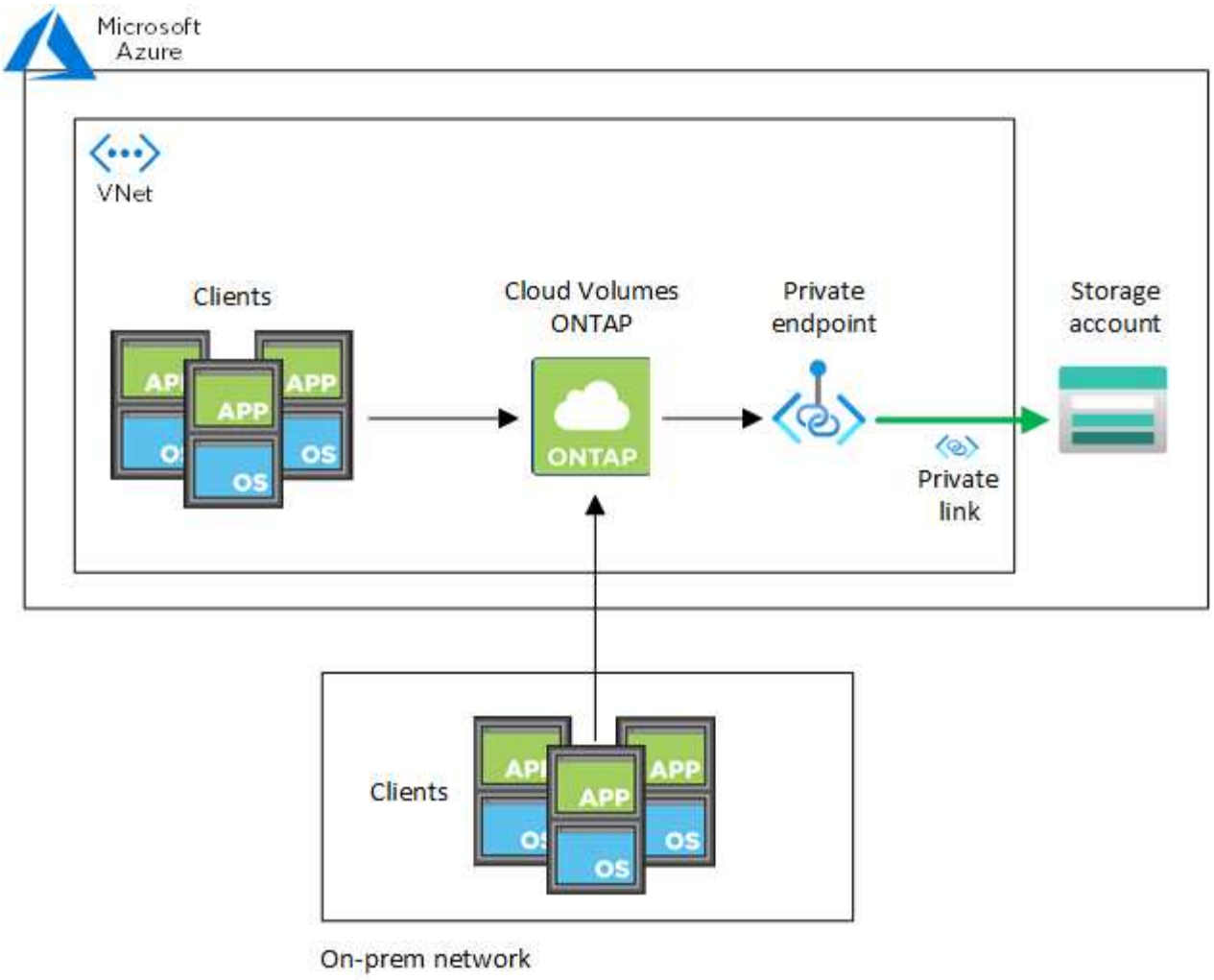
或者，如果您使用自訂 DNS，則需要從自訂 DNS 伺服器建立至 Azure 私人 DNS 區域的條件轉送器。要了解更多信息，請參閱"Azure 關於使用 DNS 轉送器的文檔"。

專用連結連接的工作原理

當控制台在 Azure 中部署Cloud Volumes ONTAP時，它會在資源組中建立一個私有端點。私有端點與Cloud Volumes ONTAP 的儲存帳戶相關聯。因此，對Cloud Volumes ONTAP儲存的存取需要透過 Microsoft 主幹網路。

當客戶端與Cloud Volumes ONTAP位於同一 VNet 內、位於對等 VNet 內或位於本機網路中時，用戶端存取將透過專用連結進行。

以下範例展示了用戶端如何透過專用連結從同一 VNet 內部以及從具有專用 VPN 或 ExpressRoute 連接的本機網路存取。



如果控制台代理程式和Cloud Volumes ONTAP系統部署在不同的 VNet 中，則必須在部署控制台代理程式的 VNet 和部署Cloud Volumes ONTAP系統的 VNet 之間設定 VNet 對等連線。

提供有關 **Azure** 專用 **DNS** 的詳細信息

如果你使用 "Azure 專用 DNS"，那麼就需要在每個Console代理上修改一個設定檔。否則，控制台無法設定Cloud Volumes ONTAP與其關聯儲存帳戶之間的 Azure Private Link 連線。

請注意，DNS 名稱必須符合 Azure DNS 命名要求 "如 Azure 文件所示"。

步驟

1. 透過 SSH 連接到控制台代理主機並登入。
2. 導航至 `/opt/application/netapp/cloudmanager/docker_occm/data`目錄。
3. 編輯 `app.conf`透過添加 `user-private-dns-zone-settings`具有以下關鍵字-值對的參數：

```
"user-private-dns-zone-settings" : {
   "resource-group" : "<resource group name of the DNS zone>",
   "subscription" : "<subscription ID>",
   "use-existing" : true,
   "create-private-dns-zone-link" : true
}
```

這 `subscription`僅當私有 DNS 區域與控制台代理的訂閱不同時才需要關鍵字。

4. 儲存檔案並登出控制台代理程式。

   不需要重新啟動。

啟用故障回滾

如果控制台無法在特定操作中建立 Azure 專用鏈接，它將在沒有 Azure 專用連結連接的情況下完成此操作。建立新系統（單一節點或 HA 對）時，或在 HA 對上執行以下操作時，可能會發生這種情況：建立新聚合、向現有聚合新增磁碟或在超過 32 TiB 時建立新的儲存帳戶。

如果控制台無法建立 Azure 專用鏈接，您可以透過啟用回溯來變更此預設行為。這有助於確保您完全遵守公司的安全規定。

如果啟用回滾，控制台將停止該操作並回滾作為該操作的一部分所建立的所有資源。

您可以透過 API 或更新 app.conf 檔案來啟用回滾。

透過 **API** 啟用回滾

步

1. 使用 `PUT /occm/config`具有以下請求主體的 API 呼叫：

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

透過更新 **app.conf** 啟用回滾

步驟

1. 透過 SSH 連接到控制台代理的主機並登入。
2. 導覽至以下目錄：/opt/application/netapp/cloudmanager/docker_occm/data
3. 編輯 app.conf，新增以下參數和值：

```
 "rollback-on-private-link-failure": true
```

. 儲存檔案並登出控制台代理程式。

不需要重新啟動。

在 **Azure** 控制台中移動**Cloud Volumes ONTAP**的 **Azure** 資源組

Cloud Volumes ONTAP支援 Azure 資源組移動，但工作流程僅在 Azure 控制台中進行。

您可以將Cloud Volumes ONTAP系統從同一 Azure 訂閱內的一個資源群組移至 Azure 中的另一個資源群組。不支援在不同的 Azure 訂閱之間行動資源群組。

步驟

1. 刪除Cloud Volumes ONTAP系統。請參閱"刪除Cloud Volumes ONTAP系統" 。
2. 在 Azure 控制台中執行資源組移動。

   若要完成移動，請參閱"Microsoft Azure 文件中的“將資源移至新的資源群組或訂閱”"。
3. 在*系統*頁面上，發現系統。
4. 在系統資訊中尋找新的資源組。

結果

系統及其資源（虛擬機器、磁碟、儲存帳戶、網路介面、快照）位於新的資源群組中。

在 **Azure** 中隔離**SnapMirror**流量

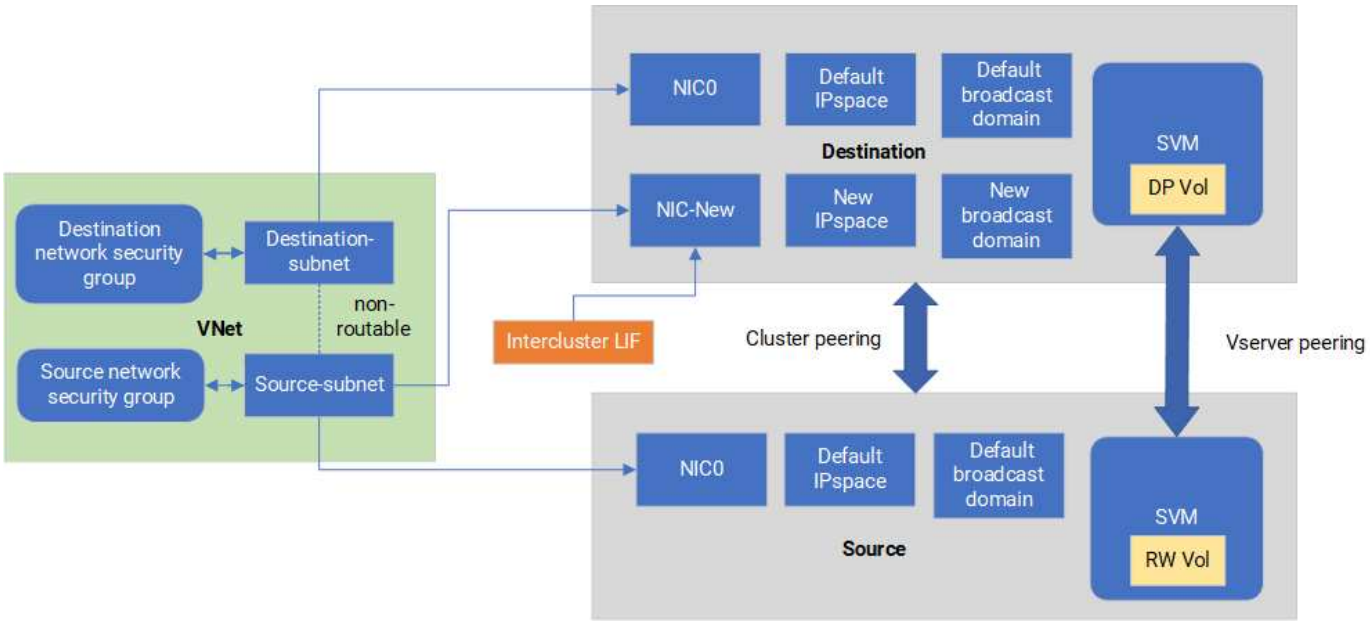
使用 Azure 中的Cloud Volumes ONTAP ，您可以將SnapMirror複製流量與資料和管理流量分開。為了將SnapMirror複製流量與資料流量隔離，您需要新增一個新的網路介面卡 (NIC)、一個相關的群集間 LIF 和一個不可路由的子網路。

關於 **Azure** 中的**SnapMirror**流量隔離

預設情況下， NetApp Console會在相同子網路上設定Cloud Volumes ONTAP部署中的所有 NIC 和 LIF。在這樣的設定中， SnapMirror複製流量和資料和管理流量使用相同的子網路。隔離SnapMirror流量利用了無法路由到用於資料和管理流量的現有子網路的額外子網路。

圖 **1**

下圖顯示了在單一節點部署中，使用附加 NIC、關聯的群集間 LIF 和不可路由子網路對SnapMirror複製流量進行隔離。 HA 對部署略有不同。



開始之前

回顧以下注意事項：

- 您只能向Cloud Volumes ONTAP單節點或 HA 對部署（VM 實例）新增單一 NIC 以實現SnapMirror流量隔離。
- 若要新增新的 NIC，您部署的 VM 實例類型必須具有未使用的 NIC。
- 來源叢集和目標叢集應該可以存取同一個虛擬網路 (VNet)。目標叢集是 Azure 中的Cloud Volumes ONTAP系統。來源叢集可以是 Azure 中的Cloud Volumes ONTAP系統或ONTAP系統。

步驟 1：建立額外的 NIC 並連接到目標 VM

本節提供有關如何建立附加 NIC 並將其附加到目標 VM 的說明。目標 VM 是 Azure 中Cloud Volumes ONTAP中的單節點或 HA 對系統，您要設定額外的 NIC。

步驟

1. 在ONTAP CLI 中，停止節點。

```
dest::> halt -node <dest_node-vm>
```

2. 在 Azure 入口網站中，檢查 VM（節點）狀態是否已停止。

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>
--query instanceView.statuses[1].displayStatus
```

3. 使用 Azure Cloud Shell 中的 Bash 環境停止節點。
   a. 停止節點。

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

b. 解除分配節點。

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-vm>
```

4. 設定網路安全群組規則，讓兩個子網路（來源叢集子網路和目標叢集子網路）互不可達。
   a. 在目標虛擬機器上建立新的 NIC。
   b. 尋找來源叢集子網路的子網路 ID。

```
az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet-name <vnet> --query id
```

   c. 使用來源叢集子網路的子網路 ID 在目標虛擬機器上建立新的 NIC。在這裡輸入新 NIC 的名稱。

```
az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new> --subnet <id_from_prev_command> --accelerated-networking true
```

   d. 保存私有IP位址。此 IP 位址 <new_added_nic_primary_addr> 用於在廣播域，新 NIC 的群集間 LIF。
5. 將新的 NIC 附加到 VM。

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics <dest_node-vm-nic-new>
```

6. 啟動虛擬機器（節點）。

```
az vm start --resource-group <dest_node-rg>  --name <dest_node-vm>
```

7. 在 Azure 入口網站中，前往 網路 並確認新的 NIC（例如 nic-new）存在並且加速網路已啟用。

```
az network nic list --resource-group azure-59806175-60147103-azure-rg --query "[].{NIC: name, VM: virtualMachine.id}"
```

對於 HA 對部署，請對合作夥伴節點重複這些步驟。

步驟 2：為新 NIC 建立新的 IP 空間、廣播域和群集間 LIF

群集間 LIF 的單獨 IP 空間為群集間複製的網路功能提供了邏輯分離。

使用ONTAP CLI 執行以下步驟。

步驟

1. 建立新的 IP 空間（new_ipspace）。

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. 在新的 IP 空間（new_ipspace）上建立廣播網域並新增 nic-new 連接埠。

```
dest::> network port show
```

3. 對於單節點系統，新增連接埠為 *e0b*。對於使用託管磁碟的 HA 配對部署，新增連接埠為 *e0d*。對於使用分頁 Blob 的 HA 配對部署，新增連接埠為 *e0e*。請使用節點名稱，而非 VM 名稱。執行 `node show`以尋找節點名稱。

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. 在新的廣播域 (new_bd) 和新的 NIC (nic-new) 上建立叢集間 LIF。

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-
lif> -service-policy default-intercluster -address
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. 驗證新的集群間 LIF 的建立。

```
dest::> net int show
```

對於 HA 對部署，請對合作夥伴節點重複這些步驟。

步驟 3：驗證來源系統和目標系統之間的叢集對等連接

本節提供有關如何驗證來源系統和目標系統之間的對等關係的說明。

使用ONTAP CLI 執行以下步驟。

步驟

1. 驗證目標群集的群集間 LIF 是否可以對來源群集的群集間 LIF 執行 ping 操作。由於目標群集執行此命令，

因此目標 IP 位址是來源上的群集間 LIF IP 位址。

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
-destination <10.161.189.6>
```

2. 驗證來源集群的集群間 LIF 是否可以 ping 通目標集群的集群間 LIF。目標是在目標上建立的新 NIC 的 IP 位址。

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
<10.161.189.18>
```

對於 HA 對部署，請對合作夥伴節點重複這些步驟。

步驟 4：在來源系統和目標系統之間建立 SVM 對等連接

本節提供如何在來源系統和目標系統之間建立 SVM 對等的說明。

使用ONTAP CLI 執行以下步驟。

步驟

1. 使用來源集群間 LIF IP 位址作為目標在目標上建立集群對等 `-peer-addrs`。對於 HA 對，列出兩個節點的來源群集間 LIF IP 位址作為 `-peer-addrs`。

```
dest::> cluster peer create -peer-addrs <10.161.189.6> -ipspace
<new_ipspace>
```

2. 輸入並確認密碼。
3. 使用目標群集 LIF IP 位址作為來源群集的 IP 位址，在來源上建立群集對等連接 `peer-addrs`。對於 HA 對，列出兩個節點的目標群集間 LIF IP 位址作為 `-peer-addrs`。

```
src::> cluster peer create -peer-addrs <10.161.189.18>
```

4. 輸入並確認密碼。
5. 檢查集群是否對等。

```
src::> cluster peer show
```

成功的對等連線在可用性欄位中顯示 可用。

6. 在目標上建立 SVM 對等連線。來源 SVM 和目標 SVM 都應該是資料 SVM。

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm>
-peer-cluster <src_cluster> -applications snapmirror``
```

7. 接受 SVM 對等連線。

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. 檢查 SVM 是否已對等。

```
dest::> vserver peer show
```

同行國家顯示*peered* 和對等應用程式顯示*snapmirror*.

步驟 5：在來源系統和目標系統之間建立SnapMirror複製關係

本節提供如何在來源系統和目標系統之間建立SnapMirror複製關係的說明。

要移動現有的SnapMirror複製關係，必須先中斷現有的SnapMirror複製關係，然後再建立新的SnapMirror複製關係。

使用ONTAP CLI 執行以下步驟。

步驟

1. 在目標 SVM 上建立資料保護磁碟區。

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. 在目標上建立SnapMirror複製關係，其中包括複製的SnapMirror策略和計劃。

```
dest::> snapmirror create -source-path src_svm:src_vol  -destination
-path  dest_svm:new_dest_vol -vserver dest_svm -policy
MirrorAllSnapshots -schedule 5min
```

3. 在目標上初始化SnapMirror複製關係。

```
dest::> snapmirror initialize -destination-path  <dest_svm:new_dest_vol>
```

4. 在ONTAP CLI 中，透過執行以下命令驗證SnapMirror關係狀態：

```
dest::> snapmirror show
```

關係狀態是 `Snapmirrored`關係的健康是 `true`。

5. 可選：在ONTAP CLI 中，執行以下命令查看SnapMirror關係的操作記錄。

```
dest::> snapmirror show-history
```

或者，您可以掛載來源磁碟區和目標卷，將檔案寫入來源卷，並驗證磁碟區是否複製到目標磁碟區。

Google Cloud 管理

變更Cloud Volumes ONTAP的 Google Cloud 機器類型

在 Google Cloud 中啟動Cloud Volumes ONTAP時，您可以從多種機器類型中進行選擇。如果您確定實例或機器類型太小或太大，無法滿足您的需求，您可以隨時變更執行個體或機器類型。

關於此任務

- 必須在Cloud Volumes ONTAP HA 對上啟用自動交還（這是預設）。如果不是，則操作將會失敗。

  "ONTAP 9 文件：用於設定自動交還的命令"

- 更改機器類型可能會影響 Google Cloud 服務費用。
- 此操作重新啟動Cloud Volumes ONTAP。

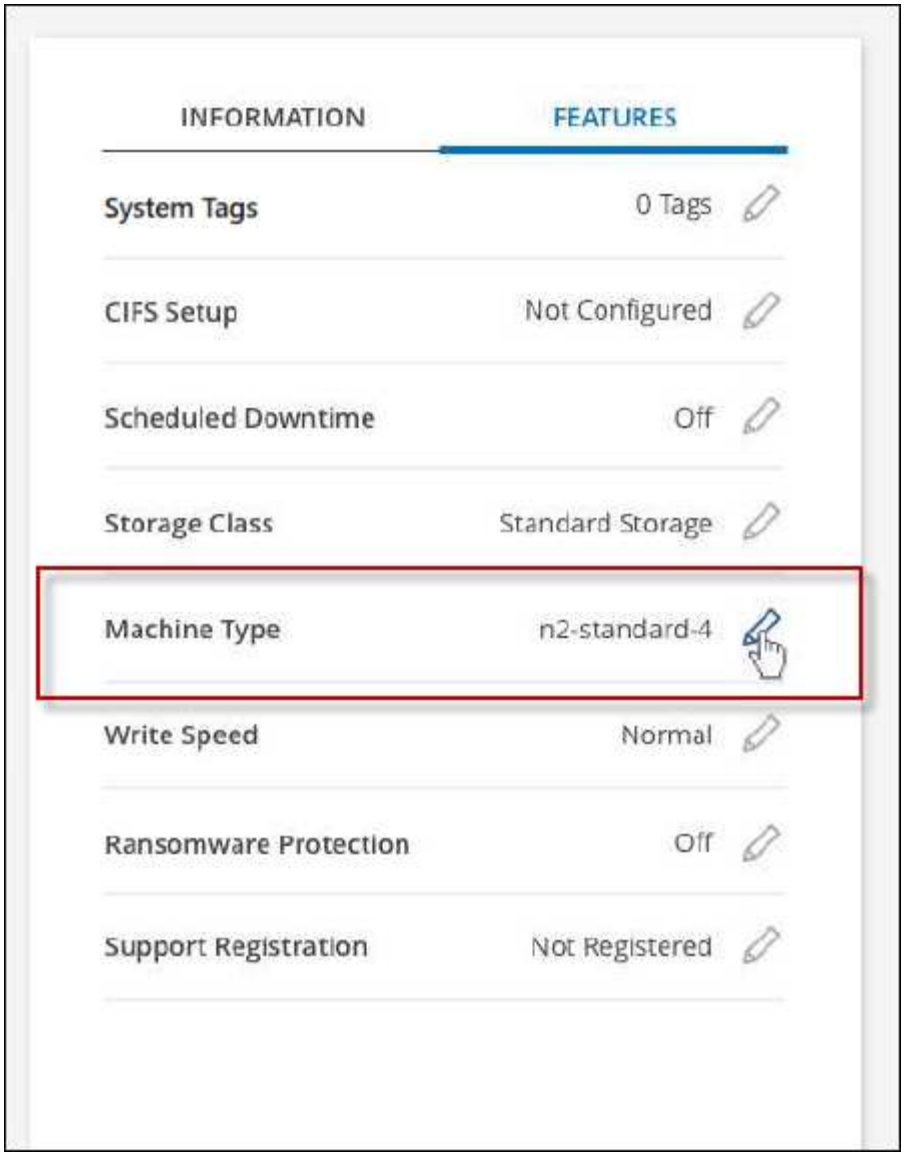
  對於單節點系統， I/O 會中斷。

  對於 HA 對來說，這種變化是無中斷的。 HA 對繼續提供數據。

NetApp Console透過啟動接管並等待返回來一次更改一個節點。 NetApp 的品質保證團隊在過程中對檔案的寫入和讀取進行了測試，並且沒有發現客戶端的任何問題。隨著連接的變化，在 I/O 層級觀察到一些重試，但應用層克服了 NFS/CIFS 連接的重新連接。

步驟

1. 在*系統*頁面上，選擇系統。
2. 在概覽標籤上，按一下功能面板，然後按一下*機器類型*旁邊的鉛筆圖示。



如果您使用的是基於節點的即用即付 (PAYGO) 許可證，則可以透過點擊「許可證類型」旁邊的鉛筆圖示來選擇不同的許可證和機器類型。

1. 選擇機器類型，選取核取方塊以確認您了解變更的含義，然後按一下*變更*。

結果

Cloud Volumes ONTAP使用新設定重新啟動。

將現有的 **Cloud Volumes ONTAP** 部署轉換為 **Infrastructure Manager**

自 2026 年 2 月 9 日起，Google Cloud 中新的 Cloud Volumes ONTAP 部署可以使用 Google Cloud Infrastructure Manager。Google 即將棄用 Google Cloud Deployment Manager，改用 Infrastructure Manager。因此，您需要手動執行遷移工具，將現有的 Cloud Volumes ONTAP 部署從 Deployment Manager 遷移到 Infrastructure Manager。此程序只需執行一次，之後您的系統將自動開始使用 Infrastructure Manager。

關於此任務

過渡工具可在 "NetApp 支援網站"中使用，並建立下列工件：

- Terraform 工件，儲存於 `conversion_output/deployment_name`。
- 轉換摘要，已儲存於 `conversion_output/batch_summary_<deployment_name>_<timestamp>.json`.
- 偵錯記錄儲存在 `<gcp project number>-<region>-blueprint-config/<cvo name>` 目錄中。您需要這些記錄進行疑難排解。 `<gcp project number>-<region>-blueprint-config` 儲存貯體儲存 Terraform 記錄。

> 使用 Infrastructure Manager 的 Cloud Volumes ONTAP 系統會將資料和記錄儲存在 Google Cloud Storage 儲存桶中。這些儲存桶可能會產生額外費用，但請勿編輯或刪除儲存桶及其內容：
>
> - `gs://netapp-cvo-infrastructure-manager-<project id>`：用於新的 Cloud Volumes ONTAP 部署的 ONTAP 版本和 SVM Terraform 範本。在此內， `dm-to-im-convert` 儲存桶包含 Cloud Volumes ONTAP Terraform 檔案。
> - `<gcp project number>-<region>-blueprint-config`：用於儲存 Google Cloud Terraform 工件。

開始之前

- 請確保您的 Cloud Volumes ONTAP 系統版本為 9.16.1 或更高版本。
- 確保沒有透過 Google Cloud Console 手動編輯過任何 Cloud Volumes ONTAP 資源或其屬性。
- 請確保已啟用 Google Cloud API。請參閱 "啟用 Google Cloud API"。請確保除了其他 API 之外，還啟用了 Google Cloud Quotas API。
- 請確認 NetApp Console agent 的服務帳戶擁有所有必要的權限。請參閱 "控制台代理的 Google Cloud 權限"。

  對於私有模式部署，請確保滿足下列附加前提條件：

  - 請確保您已安裝最新版本的 Console 代理程式。從 NetApp Support Site 下載產品安裝程式，然後手動將代理程式安裝到您的主機上，以便代理程式可以使用 Infrastructure Manager API。
  - 如果您以私有模式執行該工具，請確保除了其他 API 之外，還啟用了 Cloud Build API "啟用 Google Cloud API"。
  - 請確保您已完成網路配置並為私有模式部署建立了工作池。請參閱 "私有模式部署的 Infrastructure Manager 組態"。

- 轉換工具使用以下網域。在您的網路中於連接埠 443 上啟用它們：

網域	港口	協定	方向	目的
cloudresourcemanager.googleapis.com	443	TCP	外傳	專案驗證
deploymentmanager.googleapis.com	443	TCP	外傳	部署探索

網域	港口	協定	方向	目的
config.googleapis.com	443	TCP	外傳	Infrastructure Manager API
storage.googleapis.com	443	TCP	外傳	GCS 儲存貯體作業
iam.googleapis.com	443	TCP	外傳	服務帳戶驗證
compute.googleapis.com	443	TCP	外傳	Google Cloud 和 Terraform Import 與 Plan 使用的運算 API 呼叫
cloudbuild.googleapis.com	443	TCP	外傳	僅私有模式需要建置操作
openidconnect.googleapis.com	443	TCP	外傳	驗證
oauth2.googleapis.com	443	TCP	外傳	OAuth2 權杖交換
registry.terraform.io	443	TCP	外傳	Terraform 提供者登錄
releases.hashicorp.com	443	TCP	外傳	Terraform 二進位下載
apt.releases.hashicorp.com	443	TCP	外傳	HashiCorp APT 存儲庫
us-central1-docker.pkg.dev	443	TCP	外傳	GCP Artifact Registry
metadata.google.internal	80	HTTP	內部	VM 元資料和驗證權杖
pypi.org	443	TCP	外傳	Python 套件索引
files.pythonhosted.org	443	TCP	外傳	Python 套件下載
checkpoint-api.hashicorp.com	443	TCP	外傳	Terraform 版本檢查
download.docker.com	443	TCP	外傳	Docker APT 儲存庫
security.ubuntu.com	80/443	TCP	外傳	Ubuntu 安全更新
*.gce.archive.ubuntu.com	80	TCP	外傳	Ubuntu 軟體包鏡像

準備執行工具的環境

執行工具之前，請先執行這些步驟。

步驟

1. 建立角色並將其附加到服務帳戶：
   a. 建立具有下列權限的 YAML 檔案：

```
title: NetApp Dm TO IM Convert Solution
description: Permissions for the service account associated with the
VM where the tool will run.
stage: GA
includedPermissions:
- compute.addresses.get
- compute.disks.get
- compute.forwardingRules.get
- compute.healthChecks.get
- compute.instanceGroups.get
- compute.instances.get
- compute.regionBackendServices.get
- config.deployments.create
- config.deployments.get
- config.deployments.getLock
- config.deployments.lock
- config.deployments.unlock
- config.deployments.update
- config.deployments.delete
- config.deployments.updateState
- config.operations.get
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- iam.serviceAccounts.get
- storage.buckets.create
- storage.objects.create
- storage.objects.delete
- storage.objects.get
- storage.objects.list
```

      為私有模式部署新增額外權限

      如果您以私有模式執行該工具，請同時將 `cloudbuild.workerpools.get` 權限新增至 YAML 檔案。

   b. 在 Google Cloud 中建立自訂角色，並賦予其 YAML 檔案中定義的權限。
      `gcloud iam roles create dmtoim_convert_tool_role --project=PROJECT_ID \
      --file=YAML_FILE_PATH`如需詳細資訊，請參閱 "建立和管理自訂角色"。
   c. 將自訂角色附加到您將用於建立 VM 的服務帳戶。
   d. 將 `roles/iam.serviceAccountUser`角色新增至此服務帳戶。請參閱 "服務帳戶概覽"。

2. 建立一個具有以下組態的 VM 。您可以在此 VM 上執行此工具。
   - 機器類型：Google Compute Engine 機器類型 e2-medium
   - 作業系統：根據您的需求、選擇以下任一映像：
     - Ubuntu 25.10 AMD64 Minimal（映像：ubuntu-minimal-2510-amd64）
     - SUSE Linux Enterprise Server 15 SP7 x86_64
   - 網路：防火牆允許 HTTP 和 HTTPs
   - 磁碟大小：20GB
   - 安全性：服務帳戶：您建立的服務帳戶
   - 安全性：存取範圍 - 為每個 API 設定存取權限：
     - 雲端平台：已啟用
     - Compute Engine ：唯讀
     - 儲存：唯讀 （預設）
     - Google Cloud Logging（以前稱為 Stackdriver Logging）API：僅寫入（預設）
     - Stackdriver Monitoring（現為 Google Cloud Operations 的一部分）API：僅寫入（預設）
     - 服務管理：唯讀 （預設）
     - 服務控制：已啟用 （預設）
     - Google Cloud Trace（以前稱為 Stackdriver Trace）：僅寫入（預設）
3. 使用 SSH 連線至新建立的 VM： `gcloud compute ssh dmtoim-convert-executor-vm --zone <region where VM is deployed>`
4. 使用您的 NSS 憑證從 "NetApp 支援網站"下載轉換工具： `wget <download link from NetApp Support site>`
5. 解壓縮下載的 TAR 檔： `unzip <downloaded file name>`

Ubuntu

1. 下載並安裝以下必備套件：
   - Docker：28.2.2 build 28.2.2-0ubuntu1 或更新版本
   - Terraform：1.14.1 或更高版本
   - Python：3.13.7、python3-pip、python3 venv

   ```
   sudo apt-get update
   sudo apt-get install python3-pip python3-venv -y
   wget -O - https://apt.releases.hashicorp.com/gpg | sudo gpg
   --dearmor -o /usr/share/keyrings/hashicorp-archive-keyring.gpg
   echo "deb [arch=$(dpkg --print-architecture) signed-
   by=/usr/share/keyrings/hashicorp-archive-keyring.gpg]
   https://apt.releases.hashicorp.com noble main" | sudo tee
   /etc/apt/sources.list.d/hashicorp.list
   sudo apt update && sudo apt install terraform
   sudo apt-get install -y docker.io
   sudo systemctl start docker
   ```

   Google Cloud CLI `gcloud` 已預先安裝在虛擬機器上。

SUSE Linux Enterprise Server

1. 設定 Python： `sudo update-alternatives --install /usr/bin/python3 python3 /usr/bin/python3.11 2`
2. 安裝 pip3 以安裝套件： `python3.11 -m ensurepip --upgrade`
3. 安裝 Terraform：

   ```
   wget
   https://releases.hashicorp.com/terraform/1.7.4/terraform_1.7.4_linux
   _amd64.zip
   unzip terraform_1.7.4_linux_amd64.zip
   sudo mv terraform /usr/local/bin/
   rm terraform_1.7.4_linux_amd64.zip
   ```

4. 安裝 Google Cloud SDK（gcloud）

   ```
   curl https://sdk.cloud.google.com | bash
   exec -l $SHELL
   ```

執行轉換工具

這些步驟適用於 Ubuntu 和 SUSE Linux Enterprise Server 上執行轉換工具。

步驟

1. 將目前使用者新增至 Docker 群組，以便工具無需 `sudo` 權限即可使用 Docker。

```
sudo usermod -aG docker $USER
newgrp docker
```

2. 安裝轉換工具：

```
cd <folder where you extracted the tool>
 ./install.sh
```

這會將工具安裝在隔離的環境中 `dmconvert-venv`，並驗證是否已安裝所有必要的軟體套件。

3. 輸入工具的安裝環境： `source dmconvert-venv/bin/activate`
4. 以 `non-sudo`使用者身分執行轉換工具。確保使用與 Console 代理的服務帳戶相同的服務帳戶，並且該服務帳戶擁有所有 "Google Cloud Infrastructure Manager 所需的權限"。

```
dmconvert \
--project-id=<the Google Cloud project ID for the Cloud Volumes ONTAP
deployment> \
--cvo-name=<Cloud Volumes ONTAP system name> \
--service-account=<the service account attached to the Console agent>
```

在私有模式部署中執行該工具

指定 `--worker-pool` 參數以在私有模式部署中執行該工具。有關工作池配置，請參閱 "私有模式部署的 Infrastructure Manager 組態"。

```
dmconvert \
--project-id=<the Google Cloud project ID for the Cloud Volumes
ONTAP deployment> \
--cvo-name=<Cloud Volumes ONTAP system name> \
--service-account=<the service account attached to the Console
agent> \
--worker-pool=<worker pool name>
```

完成後

此工具會顯示所有 Cloud Volumes ONTAP 系統及其 SVM 詳細資訊的清單。運行完成後，您可以查看所有已轉

換系統的狀態。每個已轉換的系統都會以 *<system-name-imdeploy>* 格式顯示在 Google Console 的 Infrastructure Manager 下，表示 Console 現在使用 Infrastructure Manager API 來管理該 Cloud Volumes ONTAP 系統。

> 轉換完成後，請勿在 Google Cloud Console 中刪除 Deployment Manager 的部署物件。此部署物件包含您可能需要用來回滾已轉換系統的資訊。

如果需要回滾轉換，則必須使用同一台虛擬機器。如果已轉換所有系統且無需回滾到 Deployment Manager，則可以刪除該虛擬機器。

復原轉換

如果您不想繼續轉換，可以按照以下步驟回溯到 Deployment Manager：

步驟

1. 在同一個 您為執行該工具而建立的 VM 上，執行以下命令：

```
dmconvert \
--project-id=<the Google Cloud project ID for the Cloud Volumes ONTAP
deployment> \
--cvo-name=<Cloud Volumes ONTAP system name> \
--service-account=<the service account attached to the Console agent> \
--rollback
```

2. 請等待復原完成。

相關連結

- "NetApp Console Agent 4.2.0 發行說明"
- "Google Cloud Infrastructure Manager 所需的權限"

使用系統管理員管理Cloud Volumes ONTAP

Cloud Volumes ONTAP中的高階儲存管理功能可透過ONTAP系統管理器 (ONTAP System Manager) 使用，它是ONTAP系統提供的管理介面。您可以直接從NetApp Console存取系統管理員。

特徵

您可以使用控制台中的ONTAP系統管理員執行各種儲存管理功能。以下列表包含其中一些功能，但並不詳盡：

- 進階儲存管理：管理一致性群組、共用、qtree、配額和儲存虛擬機器。
- 成交量變動： "將磁碟區移動到不同的聚合。"
- 網路管理：管理 IP 空間、網路介面、連接埠集和乙太網路連接埠。
- 管理FlexGroup磁碟區：您只能透過系統管理員建立和管理FlexGroup磁碟區。 BlueXP控制台不支援FlexGroup磁碟區建立。

- 事件和作業：查看事件日誌、系統警報、作業和稽核日誌。
- 進階資料保護：保護儲存虛擬機器、LUN 和一致性群組。
- 主機管理：設定 SAN 啟動器群組和 NFS 用戶端。
- ONTAP S3 物件儲存管理：Cloud Volumes ONTAP 中的 ONTAP S3 儲存管理功能僅在 System Manager 中可用，而不在 Console 中可用。

支援的配置

- 標準雲端區域中的Cloud Volumes ONTAP 9.10.0 及更高版本可透過ONTAP System Manager 進行進階儲存管理。
- GovCloud 區域或沒有出站網路存取的區域不支援系統管理員整合。

限制

Cloud Volumes ONTAP不支援系統管理器介面中顯示的一些功能：

- NetApp Cloud Tiering： Cloud Volumes ONTAP不支援 Cloud Tiering。建立磁碟區時，您應該直接從標準視圖設定資料分層到物件儲存。
- 層級：系統管理員不支援聚合管理（包括本機層級和雲端層級）。您必須直接從標準視圖管理聚合。
- 韌體升級： Cloud Volumes ONTAP不支援從系統管理員的 叢集 **>** 設定 頁面進行自動韌體更新。
- 基於角色的存取控制：系統管理員不支援基於角色的存取控制。
- SMB 持續可用性 (CA)： Cloud Volumes ONTAP不支援 "持續可用的 SMB 共享"實現無中斷運作。

配置存取系統管理員的身份驗證

身為管理員，您可以為從控制台存取ONTAP系統管理員的使用者啟動身份驗證。您可以根據ONTAP使用者角色確定正確的存取權限級別，並根據需要啟用或停用身份驗證。如果啟用身份驗證，則使用者每次從控制台存取系統管理員或重新載入頁面時都需要輸入其ONTAP使用者憑證，因為控制台不會在內部儲存憑證。如果您停用身份驗證，使用者可以使用管理員憑證存取系統管理員。

此設定適用於您組織或帳戶中的ONTAP使用者的每個控制台代理，無論Cloud Volumes ONTAP系統為何。

所需權限

您需要指派組織或帳戶管理員權限才能修改Cloud Volumes ONTAP使用者驗證的控制台代理設定。

步驟

1. 從左側導覽窗格前往*管理>代理*。
2. 點選 ••• 所需控制台代理的圖示並選擇*編輯控制台代理*。
3. 在*強制使用者憑證*下，選取*啟用/停用*複選框。預設情況下，身份驗證是禁用的。

   如果將此值設為*啟用*，則身份驗證將會重置，並且您必須修改任何現有工作流程以適應此變更。

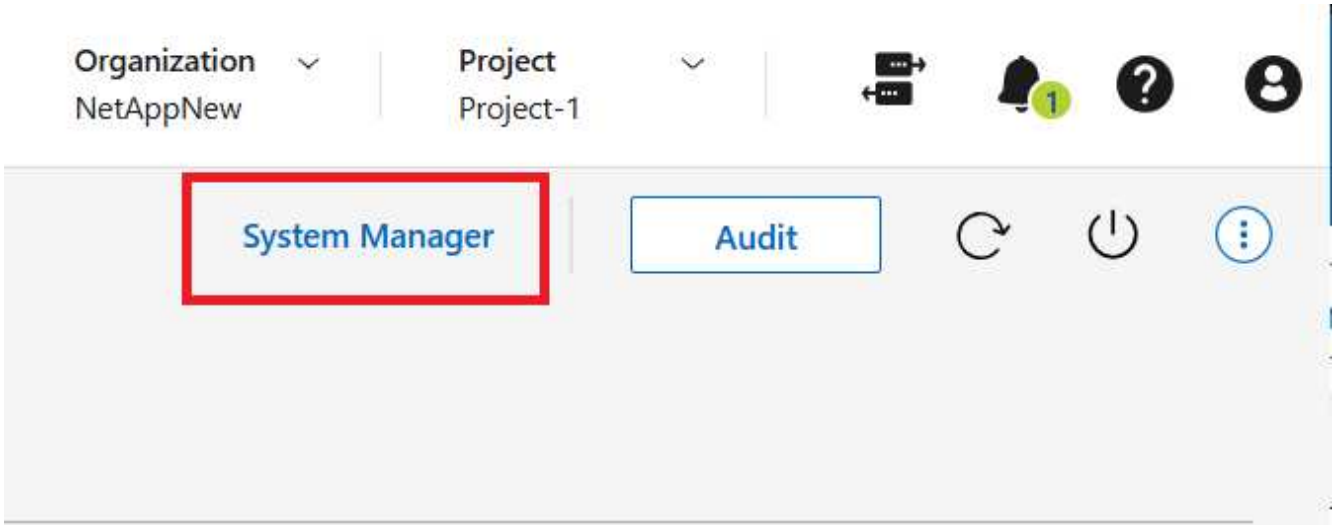
4. 點選“儲存”。

開始使用系統管理員

您可以從Cloud Volumes ONTAP系統存取ONTAP System Manager。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，雙擊所需的Cloud Volumes ONTAP系統。
3. 按一下“系統管理員”。



4. 如果出現提示，請輸入您的ONTAP使用者憑證並點擊 登入。
5. 如果出現確認訊息，請仔細閱讀並按一下「關閉」。

使用系統管理員來管理您的Cloud Volumes ONTAP系統。您可以按一下「返回」返回控制台。

有關使用系統管理員的協助

如果您需要使用 System Manager 和Cloud Volumes ONTAP 的協助，您可以參考 "ONTAP文檔"以獲得逐步說明。以下是一些可能有幫助的ONTAP文件連結：

- "ONTAP角色、應用程式和身份驗證"
- "使用 System Manager 存取叢集" 。
- "捲和 LUN 管理"
- "網管"
- "資料保護"
- "建立持續可用的 SMB 共享"

從 CLI 管理Cloud Volumes ONTAP

Cloud Volumes ONTAP CLI 讓您能夠執行所有管理命令，對於高階任務或您喜歡使用 CLI 來說，它是一個不錯的選擇。您可以使用安全外殼 (SSH) 連接到 CLI。

開始之前

使用 SSH 連線到Cloud Volumes ONTAP 的主機必須具有與Cloud Volumes ONTAP 的網路連線。例如，您可能需要從雲端供應商網路中的跳轉主機進行 SSH。

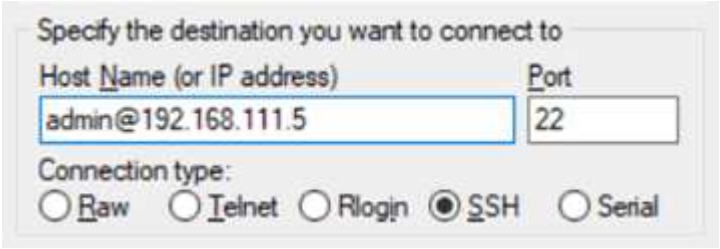
當部署在多個 AZ 中時， Cloud Volumes ONTAP HA 配置使用浮動 IP 位址作為叢集管理接口，這表示外部路由不可用。您必須從屬於相同路由域的主機進行連線。

步驟

1. 在NetApp Console中，確定叢集管理介面的 IP 位址：
   a. 從左側導覽功能表中，選擇“儲存”>“管理”。
   b. 在*系統*頁面上，選擇Cloud Volumes ONTAP系統。
   c. 複製右側窗格中顯示的叢集管理 IP 位址。
2. 使用 SSH 使用管理員帳戶連線到叢集管理介面 IP 位址。

   例子

   下圖顯示了使用 PuTTY 的範例：



3. 在登入提示字元下，輸入管理員帳戶的密碼。

   例子

```
Password: ********
COT2::>
```

系統健康和事件

驗證**Cloud Volumes ONTAP** 的**AutoSupport**設置

AutoSupport主動監控系統的健康狀況並向NetApp技術支援發送訊息。預設情況下，每個節點上都啟用AutoSupport ，以使用 HTTPS 傳輸協定向技術支援發送訊息。最好驗證AutoSupport是否可以發送這些訊息。

唯一需要的設定步驟是確保Cloud Volumes ONTAP具有外部網路連線。有關詳細信息，請參閱您的雲端提供者的網路要求。

AutoSupport要求

Cloud Volumes ONTAP節點需要NetApp AutoSupport的出站互聯網存取權限，它可以主動監控系統的健康狀況並向NetApp技術支援發送訊息。

路由和防火牆策略必須允許 HTTPS 流量到達下列端點，以便Cloud Volumes ONTAP可以傳送AutoSupport訊息：

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

如果沒有可用的出站網路連線來傳送AutoSupport訊息， NetApp Console會自動設定您的Cloud Volumes ONTAP系統以使用控制台代理程式作為代理伺服器。唯一的要求是確保控制台代理的安全群組允許透過連接埠 3128 進行入站連線。部署控制台代理程式後，您需要開啟此連接埠。

如果您為Cloud Volumes ONTAP定義了嚴格的出站規則，那麼您還需要確保Cloud Volumes ONTAP安全群組允許透過連接埠 3128 進行出站連線。

如果您使用 HA 對，則 HA 中介不需要外部網路存取。

驗證出站網路存取可用後，您可以測試AutoSupport以確保它可以發送訊息。有關說明，請參閱 "ONTAP文檔：設定AutoSupport"。

排除AutoSupport配置故障

如果出站連線不可用，且控制台無法設定您的Cloud Volumes ONTAP系統以使用控制台代理程式作為代理伺服器，您將收到來自控制台的通知，提示您的系統無法傳送AutoSupport訊息。請依照以下步驟解決此問題。

步驟

1. 使用 SSH 安全地連接到Cloud Volumes ONTAP系統，以使用ONTAP CLI。

   "了解如何透過 SSH 連線到Cloud Volumes ONTAP" 。

2. 查看AutoSupport子系統的詳細狀態：

   ```
   autosupport check show-details
   ```

   回覆內容如下：

```
    Category: smtp
          Component: mail-server
             Status: failed
             Detail: SMTP connectivity check failed for destination:
                     mailhost. Error: Could not resolve host -
'mailhost'
            Corrective Action: Check the hostname of the SMTP server

    Category: http-https
        Component: http-put-destination
            Status: ok
            Detail: Successfully connected to:
                    <https://support.netapp.com/put/AsupPut/>.

          Component: http-post-destination
             Status: ok
             Detail: Successfully connected to:

https://support.netapp.com/asupprod/post/1.0/postAsup.

    Category: on-demand
          Component: ondemand-server
             Status: ok
             Detail: Successfully connected to:
                     https://support.netapp.com/aods/asupmessage.

    Category: configuration
            Component: configuration
                Status: ok
                Detail: No configuration issues found.
    5 entries were displayed.
```

如果 http-https 類別的狀態是 `OK` 這表示AutoSupport已正確配置，可以發送訊息。

3. 否則，請驗證每個Cloud Volumes ONTAP節點的代理 URL：

   ```
   autosupport show -fields proxy-url
   ```

4. 如果代理 URL 參數為空，請設定Cloud Volumes ONTAP以使用控制台代理作為代理：

   ```
   autosupport modify -proxy-url http://<console agent private ip>:3128
   ```

5. 再次確認AutoSupport狀態：

   ```
   autosupport check show-details
   ```

6. 如果狀態仍然失敗，請驗證Cloud Volumes ONTAP和控制台代理之間是否透過連接埠建立連線。 `3128`。

7. 如果驗證後狀態仍然失敗，請透過 SSH 連線至控制台代理程式。

   "了解有關控制台代理連接到 Linux VM 的更多信息"

8. 前往 `/opt/application/netapp/cloudmanager/docker_occm/data/`。
9. 開啟代理設定檔 `squid.conf`。這是文件的結構：

```
        http_port 3128
        acl netapp_support dst support.netapp.com
        http_access allow netapp_support
        request_header_max_size 21 KB
        reply_header_max_size 21 KB
        http_access deny all
        httpd_suppress_version_string on
```

10. 如果您的檔案中沒有Cloud Volumes ONTAP系統的 CIDR 區塊條目，請新增條目並允許存取：

    `acl cvonet src <cidr>`

    `http_access allow cvonet`

    以下是一個例子：

```
        http_port 3128
        acl netapp_support dst support.netapp.com
        acl cvonet src <cidr>
        http_access allow netapp_support
        http_access allow cvonet
        request_header_max_size 21 KB
        reply_header_max_size 21 KB
        http_access deny all
        httpd_suppress_version_string on
```

11. 編輯設定檔後，重啟代理容器。 `sudo`。然後，根據您使用的是 Docker 還是 Podman，執行以下命令：

    對於 Docker，請運行 `docker restart squid`。

    如果您使用的是 Podman，請執行 `podman restart squid`。

12. 傳回ONTAP CLI 並驗證Cloud Volumes ONTAP是否可以傳送AutoSupport訊息：

    `autosupport check show-details`

相關連結

- "AWS 中Cloud Volumes ONTAP的網路需求"

- "Azure 中Cloud Volumes ONTAP的網路需求"
- "Google Cloud 中Cloud Volumes ONTAP的網路需求"

為Cloud Volumes ONTAP系統設定 EMS

事件管理系統 (EMS) 收集並顯示有關ONTAP系統上發生的事件的資訊。若要接收事件通知，您可以為特定事件嚴重性設定事件目的地（電子郵件地址、SNMP 陷阱主機或系統日誌伺服器）和事件路由。

您可以使用 CLI 設定 EMS。有關說明，請參閱 "ONTAP文件：EMS 配置概述"。

概念

授權

Cloud Volumes ONTAP許可

Cloud Volumes ONTAP有多種授權選項。每個選項都可以讓您選擇符合您需求的消費模式。

許可概述

新客戶可以使用以下授權選項。

基於容量的許可

按配置容量支付NetApp帳戶中的多個Cloud Volumes ONTAP系統的費用。包括購買附加雲端資料服務的能力。有關基於容量的許可證的消費模式或購買選項的更多信息，請參閱："了解有關基於容量的許可證的更多信息" 。

Keystone訂閱

一種按需付費的訂閱式服務，為高可用性 (HA) 對提供無縫的混合雲體驗。

以下部分提供了有關每個選項的更多詳細資訊。

對於未經許可而使用許可的功能，我們將不提供支援。

基於容量的許可

基於容量的許可包可讓您按 TiB 容量支付Cloud Volumes ONTAP費用。該許可證與您的NetApp帳戶相關聯，只要許可證提供足夠的容量，您就可以根據許可證為多個系統收費。

例如，您可以購買單一 20 TiB 許可證，部署四個Cloud Volumes ONTAP系統，然後為每個系統指派一個 5 TiB 卷，總共 20 TiB。此容量可供該帳戶中部署的每個Cloud Volumes ONTAP系統上的磁碟區使用。

基於容量的許可以_包_的形式提供。部署Cloud Volumes ONTAP系統時，您可以根據業務需求從多個授權包中進行選擇。

雖然NetApp Console中管理的產品和服務的實際使用情況和計量始終以 GiB 和 TiB 計算，但 GB/GiB 和 TB/TiB 這兩個術語可互換使用。這反映在雲端市場列表、價格報價、列表描述和其他支援文件中。

套餐

以下基於容量的軟體包可用於Cloud Volumes ONTAP。有關基於容量的許可證包的更多信息，請參閱"了解有關基於容量的許可證的更多信息"。

有關以下基於容量的套件所支援的 VM 類型的列表，請參閱：

- "Azure 中支援的配置"

- "Google Cloud 中支援的配置"

免費增值

免費提供NetApp提供的所有Cloud Volumes ONTAP功能（仍需支付雲端供應商費用）。免費增值套餐有以下特點：

- 不需要許可證或合約。
- 不包括來自NetApp的支援。
- 每個Cloud Volumes ONTAP系統的設定容量限制為 500 GiB。
- 對於任何雲端供應商，每個NetApp帳戶最多可以使用 10 個Cloud Volumes ONTAP系統和免費加值服務。
- 如果Cloud Volumes ONTAP系統的設定容量超過 500 GiB，則控制台會將系統轉換為 Essentials 套件。

  一旦系統轉換為 Essentials 包，"最低收費"適用於它。

  已轉換為 Essentials 套件的Cloud Volumes ONTAP系統無法切換回 Freemium，即使配置容量減少到 500 GiB 以下。其他預置容量少於 500 GiB 的系統仍保留在免費增值版上（只要它們是使用免費增值產品部署的）。

必需品

您可以透過多種不同的配置按容量付費：

- 選擇您的Cloud Volumes ONTAP設定：
  - 單節點或 HA 系統
  - 用於災難復原 (DR) 的檔案和區塊儲存或輔助數據
- 額外付費即可新增任何 NetApp 雲端資料服務

專業的

按容量支付任何類型的Cloud Volumes ONTAP配置的費用，並提供無限備份。

- 為任何Cloud Volumes ONTAP配置提供許可

  單節點或 HA，以相同的費率對主捲和輔助卷進行容量計費

- 包括使用NetApp Backup and Recovery進行無限磁碟區備份，但僅適用於使用專業版軟體套件的Cloud Volumes ONTAP系統。

  備份和復原需要按使用量付費 (PAYGO) 訂閱，但使用此服務不會產生任何費用。有關設定備份和恢復許可的更多信息，請參閱 "設定備份和恢復許可"。

- 額外付費即可新增任何 NetApp 雲端資料服務

基於容量的許可證的可用性

Cloud Volumes ONTAP系統的 PAYGO 和 BYOL 授權的可用性要求控制台代理程式啟動並執行。

"了解控制台代理" 。

已限制 BYOL 授權的購買、延期和續約。有關更多信息，請參閱 "Cloud Volumes ONTAPP的 BYOL 授權可用性受限" 。

如何開始

了解如何開始使用基於容量的許可：

- "在 AWS 中設定Cloud Volumes ONTAP許可"
- "在 Azure 中設定Cloud Volumes ONTAP許可"
- "在 Google Cloud 中設定Cloud Volumes ONTAP許可"

Keystone訂閱

一種按需付費的訂閱式服務，為那些喜歡 OpEx 消費模式而非前期資本支出或租賃的用戶提供無縫的混合雲端體驗。

收費是根據Keystone訂閱中一個或多個Cloud Volumes ONTAP HA 對的承諾容量大小。

每個卷的預先配置容量都會定期匯總並與您的Keystone訂閱中的承諾容量進行比較，任何超額部分都會作為Keystone訂閱中的突發容量收費。

"了解有關NetApp Keystone 的更多信息" 。

支援的配置

Keystone 訂閱支援 HA 配對。目前單節點系統不支援此授權選項。

容量限制

在基於容量的許可模型中，每個Cloud Volumes ONTAP系統都支援分層到物件存儲，並且總分層容量可以擴展到雲端提供者的存儲桶限制。雖然許可證沒有施加容量限制，但遵循 "FabricPool最佳實踐"確保在配置和管理分層時實現最佳效能、可靠性和成本效率。

有關每個雲端提供者的容量限制的信息，請參閱其文檔：

- "AWS 文件"
- "託管磁碟的 Azure 文件"和 "Azure Blob 儲存體文檔"
- "Google Cloud 文件"

如何開始

了解如何開始使用Keystone訂閱：

- "在 AWS 中設定Cloud Volumes ONTAP許可"
- "在 Azure 中設定Cloud Volumes ONTAP許可"
- "在 Google Cloud 中設定Cloud Volumes ONTAP許可"

基於節點的許可

基於節點的許可是上一代許可模式，使您能夠按節點許可Cloud Volumes ONTAP 。此許可模式不適用於新客戶。按節點充電已被上述按容量充電方法所取代。

NetApp已計劃終止基於節點的許可的可用性 (EOA) 和支援 (EOS)。在 EOA 和 EOS 之後，基於節點的許可證將需要轉換為基於容量的許可證。

有關信息，請參閱 "客戶公報：CPC-00589"。

基於節點的許可證的可用性終止

從 2024 年 11 月 11 日起，基於節點的許可證的有限可用性已終止。基於節點的授權支援將於 2024 年 12 月 31 日結束。

如果您擁有有效的基於節點的合同，並且該合約的有效期超出了 EOA 日期，那麼您可以繼續使用該許可證，直到合約到期。一旦合約到期，就需要過渡到基於容量的許可模式。如果您沒有Cloud Volumes ONTAP節點的長期合同，則務必在 EOS 日期之前規劃您的轉換。

從下表中了解有關每種許可證類型以及 EOA 對其影響的更多資訊：

許可證類型	**EOA** 之後的影響
透過自帶許可證 (BYOL) 購買的有效基於節點的許可證	許可證有效期限至到期日。現有未使用的基於節點的許可證可用於部署新的Cloud Volumes ONTAP系統。
透過 BYOL 購買的基於節點的許可證已過期	您無權使用此授權部署新的Cloud Volumes ONTAP系統。現有系統可能會繼續運行，但在 EOS 日期之後，您將不會收到任何系統支援或更新。
具有 PAYGO 訂閱的有效基於節點的許可證	自 EOS 日期起將停止獲得NetApp支持，直到您過渡到基於容量的許可證。

除外責任

NetApp意識到某些情況需要特殊考慮，基於節點的許可的 EOA 和 EOS 不適用於以下情況：

- 美國公共部門客戶
- 私有模式下的部署
- AWS 中國區Cloud Volumes ONTAP部署

對於這些特殊情況， NetApp將提供支持，以滿足符合合約義務和營運需求的獨特授權要求。

即使在這些情況下，新的基於節點的許可證和許可證續訂自批准之日起最長有效期為一年。

許可證轉換

控制台可以透過許可證轉換工具將基於節點的許可證無縫轉換為基於容量的許可證。有關基於節點的許可的 EOA 的信息，請參閱"基於節點的許可證的可用性終止"。

在轉換之前，最好先熟悉兩種授權模式之間的差異。基於節點的授權包括每個ONTAP實例的固定容量，這可能會限制靈活性。另一方面，基於容量的授權允許跨多個執行個體共用儲存池，從而提供增強的靈活性，優化資源利用率，並降低重新分配工作負載時可能產生的經濟損失。基於容量的充電可以無縫適應不斷變化的儲存需求。

若要了解如何執行此轉換，請參閱"將Cloud Volumes ONTAP基於節點的許可證轉換為基於容量的許可證"。

不支援將系統從基於容量的許可轉換為基於節點的許可。

了解有關Cloud Volumes ONTAP基於容量的許可證的更多信息

您應該熟悉基於容量的許可證的收費方式和容量使用。

消費模式或許可購買選項

我們提供基於容量的授權套餐，並有以下幾種消費模式或購買選項：

- **BYOL**：自備授權（BYOL）。從NetApp購買的許可證，可用於在任何雲端供應商中部署Cloud Volumes ONTAP 。

  已限制 BYOL 授權的購買、延期和續約。有關更多信息，請參閱 "Cloud Volumes ONTAP的 BYOL 授權可用性受限" 。

- **PAYGO**：即用即付 (PAYGO) 訂閱是從雲端供應商市場按小時訂閱的。
- 年度：來自雲端提供者市場的年度合約。

請注意以下事項：

- 如果您從NetApp購買了 BYOL 許可證，則還需要從雲端供應商的雲端市場訂閱 PAYGO 產品。 NetApp已限制 BYOL 授權。當您的 BYOL 授權到期時，您需要將其替換為雲端市場訂閱。

  您的許可證總是會先被收費，但在以下情況下，我們將按照市場上的小時費率向您收費：

  - 如果您超出許可容量
  - 如果您的許可證期限已到期
- 如果您與市場簽訂了年度合同，則您部署的所有Cloud Volumes ONTAP系統都將根據該合約收費。您不能將年度市場合約與 BYOL 混合搭配。
- 中國大陸地區僅支援採用 BYOL 的單節點系統。中國大陸地區的部署不受 BYOL 授權限制。

更改許可證包

部署後，您可以變更使用基於容量的許可的Cloud Volumes ONTAP系統的軟體包。例如，如果您使用 Essentials 套件部署了Cloud Volumes ONTAP系統，則可以在業務需求變更時將其變更為 Professional 套件。

"了解如何更改充電方式" 。

有關將基於節點的許可證轉換為基於容量的許可證的信息，請參閱

支援的儲存類型和套餐如何收費

Cloud Volumes ONTAP的計費是基於多種因素，例如套餐和卷類型。Cloud Volumes ONTAP 9.7 及更高版本提供基於容量的授權包。

有關定價的詳細信息，請訪問 "NetApp Console網站"。

儲存虛擬機

- 額外的資料服務儲存虛擬機器 (SVM) 無需額外的授權費用，但每個資料服務 SVM 至少需支付 4 TiB 的容量費用。
- 災難復原 SVM 根據預置容量收費。

HA 對

對於 HA 對，您只需為節點上配置的容量付費。您無需為同步鏡像到合作夥伴節點的資料付費。

FlexClone和FlexCache卷

- 您無需為FlexClone磁碟區所使用的容量付費。
- 來源和目標FlexCache磁碟區被視為主數據，並根據配置的空間收費。

讀/寫卷

如果您建立或使用可寫入（讀取/寫入）卷，則該磁碟區將被視為主卷，並按每個儲存虛擬機器 (SVM) 的最低費用收取已配置容量的費用。例如FlexVol讀/寫卷、 SnapLock審計捲和 CIFS/NFS 審計卷。所有用戶創建的數據量均按您的訂閱和套餐類型收費。 ONTAP內部自動建立且無法儲存資料的磁碟區（例如 SVM 根磁碟區）不收費。

基本套裝

使用 Essentials 套件時，您需要根據部署類型（HA 或單節點）和磁碟區類型（主磁碟區或輔助磁碟區）付費。價格由高至低的順序如下：*Essentials Primary HA*、*Essentials Primary Single Node*、*Essentials Secondary HA* 和 *Essentials Secondary Single Node*。或者，當您購買市場合約或接受私人優惠時，任何部署或卷類型的容量費用都是相同的。

許可證完全基於Cloud Volumes ONTAP系統內建立的磁碟區類型：

- 基本單節點：僅使用一個ONTAP節點在Cloud Volumes ONTAP系統上建立的讀取/寫入磁碟區。
- Essentials HA：使用兩個ONTAP節點讀取/寫入卷，這兩個節點可以相互故障轉移，以實現無中斷資料存取。
- 基本輔助單節點：僅使用一個ONTAP節點在Cloud Volumes ONTAP系統上建立的資料保護 (DP) 類型磁碟區（通常是唯讀的SnapMirror或SnapVault目標磁碟區）。

  如果只讀/DP 磁碟區成為主卷，則控制台會將其視為主數據，並且收費成本將根據磁碟區處於讀取/寫入模式的時間來計算。當磁碟區再次變為唯讀/DP 時，它會再次將該磁碟區視為輔助數據，並使用控制台中最匹配的授權進行相應的收費。

- 基本輔助 HA：在Cloud Volumes ONTAP系統上使用兩個可以相互故障轉移以實現無中斷資料存取的ONTAP節點建立的資料保護 (DP) 類型磁碟區（通常是唯讀的SnapMirror或SnapVault目標磁碟區）。

容量限制

在基於容量的許可模型中，每個Cloud Volumes ONTAP系統都支援分層到物件存儲，並且總分層容量可以擴展到雲端提供者的存儲桶限制。雖然許可證沒有施加容量限制，但遵循 "FabricPool最佳實踐"確保在配置和管理分層時實現最佳效能、可靠性和成本效率。

有關每個雲端提供者的容量限制的信息，請參閱其文檔：

- "AWS 文件"
- "託管磁碟的 Azure 文件"和 "Azure Blob 儲存體文檔"
- "Google Cloud 文件"

最大系統數量

採用基於容量的授權模式時，每個 NetApp Console 組織最多只能建立 24 個 Cloud Volumes ONTAP 系統。一個「系統」指的是 Cloud Volumes ONTAP HA 配對、Cloud Volumes ONTAP 單節點系統，或您建立的任何其他儲存 VM。預設儲存 VM 不計入此限制。此限制適用於所有授權模式。

例如，假設您有三個系統：

- 具有一個儲存虛擬機器的單節點Cloud Volumes ONTAP系統（這是部署Cloud Volumes ONTAP時所建立的預設儲存虛擬機器）

  該系統算一個系統。

- 具有兩個儲存虛擬機（預設儲存虛擬機，加上您建立的一個額外的儲存虛擬機）的單節點Cloud Volumes ONTAP系統

  此系統計為兩個系統：一個用於單節點系統，一個用於額外的儲存 VM。

- 具有三個儲存虛擬機（預設儲存虛擬機，以及您建立的兩個額外的儲存虛擬機）的Cloud Volumes ONTAP HA 對

  系統計為三個系統：一個用於 HA 對，兩個用於附加儲存虛擬機器。

總共有六個系統。這樣一來，您的組織中就可以再容納 14 個系統。

如果您需要部署超過 24 台系統，請聯絡您的客戶代表或銷售團隊。

"了解 AWS、Azure 和 Google Cloud 的儲存限制" 。

最低收費

對於每個具有至少一個主（讀寫）卷的提供資料的儲存虛擬機，最低收費為 4 TiB。如果主磁碟區的總和小於 4 TiB，則控制台將對該儲存虛擬機器套用 4 TiB 的最低費用。

如果您尚未配置任何卷，則不適用最低費用。

對於 Essentials 包，4 TiB 最低容量費用不適用於僅包含輔助（資料保護）磁碟區的儲存虛擬機器。例如，如果您有一個包含 1 TiB 二級資料的儲存虛擬機，那麼您只需為該 1 TiB 資料付費。對於專業套餐類型，無論卷類型如何，最低容量收費均為 4 TiB。

計費偏好和超額費用

您可以在控制台的“**Licenses and subscriptions**”部分選擇您的收費方式。當您的使用量超過許可證套餐或年度訂閱中規定的容量時，就會產生超額費用。

- * NetApp優先授權*：在此模式下，您的使用量首先會根據您的許可證包（自帶許可證）的容量進行計費。如果您超出授權容量，超出部分將根據您的年度市場訂閱或市場按需小時費率（PAYGO）收取費用。如果您的 BYOL 授權到期，您必須透過雲端市場過渡到基於容量的授權模式。更多資訊請參閱 "將Cloud Volumes ONTAP基於節點的許可證轉換為基於容量的許可證"。
- 僅限市場訂閱用戶：在此模式下，您的使用費用將首先計入您的年度市場訂閱費用。任何額外使用均按市場按需小時費率（PAYGO）收費。任何未使用的許可證容量在計費時均不予考慮。

有關帳單偏好設定的更多信息，請參閱 "了解授權和訂閱的計費方式"。

Essentials許可證超額費用如何收取

如果您從NetApp購買 Essentials 授權（自帶授權），並且超出了特定 Essentials 軟體套件的授權容量，則控制台會將超出部分的費用計入價格較高的 Essentials 授權（如果您有可用容量的授權）。遊戲主機會先使用您已付費的可用容量，然後再向市場收費。如果您的 BYOL 授權沒有可用容量，超出容量的部分將按市場按需小時費率 (PAYGO) 收費，並添加到您的月帳單中。

同樣，如果您簽訂了年度市場合約或包含多個 Essentials 套餐的私人優惠，並且您的使用量超過了特定套餐的部署和容量類型的承諾容量，則控制台會根據可用容量，向價格更高的 Essentials 套餐收取超額費用。當該容量耗盡後，剩餘的超額容量將以市場按需（PAYGO）小時費率計費，並添加到您的月帳單中。

有關 Essentials 許可證收費的信息，請參閱"基本套裝"。

這是一個例子。假設您擁有 Essentials 套件的以下許可證：

- 具有 500 TiB 承諾容量的 500 TiB *Essentials Secondary HA* 許可證
- 500 TiB 的「Essentials 單節點」許可證，僅具有 100 TiB 的承諾容量

另外 50 TiB 在具有輔助卷的 HA 對上進行配置。控制台不會向 PAYGO 收取這 50 TiB 的費用，而是向 *Essentials Single Node* 授權收取 50 TiB 的超額費用。該許可證的價格高於_Essentials Secondary HA_，但它利用您已購買的許可證，並且不會增加您的每月帳單費用。

在「管理」> 「Licenses and subscriptions」中，您可以看到針對「Essentials 單節點」許可證收取了 50 TiB 的費用。

這是另一個例子。假設您擁有 Essentials 套件的以下許可證：

- 具有 500 TiB 承諾容量的 500 TiB *Essentials Secondary HA* 許可證
- 500 TiB 的「Essentials 單節點」許可證，僅具有 100 TiB 的承諾容量

另外 100 TiB 在具有主磁碟區的 HA 對上進行設定。您購買的許可證沒有_Essentials Primary HA_承諾容量。*Essentials Primary HA* 授權的價格高於 *Essentials Primary Single Node* 和 *Essentials Secondary HA* 授權。

在此範例中，控制台會依照市場價格對額外的 100 TiB 收取超額費用。超額費用將出現在您的每月帳單上。

儲存

Cloud Volumes ONTAP支援的客戶端協定

Cloud Volumes ONTAP支援 iSCSI、NFS、SMB、NVMe-TCP 和 S3 用戶端協定。

iSCSI

iSCSI 是一種可以在標準乙太網路上運行的區塊協定。大多數客戶端作業系統都提供透過標準乙太網路連接埠運行的軟體啟動器。

NFS

NFS是UNIX和LINUX系統的傳統文件存取協定。客戶端可以使用 NFSv3、NFSv4 和 NFSv4.1 協定存取ONTAP磁碟區中的檔案。您可以使用 UNIX 樣式權限、NTFS 樣式權限或兩者的混合來控制檔案存取。

客戶端可以使用 NFS 和 SMB 協定存取相同的檔案。

中小企業

SMB是Windows系統的傳統文件存取協定。用戶端可以使用 SMB 2.0、SMB 2.1、SMB 3.0 和 SMB 3.1.1 協定存取ONTAP磁碟區中的檔案。與 NFS 一樣，支援混合的權限樣式。

S3

Cloud Volumes ONTAP支援 S3 作為橫向擴充儲存的選項。 S3 協定支援可讓您設定 S3 用戶端對儲存虛擬機器 (SVM) 中儲存桶所含物件的存取。

"ONTAP文件：了解 S3 多重協定的工作原理" 。"ONTAP文件：了解如何在ONTAP中設定和管理 S3 物件儲存服務" 。

NVMe-TCP

從ONTAP版本 9.12.1 開始，所有雲端供應商均支援 NVMe-TCP。 Cloud Volumes ONTAP在部署期間支援 NVMe-TCP 作為儲存虛擬機器 (SVM) 的區塊協議，並自動安裝所需的 NVMe 授權。

NetApp Console不提供任何針對 NVMe-TCP 的管理功能。

有關透過ONTAP配置 NVMe 的更多信息，請參閱 "ONTAP文件：為 NVMe 設定儲存虛擬機"。

用於Cloud Volumes ONTAP叢集的磁碟和聚合

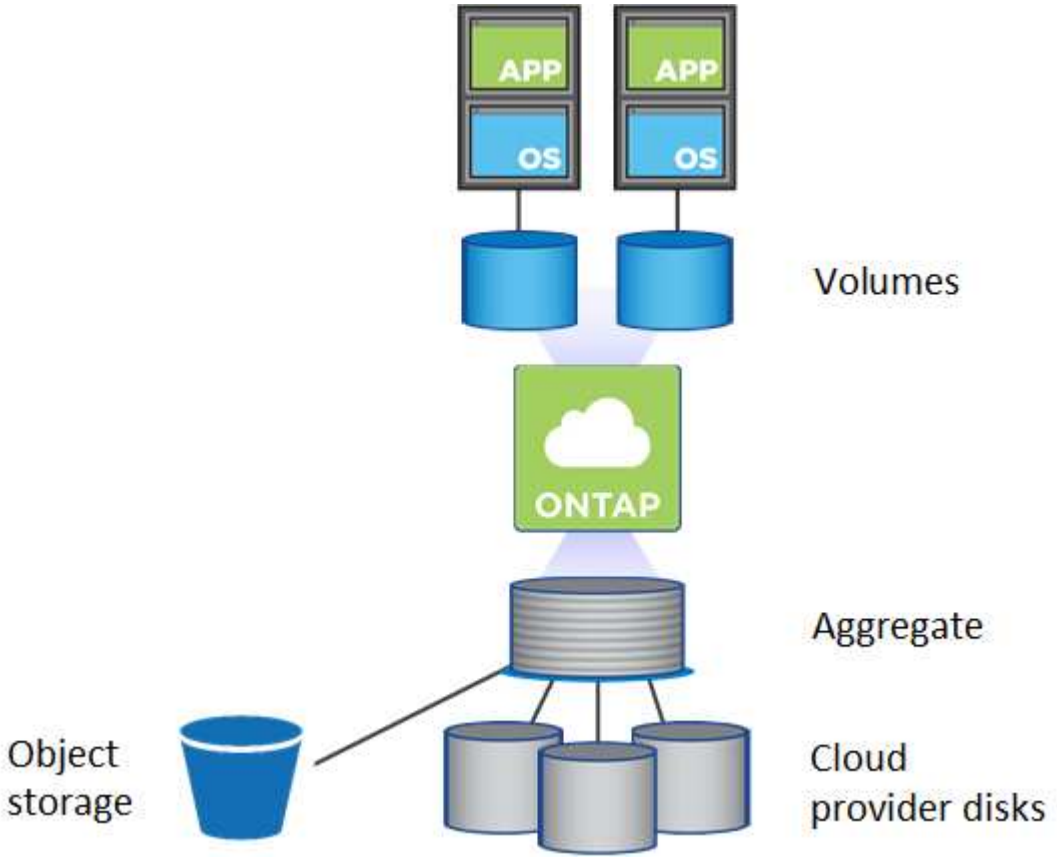
了解Cloud Volumes ONTAP如何使用雲端儲存可以幫助您了解儲存成本。

> 您必須從NetApp Console建立和刪除所有磁碟和聚合。您不應從其他管理工具執行這些操作。這樣做會影響系統穩定性，妨礙將來添加磁碟的能力，並可能產生冗餘的雲端供應商費用。

概況

Cloud Cloud Volumes ONTAP供應商儲存作為磁碟並將它們分組為一個或多個聚合。聚合為一個或多個磁碟區

提供儲存。



支援多種類型的雲端盤。建立磁碟區時選擇磁碟類型，部署Cloud Volumes ONTAP時選擇預設磁碟大小。

從雲端提供者購買的儲存總量是_原始容量_。 _可用容量_較少，因為大約 12% 到 14% 是為Cloud Volumes ONTAP使用保留的開銷。例如，如果控制台建立 500 GiB 聚合，則可用容量為 442.94 GiB。

AWS 儲存

在 AWS 中， Cloud Volumes ONTAP使用 EBS 儲存來儲存使用者數據，並在某些 EC2 執行個體類型上使用本機 NVMe 儲存作為快閃記憶體快取。

EBS 儲存

在 AWS 中，一個聚合最多可以包含 6 個大小相同的磁碟。但是，如果您的配置支援 Amazon EBS 彈性磁碟區功能，則聚合最多可以包含 8 個磁碟。"了解有關彈性卷支持的更多信息" 。

最大磁碟大小為 16 TiB。

底層 EBS 磁碟類型可以是 General Purpose SSD（gp3 或 gp2）、Provisioned IOPS SSD（io1）或 Throughput Optimized HDD（st1）。您可以將 EBS 磁碟與 Amazon Simple Storage Service（Amazon S3）配對"低成本物件存儲"。

使用吞吐量最佳化 HDD (st1) 時，不建議將資料分層到物件儲存。

本地 **NVMe** 存儲

一些 EC2 執行個體類型包括本地 NVMe 存儲， Cloud Volumes ONTAP將其用作"快閃記憶體"。

相關連結

- "AWS 文件：EBS 磁碟區類型"
- "了解如何為 AWS 中的系統選擇磁碟類型和磁碟大小"
- "查看 AWS 中Cloud Volumes ONTAP的儲存限制"
- "查看 AWS 中Cloud Volumes ONTAP支援的配置"

Azure 儲存

在 Azure 中，一個 Aggregate 最多可以包含 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節點系統還是 HA 配對：

單節點系統

單節點系統可以使用下列類型的 Azure 託管磁碟：

- 進階 *SSD* 託管磁碟 以更高的成本為 I/O 密集型工作負載提供高效能。
- 與高級 SSD 託管磁碟相比，高級 *SSD v2* 託管磁碟 為單節點和 HA 對提供了更高的效能和更低的延遲，並且成本更低。
- _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 並且想要降低成本，那麼「標準 HDD 託管磁碟」是一個不錯的選擇。

  每種託管磁碟類型的最大磁碟大小為 32 TiB。

  您可以將託管磁碟與 Azure Blob 儲存空間配對，以"低成本物件存儲"。

HA 對

HA 對使用兩種類型的磁碟，它們以更高的成本為 I/O 密集型工作負載提供高效能：

- *Premium page blob*，最大磁碟大小為 8 TiB
- 託管磁碟，最大磁碟大小為 32 TiB

相關連結

- "了解如何為 Azure 中的系統選擇磁碟類型和磁碟大小"
- "在 Azure 中啟動Cloud Volumes ONTAP HA 對"
- "Microsoft Azure 文件：Azure 託管磁碟類型"
- "Microsoft Azure 文件：Azure 頁 Blob 概述"
- "查看 Azure 中Cloud Volumes ONTAP的儲存限制"

Google 雲端儲存

在 Google Cloud 中，聚合最多可以包含 6 個大小相同的磁碟。最大磁碟大小為 64 TiB。

磁碟類型可以是_區域 SSD 持久性磁碟_、區域平衡持久性磁碟_或_區域標準持久磁碟。您可以將永久性磁碟與 Google 儲存桶配對，以"低成本物件存儲"。

相關連結

- "Google Cloud 文件：儲存選項"
- "查看 Google Cloud 中Cloud Volumes ONTAP 的儲存限制"

RAID 類型

每個Cloud Volumes ONTAP聚合的 RAID 類型是 RAID0（條帶化）。 Cloud Volumes ONTAP依賴雲端供應商來實現磁碟的可用性和耐用性。不支援其他 RAID 類型。

熱備品

RAID0 不支援使用熱備件實現冗餘。

建立連接到Cloud Volumes ONTAP實例的未使用磁碟（熱備用）是不必要的開支，並且可能會阻止根據需要配置額外的空間。因此，不建議這麼做。

了解**Cloud Volumes ONTAP**對 **AWS Elastic Volumes** 的支持

透過Cloud Volumes ONTAP聚合支援 Amazon EBS Elastic Volumes 功能可提供更好的效能和額外的容量，同時使NetApp Console能夠根據需要自動增加底層磁碟容量。

好處

- 動態磁碟成長

  當Cloud Volumes ONTAP正在運作且磁碟仍處於連線狀態時，控制台可以動態增加磁碟的大小。

- 更好的性能

  啟用彈性卷的聚合最多可以擁有八個磁碟，這些磁碟在兩個 RAID 群組中平均利用。此配置可提供更高的吞吐量和穩定的效能。

- 較大的骨材

  支援八個磁碟，最大聚合容量為 128 TiB。對於未啟用彈性磁碟區功能的聚合，這些限制高於六個磁碟限制和 96 TiB 限制。

  請注意，系統總容量限制保持不變。

"AWS 文件：了解有關 AWS 彈性磁碟區的更多信息"

支援的配置

特定Cloud Volumes ONTAP版本和特定 EBS 磁碟類型支援 Amazon EBS Elastic Volumes 功能。

Cloud Volumes ONTAP版本

從 9.11.0 或更高版本建立的 *new* Cloud Volumes ONTAP系統支援彈性磁碟區功能。 9.11.0 之前部署的現有Cloud Volumes ONTAP系統不支援此功能。

例如，如果您建立了Cloud Volumes ONTAP 9.9.0 系統，然後將系統升級到版本 9.11.0，則不支援彈性磁碟區功能。它必須是使用 9.11.0 或更高版本部署的新系統。

EBS 磁碟類型

使用通用 SSD（gp3）或預先設定 IOPS SSD（io1）時，彈性磁碟區功能會在聚合層級自動啟用。使用任何其他磁碟類型的聚合不支援彈性磁碟區功能。

所需的 AWS 權限

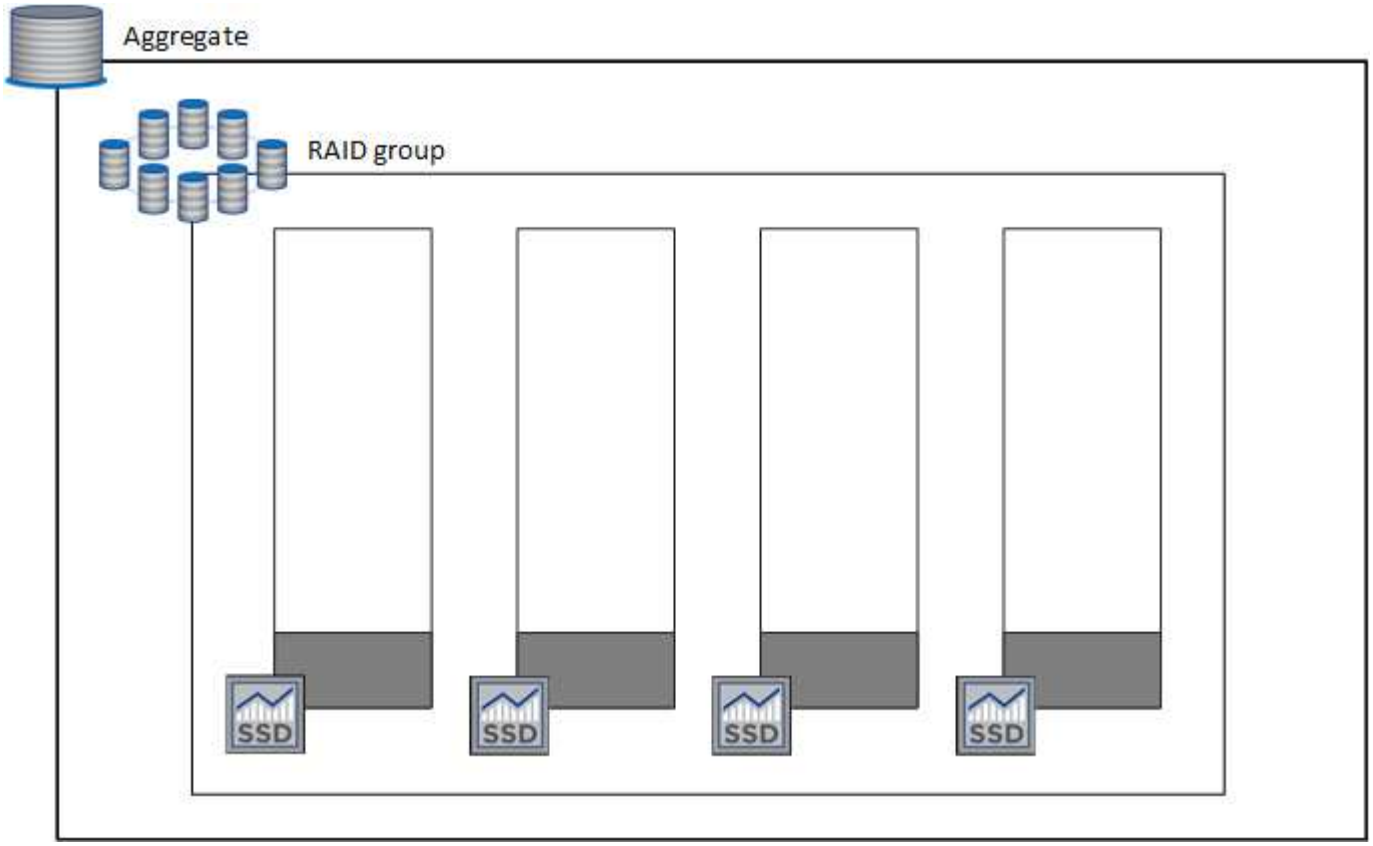
從 3.9.19 版本開始，控制台代理需要下列權限才能在Cloud Volumes ONTAP聚合上啟用和管理彈性磁碟區功能：

- ec2：描述卷修改
- ec2：修改卷

這些權限包含在 "NetApp提供的政策"

彈性卷支援如何運作

啟用了彈性磁碟區功能的聚合由一個或兩個 RAID 群組組成。每個 RAID 群組有四個相同的磁碟，容量相同。下面是一個 10 TiB 聚合的範例，該聚合包含四個磁碟，每個磁碟大小為 2.5 TiB：



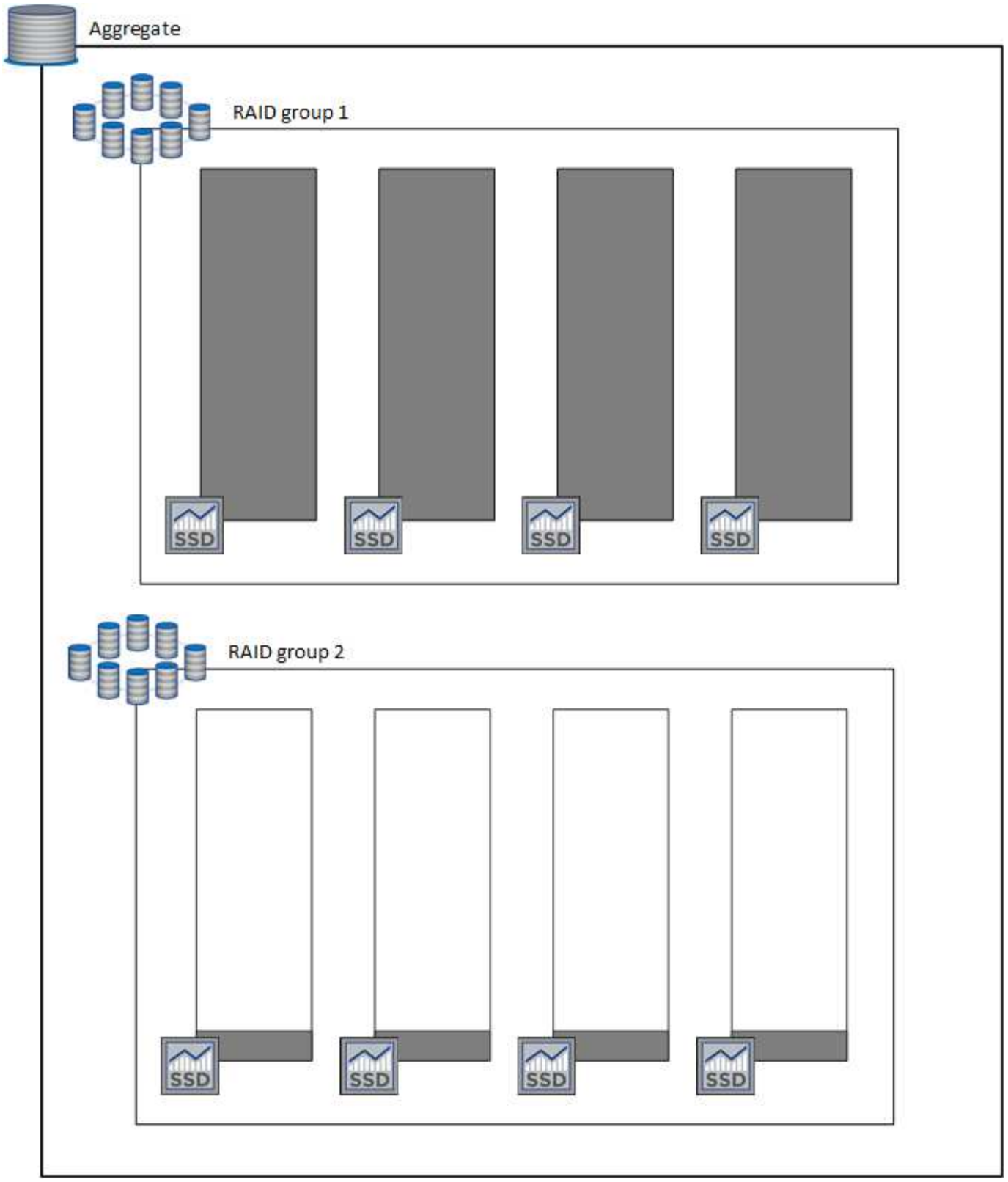
當控制台建立聚合時，它從一個 RAID 群組開始。如果需要額外的容量，它會透過將 RAID 群組中所有磁碟的容量增加相同的量來增加聚合。容量增加至少為 256 GiB 或聚合大小的 10%。

例如，如果您有一個 1 TiB 聚合，則每個磁碟為 250 GiB。聚合容量的 10% 為 100 GiB。這低於 256 GiB，因此聚合的大小增加了 256 GiB 的最小值（或每個磁碟 64 GiB）。

當Cloud Volumes ONTAP系統正在運作且磁碟仍處於連線狀態時，控制台會增加磁碟的大小。該變化不會造成破壞。

如果聚合達到 64 TiB（或每個磁碟 16 TiB），控制台將建立第二個 RAID 群組以提供額外的容量。第二個 RAID 群組的工作方式與第一個 RAID 群組相同：它有四個容量完全相同的磁碟，並且可以成長到 64 TiB。這意味著聚合的最大容量可以是 128 TiB。

以下是具有兩個 RAID 群組的聚合的範例。第一個 RAID 群組已達到容量限制，而第二個 RAID 群組中的磁碟有足夠的可用空間。



建立磁碟區時會發生什麼

如果您建立使用 gp3 或 io1 磁碟的捲，控制台將如下在聚合上建立該磁碟區：

- 如果存在啟用了彈性磁碟區的現有 gp3 或 io1 聚合，則控制台會在該聚合上建立磁碟區。
- 如果有多個啟用了彈性磁碟區的 gp3 或 io1 聚合，則控制台會在需要最少資源的聚合上建立磁碟區。

- 如果系統僅具有未啟用彈性磁碟區的 gp3 或 io1 聚合，則會在該聚合上建立磁碟區。

> 雖然這種情況不太可能發生，但在兩種情況下是有可能的：
>
> - 從 API 建立聚合時，您明確停用了彈性卷功能。
> - 您從使用者介面建立了一個新的Cloud Volumes ONTAP系統，在這種情況下，初始聚合上的彈性磁碟區功能被停用。審查[限制]請參閱下文以了解更多資訊。

- 如果現有聚合都沒有足夠的容量，控制台將建立啟用彈性磁碟區的聚合，然後在該新聚合上建立磁碟區。

  聚合的大小是基於請求的磁碟區大小加上額外的 10% 容量。

容量管理模式

控制台代理程式的容量管理模式與彈性磁碟區的工作方式類似於與其他類型的聚合的工作方式：

- 啟用自動模式（這是預設）時，如果需要額外的容量，控制台會自動增加聚合的大小。
- 如果將容量管理模式變更為手動，控制台將要求您批准購買額外容量。

"了解有關容量管理模式的更多信息" 。

限制

增加聚合體的大小最多可能需要 6 小時。在此期間，控制台無法為該聚合請求任何額外容量。

如何使用彈性卷

您可以使用彈性磁碟區執行下列任務：

- 使用 gp3 或 io1 磁碟時，建立一個在初始聚合上啟用彈性磁碟區的新系統

  "了解如何建立Cloud Volumes ONTAP系統"

- 在啟用了彈性卷的聚合上建立新卷

  如果您建立使用 gp3 或 io1 磁碟的捲，控制台會自動在啟用了彈性卷的聚合上建立該磁碟區。有關詳細信息，請參閱[建立磁碟區時會發生什麼]。

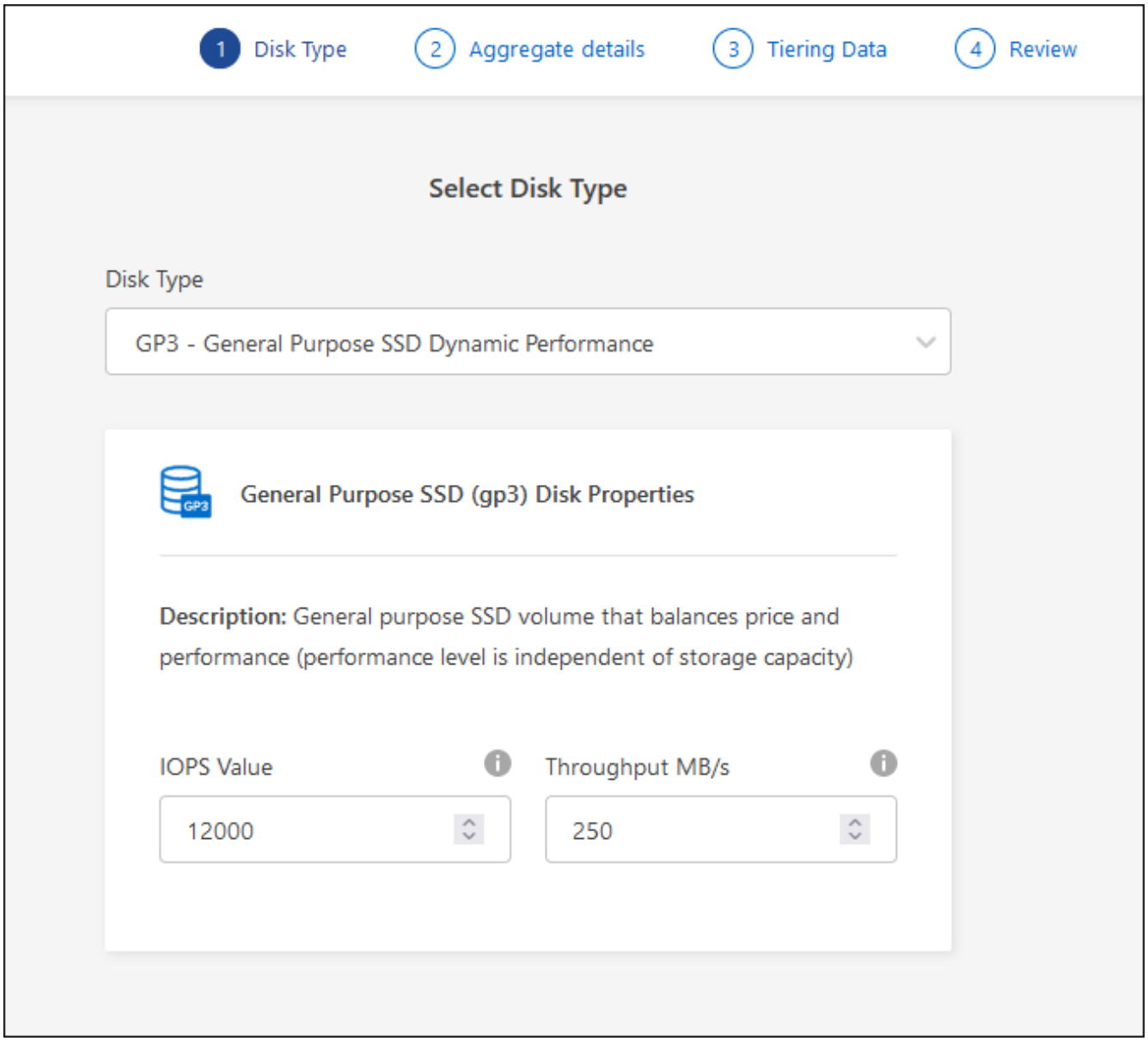
  "了解如何建立卷" 。

- 建立已啟用彈性磁碟區的新聚合

  只要Cloud Volumes ONTAP系統是從 9.11.0 或更高版本建立的，彈性磁碟區就會在使用 gp3 或 io1 磁碟的新聚合上自動啟用。

  建立聚合時，控制台會提示您輸入聚合的容量大小。這與選擇磁碟大小和磁碟數量的其他配置不同。

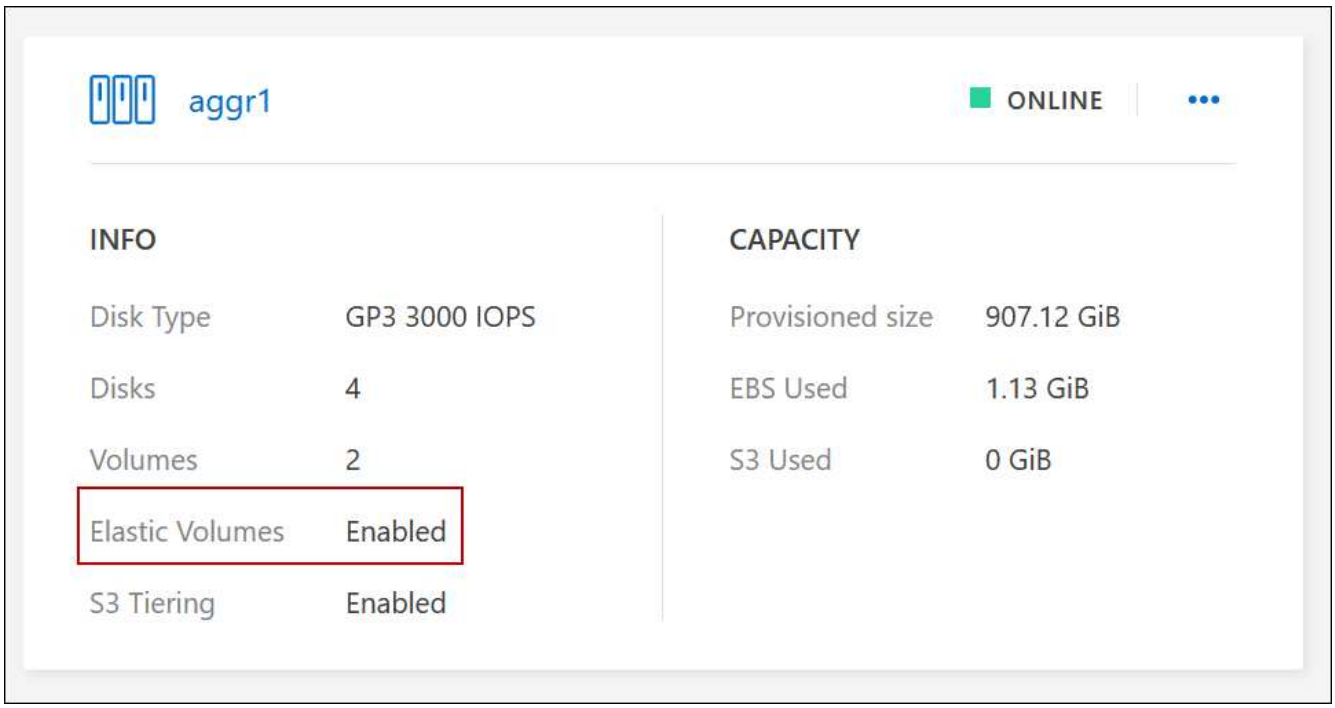
  以下螢幕截圖顯示了由 gp3 磁碟組成的新聚合的範例。



"了解如何建立聚合"。

- 識別已啟用彈性卷的聚合

  當您前往「進階分配」頁面時，您可以確定聚合上是否啟用了彈性磁碟區功能。在以下範例中，aggr1 啟用了彈性磁碟區。



- 向聚合添加容量

  雖然控制台會根據需要自動向聚合添加容量，但您也可以手動增加容量。

  "了解如何提高總容量"。

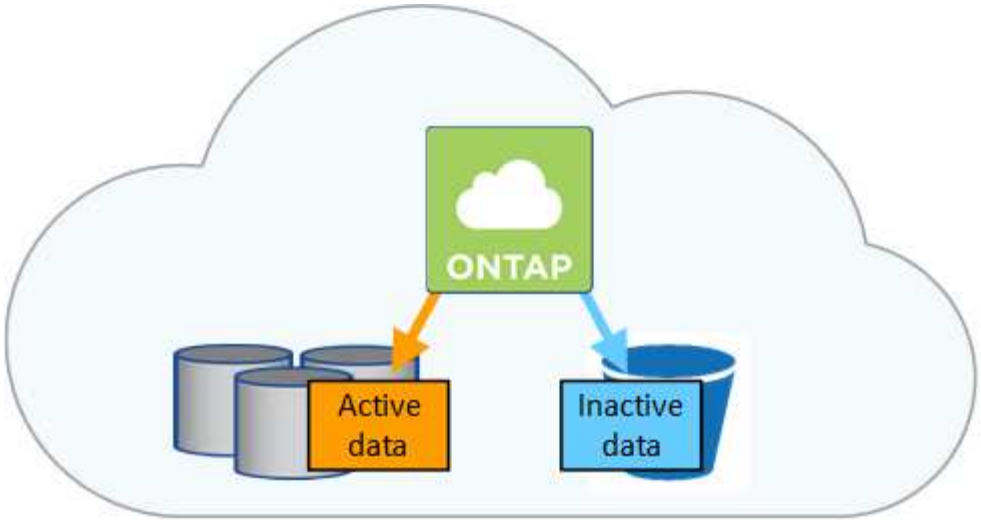
- 將資料複製到已啟用彈性卷的聚合

  如果目標Cloud Volumes ONTAP系統支援彈性卷，則目標卷將放置在啟用了彈性卷的聚合上（只要您選擇 gp3 或 io1 磁碟）。

  "了解如何設定資料複製"

了解 AWS、Azure 或 Google Cloud 中的Cloud Volumes ONTAP資料分層

透過將非活動資料自動分層到低成本物件儲存來降低儲存成本。活動資料保留在高效能 SSD 或 HDD 中，而非活動資料則分層到低成本物件儲存中。這使您能夠回收主儲存上的空間並縮小輔助儲存。



資料分層由FabricPool技術提供支援。 Cloud Volumes ONTAP為所有Cloud Volumes ONTAP叢集提供資料分層，無需額外的授權。當您啟用資料分層時，分層到物件儲存的資料會產生費用。有關對象儲存成本的詳細信息，請參閱雲端提供者的文檔。

AWS 中的資料分層

在 AWS 中啟用資料分層時，Cloud Volumes ONTAP 使用 EBS 作為熱資料的效能層，並使用 Amazon Simple Storage Service（Amazon S3）作為非作用中資料的容量層。

性能層

性能層可以是通用 SSD（gp3 或 gp2）或預先配置 IOPS SSD（io1）。

使用吞吐量最佳化 HDD (st1) 時，不建議將資料分層到物件儲存。

容量層

Cloud Volumes ONTAP系統將非活動資料分層到單一 S3 儲存桶。

NetApp Console為每個系統建立一個 S3 儲存桶，並將其命名為 fabric-pool-*cluster unique identifier*。不會為每個磁碟區建立不同的 S3 儲存桶。

當控制台建立 S3 儲存桶時，它會使用以下預設設定：

- 儲存類別：標準
- 預設加密：已停用
- 阻止公共訪問：阻止所有公共訪問
- 物件所有權：已啟用 ACL
- 儲存桶版本控制：已停用
- 物件鎖定：已停用

儲存類別

AWS 中分層資料的預設儲存類別是「標準」。標準非常適合跨多個可用區域儲存的頻繁存取的資料。

如果您不打算存取非活動數據，則可以透過將儲存類別變更為以下之一來降低儲存成本：智慧分層、單區不頻繁存取、標準不頻繁存取_或_*S3 Glacier* 即時檢索。當您變更儲存類別時，非活動數據將從標準儲存類別

開始，如果 30 天後未存取該數據，則將轉換到您選擇的儲存類別。

如果存取數據，存取成本會更高，因此在更改儲存類別之前請考慮這一點。 "Amazon S3 文件：了解有關 Amazon S3 儲存類別的更多信息" 。

您可以在建立系統時選擇儲存類，之後可以隨時變更它。有關更改儲存類別的說明，請參閱"將非活動資料分層到低成本物件存儲"。

資料分層的儲存類別是系統範圍的 - 而不是每個磁碟區的。

Azure 中的資料分層

當您在 Azure 中啟用資料分層時， Cloud Volumes ONTAP會使用 Azure 託管磁碟作為熱資料的效能層，並使用 Azure Blob 儲存作為非活動資料的容量層。

性能層

效能層可以是 SSD 或 HDD。

容量層

Cloud Volumes ONTAP系統將非活動資料分層到單一 Blob 容器。

控制台為每個Cloud Volumes ONTAP系統建立一個帶有容器的新儲存帳戶。儲存帳戶的名稱是隨機的。不會為每個磁碟區建立不同的容器。

控制台使用以下設定建立儲存帳戶：

- 訪問層：熱
- 性能：標準
- 冗餘：根據 Cloud Volume ONTAP部署
  - 單一可用區：本地冗餘儲存（LRS）
  - 多可用區域：區域冗餘儲存（ZRS）
- 帳號：StorageV2（通用 v2）
- 要求 REST API 操作進行安全傳輸：已啟用
- 儲存帳戶金鑰存取：已啟用
- 最低 TLS 版本：版本 1.2
- 基礎設施加密：已停用

儲存存取層

Azure 中分層資料的預設儲存存取層是_熱_層。熱層非常適合容量層中頻繁存取的資料。

如果您不打算存取容量層中的非活動數據，則可以選擇_cool_儲存層，其中非活動數據至少保留 30 天。您也可以選擇冷層，其中非活動資料至少儲存 90 天。根據您的儲存要求和成本考慮，您可以選擇最適合您需求的層。當您將儲存層變更為_cool_或_cold_時，非活動容量層資料將直接移至冷儲存層。與熱層相比，冷層提供的儲存成本較低，但存取成本較高，因此在更改儲存層之前請考慮這一點。參考 "Microsoft Azure 文件：了解有關 Azure Blob 儲存存取層的更多信息"。

您可以在新增Cloud Volumes ONTAP系統時選擇一個儲存層，之後可以隨時變更它。有關更改儲存層的詳細

信息，請參閱"將非活動資料分層到低成本物件存儲"。

資料分層的儲存存取層是系統範圍的，而不是每個磁碟區的。

Google Cloud 中的資料分層

當您在 Google Cloud 中啟用資料分層時， Cloud Volumes ONTAP會使用持久磁碟作為熱資料的效能層，並使用 Google Cloud Storage 儲存桶作為非活動資料的容量層。

性能層

效能層可以是 SSD 持久性磁碟、平衡持久性磁碟或標準持久性磁碟。

容量層

Cloud Volumes ONTAP系統將非活動資料分層到單一 Google Cloud Storage 儲存桶。

控制台為每個系統建立一個儲存桶並將其命名為 fabric-pool-*cluster unique identifier*。不會為每個磁碟區建立不同的儲存桶。

當控制台建立儲存桶時，它使用以下預設設定：

- 位置類型：區域
- 儲存類別：標準
- 公共存取：受物件 ACL 約束
- 存取控制：細粒度
- 保護：無
- 資料加密：Google 管理的金鑰

儲存類別

分層資料的預設儲存類別是「標準儲存」類別。如果資料不經常訪問，您可以透過變更為_Nearline Storage_或_Coldline Storage_來降低儲存成本。當您變更儲存類別時，後續非活動資料將直接移至您選擇的類別。

> ⓘ 當您變更儲存類別時，任何現有的非活動資料都將保持預設儲存類別。若要變更現有非活動資料的儲存類別，您必須手動執行指定。

如果您確實存取數據，存取成本會更高，因此在更改儲存類別之前請考慮這一點。要了解更多信息，請參閱"Google Cloud 文件：儲存類別"。

您可以在建立系統時選擇一個儲存層，之後可以隨時變更它。有關更改存儲類別的詳細信息，請參閱"將非活動資料分層到低成本物件存儲"。

資料分層的儲存類別是系統範圍的 - 而不是每個磁碟區的。

資料分層和容量限制

如果啟用資料分層，系統的容量限制將保持不變。此限制分佈在性能層和容量層。

卷分層策略

若要啟用資料分層，您必須在建立、修改或複製磁碟區時選擇磁碟區分層策略。您可以為每個磁碟區選擇不同的策略。

一些分層策略具有相關的最小冷卻期，該冷卻期規定了磁碟區中的使用者資料必須保持不活動的時間，以便資料被視為「冷」並移動到容量層。當資料寫入聚合時，冷卻期開始。

您可以變更最短冷卻期和 50% 的預設聚合閾值（更多內容請見下文）。 "了解如何更改冷卻時間" 和 "學習如何改變閾值"。

控制台可讓您在建立或修改磁碟區時從下列磁碟區分層原則中進行選擇：

僅限快照

當聚合達到 50% 容量後， Cloud Volumes ONTAP會將與活動檔案系統不關聯的 Snapshot 副本的冷用戶資料分層到容量層。冷卻期約為2天。

如果讀取，容量層上的冷資料塊會變熱並被移動到效能層。

全部

所有數據（不包括元數據）都會立即標記為冷數據，並儘快分層到物件儲存。無需等待 48 小時讓卷中的新區塊變冷。請注意，在設定「全部」策略之前位於磁碟區中的區塊需要 48 小時才能冷卻。

如果讀取，雲層上的冷資料塊將保持冷狀態並且不會寫回效能層。此策略從ONTAP 9.6 開始可用。

汽車

當聚合達到 50% 容量後， Cloud Volumes ONTAP會將磁碟區中的冷資料塊分層到容量層。冷資料不僅包括 Snapshot 副本，還包括來自活動檔案系統的冷用戶資料。冷卻期約為31天。

從Cloud Volumes ONTAP 9.4 開始支援此策略。

如果透過隨機讀取，容量層中的冷資料塊會變熱並移動到效能層。如果透過順序讀取（例如與索引和防毒掃描相關的讀取），冷資料區塊將保持冷狀態並且不會移動到效能層。

沒有任何

將磁碟區的資料保留在效能層中，防止其移動到容量層。

複製

複製磁碟區時，您可以選擇是否將資料分層到物件儲存。如果這樣做，控制台會將*備份*政策套用至資料保護磁碟區。從Cloud Volumes ONTAP 9.6 開始，*全部*分層策略取代了備份策略。刪除複製關係時，目標磁碟區將保留複製期間生效的分層策略。

關閉Cloud Volumes ONTAP會影響冷卻期

資料塊透過冷卻掃描進行冷卻。在此過程中，未使用的塊的溫度將移動（冷卻）到下一個較低的值。預設冷卻時間取決於磁碟區分層策略：

- 自動：31天
- 僅限快照：2 天

必須執行Cloud Volumes ONTAP才能使冷卻掃描正常運作。如果關閉Cloud Volumes ONTAP ，冷卻也會停止。

因此，您可以體驗更長的冷卻時間。

當Cloud Volumes ONTAP關閉時，每個區塊的溫度都會保留，直到您重新啟動系統。例如，如果關閉系統時某個區塊的溫度為 5，則重新開啟系統時溫度仍為 5。

設定資料分層

有關說明和受支援配置的列表，請參閱"將非活動資料分層到低成本物件存儲"。

Cloud Volumes ONTAP儲存管理

NetApp Console提供了對Cloud Volumes ONTAP儲存的簡化和進階管理。

您必須直接從控制台建立和刪除所有磁碟和聚合。您不應從其他管理工具執行這些操作。這樣做會影響系統穩定性，妨礙將來添加磁碟的能力，並可能產生冗餘的雲端供應商費用。

儲存配置

控制台透過為您購買磁碟和管理聚合，使Cloud Volumes ONTAP 的儲存配置變得簡單。您只需要建立磁碟區。如果您願意，您可以使用進階分配選項自行配置聚合。

簡化配置

聚合為磁碟區提供雲端儲存。當您啟動執行個體以及配置其他磁碟區時，控制台會為您建立聚合。

建立磁碟區時，控制台會執行以下三件事之一：

- 它將磁碟區放置在具有足夠可用空間的現有聚合上。
- 它透過為聚合購買更多磁碟將磁碟區放置在現有聚合上。

+ 在支援彈性磁碟區的 AWS 聚合的情況下，它也會增加 RAID 群組中磁碟的大小。"了解有關彈性卷支持的更多信息" 。

- 它為新聚合購買磁碟並將磁碟區放置在該聚合上。

控制台透過查看幾個因素來確定新磁碟區的放置位置：聚合的最大大小、是否啟用精簡配置以及聚合的可用空間閾值。

AWS 中聚合的磁碟大小選擇

當控制台在 AWS 中為Cloud Volumes ONTAP建立新聚合時，它會隨著聚合數量的增加而逐漸增加磁碟大小，以在達到 AWS 資料磁碟限制之前最大化系統容量。

例如，控制台可能會選擇以下磁碟大小：

總數	磁碟大小	最大總容量
1	500 GiB	3 TiB
4	1 TiB	6 TiB

總數	磁碟大小	最大總容量
6	2 TiB	12 TiB

此行為不適用於支援 Amazon EBS 彈性磁碟區功能的聚合。啟用了彈性卷的聚合由一個或兩個 RAID 群組組成。每個 RAID 群組有四個相同的磁碟，容量相同。"了解有關彈性卷支持的更多信息"。

您可以使用進階分配選項自行選擇磁碟大小。

進階分配

您也可以管理聚合。"從「進階分配」頁面"，您可以建立包含特定數量磁碟的新聚合、將磁碟新增至現有聚合以及在特定聚合中建立磁碟區。

容量管理

組織或帳戶管理員可以設定控制台來通知您儲存容量決策或是否自動為您管理容量需求。

此行為由控制台代理程式上的_容量管理模式_決定。容量管理模式會影響此控制台代理管理的所有Cloud Volumes ONTAP系統。如果您有另一個控制台代理，則可以進行不同的配置。

自動容量管理

容量管理模式預設為自動。在此模式下，控制台每 15 分鐘檢查一次可用空間比率，以確定可用空間比率是否低於指定的閾值。如果需要更多容量，它會啟動購買新磁碟、刪除未使用的磁碟集合（聚合）、根據需要在聚合之間移動卷，並嘗試防止磁碟故障。

以下範例說明了此模式的工作原理：

- 如果聚合達到容量閾值並且有空間容納更多磁碟，則控制台會自動為該聚合購買新磁碟，以便磁碟區可以繼續成長。

對於支援彈性磁碟區的 AWS 中的聚合，它還會增加 RAID 群組中磁碟的大小。"了解有關彈性卷支持的更多信息"。

+ * 如果聚合達到容量閾值且無法支援任何額外的磁碟，則控制台會自動將磁碟區從該聚合移至具有可用容量的聚合或新的聚合。

+ 如果控制台為磁碟區建立新的聚合，它會選擇適合該磁碟區大小的磁碟大小。

+ 請注意，原始聚合上現在有可用空間。現有磁碟區或新磁碟區可以使用該空間。在這種情況下，空間無法返回給雲端提供者。

- 如果聚合中超過 12 小時沒有捲，控制台就會將其刪除。

使用自動容量管理來管理 **LUN**

控制台的自動容量管理不適用於 LUN。當它建立 LUN 時，它會停用自動增長功能。

手動容量管理

如果組織或帳戶管理員將*容量管理模式*設定為手動，控制台會通知您採取適當的容量決策措施。自動模式中所述的相同範例也適用於手動模式，但是否接受操作取決於您。

了解更多

"了解如何修改容量管理模式"。

寫入速度

NetApp Console可讓您為大多數Cloud Volumes ONTAP設定選擇正常或高寫入速度。在選擇寫入速度之前，您應該了解正常設定和高設定之間的差異以及使用高寫入速度時的風險和建議。

正常寫入速度

當您選擇正常寫入速度時，資料將直接寫入磁碟。當資料直接寫入磁碟時，可以降低發生意外系統中斷或涉及意外系統中斷的級聯故障（僅限 HA 對）時資料遺失的可能性。

正常寫入速度是預設選項。

高寫入速度

當您選擇高寫入速度時，資料會在寫入磁碟之前緩衝在記憶體中，從而提供更快的寫入效能。由於這種緩存，如果發生意外的系統中斷，則可能會遺失資料。

發生意外系統中斷時可能遺失的資料量是最後兩個一致點的跨度。一致點是將緩衝資料寫入磁碟的行為。當寫入日誌已滿或 10 秒後（以先到者為準）就會出現一致點。但是，雲端提供者提供的儲存效能可能會影響一致點處理時間。

何時使用高寫入速度

如果您的工作負載需要快速寫入效能，並且您可以承受意外系統中斷或涉及意外系統中斷的級聯故障（僅限 HA 對）時資料遺失的風險，那麼高寫入速度是一個不錯的選擇。

使用高寫入速度時的建議

如果啟用高寫入速度，則應確保應用程式層的寫入保護，或確保應用程式能夠容忍資料遺失（如果發生）。

AWS 中的 **HA** 對具有高寫入速度

如果您打算在 AWS 中的 HA 對上啟用高寫入速度，則應了解多可用區 (AZ) 部署和單一可用區部署之間的保護等級差異。跨多個可用區部署 HA 對可提供更高的彈性，並有助於降低資料遺失的可能性。

"了解有關 AWS 中的 HA 對的更多信息"。

支援高寫入速度的配置

並非所有Cloud Volumes ONTAP配置都支援高寫入速度。這些配置預設使用正常的寫入速度。

AWS

如果您使用單節點系統，Cloud Volumes ONTAP 支援所有執行個體類型的高寫入速度。

從 9.8 版本開始， Cloud Volumes ONTAP在使用幾乎所有受支援的 EC2 執行個體類型（m5.xlarge 和 r5.xlarge 除外）時都支援具有 HA 對的高寫入速度。

"了解有關Cloud Volumes ONTAP支援的 Amazon EC2 執行個體的更多信息" 。

Azure

如果您使用單節點系統，Cloud Volumes ONTAP 支援所有 VM 類型的高寫入速度。

如果您使用 HA 對，從 9.8 版本開始， Cloud Volumes ONTAP支援多種 VM 類型的高寫入速度。前往 "Cloud Volumes ONTAP發行說明"查看支援高寫入速度的虛擬機器類型。

Google雲

如果您使用單節點系統，Cloud Volumes ONTAP 支援所有機器類型的高寫入速度。

如果您使用 HA 對，從 9.13.0 版本開始， Cloud Volumes ONTAP支援多種 VM 類型的高寫入速度。前往 "Cloud Volumes ONTAP發行說明"查看支援高寫入速度的虛擬機器類型。

"詳細了解Cloud Volumes ONTAP支援的 Google Cloud 機器類型" 。

如何選擇寫入速度

您可以在新增的Cloud Volumes ONTAP系統時選擇寫入速度，並且可以"更改現有系統的寫入速度"。

如果發生資料遺失會發生什麼

如果因寫入速度過快而導致資料遺失，事件管理系統 (EMS) 會報告以下兩個事件：

- Cloud Volumes ONTAP 9.12.1 或更高版本

```
 NOTICE nv.data.loss.possible: An unexpected shutdown occurred while in
high write speed mode, which possibly caused a loss of data.
* Cloud Volumes ONTAP 9.11.0 至 9.11.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown with High Write Speed mode"
```

```
 ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect..
* Cloud Volumes ONTAP 9.8 至 9.10.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect.
```

當這種情況發生時， Cloud Volumes ONTAP應該能夠啟動並繼續提供數據，而無需使用者乾預。

如果發生資料遺失，如何停止資料存取

如果您擔心資料遺失，希望應用程式在資料遺失時停止運行，並在正確解決資料遺失問題後恢復資料訪問，則可以使用 CLI 中的 NVFAIL 選項來實現該目標。

啟用 **NVFAIL** 選項

```
vol modify -volume <vol-name> -nvfail on
```

檢查 **NVFAIL** 設定

```
vol show -volume <vol-name> -fields nvfail
```

停用 **NVFAIL** 選項

```
vol modify -volume <vol-name> -nvfail off
```

當發生資料遺失時，啟用 NVFAIL 的 NFS 或 iSCSI 磁碟區應停止提供資料（這對無狀態協定 CIFS 沒有影響）。有關詳細信息，請參閱 "NVFAIL 如何影響對 NFS 卷或 LUN 的訪問"。

檢查 **NVFAIL** 狀態

```
vol show -fields in-nvfailed-state
```

正確解決資料遺失問題後，您可以清除 NVFAIL 狀態，然後磁碟區將可供資料存取。

清除 **NVFAIL** 狀態

```
vol modify -volume <vol-name> -in-nvfailed-state false
```

快閃記憶體

一些Cloud Volumes ONTAP配置包括本地 NVMe 存儲， Cloud Volumes ONTAP將其用作_Flash Cache_ 以獲得更好的性能。

什麼是快閃記憶體？

Flash Cache 透過即時智慧型快取最近讀取的使用者資料和NetApp元資料來加快資料存取速度。它對於隨機讀取密集型工作負載（包括資料庫、電子郵件和文件服務）非常有效。

支援的配置

特定的Cloud Volumes ONTAP設定支援 Flash Cache。查看支援的配置 "Cloud Volumes ONTAP發行說明"

限制

- 在 AWS 中為Cloud Volumes ONTAP 9.12.0 或更早版本配置 Flash Cache 時，必須在所有磁碟區上停用壓縮才能利用 Flash Cache 效能改進。當您部署或升級至Cloud Volumes ONTAP 9.12.1 或更高版本時，您無需停用壓縮。

  從NetApp Console建立磁碟區時跳過選擇儲存效率設置，或建立磁碟區然後 "使用 CLI 停用資料壓縮"。

- Cloud Volumes ONTAP不支援重新啟動後快取重新預熱。

相關主題

- "AWS 中Cloud Volumes ONTAP支援的配置"
- "Azure 中Cloud Volumes ONTAP支援的配置"
- "Google Cloud 中 Cloud Volumes ONTAP 支援的組態"

了解**Cloud Volumes ONTAP**上的 **WORM** 存儲

您可以在Cloud Volumes ONTAP系統上啟動一次寫入、多次讀取 (WORM) 存儲，以便在指定的保留期內以未修改的形式保留檔案。雲端 WORM 儲存由SnapLock技術提供支持，這意味著 WORM 檔案在檔案層級受到保護。

WORM 功能可與自帶許可證 (BYOL) 一起使用，並且無需額外付費即可在市場訂閱您的許可證。請聯絡您的NetApp銷售代表，將 WORM 新增至您目前的許可證。

WORM儲存的工作原理

一旦文件被提交到 WORM 存儲，即使保留期已過，也無法修改。防篡改時鐘確定 WORM 檔案的保留期何時結束。

保留期過後，您有責任刪除不再需要的任何文件。

啟動 **WORM** 存儲

如何啟動 WORM 儲存取決於您使用的Cloud Volumes ONTAP版本。

版本 **9.10.1** 及更高版本

從Cloud Volumes ONTAP 9.10.1 開始，您可以選擇在磁碟區層級啟用或停用 WORM。

新增Cloud Volumes ONTAP系統時，系統會提示您啟用或停用 WORM 儲存：

- 如果在新增系統時啟用 WORM 存儲，則從NetApp Console建立的每個磁碟區都將啟用 WORM。但是您可以使用ONTAP系統管理員或ONTAP CLI 來建立已停用 WORM 的磁碟區。
- 如果在新增系統時停用 WORM 存儲，則從控制台、 ONTAP系統管理器或ONTAP CLI 建立的每個磁碟區都將停用 WORM。

新增系統時，您可以在Cloud Volumes ONTAP系統上啟動 WORM 儲存。您從控制台建立的每個磁碟區都啟用了 WORM。您無法停用單一磁碟區上的 WORM 儲存。

將文件提交至 **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 自動將檔案提交至 WORM。您也可以使用 WORM 可附加檔案來保留增量寫入的數據，例如日誌資訊。

在Cloud Volumes ONTAP系統上啟動 WORM 儲存後，您必須使用ONTAP CLI 進行所有 WORM 儲存的管理。有關說明，請參閱 "有關SnapLock的ONTAP文檔"。

在**Cloud Volumes ONTAP**系統上啟用 **WORM**

您可以在控制台上建立Cloud Volumes ONTAP系統時啟用 WORM 儲存。如果在建立系統時未啟用 WORM，您也可以在系統上啟用 WORM。啟用後，您將無法停用 WORM。

關於此任務

- ONTAP 9.10.1 及更高版本支援 WORM。
- ONTAP 9.11.1 及更高版本支援具有備份的 WORM。

步驟

1. 在「系統」頁面上，雙擊要啟用 WORM 的系統的名稱。
2. 在「概述」標籤上，按一下「功能」面板，然後按一下「**WORM**」旁邊的鉛筆圖示。

   如果系統上已啟用 WORM，則鉛筆圖示將被停用。

3. 在*WORM*頁面上，設定叢集合規時鐘的保留期限。

   欲了解更多信息，請參閱 "ONTAP文件：初始化合規時鐘"。

4. 點選“設定”。

完成後

您可以在「功能」面板上驗證 **WORM** 的狀態。啟用 WORM 後， SnapLock許可證會自動安裝在叢集上。您可以在ONTAP系統管理員上查看SnapLock許可證。

刪除 **WORM** 文件

您可以使用特權刪除功能刪除保留期內的 WORM 檔案。

有關說明，請參閱 "ONTAP文檔"。

WORM 和資料分層

建立新的Cloud Volumes ONTAP 9.8 系統或更高版本時，您可以同時啟用資料分層和 WORM 儲存。使用 WORM 儲存啟用資料分層可讓您將資料分層到雲端中的物件儲存。

您應該了解有關啟用資料分層和 WORM 儲存的以下內容：

- 分層到物件儲存的資料不包含ONTAP WORM 功能。為了確保端對端 WORM 功能，您需要正確設定儲存桶權限。
- 分層到物件儲存的資料不具備 WORM 功能，這意味著從技術上講，任何擁有儲存桶和容器完全存取權限的人都可以刪除由ONTAP分層的物件。
- 啟用 WORM 和分層後，恢復或降級到Cloud Volumes ONTAP 9.8 的操作將被阻止。

限制

- Cloud Volumes ONTAP中的 WORM 儲存體在「可信任儲存管理員」模型下運作。雖然 WORM 文件受到保護以防止更改或修改，但即使這些卷包含未過期的 WORM 數據，群集管理員也可以刪除這些卷。
- 除了可信任儲存管理員模式之外， Cloud Volumes ONTAP中的 WORM 儲存也隱式地在「可信任雲端管理員」模式下運作。雲端管理員可以透過直接從雲端提供者刪除或編輯雲端儲存來在 WORM 資料到期之前將其刪除。

相關連結

- "為 WORM 儲存建立防篡改 Snapshot 副本"
- "Cloud Volumes ONTAP中的授權和計費"

高可用性對

了解 **AWS** 中的**Cloud Volumes ONTAP HA** 對

Cloud Volumes ONTAP高可用性 (HA) 設定提供無中斷操作和容錯功能。在AWS中，資料在兩個節點之間同步鏡像。

HA 組件

在 AWS 中， Cloud Volumes ONTAP HA 配置包含以下元件：

- 兩個Cloud Volumes ONTAP節點，其資料彼此同步鏡像。
- 中介實例在節點之間提供通訊通道，以協助儲存接管和交還過程。

調解員

以下是有關 AWS 中中介實例的一些關鍵細節：

實例類型
: t3-micro

磁碟
: 兩個 8 GiB 和 4 GiB 的 st1 磁碟

作業系統
: Debian 11

對於Cloud Volumes ONTAP 9.10.0 及更早版本，調解器上安裝了 Debian 10。

升級

升級Cloud Volumes ONTAP時， NetApp Console也會根據需求更新中介實例。

存取實例

當您從控制台建立Cloud Volumes ONTAP HA 對時，系統會提示您為中介實例提供金鑰對。您可以使用該金鑰對進行 SSH 訪問 `admin`用戶。

第三方代理

中介實例不支援第三方代理或 VM 擴充。

儲存接管和交還

如果一個節點發生故障，另一個節點可以為其夥伴提供資料以提供持續的資料服務。客戶端可以從夥伴節點存取相同的數據，因為資料已同步鏡像到夥伴節點。

節點重啟後，夥伴必須重新同步資料才能返回儲存。重新同步資料所需的時間取決於節點關閉時更改的資料量。

預設情況下，儲存接管、重新同步和復原都是自動的。無需用戶操作。

RPO 和 **RTO**

HA 配置透過以下方式維護資料的高可用性：

- 恢復點目標 (RPO) 為 0 秒。您的資料在事務上是一致的，沒有資料遺失。
- 恢復時間目標 (RTO) 為 120 秒。如果發生中斷，資料應在 120 秒或更短時間內可用。

HA部署模型

您可以透過跨多個可用區 (AZ) 或在單一可用區 (AZ) 中部署 HA 配置來確保資料的高可用性。您應該查看有關每種配置的更多詳細信息，以選擇最適合您需求的配置。

多個可用區域

在多個可用區 (AZ) 中部署 HA 配置可確保在 AZ 或執行Cloud Volumes ONTAP節點的執行個體發生故障時資料的高可用性。您應該了解 NAS IP 位址如何影響資料存取和儲存故障轉移。

NFS 和 **CIFS** 資料訪問

當 HA 設定分佈在多個可用區域時，_浮動 IP 位址_可啟用 NAS 用戶端存取。浮動 IP 位址必須位於區域內所有 VPC 的 CIDR 區塊之外，當發生故障時，浮動 IP 位址可以在節點之間遷移。 VPC 以外的客戶端無法原生存取它們，除非你"設定 AWS 中繼網關"。

如果您無法設定傳輸網關，則可以為 VPC 外部的 NAS 用戶端提供私人 IP 位址。但是，這些 IP 位址是靜態的——它們無法在節點之間進行故障轉移。

在跨多個可用區域部署 HA 設定之前，您應該查看浮動 IP 位址和路由表的要求。部署配置時必須指定浮動 IP 位址。私有 IP 位址是自動建立的。

有關詳細信息，請參閱"多個可用區中Cloud Volumes ONTAP HA 的 AWS 網路需求" 。

iSCSI 資料存取

由於 iSCSI 不使用浮動 IP 位址，因此跨 VPC 資料通訊不是問題。

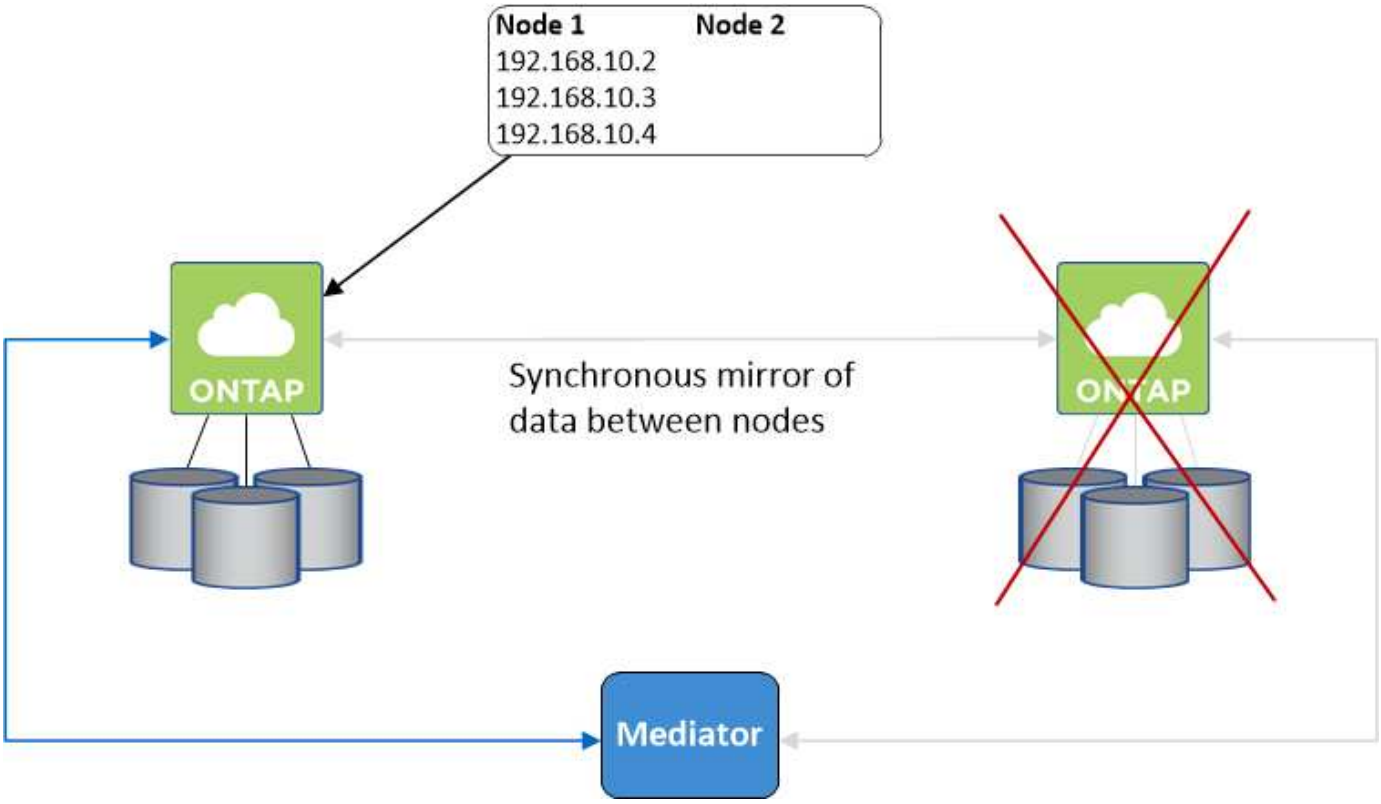
iSCSI 的接手與交還

對於 iSCSI， Cloud Volumes ONTAP使用多路徑 I/O (MPIO) 和非對稱邏輯單元存取 (ALUA) 來管理主動最佳化路徑和非最佳化路徑之間的路徑故障轉移。

有關哪些特定主機配置支援 ALUA 的信息，請參閱 "NetApp互通性表工具"以及 "SAN 主機和雲端客戶端指南"適用於您的主機作業系統。

NAS 的接管和交還

當使用浮動 IP 的 NAS 配置中發生接管時，用戶端用於存取資料的節點的浮動 IP 位址將會移至另一個節點。下圖描述了使用浮動 IP 的 NAS 配置中的儲存接管。如果節點 2 發生故障，則節點 2 的浮動 IP 位址將會移至節點 1。



用於外部 VPC 存取的 NAS 資料 IP 如果發生故障，則無法在節點之間遷移。如果某個節點離線，您必須使用另一個節點上的 IP 位址手動將磁碟區重新掛載到 VPC 外部的用戶端。

故障節點恢復上線後，使用原始 IP 位址將用戶端重新掛載到磁碟區。需要執行此步驟以避免在兩個 HA 節點之間傳輸不必要的數據，這會對效能和穩定性造成嚴重影響。

您可以透過選擇磁碟區並按一下「安裝命令」從控制台找到正確的 IP 位址。

單一可用區

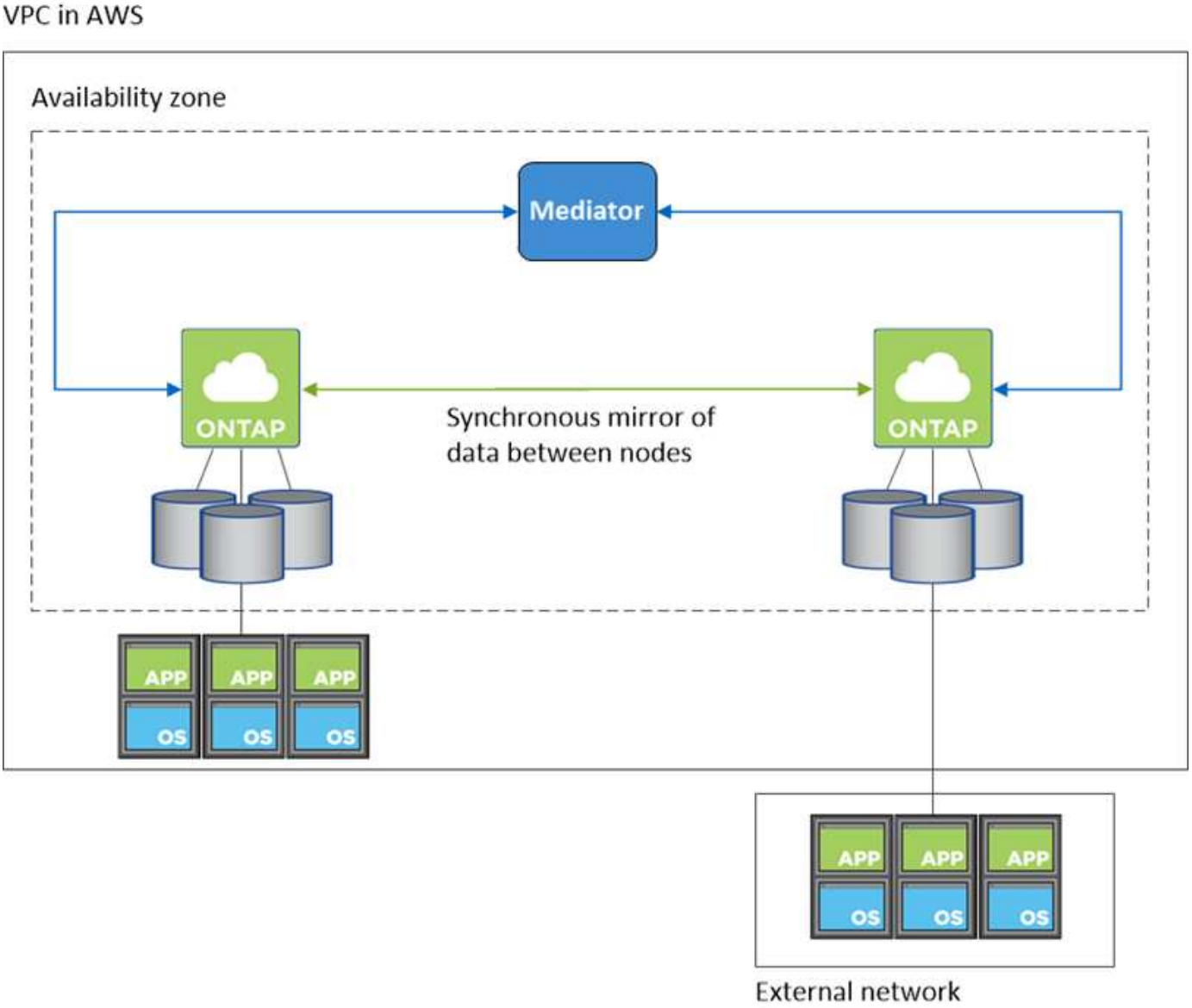
如果執行Cloud Volumes ONTAP節點的執行個體發生故障，在單一可用區 (AZ) 中部署 HA 配置可以確保資料的高可用性。所有資料都可以從 VPC 外部本地存取。

控制台建立一個 "AWS 文件：AWS 分佈置放群組"並啟動該放置組中的兩個 HA 節點。放置組透過將實例分佈在不同的底層硬體上來降低同時發生故障的風險。此功能從計算角度而不是從磁碟故障角度提高了冗餘度。

資料存取

由於此配置位於單一 AZ 中，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 外部進行資料存取。

下圖顯示了單一 AZ 中的 HA 配置。可以從 VPC 內部和 VPC 外部存取資料。



接手和返還

對於 iSCSI， Cloud Volumes ONTAP使用多路徑 I/O (MPIO) 和非對稱邏輯單元存取 (ALUA) 來管理主動最佳化路徑和非最佳化路徑之間的路徑故障轉移。

有關哪些特定主機配置支援 ALUA 的信息，請參閱 "NetApp互通性表工具"以及 "SAN 主機和雲端客戶端指南"適用於您的主機作業系統。

對於 NAS 配置，如果發生故障，資料 IP 位址可以在 HA 節點之間遷移。這確保了客戶端可以存取儲存。

AWS 本地區域

AWS 本地區域是一種基礎設施部署，其中儲存、運算、資料庫和其他精選 AWS 服務位於大城市和工業區附近。借助 AWS 本地區域，您可以讓 AWS 服務更接近您，從而改善工作負載的延遲並在本地維護資料庫。在Cloud Volumes ONTAP，

您可以在 AWS 本機區域中部署單一 AZ 或多個 AZ 配置。

在標準和私有模式下使用控制台時支援 AWS 本地區域。目前，AWS 本地區域不支援受限模式。

AWS 本機區域設定範例

AWS 中的Cloud Volumes ONTAP僅支援單一可用區域中的高可用性 (HA) 模式。不支援單節點部署。

Cloud Volumes ONTAP不支援 AWS 本地區域中的資料分層、雲端分層和不合格實例。

以下是範例配置：

- 單一可用區域：叢集節點和中介器均位於同一本地區域。
- 多重可用區 在多可用區配置中，有三個實例、兩個節點和一個中介器。三個實例中必須有一個實例位於單獨的區域。您可以選擇如何設定。

  以下是三個範例配置：

  - 每個叢集節點位於不同的本地區域，中介位於公共可用區域。
  - 一個叢集節點位於本機區域中，調解器位於本機區域中，第二個叢集節點位於可用區域中。
  - 每個叢集節點和中介器位於單獨的本地區域。

支援的磁碟和實例類型

唯一支援的磁碟類型是 GP2。目前支援以下大小從 xlarge 到 4xlarge 的 EC2 執行個體類型系列：

- M5
- C5
- C5d
- R5
- R5d

Cloud Volumes ONTAP 僅支援這些配置。在 AWS Local Zone 配置中選擇不支援的磁碟類型或不符合要求的執行個體可能會導致部署失敗。如果您的 Cloud Volumes ONTAP 系統位於 AWS Local Zone 中，則不支援將資料分層至 Amazon Simple Storage Service（Amazon S3），因為存取 Local Zone 以外的 Amazon S3 儲存貯體會產生更高的延遲，並影響 Cloud Volumes ONTAP 活動。

"AWS 文件：本地區域中的 EC2 執行個體類型" 。

HA 對中的儲存工作原理

與ONTAP叢集不同， Cloud Volumes ONTAP HA 對中的儲存不會在節點之間共用。相反，資料在節點之間同步鏡像，以便在發生故障時資料可用。

儲存分配

當您建立新磁碟區並且需要額外的磁碟時，控制台會為兩個節點指派相同數量的磁碟，建立鏡像聚合，然後建立新磁碟區。例如，如果磁碟區需要兩個磁碟，則控制台會為每個節點分配兩個磁碟，總共四個磁碟。

儲存配置

您可以將 HA 對用作主動-主動配置，其中兩個節點都向客戶端提供數據，或用作主動-被動配置，其中被動節點僅在接管主動節點的儲存後才會回應資料請求。

只有在使用儲存系統視圖中的控制台時，您才可以設定主動-主動配置。

績效預期

Cloud Volumes ONTAP HA 配置在節點之間同步複製數據，這會消耗網路頻寬。因此，與單節點Cloud Volumes ONTAP配置相比，您可以獲得以下效能：

- 對於僅從一個節點提供資料的 HA 配置，讀取效能與單節點配置的讀取效能相當，而寫入效能較低。
- 對於從兩個節點提供資料的 HA 配置，讀取效能高於單節點配置的讀取效能，寫入效能相同或更高。

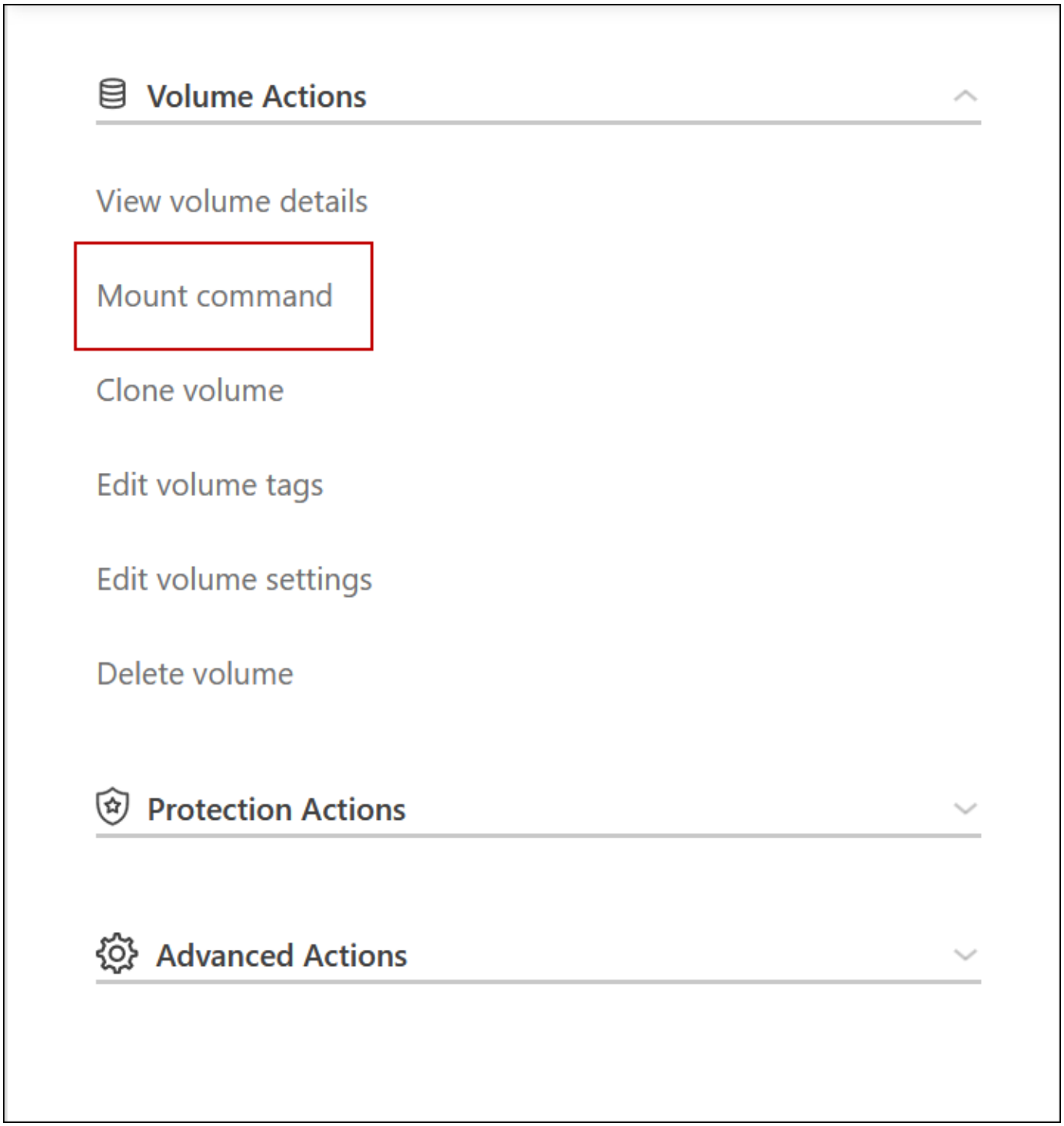
有關Cloud Volumes ONTAP效能的更多詳細信息，請參閱"表現"。

客戶端存取儲存

用戶端應使用磁碟區所在節點的資料 IP 位址存取 NFS 和 CIFS 磁碟區。如果 NAS 用戶端使用夥伴節點的 IP 位址存取卷，則流量會在兩個節點之間流動，從而降低效能。

如果在 HA 對中的節點之間移動磁碟區，則應使用另一個節點的 IP 位址重新掛載該磁碟區。否則，您可能會遇到效能下降的情況。如果用戶端支援 NFSv4 引用或 CIFS 資料夾重新導向，您可以在Cloud Volumes ONTAP系統上啟用這些功能以避免重新掛載磁碟區。有關詳細信息，請參閱ONTAP文件。

您可以透過管理磁碟區面板下的_Mount Command_選項輕鬆識別正確的IP位址。

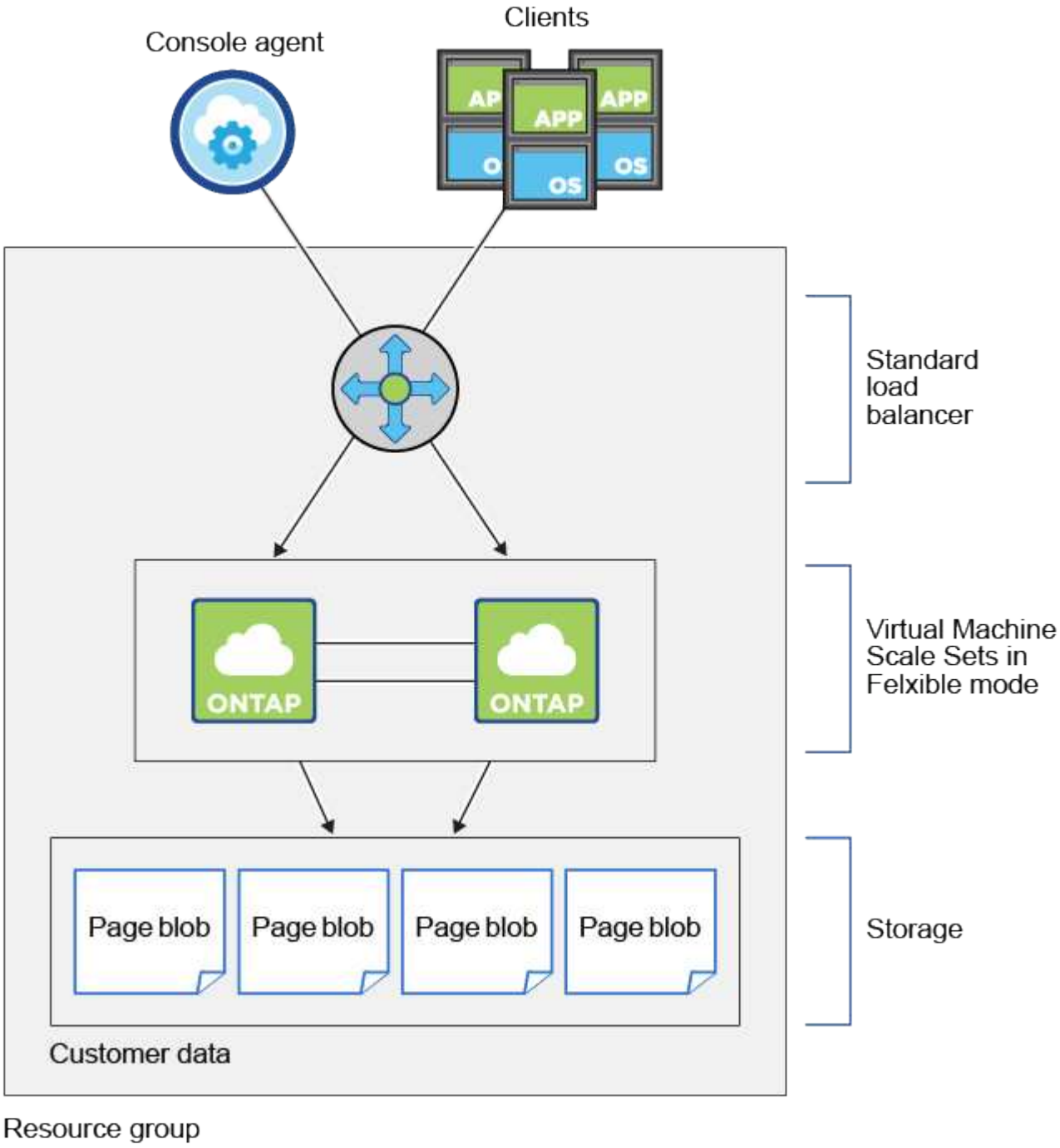


了解 **Azure** 中的**Cloud Volumes ONTAP HA** 對

Cloud Volumes ONTAP高可用性 (HA) 對可在您的雲端環境發生故障時提供企業可靠性和持續運作。在 Azure 中，儲存在兩個節點之間共用。

HA 組件

Azure 中的Cloud Volumes ONTAP HA 頁面 blob 設定包含下列元件：



請注意有關NetApp Console為您部署的 Azure 元件的以下事項：

Azure 標準負載平衡器

負載平衡器管理傳入Cloud Volumes ONTAP HA 對的流量。

單一可用區域中的虛擬機

從Cloud Volumes ONTAP 9.15.1 開始，您可以在單一可用區 (AZ) 中建立和管理異質虛擬機器 (VM)。您可以在相同可用區內的不同故障域中部署高可用性 (HA) 節點，以確保最佳可用性。要了解有關實現此功能的靈活

編排模式的更多信息，請參閱 "Microsoft Azure 文件：虛擬機器規模集"。

磁碟

客戶資料駐留在高級儲存頁面 blob 上。每個節點都可以存取其他節點的儲存。還需要額外的儲存空間"引導、根和核心數據"。

儲存帳戶

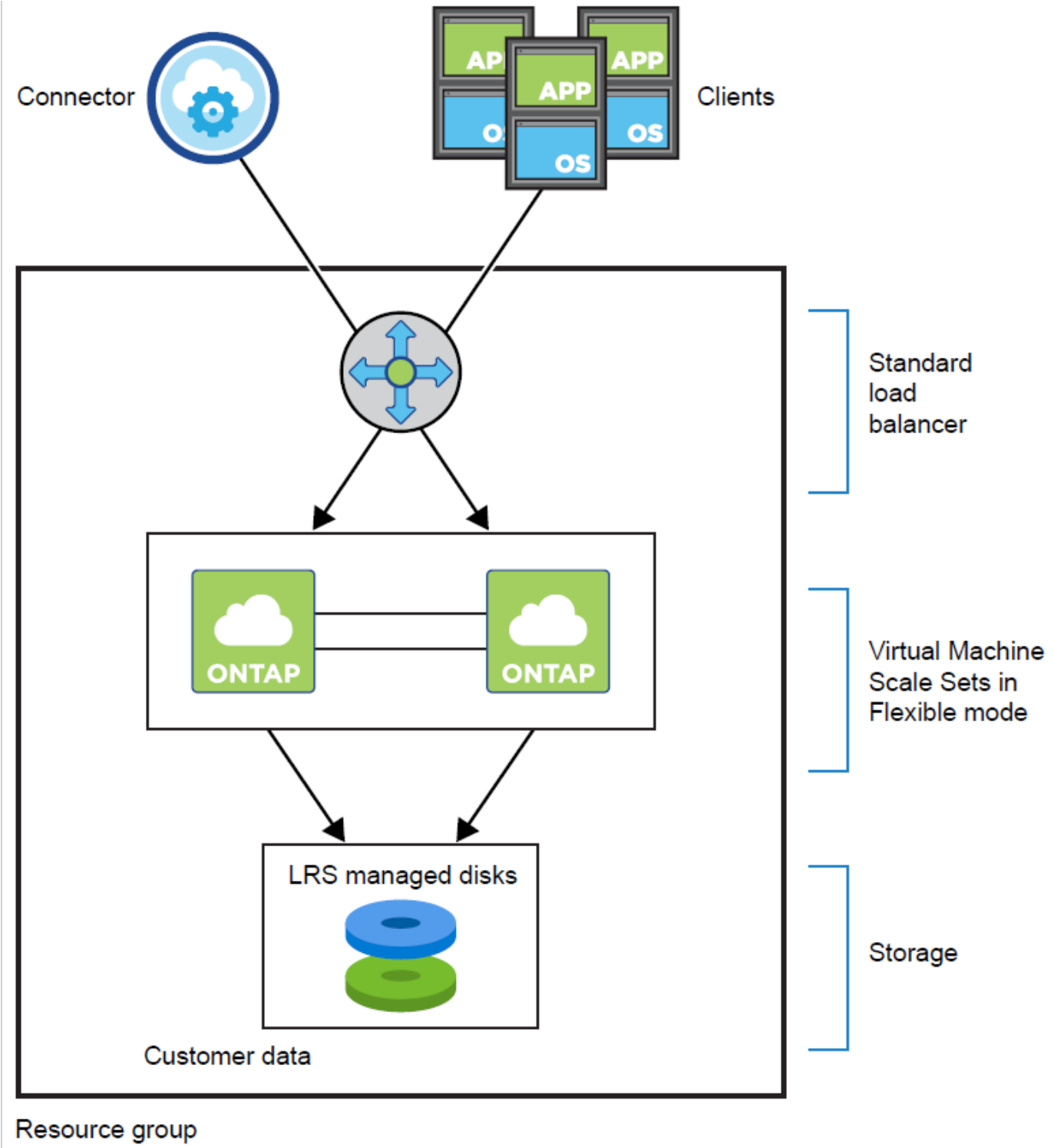
- 託管磁碟需要一個儲存帳戶。
- 由於已達到每個儲存帳戶的磁碟容量限制，因此進階儲存頁面 Blob 需要一個或多個儲存帳戶。

  "Microsoft Azure 文件：Azure 儲存空間可擴充性和儲存帳戶的效能目標" 。
- 將資料分層到 Azure Blob 儲存體需要一個儲存帳戶。
- 從Cloud Volumes ONTAP 9.7 開始，控制台為 HA 對建立的儲存帳戶是通用 v2 儲存帳戶。
- 新增Cloud Volumes ONTAP系統時，您可以啟用從Cloud Volumes ONTAP 9.7 HA 對到 Azure 儲存體帳戶的 HTTPS 連線。請注意，啟用此選項可能會影響寫入效能。建立系統後，您無法變更設定。

從Cloud Volumes ONTAP 9.15.0P1 開始，Azure 頁面 blob 不再支援新的高可用性對部署。如果您目前在現有的高可用性對部署中使用 Azure 頁 Blob，則可以移轉到 Edsv4 系列 VM 和 Edsv5 系列 VM 中較新的 VM 執行個體類型。"詳細了解 Azure 中支援的配置" 。

具有共享託管磁碟的 **HA** 單可用區域配置

在共用託管磁碟上執行的Cloud Volumes ONTAP HA 單可用區配置包括以下元件：



請注意有關控制台為您部署的 Azure 元件的下列事項：

Azure 標準負載平衡器

負載平衡器管理傳入Cloud Volumes ONTAP HA 對的流量。

單一可用區域中的虛擬機

從Cloud Volumes ONTAP 9.15.1 開始，您可以在單一可用區 (AZ) 中建立和管理異質虛擬機器 (VM)。您可以在相同可用區內的不同故障域中部署高可用性 (HA) 節點，以確保最佳可用性。要了解有關實現此功能的靈活編排模式的更多信息，請參閱 "Microsoft Azure 文件：虛擬機器規模集"。

當滿足以下條件時，區域部署將使用進階 SSD v2 託管磁碟：

- Cloud Volumes ONTAP的版本為 9.15.1 或更高版本。
- 所選區域和區域支援高級 SSD v2 託管磁碟。有關受支援區域的信息，請參閱 "Microsoft Azure 網站：按地區提供的產品"。
- 訂閱已註冊為 Microsoft"Microsoft.Compute/VMOrchestratorZonalMultiFD 功能" 。

如果您為符合上述條件的環境選擇進階 SSD 管理磁碟，控制台將自動部署進階 SSD v2 管理磁碟。您無法切換到進階 SSD v1 管理磁碟。

磁碟

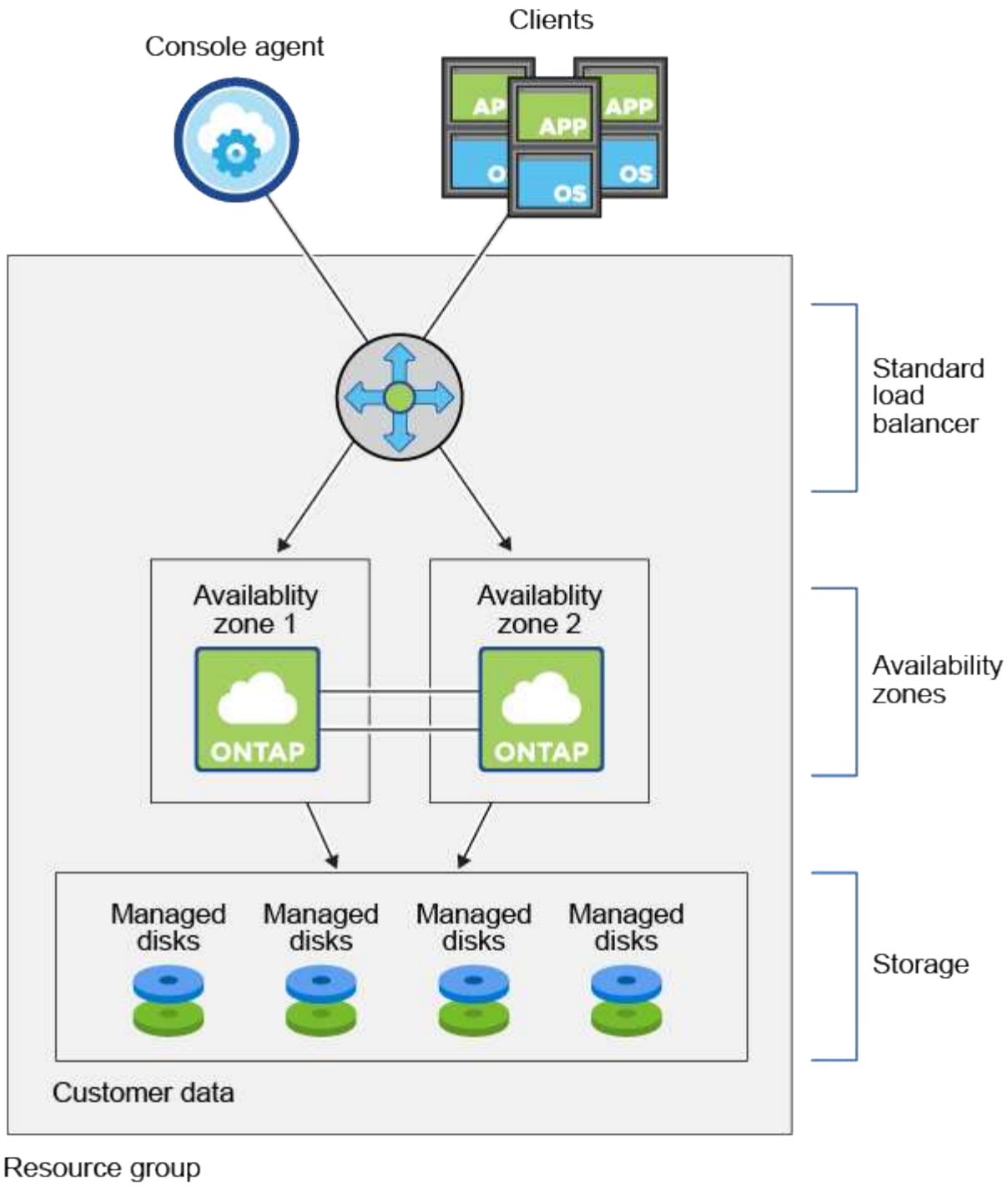
客戶資料駐留在本地冗餘儲存 (LRS) 管理的磁碟上。每個節點都可以存取其他節點的儲存。還需要額外的儲存空間"啟動、根、合作夥伴根、核心和NVRAM數據"。

儲存帳戶

儲存帳戶用於基於託管磁碟的部署，以處理診斷日誌和分層到 Blob 儲存。

HA 多可用區配置

Azure 中的Cloud Volumes ONTAP HA 多可用區域設定包含下列元件：



請注意有關控制台為您部署的 Azure 元件的下列事項：

Azure 標準負載平衡器

負載平衡器管理傳入Cloud Volumes ONTAP HA 對的流量。

可用區域

HA 多可用區配置採用部署模型，其中兩個Cloud Volumes ONTAP節點部署到不同的可用區，確保節點位於不同的故障域中以提供冗餘和可用性。若要了解在靈活編排模式下的虛擬機器規模集如何使用 Azure 中的可用性區域，請參閱 "Microsoft Azure 文件：建立使用可用性區域的虛擬機器規模集"。

磁碟

客戶資料駐留在區域冗餘儲存 (ZRS) 託管磁碟上。每個節點都可以存取其他節點的儲存。還需要額外的儲存空間"啟動、根、合作夥伴根和核心數據"。

儲存帳戶

儲存帳戶用於基於託管磁碟的部署，以處理診斷日誌和分層到 Blob 儲存。

RPO 和 RTO

HA 配置可依照以下方式維護資料的高可用性：

- 恢復點目標 (RPO) 為 0 秒。您的資料在事務上是一致的，沒有資料遺失。
- 恢復時間目標 (RTO) 為 120 秒。如果發生中斷，資料應在 120 秒或更短時間內可用。

儲存接管和交還

與實體ONTAP叢集類似，Azure HA 對中的儲存空間在節點之間共用。與合作夥伴儲存的連接允許每個節點在發生_接管_時存取其他節點的儲存。網路路徑故障轉移機制確保客戶端和主機繼續與倖存節點通訊。當節點重新上線時，合作夥伴將歸還儲存。

對於 NAS 配置，如果發生故障，資料 IP 位址會在 HA 節點之間自動遷移。

對於 iSCSI， Cloud Volumes ONTAP使用多路徑 I/O (MPIO) 和非對稱邏輯單元存取 (ALUA) 來管理主動最佳化路徑和非最佳化路徑之間的路徑故障轉移。

有關哪些特定主機配置支援 ALUA 的信息，請參閱 "NetApp互通性表工具"以及 "SAN 主機和雲端客戶端指南"適用於您的主機作業系統。

預設情況下，儲存接管、重新同步和復原都是自動的。無需用戶操作。

儲存配置

您可以將 HA 對用作主動-主動配置，其中兩個節點都向客戶端提供數據，或用作主動-被動配置，其中被動節點僅在接管主動節點的儲存後才會回應資料請求。

了解 Google Cloud 中的Cloud Volumes ONTAP HA 對

Cloud Volumes ONTAP高可用性 (HA) 設定提供無中斷操作和容錯功能。在 Google Cloud 中，資料在兩個節點之間同步鏡像。

HA 組件

Google Cloud 中的Cloud Volumes ONTAP HA 設定包含以下元件：

- 兩個Cloud Volumes ONTAP節點，其資料彼此同步鏡像。
- 中介實例在節點之間提供通訊通道，以協助儲存接管和交還過程。
- 一個區域或三個區域（建議）。

  如果您選擇三個區域，則兩個節點和中介器位於單獨的 Google Cloud 區域。

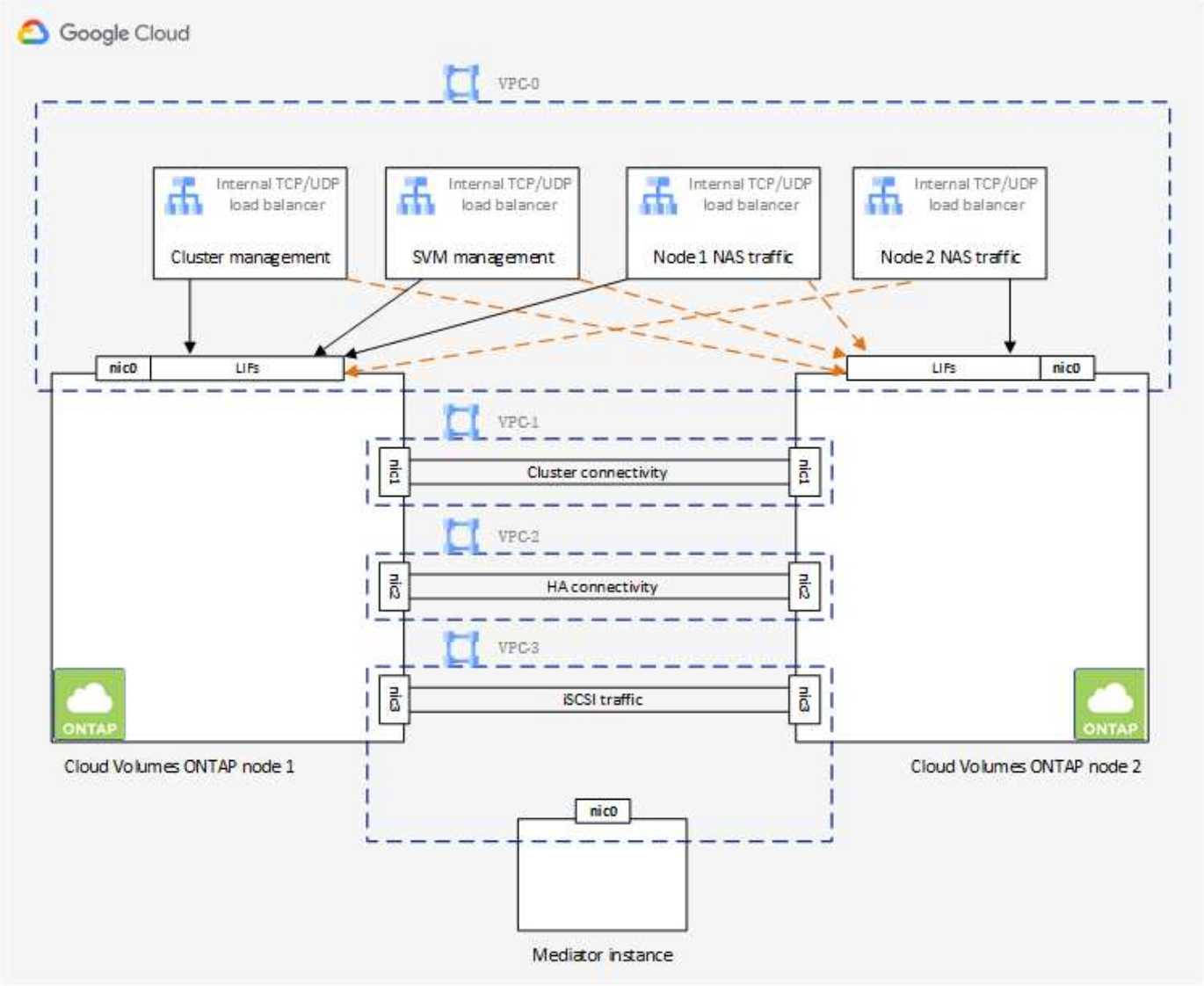
- 四個虛擬私有雲（VPC）。

  此配置使用四個 VPC，因為 GCP 要求每個網路介面位於單獨的 VPC 網路中。

- 四個 Google Cloud 內部負載平衡器（TCP/UDP），用於管理傳入Cloud Volumes ONTAP HA 對的流量。

"了解網路要求"，包括有關負載平衡器、VPC、內部 IP 位址、子網路等的更多詳細資訊。

以下概念圖展示了Cloud Volumes ONTAP HA 對及其元件：



調解員

以下是 Google Cloud 中介實例的一些關鍵細節：

實例類型

e2-micro（之前使用過 f1-micro 實例）

磁碟

兩個標準永久性磁碟，每個磁碟 10 GiB

作業系統

Debian 11

對於Cloud Volumes ONTAP 9.10.0 及更早版本，調解器上安裝了 Debian 10。

升級

升級Cloud Volumes ONTAP時， NetApp Console也會根據需求更新中介實例。

存取實例

對於 Debian 系統，預設雲端使用者是 `admin`。當透過 Google Cloud Console 或 gcloud 命令列請求 SSH 存取時，Google Cloud 會為 `admin`使用者建立並新增憑證。您可以指定 `sudo`來取得 root 權限。

第三方代理

中介實例不支援第三方代理或 VM 擴充。

儲存接管和交還

如果一個節點發生故障，另一個節點可以為其夥伴提供資料以提供持續的資料服務。客戶端可以從夥伴節點存取相同的數據，因為資料已同步鏡像到夥伴節點。

節點重啟後，夥伴必須重新同步資料才能返回儲存。重新同步資料所需的時間取決於節點關閉時更改的資料量。

預設情況下，儲存接管、重新同步和復原都是自動的。無需用戶操作。

RPO 和 **RTO**

HA 配置可依照以下方式維護資料的高可用性：

- 恢復點目標 (RPO) 為 0 秒。

  您的資料在事務上是一致的，沒有資料遺失。

- 恢復時間目標 (RTO) 為 120 秒。

  如果發生中斷，資料應在 120 秒或更短時間內可用。

HA部署模型

您可以透過在多個區域或單一區域中部署 HA 配置來確保資料的高可用性。

多區域（建議）

跨三個區域部署 HA 配置可確保當一個區域內發生故障時資料仍然可用。請注意，與使用單一區域相比，寫入效能略低，但差異很小。

單區

在單一區域中部署時， Cloud Volumes ONTAP HA 配置使用分散放置策略。此策略可確保 HA 配置免受區域內單點故障的影響，而無需使用單獨的區域來實現故障隔離。

這種部署模型確實降低了您的成本，因為區域之間沒有資料流出費用。

HA 對中的儲存工作原理

與ONTAP叢集不同，GCP 中的Cloud Volumes ONTAP HA 對中的儲存不會在節點之間共用。相反，資料在節點之間同步鏡像，以便在發生故障時資料可用。

儲存分配

當您建立新磁碟區並且需要額外的磁碟時，控制台會為兩個節點指派相同數量的磁碟，建立鏡像聚合，然後建立新磁碟區。例如，如果磁碟區需要兩個磁碟，則控制台會為每個節點分配兩個磁碟，總共四個磁碟。

儲存配置

您可以將 HA 對用作主動-主動配置，其中兩個節點都向客戶端提供數據，或用作主動-被動配置，其中被動節點僅在接管主動節點的儲存後才會回應資料請求。

HA 配置的效能預期

Cloud Volumes ONTAP HA 配置在節點之間同步複製數據，這會消耗網路頻寬。因此，與單節點Cloud Volumes ONTAP配置相比，您可以獲得以下效能：

- 對於僅從一個節點提供資料的 HA 配置，讀取效能與單節點配置的讀取效能相當，而寫入效能較低。
- 對於從兩個節點提供資料的 HA 配置，讀取效能高於單節點配置的讀取效能，寫入效能相同或更高。

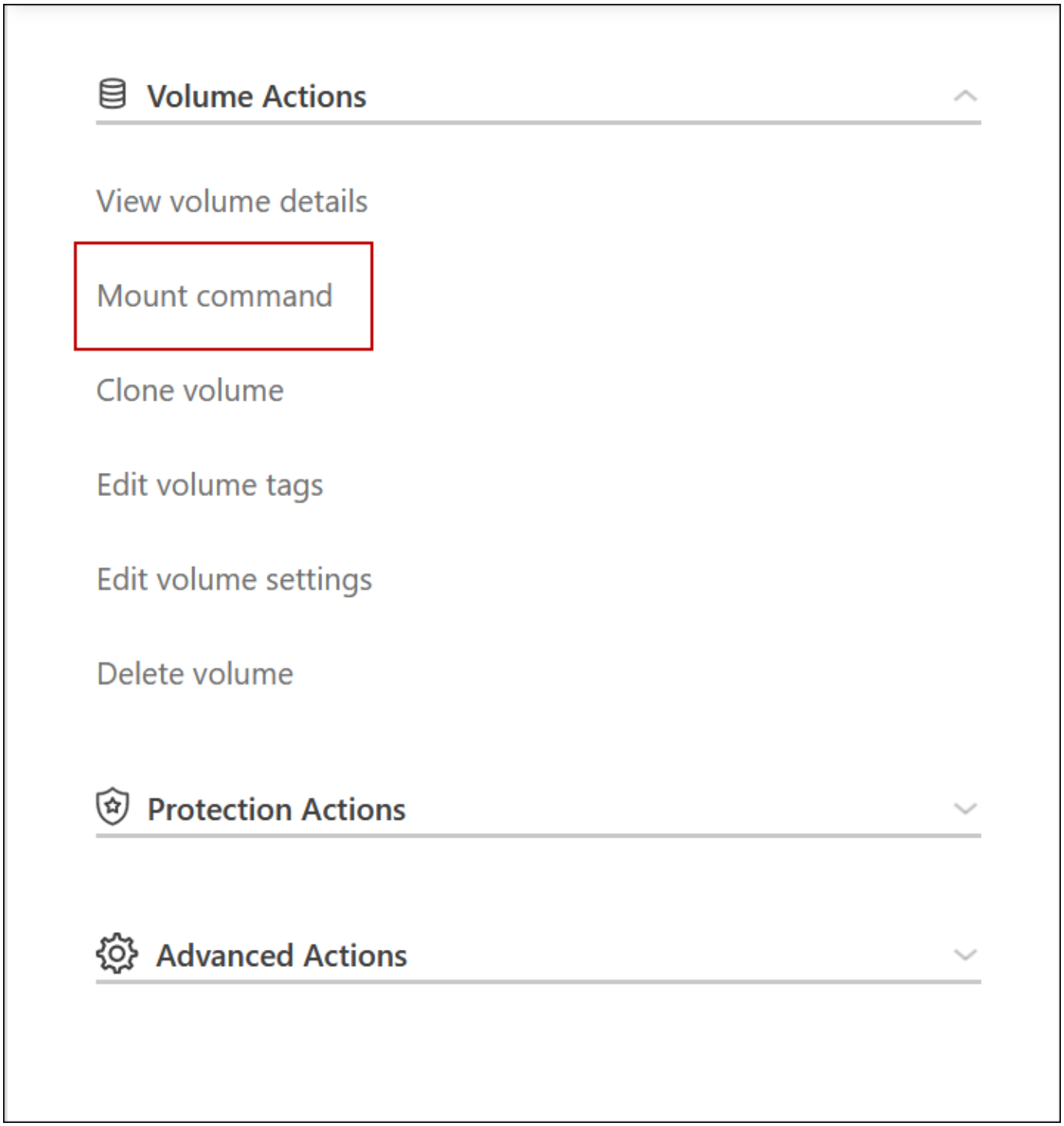
有關Cloud Volumes ONTAP效能的更多詳細信息，請參閱"表現"。

客戶端存取儲存

用戶端應使用磁碟區所在節點的資料 IP 位址存取 NFS 和 CIFS 磁碟區。如果 NAS 用戶端使用夥伴節點的 IP 位址存取卷，則流量會在兩個節點之間流動，從而降低效能。

如果在 HA 對中的節點之間移動磁碟區，則應使用另一個節點的 IP 位址重新掛載該磁碟區。否則，您可能會遇到效能下降的情況。如果用戶端支援 NFSv4 引用或 CIFS 資料夾重新導向，您可以在Cloud Volumes ONTAP系統上啟用這些功能以避免重新掛載磁碟區。有關詳細信息，請參閱ONTAP文件。

您可以透過選擇磁碟區並按一下「安裝命令」從控制台找到正確的 IP 位址。



相關連結

- "了解網路要求"
- "了解如何開始使用 GCP"

當Cloud Volumes ONTAP HA 對中的節點處於離線狀態時，操作就無法使用

當 HA 對中的一個節點不可用時，另一個節點將為其夥伴提供資料以提供持續的資料服務。這被稱為_存儲接管_。在儲存恢復完成之前，有些操作無法執行。

當 HA 對中的某個節點不可用時， NetApp Console中的系統狀態為「Degraded」。

儲存接管後無法執行以下操作：

- 支援註冊
- 許可證變更
- 實例或虛擬機器類型更改
- 寫入速度變化
- CIFS 設定
- 變更配置備份的位置
- 設定集群密碼
- 管理磁碟和聚合（高級分配）

儲存交還完成且系統狀態恢復正常後，這些操作將再次可用。

了解Cloud Volumes ONTAP資料加密與勒索軟體防護

Cloud Volumes ONTAP支援資料加密並提供防毒和勒索軟體的保護。

靜態資料加密

Cloud Volumes ONTAP支援以下加密技術：

- 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

您可以將NetApp加密解決方案與雲端提供者提供的本機加密結合使用，以在虛擬機器管理程式層級加密資料。這樣做可以提供雙重加密，這對於非常敏感的資料來說可能是必要的。當存取加密資料時，它會被解密兩次 - 一次在虛擬機管理程式層級（使用來自雲端提供者的金鑰），然後再次使用NetApp加密解決方案（使用來自外部金鑰管理員的金鑰）。

NetApp加密解決方案（NVE 和 NAE）

Cloud Volumes ONTAP支持 "NetApp磁碟區加密 (NVE) 與NetApp聚合加密 (NAE)"。 NVE 和 NAE 是基於軟體的解決方案，可實現符合 (FIPS) 140-2 標準的磁碟區靜態資料加密。 NVE 和 NAE 都使用 AES 256 位元加密。

- NVE 每次都會對一個磁碟區的靜態資料進行加密。每個資料卷都有自己獨特的加密金鑰。
- NAE 是 NVE 的擴展——它對每個磁碟區的資料進行加密，並且磁碟區在聚合體中共用一個金鑰。 NAE 還允許對聚合中所有磁碟區的公共區塊進行重複資料刪除。

Cloud Volumes ONTAP透過 AWS、Azure 和 Google Cloud 提供的外部金鑰管理服務 (EKM) 支援 NVE 和 NAE，包括第三方解決方案，例如 Fortanix。與ONTAP不同，對於Cloud Volumes ONTAP，加密金鑰是在雲端提供者端產生的，而不是在ONTAP中產生的。Cloud Volumes ONTAP不支援 "板載密鑰管理器"。

Cloud Volumes ONTAP使用ONTAP所使用的標準金鑰管理互通性協定 (KMIP) 服務。有關支援服務的更多信息，請參閱 "互通性矩陣工具"。

如果您使用 NVE，則可以選擇使用雲端提供者的金鑰保管庫來保護ONTAP加密金鑰：

- AWS 金鑰管理服務 (KMS)
- Azure 金鑰保管庫 (AKV)
- Google Cloud 金鑰管理服務

設定外部金鑰管理器後，新聚合預設啟用NetApp聚合加密 (NAE)。不屬於 NAE 聚合的新磁碟區預設啟用 NVE（例如，如果您有在設定外部金鑰管理員之前建立的現有聚合）。

設定支援的密鑰管理器是唯一需要的步驟。有關設定說明，請參閱"使用NetApp加密解決方案加密卷"。

AWS 金鑰管理服務

在 AWS 中啟動Cloud Volumes ONTAP系統時，您可以使用 "AWS 金鑰管理服務 (KMS)"。 NetApp Console使用客戶主金鑰 (CMK) 請求資料金鑰。

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

如果您想使用此加密選項，則必須確保 AWS KMS 已正確設定。有關信息，請參閱"設定 AWS KMS"。

Azure 儲存服務加密

使用以下方式在 Azure 中的Cloud Volumes ONTAP上自動加密數據 "Azure 儲存服務加密"使用 Microsoft 管理的金鑰。

如果您願意，您可以使用自己的加密金鑰。"了解如何設定Cloud Volumes ONTAP以在 Azure 中使用客戶管理的金鑰"。

Google Cloud Platform 預設加密

"Google Cloud Platform 靜態資料加密"對於Cloud Volumes ONTAP ，預設為啟用。無需設定。

雖然 Google Cloud Storage 總是會在將資料寫入磁碟之前加密，但您可以使用控制台 API 建立使用_客戶管理加密金鑰_的Cloud Volumes ONTAP系統。這些是您使用雲端金鑰管理服務在 GCP 中產生和管理的金鑰。"了解更多"。

ONTAP病毒掃描

您可以使用ONTAP系統上的整合防毒功能來保護資料免受病毒或其他惡意程式碼的侵害。

ONTAP病毒掃描（稱為「Vscan」）將一流的第三方防毒軟體與ONTAP功能結合，讓您可以靈活地控制掃描哪些檔案以及何時掃描。

有關 Vscan 支援的供應商、軟體和版本的信息，請參閱 "NetApp互通性表"。

有關如何在ONTAP系統上設定和管理防毒功能的信息，請參閱 "ONTAP 9 防毒設定指南"。

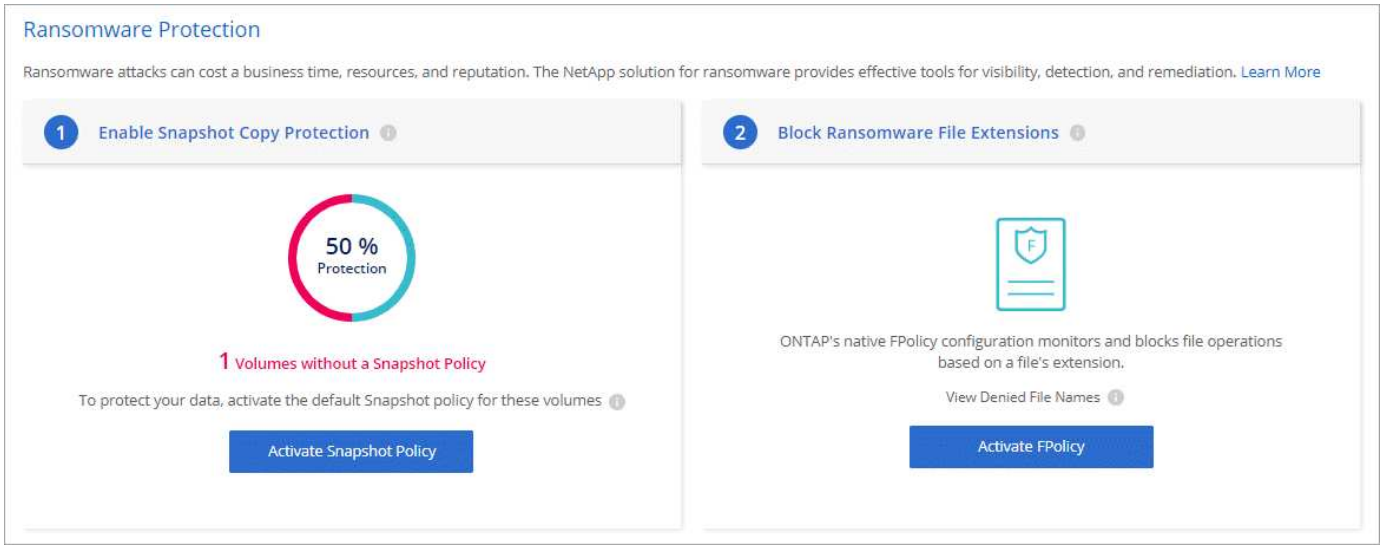
勒索軟體防護

勒索軟體攻擊會浪費企業的時間、資源和聲譽。控制台使您能夠實施針對勒索軟體的NetApp解決方案，該解決方案提供了有效的可見性、檢測和補救工具。

- 控制台識別未受快照策略保護的捲，並允許您在這些卷上啟動預設快照策略。

  快照副本是唯讀的，可防止勒索軟體破壞。他們還可以提供創建單一文件副本或完整災難復原解決方案的圖像的粒度。

- 透過啟用 ONTAP 的 FPolicy 解決方案，控制台還允許您阻止常見的勒索軟體檔案副檔名。



"了解如何實施NetApp勒索軟體解決方案" 。

了解Cloud Volumes ONTAP工作負載的效能監控

您可以查看效能結果以協助您確定哪些工作負載適合Cloud Volumes ONTAP。

性能技術報告

- 適用於 AWS 的Cloud Volumes ONTAP

  "NetApp技術報告 4383：Amazon Web Services 中Cloud Volumes ONTAP與應用程式工作負載的效能特徵"

- 適用於 Microsoft Azure 的Cloud Volumes ONTAP

  "NetApp技術報告 4671：Azure 中Cloud Volumes ONTAP與應用程式工作負載的效能特徵"

- 適用於 Google Cloud 的Cloud Volumes ONTAP

  "NetApp技術報告 4816：適用於 Google Cloud 的Cloud Volumes ONTAP的效能特徵"

CPU 效能

從您的雲端供應商的監控工具來看， Cloud Volumes ONTAP節點的使用率很高（超過 90%）。這是因為ONTAP保留了虛擬機器中存在的所有 vCPU，以便在需要時可用。

欲了解更多信息，請參閱 "NetApp知識庫文章，介紹如何使用 CLI 監控ONTAP CPU 使用率"

基於節點的 BYOL 授權管理

每個具有基於節點的自帶許可證 (BYOL) 的Cloud Volumes ONTAP系統都必須安裝具有有效訂閱的系統授權。 NetApp Console透過為您管理許可證並在許可證到期前顯示警告來簡化流程。

基於節點的許可證是Cloud Volumes ONTAP的上一代許可證。基於節點的授權可以從NetApp (BYOL) 購買，並且僅在特定情況下才可以續訂授權。

"了解有關Cloud Volumes ONTAP許可選項的更多信息" 。

"了解有關如何管理基於節點的許可證的更多信息" 。

BYOL 系統許可證

可以從 NetApp 購買基於節點的授權。您可以為單節點系統或 HA 配對購買的授權數量沒有限制。

已限制 BYOL 授權的購買、延期和續約。有關更多信息，請參閱 "Cloud Volumes ONTAPP的 BYOL 授權可用性受限" 。

基於節點的許可證最多可為單一節點或 HA 對提供 368 TiB 的容量。您可能已為Cloud Volumes ONTAP BYOL系統購買了多個許可證，以分配超過 368 TiB 的容量。例如，您可能有兩個許可證，為Cloud Volumes ONTAP分配最多 736 TiB 的容量。或者，您可能有四個許可證，以獲得最多 1.4 PiB 的容量。

請注意，磁碟限制可能會阻止您僅使用磁碟就達到容量限制。您可以透過以下方式超越磁碟限制"將非活動資料分層到物件存儲"。有關磁碟限制的信息，請參閱 "Cloud Volumes ONTAP發行說明中的儲存限制"。

新系統的許可證管理

當您建立基於節點的 BYOL 系統時，控制台會提示您輸入許可證的序號和NetApp支援網站帳戶。控制台使用該帳戶從NetApp下載許可證檔案並將其安裝在Cloud Volumes ONTAP系統上。

"了解如何將NetApp支援網站帳戶新增至控制台" 。

如果控制台無法透過安全的網路連線存取許可證文件，您可以"自行取得文件，然後手動將文件上傳到控制台"。

許可證到期

控制台會在基於節點的許可證到期前 30 天顯示警告，並在許可證到期時再次顯示警告。下圖顯示了使用者介面中出現的 30 天到期警告：

您可以選擇系統來查看該訊息。

如果您是組織或帳戶管理員並且啟用了該選項，控制台會在透過電子郵件傳送給您的Cloud Volumes ONTAP報告中包含許可證到期警告。透過電子郵件發送的報告包含每兩週一次的許可證到期警告。

如果您不及時續約許可證， Cloud Volumes ONTAP系統將自動關閉。如果您重新啟動它，它就會再次自動關閉。

執照續期

如果您透過聯絡NetApp代表續訂基於節點的 BYOL 訂閱，控制台將自動從NetApp取得新授權並將其安裝在Cloud Volumes ONTAP系統上。

如果控制台無法透過安全的網路連線存取許可證文件，您可以"自行取得文件，然後手動將文件上傳到控制台"。

許可證轉移到新系統

當您刪除現有系統然後使用相同的授權建立新系統時，基於節點的 BYOL 授權可以在Cloud Volumes ONTAP系統之間轉移。

例如，您可能想要刪除現有的授權系統，然後將授權與不同 VPC/VNet 或雲端提供者中的新 BYOL 系統一起使用。請注意，只有_cloud-agnostic_序號才適用於任何雲端提供者。與雲無關的序號以 *908xxxx* 前綴開頭。

值得注意的是，您的 BYOL 授權與您的公司和一組特定的NetApp支援網站憑證相關聯。

了解如何將AutoSupport和Digital Advisor用於Cloud Volumes ONTAP

ONTAP的AutoSupport元件收集遙測資料並將其發送以進行分析。 Active IQ Digital Advisor （也稱為Digital Advisor）分析來自AutoSupport 的數據並提供主動護理和優化。利用人工智慧，Digital Advisor可以識別潛在問題並在其影響您的業務之前幫助您解決它們。

Digital Advisor透過雲端的入口網站和行動應用程式提供可操作的預測分析和主動支持，使您能夠優化全球混合雲中的資料基礎架構。所有擁有有效SupportEdge合約的NetApp客戶均可獲得Digital Advisor的資料驅動見解和建議（功能因產品和支援層級而異）。

您可以使用Digital Advisor執行以下一些操作：

- 計劃升級。

  Digital Advisor可識別您環境中可透過升級至較新版本的ONTAP來解決的問題，而升級顧問組件可協助您規

劃成功的升級。

- 查看系統健康狀況。

  您的Digital Advisor儀表板會報告任何健康問題並幫助您糾正這些問題。監控系統容量以確保永遠不會耗盡儲存空間。查看您的系統的支援案例。

- 管理績效。

  Digital Advisor顯示的系統效能比您在ONTAP System Manager 中看到的更長。識別影響您效能的配置和系統問題。最大限度提高效率。查看儲存效率指標並確定在更少空間內儲存更多資料的方法。

- 查看庫存和配置。

  Digital Advisor顯示完整的庫存和軟體和硬體配置資訊。查看服務合約何時到期並進行續約以確保您繼續獲得支援。

相關連結

- "NetApp文件：Digital Advisor"
- "啟動Digital Advisor"
- "SupportEdge服務"

Cloud Volumes ONTAP支援的預設配置

了解Cloud Volumes ONTAP 的預設設定方式可以幫助您設定和管理系統，特別是如果您熟悉ONTAP ，因為Cloud Volumes ONTAP的預設設定與ONTAP不同。

預設設定

- NetApp Console在部署Cloud Volumes ONTAP時會建立一個資料服務儲存虛擬機器。某些配置支援額外的儲存虛擬機器。"了解有關管理儲存虛擬機的更多信息" 。

  從 3.9.5 版本開始，初始儲存虛擬機器上啟用邏輯空間報告。當邏輯報告空間時， ONTAP會報告磁碟區空間，以便儲存效率功能節省的所有實體空間也被報告為已使用。有關內聯儲存效率功能的信息，請參閱知識庫文章 "KB：CVO 支援哪些內嵌儲存效率功能？"

- 控制台會自動在Cloud Volumes ONTAP上安裝下列ONTAP功能許可證：
  - CIFS
  - FlexCache
  - FlexClone
  - iSCSI
  - 多租戶加密金鑰管理 (MTEKM)，從Cloud Volumes ONTAP 9.12.1 GA 開始
  - NetApp磁碟區加密（僅適用於自帶授權 (BYOL) 或註冊的即用即付 (PAYGO) 系統）
  - NFS ifdef::aws[] endif::aws[] ifdef::azure[] endif::azure[]
  - SnapMirror

- SnapRestore
- SnapVault

- 預設創建了幾個網路介面：
  - 集群管理 LIF
  - 集群間 LIF
- Azure 中 HA 系統上的 SVM 管理 LIF
- Google Cloud 中 HA 系統上的 SVM 管理 LIF
- AWS 單節點系統上的 SVM 管理 LIF
- 節點管理 LIF

+ 在 Google Cloud 中，此 LIF 與集群間 LIF 結合在一起。

- iSCSI 資料 LIF
- CIFS 和 NFS 資料 LIF

> 由於雲端提供者的要求， Cloud Volumes ONTAP預設為禁用 LIF 故障轉移。將 LIF 遷移到其他連接埠會破壞實例上 IP 位址和網路介面之間的外部映射，使 LIF 無法存取。

- Cloud Volumes ONTAP使用 HTTP 將設定備份傳送到控制台代理程式。

  可以從 http://ipaddress/occm/offboxconfig/ 存取備份，其中 *ipaddress* 是控制台代理主機的 IP 位址。

  您可以使用備份重新設定您的Cloud Volumes ONTAP系統。有關配置備份的更多信息，請參閱 "ONTAP 文檔"。

- 控制台設定的一些磁碟區屬性與其他管理工具（例如ONTAP系統管理員或ONTAP CLI）不同。

  下表列出了與預設值不同的磁碟區屬性設定：

屬性	控制台配置的值
自動調整大小模式	生長
最大自動調整大小	1000% 組織或帳戶管理員可以從「設定」頁面修改此值。
安全風格	NTFS 用於 CIFS 磁碟區 UNIX 用於 NFS 卷
空間保證風格	沒有任何
UNIX 權限（僅限 NFS）	777

+
有關這些屬性的信息，請參閱"ONTAP磁碟區建立手冊頁"。

用於系統資料的內部磁碟

除了用戶資料的儲存外，控制台還購買了系統資料的雲端儲存。

AWS

- 每個節點有三個磁碟用於啟動、根和核心資料：
  - 47 GiB io1 磁碟用於啟動數據
  - 140 GiB gp3 磁碟用於根數據
  - 540 GiB gp2 磁碟用於核心數據
- 對於 HA 對：
  - 兩個用於中介實例的 st1 EBS 卷，其中一個約 8 GiB，用作根磁碟，另一個約 4 GiB，用作資料磁碟
  - 每個節點中有一個 140 GiB gp3 磁碟，用於保存另一個節點的根資料副本

    在某些區域中，可用的EBS磁碟類型只能是gp2。

- 每個啟動磁碟和根磁碟一個 EBS 快照

  重新啟動時會自動建立快照。

- 當您使用金鑰管理服務 (KMS) 在 AWS 中啟用資料加密時， Cloud Volumes ONTAP的啟動磁碟和根磁碟也會被加密。這包括 HA 對中中介實例的啟動磁碟。磁碟使用您在新增Cloud Volumes ONTAP系統時選擇的 CMK 進行加密。

在 AWS 中， NVRAM位於啟動磁碟上。

Azure（單節點）

- 三個高級 SSD 磁碟：
  - 一個 10 GiB 磁碟用於啟動數據
  - 一個 140 GiB 磁碟用於根數據
  - 一個 512 GiB 磁碟用於NVRAM

    如果您為Cloud Volumes ONTAP選擇的虛擬機器支援 Ultra SSD，則係統將使用 32 GiB Ultra SSD 作為NVRAM，而不是 Premium SSD。

- 一個 1024 GiB 標準 HDD 磁碟，用於保存核心
- 每個啟動磁碟和根磁碟對應一個 Azure 快照
- 預設情況下，Azure 中的每個磁碟都是靜態加密的。

  如果您為Cloud Volumes ONTAP選擇的虛擬機器支援 Premium SSD v2 託管磁碟作為資料磁碟，系統將使用 32 GiB Premium SSD v2 託管磁碟作為NVRAM，並使用另一個磁碟作為根磁碟。

Azure（HA 對）

HA 與頁 **Blob** 對

- 兩個 10 GiB Premium SSD 磁碟用於啟動磁碟區（每個節點一個）
- 兩個用於根卷的 140 GiB 高階儲存頁 Blob（每個節點一個）
- 兩個 1024 GiB 標準 HDD 磁碟用於保存核心（每個節點一個）
- 兩個 512 GiB 高級 SSD 磁碟用於NVRAM （每個節點一個）
- 每個啟動磁碟和根磁碟對應一個 Azure 快照

  重新啟動時會自動建立快照。

- 預設情況下，Azure 中的每個磁碟都是靜態加密的。

HA 與多個可用區域中的共用託管磁碟

- 兩個 10 GiB Premium SSD 磁碟用於啟動磁碟區（每個節點一個）
- 兩個 512 GiB 高階 SSD 磁碟用於根磁碟區（每個節點一個）
- 兩個 1024 GiB 標準 HDD 磁碟用於保存核心（每個節點一個）
- 兩個 512 GiB 高級 SSD 磁碟用於NVRAM （每個節點一個）
- 每個啟動磁碟和根磁碟對應一個 Azure 快照

  重新啟動時會自動建立快照。

- 預設情況下，Azure 中的每個磁碟都是靜態加密的。

單一可用區域中具有共享託管磁碟的 **HA** 對

- 兩個 10 GiB Premium SSD 磁碟用於啟動磁碟區（每個節點一個）
- 兩個 512 GiB 高級 SSD 共享託管磁碟，用於根卷（每個節點一個）
- 兩個 1024 GiB 標準 HDD 磁碟用於保存核心（每個節點一個）
- 兩個 512 GiB 高級 SSD 託管磁碟用於NVRAM （每個節點一個）

如果您的虛擬機器支援高級 SSD v2 託管磁碟作為資料磁碟，它將使用 32 GiB 高級 SSD v2 託管磁碟作為NVRAM ，並使用 512 GiB 高級 SSD v2 共用託管磁碟作為根磁碟區。

當滿足以下條件時，您可以在單一可用區域中部署 HA 對並使用進階 SSD v2 託管磁碟：

- Cloud Volumes ONTAP的版本為 9.15.1 或更高版本。
- 所選區域和區域支援高級 SSD v2 託管磁碟。有關受支援區域的信息，請參閱 "Microsoft Azure 網站：按地區提供的產品"。
- 訂閱已註冊為 Microsoft"Microsoft.Compute/VMOrchestratorZonalMultiFD 功能" 。

Google Cloud（單節點）

- 一個 10 GiB SSD 永久磁碟，用於儲存啟動數據

- 一個 64 GiB SSD 持久性磁碟，用於儲存根數據
- 一個 500 GiB SSD 持久性磁碟，用於NVRAM
- 一個 315 GiB 標準持久性磁碟，用於保存核心
- 啟動和根資料的快照

  重新啟動時會自動建立快照。

- 預設情況下，啟動磁碟和根磁碟是加密的。

Google Cloud（高可用性對）

- 兩個 10 GiB SSD 持久性磁碟用於啟動數據
- 四個 64 GiB SSD 持久性磁碟用於根數據
- 兩個 500 GiB SSD 持久性磁碟用於NVRAM
- 兩個 315 GiB 標準持久性磁碟，用於保存核心
- 一個 10 GiB 標準持久性磁碟，用於儲存中介數據
- 一個 10 GiB 標準永久磁碟，用於中介啟動數據
- 啟動和根資料的快照

  重新啟動時會自動建立快照。

- 預設情況下，啟動磁碟和根磁碟是加密的。

磁碟所在位置

儲存佈局：

- 啟動資料駐留在連接到執行個體或虛擬機器的磁碟上。

  此磁碟包含啟動映像，但不適用於Cloud Volumes ONTAP。

- 根資料（包含系統配置和日誌）位於 aggr0 中。
- 儲存虛擬機器 (SVM) 根磁碟區位於 aggr1 中。
- 資料卷也駐留在 aggr1 中。

知識和支持

註冊以獲得支持

需要進行支援註冊才能獲得針對NetApp Console及其儲存解決方案和資料服務的技術支援。還需要支援註冊才能啟用Cloud Volumes ONTAP系統的關鍵工作流程。

註冊支援並不能使NetApp獲得雲端提供者文件服務的支援。有關雲端提供者文件服務、其基礎設施或使用該服務的任何解決方案的技術支持，請參閱該產品文件中的「取得協助」。

- "適用於ONTAP 的Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

支援註冊概述

啟動支持權利的註冊方式有兩種：

- 註冊您的NetApp Console帳戶序號（您的 20 位元 960xxxxxxxx 序號位於控制台中的「支援資源」頁面上）。

  這可作為控制台內任何服務的單一支援訂閱 ID。每個控制台帳戶都必須註冊。

- 在您的雲端供應商市場中註冊與訂閱相關的Cloud Volumes ONTAP序號（這些是 20 位元 909201xxxxxxxx 序號）。

  這些序號通常稱為_PAYGO 序號_，由NetApp Console在Cloud Volumes ONTAP部署時產生。

註冊兩種類型的序號可以實現開立支援票和自動產生案例等功能。透過將NetApp支援網站 (NSS) 帳戶新增至控制台即可完成註冊，如下所述。

註冊**NetApp Console**以取得**NetApp**支持

要註冊支援並啟動支援權利，您的NetApp Console帳戶中的一名使用者必須將NetApp支援網站帳戶與其控制台登入名稱關聯。如何註冊NetApp支援取決於您是否已經擁有NetApp支援網站 (NSS) 帳號。

擁有 **NSS** 帳戶的現有客戶

如果您是擁有 NSS 帳戶的NetApp客戶，只需透過控制台註冊即可獲得支援。

步驟

1. 選擇“管理”>“憑證”。
2. 選擇*使用者憑證*。
3. 選擇*新增 NSS 憑證*並依照NetApp支援網站 (NSS) 驗證提示進行操作。
4. 若要確認註冊過程是否成功，請選擇「幫助」圖標，然後選擇「支援」。

   *資源*頁面應顯示您的控制台帳戶已註冊以獲得支援。

請注意，如果其他控制台使用者尚未將NetApp支援網站帳戶與其登入名稱關聯，他們將看不到相同的支援註冊狀態。但是，這並不意味著您的帳戶沒有註冊支援。只要組織中的一名使用者遵循了這些步驟，您的帳戶就已註冊。

現有客戶但沒有 **NSS** 帳戶

如果您是現有的NetApp客戶，擁有現有授權和序號但沒有 NSS 帳戶，則需要建立 NSS 帳戶並將其與您的控制台登入關聯。

步驟

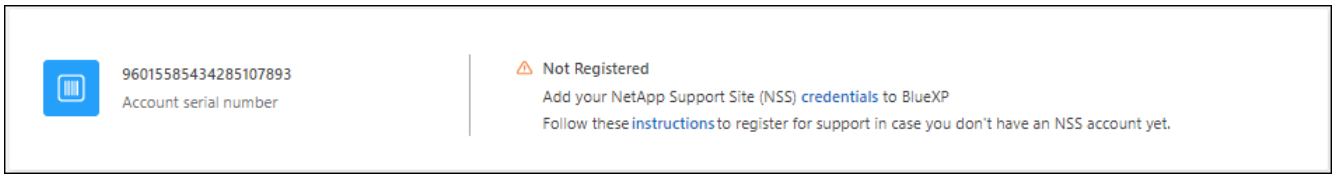
1. 透過完成以下操作建立NetApp支援網站帳戶 "NetApp支援網站使用者註冊表"
   a. 請務必選擇適當的使用者級別，通常為* NetApp客戶/最終使用者*。
   b. 請務必複製上面用於序號欄位的控制台帳戶序號（960xxxx）。這將加快帳戶處理速度。
2. 完成以下步驟，將您的新 NSS 帳戶與您的控制台登入名稱關聯擁有 NSS 帳戶的現有客戶。

NetApp全新產品

如果您是NetApp新使用者且沒有 NSS 帳戶，請依照下列步驟操作。

步驟

1. 在控制台的右上角，選擇「幫助」圖標，然後選擇「支援」。
2. 從支援註冊頁面找到您的帳戶 ID 序號。



3. 導航至 "NetApp 的支援註冊網站"並選擇*我不是註冊的NetApp客戶*。
4. 填寫必填欄位（帶有紅色星號的欄位）。
5. 在*產品線*欄位中，選擇*雲端管理員*，然後選擇適用的計費提供者。
6. 從上面的步驟 2 複製您的帳戶序號，完成安全性檢查，然後確認您已閱讀 NetApp 的全球資料隱私政策。

   一封電子郵件會立即發送到提供的郵箱以完成此安全交易。如果幾分鐘內沒有收到驗證電子郵件，請務必檢查您的垃圾郵件資料夾。

7. 從電子郵件中確認操作。

   確認向NetApp提交您的請求並建議您建立NetApp支援網站帳戶。

8. 透過完成以下操作建立NetApp支援網站帳戶 "NetApp支援網站使用者註冊表"
   a. 請務必選擇適當的使用者級別，通常為* NetApp客戶/最終使用者*。
   b. 請務必複製上面用於序號欄位的帳戶序號（960xxxx）。這將加快處理速度。

完成後

NetApp應該在過程中與您聯繫。這是針對新用戶的一次性入職培訓。

擁有NetApp支援網站帳號後，請依照下列步驟將該帳號與您的控制台登入關聯擁有 NSS 帳戶的現有客戶。

關聯 NSS 憑證以獲得Cloud Volumes ONTAP支持

需要將NetApp支援網站憑證與您的控制台帳戶關聯，才能為Cloud Volumes ONTAP啟用以下關鍵工作流程：

- 註冊即用即付Cloud Volumes ONTAP系統以獲得支持

  需要提供您的 NSS 帳戶才能啟動對您的系統的支援並獲得NetApp技術支援資源的存取權限。

- 自帶授權 (BYOL) 時部署Cloud Volumes ONTAP

  需要提供您的 NSS 帳戶，以便控制台可以上傳您的許可證金鑰並啟用您購買的期限的訂閱。這包括期限續訂的自動更新。

- 將Cloud Volumes ONTAP軟體升級至最新版本

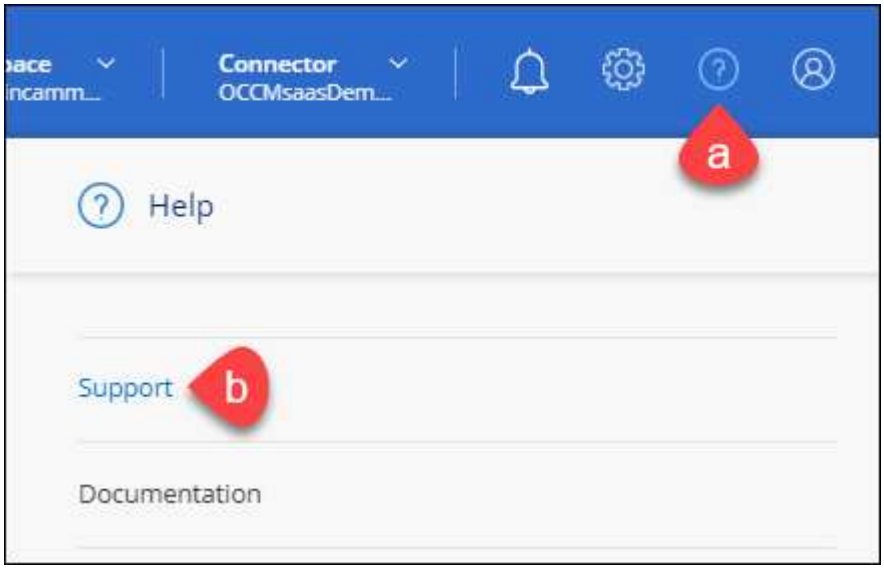
將 NSS 憑證與您的NetApp Console帳戶關聯與將 NSS 帳戶與控制台使用者登入相關聯。

這些 NSS 憑證與您的特定控制台帳戶 ID 相關聯。屬於控制台組織的使用者可以從*支援 > NSS 管理*存取這些憑證。

- 如果您有客戶級帳戶，則可以新增一個或多個 NSS 帳戶。
- 如果您有合作夥伴或經銷商帳戶，則可以新增一個或多個 NSS 帳戶，但不能與客戶級帳戶一起新增。

步驟

1. 在控制台的右上角，選擇「幫助」圖標，然後選擇「支援」。



2. 選擇*NSS 管理 > 新增 NSS 帳號*。
3. 當出現提示時，選擇「繼續」以重新導向至 Microsoft 登入頁面。

   NetApp使用 Microsoft Entra ID 作為特定於支援和授權的身份驗證服務的身份提供者。

4. 在登入頁面，提供您的NetApp支援網站註冊的電子郵件地址和密碼以執行驗證程序。

   這些操作使控制台能夠使用您的 NSS 帳戶進行許可證下載、軟體升級驗證和未來支援註冊等操作。

   請注意以下事項：

   - NSS 帳戶必須是客戶級帳戶（不是訪客或臨時帳戶）。您可以擁有多個客戶級 NSS 帳戶。
   - 如果該帳戶是合作夥伴等級帳戶，則只能有一個 NSS 帳戶。如果您嘗試新增客戶級 NSS 帳戶且合作夥伴級帳戶已存在，您將收到以下錯誤訊息：

     “此帳戶不允許使用 NSS 客戶類型，因為已經存在不同類型的 NSS 用戶。”

   如果您已有客戶級 NSS 帳戶並嘗試新增合作夥伴級帳戶，情況也是如此。

   - 成功登入後， NetApp將儲存 NSS 使用者名稱。

     這是系統產生的映射到您的電子郵件的 ID。在*NSS 管理*頁面上，您可以顯示來自 ••• 菜單。

   - 如果您需要刷新登入憑證令牌，還有一個*更新憑證*選項 ••• 菜單。

     使用此選項會提示您再次登入。請注意，這些帳戶的令牌將在 90 天後過期。我們將發布通知來提醒您此事。

獲取協助

NetApp以多種方式為NetApp Console及其雲端服務提供支援。全天候提供廣泛的免費自助支援選項，例如知識庫 (KB) 文章和社群論壇。您的支援註冊包含透過網路工單取得的遠端技術支援。

獲取雲端提供者文件服務的支持

有關雲端提供者文件服務、其基礎設施或使用該服務的任何解決方案的技術支持，請參閱該產品的文檔。

- "適用於ONTAP 的Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

要獲得特定於NetApp及其儲存解決方案和資料服務的技術支持，請使用下面所述的支援選項。

使用自助選項

這些選項每週 7 天、每天 24 小時免費提供：

- 文件

  您目前正在檢視的NetApp Console文件。

- "知識庫"

搜尋NetApp知識庫以尋找有助於解決問題的文章。

- "社群"

  加入NetApp Console社區，關注正在進行的討論或創建新的討論。

向NetApp支援建立案例

除了上述自助支援選項之外，您還可以在啟動支援後與NetApp支援專家合作解決任何問題。

開始之前

- 若要使用「建立案例」功能，您必須先將您的NetApp支援網站憑證與您的控制台登入關聯。 "了解如何管理與控制台登入相關的憑證" 。
- 如果您要為具有序號的ONTAP系統開啟案例，那麼您的 NSS 帳戶必須與該系統的序號相關聯。

步驟

1. 在NetApp Console中，選擇「說明」>「支援」 。
2. 在「資源」頁面上，選擇「技術支援」下的可用選項之一：

   a. 如果您想透過電話與某人交談，請選擇「致電我們」 。您將被引導至 netapp.com 上的一個頁面，其中列出了您可以撥打的電話號碼。

   b. 選擇「建立案例」向NetApp支援專家開立票據：

      - 服務：選擇與問題相關的服務。例如，* NetApp Console* 特定於控制台內的工作流程或功能的技術支援問題。
      - 系統：如果適用於存儲，請選擇* Cloud Volumes ONTAP* 或 **On-Prem**，然後選擇相關的工作環境。

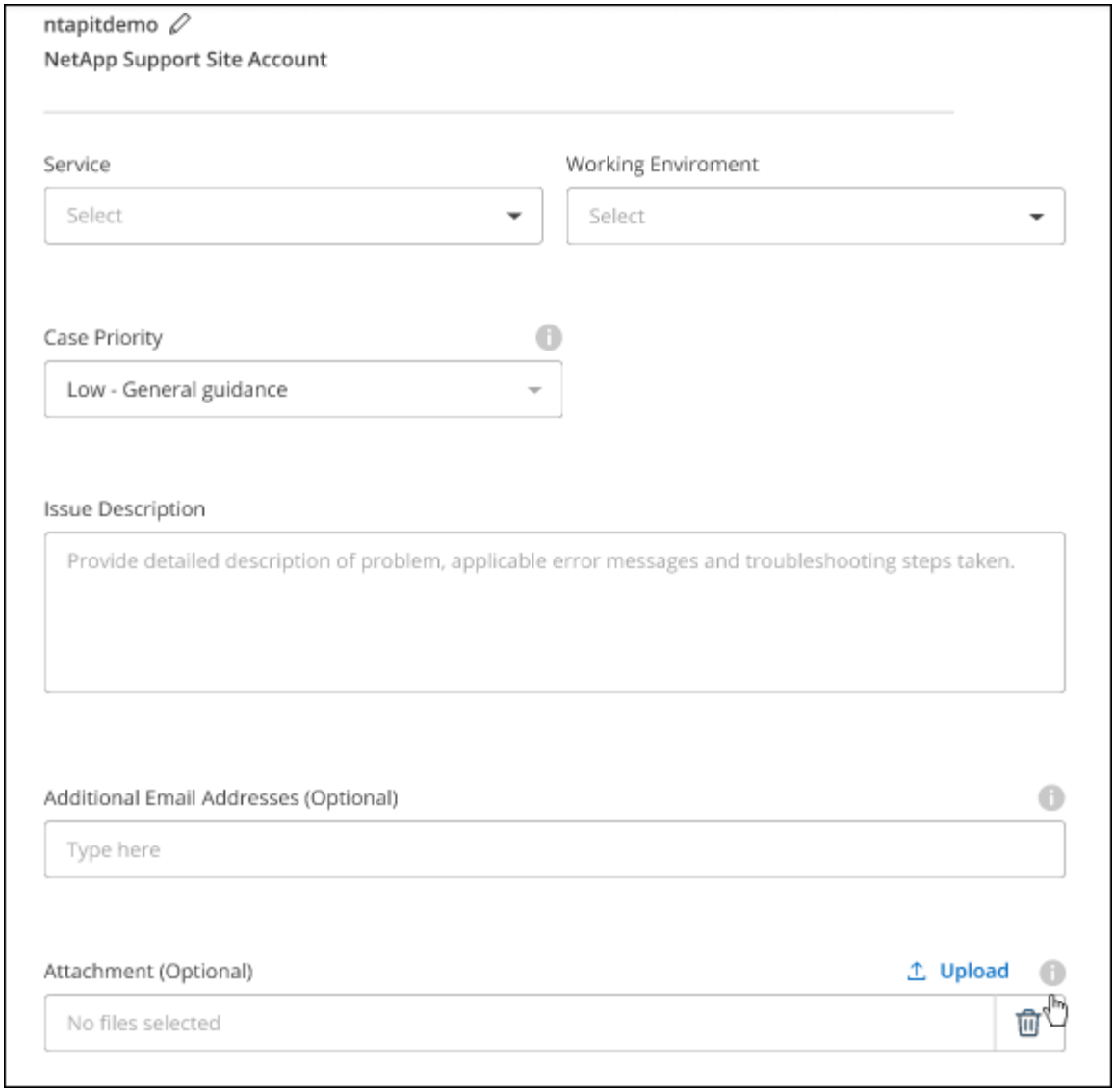
        系統清單位於控制台組織範圍內，並且您在頂部橫幅中選擇了控制台代理。

      - 個案優先級：選擇個案的優先級，可以是低、中、高或嚴重。

        要了解有關這些優先事項的更多詳細信息，請將滑鼠懸停在欄位名稱旁邊的資訊圖示上。

      - 問題描述：提供問題的詳細描述，包括任何適用的錯誤訊息或您執行的故障排除步驟。
      - 其他電子郵件地址：如果您想讓其他人知道此問題，請輸入其他電子郵件地址。
      - 附件（選購）：一次最多上傳五個附件。

        每個附件檔案大小限制為 25 MB。支援以下檔案副檔名：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。



完成後

將會出現一個彈出窗口，其中顯示您的支援案例編號。NetApp支援專家將審查您的案例並儘快回覆您。

若要查看支援案例的歷史記錄，您可以選擇*設定>時間軸*並尋找名為「建立支援案例」的操作。最右邊的按鈕可讓您展開操作以查看詳細資訊。

嘗試建立案例時，您可能會遇到以下錯誤訊息：

“您無權針對所選服務建立案例”

此錯誤可能表示 NSS 帳戶及其關聯的記錄公司與NetApp Console帳戶序號的記錄公司不同（即。960xxxx）或工作環境序號。您可以使用以下選項之一尋求協助：

- 提交非技術案例 https://mysupport.netapp.com/site/help

管理您的支援案例

您可以直接從控制台檢視和管理活動和已解決的支援案例。您可以管理與您的 NSS 帳戶和公司相關的案例。

請注意以下事項：

- 頁面頂部的案例管理儀表板提供兩種視圖：
  - 左側視圖顯示了您提供的使用者 NSS 帳戶在過去 3 個月內開啟的案件總數。
  - 右側的視圖根據您的使用者 NSS 帳戶顯示了過去 3 個月內貴公司層級開設的案件總數。

  表中的結果反映了與您選擇的視圖相關的案例。
- 您可以新增或刪除感興趣的列，並且可以過濾優先順序和狀態等列的內容。其他欄位僅提供排序功能。

  請查看以下步驟以了解更多詳細資訊。
- 在每個案件級別，我們提供更新案件記錄或關閉尚未關閉或待關閉狀態的案件的功能。

步驟

1. 在NetApp Console中，選擇「說明」>「支援」。
2. 選擇*案例管理*，如果出現提示，請將您的 NSS 帳戶新增至控制台。

   案例管理*頁面顯示與您的控制台使用者帳戶關聯的 **NSS** 帳戶相關的未結案例。這與出現在 ***NSS** 管理 頁面頂部的 NSS 帳戶相同。
3. （可選）修改表中顯示的資訊：
   - 在「組織的案例」下，選擇「查看」以查看與您的公司相關的所有案例。
   - 透過選擇精確的日期範圍或選擇不同的時間範圍來修改日期範圍。
   - 過濾列的內容。
   - 透過選擇然後選擇您想要顯示的列。
4. 透過選擇管理現有案例並選擇其中一個可用選項：
   - 查看案例：查看有關特定案例的完整詳細資訊。
   - 更新案例說明：提供有關您的問題的更多詳細信息，或選擇*上傳文件*以附加最多五個文件。

     每個附件檔案大小限制為 25 MB。支援以下檔案副檔名：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。
   - 結案：提供有關結案原因的詳細信息，然後選擇*結案*。

法律聲明

法律聲明提供對版權聲明、商標、專利等的存取。

版權

"https://www.netapp.com/company/legal/copyright/"

商標

NETAPP、NETAPP 標誌和NetApp商標頁面上列出的標誌是NetApp, Inc. 的商標。其他公司和產品名稱可能是其各自所有者的商標。

"https://www.netapp.com/company/legal/trademarks/"

專利

NetApp擁有的專利的最新清單可在以下位置找到：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隱私權政策

"https://www.netapp.com/company/legal/privacy-policy/"

開源

通知文件提供有關NetApp軟體中使用的第三方版權和許可的資訊。

- "NetApp Console通知"
- "Cloud Volumes ONTAP通知"
- "ONTAP通知"