本文檔Cloud Volumes ONTAP

Cloud Volumes ONTAP

NetApp
June 11, 2024

目錄

本文檔Cloud Volumes ONTAP

版本資訊

新功能

瞭解 BlueXP 中 Cloud Volumes ONTAP 管理的新功能。

本頁所述的增強功能僅適用於支援Cloud Volumes ONTAP 支援管理功能的BlueXP功能。若要瞭解Cloud Volumes ONTAP 有關此功能的最新消息、請參閱 "前往Cloud Volumes ONTAP 《發行說明》"

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 。

"深入瞭Cloud Volumes ONTAP 解本版的更新功能"。

2024 年 5 月 17 日

Amazon Web Services 本機區域支援

Cloud Volumes ONTAP HA 部署現在支援 AWS 本機區域。AWS 本機區域是一種基礎架構部署、其中儲存、運算、資料庫和其他精選 AWS 服務都位於大城市和產業區域附近。

> 在標準模式下使用 BlueXP 時、支援 AWS 本機區域。目前、在受限模式或私有模式下使用 BlueXP 時、並不支援 AWS 本機區域。

如需更多關於具有 HA 部署的 AWS 本機區域的資訊、請參閱 "AWS 本機區域"。

2024 年 4 月 23 日

Azure 支援多個可用區域部署的新區域

以下地區現在支援 Azure 中的 HA 多重可用性區域部署、適用於 Cloud Volumes ONTAP 9.12.1 GA 及更新版本：

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

如需所有區域的清單、請參閱 "Azure 下的 Global Regions Map"。

Google Cloud 現在支援約翰內斯堡地區

約翰內斯堡地區 (`africa-south1` Google Cloud for Cloud Volumes ONTAP 9.12.1 GA 及更新版本現在均支援區域）。

如需所有區域的清單、請參閱 "Google Cloud 下的全球區域地圖"。

不再支援 **Volume** 範本和標籤

您無法再從範本建立磁碟區、也無法編輯磁碟區的標籤。這些動作與 BlueXP 補救服務相關聯、而 BlueXP 補救服務已無法使用。

2024 年 3 月 8 日

Amazon Instant 中繼資料服務 **v2** 支援

在 AWS 、 Cloud Volumes ONTAP 、 Mediator 和 Connector 中、現在所有功能都支援 Amazon Instant 中繼資料服務 v2 （ IMDSv2 ）。IMDSv2 提供更強大的保護功能、防範弱點。之前僅支援 IMDSv1 。

如果您的安全性原則要求、您可以將 EC2 執行個體設定為使用 IMDSv2 。如需相關指示、請參閱 "用於管理現有連接器的 BlueXP 安裝與管理文件"。

2024 年 3 月 5 日

Cloud Volumes ONTAP 9.14.1 GA

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

2024 年 2 月 2 日

支援 **Azure** 中的 **Edv5** 系列 **VM**

Cloud Volumes ONTAP 現在支援從 9.14.1 版開始的下列 Edv5 系列 VM 。

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

"Azure支援的組態"

2024 年 1 月 16 日

BlueXP 中的修補程式版本

BlueXP 中只有最新三個版本的 Cloud Volumes ONTAP 才提供修補程式版本。

"升級Cloud Volumes ONTAP"

2024 年 1 月 8 日

Azure 多個可用區域的新 VM

從 Cloud Volumes ONTAP 9.13.1 開始、下列 VM 類型支援 Azure 多個可用性區域、以進行新的和現有的高可用度配對部署：

- L16s_v3
- L32s_v3
- L48s_v3
- L64s_v3

"Azure支援的組態"

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 。

"深入瞭Cloud Volumes ONTAP 解本版的更新功能"。

300 TiB FlexVol Volume 上限

現在、您可以使用系統管理員和 ONTAP CLI 、從 Cloud Volumes ONTAP 9.12.1 P2 和 9.13.0 P2 開始、在 BlueXP 中從 Cloud Volumes ONTAP 9.13.1 開始、建立最大至 300 TiB 的 FlexVol Volume 。

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

2023 年 12 月 5 日

我們進行了下列變更。

Azure 的新區域支援

單一可用性區域區域支援

以下地區現在支援 Azure 中 Cloud Volumes ONTAP 9.12.1 GA 及更新版本的高可用度單一可用度區域部署：

- 特拉維夫
- 米蘭

支援多種可用性區域

以下地區現在支援 Azure 中 Cloud Volumes ONTAP 9.12.1 GA 及更新版本的高可用度多重可用度區域部署：

- 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
- 中國北方 3.

如需所有區域的清單、請參閱 "Azure 下的 Global Regions Map"。

2023 年 11 月 10 日

在 3.9.35 版 Connector 中引入了以下變更。

Google Cloud 現在支援柏林地區

現在、 Google Cloud for Cloud Volumes ONTAP 9.12.1 GA 及更新版本均支援柏林地區。

如需所有區域的清單、請參閱 "Google Cloud 下的全球區域地圖"。

2023 年 11 月 8 日

在 3.9.35 版 Connector 中引入了以下變更。

AWS 現在支援 **Tel Aviv** 區域

AWS for Cloud Volumes ONTAP 9.12.1 GA 及更新版本現在支援 Tel Aviv 區域。

如需所有區域的清單、請參閱 "AWS 下的 Global Regions Map"。

2023 年 11 月 1 日

連接器 3.9.34 版隨附下列變更。

Google Cloud 現在支援沙烏地阿拉伯地區

現在、 Google Cloud for Cloud Volumes ONTAP 和 Connector for Cloud Volumes ONTAP 9.12.1 GA 及更新版本均支援沙烏地阿拉伯地區。

如需所有區域的清單、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 版隨附下列變更。

Azure 支援 **HA** 多重可用性區域部署的新區域

Azure 中的下列區域現在支援 Cloud Volumes ONTAP 9.12.1 GA 及更新版本的高可用度多重可用度區域部署：

- 澳洲東部
- 東南亞
- 法國中部
- 北歐洲
- 卡塔爾中部
- 瑞典中部
- 西歐
- 美國西部 2.

如需支援多個可用區域的所有區域清單、請參閱 "Azure 下的 Global Regions Map"。

2023 年 10 月 6 日

連接器 3.9.34 版隨附下列變更。

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 通用版本。

"深入瞭Cloud Volumes ONTAP 解本版的更新功能"。

2023 年 9 月 10 日

在 3.9.33 版 Connector 中引入了以下變更。

支援 **Azure** 中的 **Lsv3** 系列 **VM**

從 9.13.1 版開始、 Azure 中的 Cloud Volumes ONTAP 現在支援 L48s_v3 和 L64s_v3 執行個體類型、可在單一節點和高可用度配對部署中、在單一和多個可用性區域中部署共用託管磁碟。這些執行個體類型支援 Flash Cache 。

"檢視 Azure 中 Cloud Volumes ONTAP 支援的組態"
"檢視 Azure 中 Cloud Volumes ONTAP 的儲存限制"

2023 年 7 月 30 日

Connector 3.9.32 版隨附下列變更。

Google Cloud 中的 **Flash Cache** 和高速寫入支援

Flash Cache 和高速寫入速度可在 Cloud Volumes ONTAP 9.13.1 及更新版本的 Google Cloud 中個別啟用。所有支援的執行個體類型都提供高速寫入速度。Flash Cache 支援下列執行個體類型：

- n2-Standard-16

- n2-Standard-32
- n2 標準 -48
- n2-Standard-64

您可以在單一節點和高可用度配對部署上分別或一起使用這些功能。

"在Cloud Volumes ONTAP Google Cloud上啟動"

使用報告增強功能

使用報告中所顯示資訊的各種改善功能現已推出。以下是使用報告的增強功能：

- TiB 單元現在已包含在欄名稱中。
- 現在包含序號的新「節點」欄位。
- 儲存 VM 使用量報告中現在包含新的「工作負載類型」一欄。
- 儲存 VM 和 Volume 使用量報告中現在已包含工作環境名稱。
- Volume 類型「 file 」現在標示為「 Primary （ Read/Write ）（主要（讀取 / 寫入））」。
- Volume 類型「 Secondary 」現在標示為「 Secondary （ DP ）」（次要（ DP ））。

如需使用報告的詳細資訊、請參閱 "下載使用報告"。

2023 年 7 月 26 日

Connector 3.9.31 版本推出下列變更。

Cloud Volumes ONTAP 9.13.1 GA

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

"深入瞭Cloud Volumes ONTAP 解本版的更新功能"。

2023 年 7 月 2 日

Connector 3.9.31 版本推出下列變更。

支援 **Azure** 中的 **HA** 多重可用性區域部署

Azure 中的 Japan East 和 Korea Central 現在支援 Cloud Volumes ONTAP 9.12.1 GA 及更新版本的 HA 多重可用性區域部署。

如需支援多個可用區域的所有區域清單、請參閱 "Azure 下的 Global Regions Map"。

自主勒索軟體保護支援

Cloud Volumes ONTAP 現在支援自主勒索軟體保護（ ARP ）。Cloud Volumes ONTAP 9.12.1 版及更高版本均提供 ARP 支援。

若要深入瞭解 Cloud Volumes ONTAP 的 ARP 、請參閱 "自主勒索軟體保護"。

2023 年 6 月 26 日

Connector 3.9.30 版本推出下列變更。

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 。

"深入瞭Cloud Volumes ONTAP 解本版的更新功能"。

2023 年 6 月 4 日

Connector 3.9.30 版本推出下列變更。

Cloud Volumes ONTAP 升級版本選擇器更新

現在您可以透過「升級 Cloud Volumes ONTAP 」頁面、選擇升級至最新的 Cloud Volumes ONTAP 版本或舊版。

若要深入瞭解如何透過 BlueXP 升級 Cloud Volumes ONTAP 、請參閱 "升級Cloud Volumes ONTAP"。

2023 年 5 月 7 日

Connector 3.9.29 版隨附下列變更。

現在、 Google Cloud 支援卡塔爾地區

現在、 Google Cloud for Cloud Volumes ONTAP 和 Connector for Cloud Volumes ONTAP 9.12.1 GA 及更新版本均支援卡塔爾地區。

瑞典中部地區現在支援 Azure

現在 Azure for Cloud Volumes ONTAP 和 Connector for Cloud Volumes ONTAP 9.12.1 GA 及更新版本均支援瑞典中部地區。

支援 Azure Australia East 的 HA 多重可用性區域部署

Azure 中的澳洲東部地區現在支援 Cloud Volumes ONTAP 9.12.1 GA 及更新版本的 HA 多重可用性區域部署。

充電使用量明細

現在、您可以瞭解訂閱容量型授權時所需支付的費用。以下類型的使用報告可從 BlueXP 的數位錢包下載。使用報告會提供您訂閱的容量詳細資料、並告訴您如何為 Cloud Volumes ONTAP 訂閱中的資源收取費用。可下載的報告可輕鬆與他人共用。

- Cloud Volumes ONTAP 套件使用率
- 高階使用率
- 儲存 VM 使用率

- Volume 使用量

如需詳細資訊、請參閱 "管理容量型授權"。

現在在沒有市場訂閱的情況下存取 **BlueXP** 時會顯示通知

當您在 BlueXP 中存取 Cloud Volumes ONTAP 而不訂閱市場時、現在就會顯示通知。通知指出：「此工作環境的市場訂閱必須符合 Cloud Volumes ONTAP 條款與條件。」

2023 年 4 月 4 日

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

- 支援單一節點系統。
- 支援直接向NetApp購買的授權。

如需區域可用度、請參閱 "全球區域地圖Cloud Volumes ONTAP 、供您使用"。

2023年4月3日

Connector 3.9.28 版隨附下列變更。

Google Cloud 現在支援都靈地區

Google Cloud for Cloud Volumes ONTAP 和 Connector for Cloud Volumes ONTAP 9.12.1 GA 及更新版本均支援都靈地區。

BlueXP 數位錢包增強功能

BlueXP 數位錢包現在顯示您購買的授權容量、並提供市場私有優惠。

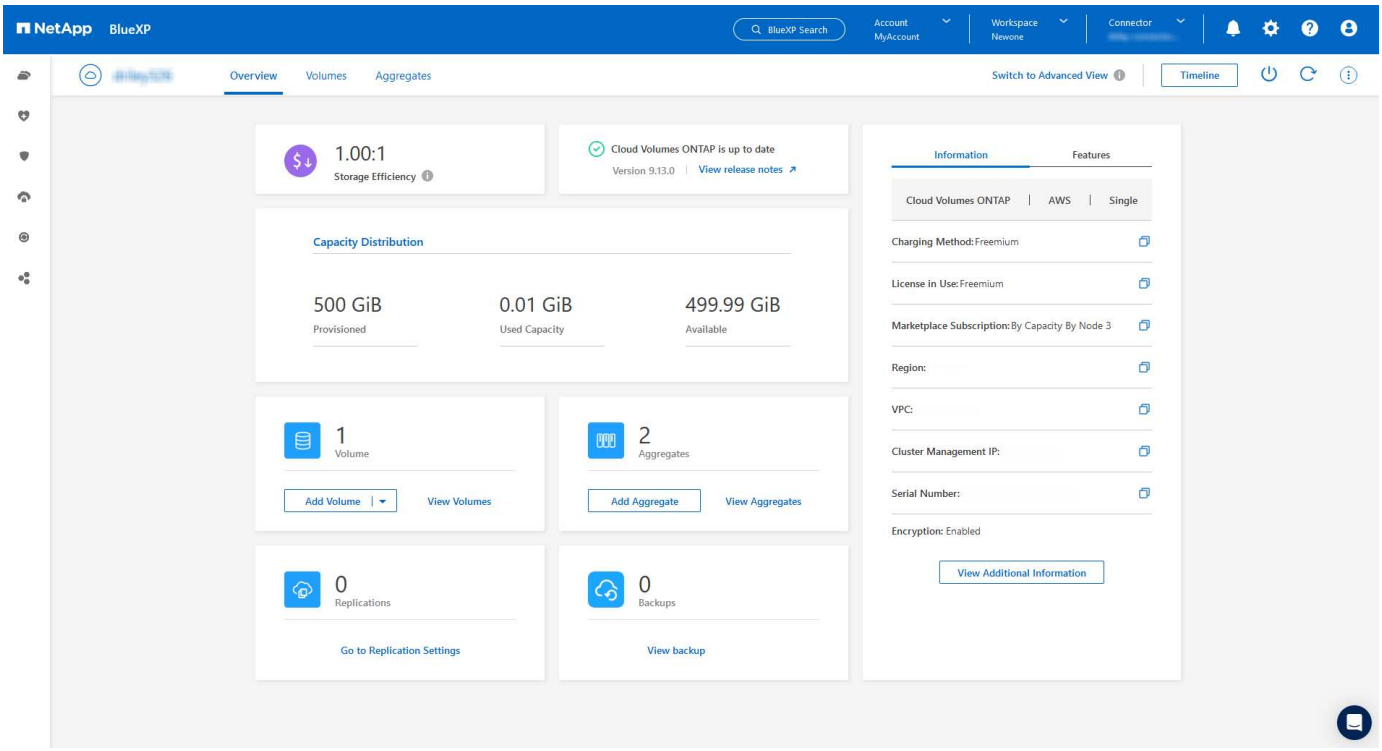
"瞭解如何檢視您帳戶中的已用容量"。

支援在磁碟區建立期間提出意見

此版本可讓您在使用 API 建立 Cloud Volumes ONTAP FlexGroup Volume 或 FlexVol Volume 時、提出意見。

重新設計 **BlueXP** 使用者介面、以重新設計 **Cloud Volumes ONTAP** 概觀、 **Volume** 和集合頁面

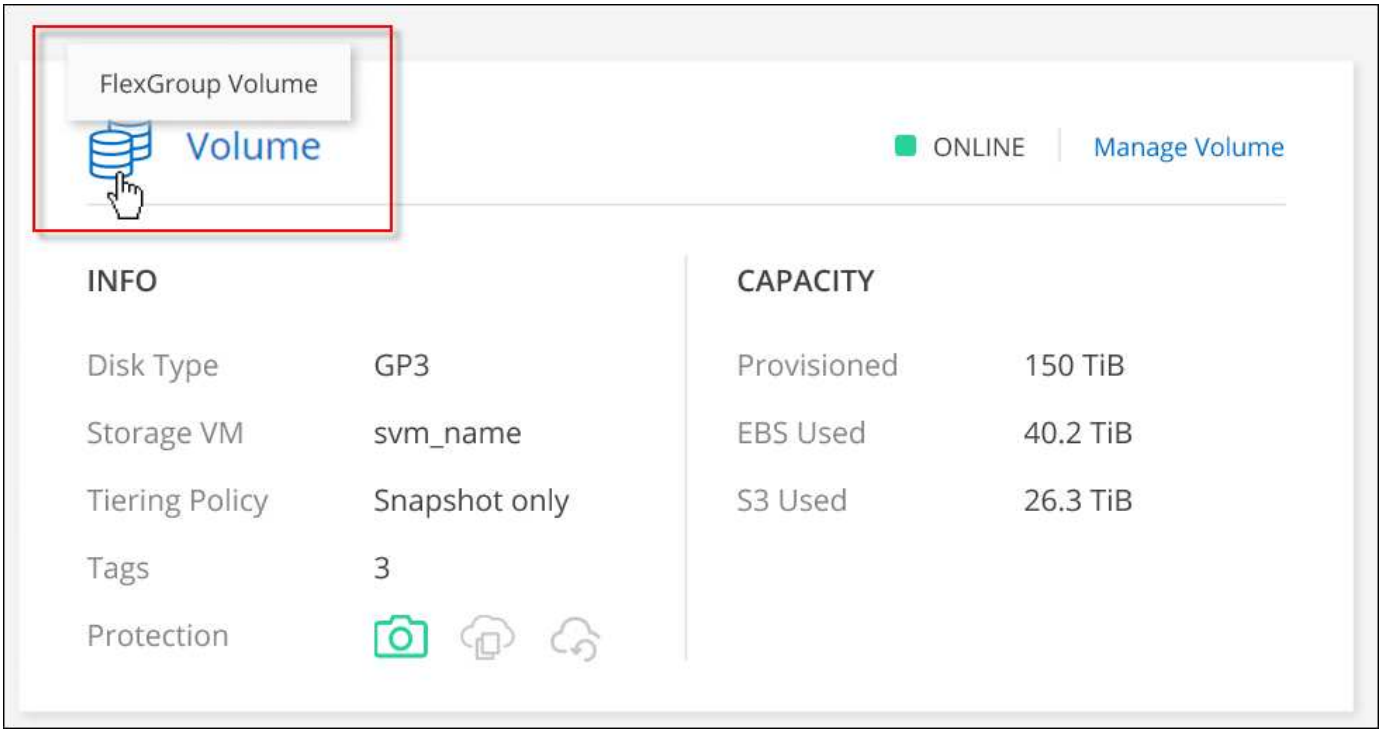
BlueXP 現在已重新設計了 Cloud Volumes ONTAP 概觀、磁碟區和集合網頁的使用者介面。並排式設計會在每個方塊中提供更完整的資訊、以提供更好的使用者體驗。



可透過 **Cloud Volumes ONTAP** 檢視的 **FlexGroup Volume**

透過 CLI 或系統管理員直接建立的 FlexGroup Volume 現在可透過 BlueXP 中重新設計的 Volumes 動態磚來檢視。BlueXP 與提供給 FlexVol Volume 的資訊相同、透過專用的 Volumes 磚提供建立的 FlexGroup Volume 的詳細資訊。

目前、您只能在 BlueXP 下檢視現有的 FlexGroup 磁碟區。在 BlueXP 中建立 FlexGroup 磁碟區的功能無法使用、但已計畫在未來版本中使用。



"深入瞭解如何檢視建立的 FlexGroup Volume 。"

2023年3月13日

中國地區支援

從推出支援中國地區的支援功能到現在起、Azure已提供下列支援Cloud Volumes ONTAP ：

- 支援中國北方3 Cloud Volumes ONTAP 。
- 支援單一節點系統。
- 支援直接向NetApp購買的授權。

如需區域可用度、請參閱 "全球區域地圖Cloud Volumes ONTAP 、供您使用"。

2023年3月5日

以下是3.9.27版Connector的變更。

支援的支援**Cloud Volumes ONTAP**

現在、BlueXP可以在Cloud Volumes ONTAP AWS、Azure和Google Cloud中部署和管理支援功能。

"深入瞭Cloud Volumes ONTAP 解本版的更新功能"。

Azure支援**16 TiB**和**32 Tib**

目前支援16個TiB和32個TiB磁碟大小、可在Azure的託管磁碟上執行高可用度部署Cloud Volumes ONTAP 。

深入瞭解 "Azure支援的磁碟大小"。

MTEKM授權

多租戶加密金鑰管理（MTEKM）授權現已隨Cloud Volumes ONTAP 附於執行9.12.1 GA或更新版本的全新及現有的支援系統中。

使用NetApp Volume Encryption時、多租戶外部金鑰管理可讓個別儲存VM（SVM）透過KMIP伺服器維護自己的金鑰。

"瞭解如何使用NetApp加密解決方案來加密磁碟區"。

支援無網際網路的環境

目前支援任何完全隔離網際網路的雲端環境Cloud Volumes ONTAP 。這些環境僅支援節點型授權（BYOL）。不支援容量型授權。若要開始使用、請手動安裝 Connector 軟體、登入 Connector 上執行的 BlueXP 主控台、將 BYOL 授權新增至 BlueXP 數位錢包、然後部署 Cloud Volumes ONTAP 。

- "將Connector安裝在沒有網際網路存取的位置"
- "存取Connector上的BlueXP主控台"
- "新增未指派的授權"

Google Cloud的Flash Cache和高速寫入速度

支援Flash Cache、高速寫入速度、以及高傳輸單位（MTU）8、896位元組、現在Cloud Volumes ONTAP 可用於發行版本為《The》（英文）的特定執行個體。

深入瞭解 "Google Cloud授權支援的組態"。

2023年2月5日

下列變更是在版本3.9.26的Connector中提出。

在AWS中建立放置群組

全新組態設定現在可透過AWS HA單一可用度區域（AZ）部署來建立放置群組。現在您可以選擇略過失敗的放置群組建立、並讓AWS HA單一AZ部署順利完成。

如需如何設定放置群組建立設定的詳細資訊、請參閱 "設定AWS HA單一AZ的放置群組建立"。

私有DNS區域組態更新

現在已有新的組態設定可供使用、以便在使用Azure私有連結時、避免在私有DNS區域和虛擬網路之間建立連結。預設會啟用建立。

"提供您Azure私有DNS的詳細資料給BlueXP"

WORM儲存與資料分層

現在您可以在建立Cloud Volumes ONTAP 一套或更新版本的版本時、同時啟用資料分層和WORM儲存。利用WORM儲存設備進行資料分層、可將資料分層至雲端的物件存放區。

"瞭解WORM儲存設備。"

2023年1月1日

以下是3.9.25版Connector的變更。

Google Cloud提供授權套件

Google Cloud Volumes ONTAP Cloud Marketplace提供最佳化的Edge Cache容量型授權套件、可作為隨用隨付方案或年度合約、以供使用。

請參閱 "提供授權Cloud Volumes ONTAP"。

的預設組態 Cloud Volumes ONTAP

多租戶加密金鑰管理（MTEKM）授權不再包含在新Cloud Volumes ONTAP 的版次部署中。

如需ONTAP 更多有關隨Cloud Volumes ONTAP 功能自動安裝的功能認證資訊、請參閱 "支援的預設組態Cloud Volumes ONTAP"。

2022年12月15日

零件9.12.0 Cloud Volumes ONTAP

現在、BlueXP可以在Cloud Volumes ONTAP AWS和Google Cloud中部署和管理功能。

"深入瞭Cloud Volumes ONTAP 解本版的更新功能"。

2022年12月8日

零點9.12.1. Cloud Volumes ONTAP

現在、BlueXP可以部署及管理Cloud Volumes ONTAP 支援全新功能和其他雲端供應商區域的功能。

"深入瞭Cloud Volumes ONTAP 解本版的更新功能"

2022年12月4日

以下是3.9.24版本的Connector所做的變更。

WORM +雲端備份現在可在Cloud Volumes ONTAP 建立過程中使用

現在、在建立流程的過程中、可以同時啟動一次寫入、多次讀取（WORM）和雲端備份功能Cloud Volumes ONTAP 。

以色列地區現已在Google Cloud中獲得支援

現在、Israel區域已在Google Cloud for Israel和Cloud Volumes ONTAP Connector for Cloud Volumes ONTAP the E29.11.1 P3及更新版本中受到支援。

2022年11月15日

下列變更是在版本3.9.23的Connector中提出。

Google Cloud 中的 ONTAP S3 授權

在Google Cloud Platform中、執行9.12.1版或更新版本的全新及現有的版本不含更新版本的S3授權Cloud Volumes ONTAP ONTAP 。

"瞭解如何在ONTAP 功能區中設定及管理S3物件儲存服務"

2022年11月6日

下列變更是在版本3.9.23的Connector中提出。

在Azure中移動資源群組

您現在可以將工作環境從同一個資源群組移至Azure中不同的資源群組、並在同一個Azure訂閱中使用。

如需詳細資訊、請參閱 "正在移動資源群組"。

NDMP複製認證

NDMP複本現已通過認證、可搭配Cloud Volume ONTAP 使用。

如需有關如何設定及使用NDMP的資訊、請參閱 "NDMP組態總覽"。

Azure的託管磁碟加密支援

新增Azure權限、讓您在建立時加密所有託管磁碟。

如需此新功能的詳細資訊、請參閱 "設定Cloud Volumes ONTAP 支援使用Azure中客戶管理的金鑰"。

2022年9月18日

以下是3.9.22版Connector的變更。

數位錢包增強功能

- 數位錢包現在會顯示最佳化I/O授權套件的摘要、以及Cloud Volumes ONTAP 整個帳戶中針對各個系統所配置的WORM容量。

  這些詳細資料可協助您更深入瞭解如何收取費用、以及是否需要購買額外容量。

  "瞭解如何檢視您帳戶中的已用容量"。

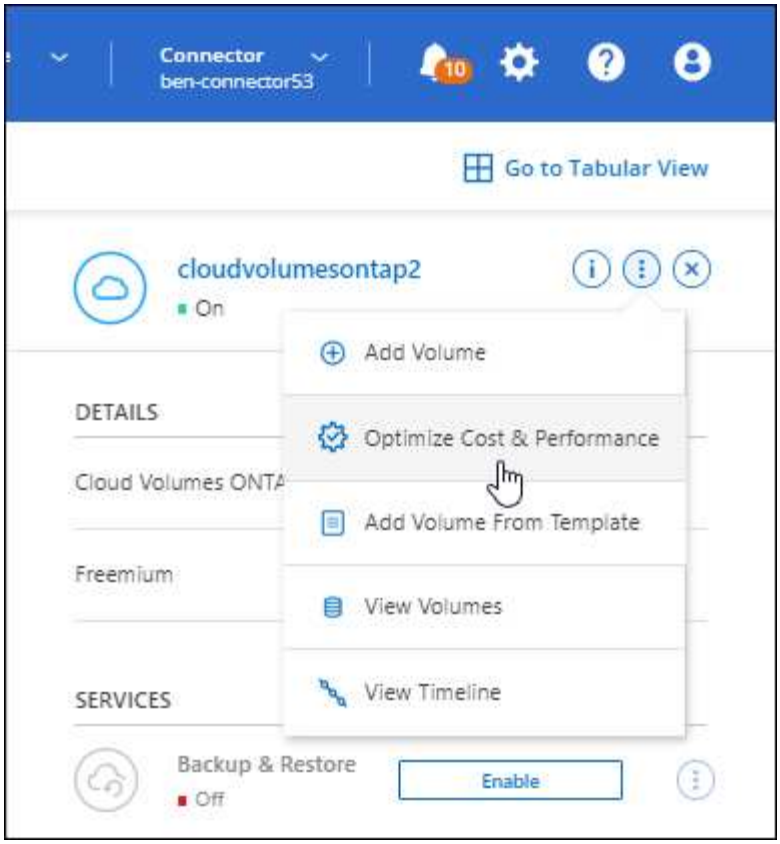
- 您現在可以從單一充電方法變更為最佳化的充電方法。

  "瞭解如何變更充電方法"。

最佳化成本與效能

您現在Cloud Volumes ONTAP 可以直接從Canvas.將效能與成本最佳化。

選擇工作環境之後、您可以選擇*最佳化成本與效能*選項、以變更Cloud Volumes ONTAP 執行個體類型以供使用。選擇較小的執行個體有助於降低成本、而改用較大的執行個體則有助於最佳化效能。



資訊通知**AutoSupport**

現在、如果Cloud Volumes ONTAP 某個不完善的系統無法傳送AutoSupport 功能介紹訊息、則BlueXP會產生通知。此通知包含可用於疑難排解網路問題的指示連結。

2022年7月31日

以下是3.9.21版Connector的變更。

MTEKM授權

多租戶加密金鑰管理（MNEKM）授權現已隨Cloud Volumes ONTAP 附於執行9.11.1版或更新版本的全新和現有的支援系統中。

使用NetApp Volume Encryption時、多租戶外部金鑰管理可讓個別儲存VM（SVM）透過KMIP伺服器維護自己的金鑰。

"瞭解如何使用NetApp加密解決方案來加密磁碟區"。

Proxy伺服器

現在、如果Cloud Volumes ONTAP 無法使用傳出的網際網路連線來傳送AutoSupport 更新訊息、則BlueXP會自動將您的還原系統設定為使用Connector做為Proxy伺服器。

可主動監控系統健全狀況、並傳送訊息給NetApp技術支援部門。AutoSupport

唯一的需求是確保連接器的安全性群組允許連接埠3128上的傳入連線。部署Connector之後、您需要開啟此連接埠。

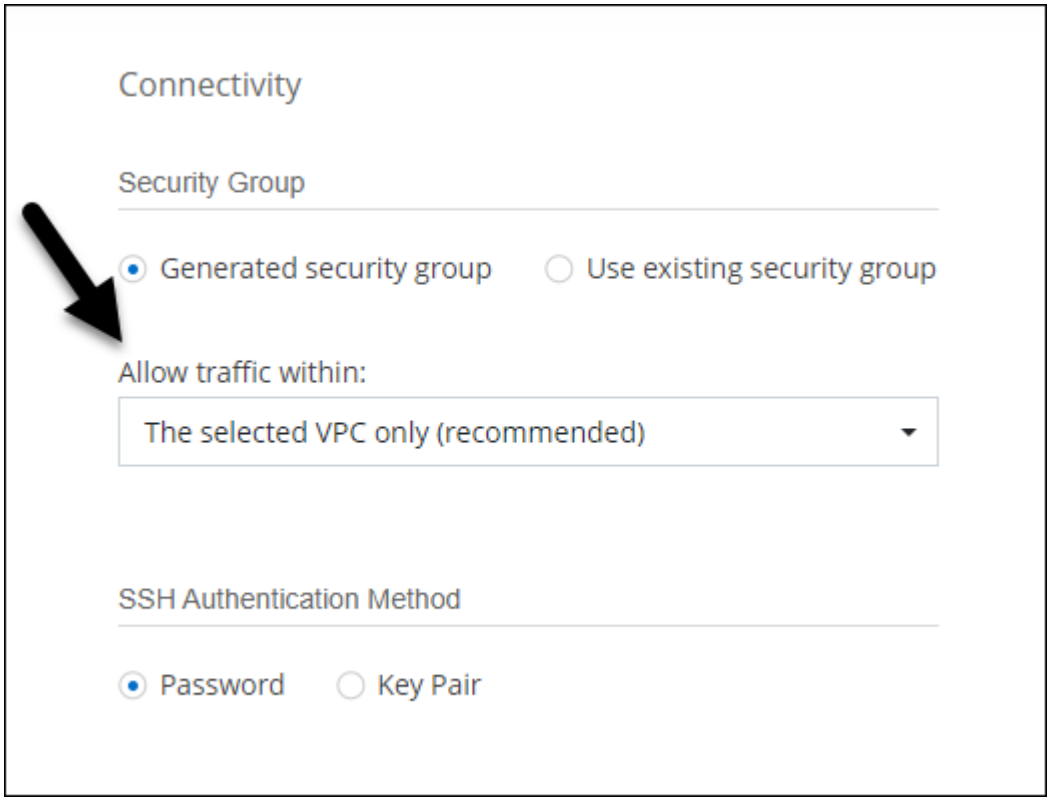
變更充電方法

您現在可以變更Cloud Volumes ONTAP 使用容量型授權的功能、以供選用的功能。例如、如果您部署Cloud Volumes ONTAP 的是含有Essentials套件的功能完善的系統、則當您的業務需求改變時、可以將其變更為Professional套件。此功能可從Digital Wallet取得。

"瞭解如何變更充電方法"。

安全性群組增強功能

當您建立Cloud Volumes ONTAP 一個運作環境時、使用者介面現在可讓您選擇是否要讓預先定義的安全性群組僅允許所選網路（建議）或所有網路內的流量。



2022年7月18日

Azure中的新授權方案

當您透過Azure Marketplace訂閱付費時、Azure上有兩個Cloud Volumes ONTAP 全新的容量型授權套件可供使用：

- 最佳化：分別為資源配置的容量和I/O作業付費
- 邊緣快取：授權 "Cloud Volumes Edge快取"

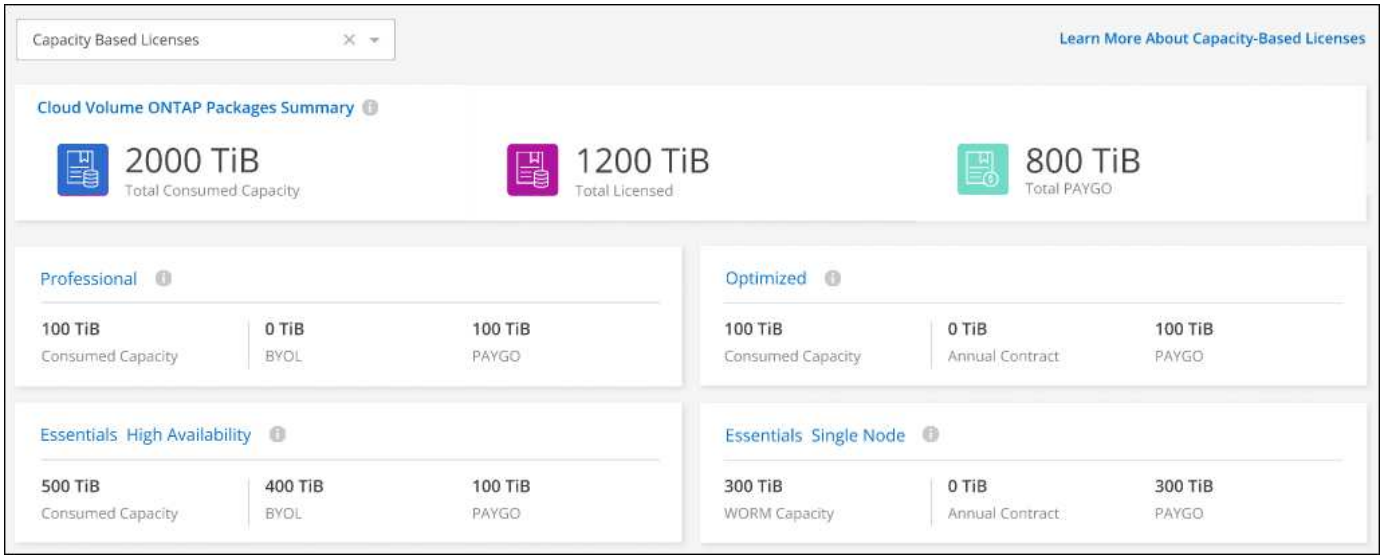
"深入瞭解這些授權套件"。

2022年7月3日

以下是3.9.20版Connector的變更。

數位錢包

數位錢包現在會顯示您帳戶的總使用容量、以及授權套件的使用容量。這有助於瞭解您的收費方式、以及您是否需要購買額外容量。



彈性磁碟區增強功能

在從Cloud Volumes ONTAP 使用者介面建立運作環境時、BlueXP現在支援Amazon EBS彈性磁碟區功能。使用GP3或IO1磁碟時、預設會啟用彈性磁碟區功能。您可以根據儲存需求來選擇初始容量、Cloud Volumes ONTAP 並在部署完畢後加以修改。

"深入瞭解AWS對彈性磁碟區的支援"。

AWS中的**SS3**授權**ONTAP**

現在AWS中執行9.11.0版或更新版本的全新和現有的版本不含支援的S3授權。ONTAP Cloud Volumes ONTAP

"瞭解如何在ONTAP 功能區中設定及管理S3物件儲存服務"

全新**Azure Cloud**區域支援

從9.10.1版開始、Cloud Volumes ONTAP 現在Azure West US 3地區支援了整套功能。

"檢視Cloud Volumes ONTAP 支援區域的完整清單以供參閱"

Azure中的**SS3**授權**ONTAP**

Azure中執行9.9.1版或更新版本的全新及現有的支援功能系統、現在已隨附一份支援功能S3的授權。ONTAP Cloud Volumes ONTAP

"瞭解如何在ONTAP 功能區中設定及管理S3物件儲存服務"

2022年6月7日

以下是3.9.19版本的Connector所做的變更。

零點9.11.1. Cloud Volumes ONTAP

現在、BlueXP可以部署及管理Cloud Volumes ONTAP 支援全新功能和其他雲端供應商區域的功能。

"深入瞭Cloud Volumes ONTAP 解本版的更新功能"

新的進階檢視

如果您需要執行Cloud Volumes ONTAP 進階的支援管理功能、可以使用ONTAP 支援ONTAP 此功能的支援功能、這個功能是隨附於一個系統的管理介面。我們已將System Manager介面直接納入BlueXP、因此您不需要離開BlueXP進行進階管理。

此「進階檢視」可作為Cloud Volumes ONTAP Preview搭配使用的版本（含E59.10.0及更新版本）。我們計畫改善這項體驗、並在即將推出的版本中加入增強功能。請使用產品內建聊天功能、向我們傳送意見反應。

"深入瞭解進階檢視"。

支援**Amazon EBS**彈性**Volume**

支援Amazon EBS Elastic Volumes功能搭配Cloud Volumes ONTAP 使用支援的不只能提供更好的效能和額外容量、還能讓BlueXP自動視需要增加基礎磁碟容量。

從_new _ Cloud Volumes ONTAP 版本-zhustr9.11.0系統、以及GP3和IO1 EBS磁碟類型開始、即可支援彈性磁碟區。

"深入瞭解彈性磁碟區的支援"。

請注意、若要支援彈性磁碟區、連接器需要新的AWS權限：

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

請務必為您新增至BlueXP的每組AWS認證資料提供這些權限。 "檢視AWS的最新Connector原則"。

支援在共享**AWS**子網路中部署**HA**配對

支援AWS VPC共享的支援範圍包括在內。Cloud Volumes ONTAP此版本的Connector可讓您在使用API時、將HA配對部署在AWS共用子網路中。

"瞭解如何在共用子網路中部署HA配對"。

使用服務端點時網路存取受限

現在、當使用vnet服務端點來連接Cloud Volumes ONTAP 時、BlueXP會限制網路存取、以利連接至各個儲存帳戶。如果您停用Azure Private Link連線、則BlueXP會使用服務端點。

"深入瞭解Azure Private Link與Cloud Volumes ONTAP NetApp的連線功能"。

支援在**Google Cloud**中建立儲存**VM**

從9.11.1版開始、Cloud Volumes ONTAP Google Cloud現在支援多個使用支援的儲存VM。從本版Connector開始、BlueXP可讓您Cloud Volumes ONTAP 使用API、在Google Cloud的「以雙埠HA配對」上建立儲存VM。

若要支援建立儲存VM、Connector需要新的Google Cloud權限：

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

請注意、您必須使用ONTAP NetApp CLI或System Manager、在單一節點系統上建立儲存VM。

- "深入瞭解Google Cloud中的儲存VM限制"
- "瞭解如何在Cloud Volumes ONTAP Google Cloud中建立資料服務儲存VM以供其使用"

2022年5月2日

以下是3.9.18版Connector所做的變更。

版本**9.11.0 Cloud Volumes ONTAP**

現在、BlueXP可以部署及管理Cloud Volumes ONTAP 功能更新9.11.0。

"深入瞭Cloud Volumes ONTAP 解本版的更新功能"。

強化中介升級

當BlueXP升級HA配對的中介程式時、它現在會在刪除開機磁碟之前驗證是否有新的中介映像可用。此變更可確保在升級程序失敗時、中介程序仍能繼續順利運作。

K8s標籤已移除

K8s索引標籤已在先前版本中過時、現在已移除。如果您想要搭配Cloud Volumes ONTAP 使用Kubernetes搭配使用、可以將託管Kubernetes叢集新增至Canvas、作為進階資料管理的工作環境。

"瞭解BlueXP中的Kubernetes資料管理"

Azure年度合約

Azure現已透過年度合約提供Essentials與Professional套裝軟體。您可以聯絡NetApp銷售代表以購買年度合約。該合約可在Azure Marketplace以私人優惠形式提供。

NetApp與您分享私人優惠之後、您可以在工作環境建立期間、從Azure Marketplace訂閱年度方案。

"深入瞭解授權"。

S3 Glacier即時擷取

您現在可以將階層式資料儲存在Amazon S3 Glacier即時擷取儲存類別中。

"瞭解如何變更階層式資料的儲存類別"。

Connector需要新的AWS權限

在單一可用度區域（AZ）中部署HA配對時、現在需要下列權限才能建立AWS分散配置群組：

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

現在需要這些權限、才能最佳化BlueXP建立放置群組的方式。

請務必為您新增至BlueXP的每組AWS認證資料提供這些權限。 "檢視AWS的最新Connector原則"。

新的Google Cloud區域支援

從9.10.1版開始、下列Google Cloud區域現在支援此功能：Cloud Volumes ONTAP

- 德里（亞洲-南2）
- 墨爾本（澳洲-蘇特斯塔2）
- Milan（Europe - west8）-僅限單一節點
- Santiago,（西南1）-僅限單一節點

"檢視Cloud Volumes ONTAP 支援區域的完整清單以供參閱"

在Google Cloud中支援n2-Standard-16

從Cloud Volumes ONTAP 9.10.1版開始、Google Cloud現在支援使用支援n2-Standard-16機器類型的功能。

"在Cloud Volumes ONTAP Google Cloud中檢視支援的支援功能組態"

Google Cloud防火牆原則的增強功能

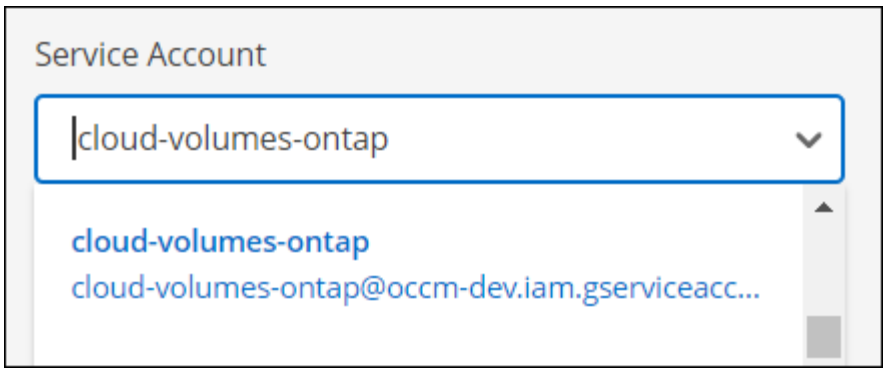
- 當您Cloud Volumes ONTAP 在Google Cloud中建立一個「叢集式HA配對」時、BlueXP現在會在VPC中顯示所有現有的防火牆原則。

  之前、BlueXP不會在VPC-1、VPC-2或VPC-3中顯示任何沒有目標標記的原則。

- 當您Cloud Volumes ONTAP 在Google Cloud中建立一個單一節點系統時、現在您可以選擇是否要預先定義的防火牆原則、僅允許所選VPC（建議）或所有VPC內的流量。

Google Cloud服務帳戶的增強功能

當您選擇要搭配Cloud Volumes ONTAP 使用的Google Cloud服務帳戶時、BlueXP現在會顯示與每個服務帳戶相關的電子郵件地址。檢視電子郵件地址可讓您更容易區分共用相同名稱的服務帳戶。



2022年4月3日

System Manager連結已移除

我們已移除Cloud Volumes ONTAP 先前可從功能環境中取得的System Manager連結。

您仍可在連線Cloud Volumes ONTAP 至該系統的網頁瀏覽器中輸入叢集管理IP位址、以連線至System Manager。 "深入瞭解連線至System Manager"。

WORM儲存設備充電

入門特惠費率已經到期、現在您將需要支付使用WORM儲存設備的費用。根據WORM磁碟區的總配置容量、每小時充電一次。這適用於新的Cloud Volumes ONTAP 和現有的不全系統。

"瞭解WORM儲存設備的定價"。

2022年2月27日

以下變更是在版本3.9.16的Connector中進行。

重新設計**Volume**精靈

我們最近推出的「建立新磁碟區精靈」、現在可從*進階分配*選項在特定的集合體上建立磁碟區。

"瞭解如何在特定的Aggregate上建立磁碟區"。

2022年2月9日

市場更新

- Essentials套件與專業版套件現已在所有雲端供應商的市場中推出。

  這些隨容量付費方法可讓您按小時付費、或直接向雲端供應商購買年度合約。您仍可選擇直接向NetApp購買隨容量授權。

  如果您在雲端市場中有現有的訂閱、您也會自動訂閱這些新服務項目。您可以在部署全新Cloud Volumes ONTAP 的運作環境時、選擇隨容量充電。

  如果您是新客戶、當您建立新的工作環境時、BlueXP會提示您訂閱。

- 所有雲端供應商市場的個別節點授權已過時、不再適用於新訂閱者。這包括年度合約和每小時訂閱（Explore、Standard和Premium）。

  目前有有效訂閱的客戶仍可使用此收費方法。

"深入瞭Cloud Volumes ONTAP 解適用於NetApp的授權選項"。

2022年2月6日

Exchange未指派的授權

如果Cloud Volumes ONTAP 您擁有尚未使用的未指派節點型支援功能、您現在可以將授權轉換成Cloud Backup授權、Cloud Data Sense授權或Cloud Tiering授權、以交換授權。

此動作會撤銷Cloud Volumes ONTAP 此「不支援」授權、並針對相同到期日的服務建立等值金額的授權。

"瞭解如何交換未指派的節點型授權"。

2022年1月30日

以下變更是在版本3.9.15的Connector中提出的。

重新設計授權選項

我們重新設計了授權選擇畫面、以建立全新Cloud Volumes ONTAP 的運作環境。這些變更突顯了2021年7月推出的附加容量充電方法、並透過雲端供應商市場支援即將推出的產品。

數位錢包更新

我們在Cloud Volumes ONTAP 單一索引標籤中整合了各種不完整的授權、藉此更新*數位錢包*。

2022年1月2日

以下變更是在3.9.14版的Connector中提出的。

支援其他**Azure VM**類型

從9.10.1版開始、下列VM類型現在可在Microsoft Azure中支援此功能：Cloud Volumes ONTAP

- E4ds_v4
- E8ds_v4
- E32ds_v4
- E48ds_v4

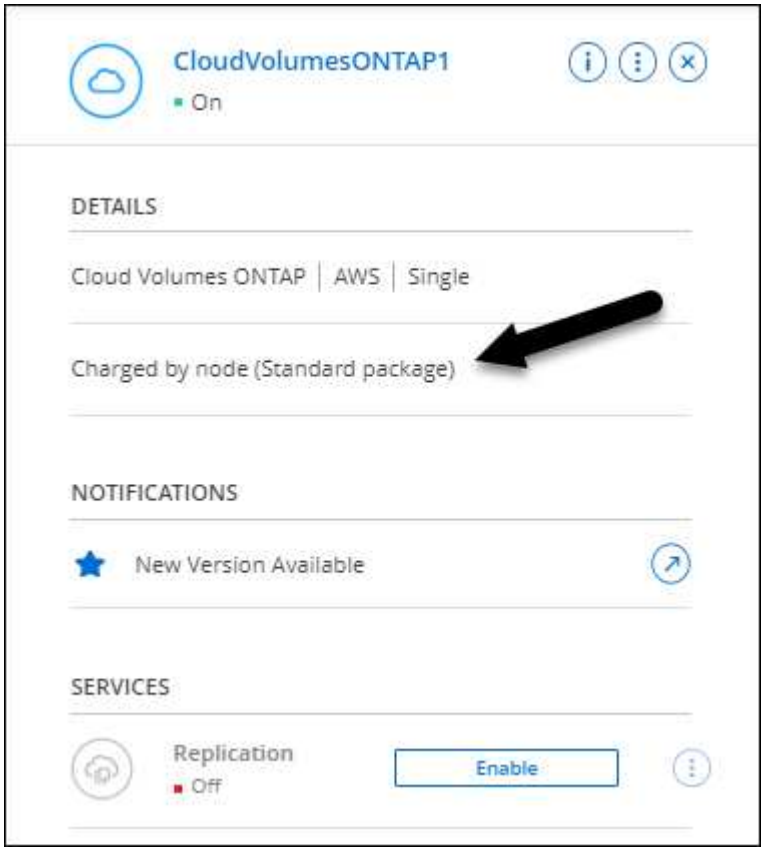
前往 "發行說明 Cloud Volumes ONTAP" 如需支援組態的詳細資訊、請參閱。

FlexClone充電更新

如果您使用 "容量型授權" 對於本產品、FlexClone磁碟區所使用的容量不再需要付費。Cloud Volumes ONTAP

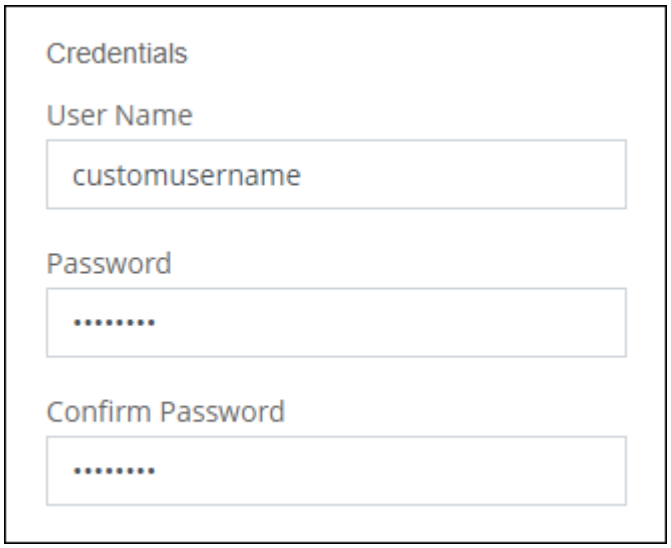
現在顯示充電方法

現在、BlueXP會在Cloud Volumes ONTAP 畫版的右側面板中顯示每個運作環境的充電方法。



選擇您的使用者名稱

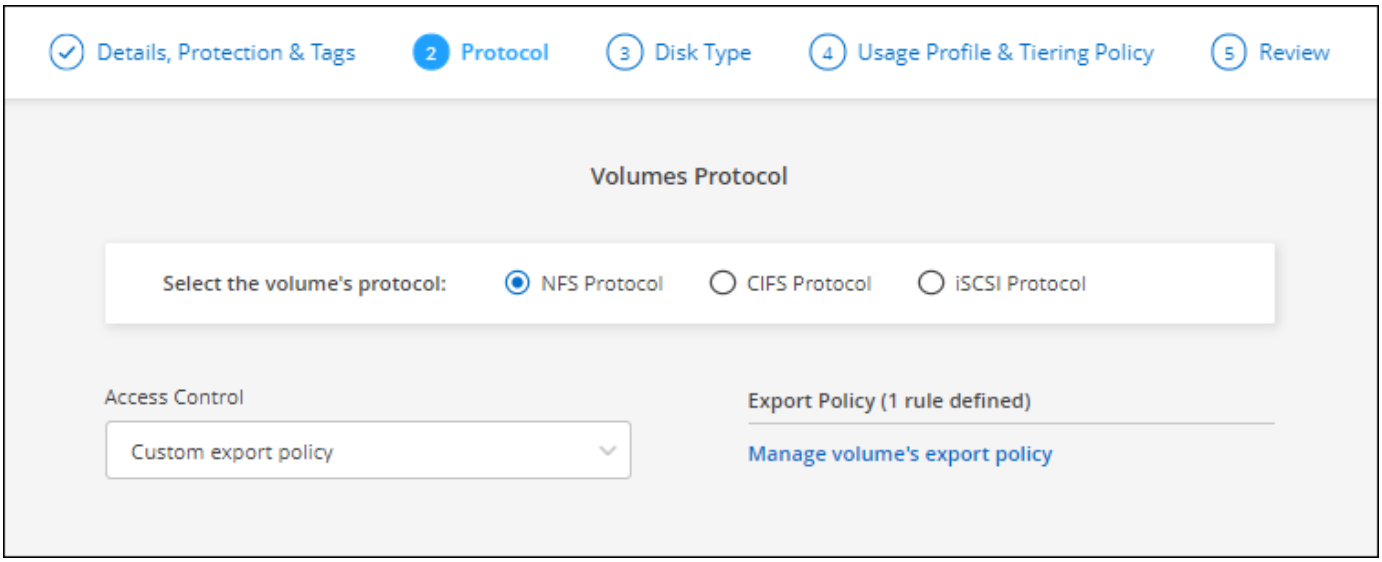
當您建立Cloud Volumes ONTAP 一個可運作的環境時、現在可以選擇輸入您偏好的使用者名稱、而非預設的管理使用者名稱。



Volume建立增強功能

我們在Volume建立方面做了一些增強：

- 我們重新設計了「建立Volume精靈」、以方便使用。
- 您現在可以選擇NFS的自訂匯出原則。



2021年11月28日

以下是連接器3.9.13版本的變更。

零點9.10.1 Cloud Volumes ONTAP

現在、BlueXP可以部署及管理Cloud Volumes ONTAP 功能更新9.10.1。

"深入瞭Cloud Volumes ONTAP 解本版的更新功能"。

NetApp Keystone 訂閱

您現在可以使用 Keystone 訂閱來支付 Cloud Volumes ONTAP HA 配對費用。

Keystone Subscription 是一項以隨成長付費訂閱為基礎的服務、可為偏好使用 OpEx 消費模式、而不選擇前期資本支出或租賃模式的使用者、提供順暢的混合雲體驗。

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

- "深入瞭解 NetApp Keystone 訂閱"。
- "瞭解如何開始使用 BlueXP 中的 Keystone 訂閱"。

全新AWS區域支援

目前支援AWS亞太地區（大阪）（亞太東北3區）的支援。Cloud Volumes ONTAP

連接埠減量

Azure中的任何一組節點系統和HA配對、連接埠8023和49000都不再開放於Cloud Volumes ONTAP 支援的整套系統上。

此變更適用於從Cloud Volumes ONTAP 連接器3.9.13版開始的_new _版。

2021年10月4日

以下是3.9.11版本的Connector所做的變更。

零點**9.10.0 Cloud Volumes ONTAP**

現在、BlueXP可以部署及管理Cloud Volumes ONTAP 功能更新9.10.0。

"深入瞭Cloud Volumes ONTAP 解本版的更新功能"。

縮短部署時間

我們縮短了在Cloud Volumes ONTAP Microsoft Azure或Google Cloud中部署運作環境所需的時間（啟用正常寫入速度時）。部署時間現在平均縮短3-4分鐘。

2021年9月2日

以下是連接器3.9.10版本的變更。

Azure中由客戶管理的加密金鑰

資料會使用在Cloud Volumes ONTAP Azure中的功能自動加密 "Azure 儲存服務加密" 使用Microsoft管理的金鑰。但您現在可以改為使用客戶管理的加密金鑰、只要完成下列步驟即可：

1. 從Azure建立金鑰保存庫、然後在該保存庫中產生金鑰。
2. 從BlueXP中、使用API建立Cloud Volumes ONTAP 使用金鑰的功能不受影響的環境。

"深入瞭解這些步驟"。

2021年7月7日

下列變更是隨附於Connector 3.9.8版中。

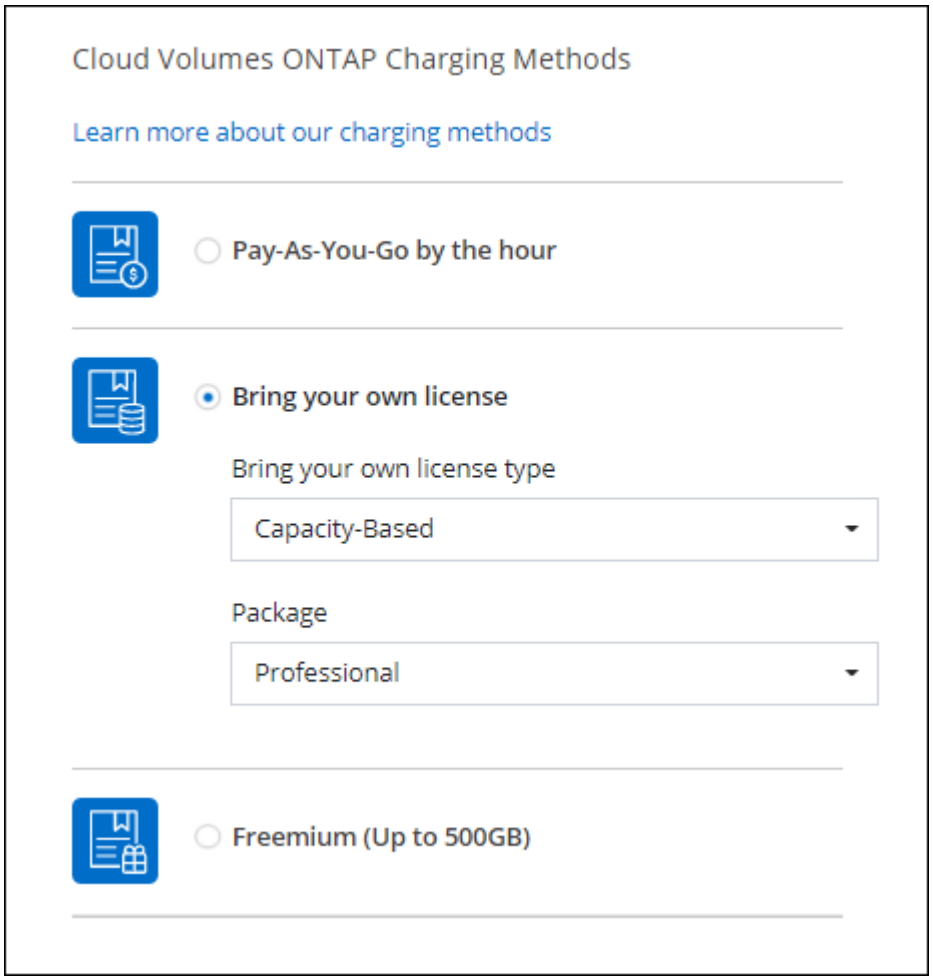
全新的充電方法

全新的充電方法Cloud Volumes ONTAP 可供使用。

- 容量型**BYOL**：容量型授權可讓您依照Cloud Volumes ONTAP 容量的每一TiB付費。授權與您的NetApp帳戶有關、只Cloud Volumes ONTAP 要您的授權有足夠的容量、您就能建立為多個版本的支援系統。容量型授權以套件形式提供、包括_Essentials或_Professional_。
- * Freemium產品*：Freemium可讓您免費使用Cloud Volumes ONTAP NetApp提供的所有功能（雲端供應商仍需付費）。每個系統的資源配置容量上限為500 GiB、而且沒有支援合約。您最多可擁有10個Freemium系統。

"深入瞭解這些授權選項"。

以下是您可以選擇的充電方法範例：



WORM儲存設備可供一般使用

一次寫入、多次讀取（WORM）儲存設備已不再處於預覽模式、現在可用於Cloud Volumes ONTAP 搭配使用。"深入瞭解 WORM 儲存設備"。

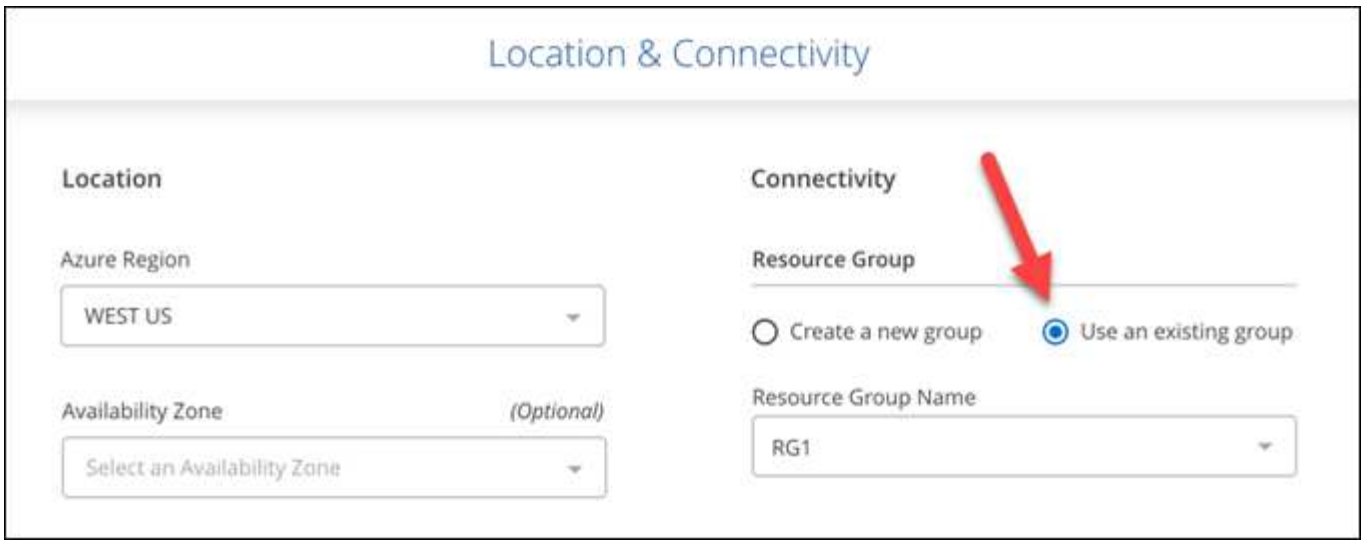
支援**AWS**中的**m5dn.24xlarge**

從9.9.1版開始、Cloud Volumes ONTAP 支援m5dn.24xLarge執行個體類型的功能如下：PAYGO Premium、自帶授權（BYOL）和Freemium。

"在Cloud Volumes ONTAP AWS中檢視支援的支援組態"。

選取現有的**Azure**資源群組

在Cloud Volumes ONTAP Azure中建立一套功能完善的系統時、您現在可以選擇現有的虛擬機器資源群組及其相關資源。



下列權限可讓BlueXP在Cloud Volumes ONTAP 部署失敗或刪除時、從資源群組中移除一些不必要的資源：

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

請務必為您新增至BlueXP的每組Azure認證提供這些權限。 "檢視Azure最新的Connector原則"。

Azure中現在已停用**BLOB**公開存取

為Cloud Volumes ONTAP 安全性增強、在建立適用於的儲存帳戶時、BlueXP現在會停用* Blob公有存取*。

Azure Private Link增強功能

根據預設、BlueXP現在可在開機診斷儲存帳戶上啟用Azure Private Link連線、以供新Cloud Volumes ONTAP 的作業系統使用。

這表示Cloud Volumes ONTAP 適用於此功能的_all_儲存帳戶現在將使用私有連結。

"深入瞭解如何搭配 Cloud Volumes ONTAP 使用 Azure 私有 Link 搭配使用功能"。

Google Cloud中的平衡式持續磁碟

從9.9.1版開始、Cloud Volumes ONTAP 支援平衡式持續磁碟（PD平衡）。

這些SSD可提供較低的每GiB IOPS、藉此平衡效能與成本。

Google Cloud不再支援**Custom-4-16384**

全新Cloud Volumes ONTAP 的功能不再支援custom 4-16384機器類型。

如果您在此機器類型上執行現有的系統、您可以繼續使用、但我們建議您切換至n2-Standard-4機器類型。

"在Cloud Volumes ONTAP GCP中檢視支援的組態"。

2021年5月30日

以下是3.9.7版本的Connector所帶來的變更。

AWS全新專業套件

全新的專業套裝軟體可Cloud Volumes ONTAP 讓您Cloud Backup Service 使用AWS Marketplace的年度合約來搭售各種功能。每TiB付款。此訂閱無法讓您備份內部資料。

如果您選擇此付款選項、Cloud Volumes ONTAP 您可以透過EBS磁碟、為每個支援系統配置最多2個PIB、並分層至S3物件儲存設備（單一節點或HA）。

前往 "AWS Marketplace頁面" 若要檢視價格詳細資料、請前往 "發行說明 Cloud Volumes ONTAP" 以深入瞭解此授權選項。

AWS中EBS磁碟區上的標記

現在、當BlueXP建立全新Cloud Volumes ONTAP 的運作環境時、它會將標記新增至EBS磁碟區。這些標記是Cloud Volumes ONTAP 在部署完畢後才建立的。

如果您的組織使用服務控制原則（SCP）來管理權限、這項變更將有助益。

自動分層原則的最低冷卻時間

如果您使用_auto_分層原則在磁碟區上啟用資料分層、您現在可以使用API調整最小冷卻時間。

"瞭解如何調整最低冷卻週期。"

增強自訂匯出原則

建立新的NFS Volume時、BlueXP現在會以遞增順序顯示自訂匯出原則、讓您更容易找到所需的匯出原則。

刪除舊的雲端快照

現在、BlueXP會刪除在Cloud Volumes ONTAP 部署完一套系統時、以及每次關機時所建立的舊版根磁碟和開機磁碟雲端快照。只有兩個最新的快照會同時保留給根磁碟區和開機磁碟區。

這項增強功能可移除不再需要的快照、協助降低雲端供應商的成本。

請注意、Connector需要新的權限才能刪除Azure快照。 "檢視Azure最新的Connector原則"。

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

2021年5月24日

部分9.9.1 Cloud Volumes ONTAP

現在、BlueXP可以部署及管理Cloud Volumes ONTAP 功能更新9.9.1。

"深入瞭Cloud Volumes ONTAP 解本版的更新功能"。

2021年4月11日

下列變更是隨附於3.9.5版的Connector所做的變更。

邏輯空間報告

現在、BlueXP可針對其建立的Cloud Volumes ONTAP 初始儲存虛擬機器、提供邏輯空間報告功能。

以邏輯方式回報空間時ONTAP 、此功能會報告磁碟區空間、讓儲存效率功能所節省的所有實體空間也會報告為已使用。

支援**AWS**中的**GP3**磁碟

從9.7版開始、支援_通用SSD（GP3）_磁碟。Cloud Volumes ONTAPGP3磁碟是成本最低的SSD、可在各種工作負載的成本與效能之間取得平衡。

"深入瞭解搭配Cloud Volumes ONTAP 使用GP3磁碟的相關資訊"。

AWS不再支援冷**HDD**磁碟

不再支援冷硬碟（SC1）磁碟。Cloud Volumes ONTAP

適用於**Azure**儲存帳戶的**TLS 1.2**

當BlueXP在Azure中建立儲存帳戶以Cloud Volumes ONTAP 供支援時、儲存帳戶的TLS版本現在是1.2版。

2021年3月8日

以下是3.9.4版連接器的變更。

版本**9.9.0 Cloud Volumes ONTAP**

現在、BlueXP可以部署及管理Cloud Volumes ONTAP 更新9.1.0。

"深入瞭Cloud Volumes ONTAP 解本版的更新功能"。

支援**AWS C2S**環境

您現在可以在Cloud Volumes ONTAP AWS商業雲端服務（C2S）環境中部署S效能 指數9.8。

"瞭解如何開始使用C2S"。

使用客戶管理的**CMK**進行**AWS**加密

BlueXP一向能讓您Cloud Volumes ONTAP 使用AWS金鑰管理服務（KMS）來加密支援的資料。從Cloud Volumes ONTAP 供應支援支援支援的9.9到0開始、如果您選擇客戶管理的CMK、EBS磁碟上的資料和階層至S3的資料都會加密。以前只會加密EBS資料。

請注意Cloud Volumes ONTAP 、您必須提供使用CMK的權限給IAM角色。

"深入瞭解如何設定AWS KMS Cloud Volumes ONTAP 搭配功能"。

支援Azure DoD

您現在可以在Cloud Volumes ONTAP Azure Department of Defence（DoD）Impact Level 6（IL6）中部署整套功能。

Google Cloud的IP位址減量

我們已經減少Cloud Volumes ONTAP 了在Google Cloud中使用NetApp 9.8及更新版本所需的IP位址數量。根據預設、需要少一個IP位址（我們將叢集間LIF與節點管理LIF統一化）。您也可以選擇在使用API時跳過SVM管理LIF的建立、如此可減少額外IP位址的需求。

"深入瞭解Google Cloud的IP位址需求"。

Google Cloud的共享VPC支援

當您在Cloud Volumes ONTAP Google Cloud中部署一組「叢集式HA」配對時、現在您可以選擇VPC-1、VPC-2和VPC-3的「共享式VPC」。以前只有VPC-0可以是共享VPC。支援此變更Cloud Volumes ONTAP 的更新版本為支援。

"深入瞭解Google Cloud網路需求"。

2021年1月4日

下列變更是隨附於Connector 3.9.2版本中。

AWS outs

幾個月前、我們宣佈 Cloud Volumes ONTAP 、在 Amazon Web Services （ AWS ）的「 Ready 」（就緒）頭銜中、此產品已獲獎。今天、我們很高興宣布、我們已驗證了BlueXP和Cloud Volumes ONTAP 以AWS outs為基礎的功能。

如果您有 AWS Outpost 、您可以 Cloud Volumes ONTAP 在「工作環境」精靈中選取 Outpost VPC 、在該 Outpost 中部署功能不全。體驗與 AWS 中的任何其他 VPC 相同。請注意、您必須先在 AWS Outpost 部署 Connector 。

有幾項限制可以指出：

- 目前僅 Cloud Volumes ONTAP 支援單一節點的不支援系統
- 您可以搭配 Cloud Volumes ONTAP 使用的 EC2 執行個體僅限於您的據點所提供的項目
- 目前僅支援通用SSD（gp2）

支援Azure地區的Ultra SSD VNVRAM

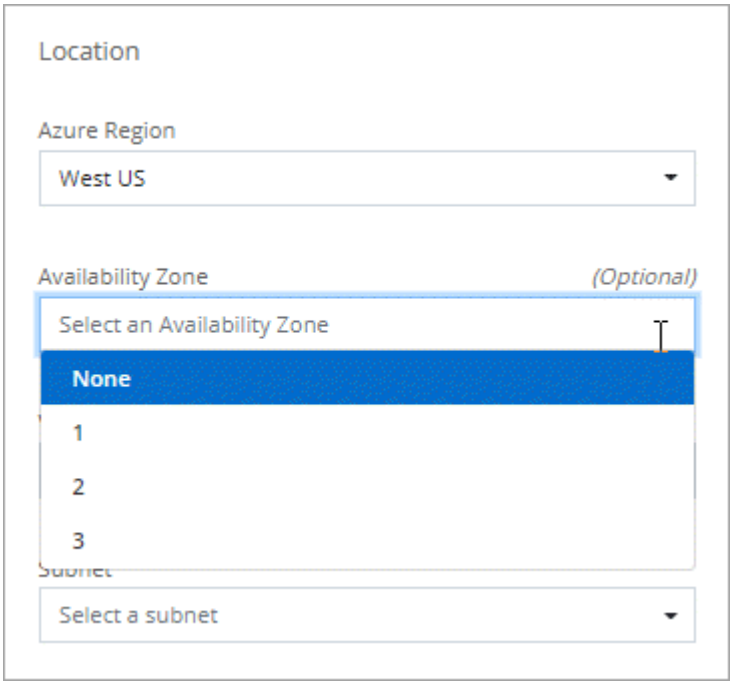
當您在單一節點系統上使用 E32s_v3 VM 類型時、可使用 Ultra SSD 做為 VNVRAM Cloud Volumes ONTAP "在任何受支援的 Azure 地區"。

VNVRAM 提供更佳的寫入效能。

選擇Azure中的可用度區域

您現在可以選擇要在其中部署單一節點 Cloud Volumes ONTAP 的可用度區域。如果您未選擇AZ、則BlueXP會

為您選擇一個。



Google Cloud中的較大磁碟

目前支援 GCP 中的 64 TB 磁碟。 Cloud Volumes ONTAP

由於 GCP 限制、單獨使用磁碟的最大系統容量仍維持在 256 TB 。

Google Cloud中的新機器類型

目前支援下列機器類型： Cloud Volumes ONTAP

- n2-Standard-4 （含 Explore 授權）及 BYOL
- n2-Standard/8 （含標準授權）及 BYOL
- n2-Standard-32 （含 Premium 授權）及 BYOL

2020年11月3日

以下是3.9.0版的Connector所做的變更。

Azure Private Link Cloud Volumes ONTAP for 功能

根據預設、BlueXP現在可在Cloud Volumes ONTAP 支援的儲存帳戶之間啟用Azure Private Link連線。私有連結可保護 Azure 中端點之間的連線安全。

- "深入瞭解 Azure 私有連結"
- "深入瞭解如何搭配 Cloud Volumes ONTAP 使用 Azure 私有 Link 搭配使用功能"

已知限制

已知限制指出本產品版本不支援的平台、裝置或功能、或是無法與產品正確互通的平台、裝置或功能。請仔細檢閱這些限制。

這些限制僅適用於 BlueXP 中的 Cloud Volumes ONTAP 管理。若要檢視Cloud Volumes ONTAP 有關此功能的限制、 "前往Cloud Volumes ONTAP 《發行說明》"

BlueXP 不支援建立 FlexGroup Volume

雖然 Cloud Volumes ONTAP 支援 FlexGroup 磁碟區、但 BlueXP 目前不支援建立 FlexGroup 磁碟區。如果FlexGroup 您從System Manager或CLI建立一個支援功能區、則應將BlueXP的容量管理模式設為手動。自動模式可能無法與 FlexGroup 功能不全的功能搭配使用。

在 BlueXP 中建立 FlexGroup 磁碟區的能力已計畫在未來的版本中推出。

BlueXP不支援Cloud Volumes ONTAP S3搭配使用

雖然 Cloud Volumes ONTAP 支援 S3 作為橫向擴充儲存設備的選項、但 BlueXP 並未提供任何此功能的管理功能。使用CLI是設定S3用戶端從Cloud Volumes ONTAP 功能支援的最佳實務做法。如需詳細資訊、請參閱 "S3組態電源指南"。

"深入瞭Cloud Volumes ONTAP 解支援S3和其他用戶端傳輸協定的功能"。

BlueXP不支援儲存VM的災難恢復

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

"深入瞭解 SVM 災難恢復"。

發行說明 Cloud Volumes ONTAP

《發行說明Cloud Volumes ONTAP 》for the發行說明提供特定版本的資訊。版本的新功能、支援的組態、儲存限制、以及任何可能影響產品功能的已知限制或問題。

"前往Cloud Volumes ONTAP 《發行說明》"

開始使用

深入瞭解 Cloud Volumes ONTAP

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

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

- 儲存效率

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

- 高可用度

  確保雲端環境發生故障時、企業的可靠性和持續營運。

- 資料保護

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

  Cloud Volumes ONTAP 也與 BlueXP 備份與還原整合、提供保護的備份與還原功能、以及雲端資料的長期歸檔。

  "深入瞭解 BlueXP 備份與還原"

- 資料分層

  在高效能與低效能儲存資源池之間隨需切換、而不需將應用程式離線。

- 應用程式一致性

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

  "深入瞭SnapCenter 解功能"

- 資料安全

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

- 隱私權法規遵循控管

  與 BlueXP 分類整合可協助您瞭解資料內容並識別敏感資料。

  "深入瞭解 BlueXP 分類"

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

"檢視支援 Cloud Volumes ONTAP 的支援的支援功能"

"深入瞭 Cloud Volumes ONTAP 解功能"

支援的新部署 ONTAP 版本

在ONTAP 您建立全新Cloud Volumes ONTAP 的支援環境時、BlueXP可讓您從多個不同的支援版本中進行選擇。

此處列出的 Cloud Volumes ONTAP 版本以外的版本不適用於新部署。如需有關升級的資訊、請參閱 "支援的升級途徑"。

AWS

單一節點

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 正式
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 p6

HA配對

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 正式
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1

- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 p6

Azure

單一節點

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 正式
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6
- 9.5 p6

HA配對

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 正式
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6

Google Cloud

單一節點

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 正式
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

HA配對

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 正式
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

Amazon Web Services入門

在**AWS**中快速入門**Cloud Volumes ONTAP**

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

建立連接器

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

請注意、如果您想要在Cloud Volumes ONTAP 無法存取網際網路的子網路中部署支援、則必須手動安裝Connector、並存取在該Connector上執行的BlueXP使用者介面。 "瞭解如何在無法存取網際網路的位置手動安裝Connector"

2 規劃您的組態

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

3 設定您的網路

1. 確保您的 VPC 和子網路支援連接器與 Cloud Volumes ONTAP 支援之間的連線。
2. 啟用從目標VPC for NetApp AutoSupport 的傳出網際網路存取功能。

   如果您在Cloud Volumes ONTAP 無法存取網際網路的位置部署支援、則不需要執行此步驟。

3. 設定 S3 服務的 VPC 端點。

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

"深入瞭解網路需求"。

4 設定 **AWS KMS**

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

5 使用**BlueXP**啟動**Cloud Volumes ONTAP**

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

相關連結

- "在AWS中從BlueXP建立連接器"
- "從AWS Marketplace建立連接器"
- "在內部部署安裝並設定 Connector"
- "Connector的AWS權限"

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

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

選擇**Cloud Volumes ONTAP** 一個不含功能的授權

有多種授權選項可供Cloud Volumes ONTAP 選擇。每個選項都能讓您選擇符合需求的消費模式。

- "深入瞭Cloud Volumes ONTAP 解適用於此功能的授權選項"
- "瞭解如何設定授權"

選擇支援的地區

支援大部分 AWS 地區的支援。 Cloud Volumes ONTAP "檢視支援區域的完整清單"。

您必須先啟用較新的 AWS 區域、才能在這些區域中建立及管理資源。 "瞭解如何啟用地區"。

選擇支援的本機區域

某些 AWS 本機區域（包括新加坡）支援 Cloud Volumes ONTAP 。選擇本機區域是選擇性的。

"檢視本機區域的完整清單"。
您必須先啟用本機區域、才能在這些區域中建立和管理資源。

"瞭解如何啟用本機區域"。

Phoenix 不是支援的本機區域。

選擇支援的執行個體

根據您選擇的授權類型、支援多種執行個體類型。 Cloud Volumes ONTAP

"AWS支援Cloud Volumes ONTAP 的支援組態"

瞭解儲存限制

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

"AWS的儲存限制Cloud Volumes ONTAP"

在**AWS**中調整系統規模

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

執行個體類型

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

EBS 磁碟類型

EBS磁碟類型之間的差異較高、如下所示。若要深入瞭解EBS磁碟的使用案例、請參閱 "AWS 文件： EBS Volume 類型"。

- _通用SSD（GP3）_磁碟是成本最低的SSD、可在各種工作負載的成本與效能之間取得平衡。效能是以IOPS和處理量來定義。支援GP3磁碟Cloud Volumes ONTAP 的版本可搭配使用。9.7及更新版本。

  當您選取GP3磁碟時、BlueXP會填入預設的IOPS和處理量值、這些值會根據選取的磁碟大小提供相當於gp2磁碟的效能。您可以提高價值、以更高的成本獲得更好的效能、但我們不支援較低的值、因為這樣可能導致效能低落。簡而言之、請保留預設值或增加預設值。請勿降低。 "深入瞭解GP3磁碟及其效能"。

  請注意Cloud Volumes ONTAP 、此功能可搭配GP3磁碟支援Amazon EBS彈性磁碟區功能。 "深入瞭解彈性磁碟區支援"。

- _通用SSD（gp2）_磁碟可平衡各種工作負載的成本與效能。效能是以 IOPS 定義。
- _資源配置的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Amazon EBS彈性Volume功能搭配IO1磁碟。 "深入瞭解彈性磁碟區支援"。

- _Throued Optimized HDD（ST1）_磁碟適用於經常存取的工作負載、這些工作負載需要以較低的價格提供快速且一致的處理量。

  使用處理量最佳化的HDD（ST1）時、不建議將資料分層至物件儲存設備。

EBS 磁碟大小

如果您選擇不支援的組態 "Amazon EBS彈性磁碟區功能"之後、您需要在啟動Cloud Volumes ONTAP 一套系統時選擇初始磁碟大小。之後、您就可以了 "讓BlueXP為您管理系統容量"但如果您想要的話 "自行建立集合體"請注意下列事項：

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

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

  如上所述、Cloud Volumes ONTAP 支援Amazon EBS彈性Volume功能的各種組態不支援選擇磁碟大小。 "深入瞭解彈性磁碟區支援"。

檢視預設系統磁碟

除了儲存使用者資料之外、BlueXP也購買雲端儲存設備來儲存Cloud Volumes ONTAP 作業系統資料（開機資料、根資料、核心資料和NVRAM）。為了規劃目的、在部署Cloud Volumes ONTAP 完更新之前、您可能需要先檢閱這些詳細資料。

"在Cloud Volumes ONTAP AWS中檢視系統資料的預設磁碟"。

連接器也需要系統磁碟。 "檢視Connector預設組態的詳細資料"。

準備在**Cloud Volumes ONTAP AWS Outpost**部署功能

如果您有 AWS Outpost 、您可以 Cloud Volumes ONTAP 在「工作環境」精靈中選取 Outpost VPC 、在該 Outpost 中部署功能不全。體驗與 AWS 中的任何其他 VPC 相同。請注意、您必須先在 AWS Outpost 部署 Connector 。

有幾項限制可以指出：

- 目前僅 Cloud Volumes ONTAP 支援單一節點的不支援系統
- 您可以搭配 Cloud Volumes ONTAP 使用的 EC2 執行個體僅限於您的據點所提供的項目
- 目前僅支援通用SSD（gp2）

收集網路資訊

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

單一**AZ**中的單一節點或**HA**配對

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

多個**AZs**中的**HA**配對

AWS 資訊	您的價值
區域	
VPC	
安全性群組（如果使用您自己的）	
節點 1 可用度區域	
節點 1 子網路	
節點 2 可用度區域	
節點 2 子網路	
中介可用度區域	
中介子網路	

AWS 資訊	您的價值
中介器的金鑰配對	
叢集管理連接埠的浮動 IP 位址	
節點 1 上資料的浮動 IP 位址	
節點 2 上資料的浮動 IP 位址	
浮動 IP 位址的路由表	

選擇寫入速度

BlueXP可讓您選擇Cloud Volumes ONTAP 適合的寫入速度設定。在您選擇寫入速度之前、您應該先瞭解一般與高設定之間的差異、以及使用高速寫入速度時的風險與建議。 "深入瞭解寫入速度"。

選擇**Volume**使用設定檔

包含多項儲存效率功能、可減少您所需的總儲存容量。 ONTAP在BlueXP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。您應該深入瞭解這些功能、以協助您決定要使用的設定檔。

NetApp 儲存效率功能提供下列效益：

資源隨需配置

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

重複資料刪除

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

壓縮

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

設定您的網路

AWS 的網路需求 **Cloud Volumes ONTAP**

BlueXP負責Cloud Volumes ONTAP 設定功能完善的網路元件、例如IP位址、網路遮罩和路由。您需要確保可以存取傳出網際網路、有足夠的私有IP位址可用、有適當的連線位置等等。

一般要求

AWS 必須符合下列要求。

對節點的輸出網際網路存取 **Cloud Volumes ONTAP**

支援NetApp功能的支援節點需要外傳網際網路存取功能、此功能可主動監控系統健全狀況、並將訊息傳送給NetApp技術支援部門。Cloud Volumes ONTAP AutoSupport

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

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

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

如果傳出的網際網路連線無法傳送AutoSupport 功能性訊息、則BlueXP會自動將Cloud Volumes ONTAP 您的功能性更新系統設定為使用Connector做為Proxy伺服器。唯一的需求是確保連接器的安全性群組允許連接埠3128上的傳入連線。部署Connector之後、您需要開啟此連接埠。

如果您定義了Cloud Volumes ONTAP 嚴格的傳出規則以供支援、那麼Cloud Volumes ONTAP 您也必須確保支援透過連接埠3128建立_Outbound _連線的安全性群組。

在您確認可以存取傳出網際網路之後、您可以測試AutoSupport 以確保能夠傳送訊息。如需相關指示、請參閱 "文件：設定檔ONTAP AutoSupport"。

如果BlueXP通知您AutoSupport 無法傳送資訊、 "疑難排解AutoSupport 您的VMware組態"。

HA 中介器的傳出網際網路存取

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

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

私有**IP**位址

BlueXP會自動分配所需的私有IP位址數量給Cloud Volumes ONTAP 整個過程。您必須確保網路有足夠的私有IP位址可用。

BlueXP分配Cloud Volumes ONTAP 給功能的生命量取決於您是部署單一節點系統或HA配對。LIF 是與實體連接埠相關聯的 IP 位址。

單一節點系統的**IP**位址

BlueXP會將6個IP位址分配給單一節點系統。

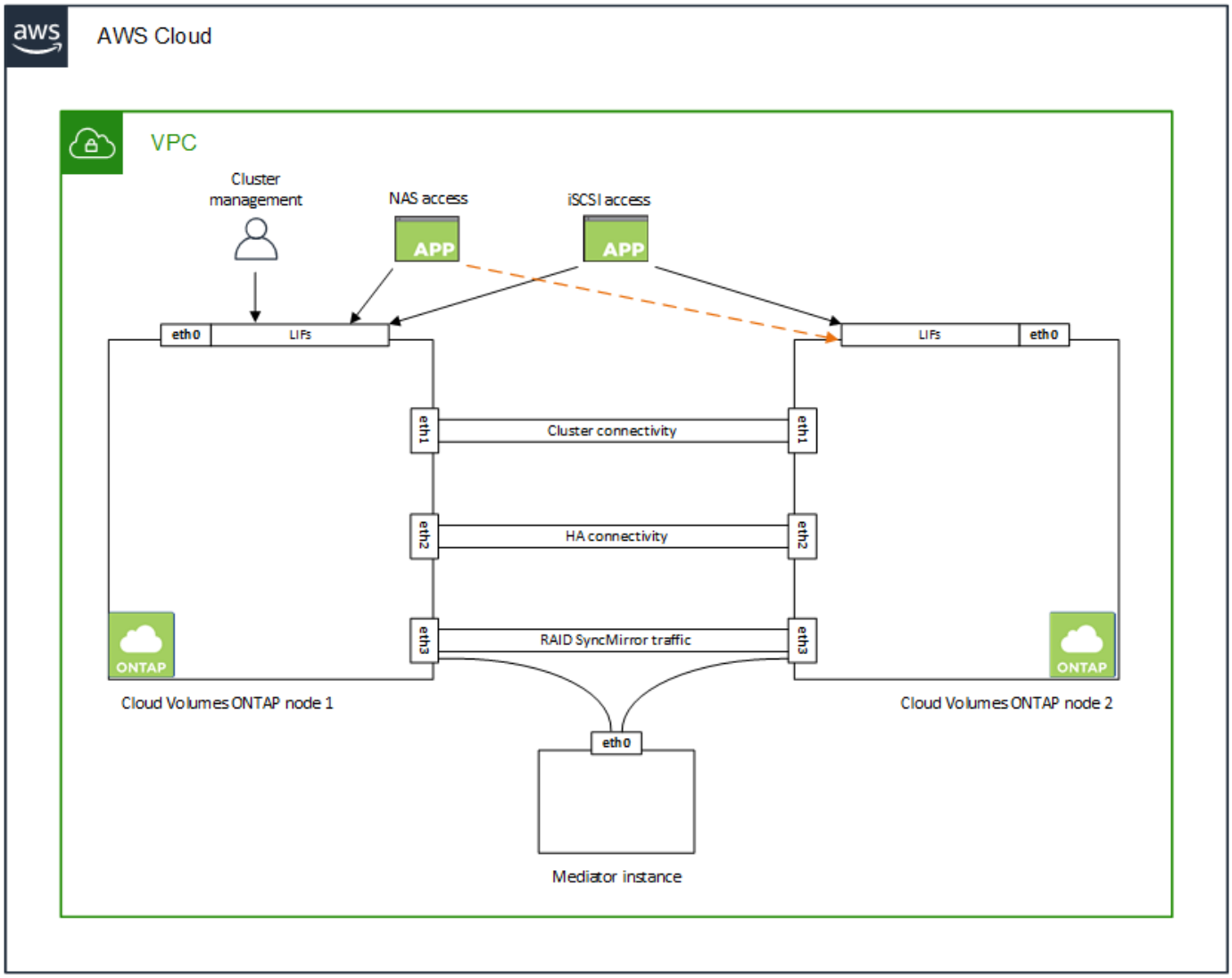
下表提供與每個私有IP位址相關聯的LIF詳細資料。

LIF	目的
叢集管理	整個叢集（HA配對）的管理管理。
節點管理	節點的管理管理。
叢集間	跨叢集通訊、備份與複寫。
NAS資料	透過NAS傳輸協定進行用戶端存取。
iSCSI資料	透過iSCSI傳輸協定進行用戶端存取。系統也用於其他重要的網路工作流程。此LIF為必填項目、不應刪除。

LIF	目的
儲存VM管理	儲存VM管理LIF可搭配SnapCenter 使用諸如VMware等管理工具。

HA配對的**IP**位址

HA配對比單一節點系統需要更多IP位址。這些IP位址分佈在不同的乙太網路介面上、如下圖所示：



HA配對所需的私有IP位址數目取決於您選擇的部署模式。部署在_onle_ AWS可用區域（AZ）中的HA配對需要15個私有IP位址、而部署在_multi__ AZs中的HA配對則需要13個私有IP位址。

下表提供與每個私有IP位址相關聯的LIF詳細資料。

HA配對的生命週數、在單一**AZ**中

LIF	介面	節點	目的
叢集管理	eth0	節點1	整個叢集（HA配對）的管理管理。
節點管理	eth0	節點1和節點2	節點的管理管理。
叢集間	eth0	節點1和節點2	跨叢集通訊、備份與複寫。

LIF	介面	節點	目的
NAS資料	eth0	節點1	透過NAS傳輸協定進行用戶端存取。
iSCSI資料	eth0	節點1和節點2	透過iSCSI傳輸協定進行用戶端存取。系統也用於其他重要的網路工作流程。這些生命是必要的、不應刪除。
叢集連線能力	eth1	節點1和節點2	可讓節點彼此通訊、並在叢集內移動資料。
HA連線能力	eth2	節點1和節點2	在發生容錯移轉時、兩個節點之間的通訊。
RSMiSCSI流量	eth3	節點1和節點2	RAID SyncMirror 支援iSCSI流量、以及兩Cloud Volumes ONTAP 個支援節點與中介器之間的通訊。
中介者	eth0	中介者	節點與中介器之間的通訊通道、可協助進行儲存接管與恢復程序。

多個**AZs**中**HA**配對的**LIF**

LIF	介面	節點	目的
節點管理	eth0	節點1和節點2	節點的管理管理。
叢集間	eth0	節點1和節點2	跨叢集通訊、備份與複寫。
iSCSI資料	eth0	節點1和節點2	透過iSCSI傳輸協定進行用戶端存取。這些LIF也能管理節點之間的浮動IP位址移轉作業。這些生命是必要的、不應刪除。
叢集連線能力	eth1	節點1和節點2	可讓節點彼此通訊、並在叢集內移動資料。
HA連線能力	eth2	節點1和節點2	在發生容錯移轉時、兩個節點之間的通訊。
RSMiSCSI流量	eth3	節點1和節點2	RAID SyncMirror 支援iSCSI流量、以及兩Cloud Volumes ONTAP 個支援節點與中介器之間的通訊。
中介者	eth0	中介者	節點與中介器之間的通訊通道、可協助進行儲存接管與恢復程序。

部署在多個可用度區域時、會與多個生命區建立關聯 "浮動 IP 位址"、不計入AWS私有IP限制。

安全性群組

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

正在尋找Connector的相關資訊？ "檢視Connector的安全群組規則"

資料分層連線

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

當您建立 VPC 端點時、請務必選取與 Cloud Volumes ONTAP 該實例相對應的區域、 VPC 和路由表。您也必

須修改安全性群組、以新增允許流量到 S3 端點的傳出 HTTPS 規則。否則 Cloud Volumes ONTAP 、無法連線至 S3 服務。

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

連線**ONTAP** 至功能鏈接

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

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

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

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

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

VPC共享

從9.11.1版開始、Cloud Volumes ONTAP AWS支援搭配VPC共享功能的更新版、VPC共用功能可讓您的組織與其他AWS帳戶共用子網路。若要使用此組態、您必須設定AWS環境、然後使用API部署HA配對。

"瞭解如何在共用子網路中部署HA配對"。

多個 **AZs** 的 **HA** 配對需求

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

若要瞭解 HA 配對的運作方式、請參閱 "高可用度配對"。

可用度區域

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

每個可用區域都應有一個子網路。

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

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

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

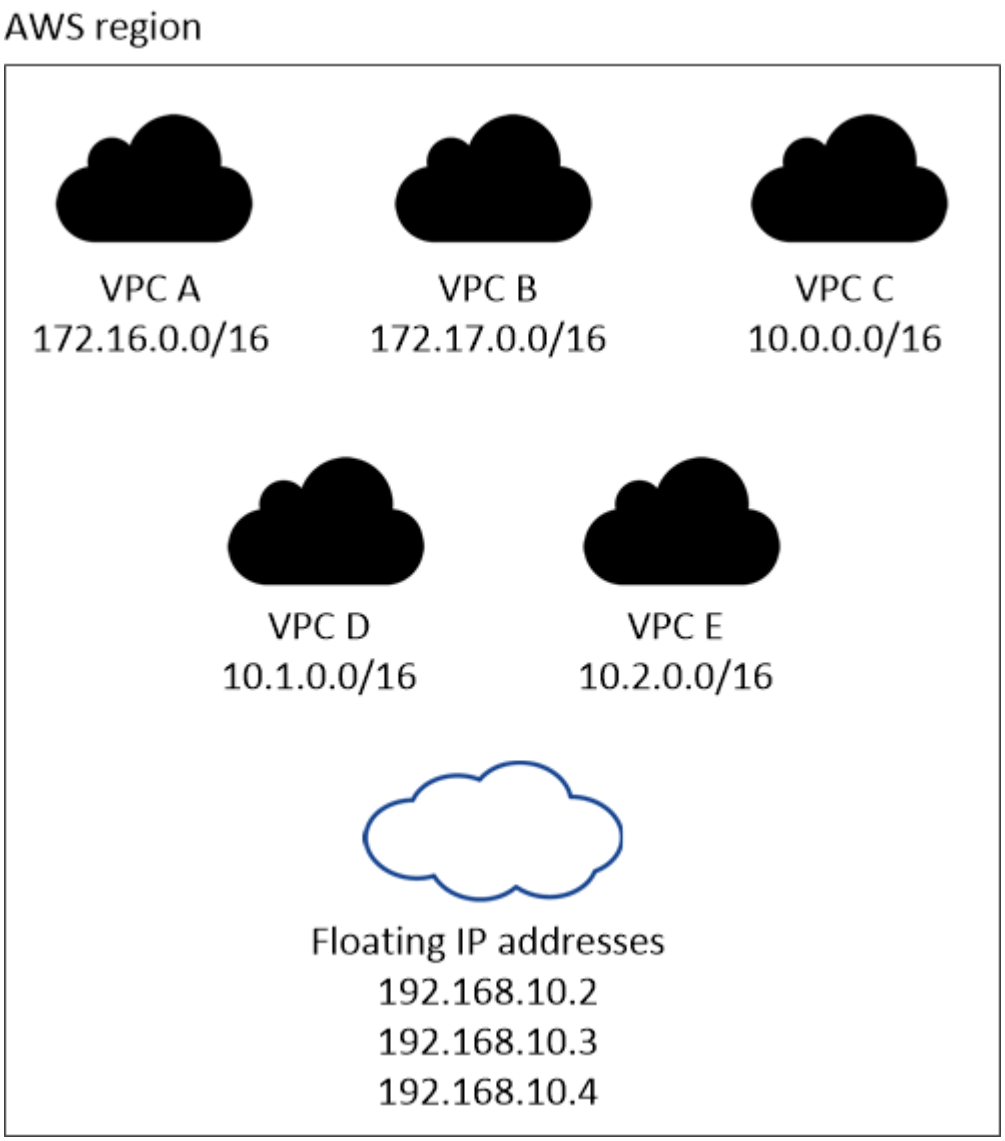
如果您使用 SnapDrive 適用於 Windows 的 SHIP 或 SnapCenter 搭配 HA 配對的 SHIP 、則 SVM 管理 LIF 需要一個浮動 IP 位址。

建立Cloud Volumes ONTAP 一套功能完善的運作環境時、您需要在BlueXP中輸入浮動IP位址。在啟動系統

時、BlueXP會將IP位址分配給HA配對。

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

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



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

傳輸閘道、可從 **VPC** 外部啟用浮動 **IP** 存取

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

路由表

在BlueXP中指定浮動IP位址之後、系統會提示您選取路由表、其中應包含通往浮動IP位址的路由。這可讓用戶端存取 HA 配對。

如果VPC中只有一個子網路路由表（主路由表）、則BlueXP會自動將浮動IP位址新增至該路由表。如果您有

多個路由表、在啟動 HA 配對時、請務必選取正確的路由表。否則、部分用戶端可能無法存取 Cloud Volumes ONTAP 功能不完全。

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

如需路由表的詳細資訊、請參閱 "AWS 文件：路由表"。

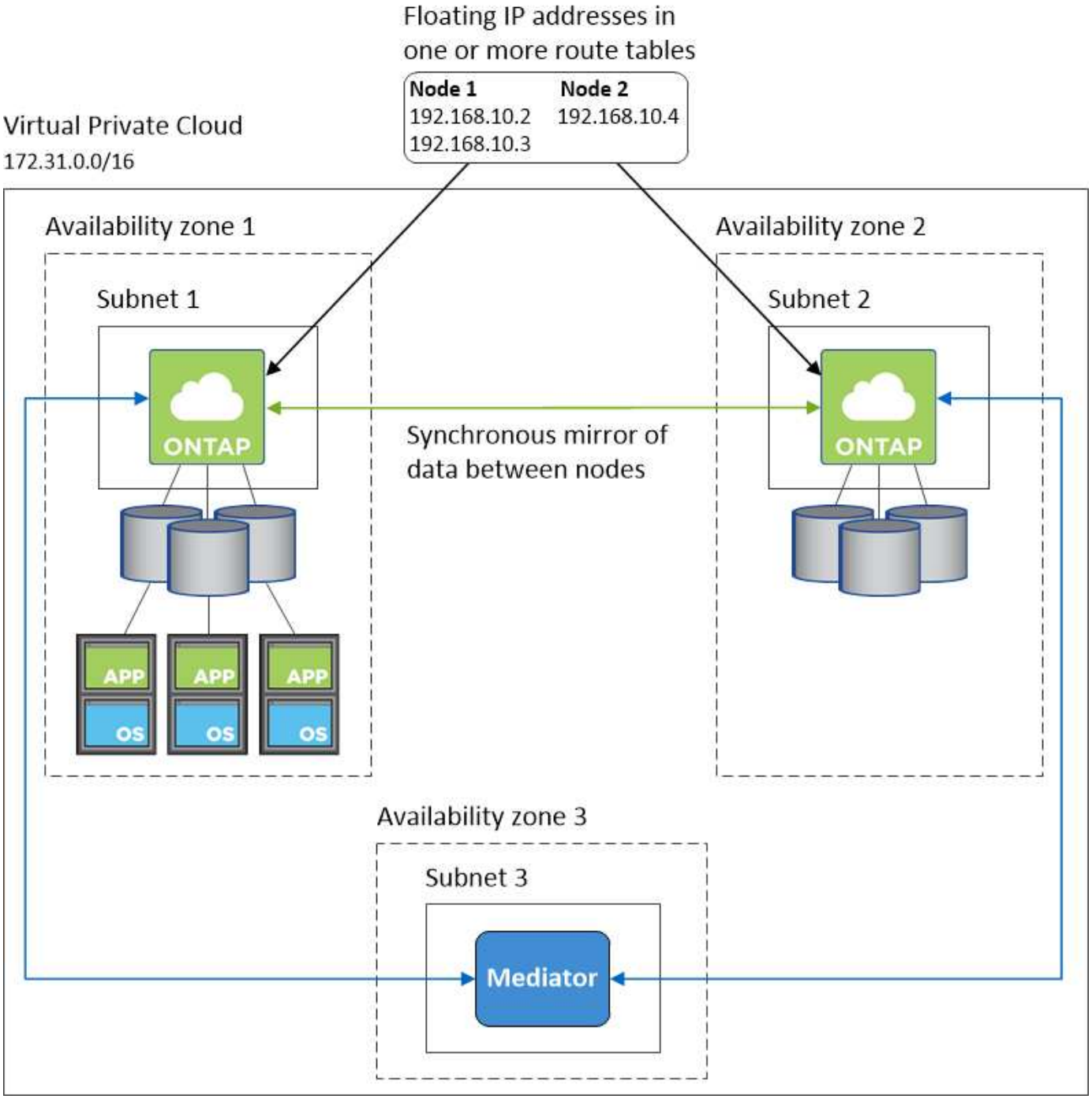
連線至 **NetApp** 管理工具

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

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

HA 組態範例

下圖說明多個AZs中HA配對的特定網路元件：三個可用度區域、三個子網路、浮動IP位址和路由表。



連接器需求

如果您尚未建立連接器、也應該檢閱連接器的網路需求。

- "檢視連接器的網路需求"
- "AWS中的安全群組規則"

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

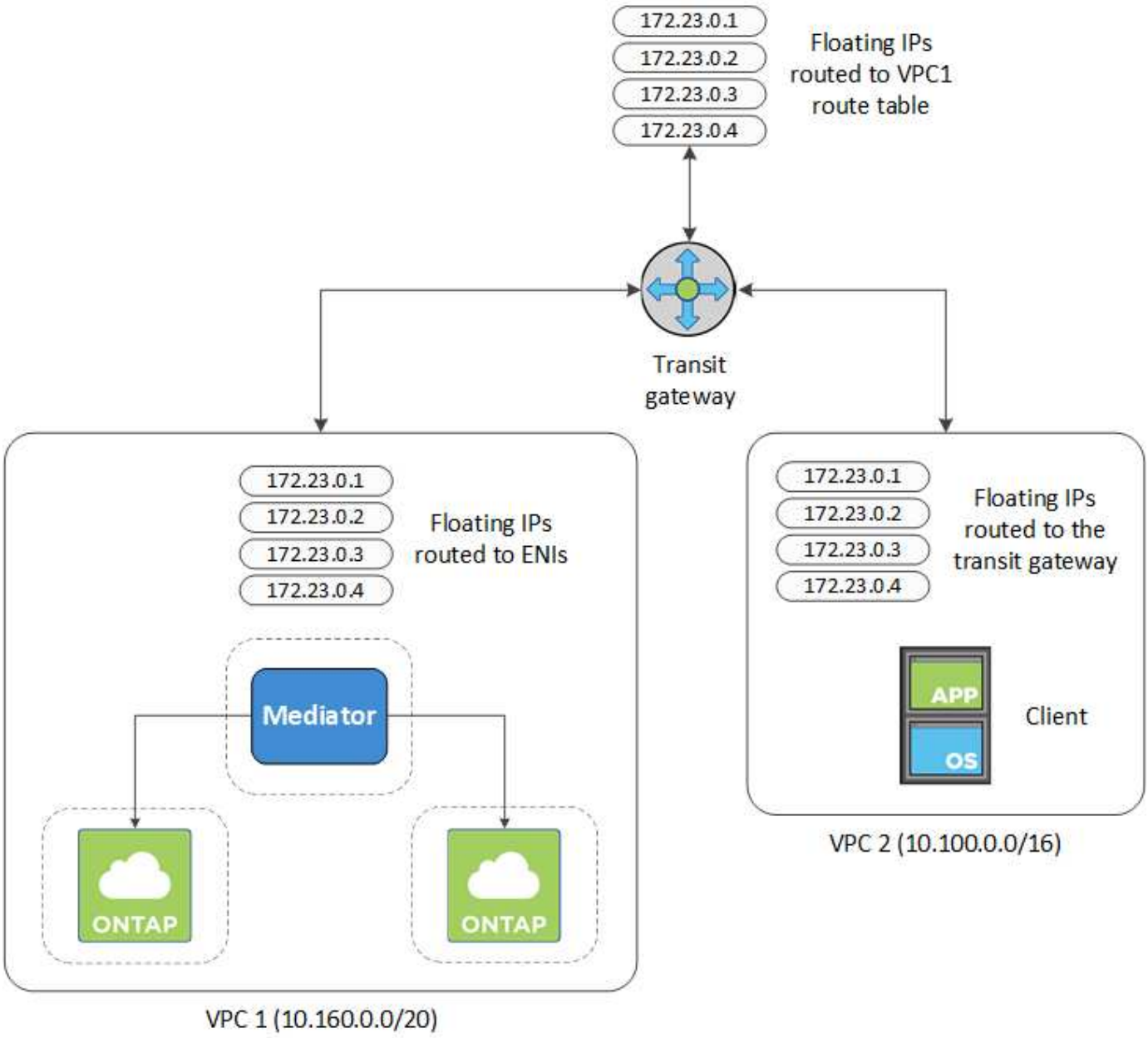
設定 AWS 傳輸閘道、以便存取 HA 配對 "浮動 IP 位址" 從 HA 配對所在的 VPC 外部。

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

叢集管理介面和選用的 SVM 管理 LIF 也需要浮動 IP 位址。

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

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



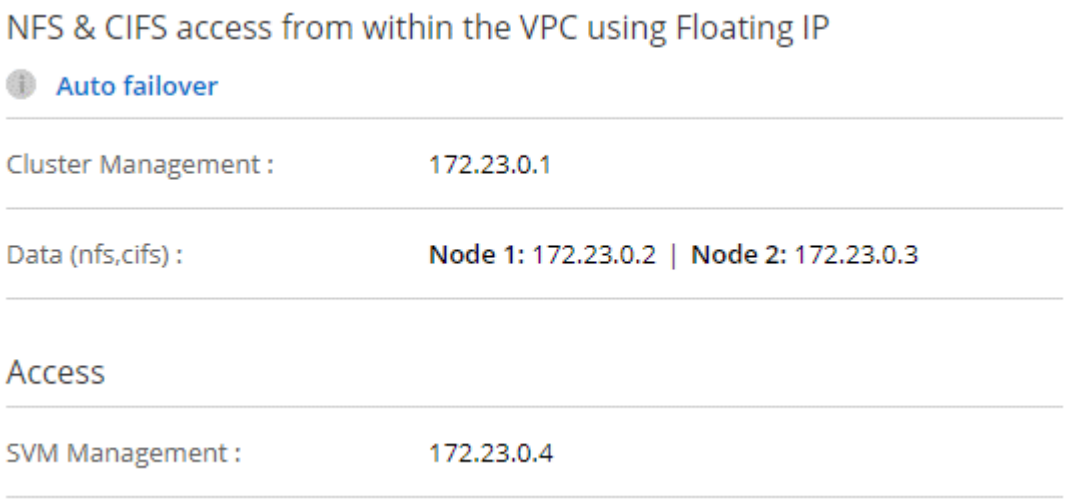
下列步驟說明如何設定類似的組態。

步驟

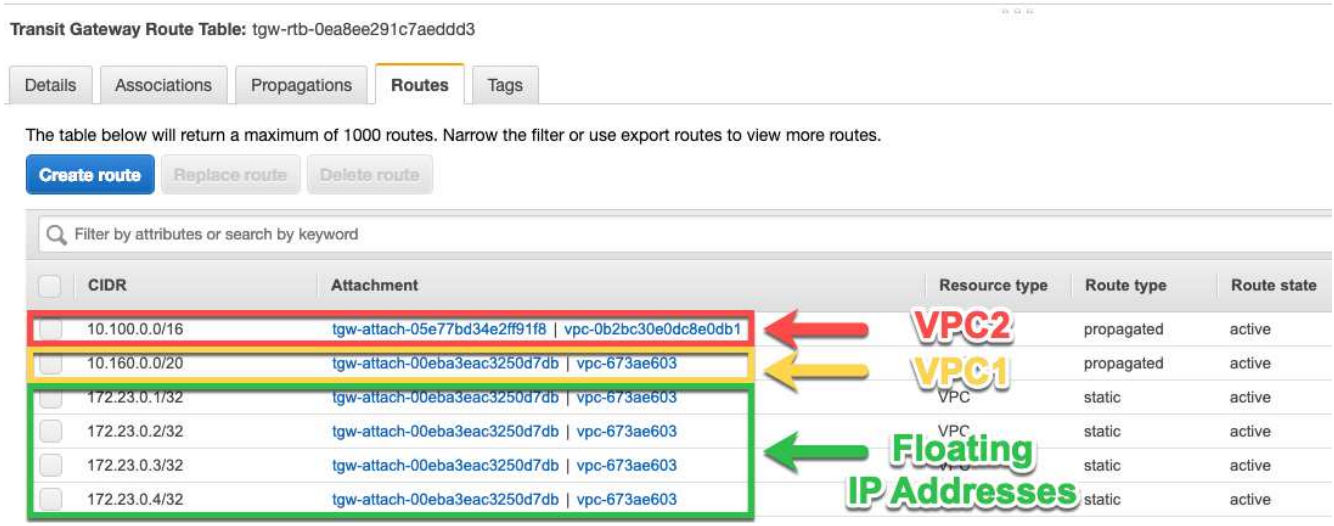
1. "建立傳輸閘道、並將 VPC 附加至閘道"。

2. 將VPC與傳輸閘道路由表建立關聯。
   a. 在* VPC*服務中、按一下* Transit Gateway Route Tables *。
   b. 選取路由表。
   c. 按一下「關聯」、然後選取「建立關聯」。
   d. 選擇要關聯的附件（VPC）、然後按一下*建立關聯*。
3. 指定 HA 配對的浮動 IP 位址、在傳輸閘道的路由表中建立路由。

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

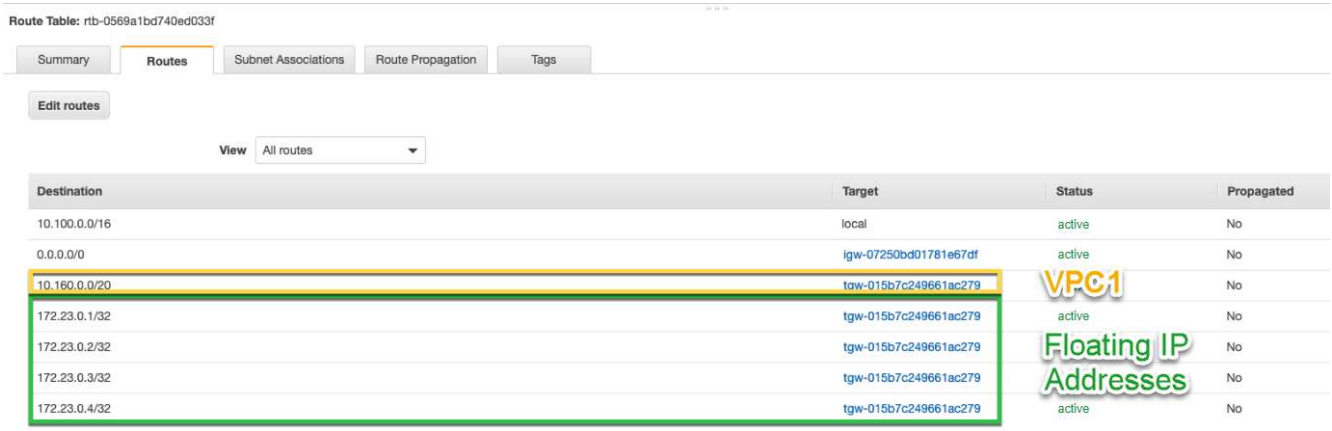


   下列範例影像顯示傳輸閘道的路由表。其中包括兩部 VPC 的 CIDR 區塊路由、 Cloud Volumes ONTAP 以及由 R1 使用的四個浮動 IP 位址。



4. 修改需要存取浮動 IP 位址的 VPC 路由表。
   a. 新增路由項目至浮動 IP 位址。
   b. 將路由項目新增至 HA 配對所在 VPC 的 CIDR 區塊。

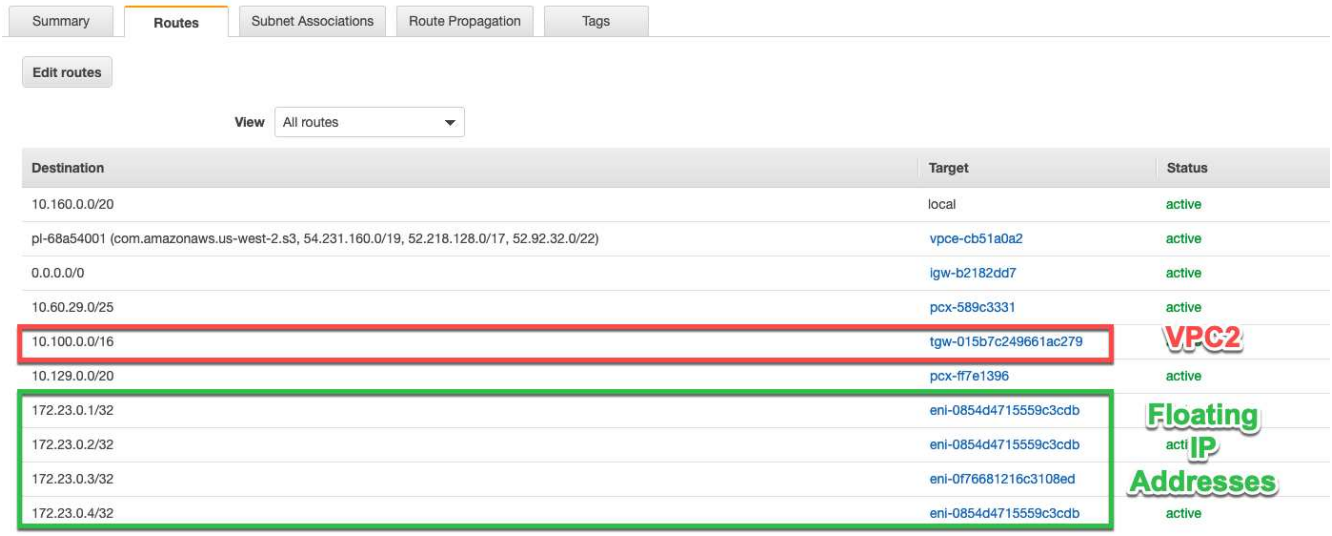
      下列範例影像顯示 VPC 2 的路由表、其中包括通往 VPC 1 的路由和浮動 IP 位址。



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

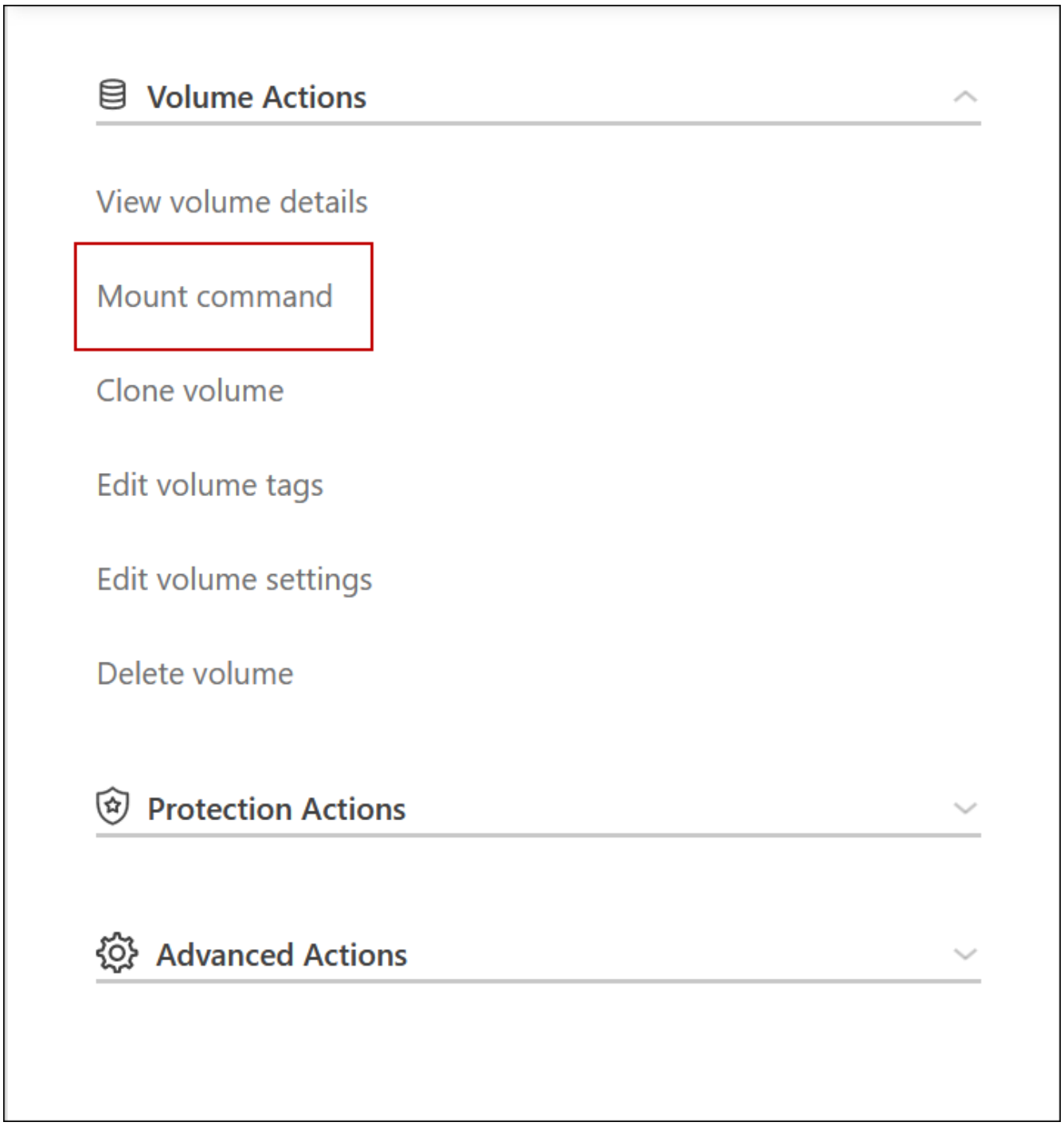
   此步驟非常重要、因為它會完成 VPC 之間的路由。

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



6. 將 VPC 的安全性群組設定更新為「所有流量」。
   a. 按一下 [虛擬私有雲] 底下的 [子網路] 。
   b. 按一下 * 路由表 * 索引標籤、為 HA 配對的其中一個浮動 IP 位址選取所需的環境。
   c. 按一下 * 安全性群組 * 。
   d. 選取 * 編輯輸入規則 * 。
   e. 按一下*新增規則*。
   f. 在 [類型] 下，選取 [* 所有流量] ，然後選取 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用戶端。

   您可以透過 BlueXP 中「管理磁碟區」面板下的 * 掛載命令 * 選項、在 BlueXP 中找到正確的 IP 位址。



8. 如果您要掛載NFS Volume、請設定匯出原則以符合用戶端VPC的子網路。

   "瞭解如何編輯Volume"。

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

在共享子網路中部署**HA**配對

從9.11.1版開始、Cloud Volumes ONTAP AWS支援搭配VPC共享功能的更新版、VPC共

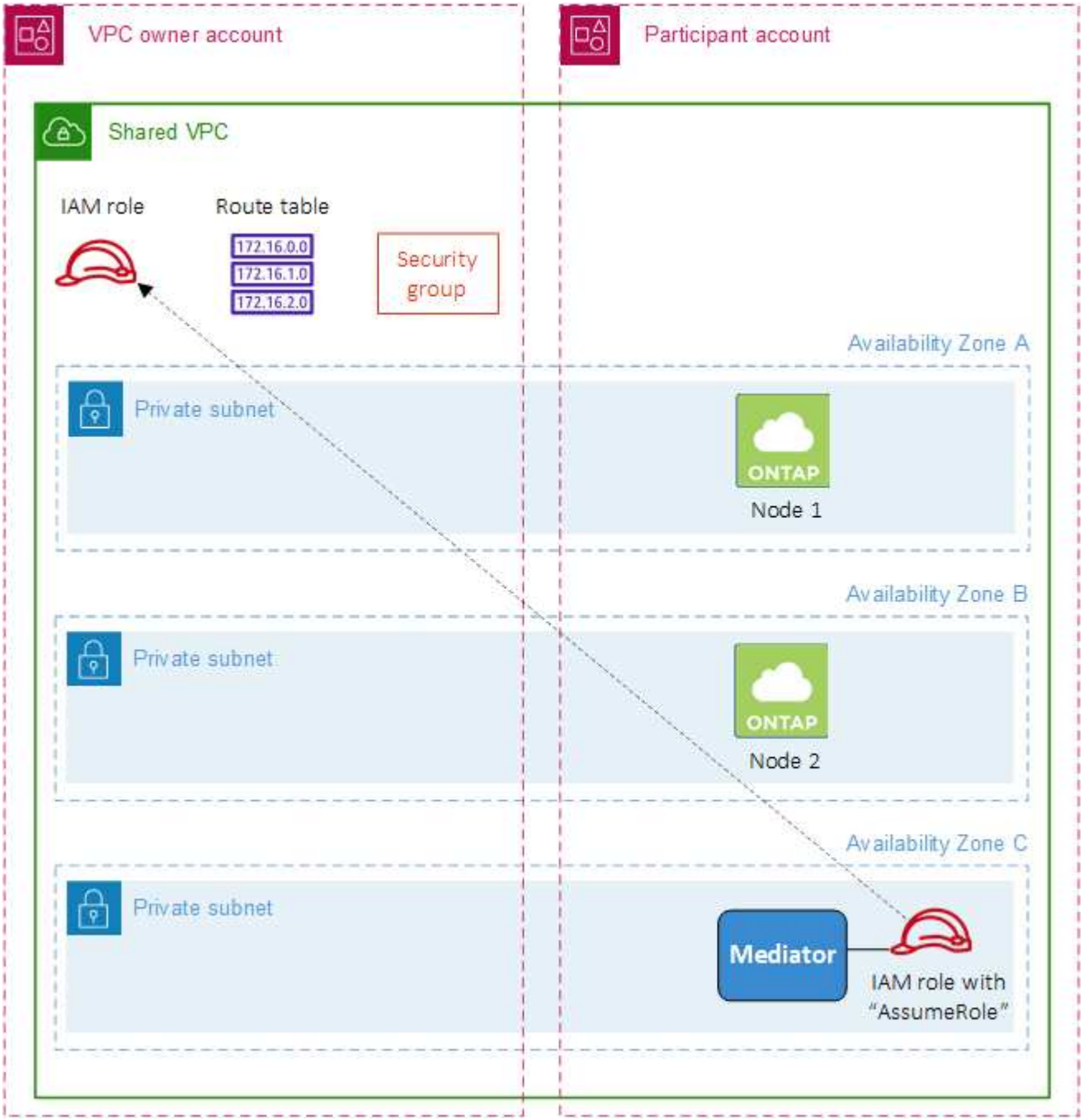
用功能可讓您的組織與其他AWS帳戶共用子網路。若要使用此組態、您必須設定AWS環境、然後使用API部署HA配對。

與 "VPC共享"、將一個功能豐富的全功能HA組態分佈於兩個帳戶：Cloud Volumes ONTAP

- VPC擁有者帳戶、擁有網路（VPC、子網路、路由表和Cloud Volumes ONTAP 保密群組）
- 參與者帳戶、其中EC2執行個體部署在共享子網路中（包括兩個HA節點和中介器）

若將某個版本部署在多個可用度區域中、HA中介程式需要特定權限、才能寫入VPC擁有者帳戶中的路由表。Cloud Volumes ONTAP您必須設定協調員可以承擔的IAM角色、以提供這些權限。

下圖顯示此部署所涉及的元件：



如下列步驟所述、您必須與參與者帳戶共用子網路、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 不協調作業環境時、BlueXP會自動建立IAM角色、並將其附加至協調者。此角色會假設您在VPC擁有者帳戶中建立的IAM角色、以便變更與HA配對相關的路由表。

步驟

1. 與參與者帳戶共用VPC擁有者帳戶中的子網路。

   若要在共用子網路中部署HA配對、必須執行此步驟。

   "AWS文件：共用子網路"

2. 在VPC擁有者帳戶中、建立Cloud Volumes ONTAP 一個安全群組以供使用。

   "請參閱Cloud Volumes ONTAP 安全性群組規則以瞭解相關資訊"。請注意、您不需要為HA中介者建立安全性群組。BlueXP能為您實現這項目標。

3. 在VPC擁有者帳戶中、建立包含下列權限的IAM角色：

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

4. 使用BlueXP API建立新Cloud Volumes ONTAP 的功能不全的工作環境。

   請注意、您必須指定下列欄位：

   - "安全性群組Id"

     「安全性GroupId」欄位應指定您在VPC擁有者帳戶中建立的安全性群組（請參閱上述步驟2）。

   - 「haParam」物件中的「assugerme勞力Arn」

     「assume勞力arn」欄位應包含您在VPC擁有者帳戶中建立的IAM角色ARN（請參閱上述步驟3）。

   例如：

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

+
"深入瞭Cloud Volumes ONTAP 解NetApp API"

AWS 的安全群組規則

BlueXP會建立AWS安全性群組、其中包括Cloud Volumes ONTAP 需要順利運作的傳入和傳出規則。您可能想要參照連接埠進行測試、或是想要使用自己的安全性群組。

規則 Cloud Volumes ONTAP

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

傳入規則

當您建立工作環境並選擇預先定義的安全性群組時、可以選擇允許下列其中一項的流量：

- *僅限選定VPC *：傳入流量的來源是VPC的子網路範圍（適用於Cloud Volumes ONTAP 整個系統）、以及連接器所在VPC的子網路範圍。這是建議的選項。
- 所有**VPC**：傳入流量的來源為0.00.0.0/0 IP範圍。

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

傳輸協定	連接埠	目的
UDP	161-162	簡單的網路管理傳輸協定
UDP	635	NFS 掛載
UDP	2049	NFS 伺服器精靈
UDP	4045	NFS 鎖定精靈
UDP	4046	NFS 的網路狀態監控
UDP	4049	NFS rquotad 傳輸協定

傳出規則

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

基本傳出規則

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

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

進階傳出規則

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

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

服務	傳輸協定	連接埠	來源	目的地	目的
Active Directory	TCP	88	節點管理 LIF	Active Directory 樹系	Kerberos V 驗證
	UDP	137.	節點管理 LIF	Active Directory 樹系	NetBios 名稱服務
	UDP	138	節點管理 LIF	Active Directory 樹系	NetBios 資料報服務
	TCP	139.	節點管理 LIF	Active Directory 樹系	NetBios 服務工作階段
	TCP 與 UDP	389	節點管理 LIF	Active Directory 樹系	LDAP
	TCP	445	節點管理 LIF	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	TCP	464. 64	節點管理 LIF	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	UDP	464. 64	節點管理 LIF	Active Directory 樹系	Kerberos 金鑰管理
	TCP	749	節點管理 LIF	Active Directory 樹系	Kerberos V 變更與設定密碼（ RPCSEC_GSS ）
	TCP	88	資料 LIF （ NFS 、 CIFS 、 iSCSI ）	Active Directory 樹系	Kerberos V 驗證
	UDP	137.	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 名稱服務
	UDP	138	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 資料報服務
	TCP	139.	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 服務工作階段
	TCP 與 UDP	389	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	LDAP
	TCP	445	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	TCP	464. 64	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	UDP	464. 64	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos 金鑰管理
	TCP	749	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos V 變更及設定密碼（ RPCSEC_GSS ）
AutoSupport	HTTPS	443..	節點管理 LIF	support.netapp.com	支援（預設為HTTPS）AutoSupport
	HTTP	80	節點管理 LIF	support.netapp.com	僅當傳輸傳輸傳輸傳輸傳輸傳輸協定從HTTPS變更為HTTP時、AutoSupport
	TCP	3128	節點管理 LIF	連接器	如果無法使用傳出的網際網路連線、請透過Connector上的Proxy伺服器傳送AutoSupport 功能介紹訊息

服務	傳輸協定	連接埠	來源	目的地	目的
備份至 S3	TCP	5010.	叢集間 LIF	備份端點或還原端點	備份與還原備份至 S3 功能的作業
叢集	所有流量	所有流量	一個節點上的所有 LIF	其他節點上的所有 LIF	叢集間通訊（ Cloud Volumes ONTAP 僅限不含 HA ）
	TCP	3000	節點管理 LIF	HA 中介	ZAPI 呼叫（ Cloud Volumes ONTAP 僅限 RHA ）
	ICMP	1.	節點管理 LIF	HA 中介	Keepive Alive （ Cloud Volumes ONTAP 僅限 HHA ）
組態備份	HTTP	80	節點管理 LIF	\http ：//Wese/occm/offboxconfig <connector-IP-address>	將組態備份傳送至Connector。 "深入瞭解組態備份檔案"。
DHCP	UDP	68	節點管理 LIF	DHCP	第一次設定的 DHCP 用戶端
DHCPS	UDP	67	節點管理 LIF	DHCP	DHCP 伺服器
DNS	UDP	53.	節點管理 LIF 與資料 LIF （ NFS 、 CIFS ）	DNS	DNS
NDMP	TCP	18600 – 18699	節點管理 LIF	目的地伺服器	NDMP 複本
SMTP	TCP	25	節點管理 LIF	郵件伺服器	可以使用 SMTP 警示 AutoSupport 來執行功能
SNMP	TCP	161.	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	UDP	161.	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	TCP	162%	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	UDP	162%	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
SnapMirror	TCP	11104.	叢集間 LIF	叢集間 LIF ONTAP	管理 SnapMirror 的叢集間通訊工作階段
	TCP	11105.	叢集間 LIF	叢集間 LIF ONTAP	SnapMirror 資料傳輸
系統記錄	UDP	514	節點管理 LIF	系統記錄伺服器	系統記錄轉送訊息

HA 協調器外部安全群組的規則

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

傳入規則

HA中介器的預先定義安全性群組包括下列傳入規則。

傳輸協定	連接埠	來源	目的
TCP	3000	連接器的CIDR	從 Connector 進行 RESTful API 存取

傳出規則

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

基本傳出規則

HA 中介器的預先定義安全性群組包括下列傳出規則。

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

進階傳出規則

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

傳輸協定	連接埠	目的地	目的
HTTP	80	AWS EC2執行個體上Connector的IP位址	下載中介程式升級
HTTPS	443..	ec2.amazonaws.com	協助進行儲存容錯移轉
UDP	53.	ec2.amazonaws.com	協助進行儲存容錯移轉

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

HA組態內部安全性群組的規則

針對某個不穩定的HA組態、預先定義的內部安全群組Cloud Volumes ONTAP 包括下列規則。此安全性群組可在HA節點之間以及中介器與節點之間進行通訊。

BlueXP一律會建立此安全性群組。您沒有使用自己的選項。

傳入規則

預先定義的安全性群組包含下列傳入規則。

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

傳出規則

預先定義的安全性群組包括下列傳出規則。

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

Connector 規則

"檢視Connector的安全群組規則"

設定 **AWS KMS**

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

步驟

1. 確認存在作用中的客戶主金鑰（ CMK ）。

   CMK 可以是 AWS 託管的 CMK 、也可以是客戶託管的 CMK 。它可以與BlueXP和Cloud Volumes ONTAP Sfor相同的AWS帳戶、也可以位於不同的AWS帳戶中。

   "AWS 文件：客戶主要金鑰（ CMK ）"

2. 新增IAM角色、將權限提供給BlueXP做為_key使用者_、以修改每個CMK的金鑰原則。

   將IAM角色新增為主要使用者後、即可讓BlueXP擁有權限、可搭配Cloud Volumes ONTAP 使用CMK搭配使用。

   "AWS 文件：編輯金鑰"

3. 如果 CMK 位於不同的 AWS 帳戶、請完成下列步驟：

   a. 從 CMK 所在的帳戶移至 KMS 主控台。

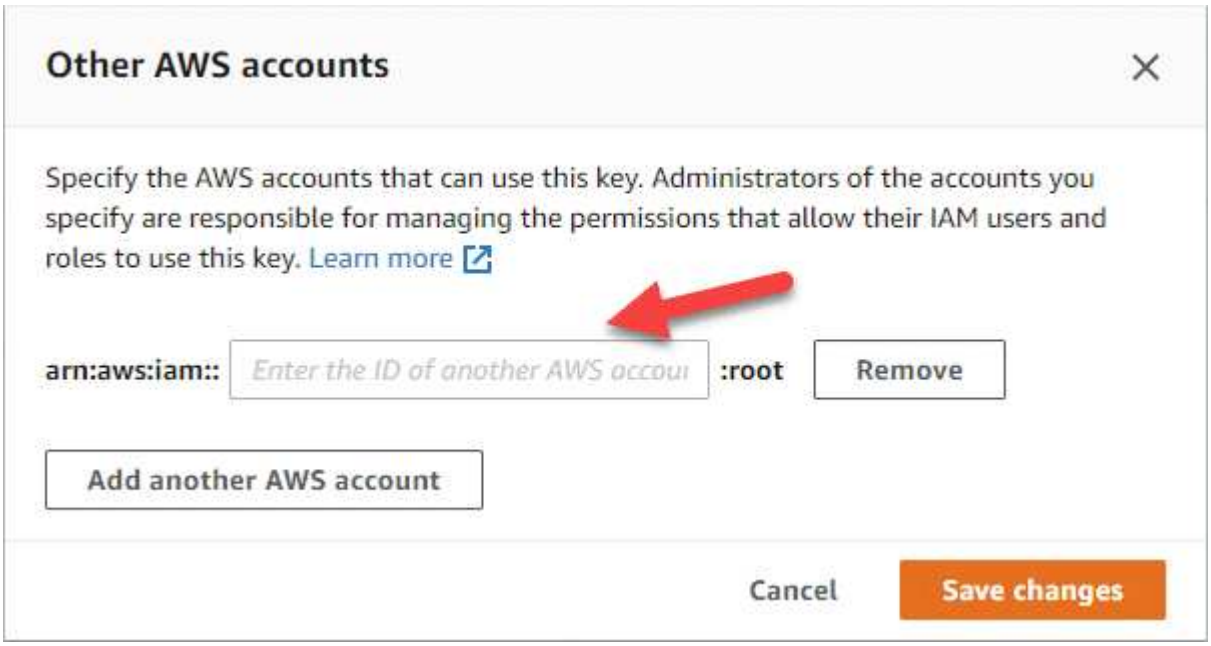
   b. 選取金鑰。

   c. 在「 * 一般組態 * 」窗格中、複製金鑰的 ARN 。

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

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

      在大多數情況下、這是BlueXP所在的帳戶。如果AWS中未安裝BlueXP、您將會為其提供AWS存取金鑰給BlueXP。



e. 現在請切換至AWS帳戶、該帳戶可為BlueXP提供權限、並開啟IAM主控台。

f. 建立包含下列權限的 IAM 原則。

g. 將原則附加至IAM角色或IAM使用者、以提供對BlueXP的權限。

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

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

+
如需此程序的其他詳細資料、請參閱 "AWS文件：允許其他帳戶的使用者使用KMS金鑰"。

4. 如果您使用由客戶管理的CMK、請將Cloud Volumes ONTAP 「IAM角色」新增為「_key使用者」、以修改CMK的金鑰原則。

   如果您在Cloud Volumes ONTAP 支援資料分層的情況下、想要加密儲存在S3儲存區中的資料、就必須執行

此步驟。

您需要在部署Cloud Volumes ONTAP 完時執行此步驟_after、因為IAM角色是在您建立工作環境時建立的。（當然、您可以選擇使用現有Cloud Volumes ONTAP 的ISIAM角色、因此可以在之前執行此步驟。）

"AWS 文件：編輯金鑰"

設定IAM角色Cloud Volumes ONTAP 以供使用

具有所需權限的IAM角色必須附加至每Cloud Volumes ONTAP 個節點。HA中介者也是如此。讓BlueXP為您建立IAM角色最簡單、但您可以使用自己的角色。

此工作為選用工作。當您建立Cloud Volumes ONTAP 一個運作環境時、預設選項是讓BlueXP為您建立IAM角色。如果貴企業的安全性原則要求您自行建立IAM角色、請遵循下列步驟。

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

步驟

1. 前往AWS IAM主控台。
2. 建立包含下列權限的IAM原則：

    - 適用於節點的基礎原則Cloud Volumes ONTAP

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）地區

```
{
    "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"
    }]
}
```

最高機密區域

```
{
    "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"
    }]
}
```

- 適用於節點的備份原則Cloud Volumes ONTAP

  如果您計畫在 Cloud Volumes ONTAP 系統上使用 BlueXP 備份與還原、節點的 IAM 角色必須包含以下所示的第二個原則。

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）地區

```
{
    "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"
        }
    ]
}
```

最高機密區域

```
{
    "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 中介

```
{
    "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IAM角色、並將您建立的原則附加至角色。

結果

現在您可以在建立新Cloud Volumes ONTAP 的運作環境時選擇IAM角色。

更多資訊

- "AWS文件：建立IAM原則"
- "AWS文件：建立IAM角色"

在Cloud Volumes ONTAP AWS中設定適用於此功能的授權

決定Cloud Volumes ONTAP 要搭配使用哪種授權選項之後、您必須先執行幾個步驟、才能在建立新的工作環境時選擇授權選項。

Freemium

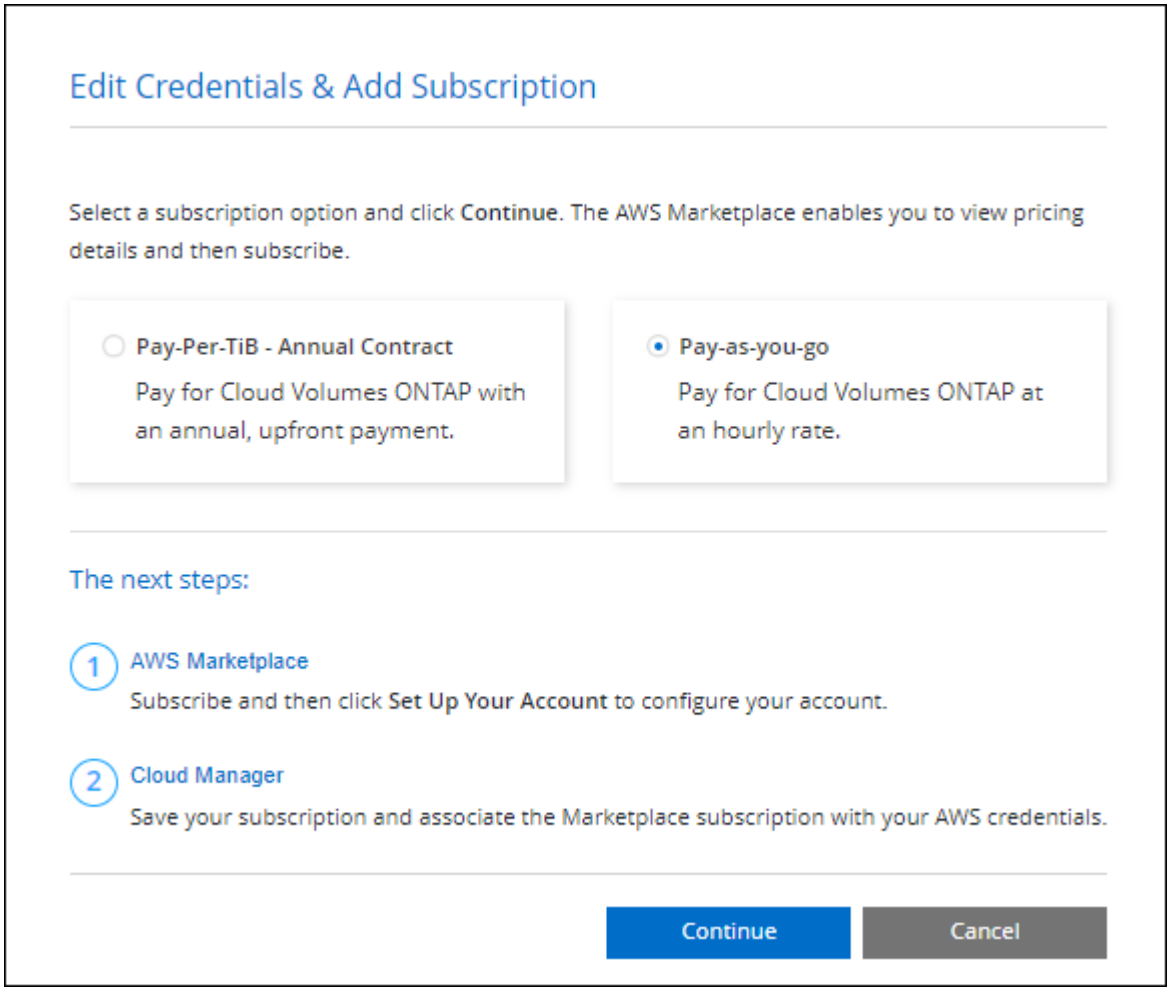
選擇Freemium產品、即可免費使用Cloud Volumes ONTAP 多達500 GiB的配置容量。 "深入瞭解Freemium產品"。

步驟

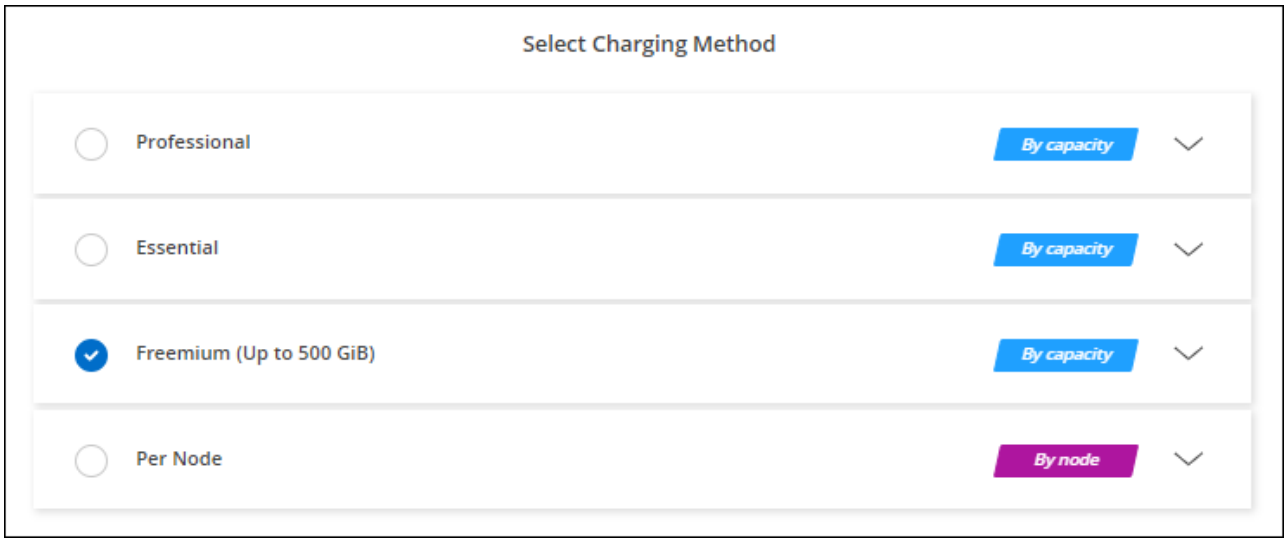
1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。
    a. 在*詳細資料與認證*頁面上、按一下*編輯認證>新增訂閱*、然後依照提示訂閱AWS Marketplace中的隨

用隨付方案。

除非您超過500 GiB的已配置容量、系統會自動轉換為、否則不會透過市場訂閱付費 "Essentials套件"。



a. 返回BluetXP之後、當您到達「充電方法」頁面時、請選取* Freemium *。



"請參閱逐步指示、以在Cloud Volumes ONTAP AWS中啟動功能"。

容量型授權

容量型授權可讓您針對Cloud Volumes ONTAP 容量的每個TiB付費。容量型授權的形式為_package_：Essentials套件或Professional套件。

Essentials和Professional套件可搭配下列消費模式使用：

- 向NetApp購買的授權（BYOL）
- 從AWS Marketplace訂閱時數小時隨付（PAYGO）
- AWS Marketplace的年度合約

"深入瞭解容量型授權"。

下列各節將說明如何開始使用這些消費模式。

BYOL

事先向NetApp購買授權（BYOL）、即可在Cloud Volumes ONTAP 任何雲端供應商部署支援系統。

步驟

1. "請聯絡NetApp銷售人員以取得授權"
2. "將NetApp 支援網站 您的不更新帳戶新增至藍圖XP"

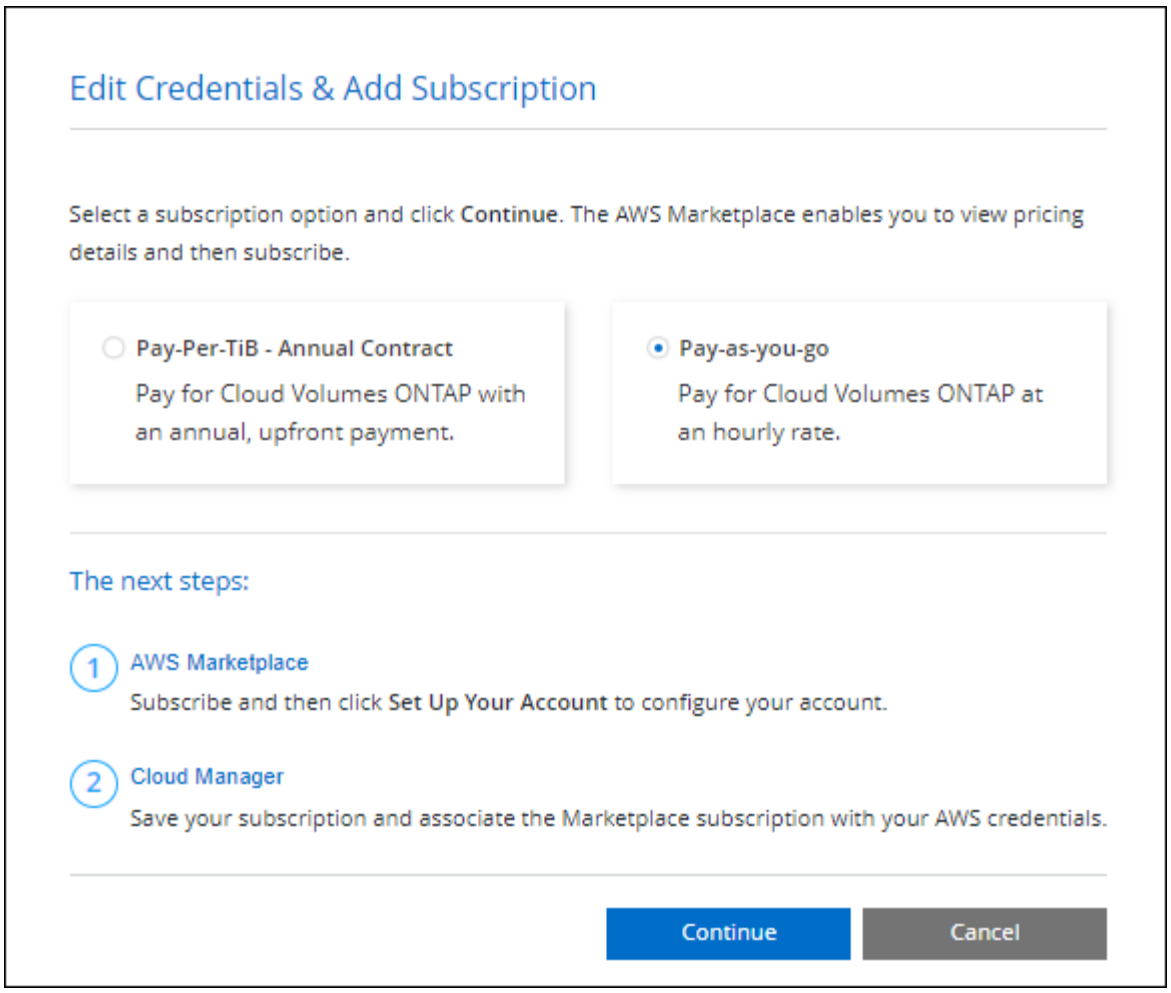
   BlueXP會自動查詢NetApp的授權服務、以取得NetApp 支援網站 與您的還原帳戶相關之授權的詳細資料。如果沒有錯誤、 BlueXP 會自動將授權新增至數位錢包。

   您必須先從 BlueXP 數位錢包取得授權、才能搭配 Cloud Volumes ONTAP 使用。如有需要、您可以 "手動將授權新增至 BlueXP 數位錢包"。

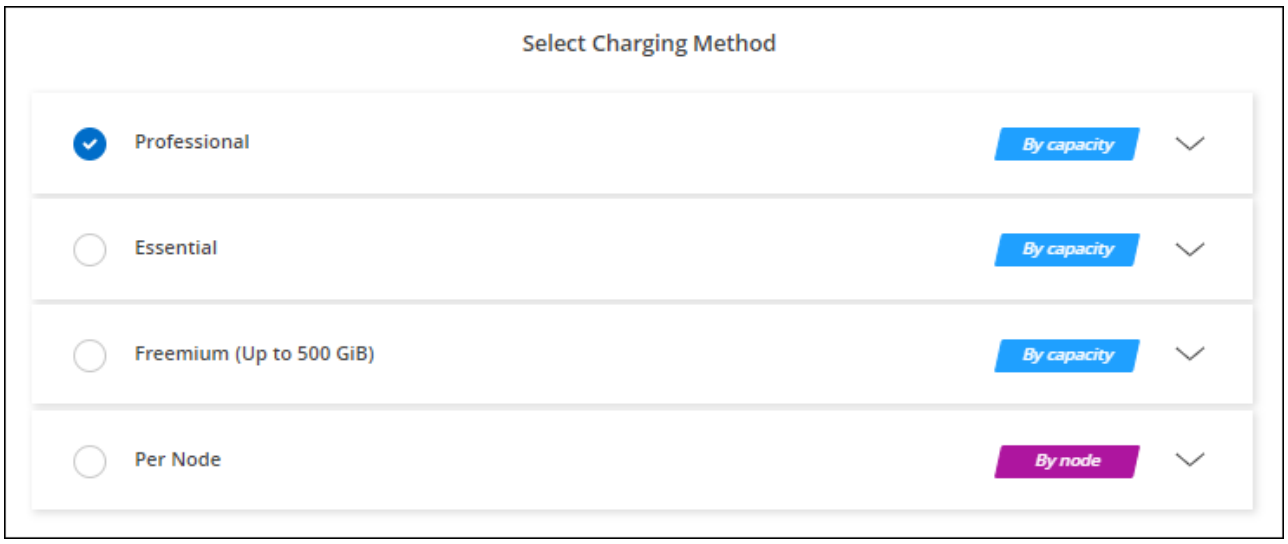
3. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。

   a. 在*詳細資料與認證*頁面上、按一下*編輯認證>新增訂閱*、然後依照提示訂閱AWS Marketplace中的隨用隨付方案。

      您向NetApp購買的授權一律會先收取費用、但如果您超過授權容量或授權到期、則會從市場的每小時費率中收取費用。



a. 返回BlueXP之後、當您到達「充電方法」頁面時、請選取容量型套件。



"請參閱逐步指示、以在Cloud Volumes ONTAP AWS中啟動功能"。

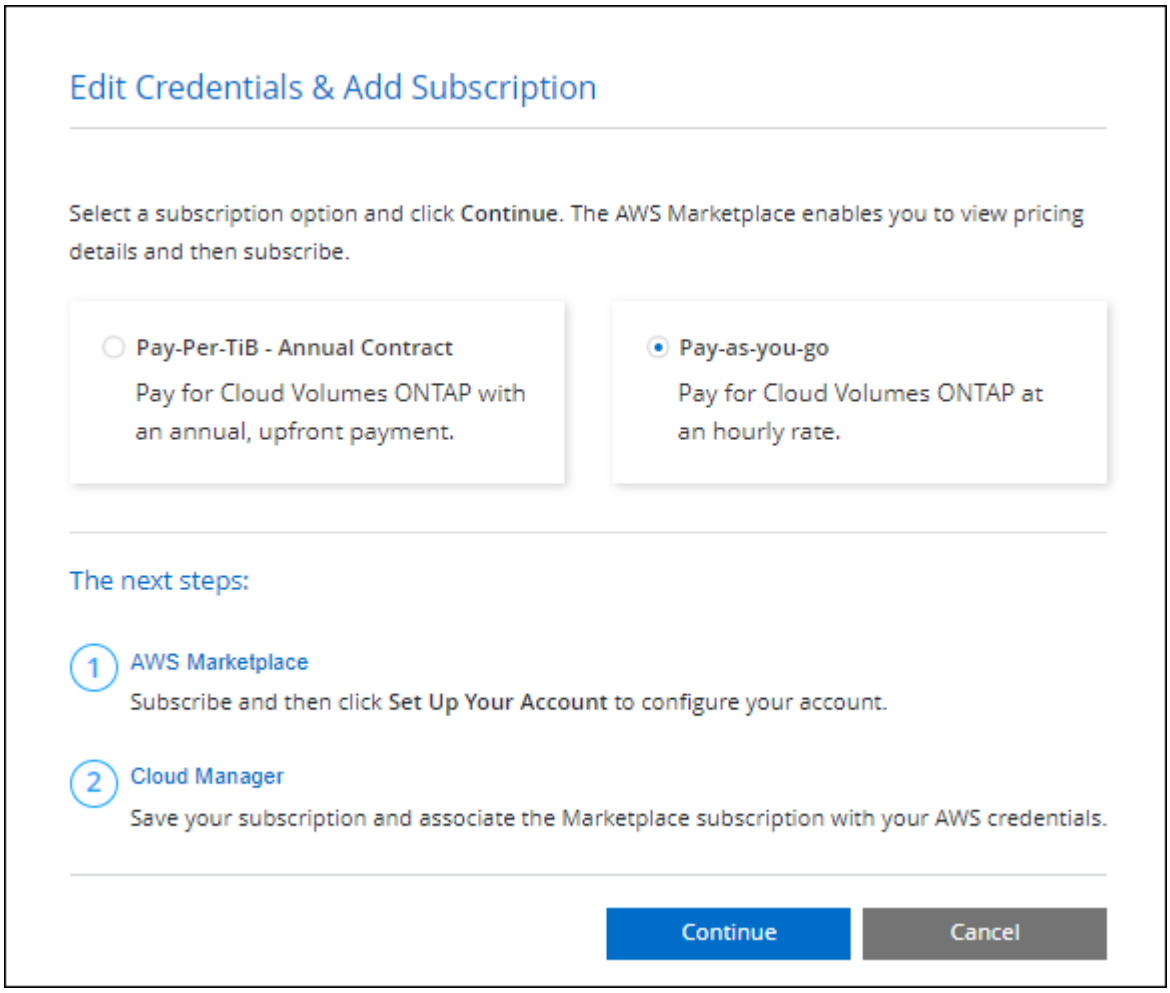
PAYGO訂閱

從雲端供應商的市場訂閱優惠、每小時支付一次。

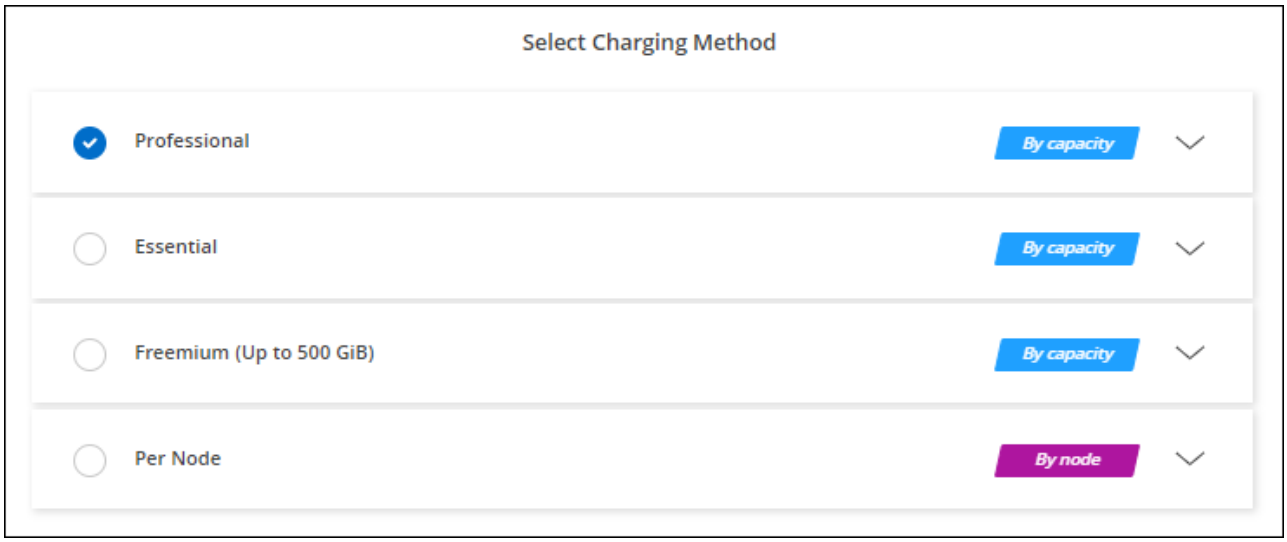
當您建立Cloud Volumes ONTAP 一個運作環境時、BlueXP會提示您訂閱AWS Marketplace提供的合約。該訂閱之後會與工作環境建立關聯、以便進行充電。您可以在其他工作環境中使用相同的訂閱。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。
   a. 在*詳細資料與認證*頁面上、按一下*編輯認證>新增訂閱*、然後依照提示訂閱AWS Marketplace中的隨用隨付方案。



   b. 返回BlueXP之後、當您到達「充電方法」頁面時、請選取容量型套件。



"請參閱逐步指示、以在Cloud Volumes ONTAP AWS中啟動功能"。

您可以從「設定」>「認證」頁面管理與AWS帳戶相關的AWS Marketplace訂閱。 "瞭解如何管理AWS帳戶和訂閱"

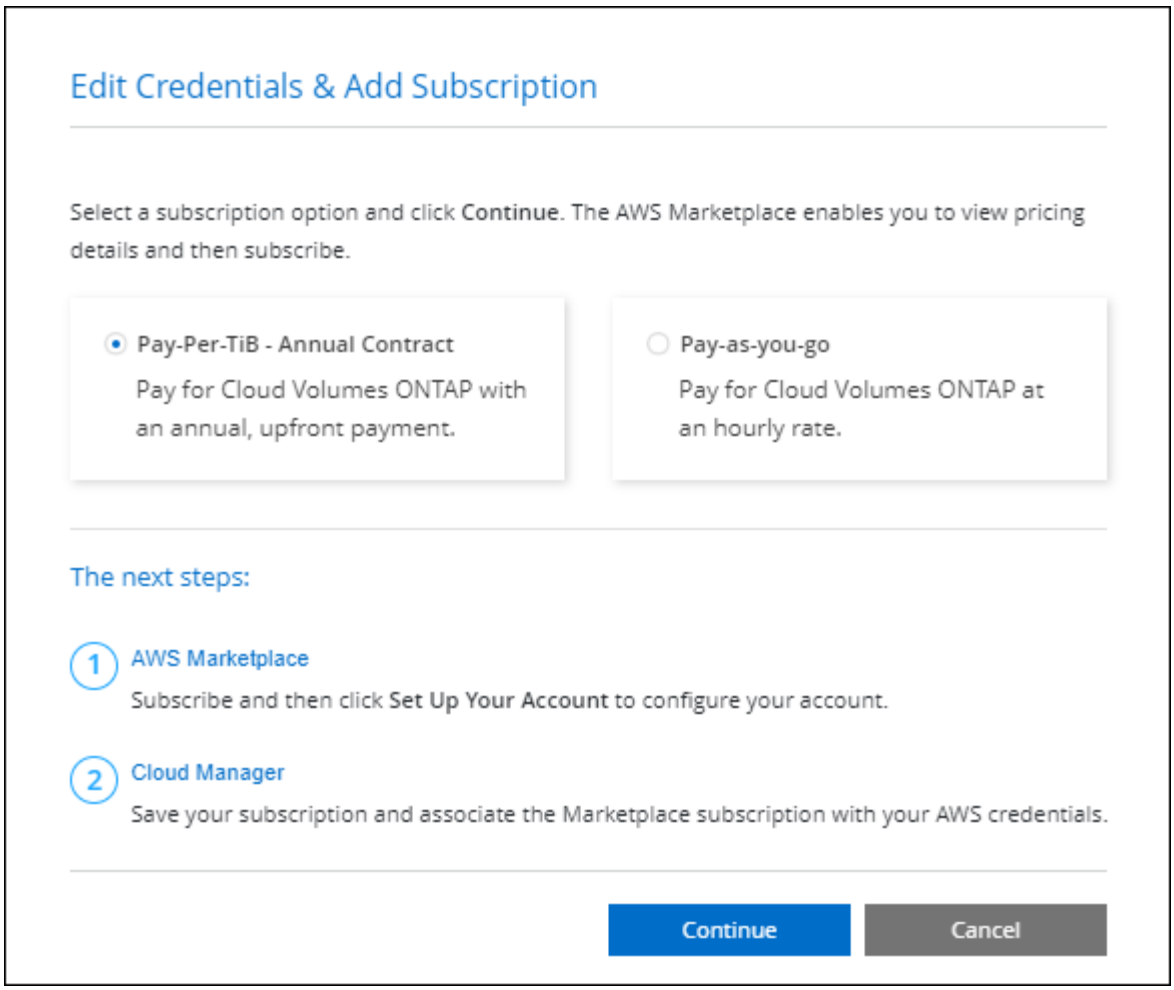
年度合約

每年向雲端供應商的市場購買一年一度的合約即可付款。

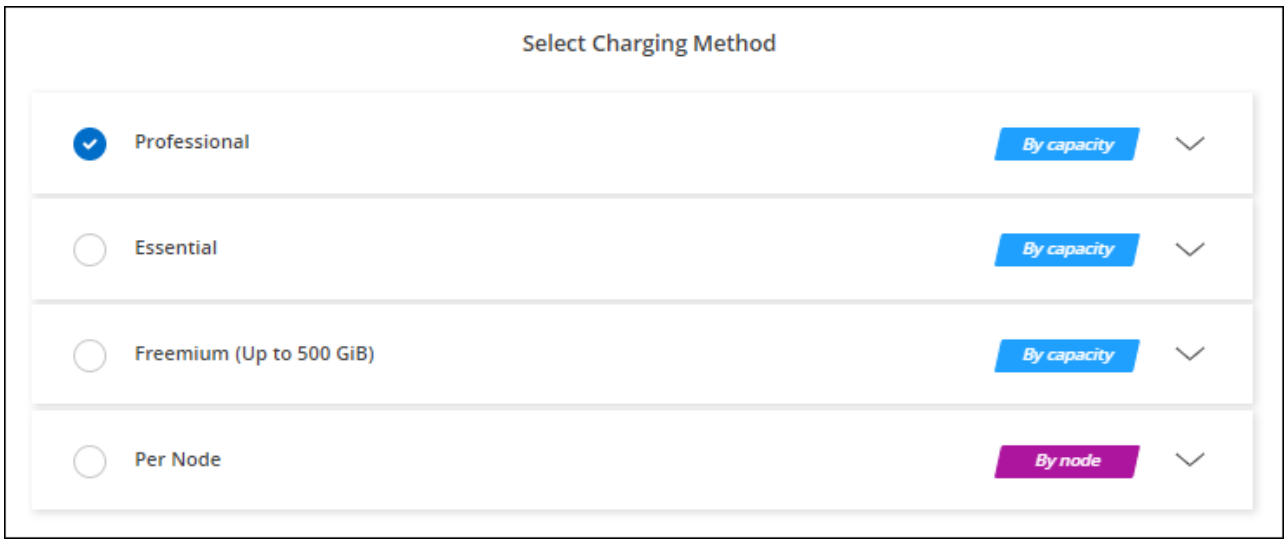
如同每小時訂閱、BlueXP會提示您訂閱AWS Marketplace提供的年度合約。

步驟

1. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。
   a. 在*詳細資料與認證*頁面上、按一下*編輯認證>新增訂閱*、然後依照提示在AWS Marketplace訂閱年度合約。



b. 返回BlueXP之後、當您到達「充電方法」頁面時、請選取容量型套件。



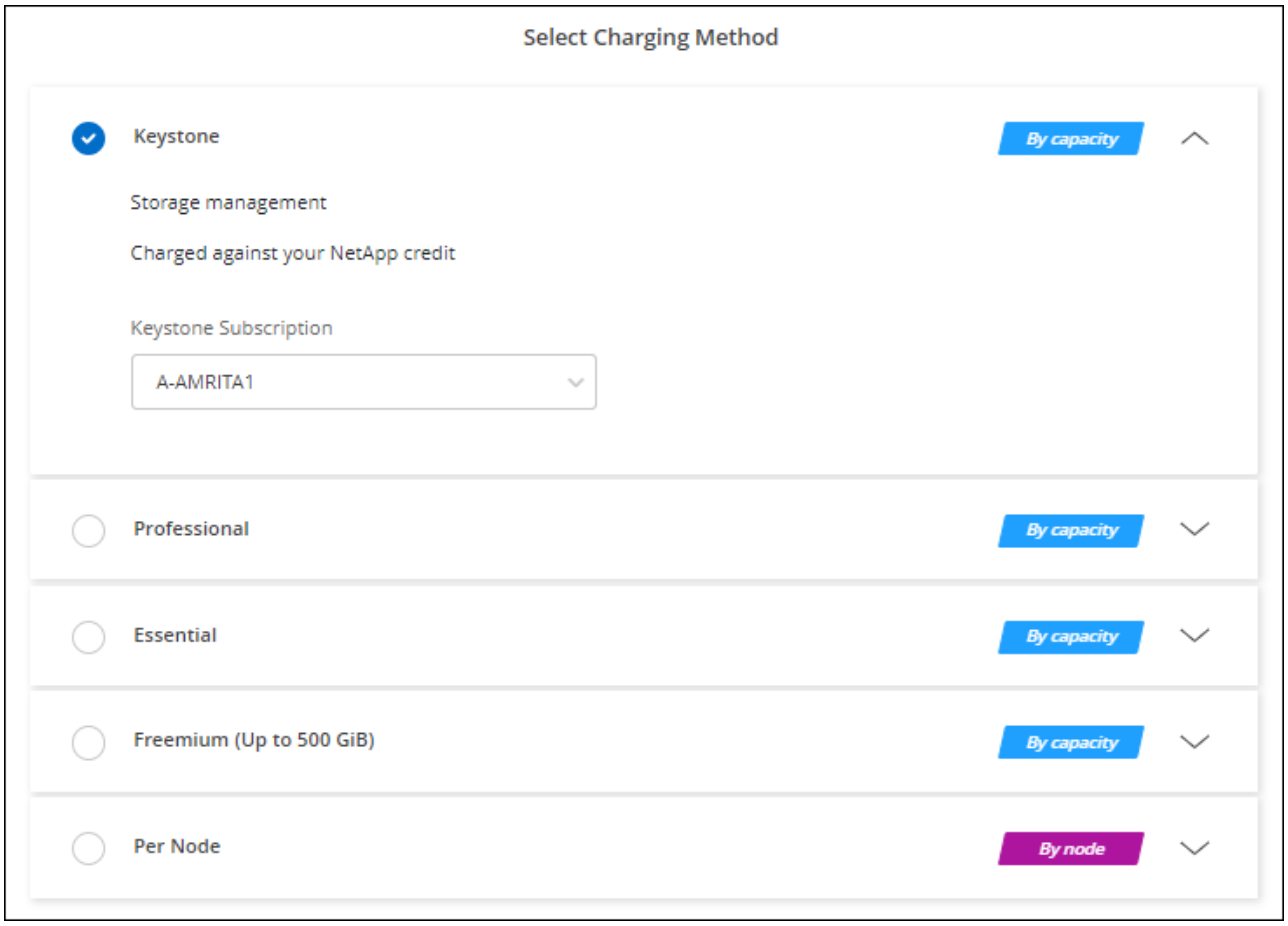
"請參閱逐步指示、以在Cloud Volumes ONTAP AWS中啟動功能"。

Keystone訂閱

Keystone 訂閱是一項隨成長付費訂閱服務。 "深入瞭解 NetApp Keystone 訂閱"。

步驟

1. 如果您尚未訂閱、 "請聯絡NetApp"
2. mailto ： ng-keystone-success@netapp.com [聯絡 NetApp] 以使用一或多個 Keystone 訂閱來授權您的 BlueXP 使用者帳戶。
3. NetApp授權您的帳戶之後、 "連結您的訂閱內容以供Cloud Volumes ONTAP 搭配使用"。
4. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。
   a. 當系統提示您選擇充電方法時、請選取 Keystone Subscription 充電方法。



"請參閱逐步指示、以在Cloud Volumes ONTAP AWS中啟動功能"。

在 Cloud Volumes ONTAP AWS 中啟動

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

開始之前

您需要下列項目才能建立工作環境。

- 已啟動並執行的連接器。
  - 您應該擁有 "與工作區相關的連接器"。
  - "您應該隨時準備好讓 Connector 保持運作"。

- 瞭解您要使用的組態。

  您應該已做好準備、選擇組態、並從系統管理員取得 AWS 網路資訊。如需詳細資訊、請參閱 "規劃 Cloud Volumes ONTAP 您的需求組態"。

- 瞭解設定Cloud Volumes ONTAP 驗證功能所需的條件。

  "瞭解如何設定授權"。

- 適用於CIFS組態的DNS與Active Directory。

  如需詳細資訊、請參閱 "AWS 的網路需求 Cloud Volumes ONTAP"。

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

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

關於這項工作

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

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. [[訂閱]在「畫版」頁面上、按一下「新增工作環境」、然後依照提示進行。
3. * 選擇位置 * ：選擇 * Amazon Web Services* 和 * Cloud Volumes ONTAP 《單一節點 * 》。
4. 如果出現提示、 "建立連接器"。
5. * 詳細資料與認證 * ：選擇性地變更 AWS 認證資料與訂閱、輸入工作環境名稱、視需要新增標記、然後輸入密碼。

   本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

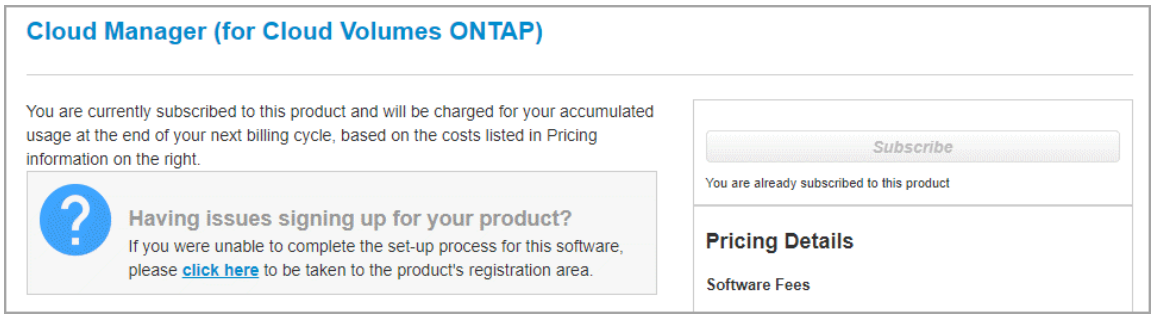
欄位	說明
工作環境名稱	BlueXP使用工作環境名稱來命名Cloud Volumes ONTAP 整個系統、以及Amazon EC2執行個體。如果您選取該選項、它也會使用名稱做為預先定義安全性群組的前置詞。
新增標記	AWS 標籤是 AWS 資源的中繼資料。BlueXP會將標記新增Cloud Volumes ONTAP 至該執行個體、以及與該執行個體相關聯的每個AWS資源。建立工作環境時、您最多可以從使用者介面新增四個標記、然後在建立之後新增更多標記。請注意、在建立工作環境時、 API 不會限制您使用四個標記。如需標記的相關資訊、請參閱 "AWS 文件：標記 Amazon EC2 資源"。
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

欄位	說明
編輯認證資料	選擇與您要部署此系統之帳戶相關的AWS認證資料。您也可以將AWS Marketplace訂閱與此Cloud Volumes ONTAP 款作業系統建立關聯。 按一下*新增訂閱*、將所選認證資料與新的AWS Marketplace訂閱建立關聯。訂閱可以是一年一度的合約、或Cloud Volumes ONTAP 是以每小時的費率支付。 "瞭解如何將額外的AWS認證資料新增至BlueXP"。

下列影片說明如何將隨用隨付服務市場訂閱與 AWS 認證資料建立關聯：

從 AWS Marketplace 訂閱 BlueXP

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



6. * 服務 * ：啟用或停用 Cloud Volumes ONTAP 您不想搭配使用的個別服務。
   - "深入瞭解 BlueXP 分類"
   - "深入瞭解 BlueXP 備份與還原"

   如果您想要使用 WORM 和資料分層功能、您必須停用 BlueXP 備份與還原、並部署 9.8 版或更新版本的 Cloud Volumes ONTAP 工作環境。

7. 位置與連線：輸入您在中記錄的網路資訊 "AWS工作表"。

   下表說明您可能需要指導的欄位：

欄位	說明
VPC	如果您有 AWS Outpost 、 Cloud Volumes ONTAP 您可以選擇 Outpost VPC 、在該 Outpost 中部署單一節點的一套系統。體驗與 AWS 中的任何其他 VPC 相同。

欄位	說明
產生的安全性群組	如果讓BlueXP為您產生安全性群組、您必須選擇允許流量的方式： • 如果您選擇*僅限VPC*、則傳入流量的來源為所選VPC的子網路範圍、以及連接器所在VPC的子網路範圍。這是建議的選項。 • 如果您選擇*所有VPC*、則傳入流量的來源為0.00.0.0/0 IP範圍。
使用現有的安全性群組	如果您使用現有的防火牆原則、請確定其中包含必要的規則。 "深入瞭Cloud Volumes ONTAP 解適用於此功能的防火牆規則"。

8. * 資料加密 * ：不選擇資料加密或 AWS 管理的加密。

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

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

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

   "深入瞭解支援的加密技術"。

9. 充電方法與**NSS**帳戶：指定您要搭配此系統使用的收費選項、然後指定NetApp支援網站帳戶。
   - "深入瞭Cloud Volumes ONTAP 解適用於此功能的授權選項"。
   - "瞭解如何設定授權"。
10. 《》（僅限AWS Marketplace年度合約）：請檢閱預設組態、然後按一下*「Continue」（繼續）或按一下「Change Configuration」（變更組態）*以選取您自己的組態。Cloud Volumes ONTAP

    如果您保留預設組態、則只需指定一個Volume、然後檢閱並核准組態。

11. 預先設定的套件：選取其中一個套件以快速啟動Cloud Volumes ONTAP 功能、或按一下*變更組態*以選取您自己的組態。

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

12. * IAM角色*：最好保留預設選項、讓BlueXP為您建立角色。

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

13. 授權：視Cloud Volumes ONTAP 需要變更此版本、並選取執行個體類型和執行個體租賃。

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

14. 基礎儲存資源：選擇磁碟類型、設定基礎儲存設備、然後選擇是否要啟用資料分層。

    請注意下列事項：

    - 磁碟類型適用於初始磁碟區（和Aggregate）。您可以為後續磁碟區（和Aggregate）選擇不同的磁碟類

型。

- 如果您選擇GP3或IO1磁碟、則BlueXP會使用AWS中的彈性磁碟區功能、視需要自動增加基礎儲存磁碟容量。您可以根據儲存需求來選擇初始容量、Cloud Volumes ONTAP 並在部署完畢後加以修改。 "深入瞭解AWS對彈性磁碟區的支援"。
- 如果您選擇gp2或ST1磁碟、則可以針對初始Aggregate中的所有磁碟、以及使用Simple Provisioning選項時、BlueXP所建立的任何其他Aggregate、選取磁碟大小。您可以使用進階配置選項、建立使用不同磁碟大小的集合體。
- 您可以在建立或編輯磁碟區時、選擇特定的磁碟區分層原則。
- 如果停用資料分層、您可以在後續的 Aggregate 上啟用。

  "瞭解資料分層的運作方式"。

15. *寫入速度與WORM *：

    a. 如果需要、請選擇*正常*或*高速*寫入速度。

       "深入瞭解寫入速度"。

    b. 視需要啟動一次寫入、多次讀取（WORM）儲存設備。

       如果啟用Cloud Volumes ONTAP 資料分層功能、無法啟用WORM 9.7版及更低版本。啟用WORM和分層後、將Cloud Volumes ONTAP 會封鎖還原或降級至物件9.8。

    "深入瞭解 WORM 儲存設備"。

    a. 如果您啟動WORM儲存設備、請選取保留期間。

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

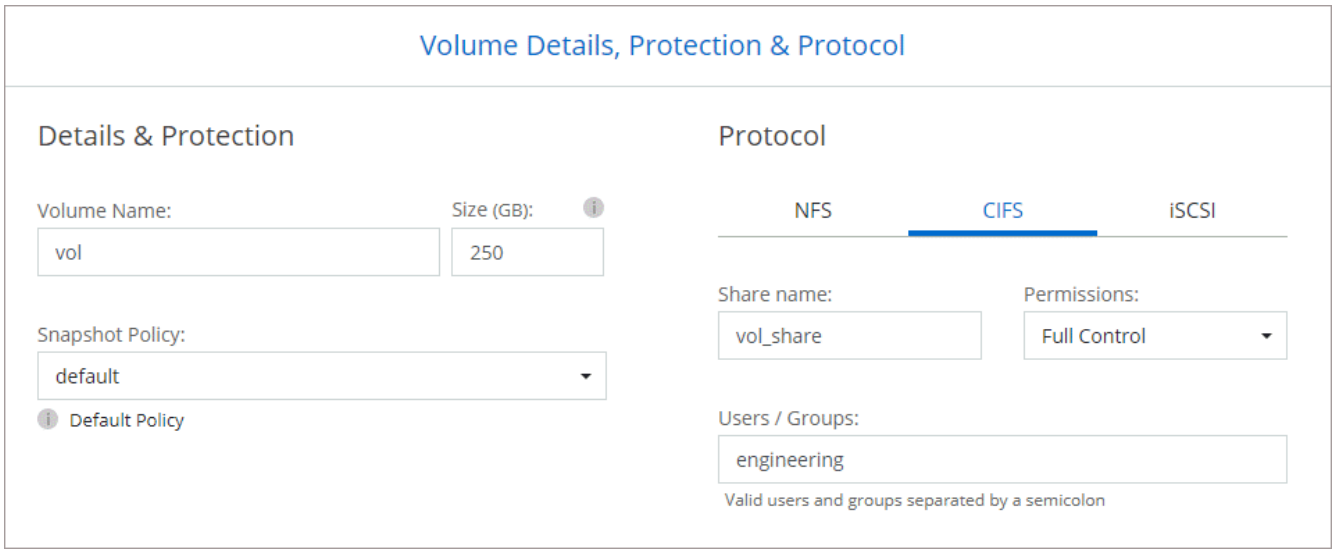
    "瞭解支援的用戶端傳輸協定和版本"。

    本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

欄位	說明
尺寸	您可以輸入的最大大小、主要取決於您是否啟用精簡配置、這可讓您建立比目前可用實體儲存容量更大的磁碟區。
存取控制（僅適用於 NFS ）	匯出原則會定義子網路中可存取磁碟區的用戶端。根據預設、BlueXP會輸入一個值、以供存取子網路中的所有執行個體。
權限與使用者 / 群組（僅限 CIFS ）	這些欄位可讓您控制使用者和群組（也稱為存取控制清單或 ACL ）的共用存取層級。您可以指定本機或網域 Windows 使用者或群組、或 UNIX 使用者或群組。如果您指定網域 Windows 使用者名稱、則必須使用網域 \ 使用者名稱格式來包含使用者的網域。
Snapshot 原則	Snapshot 複製原則會指定自動建立的 NetApp Snapshot 複本的頻率和數量。NetApp Snapshot 複本是一種不影響效能的時間點檔案系統映像、需要最少的儲存容量。您可以選擇預設原則或無。您可以針對暫時性資料選擇「無」：例如、 Microsoft SQL Server 的 Tempdb 。
進階選項（僅適用於 NFS ）	為磁碟區選取 NFS 版本： NFSv3 或 NFSv3 。

欄位	說明
啟動器群組和 IQN （僅適用於 iSCSI ）	iSCSI 儲存目標稱為 LUN （邏輯單元）、以標準區塊裝置的形式呈現給主機。啟動器群組是 iSCSI 主機節點名稱的表格、可控制哪些啟動器可存取哪些 LUN 。iSCSI 目標可透過標準乙太網路介面卡（ NIC ）、 TCP 卸載引擎（ TOE ）卡（含軟體啟動器）、整合式網路介面卡（ CNA ）或專用主機匯流排介面卡（ HBA ）連線至網路、並由 iSCSI 合格名稱（ IQN ）識別。建立iSCSI磁碟區時、BlueXP會自動為您建立LUN。我們只要在每個磁碟區建立一個 LUN 、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 "使用 IQN 從主機連線至 LUN"。

下圖顯示 CIFS 傳輸協定的「 Volume 」（磁碟區）頁面：



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

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

欄位	說明
NTP 伺服器	選擇 * 使用 Active Directory 網域 * 來使用 Active Directory DNS 設定 NTP 伺服器。如果您需要使用不同的位址來設定 NTP 伺服器、則應該使用 API 。請參閱 "藍圖XP自動化文件" 以取得詳細資料。 請注意、您只能在建立CIFS伺服器時設定NTP伺服器。您建立CIFS伺服器之後、就無法進行設定。

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

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

19. * 審查與核准 * ：檢閱並確認您的選擇。
    a. 檢閱組態的詳細資料。
    b. 按一下*更多資訊*以檢閱有關支援和BlueXP將購買的AWS資源的詳細資料。
    c. 選取「 * 我瞭解 … * 」核取方塊。
    d. 按一下「 * 執行 * 」 。

結果

BlueXP會啟動Cloud Volumes ONTAP 這個執行個體。您可以追蹤時間表的進度。

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

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

完成後

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

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

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

如果您想要在Cloud Volumes ONTAP AWS中啟動一個「叢集HA配對」、您需要在BlueXP中建立HA工作環境。

限制

目前 AWS out貼 文不支援 HA 配對。

關於這項工作

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

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。

2. 在「畫版」頁面上、按一下「 * 新增工作環境 * 」、然後依照提示進行。
3. 選擇位置：選擇* Amazon Web Services*和* Cloud Volumes ONTAP 《*》HA *。

   有些 AWS 本機區域可供使用。

   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路、才能使用 AWS 本機區域。請遵循 * 選擇加入 AWS 本機區域 * 、並 * 將 Amazon VPC 延伸至中的本機區域 * 步驟 "AWS 教學課程「開始使用 AWS 本機區域部署低延遲應用程式」"。

   如果您執行的是 Connector 3.9.36 版或更低版本、則必須在 AWS EC2 主控台中、將下列權限新增至 AWS Connector 角色： DescribeAvailabilityZones 。
4. * 詳細資料與認證 * ：選擇性地變更 AWS 認證資料與訂閱、輸入工作環境名稱、視需要新增標記、然後輸入密碼。

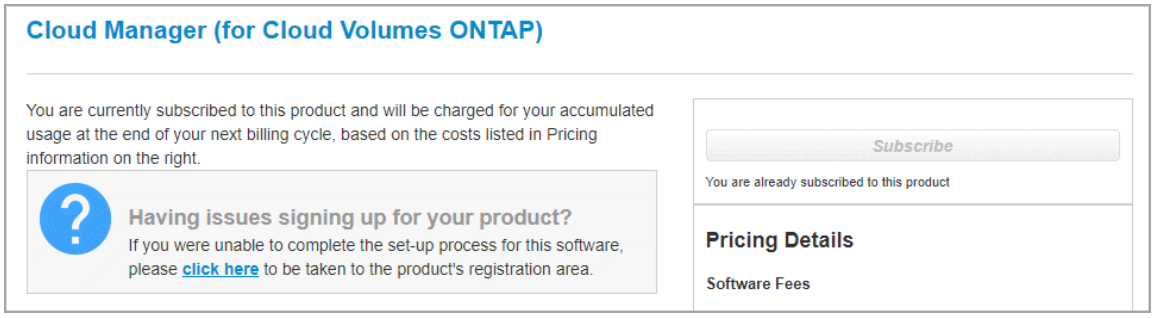
   本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

欄位	說明
工作環境名稱	BlueXP使用工作環境名稱來命名Cloud Volumes ONTAP 整個系統、以及Amazon EC2執行個體。如果您選取該選項、它也會使用名稱做為預先定義安全性群組的前置詞。
新增標記	AWS 標籤是 AWS 資源的中繼資料。BlueXP會將標記新增Cloud Volumes ONTAP 至該執行個體、以及與該執行個體相關聯的每個AWS資源。建立工作環境時、您最多可以從使用者介面新增四個標記、然後在建立之後新增更多標記。請注意、在建立工作環境時、 API 不會限制您使用四個標記。如需標記的相關資訊、請參閱 "AWS 文件：標記 Amazon EC2 資源"。
使用者名稱和密碼	這些是Cloud Volumes ONTAP 適用於整個叢集管理員帳戶的認證資料。您可以使用這些認證資料、 Cloud Volumes ONTAP 透過 System Manager 或其 CLI 連線至功能驗證。保留預設的_admin_使用者名稱、或將其變更為自訂使用者名稱。
編輯認證資料	選擇 AWS 認證資料和市場訂閱、以搭配此 Cloud Volumes ONTAP 款功能系統使用。 按一下*新增訂閱*、將所選認證資料與新的AWS Marketplace訂閱建立關聯。訂閱可以是一年一度的合約、或Cloud Volumes ONTAP 是以每小時的費率支付。 如果直接向NetApp（BYOL）購買授權、則無需訂閱AWS。 "瞭解如何將額外的AWS認證資料新增至BlueXP"。

   下列影片說明如何將隨用隨付服務市場訂閱與 AWS 認證資料建立關聯：

   從 AWS Marketplace 訂閱 BlueXP

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



5. * 服務 * ：讓服務保持啟用或停用您不想搭配 Cloud Volumes ONTAP 此作業系統使用的個別服務。
   - "深入瞭解 BlueXP 分類"
   - "深入瞭解 BlueXP 備份與還原"

   如果您想要使用 WORM 和資料分層功能、您必須停用 BlueXP 備份與還原、並部署 9.8 版或更新版本的 Cloud Volumes ONTAP 工作環境。

6. * HA 部署模式 * ：選擇 HA 組態。

   如需部署模型的總覽、請參閱 "適用於 AWS 的 HA Cloud Volumes ONTAP"。

7. 位置與連線（單一AZ）或*地區與VPC*（多個AZ）：輸入您在AWS工作表中記錄的網路資訊。

   下表說明您可能需要指導的欄位：

欄位	說明
產生的安全性群組	如果讓BlueXP為您產生安全性群組、您必須選擇允許流量的方式： • 如果您選擇*僅限VPC*、則傳入流量的來源為所選VPC的子網路範圍、以及連接器所在VPC的子網路範圍。這是建議的選項。 • 如果您選擇*所有VPC*、則傳入流量的來源為0.00.0.0/0 IP範圍。
使用現有的安全性群組	如果您使用現有的防火牆原則、請確定其中包含必要的規則。 "深入瞭Cloud Volumes ONTAP 解適用於此功能的防火牆規則"。

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

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

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

    如果您有多個路由表、請務必選取正確的路由表。否則、部分用戶端可能無法存取 Cloud Volumes ONTAP

此功能配對。如需路由表的詳細資訊、請參閱 "AWS 文件：路由表"。

11. * 資料加密 * ：不選擇資料加密或 AWS 管理的加密。

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

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

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

    "深入瞭解支援的加密技術"。

12. 充電方法與**NSS**帳戶：指定您要搭配此系統使用的收費選項、然後指定NetApp支援網站帳戶。
    - "深入瞭Cloud Volumes ONTAP 解適用於此功能的授權選項"。
    - "瞭解如何設定授權"。

13. 《》（僅限AWS Marketplace年度合約）：請檢閱預設組態、然後按一下*「Continue」（繼續）或按一下「Change Configuration」（變更組態）*以選取您自己的組態。Cloud Volumes ONTAP

    如果您保留預設組態、則只需指定一個Volume、然後檢閱並核准組態。

14. 預先設定的套件（僅限每小時或BYOL）：選取其中一個套件以快速啟動Cloud Volumes ONTAP 功能、或按一下*變更組態*以選取您自己的組態。

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

15. * IAM角色*：最好保留預設選項、讓BlueXP為您建立角色。

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

16. 授權：視Cloud Volumes ONTAP 需要變更此版本、並選取執行個體類型和執行個體租賃。

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

17. 基礎儲存資源：選擇磁碟類型、設定基礎儲存設備、然後選擇是否要啟用資料分層。

    請注意下列事項：

    - 磁碟類型適用於初始磁碟區（和Aggregate）。您可以為後續磁碟區（和Aggregate）選擇不同的磁碟類型。
    - 如果您選擇GP3或IO1磁碟、則BlueXP會使用AWS中的彈性磁碟區功能、視需要自動增加基礎儲存磁碟容量。您可以根據儲存需求來選擇初始容量、Cloud Volumes ONTAP 並在部署完畢後加以修改。 "深入瞭解AWS對彈性磁碟區的支援"。
    - 如果您選擇gp2或ST1磁碟、則可以針對初始Aggregate中的所有磁碟、以及使用Simple Provisioning選項時、BlueXP所建立的任何其他Aggregate、選取磁碟大小。您可以使用進階配置選項、建立使用不同磁碟大小的集合體。
    - 您可以在建立或編輯磁碟區時、選擇特定的磁碟區分層原則。

◦ 如果停用資料分層、您可以在後續的 Aggregate 上啟用。

"瞭解資料分層的運作方式"。

18. *寫入速度與WORM *：

a. 如果需要、請選擇*正常*或*高速*寫入速度。

"深入瞭解寫入速度"。

b. 視需要啟動一次寫入、多次讀取（WORM）儲存設備。

如果啟用Cloud Volumes ONTAP 資料分層功能、無法啟用WORM 9.7版及更低版本。啟用WORM和分層後、將Cloud Volumes ONTAP 會封鎖還原或降級至物件9.8。

"深入瞭解 WORM 儲存設備"。

a. 如果您啟動WORM儲存設備、請選取保留期間。

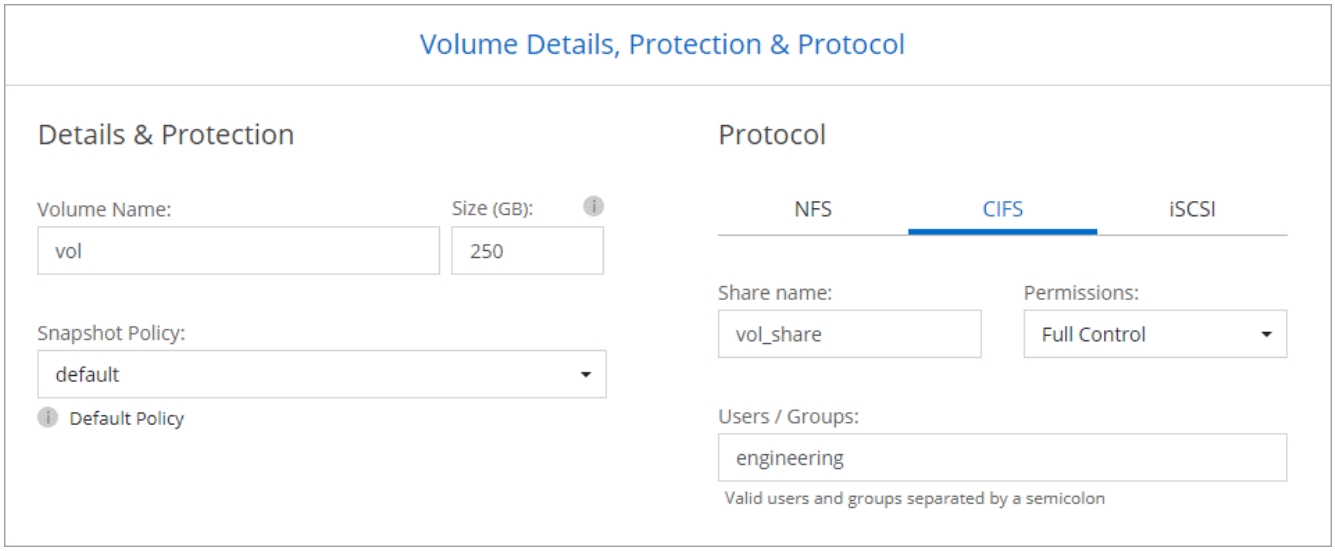
19. * 建立 Volume * ：輸入新磁碟區的詳細資料、或按一下 * 跳過 * 。

"瞭解支援的用戶端傳輸協定和版本"。

本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

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

下圖顯示 CIFS 傳輸協定的「 Volume 」（磁碟區）頁面：



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

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

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

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

22. * 審查與核准 * ：檢閱並確認您的選擇。

    a. 檢閱組態的詳細資料。

    b. 按一下*更多資訊*以檢閱有關支援和BlueXP將購買的AWS資源的詳細資料。

c. 選取「 * 我瞭解 … * 」核取方塊。

d. 按一下「 * 執行 * 」。

結果

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

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

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

完成後

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

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

在 **AWS Secret Cloud** 和 **Top Secret Cloud** 地區部署 **Cloud Volumes ONTAP**

與標準 AWS 區域類似、您可以在中使用 BlueXP "AWS Secret Cloud" 和 "AWS Top Secret Cloud" 部署 Cloud Volumes ONTAP 、為您的雲端儲存設備提供企業級功能。AWS Secret Cloud 和 Top Secret Cloud 是美國特有的封閉區域智慧社群：本頁的指示僅適用於 AWS Secret Cloud 和 Top Secret Cloud 地區使用者。

開始之前

開始之前、請先檢閱 AWS Secret Cloud 和 Top Secret Cloud 中支援的版本、並瞭解 BlueXP 中的私有模式。

- 檢閱 AWS Secret Cloud 和 Top Secret Cloud 中支援的下列版本：
  - Cloud Volumes ONTAP 9.12.1 P2
  - Connector 3.9.32 版

    Connector是在Cloud Volumes ONTAP AWS中部署和管理功能所需的軟體。您將從安裝在Connector執行個體上的軟體登入BlueXP。AWS Secret Cloud 和 Top Secret Cloud 不支援 BlueXP 的 SaaS 網站。
- 瞭解私有模式

  在 AWS Secret Cloud 和 Top Secret Cloud 中、 BlueXP 以 _private 模式運作。在私有模式中、無法連線至 BlueXP SaaS 層。使用者可從 Connector 提供的網路型主控台、而非從 SaaS 層、在本機存取 BlueXP 。

  若要深入瞭解私有模式的運作方式、請參閱 "BlueXP 私有部署模式"。

步驟 **1** ：設定您的網路

設定AWS網路、Cloud Volumes ONTAP 使其能夠正常運作。

步驟

1. 選擇要在其中啟動Connector執行個體和Cloud Volumes ONTAP 例項的VPC和子網路。

2. 確保您的 VPC 和子網路支援連接器與 Cloud Volumes ONTAP 支援之間的連線。
3. 設定 S3 服務的 VPC 端點。

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

步驟 **2** ：設定權限

設定 IAM 原則和角色、為 Connector 和 Cloud Volumes ONTAP 提供在 AWS Secret Cloud 或 Top Secret Cloud 中執行動作所需的權限。

您需要IAM原則和IAM角色來執行下列各項：

- Connector執行個體
- 執行個體Cloud Volumes ONTAP
- 對於 HA 配對、 Cloud Volumes ONTAP HA 中介執行個體（如果您想要部署 HA 配對）

步驟

1. 移至AWS IAM主控台、然後按一下* Policies *。
2. 建立Connector執行個體的原則。

   您可以建立這些原則來支援 AWS 環境中的 S3 儲存區。稍後建立貯體時、請確定貯體名稱以開頭 `fabric-pool-`。這項要求同時適用於 AWS Secret Cloud 和 Top Secret Cloud 地區。

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/*"
            ]
        }
    ]
}
```

最高機密區域

```
{
    "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: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. 建立Cloud Volumes ONTAP 一套適用於此功能的原則。

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"
    }]
}
```

最高機密區域

```
{
    "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 配對、如果您打算部署 Cloud Volumes ONTAP HA 配對、請為 HA 協調器建立原則。

```
{
    "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. 使用角色類型Amazon EC2建立IAM角色、並附加您在先前步驟中建立的原則。

   建立角色：

   與原則類似、您應該有一個用於連接器的 IAM 角色、另一個用於 Cloud Volumes ONTAP 節點。
   對於 HA 配對：與原則類似、您應該有一個用於連接器的 IAM 角色、一個用於 Cloud Volumes ONTAP 節點、另一個用於 HA 協調器（如果您想要部署 HA 配對）。

   選取角色：

   啟動Connector執行個體時、您必須選取Connector IAM角色。從 BlueXP 建立 Cloud Volumes ONTAP 工作環境時、您可以為 Cloud Volumes ONTAP 選取 IAM 角色。
   對於 HA 配對、您可以在從 BlueXP 建立 Cloud Volumes ONTAP 工作環境時、為 Cloud Volumes ONTAP 和 HA 協調器選取 IAM 角色。

步驟 3 ：設定 AWS KMS

如果您想搭配 Cloud Volumes ONTAP 使用 Amazon 加密、請確保 AWS 金鑰管理服務（ KMS ）符合要求。

步驟

1. 請確定您的帳戶或其他AWS帳戶中存在使用中的客戶主金鑰（CMK）。

   CMK 可以是 AWS 託管的 CMK 、也可以是客戶託管的 CMK 。

2. 如果CMK位於AWS帳戶中、而該帳戶與您打算部署Cloud Volumes ONTAP 的帳戶不同、則您需要取得該金鑰的ARN。

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

3. 將Connector執行個體的IAM角色新增至CMK的主要使用者清單。

如此一來、BlueXP就有權將CMK搭配Cloud Volumes ONTAP 使用。

步驟 4 ：安裝 Connector 並設定 BlueXP

在開始使用 BlueXP 在 AWS 中部署 Cloud Volumes ONTAP 之前、您必須先安裝並設定 BlueXP Connector 。Connector讓BlueXP能夠管理公有雲環境中的資源和程序（包括Cloud Volumes ONTAP 整個過程）。

步驟

1. 取得由憑證授權單位（CA）簽署的根憑證（採用隱私權增強型郵件（PEF）Base - 64編碼的X・509格式）。請參閱貴組織的原則與程序、以取得該憑證。

   對於 AWS Secret Cloud 地區、您應該上傳 `NSS Root CA 2` 憑證、以及 Top Secret Cloud 的 `Amazon Root CA 4` 憑證：請務必僅上傳這些憑證、而非整個鏈結。憑證鏈結的檔案很大、上傳可能會失敗。如果您有其他憑證、您可以在稍後上傳、如下一步所述。

   您必須在設定程序期間上傳憑證。透過HTTPS傳送要求至AWS時、BlueXP會使用信任的憑證。

2. 啟動Connector執行個體：
   a. 前往適用於BlueXP的AWS Intelligence Community Marketplace頁面。
   b. 在「自訂啟動」索引標籤上、選擇從EC2主控台啟動執行個體的選項。
   c. 依照提示設定執行個體。

      設定執行個體時請注意下列事項：

      - 建議使用T3.xLarge。
      - 您必須選擇設定權限時所建立的 IAM 角色。
      - 您應該保留預設的儲存選項。
      - Connector所需的連線方法如下：SSH、HTTP和HTTPS。
3. 從連線至Connector執行個體的主機設定BlueXP：
   a. 開啟網頁瀏覽器並輸入 https://ipaddress 其中 ipaddress 是您安裝 Connector 的 Linux 主機的 IP 位址。
   b. 指定用於連線至AWS服務的Proxy伺服器。
   c. 上傳您在步驟1中取得的憑證。
   d. 選取 * 設定新的 BlueXP* 、然後依照提示設定系統。
      - 系統詳細資料：輸入Connector的名稱及您的公司名稱。
      - 建立管理使用者：建立系統的管理使用者。

        此使用者帳戶在本機系統上執行。無法透過BlueXP連線至驗證0服務。

      - * 審查 * ：檢閱詳細資料、接受授權合約、然後選取 * 設定 * 。
   e. 若要完成CA簽署憑證的安裝、請從EC2主控台重新啟動Connector執行個體。
4. 重新啟動Connector之後、請使用您在設定精靈中建立的系統管理員使用者帳戶登入。

步驟 **5** ：（選用）安裝私有模式憑證

此步驟對於 AWS Secret Cloud 和 Top Secret Cloud 地區為選用步驟、只有在您有其他憑證（除了您在前一步驟中安裝的根憑證）時才需要。

步驟

1. 列出現有的已安裝憑證。
   a. 若要收集 occm Container 泊塢視窗 ID （識別名稱為「 DS-occm-1 」）、請執行下列命令：

   ```
   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 儲存區密碼 " 環境變數收集密碼、請執行下列命令：

   ```
   env
   ```

   d. 若要列出信任存放區中所有已安裝的憑證、請執行下列命令、並使用上一步收集的密碼：

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

2. 新增憑證。
   a. 若要收集 occm Container 泊塢視窗 id （識別名稱為「 DS-occm-1 」）、請執行下列命令：

   ```
   docker ps
   ```

   b. 若要進入 occm 容器、請執行下列命令：

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

   將新的憑證檔案儲存在內。

   c. 若要從 "trust 儲存區密碼 " 環境變數收集密碼、請執行下列命令：

   ```
   env
   ```

   d. 若要將憑證新增至信任存放區、請執行下列命令、並使用上一步的密碼：

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

e. 若要檢查是否已安裝憑證、請執行下列命令：

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

f. 若要結束 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** ：新增授權至 **BlueXP** 數位錢包

如果您向 NetApp 購買授權、則需要將其新增至 BlueXP 數位錢包、以便在建立新的 Cloud Volumes ONTAP 系統時選取授權。數位錢包會將這些授權識別為未指派。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》*索引標籤上、從下拉式清單中選取「*節點型授權」。
3. 按一下*未指派*。
4. 按一下「新增未指派的授權」。
5. 輸入授權的序號或上傳授權檔案。
6. 如果您還沒有使用許可檔案、則需要從 netapp.com 手動上傳使用許可檔案。
   a. 前往 "NetApp 授權檔案產生器" 並使用您的 NetApp 支援網站認證資料登入。
   b. 輸入您的密碼、選擇產品、輸入序號、確認您已閱讀並接受隱私權政策、然後按一下 * 提交 * 。
   c. 選擇您要透過電子郵件或直接下載來接收 serialNumber.NLF Json 檔案。
7. 按一下「 * 新增授權 * 」。

結果

BlueXP 將授權新增至數位錢包。授權將被識別為未指派、直到您將其與新Cloud Volumes ONTAP 的一套系統關聯為止。之後、授權便會移至數位錢包中的 BYOL 標籤。

步驟 **7** ：從 **BlueXP** 啟動 **Cloud Volumes ONTAP**

您可以在 BlueXP 中建立新的工作環境、在 AWS Secret Cloud 和 Top Secret Cloud 中啟動 Cloud Volumes ONTAP 執行個體。

開始之前

對於 HA 配對、必須有金鑰配對、才能啟用金鑰型 SSH 驗證給 HA 中介者。

步驟

1. 在「工作環境」頁面上、按一下「新增工作環境」。
2. 在 * 建立 * 下、選取 Cloud Volumes ONTAP 。

   對於 HA ：在 * 建立 * 下、選取 Cloud Volumes ONTAP 或 Cloud Volumes ONTAP HA 。
3. 完成精靈中的步驟以啟動Cloud Volumes ONTAP 整套系統。

> 在精靈中進行選擇時、請勿在 * 服務 * 下選取 * 資料感知與法規遵循 * 和 * 備份至雲端 * 。在 * 預先設定的封裝 * 下、選取 * 僅變更組態 * 、並確定您尚未選取任何其他選項。AWS Secret Cloud 和 Top Secret Cloud 地區不支援預先設定的套件、如果選取、您的部署將會失敗。

在多個可用性區域中部署 **Cloud Volumes ONTAP HA** 的注意事項

當您完成 HA 配對精靈時、請注意下列事項。

- 當您在多個可用性區域（ AZs ）中部署 Cloud Volumes ONTAP HA 時、應該設定傳輸閘道。請參閱 "設定 AWS 傳輸閘道"。
- 部署組態如下、因為在發佈時、 AWS Top Secret Cloud 只有兩個 AZs 可用：
  - 節點1：可用度區域A
  - 節點2：可用度區域B
  - 中介：可用度區域A或B

在單一和 **HA** 節點上部署 **Cloud Volumes ONTAP** 的注意事項

完成精靈時請注意下列事項：

- 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 一些規則、這些規則是讓整個公司順利運作所需的。如果您需要使用自己的安全性、請參閱下方的安全性群組一節。
- 您必須選擇在準備AWS環境時所建立的IAM角色。
- 基礎AWS磁碟類型適用於初始Cloud Volumes ONTAP 的流通量。

  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有關。

  您應該選擇能提供所需持續效能的磁碟大小。如需EBS效能的詳細資訊、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、可以使用「進階配置」選項來建立使用特定大小磁碟的集合體。

結果

BlueXP會啟動Cloud Volumes ONTAP 這個執行個體。您可以追蹤時間表的進度。

步驟 **8** ：安裝資料分層的安全性憑證

您必須手動安裝安全性憑證、才能在 AWS Secret Cloud 和 Top Secret Cloud 區域中進行資料分層。

開始之前

1. 建立 S3 儲存區。

   請確定貯體名稱以開頭 `fabric-pool-`. 例如 `fabric-pool-testbucket`。

2. 保留您安裝的根憑證 `step 4` 方便。

步驟

1. 從您安裝的根憑證複製文字 `step 4`。
2. 使用 CLI 安全連線至 Cloud Volumes ONTAP 系統。
3. 安裝根憑證。您可能需要按下 `ENTER` 金鑰多次：

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

4. 出現提示時、輸入完整複製的文字、包括和寄件者 `----- BEGIN CERTIFICATE -----` 至 `----- END CERTIFICATE -----`。
5. 保留 CA 簽署數位憑證的複本、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 區域設定物件存放區： `set -privilege advanced -confirmations off`
8. 執行此命令以設定物件存放區。

   所有 Amazon 資源名稱（ ARN ）都應以後綴為後綴 `-iso-b`、例如 `arn:aws-iso-b`。例如、如果某個資源需要區域的 ARN 、對於 Top Secret Cloud 、請使用命名慣例 AS `us-iso-b` 適用於 `-server` 旗標。若為 AWS Secret Cloud 、請使用 `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. 確認物件存放區已成功建立： `storage aggregate object-store show -instance`
10. 將物件存放區附加至 Aggregate 。每個新的集合體都應該重複此步驟： `storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>`

開始使用Microsoft Azure

Azure中的功能快速入門Cloud Volumes ONTAP

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


建立連接器

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

請注意、如果您想要在Cloud Volumes ONTAP 無法存取網際網路的子網路中部署支援、則必須手動安裝Connector、並存取在該Connector上執行的BlueXP使用者介面。 "瞭解如何在無法存取網際網路的位置手動安裝Connector"


規劃您的組態

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


設定您的網路

1. 確保您的 Vnet 和子網路可支援連接器與 Cloud Volumes ONTAP 支援的連接功能。
2. 啟用從目標VPC for NetApp AutoSupport 的傳出網際網路存取功能。

   如果您在Cloud Volumes ONTAP 無法存取網際網路的位置部署支援、則不需要執行此步驟。

"深入瞭解網路需求"。


使用**BlueXP**啟動**Cloud Volumes ONTAP**

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

相關連結

- "從BlueXP建立連接器"
- "從 Azure Marketplace 建立 Connector"
- "在 Linux 主機上安裝 Connector 軟體"
- "BlueXP具備權限的功能"

在Cloud Volumes ONTAP Azure中規劃您的不一樣組態

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

選擇**Cloud Volumes ONTAP** 一個不含功能的授權

有多種授權選項可供Cloud Volumes ONTAP 選擇。每個選項都能讓您選擇符合需求的消費模式。

- "深入瞭Cloud Volumes ONTAP 解適用於此功能的授權選項"
- "瞭解如何設定授權"

選擇支援的地區

大多數Microsoft Azure地區均支援此功能。Cloud Volumes ONTAP "檢視支援區域的完整清單"。

選擇支援的**VM**類型

根據您選擇的授權類型、支援多種 VM 類型。 Cloud Volumes ONTAP

"Azure支援Cloud Volumes ONTAP 的支援功能組態"

瞭解儲存限制

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

"Azure的Cloud Volumes ONTAP 儲存限制"

在**Azure**中調整系統規模

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

虛擬機器類型

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

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

Azure磁碟類型搭配單一節點系統

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

單一節點系統可使用三種 Azure 託管磁碟：

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

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

Azure磁碟類型搭配HA配對

HA系統使用優質的SSD共享託管磁碟、兩者都能以較高的成本為I/O密集型工作負載提供高效能。在9.12.1版本之前建立的HA部署會使用優質網頁。

Azure 磁碟大小

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

集合體中的所有磁碟大小必須相同。

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

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

標準儲存設備的磁碟大小沒有效能差異。您應該根據所需的容量來選擇磁碟大小。

請參閱 Azure 、瞭解每個磁碟大小的 IOPS 與處理量：

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

檢視預設系統磁碟

除了儲存使用者資料之外、BlueXP也購買雲端儲存設備來儲存Cloud Volumes ONTAP 作業系統資料（開機資料、根資料、核心資料和NVRAM）。為了規劃目的、在部署Cloud Volumes ONTAP 完更新之前、您可能需要先檢閱這些詳細資料。

"在Cloud Volumes ONTAP Azure中檢視系統資料的預設磁碟"。

連接器也需要系統磁碟。 "檢視Connector預設組態的詳細資料"。

收集網路資訊

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

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

選擇寫入速度

BlueXP可讓您選擇Cloud Volumes ONTAP 適合的寫入速度設定。在您選擇寫入速度之前、您應該先瞭解一般與高設定之間的差異、以及使用高速寫入速度時的風險與建議。 "深入瞭解寫入速度"。

選擇**Volume**使用設定檔

包含多項儲存效率功能、可減少您所需的總儲存容量。 ONTAP在BlueXP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。您應該深入瞭解這些功能、以協助您決定要使用的設定檔。

NetApp 儲存效率功能提供下列效益：

資源隨需配置

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

重複資料刪除

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

壓縮

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

Azure 的網路需求 Cloud Volumes ONTAP

設定您的 Azure 網路、 Cloud Volumes ONTAP 使其能夠正常運作。

需求 **Cloud Volumes ONTAP**

Azure 必須符合下列網路需求。

傳出網際網路存取

支援NetApp功能的支援節點需要外傳網際網路存取功能、此功能可主動監控系統健全狀況、並將訊息傳送給NetApp技術支援部門。Cloud Volumes ONTAP AutoSupport

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

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

如果傳出的網際網路連線無法傳送AutoSupport 功能性訊息、則BlueXP會自動將Cloud Volumes ONTAP 您的功能性更新系統設定為使用Connector做為Proxy伺服器。唯一的需求是確保連接器的安全性群組允許連接埠3128上的傳入連線。部署Connector之後、您需要開啟此連接埠。

如果您定義了Cloud Volumes ONTAP 嚴格的傳出規則以供支援、那麼Cloud Volumes ONTAP 您也必須確保支援透過連接埠3128建立_Outbound _連線的安全性群組。

在您確認可以存取傳出網際網路之後、您可以測試AutoSupport 以確保能夠傳送訊息。如需相關指示、請參閱 "文件：設定檔ONTAP AutoSupport"。

如果BlueXP通知您AutoSupport 無法傳送資訊、 "疑難排解AutoSupport 您的VMware組態"。

IP位址

BlueXP會自動將所需數量的私有IP位址分配Cloud Volumes ONTAP 給Azure中的所有人。您必須確定網路有足夠的私有IP位址可用。

BlueXP分配Cloud Volumes ONTAP 給功能的生命量取決於您是部署單一節點系統或HA配對。LIF 是與實體連接埠相關聯的 IP 位址。諸如 VMware 的管理工具需要 SVM 管理 LIF SnapCenter 。

> iSCSI LIF可透過iSCSI傳輸協定提供用戶端存取、並供系統用於其他重要的網路工作流程。這些生命是必要的、不應刪除。

單一節點系統的**IP**位址

BlueXP會將5或6個IP位址分配給單一節點系統：

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

> iSCSI IP可透過iSCSI傳輸協定提供用戶端存取。系統也會將其用於其他重要的網路工作流程。此LIF為必填項目、不應刪除。

- SVM管理（選用-預設為未設定）

HA配對的**IP**位址

在部署期間、BlueXP會將IP位址分配給4個NIC（每個節點）。

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

網卡**0**

- 節點管理IP
- 叢集間IP
- iSCSI IP

> iSCSI IP可透過iSCSI傳輸協定提供用戶端存取。系統也會將其用於其他重要的網路工作流程。此LIF為必填項目、不應刪除。

網卡**1**

- 叢集網路IP

*網卡2 *

- 叢集互連IP（HA IC）
- NIC 3 *
- Pageblob NIC IP（磁碟存取）

NIC 3僅適用於使用網頁BLOB儲存設備的HA部署。

上述IP位址不會在容錯移轉事件上移轉。

此外、還設定4個前端IP（FIPS）在容錯移轉事件上進行移轉。這些前端IP位於負載平衡器中。

- 叢集管理IP
- 節點A資料IP（NFS/CIFS）
- 節點B資料IP（NFS/CIFS）
- SVM管理IP

安全連線至**Azure**服務

根據預設、BlueXP會啟用Azure Private Link、以便Cloud Volumes ONTAP 在支援鏈接的情況下連接到支援鏈接的畫面和Azure網頁BLOB儲存帳戶。

在大多數情況下、您無需做任何事、因為BlueXP會為您管理Azure Private Link。但如果您使用Azure私有DNS、則必須編輯組態檔。您也應該瞭解Azure中的Connector位置需求。

您也可以視業務需求而停用「私有連結」連線。如果您停用連結、則BlueXP會設定Cloud Volumes ONTAP 使用服務端點的功能。

"深入瞭解如何搭配Cloud Volumes ONTAP 使用Azure私有連結或服務端點搭配使用"。

連線至其他**ONTAP** 的系統

若要在Cloud Volumes ONTAP Azure中的某個系統與ONTAP 其他網路中的某些系統之間複寫資料、您必須在Azure vnet與其他網路（例如您的公司網路）之間建立VPN連線。

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

HA互連的連接埠

一個包含HA互連的「支援功能」配對、可讓每個節點持續檢查其合作夥伴是否正常運作、並鏡射另一個非揮發性記憶體的記錄資料。Cloud Volumes ONTAPHA互連使用TCP連接埠10006進行通訊。

依預設、HA互連生命體之間的通訊會開啟、而且此連接埠沒有安全性群組規則。但是、如果您在HA互連生命期之間建立防火牆、則必須確保TCP流量已開啟連接埠10006、如此HA配對才能正常運作。

Azure資源群組中只有一組**HA**配對

您必須使用_Dedicated資源群組來處理Cloud Volumes ONTAP 您在Azure中部署的每一組EHA。資源群組僅支援一個HA配對。

如果您嘗試在Cloud Volumes ONTAP Azure資源群組中部署第二個「鏈接HA配對」、則BlueXP會遇到連線問題。

安全性群組規則

BlueXP會建立Azure安全性群組、其中包含Cloud Volumes ONTAP 了順利運作所需的傳入和傳出規則。您可能想要參照連接埠進行測試、或是想要使用自己的安全性群組。

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

正在尋找Connector的相關資訊？ "檢視Connector的安全群組規則"

單一節點系統的傳入規則

當您建立工作環境並選擇預先定義的安全性群組時、可以選擇允許下列其中一項的流量：

- 僅限所選**vnet**：傳入流量的來源是vnet的子網路範圍、Cloud Volumes ONTAP 以及連接器所在vnet的子網路範圍。這是建議的選項。
- 所有**VNet**：傳入流量的來源為0.00.0.0/0 IP範圍。

優先順序和名稱	連接埠與傳輸協定	來源與目的地	說明
1000 inbound SSH	22 TCP	任意	SSH 存取叢集管理 LIF 的 IP 位址或節點管理 LIF
1001 inbound http	80 TCP	任意	使用叢集管理 LIF 的 IP 位址、以 HTTP 存取 System Manager Web 主控台
1002inbound （入站）_111_TCP	111 TCP	任意	遠端程序需要 NFS
1003 inbound _111_udp	111 udp	任意	遠端程序需要 NFS
1004 inbound （傳入）_139	139 TCP	任意	CIFS 的 NetBios 服務工作階段
1005inbound （傳入）_161-162 _tcp	161-162 TCP	任意	簡單的網路管理傳輸協定
1006 inbound （傳入）_161-162 _udp	161-162 udp	任意	簡單的網路管理傳輸協定
1007 inbound _443	443 TCP	任意	使用叢集管理LIF的IP位址、連線到Connector和HTTPS、存取System Manager Web主控台
1008 inbound _445	445 TCP	任意	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
1009 inbound _6335_tcp	635 TCP	任意	NFS 掛載
1010 inbound _6335_udp	635 udp	任意	NFS 掛載
1011 inbound （傳入）_749	749 TCP	任意	Kerberos

優先順序和名稱	連接埠與傳輸協定	來源與目的地	說明
1012 inbound _2049_tcp	2049 TCP	任意	NFS 伺服器精靈
1013 inbound _2049_udp	2049 udp	任意	NFS 伺服器精靈
1014 inbound （傳入）_3260	3260 TCP	任意	透過 iSCSI 資料 LIF 存取 iSCSI
1015 inbound _4045-4046_tcp	4045-4046 TCP	任意	NFS 鎖定精靈和網路狀態監控
1016 inbound _4045-4046_udp	4045-4046 udp	任意	NFS 鎖定精靈和網路狀態監控
1017 inbound _10000	10000 TCP	任意	使用 NDMP 備份
1018 inbound （傳入）_11104-11105	11104-11105 TCP	任意	SnapMirror 資料傳輸
3000 inbound 拒絕_all_tcp	任何連接埠 TCP	任意	封鎖所有其他 TCP 傳入流量
3001 inbound 拒絕_all_udp	任何連接埠 udp	任意	封鎖所有其他的 UDP 傳入流量
65000 AllowVnetInBound	任何連接埠任何傳輸協定	虛擬網路至虛擬網路	來自 vnet 的傳入流量
65001 AllowAzureLoad BalancerInBound	任何連接埠任何傳輸協定	將 AzureLoadBalancer 移至任何	Azure Standard 負載平衡器的資料流量
65500 DenyAllInBound	任何連接埠任何傳輸協定	任意	封鎖所有其他傳入流量

HA 系統的傳入規則

當您建立工作環境並選擇預先定義的安全性群組時、可以選擇允許下列其中一項的流量：

- 僅限所選**vnet**：傳入流量的來源是vnet的子網路範圍、Cloud Volumes ONTAP 以及連接器所在vnet的子網路範圍。這是建議的選項。
- 所有**VNet**：傳入流量的來源為0.00.0.0/0 IP範圍。

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

優先順序和名稱	連接埠與傳輸協定	來源與目的地	說明
100 inbound （傳入）_443	443 任何傳輸協定	任意	使用叢集管理LIF的IP位址、連線到Connector和HTTPS、存取System Manager Web主控台
101 inbound （傳入）_111_TCP	111 任何傳輸協定	任意	遠端程序需要 NFS
102 inbound _2049_tcp	2049 任何傳輸協定	任意	NFS 伺服器精靈
111 inbound （傳入）_ssh	22 任何傳輸協定	任意	SSH 存取叢集管理 LIF 的 IP 位址或節點管理 LIF

優先順序和名稱	連接埠與傳輸協定	來源與目的地	說明
121inbound （傳入） _53	53 任何傳輸協定	任意	DNS 與 CIFS
65000 AllowVnetInBound	任何連接埠任何傳輸協定	虛擬網路至虛擬網路	來自 vnet 的傳入流量
65001 AllowAzureLoad BalancerInBound	任何連接埠任何傳輸協定	將 AzureLoadBalancer 移至任何	Azure Standard 負載平衡器的資料流量
65500 DenyAllInBound	任何連接埠任何傳輸協定	任意	封鎖所有其他傳入流量

傳出規則

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

基本傳出規則

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

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

進階傳出規則

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

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

服務	連接埠	傳輸協定	來源	目的地	目的
Active Directory	88	TCP	節點管理 LIF	Active Directory 樹系	Kerberos V 驗證
	137.	UDP	節點管理 LIF	Active Directory 樹系	NetBios 名稱服務
	138	UDP	節點管理 LIF	Active Directory 樹系	NetBios 資料報服務
	139.	TCP	節點管理 LIF	Active Directory 樹系	NetBios 服務工作階段
	389	TCP 與 UDP	節點管理 LIF	Active Directory 樹系	LDAP
	445	TCP	節點管理 LIF	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	464.64	TCP	節點管理 LIF	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	464.64	UDP	節點管理 LIF	Active Directory 樹系	Kerberos 金鑰管理
	749	TCP	節點管理 LIF	Active Directory 樹系	Kerberos V 變更與設定密碼（ RPCSEC_GSS ）
	88	TCP	資料 LIF （ NFS 、 CIFS 、 iSCSI ）	Active Directory 樹系	Kerberos V 驗證
	137.	UDP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 名稱服務
	138	UDP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 資料報服務
	139.	TCP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 服務工作階段
	389	TCP 與 UDP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	LDAP
	445	TCP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	464.64	TCP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	464.64	UDP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos 金鑰管理
	749	TCP	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos V 變更及設定密碼（ RPCSEC_GSS ）
AutoSupport	HTTPS	443..	節點管理 LIF	support.netapp.com	支援（預設為HTTPS）AutoSupport
	HTTP	80	節點管理 LIF	support.netapp.com	僅當傳輸傳輸傳輸傳輸傳輸傳輸協定從HTTPS變更為HTTP 時、AutoSupport
	TCP	3128	節點管理 LIF	連接器	如果無法使用傳出的網際網路連線、請透過Connector上的Proxy伺服器傳送AutoSupport 功能介紹訊息

服務	連接埠	傳輸協定	來源	目的地	目的
組態備份	HTTP	80	節點管理 LIF	\http ：//Wese/occm/offboxconfig <connector-IP-address>	將組態備份傳送至Connector。 "深入瞭解組態備份檔案"。
DHCP	68	UDP	節點管理 LIF	DHCP	第一次設定的 DHCP 用戶端
DHCPS	67	UDP	節點管理 LIF	DHCP	DHCP 伺服器
DNS	53.	UDP	節點管理 LIF 與資料 LIF （ NFS 、 CIFS ）	DNS	DNS
NDMP	18600 – 18699	TCP	節點管理 LIF	目的地伺服器	NDMP 複本
SMTP	25	TCP	節點管理 LIF	郵件伺服器	可以使用 SMTP 警示 AutoSupport 來執行功能
SNMP	161.	TCP	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	161.	UDP	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	162%	TCP	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	162%	UDP	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
SnapMirror	11104.	TCP	叢集間 LIF	叢集間 LIF ONTAP	管理 SnapMirror 的叢集間通訊工作階段
	11105.	TCP	叢集間 LIF	叢集間 LIF ONTAP	SnapMirror 資料傳輸
系統記錄	514	UDP	節點管理 LIF	系統記錄伺服器	系統記錄轉送訊息

連接器需求

如果您尚未建立連接器、也應該檢閱連接器的網路需求。

- "檢視連接器的網路需求"
- "Azure中的安全性群組規則"

設定Cloud Volumes ONTAP 支援使用Azure中客戶管理的金鑰

資料會使用在Cloud Volumes ONTAP Azure中的功能自動加密 "Azure 儲存服務加密" 使用Microsoft管理的金鑰。但您可以改用自己的加密金鑰、只要執行本頁的步驟即可。

資料加密總覽

Azure中的資料會使用自動加密Cloud Volumes ONTAP "Azure 儲存服務加密"。預設實作使用Microsoft管理的金鑰。無需設定。

如果您想要使用客戶管理的支援服務金鑰Cloud Volumes ONTAP 搭配使用、則必須完成下列步驟：

1. 從Azure建立金鑰保存庫、然後在該保存庫中產生金鑰

2. 從BlueXP中、使用API建立Cloud Volumes ONTAP 使用金鑰的功能不受影響的環境

金鑰旋轉

如果您建立新版的金鑰、Cloud Volumes ONTAP 則更新版本會自動使用最新的金鑰版本。

資料加密方式

BlueXP 使用磁碟加密集、可透過託管磁碟管理加密金鑰、而非分頁式分頁。任何新的資料磁碟也會使用相同的磁碟加密集。較低版本將使用Microsoft管理的金鑰、而非客戶管理的金鑰。

建立Cloud Volumes ONTAP 一個設定為使用客戶管理金鑰的功能完善的支援環境之後Cloud Volumes ONTAP 、即可將下列資料加密。

組態**Cloud Volumes ONTAP**	用於金鑰加密的系統磁碟	用於金鑰加密的資料磁碟
單一節點	• 開機 • 核心 • NVRAM	• 根目錄 • 資料
Azure HA 單一可用性區域、含頁面 Blobs	• 開機 • 核心 • NVRAM	無
Azure HA 單一可用性區域、含共用託管磁碟	• 開機 • 核心 • NVRAM	• 根目錄 • 資料
Azure HA 多個可用性區域、含共用託管磁碟	• 開機 • 核心 • NVRAM	• 根目錄 • 資料

所有的Azure儲存帳戶Cloud Volumes ONTAP 均使用客戶管理的金鑰進行加密。如果您想要在建立儲存帳戶期間加密、則必須在CVO建立要求中建立並提供資源ID。這適用於所有類型的部署。如果您未提供、儲存帳戶仍會加密、但BlueXP會先使用Microsoft管理的金鑰加密來建立儲存帳戶、然後再更新儲存帳戶以使用客戶管理的金鑰。

建立使用者指派的託管身分識別

您可以選擇建立稱為使用者指派之託管身分識別的資源。這樣做可讓您在建立 Cloud Volumes ONTAP 工作環境時加密儲存帳戶。建議您在建立金鑰資料保險箱和產生金鑰之前先建立此資源。

資源具有以下 ID ： `userassignedidentity`。

步驟

1. 在 Azure 中、前往 Azure 服務並選取 * 託管身分識別 * 。

2. 按一下「 * 建立 * 」。
3. 提供下列詳細資料：
   - * 訂閱 * ：選擇訂閱。我們建議您選擇與 Connector 訂閱相同的訂閱。
   - * 資源群組 * ：使用現有的資源群組或建立新的資源群組。
   - * 區域 * ：您也可以選擇與 Connector 相同的區域。
   - * 名稱 * ：輸入資源的名稱。
4. 您也可以新增標記。
5. 按一下「 * 建立 * 」。

建立金鑰保存庫並產生金鑰

金鑰庫必須位於您計畫建立Cloud Volumes ONTAP 此系統的同一個Azure訂閱和地區。

如果您 建立使用者指派的託管身分識別在建立金鑰資料保險箱時、您也應該為金鑰資料保險箱建立存取原則。

步驟

1. "在您的Azure訂閱中建立金鑰庫"。

   請注意金鑰庫的下列需求：

   - 金鑰保存庫必須與Cloud Volumes ONTAP 該系統位於相同的區域。
   - 應啟用下列選項：
     - 軟刪除（此選項預設為啟用、但不可停用）
     - 清除保護
     - 適用於**Volume**加密的**Azure**磁碟加密（適用於多個區域中的單一節點系統或HA配對）
   - 如果您建立使用者指派的託管身分識別、則應啟用下列選項：
     - * 資料保險箱存取原則 *
2. 如果您選取了 Vault 存取原則、請按一下「建立」來建立金鑰資料保險箱的存取原則。如果沒有、請跳至步驟 3 。
   a. 選取下列權限：
      - 取得
      - 清單
      - 解密
      - 加密
      - 解開密鑰
      - 換行鍵
      - 驗證
      - 簽署
   b. 選取使用者指派的託管身分識別（資源）做為主體。

c. 檢閱並建立存取原則。

3. "在金鑰保存庫中產生金鑰"。

   請注意金鑰的下列需求：

   - 金鑰類型必須為* RSA*。
   - 建議的RSA金鑰大小為* 2048*、但支援其他大小。

建立使用加密金鑰的工作環境

建立金鑰庫並產生加密金鑰之後、您可以建立Cloud Volumes ONTAP 新的、設定為使用金鑰的整套系統。使用BlueXP API可支援這些步驟。

必要權限

如果您想將客戶管理的金鑰與單一節點Cloud Volumes ONTAP 的一套系統整合、請確認BlueXP Connector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"
```

"檢視最新的權限清單"

步驟

1. 請使用下列BlueXP API呼叫、取得Azure訂閱中的金鑰保存清單。

   對於HA配對：「Get /azure/ha/mata/Vault」

   對於單一節點：「Get /azure/VSA/中繼資料/資料保存」

   請記下*名稱*和*資源群組*。您需要在下一步中指定這些值。

   "深入瞭解此API呼叫"。

2. 使用下列BlueXP API呼叫取得資料保險箱內的金鑰清單。

   對於HA配對：「Get /azure/ha/matmata/keys/Vault」

   對於單一節點：「Get /azure/VSA/中繼資料/金鑰庫」

   請記下*金鑰名稱*。您需要在下一步中指定該值（連同資料保險箱名稱）。

   "深入瞭解此API呼叫"。

3. 使用Cloud Volumes ONTAP 下列BlueXP API呼叫建立一個系統。

   a. 對於HA配對：

      「POST /azure/ha/辦公 環境」

      申請本文必須包含下列欄位：

      ```
      "azureEncryptionParameters": {
                    "key": "keyName",
                    "vaultName": "vaultName"
      }
      ```

      包括 "userAssignedIdentity": " userAssignedIdentityId" 如果您建立此資源以用於儲存帳戶加密、請輸入此欄位。

      "深入瞭解此API呼叫"。

   b. 對於單一節點系統：

      「POST /azure/VSA/工作環境」

      申請本文必須包含下列欄位：

      ```
      "azureEncryptionParameters": {
                    "key": "keyName",
                    "vaultName": "vaultName"
      }
      ```

      包括 "userAssignedIdentity": " userAssignedIdentityId" 如果您建立此資源以用於儲存帳戶加密、請輸入此欄位。

   "深入瞭解此API呼叫"。

結果

您有一個Cloud Volumes ONTAP 全新的支援系統、可設定使用客戶管理的金鑰進行資料加密。

在Cloud Volumes ONTAP Azure中設定for NetApp的授權

決定Cloud Volumes ONTAP 要搭配使用哪種授權選項之後、您必須先執行幾個步驟、才能在建立新的工作環境時選擇授權選項。

Freemium

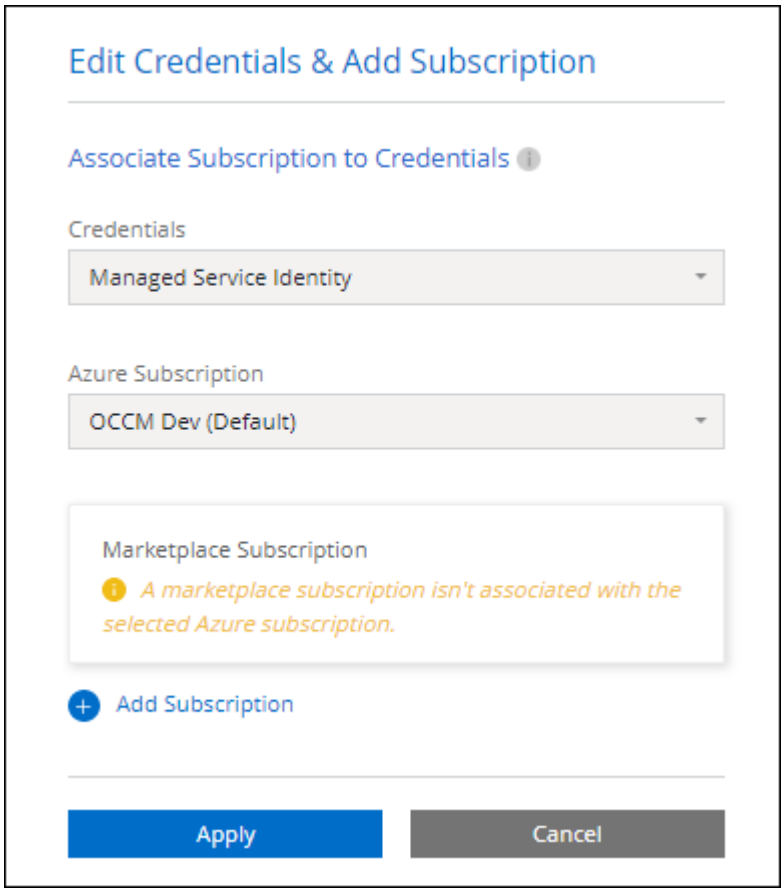
選擇Freemium產品、即可免費使用Cloud Volumes ONTAP 多達500 GiB的配置容量。 "深入瞭解Freemium產品"。

步驟

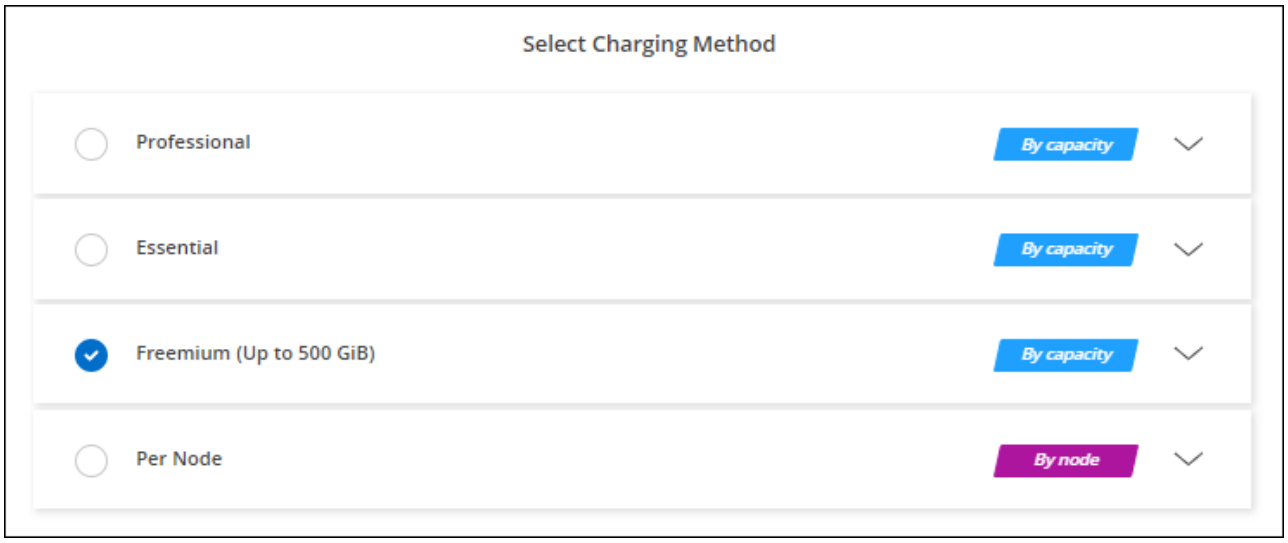
1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。

   a. 在*詳細資料與認證*頁面上、按一下*編輯認證>新增訂閱*、然後依照提示訂閱Azure Marketplace中的隨用隨付方案。

      除非您超過500 GiB的已配置容量、系統會自動轉換為、否則不會透過市場訂閱付費 "Essentials套件"。



   a. 返回BluetXP之後、當您到達「充電方法」頁面時、請選取* Freemium *。



"請參閱Cloud Volumes ONTAP 逐步指示、以在Azure中推出《功能不全》"。

容量型授權

容量型授權可讓您針對Cloud Volumes ONTAP 容量的每個TiB付費。容量型授權的形式為_package_：Essentials套件或Professional套件。

Essentials和Professional套件可搭配下列消費模式使用：

- 向NetApp購買的授權（BYOL）
- Azure Marketplace的每小時隨付隨付（PAYGO）訂閱
- 年度合約

"深入瞭解容量型授權"。

下列各節將說明如何開始使用這些消費模式。

BYOL

事先向NetApp購買授權（BYOL）、即可在Cloud Volumes ONTAP 任何雲端供應商部署支援系統。

步驟

1. "請聯絡NetApp銷售人員以取得授權"
2. "將NetApp 支援網站 您的不更新帳戶新增至藍圖XP"

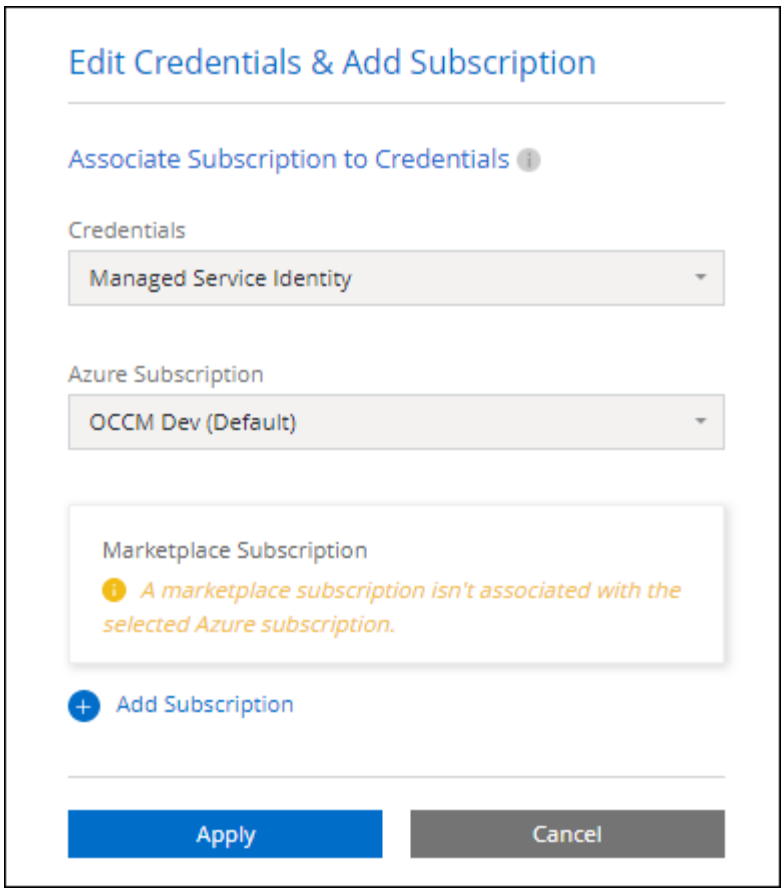
   BlueXP會自動查詢NetApp的授權服務、以取得NetApp 支援網站 與您的還原帳戶相關之授權的詳細資料。如果沒有錯誤、 BlueXP 會自動將授權新增至數位錢包。

   您必須先從 BlueXP 數位錢包取得授權、才能搭配 Cloud Volumes ONTAP 使用。如有需要、您可以 "手動將授權新增至 BlueXP 數位錢包"。

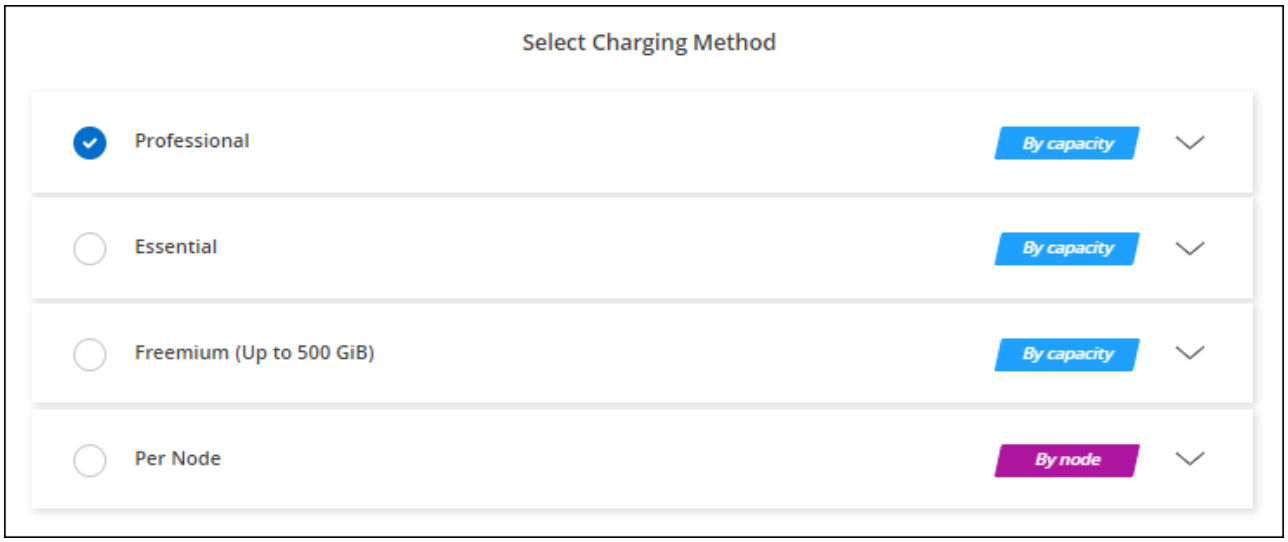
3. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。

   a. 在*詳細資料與認證*頁面上、按一下*編輯認證>新增訂閱*、然後依照提示訂閱Azure Marketplace中的隨用隨付方案。

      您向NetApp購買的授權一律會先收取費用、但如果您超過授權容量或授權到期、則會從市場的每小時費率中收取費用。



a. 返回BlueXP之後、當您到達「充電方法」頁面時、請選取容量型套件。



"請參閱Cloud Volumes ONTAP 逐步指示、以在Azure中推出《功能不全》"。

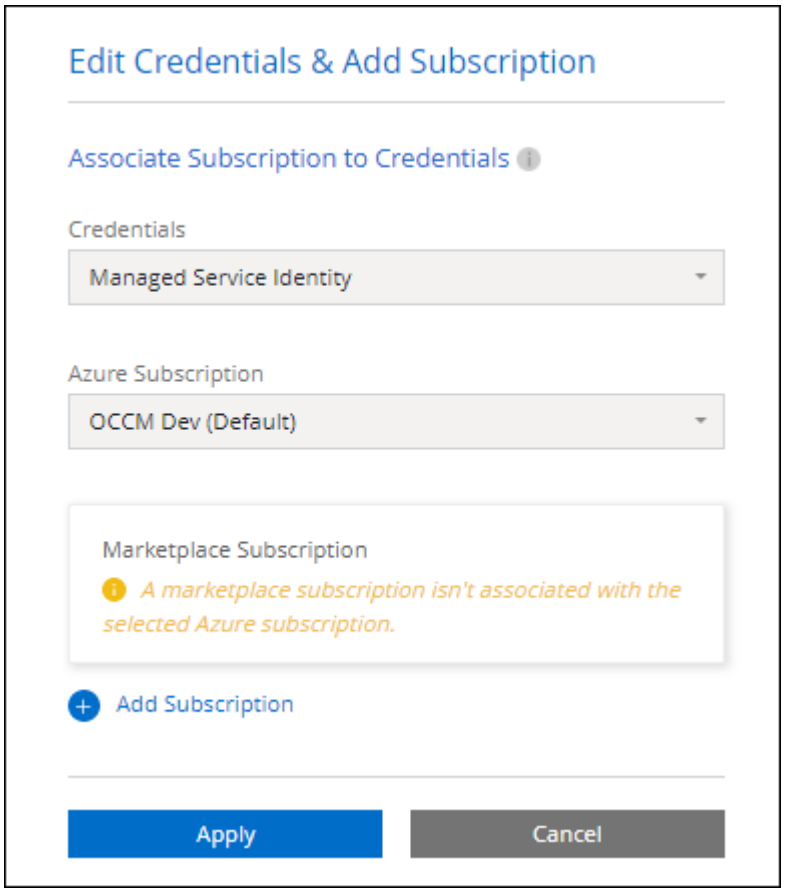
PAYGO訂閱

從雲端供應商的市場訂閱優惠、每小時支付一次。

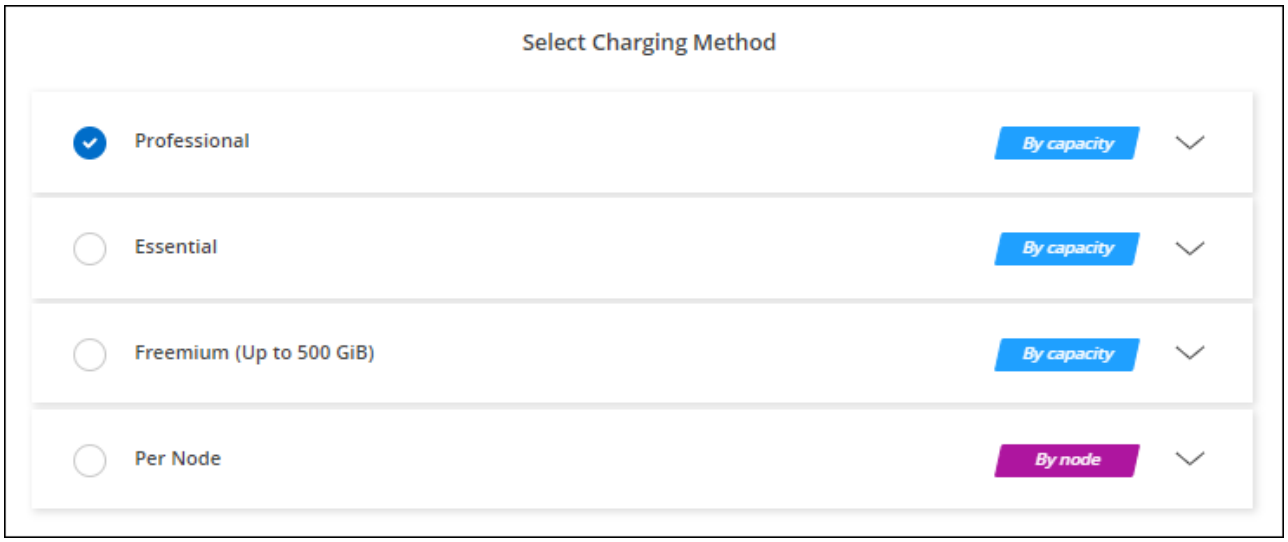
當您建立Cloud Volumes ONTAP 一個運作環境時、BlueXP會提示您訂閱Azure Marketplace提供的合約。該訂閱之後會與工作環境建立關聯、以便進行充電。您可以在其他工作環境中使用相同的訂閱。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。
   a. 在*詳細資料與認證*頁面上、按一下*編輯認證>新增訂閱*、然後依照提示訂閱Azure Marketplace中的隨用隨付方案。



   b. 返回BlueXP之後、當您到達「充電方法」頁面時、請選取容量型套件。



"請參閱Cloud Volumes ONTAP 逐步指示、以在Azure中推出《功能不全》"。

您可以從「設定」>「認證」頁面管理Azure Marketplace與Azure帳戶相關的訂閱。 "瞭解如何管理您的Azure帳戶和訂閱"

年度合約

購買年度合約、每年支付Cloud Volumes ONTAP 一份銷售費。

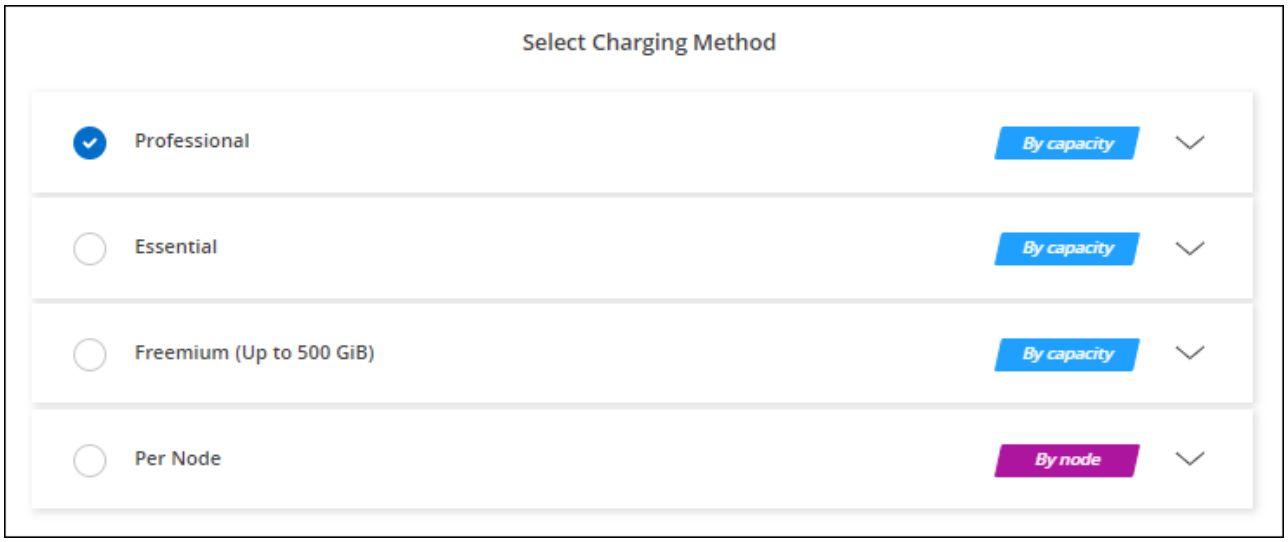
步驟

1. 請聯絡您的NetApp銷售代表以購買年度合約。

   該合約可在Azure Marketplace以_Private _優惠形式提供。

   NetApp與您分享私人優惠之後、您可以在工作環境建立期間、從Azure Marketplace訂閱年度方案。

2. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。
   a. 在*詳細資料與認證*頁面上、按一下*編輯認證>新增訂閱>繼續*。
   b. 在Azure入口網站中、選取與Azure帳戶共享的年度計畫、然後按一下*訂閱*。
   c. 返回BlueXP之後、當您到達「充電方法」頁面時、請選取容量型套件。



"請參閱Cloud Volumes ONTAP 逐步指示、以在Azure中推出《功能不全》"。

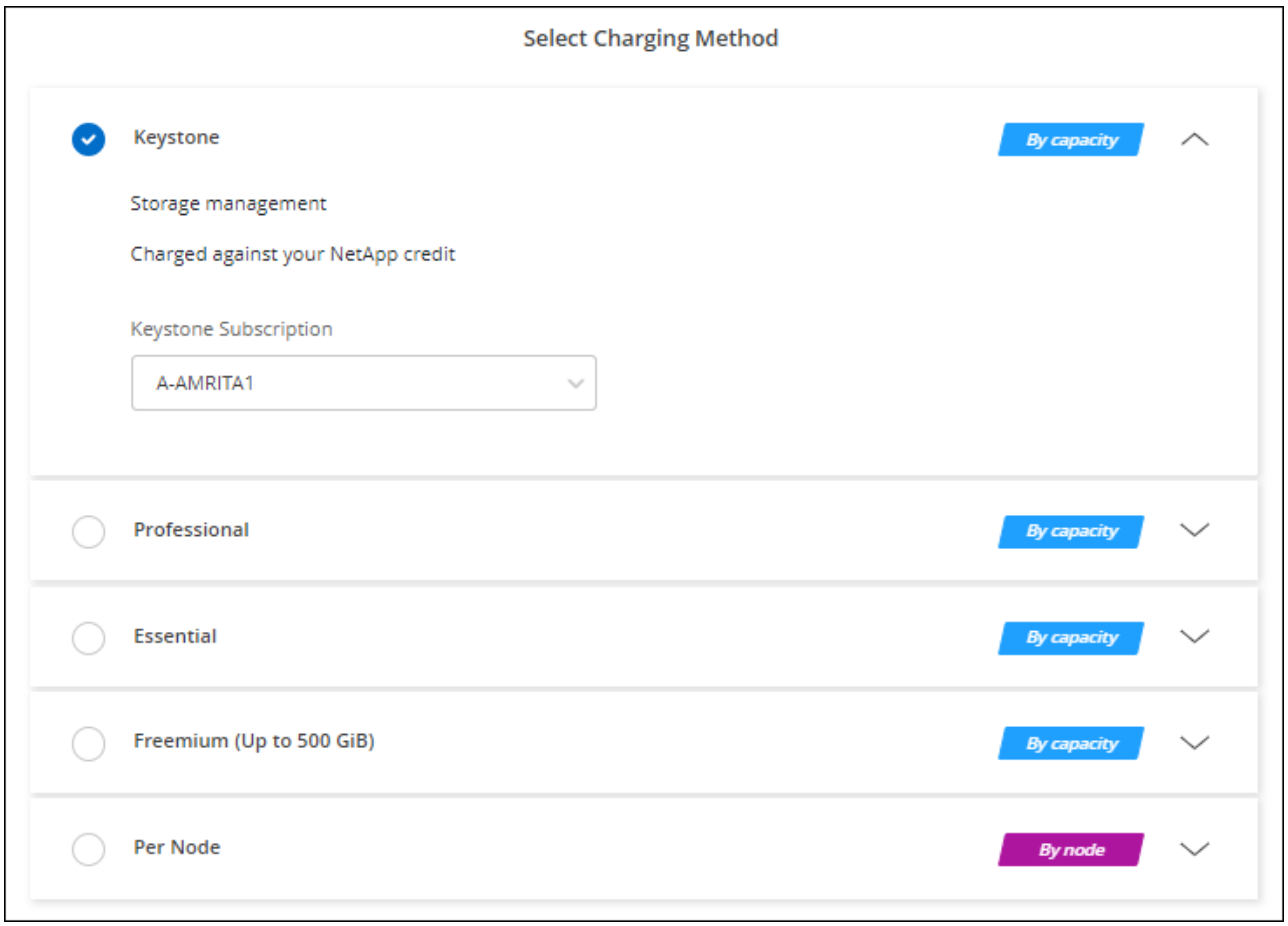
Keystone訂閱

Keystone 訂閱是一項隨成長付費訂閱服務。 "深入瞭解 NetApp Keystone 訂閱"。

步驟

1. 如果您尚未訂閱、 "請聯絡NetApp"
2. mailto ： ng-keystone-success@netapp.com [聯絡 NetApp] 以使用一或多個 Keystone 訂閱來授權您的 BlueXP 使用者帳戶。
3. NetApp授權您的帳戶之後、 "連結您的訂閱內容以供Cloud Volumes ONTAP 搭配使用"。
4. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。

a. 當系統提示您選擇充電方法時、請選取 Keystone Subscription 充電方法。



"請參閱Cloud Volumes ONTAP 逐步指示、以在Azure中推出《功能不全》"。

在**Azure**中啟用高可用度模式

Microsoft Azure的高可用度模式應可減少非計畫性容錯移轉時間、並啟用NFSv4 for Cloud Volumes ONTAP 功能。

從發行版《S21》開始Cloud Volumes ONTAP 、我們縮短Cloud Volumes ONTAP 了在Microsoft Azure上執行的《21個HA配對》的非計畫性容錯移轉時間、並增加了對NFSv4的支援。若要讓Cloud Volumes ONTAP 這些增強功能適用於整個過程、您必須啟用Azure訂閱的高可用度功能。

當您需要在Azure訂閱中啟用此功能時、BlueXP會在必要行動訊息中提示您提供這些詳細資料。

請注意下列事項：

- 高可用度Cloud Volumes ONTAP 的不存在任何問題。此Azure功能可搭配ONTAP 使用、以減少因非計畫性容錯移轉事件而導致NFS傳輸協定的應用程式停機時間。
- 啟用此功能對Cloud Volumes ONTAP 功能不中斷運作、不中斷對功能的支援。
- 在您的Azure訂閱中啟用此功能、不會對其他VM造成問題。

具備「擁有者」權限的Azure使用者可從Azure CLI啟用此功能。

步驟

1. "從Azure Portal存取Azure Cloud Shell"
2. 註冊高可用度模式功能：

```
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）驗證功能是否已註冊：

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

Azure CLI應傳回類似下列的結果：

```
{
  "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"
}
```

在 **Cloud Volumes ONTAP Azure** 中啟動

您可以在Cloud Volumes ONTAP BlueXP中建立運作環境、在Azure中啟動單一節點系統或HA配對。

您需要的產品

您需要下列項目才能建立工作環境。

- 已啟動並執行的連接器。
  - 您應該擁有 "與工作區相關的連接器"。
  - "您應該隨時準備好讓 Connector 保持運作"。
- 瞭解您要使用的組態。

  您應該已經選擇組態、並從系統管理員取得 Azure 網路資訊。如需詳細資訊、請參閱 "規劃 Cloud Volumes ONTAP 您的需求組態"。

- 瞭解設定Cloud Volumes ONTAP 驗證功能所需的條件。

  "瞭解如何設定授權"。

關於這項工作

當BlueXP在Cloud Volumes ONTAP Azure中建立一個功能完善的系統時、它會建立多個Azure物件、例如資源群組、網路介面和儲存帳戶。您可以在精靈結束時檢閱資源摘要。

> 資料遺失的可能性
>
> 最佳實務做法是針對每Cloud Volumes ONTAP 個系統使用新的專屬資源群組。
>
> 由於資料遺失的風險、不建議在 Cloud Volumes ONTAP 現有的共享資源群組中部署此功能。雖然在Cloud Volumes ONTAP 部署失敗或刪除的情況下、BlueXP可以從共用資源群組移除一些不必要的資源、但Azure使用者可能會不小心從Cloud Volumes ONTAP 共用資源群組中刪除一些不必要的資源。

在Cloud Volumes ONTAP Azure中啟動單一節點的不完整系統

如果您想要在Cloud Volumes ONTAP Azure中啟動單一節點的功能、您需要在BlueXP中建立單一節點的工作環境。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. [[訂閱]在「畫版」頁面上、按一下「新增工作環境」、然後依照提示進行。
3. 選擇位置：選擇* Microsoft Azure 和 Cloud Volumes ONTAP 《單一節點*》。
4. 如果出現提示、 "建立連接器"。
5. 詳細資料與認證：選擇性變更Azure認證與訂閱、指定叢集名稱、視需要新增標籤、然後指定認證資料。

   下表說明您可能需要指導的欄位：

欄位	說明
工作環境名稱	BlueXP使用工作環境名稱來命名Cloud Volumes ONTAP 整個系統、以及Azure虛擬機器。如果您選取該選項、它也會使用名稱做為預先定義安全性群組的前置詞。
資源群組標記	標記是 Azure 資源的中繼資料。在此欄位中輸入標記時、BlueXP會將標記新增至與Cloud Volumes ONTAP 該系統相關聯的資源群組。建立工作環境時、您最多可以從使用者介面新增四個標記、然後在建立之後新增更多標記。請注意、在建立工作環境時、 API 不會限制您使用四個標記。如需標記的相關資訊、請參閱 "Microsoft Azure 說明文件：使用標籤來組織 Azure 資源"。
使用者名稱和密碼	這些是Cloud Volumes ONTAP 適用於整個叢集管理員帳戶的認證資料。您可以使用這些認證資料、 Cloud Volumes ONTAP 透過 System Manager 或其 CLI 連線至功能驗證。保留預設的_admin_使用者名稱、或將其變更為自訂使用者名稱。
[[video ）] 編輯認證資料	您可以選擇不同的 Azure 認證資料和其他 Azure 訂閱、以搭配此 Cloud Volumes ONTAP 款作業系統使用。您必須將 Azure Marketplace 訂閱與所選 Azure 訂閱建立關聯、才能部署隨用隨付 Cloud Volumes ONTAP 的功能。 "瞭解如何新增認證"。

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

從 Azure Marketplace 訂閱 BlueXP

6. * 服務 * ：啟用或停用 Cloud Volumes ONTAP 您不想搭配使用的個別服務。
   - "深入瞭解 BlueXP 分類"
   - "深入瞭解 BlueXP 備份與還原"

   如果您想要使用 WORM 和資料分層功能、您必須停用 BlueXP 備份與還原、並部署 9.8 版或更新版本的 Cloud Volumes ONTAP 工作環境。

7. 位置：選取區域、可用度區域、vnet和子網路、然後選取核取方塊以確認連接器與目標位置之間的網路連線。

   對於單一節點系統、您可以選擇要部署 Cloud Volumes ONTAP 的可用度區域。如果您未選擇AZ、則BlueXP會為您選擇一個。

8. 連線能力：選擇新的或現有的資源群組、然後選擇是使用預先定義的安全性群組、還是使用自己的。

   下表說明您可能需要指導的欄位：

欄位	說明
資源群組	建立Cloud Volumes ONTAP 新的資源群組以供使用、或使用現有的資源群組。最佳實務做法是使用全新的資源群組 Cloud Volumes ONTAP 來進行支援。雖然可以在Cloud Volumes ONTAP 現有的共享資源群組中部署功能、但由於資料遺失的風險、不建議這麼做。如需詳細資料、請參閱上述警告。 如果您使用的Azure帳戶具有 "必要權限"、在Cloud Volumes ONTAP 部署失敗或刪除的情況下、BlueXP會從資源群組移除一些不必要的資源。
產生的安全性群組	如果讓BlueXP為您產生安全性群組、您必須選擇允許流量的方式： • 如果您選擇*選取的vnet only *、則傳入流量的來源是所選vnet的子網路範圍、以及連接器所在vnet的子網路範圍。這是建議的選項。 • 如果您選擇*所有VNet*、則傳入流量的來源為0.00.0.0/0 IP範圍。
使用現有的	如果您選擇現有的安全群組、則必須符合Cloud Volumes ONTAP 下列需求： "檢視預設的安全性群組"。

9. 充電方法與**NSS**帳戶：指定您要搭配此系統使用的收費選項、然後指定NetApp支援網站帳戶。
   - "深入瞭Cloud Volumes ONTAP 解適用於此功能的授權選項"。
   - "瞭解如何設定授權"。
10. * 預先設定的套件 * ：選取其中一個套件以快速部署 Cloud Volumes ONTAP 某個作業系統、或按一下 * 建立我自己的組態 * 。

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

11. 授權：視Cloud Volumes ONTAP 需要變更此版本、然後選取虛擬機器類型。

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

12. * 訂閱 Azure Marketplace* ：如果 BlueXP 無法啟用 Cloud Volumes ONTAP 的程式設計部署、您會看到此頁面。請依照畫面上列出的步驟進行。請參閱 "市場產品的程式化部署" 以取得更多資訊。

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

    請注意下列事項：

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

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

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

      "深入瞭解資料分層"。

14. *寫入速度與WORM *：

    a. 如果需要、請選擇*正常*或*高速*寫入速度。

       "深入瞭解寫入速度"。

    b. 視需要啟動一次寫入、多次讀取（WORM）儲存設備。

       此選項僅適用於特定VM類型。若要瞭解支援哪些VM類型、請參閱 "HA配對授權的支援組態"。

       如果啟用Cloud Volumes ONTAP 資料分層功能、無法啟用WORM 9.7版及更低版本。啟用WORM和分層後、將Cloud Volumes ONTAP 會封鎖還原或降級至物件9.8。

    "深入瞭解 WORM 儲存設備"。

    a. 如果您啟動WORM儲存設備、請選取保留期間。

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

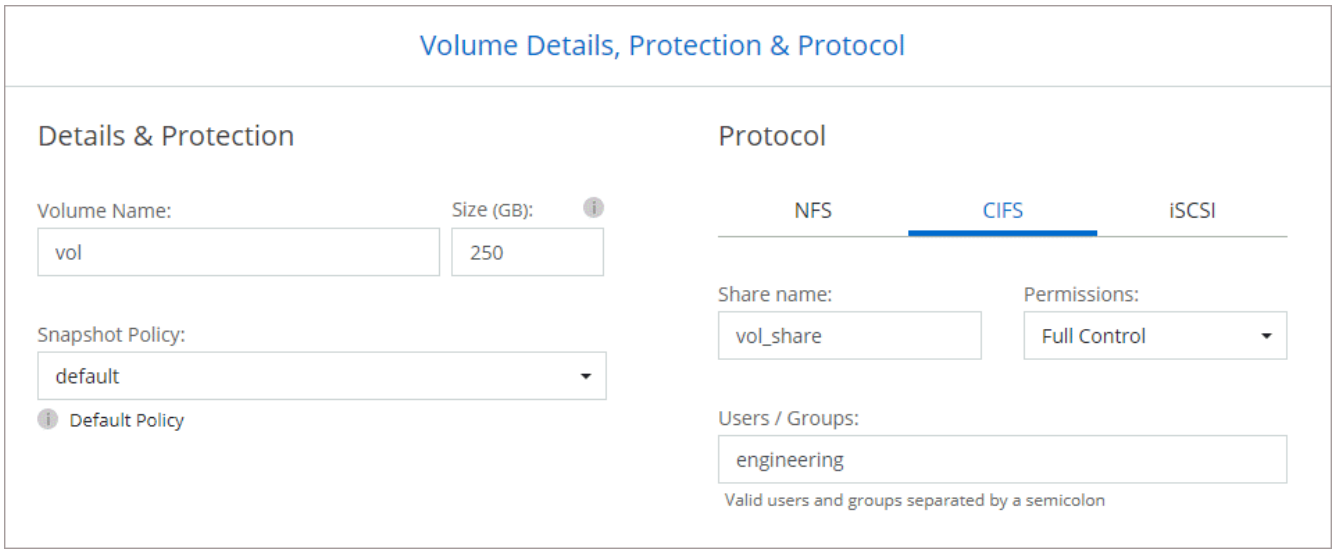
    "瞭解支援的用戶端傳輸協定和版本"。

    本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

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

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

下圖顯示 CIFS 傳輸協定的「 Volume 」（磁碟區）頁面：



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

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

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

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

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

18. * 審查與核准 * ：檢閱並確認您的選擇。
    a. 檢閱組態的詳細資料。
    b. 按一下*更多資訊*以檢閱有關支援與BlueXP將購買之Azure資源的詳細資料。
    c. 選取「 * 我瞭解 … * 」核取方塊。
    d. 按一下「 * 執行 * 」。

結果

BlueXP部署Cloud Volumes ONTAP 了這個功能完善的系統。您可以追蹤時間表的進度。

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

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

完成後

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

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

在Cloud Volumes ONTAP Azure中啟動一套功能完善的

如果您想要在Cloud Volumes ONTAP Azure中啟動一套功能不均的HA配對、您必須在BlueXP中建立HA工作環境。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. [[訂閱]在「畫版」頁面上、按一下「新增工作環境」、然後依照提示進行。
3. 如果出現提示、 "建立連接器"。
4. 詳細資料與認證：選擇性變更Azure認證與訂閱、指定叢集名稱、視需要新增標籤、然後指定認證資料。

   下表說明您可能需要指導的欄位：

欄位	說明
工作環境名稱	BlueXP使用工作環境名稱來命名Cloud Volumes ONTAP 整個系統、以及Azure虛擬機器。如果您選取該選項、它也會使用名稱做為預先定義安全性群組的前置詞。
資源群組標記	標記是 Azure 資源的中繼資料。在此欄位中輸入標記時、BlueXP會將標記新增至與Cloud Volumes ONTAP 該系統相關聯的資源群組。建立工作環境時、您最多可以從使用者介面新增四個標記、然後在建立之後新增更多標記。請注意、在建立工作環境時、 API 不會限制您使用四個標記。如需標記的相關資訊、請參閱 "Microsoft Azure 說明文件：使用標籤來組織 Azure 資源"。
使用者名稱和密碼	這些是Cloud Volumes ONTAP 適用於整個叢集管理員帳戶的認證資料。您可以使用這些認證資料、 Cloud Volumes ONTAP 透過 System Manager 或其 CLI 連線至功能驗證。保留預設的_admin_使用者名稱、或將其變更為自訂使用者名稱。
[[video ）] 編輯認證資料	您可以選擇不同的 Azure 認證資料和其他 Azure 訂閱、以搭配此 Cloud Volumes ONTAP 款作業系統使用。您必須將 Azure Marketplace 訂閱與所選 Azure 訂閱建立關聯、才能部署隨用隨付 Cloud Volumes ONTAP 的功能。 "瞭解如何新增認證"。

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

   從 Azure Marketplace 訂閱 BlueXP

5. * 服務 * ：啟用或停用 Cloud Volumes ONTAP 您不想搭配使用的個別服務。
   - "深入瞭解 BlueXP 分類"
   - "深入瞭解 BlueXP 備份與還原"

   如果您想要使用 WORM 和資料分層功能、您必須停用 BlueXP 備份與還原、並部署 9.8 版或更新版本的 Cloud Volumes ONTAP 工作環境。

6. * HA部署模式*：
   a. 選擇*單一可用度區域*或*多個可用度區域*。
   b. 位置與連線（單一AZ）及*地區與連線*（多個AZs）
      - 對於單一AZ、請選取一個地區、vnet和子網路。

- 對於多個AZs、請為節點1選取區域、vnet、子網路、區域、為節點2選取區域。

c. 選取「我已驗證網路連線能力...」核取方塊。

7. 連線能力：選擇新的或現有的資源群組、然後選擇是使用預先定義的安全性群組、還是使用自己的。

   下表說明您可能需要指導的欄位：

欄位	說明
資源群組	建立Cloud Volumes ONTAP 新的資源群組以供使用、或使用現有的資源群組。最佳實務做法是使用全新的資源群組 Cloud Volumes ONTAP 來進行支援。雖然可以在Cloud Volumes ONTAP 現有的共享資源群組中部署功能、但由於資料遺失的風險、不建議這麼做。如需詳細資料、請參閱上述警告。 您必須使用專屬的資源群組來處理Cloud Volumes ONTAP 您在Azure中部署的每個「EHA配對」。資源群組僅支援一個HA配對。如果您嘗試在Cloud Volumes ONTAP Azure資源群組中部署第二個「鏈接HA配對」、則BlueXP會遇到連線問題。 如果您使用的Azure帳戶具有 "必要權限"、在Cloud Volumes ONTAP 部署失敗或刪除的情況下、BlueXP會從資源群組移除一些不必要的資源。
產生的安全性群組	如果讓BlueXP為您產生安全性群組、您必須選擇允許流量的方式： • 如果您選擇*選取的vnet only *、則傳入流量的來源是所選vnet的子網路範圍、以及連接器所在vnet的子網路範圍。這是建議的選項。 • 如果您選擇*所有VNet*、則傳入流量的來源為0.00.0.0/0 IP範圍。
使用現有的	如果您選擇現有的安全群組、則必須符合Cloud Volumes ONTAP 下列需求： "檢視預設的安全性群組"。

8. 充電方法與**NSS**帳戶：指定您要搭配此系統使用的收費選項、然後指定NetApp支援網站帳戶。
   - "深入瞭Cloud Volumes ONTAP 解適用於此功能的授權選項"。
   - "瞭解如何設定授權"。
9. 預先設定的套件：選取其中一個套件以快速部署Cloud Volumes ONTAP 一個作業系統、或按一下*變更組態*。

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

10. 授權：視Cloud Volumes ONTAP 需要變更此版本、然後選取虛擬機器類型。

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

11. 從**Azure Marketplace**訂閱：如果BlueXP無法啟用Cloud Volumes ONTAP 程式化部署的功能、請依照下列步驟進行。

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

    請注意下列事項：

    - 磁碟大小適用於初始Aggregate中的所有磁碟、以及使用Simple Provisioning選項時、BlueXP所建立的任何其他Aggregate。您可以使用進階配置選項、建立使用不同磁碟大小的集合體。

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

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

      "深入瞭解資料分層"。

13. *寫入速度與WORM *：

    a. 如果需要、請選擇*正常*或*高速*寫入速度。

       "深入瞭解寫入速度"。

    b. 視需要啟動一次寫入、多次讀取（WORM）儲存設備。

       此選項僅適用於特定VM類型。若要瞭解支援哪些VM類型、請參閱 "HA配對授權的支援組態"。

       如果啟用Cloud Volumes ONTAP 資料分層功能、無法啟用WORM 9.7版及更低版本。啟用WORM和分層後、將Cloud Volumes ONTAP 會封鎖還原或降級至物件9.8。

    "深入瞭解 WORM 儲存設備"。

    a. 如果您啟動WORM儲存設備、請選取保留期間。

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

    HTTPS連線是Cloud Volumes ONTAP 從一個畫面9.7 HA配對到Azure網頁blob儲存帳戶。請注意、啟用此選項可能會影響寫入效能。您無法在建立工作環境之後變更設定。

    "深入瞭解 WORM 儲存設備"。

    如果資料分層已啟用、則無法啟用 WORM 。

    "深入瞭解 WORM 儲存設備"。

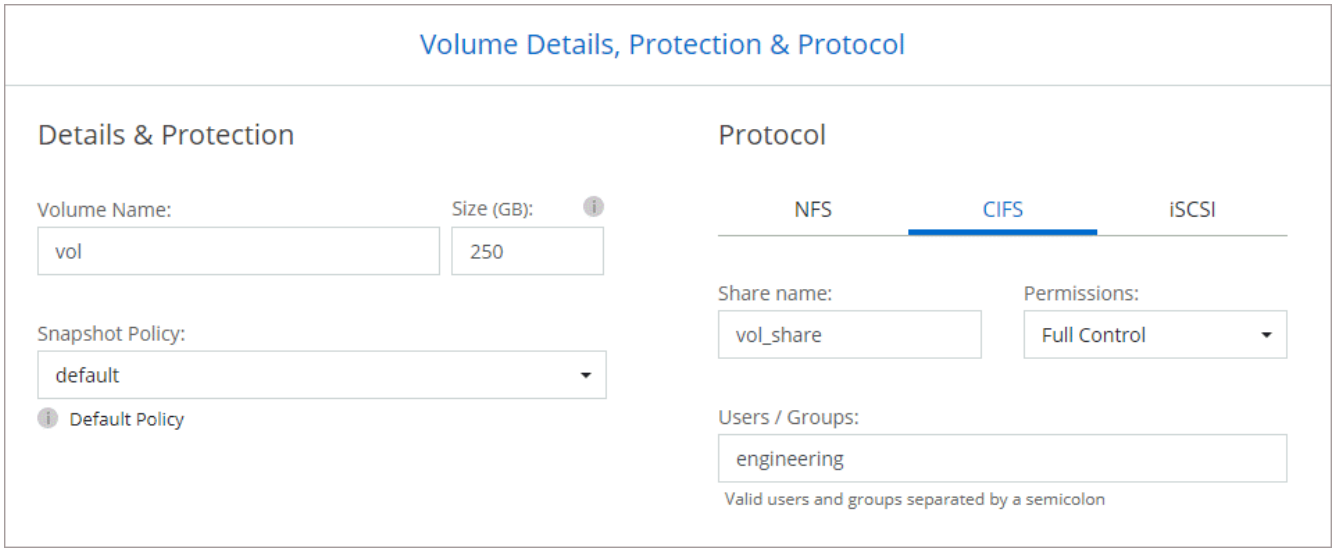
15. * 建立 Volume * ：輸入新磁碟區的詳細資料、或按一下 * 跳過 * 。

    "瞭解支援的用戶端傳輸協定和版本"。

    本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

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

下圖顯示 CIFS 傳輸協定的「 Volume 」（磁碟區）頁面：



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

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

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

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

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

18. * 審查與核准 * ：檢閱並確認您的選擇。
    a. 檢閱組態的詳細資料。
    b. 按一下*更多資訊*以檢閱有關支援與BlueXP將購買之Azure資源的詳細資料。
    c. 選取「 * 我瞭解 … * 」核取方塊。
    d. 按一下「 * 執行 * 」。

結果

BlueXP部署Cloud Volumes ONTAP 了這個功能完善的系統。您可以追蹤時間表的進度。

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

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

完成後

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

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

Azure 平台影像驗證

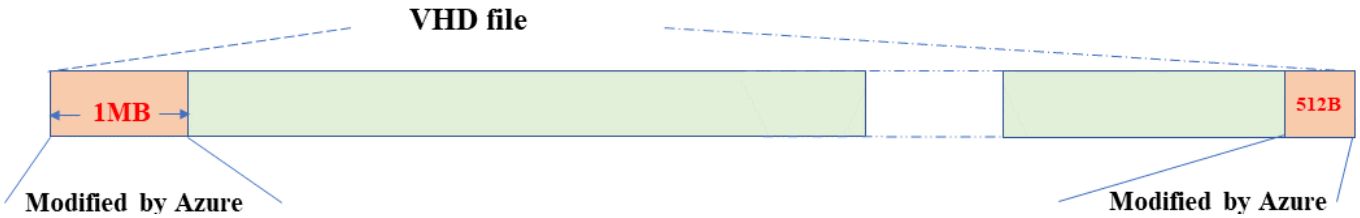
Azure 影像驗證總覽

Azure 影像驗證符合增強的 NetApp 安全要求。雖然驗證映像檔案是一項簡單的程序、但 Azure 映像簽章驗證確實需要特別的資料、才能將其傳送至知名的 Azure VHD 映像檔、因為 Azure 市場已進行了一次替代。

Cloud Volumes ONTAP 軟體 9.15.0 版或更新版本支援 Azure 影像驗證。

Azure 對已發佈 VHD 檔案的變更

Azure 修改了領先業界的 1MB （ 1048576 位元組）和結束 512 位元組 VHD 檔案。NetApp 映像簽署會略過前導的 1MB 並結束 512 個位元組、然後簽署剩餘的 VHD 映像部分。



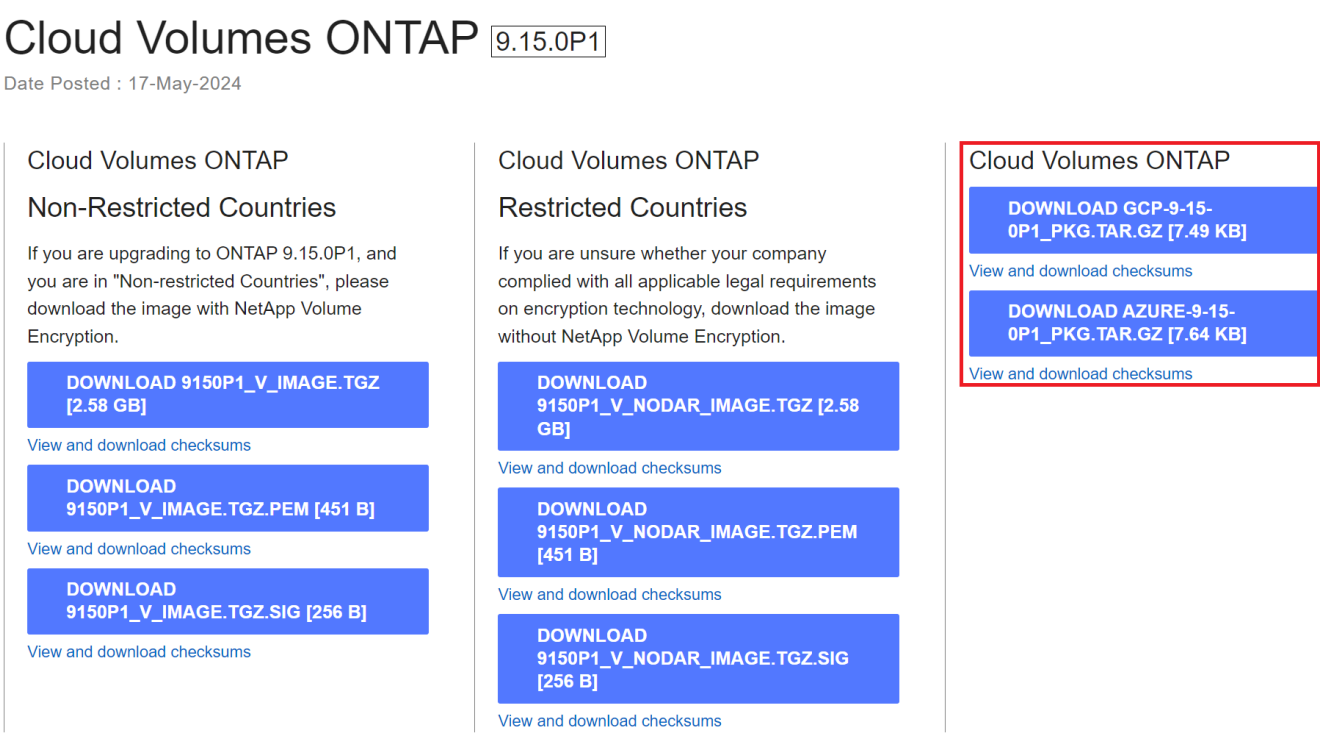
例如、上圖顯示大小為 10GB 的 VHD 檔案。但 NetApp 簽署部分會以綠色標示、大小為 10GB - 1MB - 512B 。

下載 Azure Image Digest File

Azure Image Digest File 可從下載 "NetApp 支援網站"。下載檔案為 tar.gz 格式、包含用於影像簽章驗證的檔案。

步驟

1. 前往 "NetApp 支援網站 上的 Cloud Volumes ONTAP 產品頁面" 並在「下載」區段下載所需的軟體版本。
2. 在 Cloud Volumes ONTAP 下載頁面下、按一下 Azure 影像摘要檔案的 * 下載按鈕 * 、即可下載 TAR 。 gz 檔案。



3. 對於 Linux 和 MacOS 、您必須執行下列步驟、才能取得下載 Azure Image Digest 檔案的 md5sum 和 shav256sum 。
   a. 若為 md5sum 、請輸入 `md5sum` 命令。
   b. 若為 shaf256sum 、請輸入 `sha256sum` 命令。
4. 驗證 `md5sum` 和 `sha256sum` 值符合 Azure Image Digest File 下載。
5. 在 Linux 和 Mac OS 上、執行 `tar -xzf` 擷取 tar.gz 檔案的命令。

   擷取的 TAR 。 gz 檔案包含摘要檔案（ .sig ）、公開金鑰憑證檔案（ .pem ）和鏈結憑證檔案（ .pem ）。

   。列出解壓縮 tar.gz 檔案的結果 *

```
$ 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
```

映像從 **Azure Marketplace** 匯出

一旦 VHD 映像發佈至 Azure 雲端、該映像就不再由 NetApp 管理。而是將發佈的映像放在 Azure 市場上。Azure 對 VHD 的領先 1MB 和結尾 512B 的變更是在 Azure 市場上分段及發佈映像時發生的。若要驗證 VHD 檔案的簽章、 Azure 修改的 VHD 映像必須先從 Azure 市場匯出。

您需要的產品

您必須在系統上安裝必要的程式。

- Azure CLI 已安裝、或 Azure Cloud Shell 透過 Azure 入口網站隨時可供使用。

  如需如何安裝 Azure CLI 的詳細資訊、請參閱 "Azure 說明文件：如何安裝 Azure CLI"。

步驟

1. 使用 version_readme.Me 檔案的內容、將 ONTAP 版本對應至 Azure 市場映像版本。

   對於版本 _ 讀我檔案中列出的每個版本對應、 ONTAP 版本以「 buildname 」表示、 Azure 市場映像版本以「 version 」表示。

   例如、在下列版本 _ 讀我檔案中、 ONTAP 版本「 9.15.0P1 」對應至 Azure 市場映像版本「 9150.01000024.05090105 」。此 Azure 市場映像版本稍後會用於設定映像 URN 。

   ```
   [
       {
           "buildname": "9.15.0P1",
           "publisher": "netapp",
           "version": "9150.01000024.05090105"
       }
   ]
   ```

2. 識別您要建立 VM 的區域名稱。

   設定市場映像的 URN 時、此區域名稱會用作「 locName 」變數的值。

   a. 若要接收可用區域的清單、請輸入 `az account list-locations -o table` 命令。

      在下表中、區域名稱稱為「名稱」欄位。

   ```
   $ 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. 請從下表中檢閱對應 VM 部署類型的 SKU 名稱。

   當設定市場映像的 URN 時、 SKU 名稱會用作「 skuName 」變數的值。

   例如、單一節點部署應使用「 ONTAP 雲端 byol 」 SKU 名稱。

VM 部署類型	SKU 名稱
單一節點	ONTAP 雲端
高可用度	ONTAP 雲端 _ byol_ha

4. ONTAP 版本和 Azure 市場映像對應完成後、即可透過 Azure Cloud Shell 或 Azure CLI 、從 Azure 市場匯出 VHD 檔案。

透過 **Azure** 入口網站上的 **Azure Cloud Shell** 匯出 **VHD** 檔案

1. 從 Azure Cloud Shell 將市場映像匯出至 vhd （ image2 、例如 9150.01000024.05090105.vhd ）、然後下載至您的本機機器（例如 Linux 機器或 Windows PC ）。

按一下以顯示

```
#Azure Cloud Shell on Azure portal to get VHD image from Azure
Marketplace
a) Set the URN and other parameters of the marketplace image. URN is
with format "<publisher>:<offer>:<sku>:<version>". Optionally, a
user can list NetApp marketplace images to confirm the proper image
version.
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
...

b) Create a new managed disk from the Marketplace image with the
matching image version
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

c) Export a VHD from the managed disk to Azure Storage
Create a container with proper access level. As an example, a
container named 'vm-images' with 'Container' access level is used
here.
Get storage account access key, on Azure portal, 'Storage
Accounts'/'examplesaname'/'Access Key'/'key1'/'key'/'show'/<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

d) Download the generated image to your server, e.g., a Linux
machine.
Use "wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>".
The URL is organized in a formatted way. For automation tasks, the
following example could be used to derive the URL string. Otherwise,
Azure CLI 'az' command could be issued to get the URL, which is not
covered in this guide. URL Example:
https://examplesaname.blob.core.windows.net/vm-
images/9150.01000024.05090105.vhd

e) Clean up the managed disk
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG
-DiskName $diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

從本機 **Linux** 機器透過 **Azure CLI** 匯出 **VHD** 檔案

1. 從本機 Linux 機器透過 Azure CLI 將市場映像匯出至 vhd 。

按一下以顯示

```
#Azure CLI on local Linux machine to get VHD image from Azure
Marketplace
a) Login Azure CLI and list marketplace images
% az login --use-device-code
To sign in, use a web browser to open the page
https://microsoft.com/devicelogin and enter the code XXXXXXXXX to
authenticate.

% 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"
},
...

b) Create a new managed disk from the Marketplace image with the
matching image version
% 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.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxx"
}

% export diskAccessSAS="https://md-
xxxxxx.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxx"
#To automate the process, the SAS needs to be extracted from the
standard output. This is not included in this guide.
```

```
c) export vhd from managed disk
Create a container with proper access level. As an example, a
container named 'vm-images' with 'Container' access level is used
here.
Get storage account access key, on Azure portal, 'Storage
Accounts'/'examplesaname'/'Access Key'/'key1'/'key'/'show'/<copy>.
There should be az command that can achieve the same, but this is
not included in this guide.
% 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": "\"0xXXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}

#to check the status of the blob copying
% 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.blob.core.windows.net/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
```

```
    },
....

d) Download the generated image to your server, e.g., a Linux
machine.
Use "wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>".
The URL is organized in a formatted way. For automation tasks, the
following example could be used to derive the URL string. Otherwise,
Azure CLI 'az' command could be issued to get the URL, which is not
covered in this guide. URL Example:
https://examplesaname.blob.core.windows.net/vm-
images/9150.01000024.05090105.vhd

e) Clean up the managed disk
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

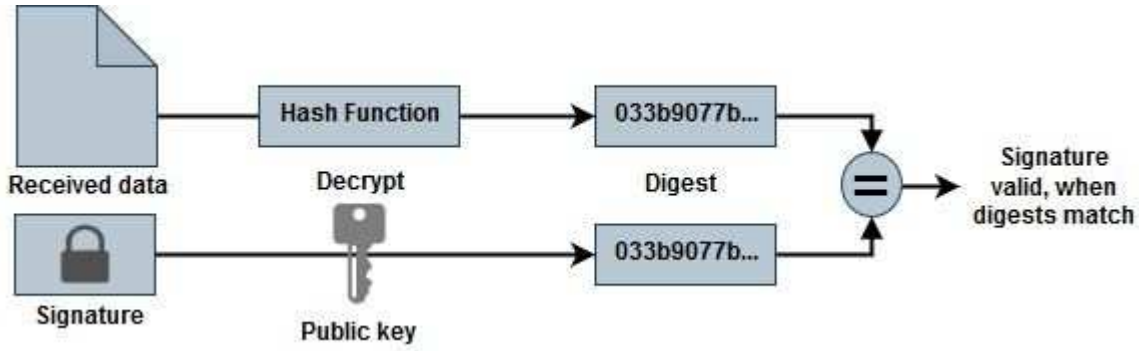
檔案簽章驗證

檔案簽章驗證

Azure 影像驗證程序將使用雜湊功能、從 VHD 檔案產生內含前導式 1MB 等量區塊的摘要、並結束 512B 等量區塊區塊區塊。為了符合簽署程序、使用 SHA256 進行雜湊。您需要從 VHD 檔案移除前導式 1MB 和最終版 512B 、然後驗證 VHD 檔案的其餘部分。

檔案簽章驗證工作流程摘要

以下是檔案簽章驗證工作流程程序的概觀。



- 從下載 Azure Image Digest 檔案 "NetApp 支援網站" 然後擷取摘要檔案（ .SIG ）、公開金鑰憑證檔案（ .pem ）和鏈結憑證檔案（ .pem ）。

  請參閱 "下載 Azure Image Digest File" 以取得更多資訊。

- 驗證信任鏈結。

- 從公開金鑰憑證（ .pem ）擷取公開金鑰（ .pub ）。
- 解壓縮的公開金鑰用於解密摘要檔案。然後將結果與從映像檔案建立的新未加密暫存檔案摘要進行比較、並移除前導式 1MB 與結尾 512 位元組的檔案。

  此步驟可透過下列 openssl 命令來達成。

  - 一般 CLI 聲明如下所示：

    ```
    openssl dgst -verify <public_key> -keyform <form> <hash_function>
    -signature <digest_file> -binary <temporary_file>
    ```

  - 如果檔案相符、則 Openssl CLI 工具會顯示「驗證成功」訊息、如果檔案不符、則會顯示「驗證失敗」訊息。

Linux 上的檔案簽章驗證

您可以依照下列步驟驗證匯出的 VHD 檔案簽章適用於 Linux 。

步驟

1. 從下載 Azure Image Digest 檔案 "NetApp 支援網站" 然後擷取摘要檔案（ .SIG ）、公開金鑰憑證檔案（ .pem ）和鏈結憑證檔案（ .pem ）。

   請參閱 "下載 Azure Image Digest File" 以取得更多資訊。

2. 驗證信任鏈結。

   ```
   % openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
   Certificate-9.15.0P1_azure.pem
   Certificate-9.15.0P1_azure.pem: OK
   ```

3. 移除前導的 1MB （ 1048576 位元組）、並結束 512 位元組的 VHD 檔案。

   如果使用「 tail 」、選項「 -c +K 」會以指定檔案的 KTH 位元組開始輸出位元組。因此、 1048577 會傳送至 '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 從憑證擷取公開金鑰、並使用簽章檔案和公開金鑰驗證等量分佈的檔案（ sign.tmp ）。

   如果輸入檔通過驗證、則會顯示命令
   " 驗證正常 " 。否則將顯示「驗證失敗」。

```
% 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
```

Mac OS 上的檔案簽章驗證

您可以依照下列步驟、驗證 Mac OS 匯出的 VHD 檔案簽章。

步驟

1. 從下載 Azure Image Digest 檔案 "NetApp 支援網站" 然後擷取摘要檔案（ .SIG ）、公開金鑰憑證檔案（ .pem ）和鏈結憑證檔案（ .pem ）。

   請參閱 "下載 Azure Image Digest File" 以取得更多資訊。

2. 驗證信任鏈結。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. 移除前導的 1MB （ 1048576 位元組）、並結束 512 位元組的 VHD 檔案。

   如果使用「 tail 」、選項「 -c +K 」會以 KTH 位元組開始輸出位元組
   指定檔案的。因此、 1048577 會傳送至 'tail -c 。大約需要 13 分鐘
   以在 Mac OS 上完成 tail 命令。

```
% 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 從憑證擷取公開金鑰、並驗證等量分割

檔案（ sign.tmp ）、含簽章檔案和公開金鑰。

如果輸入檔案通過驗證、命令會顯示「驗證正常」。
否則將顯示「驗證失敗」。

```
% 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
```

何處可以找到 **Azure** 影像驗證的其他資訊

如需 Azure 影像驗證的其他資訊、請參閱下列連結。以下連結將帶您前往非 NetApp 網站。

參考資料

- "網頁故障部落格：如何使用 OpenSSL 簽署及驗證"
- "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 Quickstart - Bash | Microsoft Learn"
- "如何安裝 Azure CLI | Microsoft Learn"
- "AZ 儲存資源膨脹複本 | Microsoft Learn"
- "使用 Azure CLI 登入：登入與驗證 | Microsoft Learn"

開始使用Google Cloud

在Google Cloud中快速入門Cloud Volumes ONTAP

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

1 建立連接器

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

請注意、如果您想要在Cloud Volumes ONTAP 無法存取網際網路的子網路中部署支援、則必須手動安裝Connector、並存取在該Connector上執行的BlueXP使用者介面。 "瞭解如何在無法存取網際網路的位置手動安裝Connector"

2 規劃您的組態

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

"深入瞭解規劃組態"。

3 設定您的網路

1. 確保您的 VPC 和子網路支援連接器與 Cloud Volumes ONTAP 支援之間的連線。
2. 如果您打算啟用資料分層、 "設定Cloud Volumes ONTAP 私有Google Access的子網路"。
3. 如果您要部署 HA 配對、請確定您有四個 VPC 、每個 VPC 都有自己的子網路。
4. 如果您使用的是共享VPC、請將_Compute Network User_角色提供給Connector服務帳戶。
5. 啟用從目標VPC for NetApp AutoSupport 的傳出網際網路存取功能。

   如果您在Cloud Volumes ONTAP 無法存取網際網路的位置部署支援、則不需要執行此步驟。

"深入瞭解網路需求"。

4 設定服務帳戶

下列兩種用途需要Google Cloud服務帳戶：Cloud Volumes ONTAP第一個是啟用時 "資料分層" 將冷資料分層至Google Cloud中的低成本物件儲存設備。第二個是啟用時 "BlueXP 備份與還原" 將磁碟區備份至低成本的物件儲存設備。

您可以設定一個服務帳戶、並將其用於這兩種用途。服務帳戶必須具有*儲存設備管理*角色。

"閱讀逐步指示"。

5 啟用 **Google Cloud API**

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

- Cloud Deployment Manager V2 API
- 雲端記錄 API
- Cloud Resource Manager API

- 運算引擎 API
- 身分識別與存取管理（ IAM ） API

6 使用**BlueXP**啟動**Cloud Volumes ONTAP**

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

相關連結

- "從BlueXP建立連接器"
- "在 Linux 主機上安裝 Connector 軟體"
- "BlueXP使用Google Cloud權限的功能"

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

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

選擇**Cloud Volumes ONTAP** 一個不含功能的授權

有多種授權選項可供Cloud Volumes ONTAP 選擇。每個選項都能讓您選擇符合需求的消費模式。

- "深入瞭Cloud Volumes ONTAP 解適用於此功能的授權選項"
- "瞭解如何設定授權"

選擇支援的地區

支援大部分Google Cloud地區的支援。Cloud Volumes ONTAP "檢視支援區域的完整清單"。

選擇支援的機器類型

根據您選擇的授權類型、支援多種機器類型。 Cloud Volumes ONTAP

"支援的GCP組態Cloud Volumes ONTAP"

瞭解儲存限制

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

"適用於GCP的儲存限制Cloud Volumes ONTAP"

在**GCP**中調整系統規模

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

機器類型

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

如需詳細資料、請參閱下列內容：

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

GCP 磁碟類型

當您建立 Cloud Volumes ONTAP 用於資料的 Volume 時、您需要選擇 Cloud Volumes ONTAP 基礎雲端儲存設備、以便將其用於磁碟。磁碟類型可以是下列任一種：

- *Zonal SSD*持續式磁碟：SSD持續式磁碟最適合需要高隨機IOPS速率的工作負載。
- 分區平衡的持續磁碟：這些SSD可提供較低的每GB IOPS、以平衡效能與成本。
- *Zonal Standard*持續式磁碟：標準持續式磁碟經濟實惠、可處理連續讀寫作業。

  如需詳細資料、請參閱 "Google Cloud 文件：分區持續磁碟（標準和 SSD ）"。

GCP 磁碟大小

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

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

  如需詳細資料、請參閱下列內容：

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

檢視預設系統磁碟

除了儲存使用者資料之外、BlueXP也購買雲端儲存設備來儲存Cloud Volumes ONTAP 作業系統資料（開機資料、根資料、核心資料和NVRAM）。為了規劃目的、在部署Cloud Volumes ONTAP 完更新之前、您可能需要先檢閱這些詳細資料。

- "在Cloud Volumes ONTAP Google Cloud中檢視系統資料的預設磁碟"。
- "Google Cloud文件：資源配額"

  Google Cloud Compute Engine會強制執行資源使用量配額、因此您應該在部署Cloud Volumes ONTAP 時確保未達到上限。

連接器也需要系統磁碟。 "檢視Connector預設組態的詳細資料"。

收集網路資訊

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

- 單節點系統的網路資訊 *

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

- 多個區域中 HA 配對的網路資訊 *

GCP 資訊	您的價值
區域	
節點 1 的區域	
節點 2 的區域	
中介人區域	
VPC-0 和子網路	
VPC-1 和子網路	
VPC-2 和子網路	
VPC-3 和子網路	
防火牆原則（如果使用您自己的）	

- 單一區域中 HA 配對的網路資訊 *

GCP 資訊	您的價值
區域	
區域	
VPC-0 和子網路	
VPC-1 和子網路	
VPC-2 和子網路	
VPC-3 和子網路	
防火牆原則（如果使用您自己的）	

選擇寫入速度

BlueXP可讓您選擇Cloud Volumes ONTAP 適合的寫入速度設定、但Google Cloud中的高可用度（HA）配對除外。在您選擇寫入速度之前、您應該先瞭解一般與高設定之間的差異、以及使用高速寫入速度時的風險與建議。"深入瞭解寫入速度"。

選擇**Volume**使用設定檔

包含多項儲存效率功能、可減少您所需的總儲存容量。 ONTAP在BlueXP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。您應該深入瞭解這些功能、以協助您決定要使用的設定檔。

NetApp 儲存效率功能提供下列效益：

資源隨需配置

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

重複資料刪除

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

壓縮

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

Google Cloud中的功能需求Cloud Volumes ONTAP

設定您的Google Cloud網路功能、Cloud Volumes ONTAP 讓各個系統都能正常運作。

如果您想要部署 HA 配對、應該這樣做 "瞭解HA配對如何在Google Cloud中運作"。

需求 **Cloud Volumes ONTAP**

Google Cloud必須符合下列要求。

單一節點系統的特定需求

如果您要部署單一節點系統、請確定您的網路符合下列需求。

一個**VPC**

單一節點系統需要一個虛擬私有雲（VPC）。

私有**IP**位址

BlueXP會將3或4個私有IP位址分配給Google Cloud中的單一節點系統。

如果Cloud Volumes ONTAP 您使用API部署了Sf2並指定下列旗標、則可以跳過儲存VM（SVM）管理LIF的建立：

「kipSvmManagementLif: true」

LIF 是與實體連接埠相關聯的 IP 位址。諸如VMware等管理工具需要儲存VM（SVM）管理LIF SnapCenter 。

HA配對的特定需求

如果您要部署HA配對、請確定您的網路符合下列需求。

一個或多個區域

您可以跨多個區域或單一區域部署HA組態、確保資料的高可用度。建立HA配對時、BlueXP會提示您選擇多個區域或單一區域。

- 多個區域（建議）

  跨三個區域部署 HA 組態、可確保在區域內發生故障時、仍能持續提供資料。請注意、與使用單一區域相比、寫入效能略低、但卻是最低的。

- 單一區域

  當部署在單一區域時、 Cloud Volumes ONTAP 使用分散配置原則的即可實現不受限制的 HA 組態。此原則可確保 HA 組態不會在區域內發生單點故障、而無需使用個別區域來實現故障隔離。

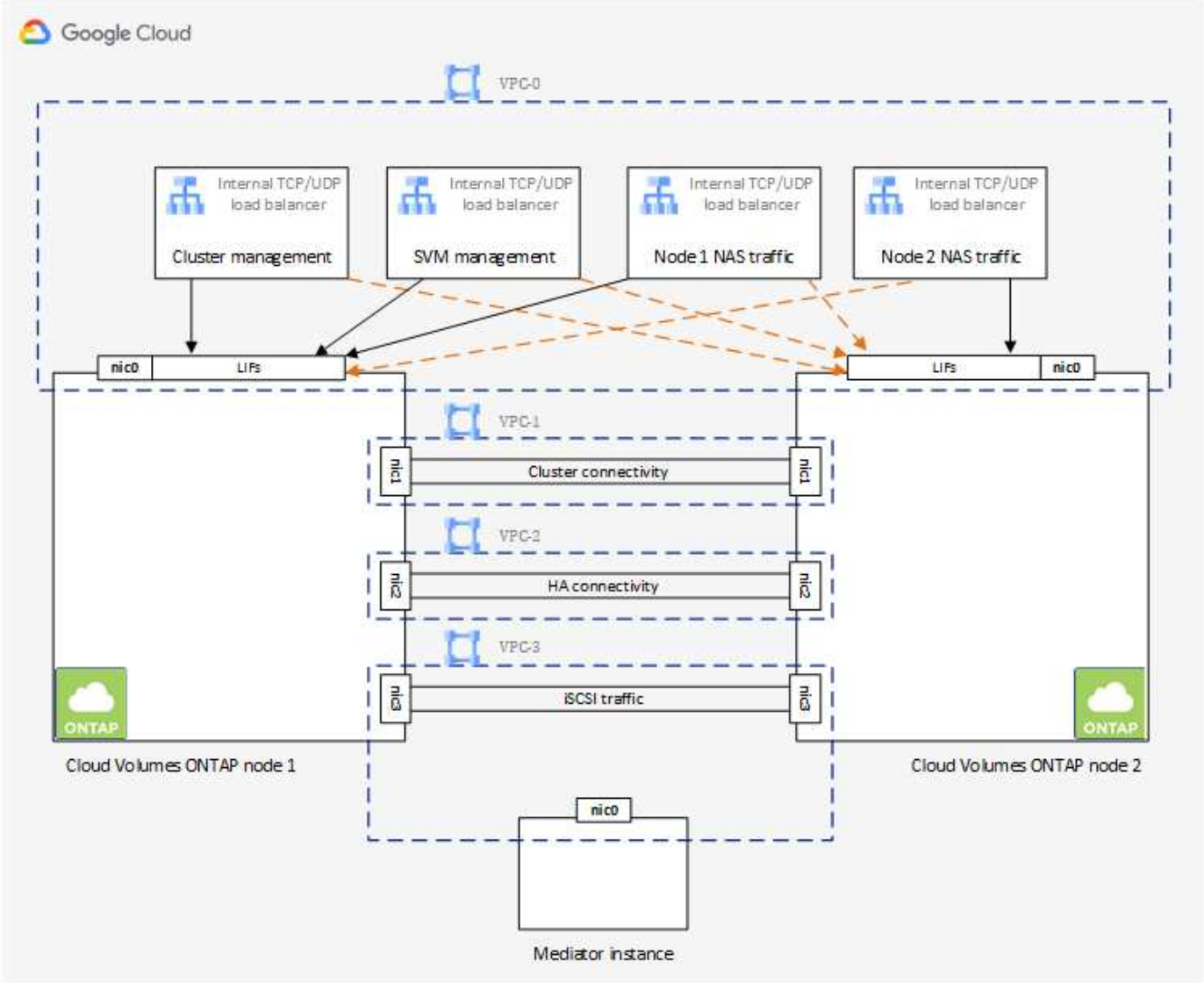
  此部署模式可降低成本、因為各區域之間不需支付任何資料出口費用。

四個虛擬私有雲端

HA組態需要四個虛擬私有雲端（VPC）。由於Google Cloud要求每個網路介面都位於獨立的VPC網路、因此需要四個VPC。

在建立HA配對時、BlueXP會提示您選擇四個VPC：

- VPC-0 用於資料和節點的傳入連線
- VPC-1 、 VPC-2 和 VPC-3 用於節點與 HA 中介器之間的內部通訊



子網路

每個VPC都需要私有子網路。

如果您將Connector放在VPC-0中、則必須在子網路上啟用私有Google Access、才能存取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。

私有**IP**位址

在Cloud Volumes ONTAP Google Cloud中、BlueXP會自動分配所需數量的私有IP位址給功能。您必須確定網路有足夠的私有位址可供使用。

BlueXP分配Cloud Volumes ONTAP 給功能的生命量取決於您是部署單一節點系統或HA配對。LIF 是與實體連接埠相關聯的 IP 位址。諸如 VMware 的管理工具需要 SVM 管理 LIF SnapCenter 。

- 單一節點 BlueXP會將4個IP位址分配給單一節點系統：
  - 節點管理 LIF

- 叢集管理LIF
- iSCSI資料LIF

  iSCSI LIF可透過iSCSI傳輸協定提供用戶端存取、並供系統用於其他重要的網路工作流程。這些生命是必要的、不應刪除。

- NAS LIF

  如果Cloud Volumes ONTAP 您使用API部署了Sf2並指定下列旗標、則可以跳過儲存VM（SVM）管理LIF的建立：

「kipSvmManagementLif: true」

- * HA配對* BlueXP會將12-13個IP位址分配給HA配對：
  - 2個節點管理生命里數（e0a）
  - 1叢集管理LIF（e0a）
  - 2個iSCSI LIF（e0a）

    iSCSI LIF可透過iSCSI傳輸協定提供用戶端存取、並供系統用於其他重要的網路工作流程。這些生命是必要的、不應刪除。

  - 1或2個NAS lifs（e0a）
  - 2個叢集LIF（e0b）
  - 2個HA互連IP位址（e0c）
  - 2個RSMiSCSI IP位址（e0d）

    如果Cloud Volumes ONTAP 您使用API部署了Sf2並指定下列旗標、則可以跳過儲存VM（SVM）管理LIF的建立：

「kipSvmManagementLif: true」

內部負載平衡器

BlueXP會自動建立四個Google Cloud內部負載平衡器（TCP/IP）、以管理Cloud Volumes ONTAP 傳入至該HA配對的流量。您不需要在結束時進行任何設定我們將此列為一項要求、只是告知您網路流量、並減輕任何安全顧慮。

其中一個負載平衡器用於叢集管理、一個用於儲存VM（SVM）管理、一個用於連接節點1的NAS流量、最後一個用於連接節點2的NAS流量。

每個負載平衡器的設定如下：

- 一個共享的私有IP位址
- 一次全域健全狀況檢查

  根據預設、狀況檢查所使用的連接埠為63001、63002和63003。

- 一個區域TCP後端服務
- 一個區域性的udp後端服務
- 一個TCP轉送規則
- 一個udp轉送規則
- 全域存取已停用

  即使預設停用全域存取、仍支援在部署後啟用IT。我們停用此功能、因為跨區域流量的延遲時間會大幅增加。我們希望確保您不會因為意外的跨區域裝載而有負面體驗。啟用此選項是專為您的業務需求所打造。

共享VPC

支援的對象包括 Google Cloud 共享 VPC 和獨立 VPC 。 Cloud Volumes ONTAP

對於單一節點系統、VPC可以是共享VPC或獨立VPC。

HA配對需要四個VPC。每個VPC都可以是共享的或獨立的。例如、VPC-0可以是共享VPC、VPC-1、VPC-2和VPC-3則可以是獨立式VPC。

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

"檢閱Connector部署所涵蓋的必要共享VPC權限"

VPC中的封包鏡射

"封包鏡射" 您必須在部署 Cloud Volumes ONTAP 的 Google Cloud 子網路中停用。啟用封包鏡射時、無法正常運作。Cloud Volumes ONTAP

傳出網際網路存取

NetApp支援需要外傳網際網路存取功能、才能主動監控系統健全狀況、並將訊息傳送給NetApp技術支援部門。Cloud Volumes ONTAP AutoSupport

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

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

如果傳出的網際網路連線無法傳送AutoSupport 功能性訊息、則BlueXP會自動將Cloud Volumes ONTAP 您的功能性更新系統設定為使用Connector做為Proxy伺服器。唯一的需求是確保連接器的防火牆允許連接埠3128上的傳入連線。部署Connector之後、您需要開啟此連接埠。

如果您定義了Cloud Volumes ONTAP 嚴格的出站規則以供支援、那麼您也必須確保Cloud Volumes ONTAP 透過連接埠3128建立的支援_出站_連線。

在您確認可以存取傳出網際網路之後、您可以測試AutoSupport 以確保能夠傳送訊息。如需相關指示、請參閱 "文件：設定檔ONTAP AutoSupport"。

如果您使用 HA 配對、 HA 中介器不需要傳出網際網路存取。

如果BlueXP通知您AutoSupport 無法傳送資訊、 "疑難排解AutoSupport 您的VMware組態"。

防火牆規則

您不需要建立防火牆規則、因為BlueXP會為您執行這些規則。如果您需要使用自己的防火牆、請參閱下列防火牆規則。

請注意、 HA 組態需要兩組防火牆規則：

- VPC-0 中 HA 元件的一組規則。這些規則可讓您存取 Cloud Volumes ONTAP 資料以存取資料。 深入瞭解。
- VPC-1 、 VPC-2 和 VPC-3 中的另一組 HA 元件規則。這些規則可用於 HA 元件之間的傳入和傳出通訊。 深入瞭解。

如果您想要將冷資料分層至 Google Cloud Storage 資源桶、 Cloud Volumes ONTAP 則必須將駐留的子網路設定為私有 Google Access （如果您使用 HA 配對、則此子網路位於 VPC-0 ）。如需相關指示、請參閱 "Google Cloud 文件：設定私有 Google Access"。

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

連線 **ONTAP** 至其他網路中的不二系統

若要在Cloud Volumes ONTAP Google Cloud中的某個支援中心系統與ONTAP 其他網路中的支援中心系統之間複寫資料、您必須在VPC與其他網路（例如公司網路）之間建立VPN連線。

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

防火牆規則

BlueXP會建立Google Cloud防火牆規則、其中包括Cloud Volumes ONTAP 需要順利運作的傳入和傳出規則。您可能想要參考連接埠以進行測試、或是想要使用自己的防火牆規則。

適用於此功能的防火牆規則 Cloud Volumes ONTAP 需要傳入和傳出規則。如果您要部署 HA 組態、 Cloud Volumes ONTAP 以下是 VPC-0 中的防火牆規則。

請注意、 HA 組態需要兩組防火牆規則：

- VPC-0 中 HA 元件的一組規則。這些規則可讓您存取 Cloud Volumes ONTAP 資料以存取資料。
- VPC-1 、 VPC-2 和 VPC-3 中的另一組 HA 元件規則。這些規則可用於 HA 元件之間的傳入和傳出通訊。 深入瞭解。

正在尋找Connector的相關資訊？ "檢視Connector的防火牆規則"

傳入規則

建立工作環境時、您可以在部署期間選擇預先定義防火牆原則的來源篩選器：

- *限選定VPC *：傳入流量的來源篩選器為VPC的子網路範圍、Cloud Volumes ONTAP 適用於該系統、以及連接器所在VPC的子網路範圍。這是建議的選項。

- 所有**VPC**：傳入流量的來源篩選器為0.00.0.0/0 IP範圍。

如果您使用自己的防火牆原則、請確定您新增了所有需要與Cloud Volumes ONTAP 之通訊的網路、但同時也請務必新增這兩個位址範圍、以讓內部Google負載平衡器正常運作。這些位址分別為130.211.0.0/22和35.191.0/16。如需詳細資訊、請參閱 "Google Cloud文件：負載平衡器防火牆規則"。

傳輸協定	連接埠	目的
所有ICMP	全部	Ping 執行個體
HTTP	80	使用叢集管理 LIF 的 IP 位址、以 HTTP 存取 System Manager Web 主控台
HTTPS	443..	使用叢集管理LIF的IP位址、連線到Connector和HTTPS、存取System Manager Web主控台
SSH	22	SSH 存取叢集管理 LIF 的 IP 位址或節點管理 LIF
TCP	111.	遠端程序需要 NFS
TCP	139.	CIFS 的 NetBios 服務工作階段
TCP	161-162	簡單的網路管理傳輸協定
TCP	445	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
TCP	635	NFS 掛載
TCP	749	Kerberos
TCP	2049	NFS 伺服器精靈
TCP	3260	透過 iSCSI 資料 LIF 存取 iSCSI
TCP	4045	NFS 鎖定精靈
TCP	4046	NFS 的網路狀態監控
TCP	10000	使用 NDMP 備份
TCP	11104.	管理 SnapMirror 的叢集間通訊工作階段
TCP	11105.	使用叢集間生命體進行 SnapMirror 資料傳輸
TCP	63001-63050	負載平衡探針連接埠、判斷哪個節點正常（僅 HA 配對需要）
UDP	111.	遠端程序需要 NFS
UDP	161-162	簡單的網路管理傳輸協定
UDP	635	NFS 掛載
UDP	2049	NFS 伺服器精靈
UDP	4045	NFS 鎖定精靈
UDP	4046	NFS 的網路狀態監控
UDP	4049	NFS rquotad 傳輸協定

傳出規則

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

基本傳出規則

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

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

進階傳出規則

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

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

服務	傳輸協定	連接埠	來源	目的地	目的
Active Directory	TCP	88	節點管理 LIF	Active Directory 樹系	Kerberos V 驗證
	UDP	137.	節點管理 LIF	Active Directory 樹系	NetBios 名稱服務
	UDP	138	節點管理 LIF	Active Directory 樹系	NetBios 資料報服務
	TCP	139.	節點管理 LIF	Active Directory 樹系	NetBios 服務工作階段
	TCP 與 UDP	389	節點管理 LIF	Active Directory 樹系	LDAP
	TCP	445	節點管理 LIF	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	TCP	464. 64	節點管理 LIF	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	UDP	464. 64	節點管理 LIF	Active Directory 樹系	Kerberos 金鑰管理
	TCP	749	節點管理 LIF	Active Directory 樹系	Kerberos V 變更與設定密碼（ RPCSEC_GSS ）
	TCP	88	資料 LIF （ NFS 、 CIFS 、 iSCSI ）	Active Directory 樹系	Kerberos V 驗證
	UDP	137.	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 名稱服務
	UDP	138	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 資料報服務
	TCP	139.	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	NetBios 服務工作階段
	TCP 與 UDP	389	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	LDAP
	TCP	445	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	TCP	464. 64	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos V 變更及設定密碼（ Set_change ）
	UDP	464. 64	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos 金鑰管理
	TCP	749	資料 LIF （ NFS 、 CIFS ）	Active Directory 樹系	Kerberos V 變更及設定密碼（ RPCSEC_GSS ）
AutoSupport	HTTPS	443..	節點管理 LIF	support.netapp.com	支援（預設為HTTPS）AutoSupport
	HTTP	80	節點管理 LIF	support.netapp.com	僅當傳輸傳輸傳輸傳輸傳輸傳輸協定從HTTPS變更為HTTP 時、AutoSupport
	TCP	3128	節點管理 LIF	連接器	如果無法使用傳出的網際網路連線、請透過Connector上的Proxy伺服器傳送AutoSupport 功能介紹訊息

服務	傳輸協定	連接埠	來源	目的地	目的
叢集	所有流量	所有流量	一個節點上的所有 LIF	其他節點上的所有 LIF	叢集間通訊（ Cloud Volumes ONTAP 僅限不含 HA ）
組態備份	HTTP	80	節點管理 LIF	\http ：//Wese/occm/offboxconfig <connector-IP-address>	將組態備份傳送至Connector。 "深入瞭解組態備份檔案"。
DHCP	UDP	68	節點管理 LIF	DHCP	第一次設定的 DHCP 用戶端
DHCPS	UDP	67	節點管理 LIF	DHCP	DHCP 伺服器
DNS	UDP	53.	節點管理 LIF 與資料 LIF （ NFS 、 CIFS ）	DNS	DNS
NDMP	TCP	18600 – 18699	節點管理 LIF	目的地伺服器	NDMP 複本
SMTP	TCP	25	節點管理 LIF	郵件伺服器	可以使用 SMTP 警示 AutoSupport 來執行功能
SNMP	TCP	161.	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	UDP	161.	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	TCP	162 %	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	UDP	162 %	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
SnapMirror	TCP	11104.	叢集間 LIF	叢集間 LIF ONTAP	管理 SnapMirror 的叢集間通訊工作階段
	TCP	11105.	叢集間 LIF	叢集間 LIF ONTAP	SnapMirror 資料傳輸
系統記錄	UDP	514	節點管理 LIF	系統記錄伺服器	系統記錄轉送訊息

VPC-1、**VPC-2**和**VPC-3**的規則

在Google Cloud中、HA組態部署於四個VPC上。VPC-0 中 HA 組態所需的防火牆規則為 以上所列 Cloud Volumes ONTAP 的 for 列舉。

同時、BlueXP針對VPC-1、VPC-2和VPC-3中的執行個體所建立的預先定義防火牆規則、可透過_all_傳輸協定和連接埠進行入侵通訊。這些規則可在HA節點之間進行通訊。

HA節點與HA中介器之間的通訊會透過連接埠3260（iSCSI）進行。

若要為新的Google Cloud HA配對部署啟用高速寫入速度、VPC-1、VPC-2和VPC-3至少需要8、896位元組的最大傳輸單元（MTU）。如果您選擇將現有VPC-1、VPC-2和VPC-3升級為8、896位元組的MTU、則必須在組態程序期間使用這些VPC關閉所有現有的HA系統。

連接器需求

如果您尚未建立連接器、也應該檢閱連接器的網路需求。

- "檢視連接器的網路需求"
- "Google Cloud中的防火牆規則"

在GCP中規劃VPC服務控制

選擇使用VPC服務控制來鎖定Google Cloud環境時、您應該瞭解BlueXP和Cloud Volumes ONTAP Isa如何與Google Cloud API互動、以及如何設定服務邊界以部署BlueXP和Cloud Volumes ONTAP Isa。

VPC服務控管可讓您控制在信任邊界之外存取Google管理的服務、封鎖來自不信任位置的資料存取、並降低未獲授權的資料傳輸風險。 "深入瞭解Google Cloud VPC服務控制"。

NetApp服務如何與VPC服務控制通訊

BlueXP直接與Google Cloud API通訊。這可能是從Google Cloud外部的外部IP位址觸發（例如從api.services.cloud.netapp.com）、或從指派給BlueXP Connector的內部位址觸發。

視連接器的部署風格而定、您可能需要針對服務邊界進行某些例外。

映像

支援使用NetApp管理的GCP專案影像。Cloud Volumes ONTAP如果Cloud Volumes ONTAP 您的組織有封鎖使用組織內未託管之映像的原則、這可能會影響到BlueXP Connector和功能的部署。

您可以使用手動安裝方法手動部署Connector、Cloud Volumes ONTAP 但也需要從NetApp專案中擷取影像。您必須提供允許的清單、才能部署連接器和Cloud Volumes ONTAP 功能表。

部署Connector

部署Connector的使用者必須能夠參考專案ID *NetApp-cloudmanag__*中裝載的映像、以及專案編號*_14190056516*。

部署Cloud Volumes ONTAP 功能

- BlueXP服務帳戶需要參考專案ID *NetApp-cloudmanager-_*中的映像、以及服務專案中的專案編號*_14190056516*。
- 預設Google API服務代理程式的服務帳戶必須參考專案ID *NetApp-cloudmanag__*中所裝載的映像、以及服務專案中的專案編號*_14190056516*。

以下是使用VPC服務控制擷取這些影像所需的規則範例。

VPC服務控制周邊原則

原則允許VPC服務控制規則集例外。如需原則的詳細資訊、請參閱 "GCP VPC服務控制原則文件"。

若要設定BlueXP所需的原則、請瀏覽至組織內部的VPC服務控制周邊、然後新增下列原則。這些欄位應符合VPC服務控制原則頁面中提供的選項。另請注意、* all *規則是必要的、且*或*參數應用於規則集中。

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

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

或

```
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
```

上述專案編號是NetApp用來儲存Connector和Cloud Volumes ONTAP for the SURO影像的專案_NetApp-cloudmanag__。

建立資料分層與備份的服務帳戶

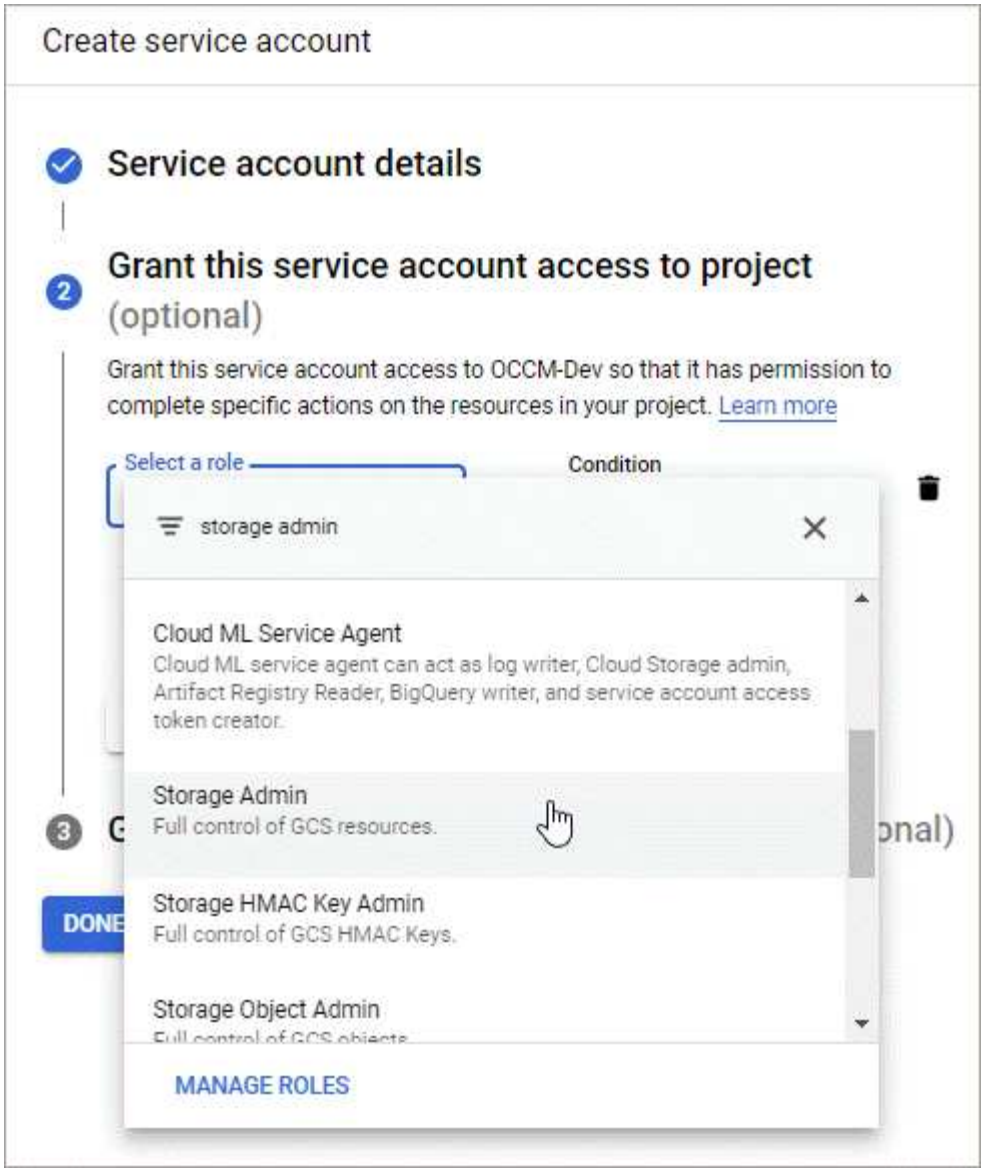
下列兩種用途需要Google Cloud服務帳戶：Cloud Volumes ONTAP第一個是啟用時 "資料分層" 將冷資料分層至Google Cloud中的低成本物件儲存設備。第二個是啟用時 "BlueXP 備份與還原" 將磁碟區備份至低成本的物件儲存設備。

使用服務帳戶存取及管理階層資料的儲存庫、以及另一個儲存庫進行備份。Cloud Volumes ONTAP

您可以設定一個服務帳戶、並將其用於這兩種用途。服務帳戶必須具有*儲存設備管理*角色。

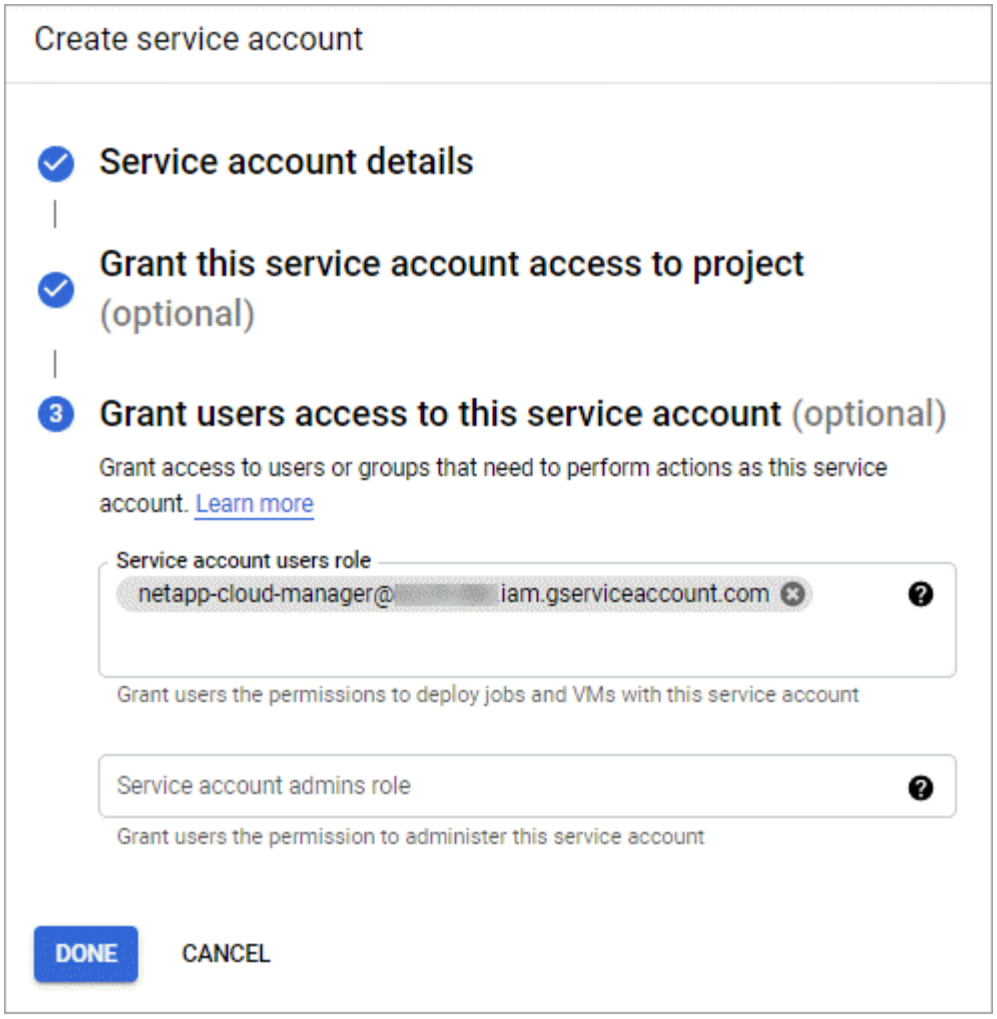
步驟

1. 在Google Cloud主控台中、 "前往「服務帳戶」頁面"。
2. 選取您的專案。
3. 按一下「建立服務帳戶」、並提供必要資訊。
    a. 服務帳戶詳細資料：輸入名稱和說明。
    b. 授予此服務帳戶專案存取權：選取*儲存管理員*角色。



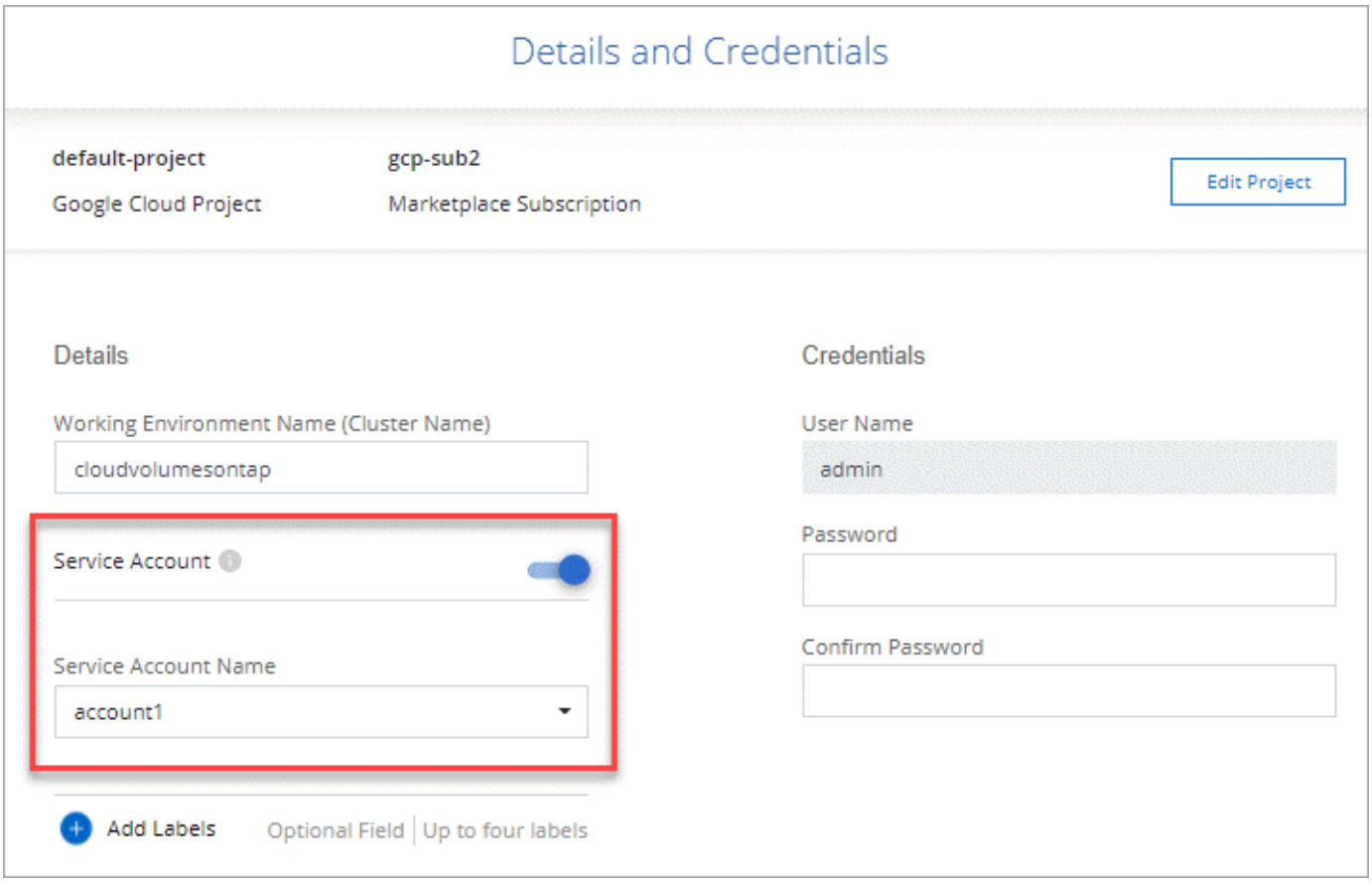
c. 授予使用者此服務帳戶的存取權：將Connector服務帳戶新增為_Service Account User_至此新的服務帳戶。

此步驟僅適用於資料分層。BlueXP 備份與還原不需要此功能。



接下來呢？

建立Cloud Volumes ONTAP 一套運作環境時、您稍後需要選擇服務帳戶。



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

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

步驟

1. 確認BlueXP Connector服務帳戶在專案層級（儲存金鑰的專案）擁有正確的權限。

   權限會在中提供 "連接器服務帳戶權限依預設"、但如果您使用雲端金鑰管理服務的替代專案、則可能無法套用。

   權限如下：

   ```
   - cloudkms.cryptoKeyVersions.useToEncrypt
   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.list
   ```

2. 確認的服務帳戶 "Google Compute Engine服務代理程式" 具有金鑰的Cloud KMS Encrypter/Dec供 解密權限。

   服務帳戶名稱使用下列格式：「service-[service_project _number]@ compute-system.iam.gserviceaccount.com」。

"Google Cloud文件：使用IAM搭配Cloud KMS使用-授予資源角色"

3. 若要取得金鑰的「ID」、請叫用「/GCP / VSA /中繼資料/ GCP加密金鑰」API呼叫的「Get」命令、或在GCP主控台的金鑰上選擇「Copy Resource Name」（複製資源名稱）。
4. 如果使用客戶管理的加密金鑰和分層資料來物件儲存設備、則BlueXP會嘗試使用相同的金鑰來加密持續磁碟。但您必須先啟用Google Cloud Storage儲存桶、才能使用這些金鑰：

   a. 請依照下列步驟尋找Google Cloud Storage服務代理程式 "Google Cloud文件：取得Cloud Storage服務代理程式"。

   b. 瀏覽至加密金鑰、並指派具有Cloud KMS Encrypter/Decypter權限的Google Cloud Storage服務代理程式。

   如需詳細資訊、請參閱 "Google Cloud文件：使用客戶管理的加密金鑰"

5. 建立工作環境時、請將「 GcpEncryption 」參數搭配 API 要求使用。

   。範例 *

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-1/cryptoKeys/generatedkey1"
  }
```

請參閱 "藍圖XP自動化文件" 如需使用「 GcpEncryption 」參數的詳細資訊、

在Cloud Volumes ONTAP Google Cloud中設定適用於此技術的授權

決定Cloud Volumes ONTAP 要搭配使用哪種授權選項之後、您必須先執行幾個步驟、才能在建立新的工作環境時選擇授權選項。

Freemium

選擇Freemium產品、即可免費使用Cloud Volumes ONTAP 多達500 GiB的配置容量。 "深入瞭解Freemium產品"。

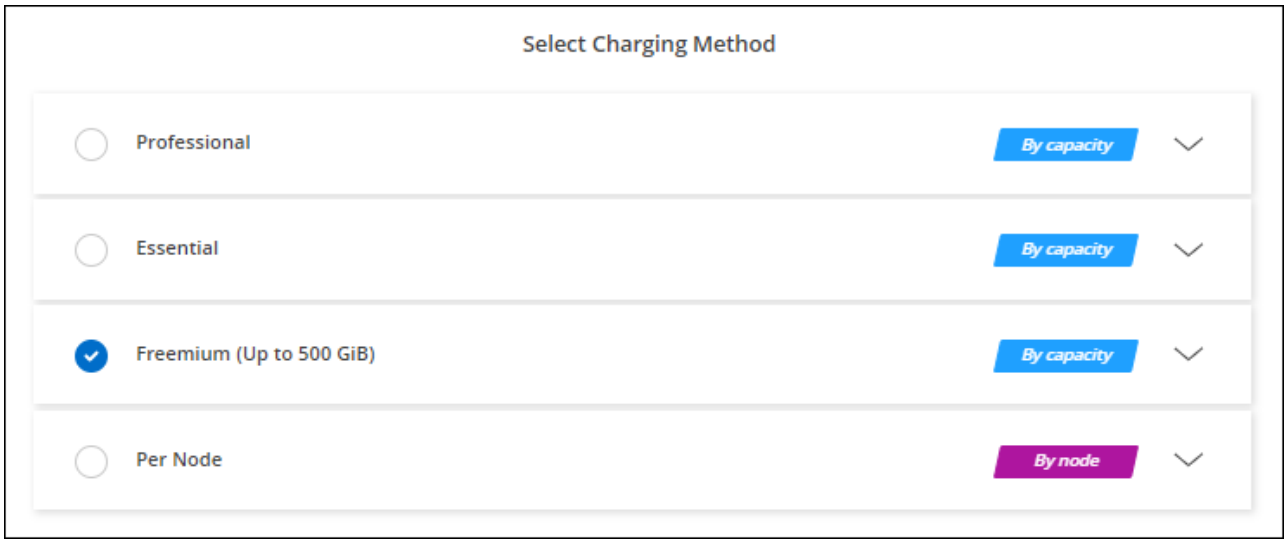
步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。

   a. 在*詳細資料與認證*頁面上、按一下*編輯認證>新增訂閱*、然後依照提示訂閱Google Cloud Marketplace中的隨用隨付方案。

      除非您超過500 GiB的已配置容量、系統會自動轉換為、否則不會透過市場訂閱付費 "Essentials套件"。

   b. 返回BluetXP之後、當您到達「充電方法」頁面時、請選取* Freemium *。



"請參閱逐步指示Cloud Volumes ONTAP 、在Google Cloud中啟動「功能不全」"。

容量型授權

容量型授權可讓您針對Cloud Volumes ONTAP 容量的每個TiB付費。容量型授權的形式為_package_：Essentials套件或Professional套件。

Essentials和Professional套件可搭配下列消費模式使用：

- 向NetApp購買的授權（BYOL）
- 從Google Cloud Marketplace訂閱時數小時隨付（PAYGO）
- 年度合約

"深入瞭解容量型授權"。

下列各節將說明如何開始使用這些消費模式。

BYOL

事先向NetApp購買授權（BYOL）、即可在Cloud Volumes ONTAP 任何雲端供應商部署支援系統。

步驟

1. "請聯絡NetApp銷售人員以取得授權"
2. "將NetApp 支援網站 您的不更新帳戶新增至藍圖XP"

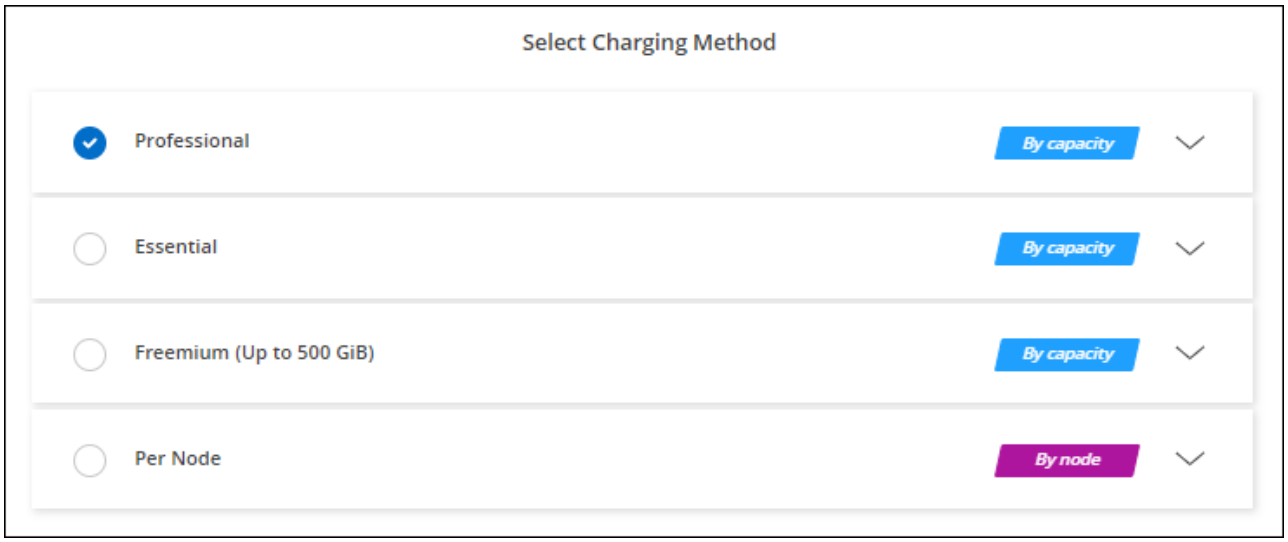
   BlueXP會自動查詢NetApp的授權服務、以取得NetApp 支援網站 與您的還原帳戶相關之授權的詳細資料。如果沒有錯誤、 BlueXP 會自動將授權新增至數位錢包。

   您必須先從 BlueXP 數位錢包取得授權、才能搭配 Cloud Volumes ONTAP 使用。如有需要、您可以 "手動將授權新增至 BlueXP 數位錢包"。

3. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。
   a. 在*詳細資料與認證*頁面上、按一下*編輯認證>新增訂閱*、然後依照提示訂閱Google Cloud Marketplace中的隨用隨付方案。

您向NetApp購買的授權一律會先收取費用、但如果您超過授權容量或授權到期、則會從市場的每小時費率中收取費用。

b. 返回BlueXP之後、當您到達「充電方法」頁面時、請選取容量型套件。



"請參閱逐步指示Cloud Volumes ONTAP 、在Google Cloud中啟動「功能不全」"。

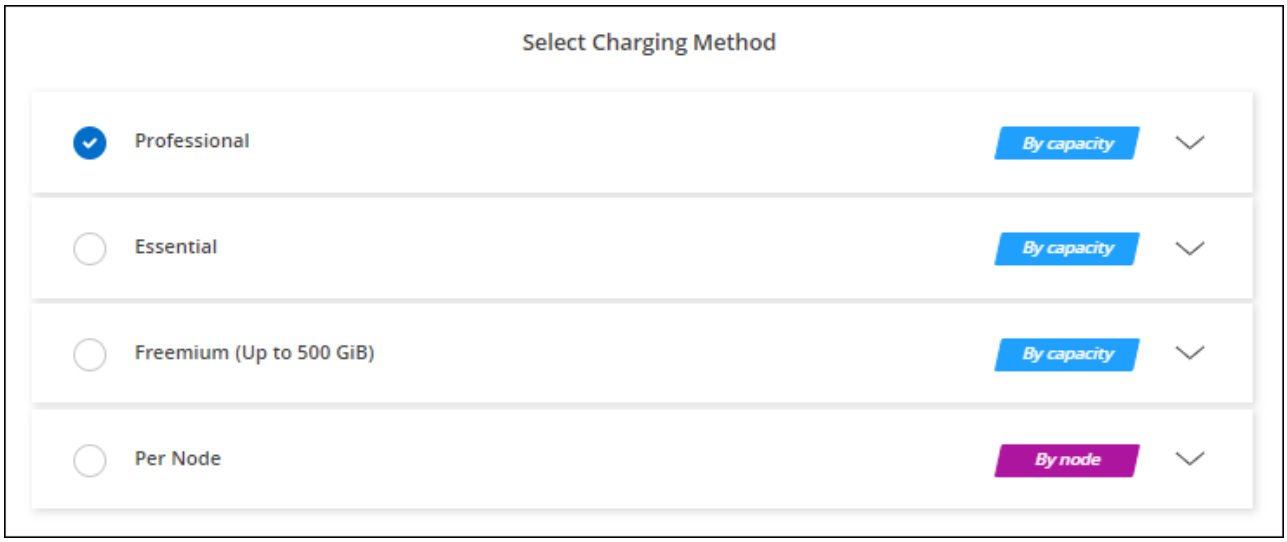
PAYGO訂閱

從雲端供應商的市場訂閱優惠、每小時支付一次。

當您建立Cloud Volumes ONTAP 一個運作環境時、BlueXP會提示您訂閱Google Cloud Marketplace提供的合約。該訂閱之後會與工作環境建立關聯、以便進行充電。您可以在其他工作環境中使用相同的訂閱。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。
   a. 在*詳細資料與認證*頁面上、按一下*編輯認證>新增訂閱*、然後依照提示訂閱Google Cloud Marketplace中的隨用隨付方案。
   b. 返回BlueXP之後、當您到達「充電方法」頁面時、請選取容量型套件。



"請參閱逐步指示Cloud Volumes ONTAP 、在Google Cloud中啟動「功能不全」"。

您可以從「設定」>「認證」頁面管理與您帳戶相關的Google Cloud Marketplace訂閱。 "瞭解如何管理您的Google Cloud認證與訂閱"

年度合約

購買年度合約、每年支付Cloud Volumes ONTAP 一份銷售費。

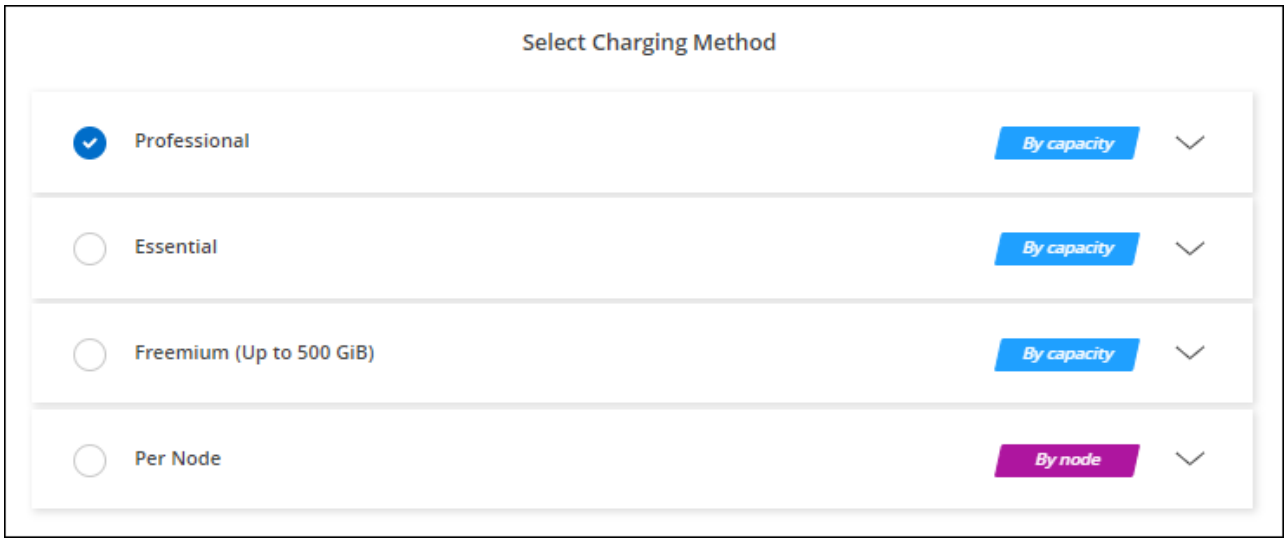
步驟

1. 請聯絡您的NetApp銷售代表以購買年度合約。

   合約可在Google Cloud Marketplace以_Private _優惠形式提供。

   在NetApp與您分享私人優惠之後、您可以在工作環境建立期間、從Google Cloud Marketplace訂閱年度方案。

2. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。
   a. 在*詳細資料與認證*頁面上、按一下*編輯認證>新增訂閱*、然後依照提示在Google Cloud Marketplace訂閱年度計畫。
   b. 在Google Cloud中、選取與您的帳戶共享的年度計畫、然後按一下*訂閱*。
   c. 返回BlueXP之後、當您到達「充電方法」頁面時、請選取容量型套件。



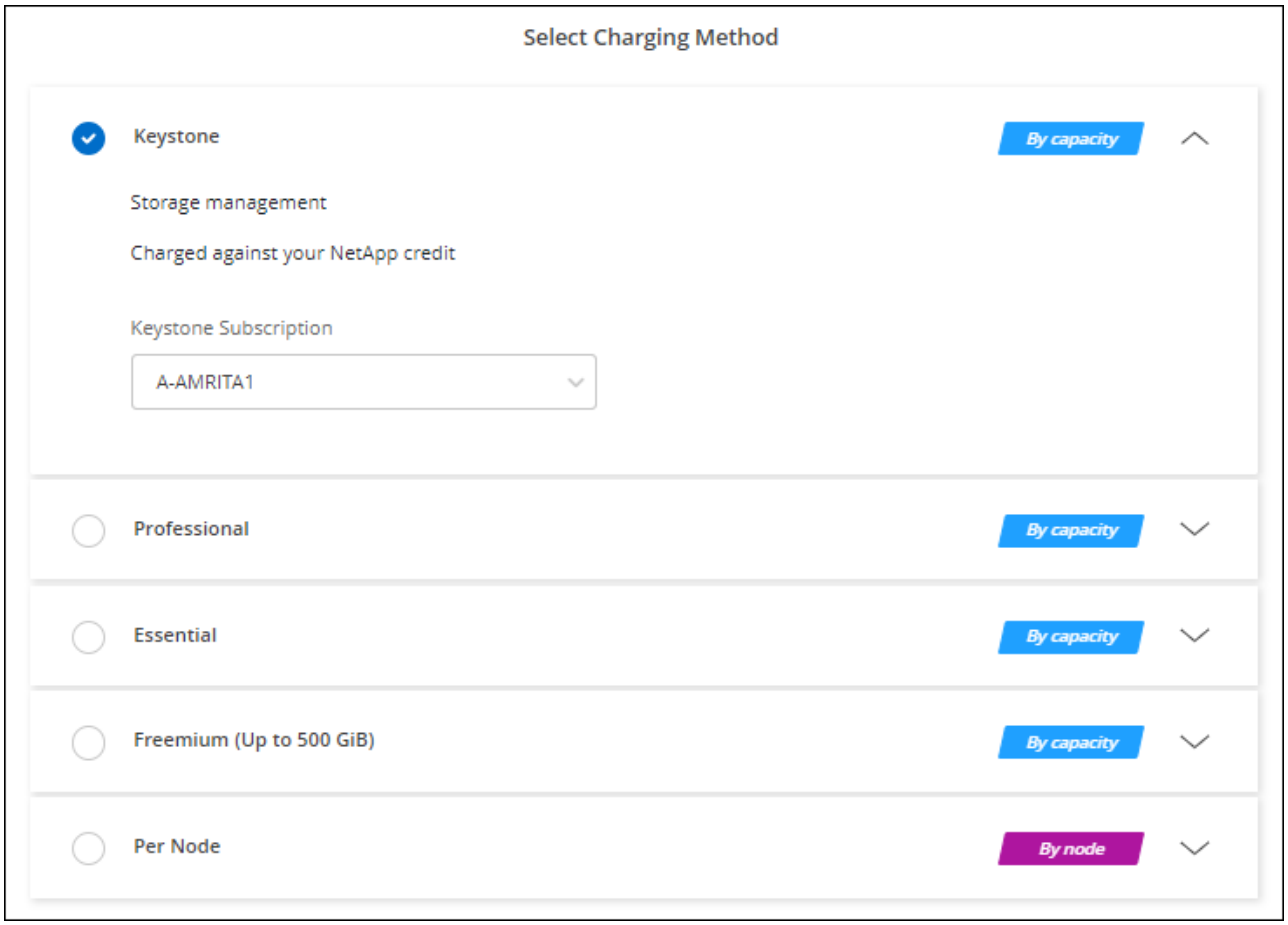
"請參閱逐步指示Cloud Volumes ONTAP 、在Google Cloud中啟動「功能不全」"。

Keystone訂閱

Keystone 訂閱是一項隨成長付費訂閱服務。 "深入瞭解 NetApp Keystone 訂閱"。

步驟

1. 如果您尚未訂閱、 "請聯絡NetApp"
2. mailto ： ng-keystone-success@netapp.com [聯絡 NetApp] 以使用一或多個 Keystone 訂閱來授權您的 BlueXP 使用者帳戶。
3. NetApp授權您的帳戶之後、 "連結您的訂閱內容以供Cloud Volumes ONTAP 搭配使用"。
4. 在「畫版」頁面上、按一下「新增工作環境」、然後依照BlueXP中的步驟進行。
   a. 當系統提示您選擇充電方法時、請選取 Keystone Subscription 充電方法。



"請參閱逐步指示Cloud Volumes ONTAP 、在Google Cloud中啟動「功能不全」"。

在Cloud Volumes ONTAP Google Cloud上啟動

您可以Cloud Volumes ONTAP 在單一節點組態中或在Google Cloud中以HA配對的形式啟動功能。

開始之前

您需要下列項目才能建立工作環境。

- 已啟動並執行的連接器。
  - 您應該擁有 "與工作區相關的連接器"。
  - "您應該隨時準備好讓 Connector 保持運作"。
  - 與 Connector 相關的服務帳戶 "應具備所需的權限"
- 瞭解您要使用的組態。

  您應該已做好準備、選擇組態、並向系統管理員取得Google Cloud網路資訊。如需詳細資訊、請參閱 "規劃 Cloud Volumes ONTAP 您的需求組態"。

- 瞭解設定Cloud Volumes ONTAP 驗證功能所需的條件。

"瞭解如何設定授權"。

- Google Cloud API應該是 "在您的專案中啟用"：
  - Cloud Deployment Manager V2 API
  - 雲端記錄 API
  - Cloud Resource Manager API
  - 運算引擎 API
  - 身分識別與存取管理（ IAM ） API

在**Google Cloud**中啟動單一節點系統

在BlueXP中建立工作環境、在Cloud Volumes ONTAP Google Cloud中推出功能更新。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. [[訂閱]在「畫版」頁面上、按一下「新增工作環境」、然後依照提示進行。
3. * 選擇位置 * ：選擇 * Google Cloud * 和 * Cloud Volumes ONTAP
4. 如果出現提示、 "建立連接器"。
5. 詳細資料與認證：選取專案、指定叢集名稱、選擇性地選取服務帳戶、選擇性地新增標籤、然後指定認證資料。

   下表說明您可能需要指導的欄位：

欄位	說明
工作環境名稱	BlueXP使用工作環境名稱來命名Cloud Volumes ONTAP 支援系統和Google Cloud VM執行個體。如果您選取該選項、它也會使用名稱做為預先定義安全性群組的前置詞。
服務帳戶名稱	如果您打算使用 "資料分層" 或 "BlueXP 備份與還原" 有了這個功能、您就需要啟用*服務帳戶*、並選取具有預先定義儲存管理員角色的服務帳戶。Cloud Volumes ONTAP "瞭解如何建立服務帳戶"。
新增標籤	標籤是Google Cloud資源的中繼資料。BlueXP會將標籤新增Cloud Volumes ONTAP 至與系統相關的支援系統和Google Cloud資源。建立工作環境時、您最多可以從使用者介面新增四個標籤、然後在建立之後新增更多標籤。請注意、在建立工作環境時、 API 不會限制您使用四個標籤。如需標籤的相關資訊、請參閱 "Google Cloud 文件：標示資源"。
使用者名稱和密碼	這些是Cloud Volumes ONTAP 適用於整個叢集管理員帳戶的認證資料。您可以使用這些認證資料、 Cloud Volumes ONTAP 透過 System Manager 或其 CLI 連線至功能驗證。保留預設的_admin_使用者名稱、或將其變更為自訂使用者名稱。

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

下列影片說明如何將隨用隨付服務市場訂閱關聯至Google Cloud專案。或者、請依照中的步驟訂閱 "將Marketplace訂閱與Google Cloud認證建立關聯" 區段。

從 Google Cloud Marketplace 訂閱 BlueXP

6. * 服務 * ：選取您要在此系統上使用的服務。若要選取 BlueXP 備份與還原、或使用 BlueXP 分層、您必須在步驟 3 中指定服務帳戶。

   如果您想要使用 WORM 和資料分層功能、您必須停用 BlueXP 備份與還原、並部署 9.8 版或更新版本的 Cloud Volumes ONTAP 工作環境。

7. 位置與連線：選擇位置、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。

   下表說明您可能需要指導的欄位：

欄位	說明
連線驗證	若要將冷資料分層至Google Cloud Storage儲存庫、Cloud Volumes ONTAP 必須將駐留的子網路設定為私有Google Access。如需相關指示、請參閱 "Google Cloud 文件：設定私有 Google Access"。
產生的防火牆原則	如果讓BlueXP為您產生防火牆原則、您必須選擇允許流量的方式： • 如果您選擇*選取的VPC only（僅VPC）*、則傳入流量的來源篩選器為所選VPC的子網路範圍、以及連接器所在VPC的子網路範圍。這是建議的選項。 • 如果您選擇*所有VPC*、傳入流量的來源篩選器為0.00.0.0/0 IP範圍。
使用現有的防火牆原則	如果您使用現有的防火牆原則、請確定其中包含必要的規則。連結： Learn 關於 Cloud Volumes ONTAP 的防火牆規則 。

8. 充電方法與**NSS**帳戶：指定您要搭配此系統使用的收費選項、然後指定NetApp支援網站帳戶。

- "深入瞭Cloud Volumes ONTAP 解適用於此功能的授權選項"。
- "瞭解如何設定授權"。

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

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

10. 授權：視Cloud Volumes ONTAP 需要變更此版本、然後選取機器類型。

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

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

    磁碟類型適用於初始磁碟區。您可以為後續磁碟區選擇不同的磁碟類型。

    磁碟大小適用於初始Aggregate中的所有磁碟、以及使用Simple Provisioning選項時、BlueXP所建立的任何其他Aggregate。您可以使用進階配置選項、建立使用不同磁碟大小的集合體。

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

12. * Flash Cache 、寫入速度與 WORM * ：

    a. 如有需要、請啟用 * Flash Cache* 。

       從 Cloud Volumes ONTAP 9.13.1 開始、 n2-Standard-32 、 n2-Standard-48 和 n2-Standard-64 執行個體類型支援 _Flash Caches 。您無法在部署後停用 Flash Cache 。

    b. 如果需要、請選擇*正常*或*高速*寫入速度。

       "深入瞭解寫入速度"。

       高寫入速度和高傳輸單位（ MTU ） 8 、 896 位元組可透過 * 高 * 寫入速度選項取得。此外、較高的MTU為8、896、需要選擇VPC-1、VPC-2和VPC-3來進行部署。如需VPC-1、VPC-2和VPC-3的詳細資訊、請參閱 "VPC-1、VPC-2和VPC-3的規則"。

    c. 視需要啟動一次寫入、多次讀取（WORM）儲存設備。

       如果啟用Cloud Volumes ONTAP 資料分層功能、無法啟用WORM 9.7版及更低版本。啟用WORM和分層後、將Cloud Volumes ONTAP 會封鎖還原或降級至物件9.8。

    "深入瞭解 WORM 儲存設備"。

    a. 如果您啟動WORM儲存設備、請選取保留期間。

13. * Google Cloud Platform中的資料分層*：選擇是否要在初始Aggregate上啟用資料分層、選擇階層式資料的儲存類別、然後選擇具有預先定義儲存管理角色的服務帳戶（Cloud Volumes ONTAP 適用於更新版本的更新版本）、或是選擇Google Cloud帳戶（Cloud Volumes ONTAP 不支援支援支援功能9.6）。

    請注意下列事項：

- BlueXP會在Cloud Volumes ONTAP 整個過程中設定服務帳戶。此服務帳戶提供資料分層至 Google Cloud Storage 儲存庫的權限。請務必將Connector服務帳戶新增為分層服務帳戶的使用者、否則您無法從BlueXP中選取該帳戶
- 如需新增Google Cloud帳戶的說明、請參閱 "設定及新增Google Cloud帳戶、以便使用9.6進行資料分層"。
- 您可以在建立或編輯磁碟區時、選擇特定的磁碟區分層原則。
- 如果停用資料分層、您可以在後續的Aggregate上啟用、但您需要關閉系統、並從Google Cloud主控台新增服務帳戶。

  "深入瞭解資料分層"。

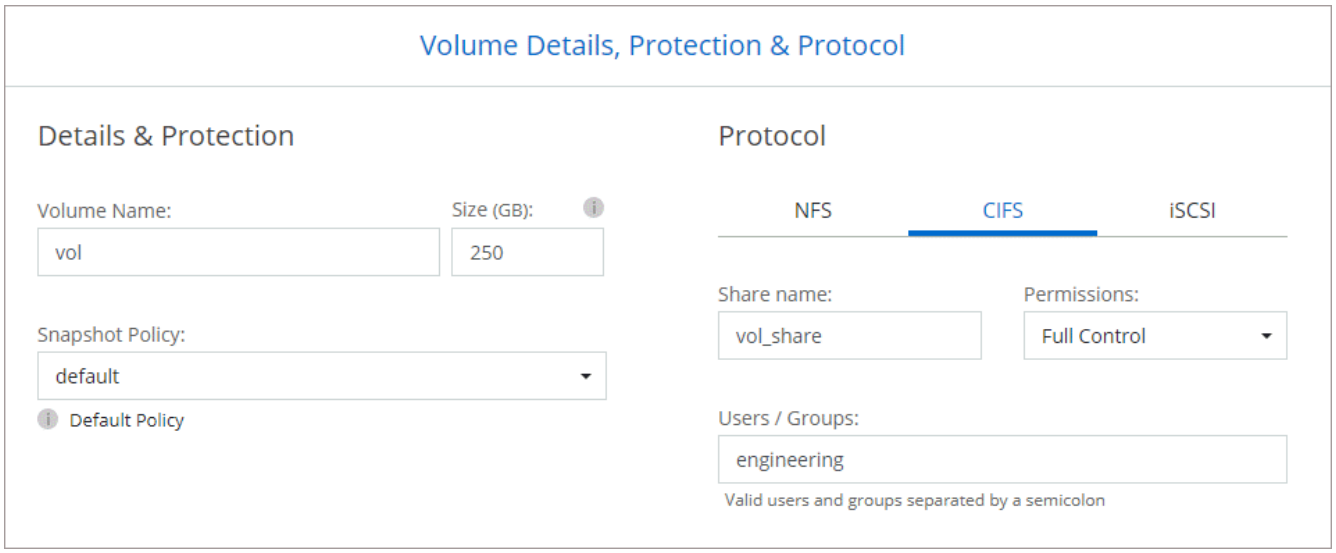
14. * 建立 Volume * ：輸入新磁碟區的詳細資料、或按一下 * 跳過 * 。

    "瞭解支援的用戶端傳輸協定和版本"。

    本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

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

    下圖顯示 CIFS 傳輸協定的「 Volume 」（磁碟區）頁面：



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

欄位	說明
DNS 主要和次要 IP 位址	提供 CIFS 伺服器名稱解析的 DNS 伺服器 IP 位址。列出的 DNS 伺服器必須包含所需的服務位置記錄（ SRV), 才能找到 CIFS 伺服器要加入之網域的 Active Directory LDAP 伺服器和網域控制器。如果您要設定Google Managed Active Directory、AD預設可透過169.254.169.254 IP位址存取。
要加入的 Active Directory 網域	您要 CIFS 伺服器加入之 Active Directory （ AD ）網域的 FQDN 。
授權加入網域的認證資料	具有足夠權限的 Windows 帳戶名稱和密碼、可將電腦新增至 AD 網域內的指定組織單位（ OU ）。
CIFS 伺服器 NetBios 名稱	AD 網域中唯一的 CIFS 伺服器名稱。
組織單位	AD 網域中與 CIFS 伺服器相關聯的組織單位。預設值為「 CN= 電腦」。若要將Google託管Microsoft AD設定為Cloud Volumes ONTAP AD伺服器以供使用、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託管Microsoft AD的組織單位"^]
DNS 網域	適用於整個儲存虛擬 Cloud Volumes ONTAP 機器（ SVM ）的 DNS 網域。在大多數情況下、網域與 AD 網域相同。
NTP 伺服器	選擇 * 使用 Active Directory 網域 * 來使用 Active Directory DNS 設定 NTP 伺服器。如果您需要使用不同的位址來設定 NTP 伺服器、則應該使用 API 。請參閱 "藍圖XP自動化文件" 以取得詳細資料。 請注意、您只能在建立CIFS伺服器時設定NTP伺服器。您建立CIFS伺服器之後、就無法進行設定。

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

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

17. * 審查與核准 * ：檢閱並確認您的選擇。

a. 檢閱組態的詳細資料。

b. 按一下*更多資訊*以檢閱有關支援與BlueXP將購買的Google Cloud資源的詳細資料。

c. 選取「 * 我瞭解 … * 」核取方塊。

d. 按一下「 * 執行 * 」。

結果

BlueXP部署Cloud Volumes ONTAP 了這個功能完善的系統。您可以追蹤時間表的進度。

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

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

完成後

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

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

在**Google Cloud**上啟動**HA**配對

在BlueXP中建立工作環境、在Cloud Volumes ONTAP Google Cloud中推出功能更新。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按一下「 * 新增工作環境 * 」、然後依照提示進行。
3. * 選擇位置 * ：選擇 * Google Cloud * 和 * Cloud Volumes ONTAP 《 * 》 HA * 。
4. * 詳細資料與認證 * ：選取專案、指定叢集名稱、選擇性地選取服務帳戶、選擇性地新增標籤、然後指定認證資料。

   下表說明您可能需要指導的欄位：

欄位	說明
工作環境名稱	BlueXP使用工作環境名稱來命名Cloud Volumes ONTAP 支援系統和Google Cloud VM執行個體。如果您選取該選項、它也會使用名稱做為預先定義安全性群組的前置詞。
服務帳戶名稱	如果您打算使用 "BlueXP 分層" 或 "BlueXP 備份與還原" 服務、您必須啟用 * 服務帳戶 * 交換器、然後選取具有預先定義儲存管理角色的服務帳戶。
新增標籤	標籤是Google Cloud資源的中繼資料。BlueXP會將標籤新增Cloud Volumes ONTAP 至與系統相關的支援系統和Google Cloud資源。建立工作環境時、您最多可以從使用者介面新增四個標籤、然後在建立之後新增更多標籤。請注意、在建立工作環境時、 API 不會限制您使用四個標籤。如需標籤的相關資訊、請參閱 "Google Cloud 文件：標示資源"。

欄位	說明
使用者名稱和密碼	這些是Cloud Volumes ONTAP 適用於整個叢集管理員帳戶的認證資料。您可以使用這些認證資料、 Cloud Volumes ONTAP 透過 System Manager 或其 CLI 連線至功能驗證。保留預設的_admin_使用者名稱、或將其變更為自訂使用者名稱。
編輯專案	選取 Cloud Volumes ONTAP 您要駐留的專案。預設專案是BlueXP所在的專案。 如果在下拉式清單中沒有看到任何其他專案、表示您尚未將BlueXP服務帳戶與其他專案建立關聯。前往 Google Cloud 主控台、開啟 IAM 服務、然後選取專案。將具有BlueXP角色的服務帳戶新增至該專案。您必須針對每個專案重複此步驟。 這是您為BlueXP設定的服務帳戶、 "如本頁所述"。 按一下 * 「新增訂閱」 * 、將選取的認證資料與訂閱建立關聯。 若要建立隨用隨付Cloud Volumes ONTAP 功能的功能性支援系統、您需要從Cloud Volumes ONTAP Google Cloud Marketplace選擇與訂閱功能相關的Google Cloud專案。

下列影片說明如何將隨用隨付服務市場訂閱關聯至Google Cloud專案。 或者、請依照中的步驟訂閱 "將Marketplace訂閱與Google Cloud認證建立關聯" 區段。

從 Google Cloud Marketplace 訂閱 BlueXP

5. * 服務 * ：選取您要在此系統上使用的服務。若要選取 BlueXP 備份與還原、或使用 BlueXP 分層、您必須在步驟 3 中指定服務帳戶。

   如果您想要使用 WORM 和資料分層功能、您必須停用 BlueXP 備份與還原、並部署 9.8 版或更新版本的 Cloud Volumes ONTAP 工作環境。

6. * HA 部署模式 * ：選擇多個區域（建議）或單一區域進行 HA 組態。然後選取區域和區域。

   "深入瞭解 HA 部署模式"。

7. * 連線能力 * ：為 HA 組態選取四個不同的 VPC 、在每個 VPC 中選取一個子網路、然後選擇防火牆原則。

   "深入瞭解網路需求"。

   下表說明您可能需要指導的欄位：

欄位	說明
產生的原則	如果讓BlueXP為您產生防火牆原則、您必須選擇允許流量的方式： • 如果您選擇*選取的VPC only（僅VPC）*、則傳入流量的來源篩選器為所選VPC的子網路範圍、以及連接器所在VPC的子網路範圍。這是建議的選項。 • 如果您選擇*所有VPC*、傳入流量的來源篩選器為0.00.0.0/0 IP範圍。
使用現有的	如果您使用現有的防火牆原則、請確定其中包含必要的規則。 "深入瞭Cloud Volumes ONTAP 解適用於此功能的防火牆規則"。

8. 充電方法與**NSS**帳戶：指定您要搭配此系統使用的收費選項、然後指定NetApp支援網站帳戶。
   - "深入瞭Cloud Volumes ONTAP 解適用於此功能的授權選項"。
   - "瞭解如何設定授權"。
9. * 預先設定的套件 * ：選取其中一個套件以快速部署 Cloud Volumes ONTAP 某個作業系統、或按一下 * 建立我自己的組態 * 。

   如果您選擇其中一個套件、則只需指定一個 Volume 、然後檢閱並核准組態。
10. 授權：視Cloud Volumes ONTAP 需要變更此版本、然後選取機器類型。

    如果所選版本有較新的發行候選版本、一般可用度或修補程式版本、則在建立工作環境時、BlueXP會將系統更新至該版本。例如、如果您選擇Cloud Volumes ONTAP 了「更新」功能、就會進行更新。更新不會從一個版本發生到另一個版本、例如從 9.6 到 9.7 。
11. * 基礎儲存資源 * ：選擇初始 Aggregate 的設定：每個磁碟的磁碟類型和大小。

    磁碟類型適用於初始磁碟區。您可以為後續磁碟區選擇不同的磁碟類型。

    磁碟大小適用於初始Aggregate中的所有磁碟、以及使用Simple Provisioning選項時、BlueXP所建立的任何其他Aggregate。您可以使用進階配置選項、建立使用不同磁碟大小的集合體。

    如需選擇磁碟類型和大小的說明、請參閱 "在 Google Cloud 中調整系統規模"。
12. * Flash Cache 、寫入速度與 WORM * ：
    a. 如有需要、請啟用 * Flash Cache* 。

       從 Cloud Volumes ONTAP 9.13.1 開始、 n2-Standard-32 、 n2-Standard-48 和 n2-Standard-64 執行個體類型支援 _Flash Caches 。您無法在部署後停用 Flash Cache 。
    b. 如果需要、請選擇*正常*或*高速*寫入速度。

       "深入瞭解寫入速度"。

透過使用 n2-Standard-16 、 n2-Standard-32 、 n2-Standard-48 及 n2-Standard-64 執行個體類型的 * High * 寫入速度選項、可獲得高寫入速度及高傳輸單位（ MTU ） 8 、 896 位元組。此外、較高的MTU為8、896、需要選擇VPC-1、VPC-2和VPC-3來進行部署。高寫入速度和 8 、 896 的 MTU 與功能有關、無法在設定的執行個體中個別停用。如需VPC-1、VPC-2和VPC-3的詳細資訊、請參閱 "VPC-1、VPC-2和VPC-3的規則"。

c. 視需要啟動一次寫入、多次讀取（WORM）儲存設備。

如果啟用Cloud Volumes ONTAP 資料分層功能、無法啟用WORM 9.7版及更低版本。啟用WORM和分層後、將Cloud Volumes ONTAP 會封鎖還原或降級至物件9.8。

"深入瞭解 WORM 儲存設備"。

a. 如果您啟動WORM儲存設備、請選取保留期間。

13. * Google Cloud中的資料分層*：選擇是否要在初始Aggregate上啟用資料分層、選擇階層式資料的儲存類別、然後選取具有預先定義儲存管理角色的服務帳戶。

請注意下列事項：

- BlueXP會在Cloud Volumes ONTAP 整個過程中設定服務帳戶。此服務帳戶提供資料分層至 Google Cloud Storage 儲存庫的權限。請務必將Connector服務帳戶新增為分層服務帳戶的使用者、否則您無法從BlueXP中選取該帳戶。
- 您可以在建立或編輯磁碟區時、選擇特定的磁碟區分層原則。
- 如果停用資料分層、您可以在後續的Aggregate上啟用、但您需要關閉系統、並從Google Cloud主控台新增服務帳戶。

"深入瞭解資料分層"。

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

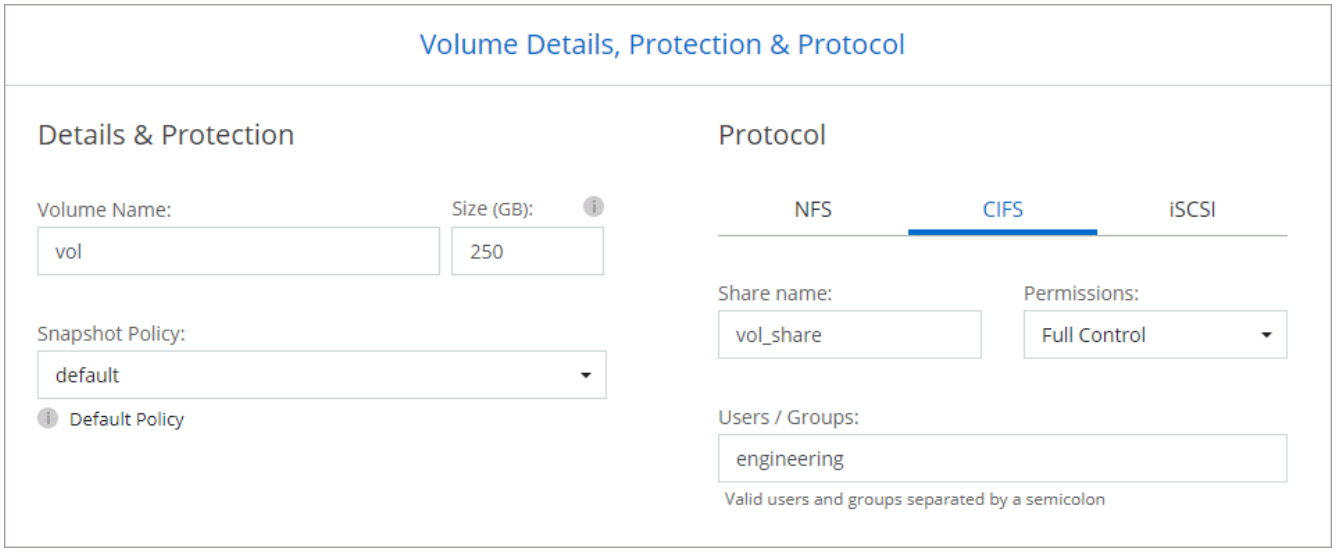
"瞭解支援的用戶端傳輸協定和版本"。

本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

欄位	說明
尺寸	您可以輸入的最大大小、主要取決於您是否啟用精簡配置、這可讓您建立比目前可用實體儲存容量更大的磁碟區。
存取控制（僅適用於 NFS ）	匯出原則會定義子網路中可存取磁碟區的用戶端。根據預設、BlueXP會輸入一個值、以供存取子網路中的所有執行個體。
權限與使用者 / 群組（僅限 CIFS ）	這些欄位可讓您控制使用者和群組（也稱為存取控制清單或 ACL ）的共用存取層級。您可以指定本機或網域 Windows 使用者或群組、或 UNIX 使用者或群組。如果您指定網域 Windows 使用者名稱、則必須使用網域 \ 使用者名稱格式來包含使用者的網域。
Snapshot 原則	Snapshot 複製原則會指定自動建立的 NetApp Snapshot 複本的頻率和數量。NetApp Snapshot 複本是一種不影響效能的時間點檔案系統映像、需要最少的儲存容量。您可以選擇預設原則或無。您可以針對暫時性資料選擇「無」：例如、 Microsoft SQL Server 的 Tempdb 。

欄位	說明
進階選項（僅適用於 NFS ）	為磁碟區選取 NFS 版本： NFSv3 或 NFSv3 。
啟動器群組和 IQN （僅適用於 iSCSI ）	iSCSI 儲存目標稱為 LUN （邏輯單元）、以標準區塊裝置的形式呈現給主機。啟動器群組是 iSCSI 主機節點名稱的表格、可控制哪些啟動器可存取哪些 LUN 。iSCSI 目標可透過標準乙太網路介面卡（ NIC ）、 TCP 卸載引擎（ TOE ）卡（含軟體啟動器）、整合式網路介面卡（ CNA ）或專用主機匯流排介面卡（ HBA ）連線至網路、並由 iSCSI 合格名稱（ IQN ）識別。建立iSCSI磁碟區時、BlueXP會自動為您建立LUN。我們只要在每個磁碟區建立一個 LUN 、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 "使用 IQN 從主機連線至 LUN"。

下圖顯示 CIFS 傳輸協定的「 Volume 」（磁碟區）頁面：



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

欄位	說明
DNS 主要和次要 IP 位址	提供 CIFS 伺服器名稱解析的 DNS 伺服器 IP 位址。列出的 DNS 伺服器必須包含所需的服務位置記錄（ SRV), 才能找到 CIFS 伺服器要加入之網域的 Active Directory LDAP 伺服器和網域控制器。如果您要設定Google Managed Active Directory、AD預設可透過169.254.169.254 IP位址存取。
要加入的 Active Directory 網域	您要 CIFS 伺服器加入之 Active Directory （ AD ）網域的 FQDN 。
授權加入網域的認證資料	具有足夠權限的 Windows 帳戶名稱和密碼、可將電腦新增至 AD 網域內的指定組織單位（ OU ）。
CIFS 伺服器 NetBios 名稱	AD 網域中唯一的 CIFS 伺服器名稱。

欄位	說明
組織單位	AD 網域中與 CIFS 伺服器相關聯的組織單位。預設值為「 CN= 電腦」 。若要將Google託管Microsoft AD設定為Cloud Volumes ONTAP AD伺服器以供使用、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託管Microsoft AD的組織單位"^]
DNS 網域	適用於整個儲存虛擬 Cloud Volumes ONTAP 機器（ SVM ）的 DNS 網域。在大多數情況下、網域與 AD 網域相同。
NTP 伺服器	選擇 * 使用 Active Directory 網域 * 來使用 Active Directory DNS 設定 NTP 伺服器。如果您需要使用不同的位址來設定 NTP 伺服器、則應該使用 API 。請參閱 "藍圖XP自動化文件" 以取得詳細資料。 請注意、您只能在建立CIFS伺服器時設定NTP伺服器。您建立CIFS伺服器之後、就無法進行設定。

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

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

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

結果

BlueXP部署Cloud Volumes ONTAP 了這個功能完善的系統。您可以追蹤時間表的進度。

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

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

完成後

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

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

Google Cloud Platform映像驗證

Google Cloud映像驗證總覽

Google Cloud映像驗證符合增強的NetApp安全要求。已對產生映像的指令碼進行變更、以

便在過程中使用專為此工作所產生的私密金鑰來簽署映像。您可以使用已簽署的Google Cloud摘要與公開憑證來驗證GCP映像的完整性、此憑證可透過下載 "NSS" 以取得特定版本。

支援Google Cloud映像驗證Cloud Volumes ONTAP 功能的更新版本為9.13.0或更新版本。

將**Google Cloud**上的影像轉換成原始格式

用於部署新執行個體、升級或用於現有映像的映像、將透過與用戶端共用 "The》（NSS）NetApp 支援網站"。已簽署的摘要及憑證將可透過NSS入口網站下載。請確定您下載的摘要和憑證是與NetApp支援部門共用的映像相對應的適當版本。例如、9.13.0映像會有9.13.0簽署的摘要和證書、可在NSS上取得。

為何需要此步驟？

無法直接從Google Cloud下載影像。若要根據簽署的摘要和憑證來驗證映像、您需要有機制來比較這兩個檔案並下載映像。若要這麼做、您必須將映像匯出/轉換成磁碟.RAW格式、並將結果儲存在Google Cloud的儲存庫中。磁碟.RAW檔案會在處理過程中產生損及壓縮。

使用者/服務帳戶需要權限才能執行下列作業：

- 存取Google儲存庫
- 寫入Google Storage儲存區
- 建立雲端建置工作（在匯出程序期間使用）
- 存取所需的映像
- 建立匯出映像工作

若要驗證映像、必須先將其轉換成磁碟.RAW格式、然後再下載。

使用**Google Cloud**命令列匯出**Google Cloud**映像

將映像匯出至雲端儲存設備的首選方法是使用 "gCloud運算映像匯出命令"。此命令會取得所提供的映像、並將其轉換成磁碟.原始 檔案、並取得tar和gzipped。產生的檔案會儲存在目的地URL、然後下載以供驗證。

使用者/帳戶必須擁有存取及寫入所需儲存區、匯出映像及雲端建置（Google用於匯出映像）的權限、才能執行此作業。

使用**gCloud**匯出**Google Cloud**映像

按一下以顯示

```
$ 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
```

解壓縮檔案

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

請參閱 "匯出影像的Google Cloud文件" 如需如何透過Google Cloud匯出影像的詳細資訊、

影像簽名驗證

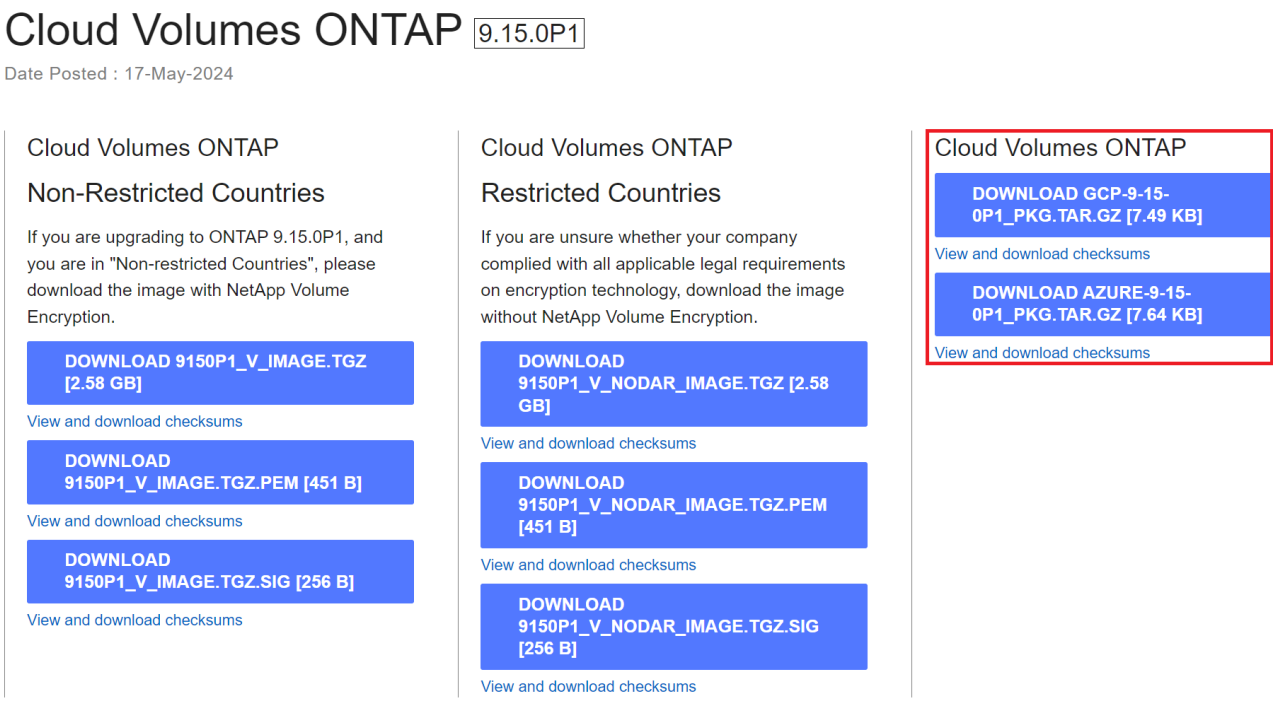
驗證Google Cloud簽署的映像

若要驗證匯出的Google Cloud簽署映像、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。

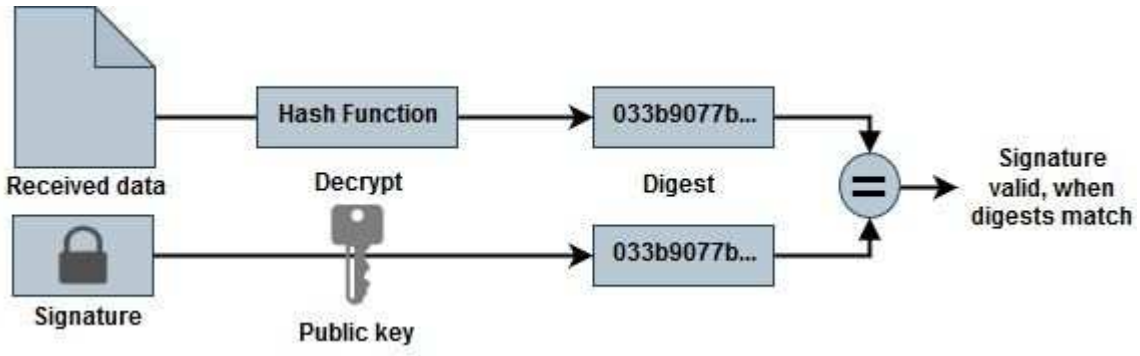
簽署映像驗證工作流程摘要

以下是Google Cloud簽署映像驗證工作流程的總覽。

- 從 "NSS"下載內含下列檔案的Google Cloud歸檔：
  - 簽名摘要（.sig）
  - 包含公開金鑰（.pem）的憑證
  - 憑證鏈結（.pem）



- 下載轉換後的disk.原始 檔案
- 使用憑證鏈結驗證憑證
- 使用含有公開金鑰的憑證來驗證已簽署的摘要
  - 使用公開金鑰解密已簽署的摘要、以擷取映像檔摘要
  - 建立已下載磁碟.原始 檔案的摘要
  - 比較兩個摘要檔案以進行驗證



使用**OpenSSL**驗證磁碟**.RAW**檔案和摘要檔案內容

您可以根據可透過取得的摘要檔案內容、驗證Google Cloud下載的disk.RAW檔案 "NSS" 使用OpenSSL。

用於驗證映像的OpenSSL命令與Linux、Mac OS和Windows機器相容。

步驟

1. 使用OpenSSL驗證憑證。

按一下以顯示

```
# 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.原始 檔案、簽名及憑證放在目錄中。
3. 使用OpenSSL從憑證擷取公開金鑰。
4. 使用擷取的公開金鑰解密簽名、並驗證下載的disk.原始 檔案內容。

按一下以顯示

```
# 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

授權管理

管理容量型授權

從 BlueXP 數位錢包管理容量型授權、以確保您的 NetApp 帳戶擁有足夠的容量供 Cloud Volumes ONTAP 系統使用。

_容量型授權_可讓您針對Cloud Volumes ONTAP 每個TiB的容量付費。

_BlueXP 數位錢包 _ 可讓您從單一位置管理 Cloud Volumes ONTAP 的授權。您可以新增授權並更新現有授權。

> 雖然 BlueXP 管理的產品和服務的實際使用量和計量都是以 GiB 和 TiB 計算、但是會交替使用「 GB/GiB 」和「 TB/TiB 」這兩個詞彙。這會反映在 Cloud Marketplace 清單、價格報價、上市說明及其他支援文件中

"深入瞭Cloud Volumes ONTAP 解不知如何取得授權"。

如何將授權新增至 **BlueXP** 數位錢包

向NetApp銷售代表購買授權後、NetApp會寄送一封電子郵件給您、附上序號和其他授權詳細資料。

在此期間、BlueXP會自動查詢NetApp的授權服務、以取得NetApp 支援網站 與您的帳戶相關之授權的詳細資料。如果沒有錯誤、 BlueXP 會自動將授權新增至數位錢包。

如果 BlueXP 無法新增授權、您必須自行手動將授權新增至數位錢包。例如、如果Connector安裝在無法存取網際網路的位置、您就必須自行新增授權。 瞭解如何將購買的授權新增至您的帳戶。

檢視您帳戶中的已用容量

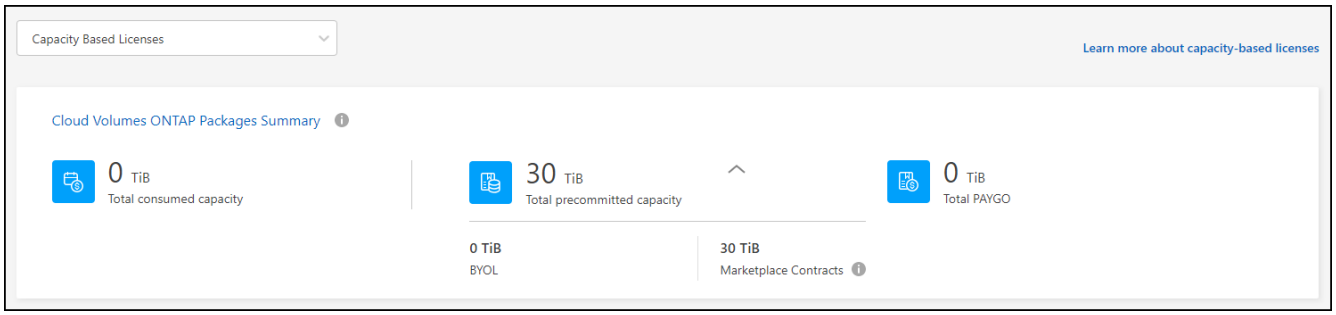
BlueXP 數位錢包可顯示您帳戶的總使用容量、以及授權套件所耗用的容量。這有助於瞭解您的收費方式、以及您是否需要購買額外容量。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在 * Cloud Volumes ONTAP * 標籤上、選取 * 容量型授權 * 。
3. 檢視套件摘要、其中會顯示您已耗用的容量、預先認可的總容量和 PAYGO 總容量。

    - _總使用容量_是Cloud Volumes ONTAP NetApp帳戶中所有供應系統的總容量。無論磁碟區內的本機、已用、已儲存或有效空間為何、充電都是根據每個磁碟區的已配置大小而計算。
    - *Total preconted capacity* 是您從 NetApp 購買的總授權容量（ BYOL 或 Marketplace Contract ）。
    - _Total PAYGO_是使用雲端市場訂閱的已配置總容量。只有當使用容量高於授權容量、或 BlueXP 數位錢包中沒有 BYOL 授權時、才會使用 PAYGO 進行收費。

      以下是 BlueXP 數位錢包中 Cloud Volumes ONTAP 套件摘要的範例：



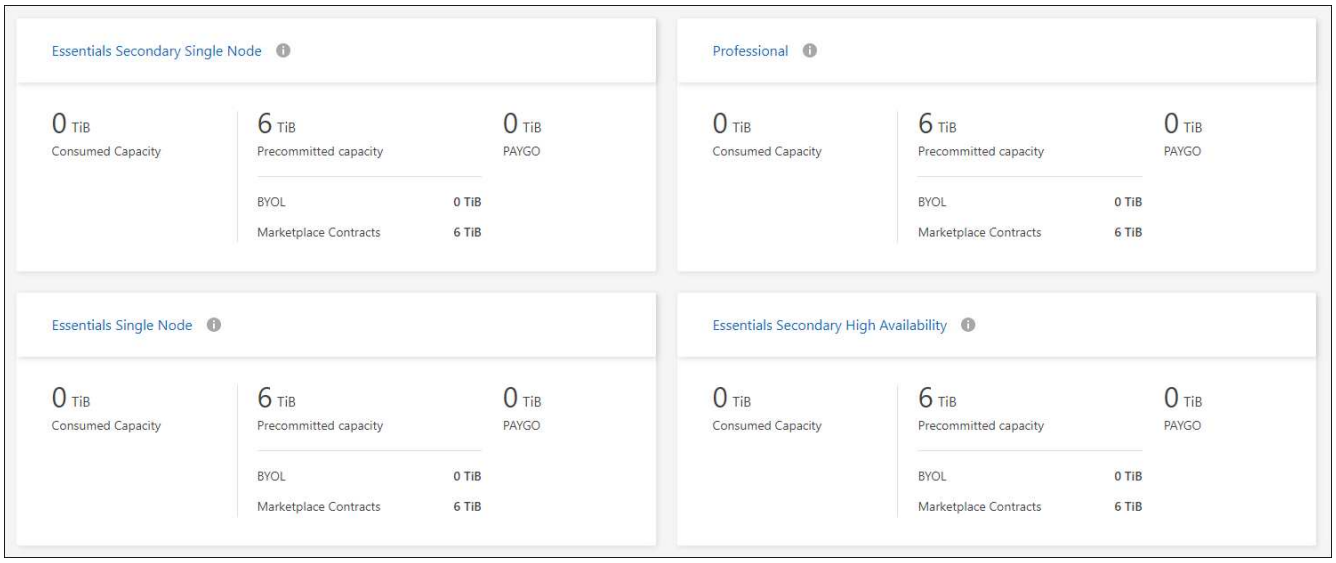
4. 在摘要下、檢視每個授權套件的耗用容量。

   - 耗用容量 _ 顯示該套件的磁碟區容量。如需特定套件的詳細資料、請將滑鼠游標移到工具提示上。

     若要更深入瞭解Essentials套件的顯示容量、您應該熟悉充電的運作方式。 "瞭解如何為Essentials套裝方案充電"。

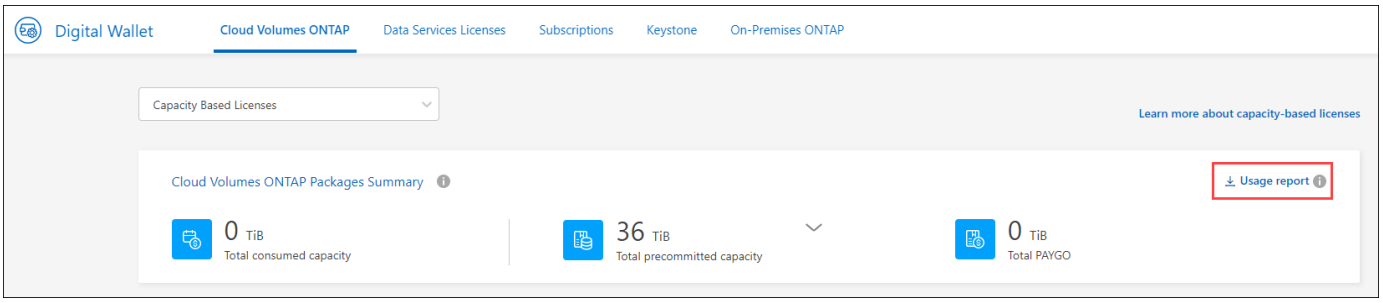
   - _ 預先承諾容量 _ 是您從 NetApp 購買的授權容量（ BYOL 或 Marketplace 合約）。
     - *BYOL* 顯示您從 NetApp 購買的此套件類型的授權容量。
     - *Marketplace Contracts* 顯示您購買的此套件類型的市場合約授權容量。
   - *PAYGO* 會依授權使用模式顯示使用容量。

     以下是一個擁有多個授權套件的帳戶範例：



下載使用報告

帳戶管理員可以從 BlueXP 的數位錢包下載四份使用報告。這些使用報告會提供您訂閱的容量詳細資料、並告訴您如何為 Cloud Volumes ONTAP 訂閱中的資源收取費用。可下載的報告會在某個時間點擷取資料、並可輕鬆與他人共用。



以下報告可供下載。顯示的容量值以 TiB 為單位。

- * 高階使用率 * ：此報告會清楚顯示數位錢包中「 Cloud Volumes ONTAP 套件摘要」卡的內容。其中包括下列資訊：
  - 總使用容量
  - 預認可容量總計
  - BYOL 總容量
  - 市場總合約容量
  - PAYGO 總容量
- * Cloud Volumes ONTAP 套件使用 * ：此報告會清楚顯示數位錢包內的套裝卡片內容。除了最佳化的 I/O 套件外、其中包括每個套件的下列資訊：
  - 總使用容量
  - 預認可容量總計
  - BYOL 總容量
  - 市場總合約容量
  - PAYGO 總容量
- * 儲存虛擬機器使用率 * ：此報告顯示如何在 Cloud Volumes ONTAP 系統和儲存虛擬機器（ SVM ）之間分解已計費的容量。此資訊無法在數位錢包的任何畫面上取得。其中包括下列資訊：
  - 工作環境 ID 和名稱（顯示為 UUID ）
  - 雲端
  - NetApp 帳戶 ID
  - 工作環境組態
  - SVM名稱
  - 已配置的容量
  - 充電容量綜合報告
  - 市場帳單期限
  - Cloud Volumes ONTAP 套件或功能
  - 向 SaaS Marketplace 訂閱名稱收費
  - 向 SaaS Marketplace 訂閱 ID 收費
  - 工作負載類型

- * Volume 使用量 * ：此報告顯示如何在工作環境中、依磁碟區來分解收費容量。此資訊無法在數位錢包的任何畫面上取得。其中包括下列資訊：
  - 工作環境 ID 和名稱（顯示為 UUID ）
  - SVN 名稱
  - Volume ID
  - Volume類型
  - Volume 資源配置容量

    此報告不包含 FlexClone Volume 、因為這些類型的磁碟區不會產生費用。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在 * Cloud Volumes ONTAP * 標籤上、選取 * 容量型授權 * 、然後按一下 * 使用報告 * 。

   使用報告會下載。
3. 開啟下載的檔案以存取報告。

將購買的授權新增至您的帳戶

如果您在 BlueXP 數位錢包中沒有看到購買的授權、則需要將授權新增至 BlueXP 、以便 Cloud Volumes ONTAP 可以使用該容量。

您需要的產品

- 您需要提供BlueXP授權或授權檔案的序號。
- 如果您要輸入序號、請先輸入 "將NetApp 支援網站 您的不更新帳戶新增至藍圖XP"。這是獲授權可以存取序號的 NetApp 支援網站帳戶。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》索引標籤上、保留*容量型授權、然後按一下*新增授權*。
3. 輸入容量型授權的序號、或上傳授權檔案。

   如果您輸入序號、您也需要選擇獲授權存取序號的NetApp Support Site帳戶。
4. 按一下「 * 新增授權 * 」 。

更新容量型授權

如果您購買額外容量或延長授權期限、 BlueXP 會自動更新數位錢包中的授權。您無需做任何事。

不過、如果您在無法存取網際網路的位置部署了BlueXP、則需要手動更新BlueXP中的授權。

您需要的產品

授權檔案（如果您有HA配對、則為_file_）。

如需如何取得授權檔案的詳細資訊、請參閱 "取得系統授權檔案"。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》索引標籤上、按一下授權旁的動作功能表、然後選取*更新授權。
3. 上傳授權檔案。
4. 按一下*上傳授權*。

變更充電方法

容量型授權的形式為_package_。建立 Cloud Volumes ONTAP 工作環境時、您可以根據業務需求、從多個授權套件中選擇。如果您在建立工作環境之後需要變更、您可以隨時變更套件。例如、您可以將 Essentials 套件變更為專業版套件。

"深入瞭解容量型授權套件"。

關於這項工作

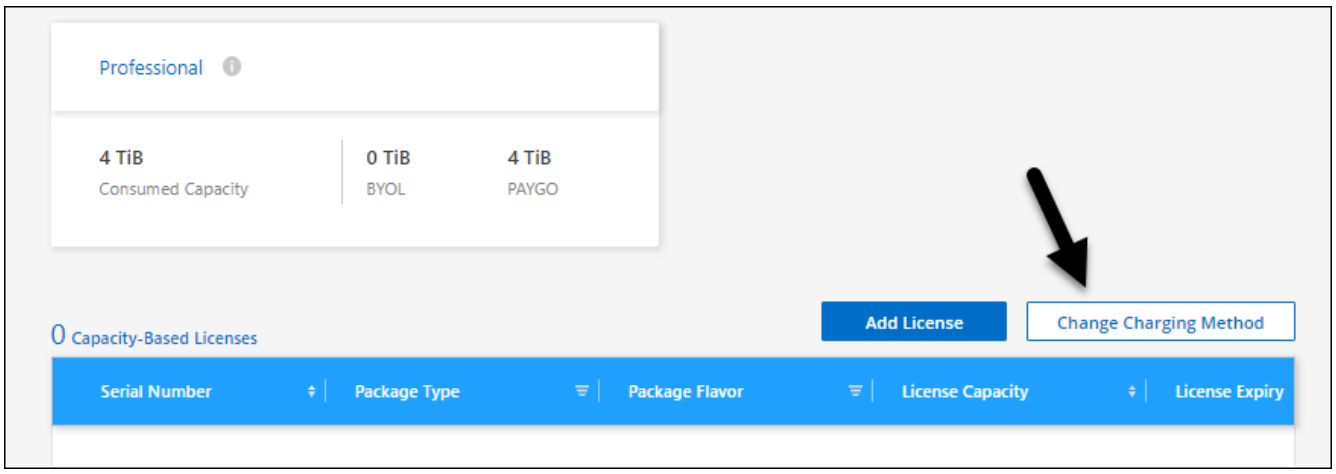
- 變更收費方式並不會影響您是透過從 NetApp （ BYOL ）購買的授權或雲端供應商的市場（隨用付費）收取費用。

  BlueXP 一律會先嘗試根據授權收費。如果沒有可用的授權、就會根據市場訂閱收費。BYOL 不需要「轉換」即可訂閱市場、反之亦然。

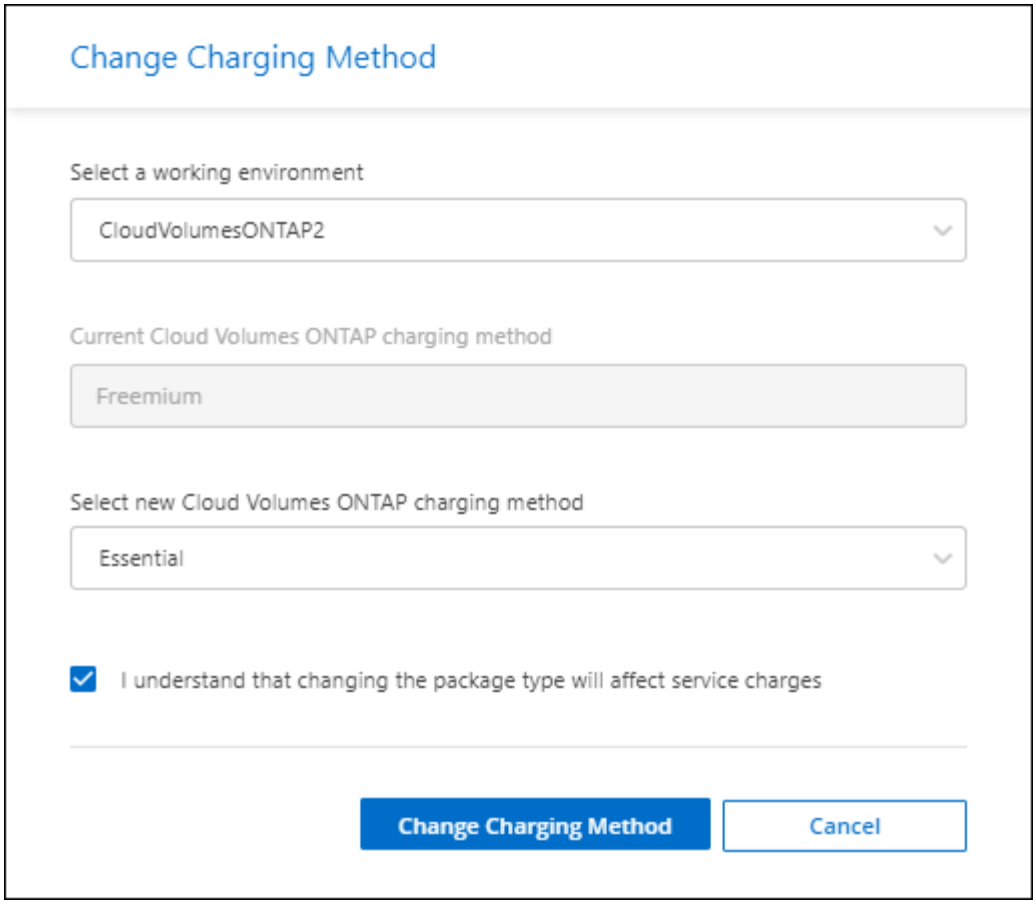
- 如果您有來自雲端供應商市場的私人優惠或合約、改用未包含在合約中的收費方法、將會導致依BYOL（如果您向NetApp購買授權）或PAYGO收取費用。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》索引標籤上、按一下「*變更充電方法」。



3. 選取工作環境、選擇新的充電方法、然後確認您瞭解變更套件類型將會影響服務費用。



4. 按一下*變更收費方法*。

結果

BlueXP改變Cloud Volumes ONTAP 了這個系統的充電方法。

您可能也會注意到 BlueXP 數位錢包會重新整理每個套件類型的已用容量、以因應您剛做的變更。

移除容量型授權

如果容量型授權過期且不再使用、您可以隨時將其移除。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》索引標籤上、按一下授權旁的動作功能表、然後選取*移除授權。
3. 按一下「 * 移除 * 」以確認。

管理 **Keystone** 訂閱

從 BlueXP 數位電子錢包管理 Keystone 訂閱、只要啟用 Cloud Volumes ONTAP 訂閱、並要求變更訂閱服務層級的承諾容量即可。為服務層級要求額外容量、可為內部部署 ONTAP 叢集或 Cloud Volumes ONTAP 系統提供更多儲存空間。

NetApp Keystone 是彈性的隨成長付費訂閱型服務、可為偏好營運成本而非資本支出或租賃的客戶、提供混合雲體驗。

"深入瞭解 Keystone"

授權您的帳戶

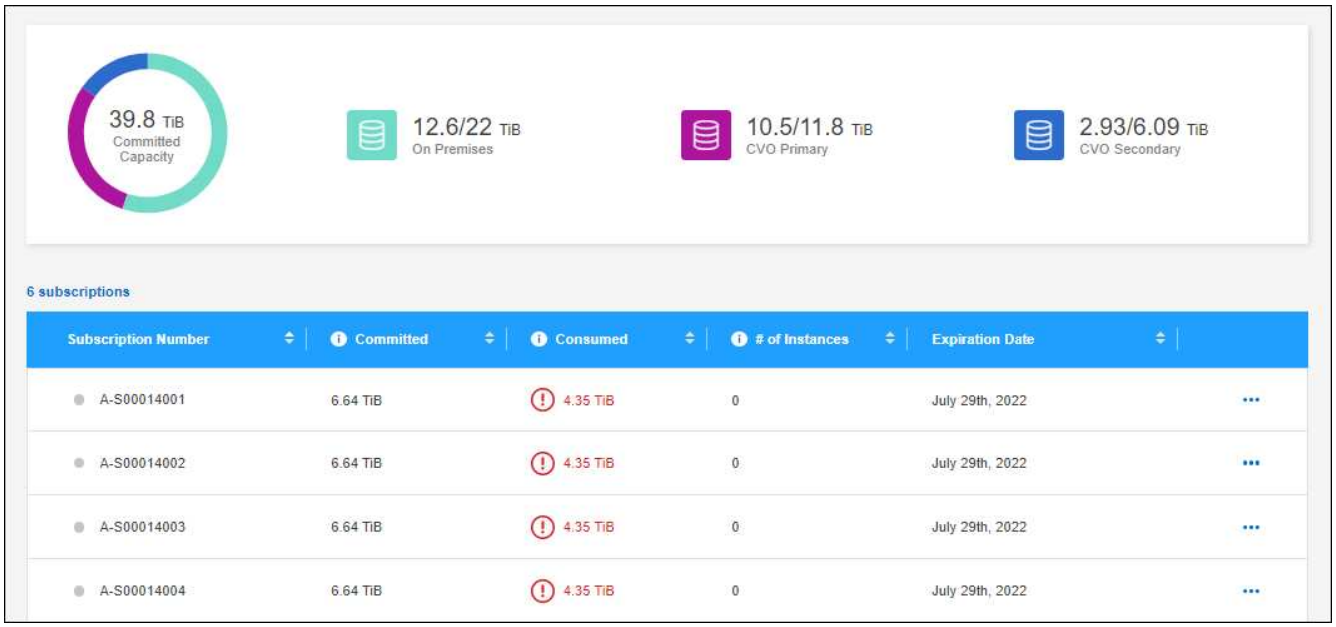
在 BlueXP 中使用和管理 Keystone 訂閱之前、您必須先聯絡 NetApp 、以授權您的 BlueXP 使用者帳戶使用 Keystone 訂閱。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 選取 * Keystone * 。
3. 如果您看到*歡迎使用NetApp Keystone S不到*頁面、請傳送電子郵件至頁面上所列的地址。

   NetApp代表將授權您的使用者帳戶存取訂閱、以處理您的申請。

4. 返回 * Keystone Subscription* 檢視您的訂閱。

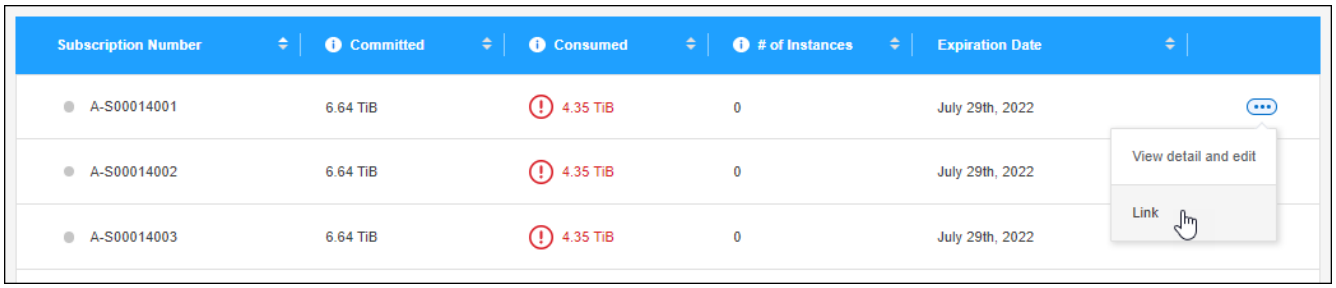


連結訂閱

NetApp 授權您的帳戶後、您可以連結 Keystone 訂閱以搭配 Cloud Volumes ONTAP 使用。此動作可讓使用者選擇訂閱做為新Cloud Volumes ONTAP 版的功能表系統的充電方法。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 選取 * Keystone * 。
3. 如需您要連結的訂閱、請按一下 ••• 然後選取*連結*。



結果

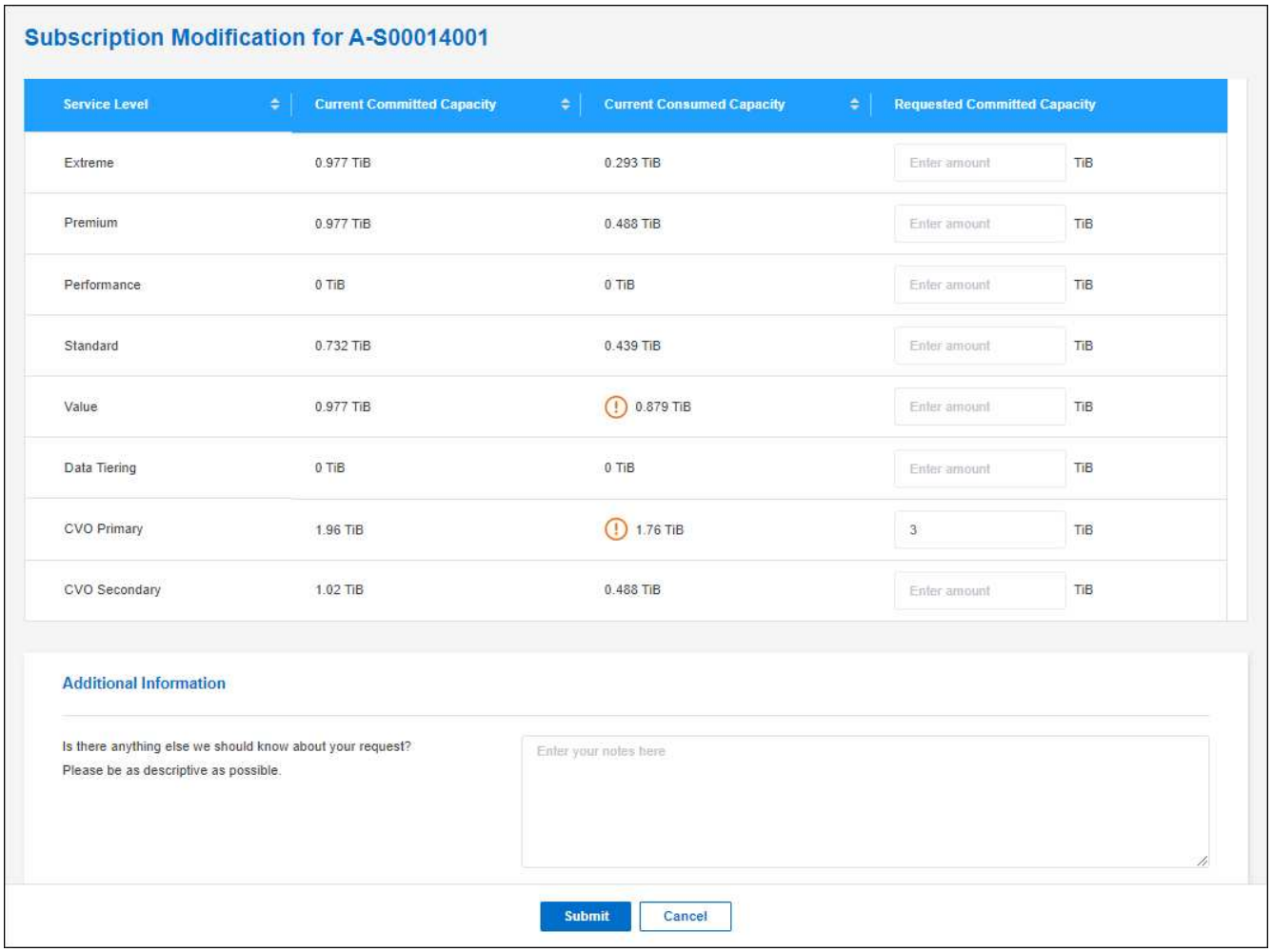
訂閱內容現已連結至您的BlueXP帳戶、可在建立Cloud Volumes ONTAP 運作環境時選擇。

申請更多或更少的已認可容量

如果您想要變更訂閱服務層級的認可容量、可以直接從 BlueXP 傳送要求至 NetApp 。為服務層級要求額外容量、可為內部部署叢集或 Cloud Volumes ONTAP 系統提供更多儲存空間。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 選取 * Keystone * 。
3. 如需調整容量的訂閱、請按一下 ••• 然後選取*檢視詳細資料並編輯*。
4. 輸入一或多個訂閱所需的已提交容量。



5. 向下捲動、輸入申請的任何其他詳細資料、然後按一下*提交*。

結果

您的申請會在NetApp系統中建立Ticket以供處理。

監控使用率

BlueXP 數位顧問儀表板可讓您監控 Keystone 訂閱使用量並產生報告。

"深入瞭解監控訂閱使用率"

取消訂閱連結

如果您不想再使用 Keystone Subscription with BlueXP 、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 的訂閱內容的訂閱。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 選取 * Keystone * 。
3. 若要取消連結訂閱、請按一下 ••• 然後選取*取消連結*。

結果

訂閱內容會從您的BlueXP帳戶中取消連結、因此在建立Cloud Volumes ONTAP 運作中的環境時無法再選取。

管理節點型授權

在 BlueXP 數位錢包中管理節點型授權、以確保每個 Cloud Volumes ONTAP 系統都擁有具有所需容量的有效授權。

_Node型授權_是前一代授權模式（不適用於新客戶）：

- 向NetApp購買BYOL授權
- 從雲端供應商的市場訂閱每小時隨付（PAYGO）

_BlueXP 數位錢包 _ 可讓您從單一位置管理 Cloud Volumes ONTAP 的授權。您可以新增授權並更新現有授權。

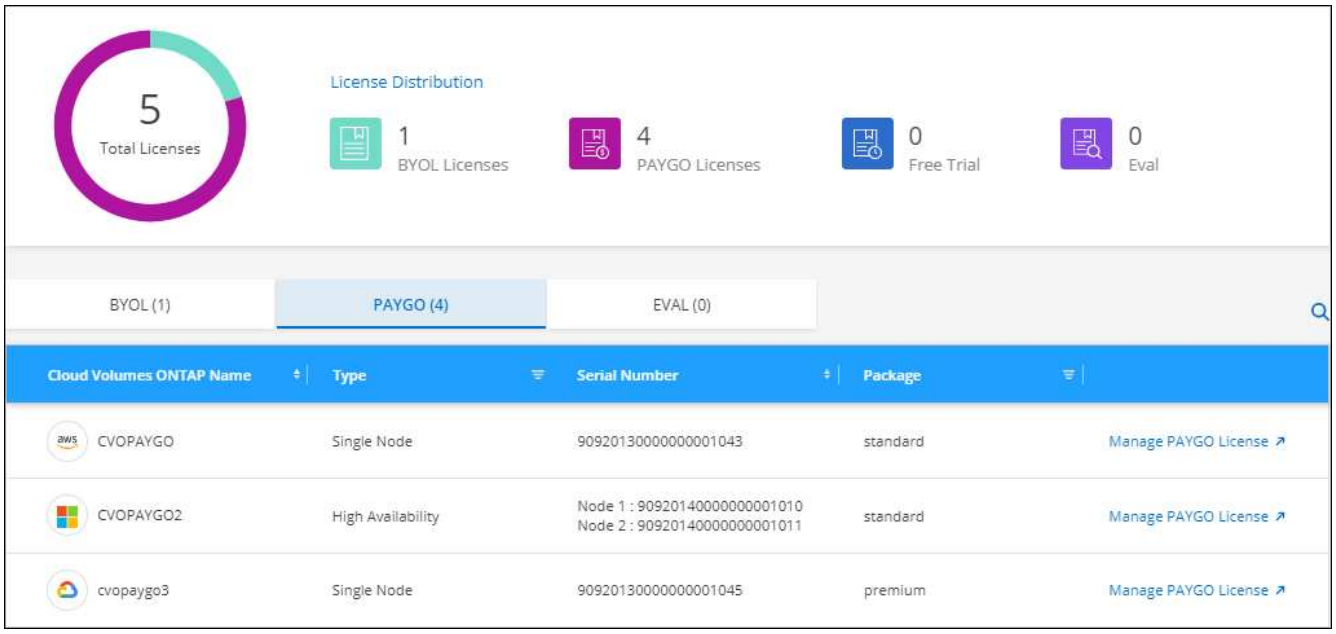
"深入瞭Cloud Volumes ONTAP 解不知如何取得授權"。

管理**PAYGO**授權

BlueXP 數位錢包頁面可讓您檢視每個 PAYGO Cloud Volumes ONTAP 系統的詳細資料、包括序號和 PAYGO 授權類型。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》*索引標籤上、從下拉式清單中選取「*節點型授權」。
3. 按一下* PAYGO*。
4. 請在表格中檢視每個PAYGO授權的詳細資料。



5. 如有需要、請按一下*管理PAYGO授權*以變更PAYGO授權或變更執行個體類型。

管理 **BYOL** 授權

透過新增及移除系統授權與額外容量授權、來管理您直接向NetApp購買的授權。

新增未指派的授權

將節點型授權新增至 BlueXP 數位錢包、以便在建立新的 Cloud Volumes ONTAP 系統時選取授權。數位錢包會將這些授權識別為 *disally*.

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》*索引標籤上、從下拉式清單中選取「*節點型授權」。
3. 按一下*未指派*。
4. 按一下「新增未指派的授權」。
5. 輸入授權的序號或上傳授權檔案。

   如果您還沒有授權檔案、請參閱下列章節。
6. 按一下「 * 新增授權 * 」。

結果

BlueXP 將授權新增至數位錢包。授權將被識別為未指派、直到您將其與新Cloud Volumes ONTAP 的一套系統關聯為止。之後、授權便會移至數位錢包中的 * BYOL* 標籤。

Exchange未指派的節點型授權

如果您尚未使用未指派的 Cloud Volumes ONTAP 節點型授權、則可將授權轉換為 BlueXP 備份與還原授權、BlueXP 分類授權或 BlueXP 分層授權、以交換授權。

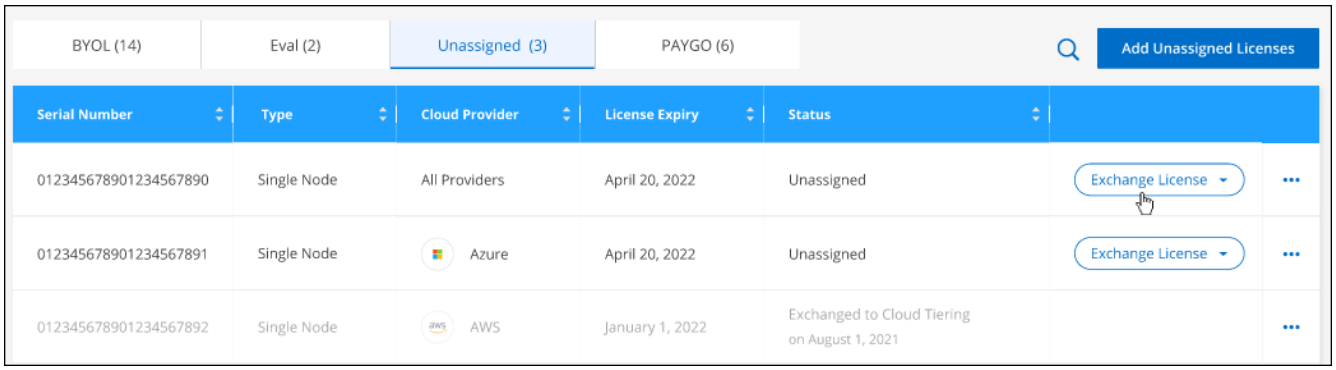
交換授權會撤銷Cloud Volumes ONTAP 該服務的不含美元的授權、並為該服務建立相當於美元的授權：

- 針對某個不符合需求的HA配對授權Cloud Volumes ONTAP 會轉換為51 TiB資料服務授權
- 針對單一節點的授權Cloud Volumes ONTAP 會轉換為32 TiB資料服務授權

轉換後的授權到期日與Cloud Volumes ONTAP 不含更新授權的到期日相同。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》*索引標籤上、從下拉式清單中選取「*節點型授權」。
3. 按一下*未指派*。
4. 按一下「* Exchange授權*」。



5. 選取您要與其交換授權的服務。
6. 如果出現提示、請為HA配對選取額外的授權。
7. 閱讀法律同意書、然後按一下*同意*。

結果

BlueXP會將未指派的授權轉換成您選取的服務。您可以在「資料服務授權」標籤中檢視新授權。

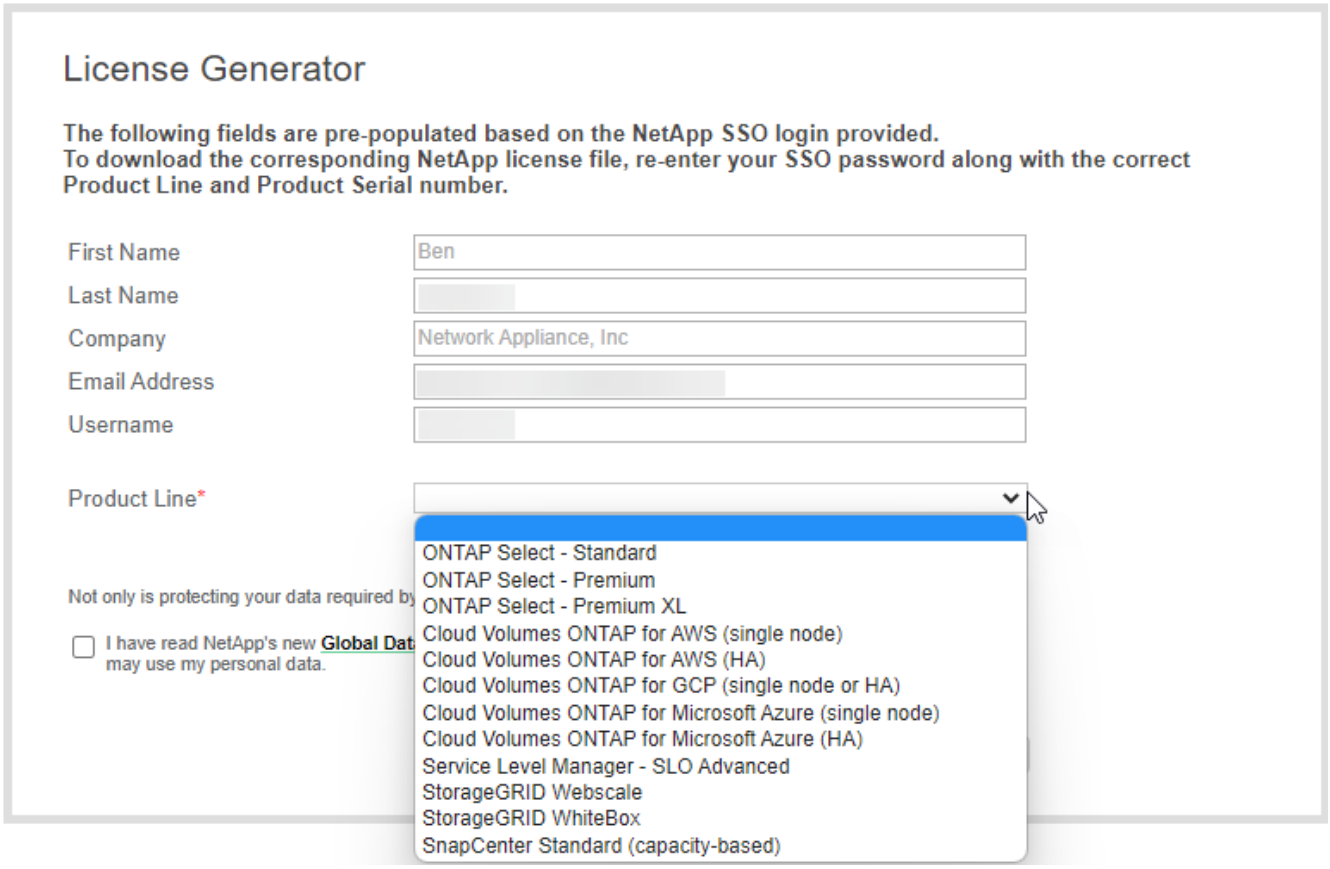
取得系統授權檔案

在大多數情況下、BlueXP可以使用NetApp 支援網站 您的還原帳戶自動取得授權檔案。但如果無法、則需要手動上傳授權檔案。如果您沒有授權檔案、可以從 netapp.com 取得。

步驟

1. 前往 "NetApp 授權檔案產生器" 並使用您的 NetApp 支援網站認證登入。
2. 輸入您的密碼、選擇產品、輸入序號、確認您已閱讀並接受隱私權政策、然後按一下 * 提交 * 。

    ◦ 範例 *



3. 選擇您要透過電子郵件或直接下載來接收 serialNumber.NLF Json 檔案。

更新系統授權

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

如果BlueXP無法透過安全的網際網路連線存取授權檔案、您可以自行取得檔案、然後手動將檔案上傳至BluXP。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》*索引標籤上、從下拉式清單中選取「*節點型授權」。
3. 在「* BYOL*」標籤中、展開Cloud Volumes ONTAP 關於某個系統的詳細資料。
4. 按一下系統授權旁的動作功能表、然後選取*更新授權*。
5. 上傳授權檔案（若您有HA配對、則為檔案）。
6. 按一下 * 更新授權 * 。

結果

BlueXP會更新Cloud Volumes ONTAP 整個作業系統的授權。

管理額外容量授權

您可以購買Cloud Volumes ONTAP 額外容量授權給某個不含BYOL的系統、以配置超過368TiB的BYOL系統授

權容量。例如、您可以購買一個額外的授權容量、以配置多達736 TiB的容量來Cloud Volumes ONTAP 供使用。或者、您也可以購買三份額外容量授權、最多可取得1.4 PIB。

單一節點系統或 HA 配對可購買的授權數量不受限制。

新增容量授權

透過BlueXP右下角的聊天圖示聯絡我們、購買額外的容量授權。購買授權後、您可以將其套用Cloud Volumes ONTAP 至一套系統。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》*索引標籤上、從下拉式清單中選取「*節點型授權」。
3. 在「* BYOL*」標籤中、展開Cloud Volumes ONTAP 關於某個系統的詳細資料。
4. 按一下「新增容量授權」。
5. 輸入序號或上傳授權檔案（如果您有HA配對、也可以輸入檔案）。
6. 按一下「新增容量授權」。

更新容量授權

如果您延長額外容量授權的期限、則需要更新BlueXP中的授權。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》*索引標籤上、從下拉式清單中選取「*節點型授權」。
3. 在「* BYOL*」標籤中、展開Cloud Volumes ONTAP 關於某個系統的詳細資料。
4. 按一下容量授權旁邊的動作功能表、然後選取*更新授權*。
5. 上傳授權檔案（若您有HA配對、則為檔案）。
6. 按一下 * 更新授權 * 。

移除容量授權

如果額外的容量授權過期且不再使用、您可以隨時將其移除。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》*索引標籤上、從下拉式清單中選取「*節點型授權」。
3. 在「* BYOL*」標籤中、展開Cloud Volumes ONTAP 關於某個系統的詳細資料。
4. 按一下容量授權旁的動作功能表、然後選取*移除授權*。
5. 按一下「移除」。

將試用版授權轉換為**BYOL**

試用版授權可提供30天的使用時間。您可以在就地升級的評估授權上套用新的BYOL授權。

當您將試用版授權轉換為BYOL時、BlueXP會重新啟動Cloud Volumes ONTAP 該系統。

- 對於單節點系統、重新啟動會在重新開機程序期間導致I/O中斷。
- 對於HA配對、重新啟動會啟動接管和恢復、以繼續為用戶端提供I/O服務。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》*索引標籤上、從下拉式清單中選取「*節點型授權」。
3. 按一下* Eval*。
4. 在表格中、按一下*「轉換成BYOL授權*」以取得Cloud Volumes ONTAP 一套系統。
5. 輸入序號或上傳授權檔案。
6. 按一下*「轉換授權*」。

結果

BlueXP開始轉換程序。此程序會自動重新啟動。Cloud Volumes ONTAP備份時、授權資訊會反映出新的授權。

在**PAYGO**和**BYOL**之間切換

不支援將系統從PAYGO的節點授權轉換成BYOL的節點授權（反之亦然）。如果您想要在隨用隨付訂閱和BYOL訂閱之間切換、則必須部署新系統、並將資料從現有系統複寫到新系統。

步驟

1. 打造全新 Cloud Volumes ONTAP 的運作環境。
2. 針對您需要複寫的每個磁碟區、在系統之間設定一次性資料複寫。

   "瞭解如何在系統之間複寫資料"

3. 刪除原始工作環境、終止Cloud Volumes ONTAP 不再需要的功能。

   "瞭解如何刪除Cloud Volumes ONTAP 功能不正常的工作環境"。

Volume與LUN管理

建立**FlexVol** 功能區

如果您在啟動初始Cloud Volumes ONTAP 的支援功能後需要更多儲存設備、您可以從FlexVol BlueXP建立新的支援NFS、CIFS或iSCSI的支援功能。

BlueXP提供多種建立新磁碟區的方法：

- 指定新磁碟區的詳細資料、讓BlueXP為您處理基礎資料集合體。 深入瞭解
- 在您選擇的資料集合體上建立磁碟區。 深入瞭解
- 在HA組態的第二個節點上建立磁碟區。 深入瞭解

開始之前

關於Volume資源配置的幾點注意事項：

- 建立iSCSI磁碟區時、BlueXP會自動為您建立LUN。我們只要在每個磁碟區建立一個 LUN 、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 "使用 IQN 從主機連線至 LUN"。
- 您可以從 System Manager 或 CLI 建立其他 LUN 。
- 如果您想在 AWS 中使用 CIFS 、則必須設定 DNS 和 Active Directory 。如需詳細資訊、請參閱 "AWS 的 Cloud Volumes ONTAP 網路需求"。
- 如果Cloud Volumes ONTAP 您的支援Amazon EBS彈性Volume功能的組態、您可能會想要 "深入瞭解建立Volume時會發生什麼事"。

建立**Volume**

建立磁碟區最常見的方法是指定所需的磁碟區類型、然後由BlueXP為您處理磁碟配置。但您也可以選擇要在其上建立磁碟區的特定Aggregate。

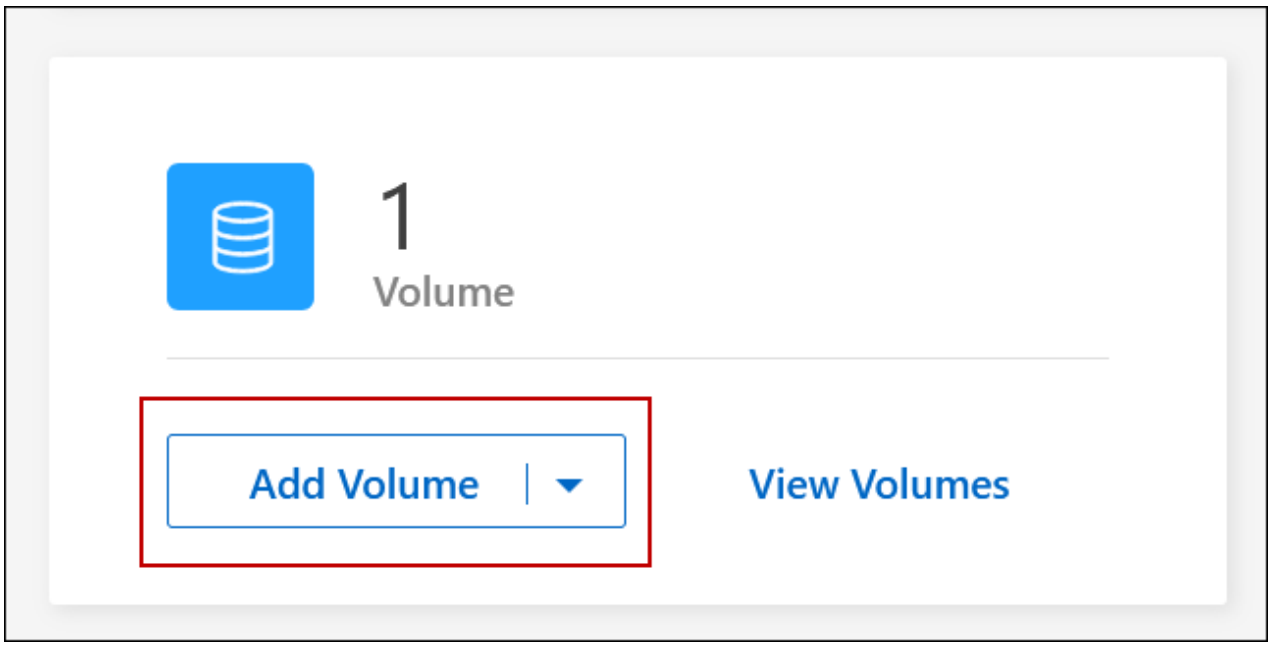
步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按兩下Cloud Volumes ONTAP 您要在其中配置FlexVol 一份「功能區」的「功能區」系統名稱。
3. 請讓BlueXP為您處理磁碟配置、或為磁碟區選擇特定的集合體、以建立新的磁碟區。

   只有在您對Cloud Volumes ONTAP 自己的系統上的資料集合體有充分的瞭解時、才建議您選擇特定的集合體。

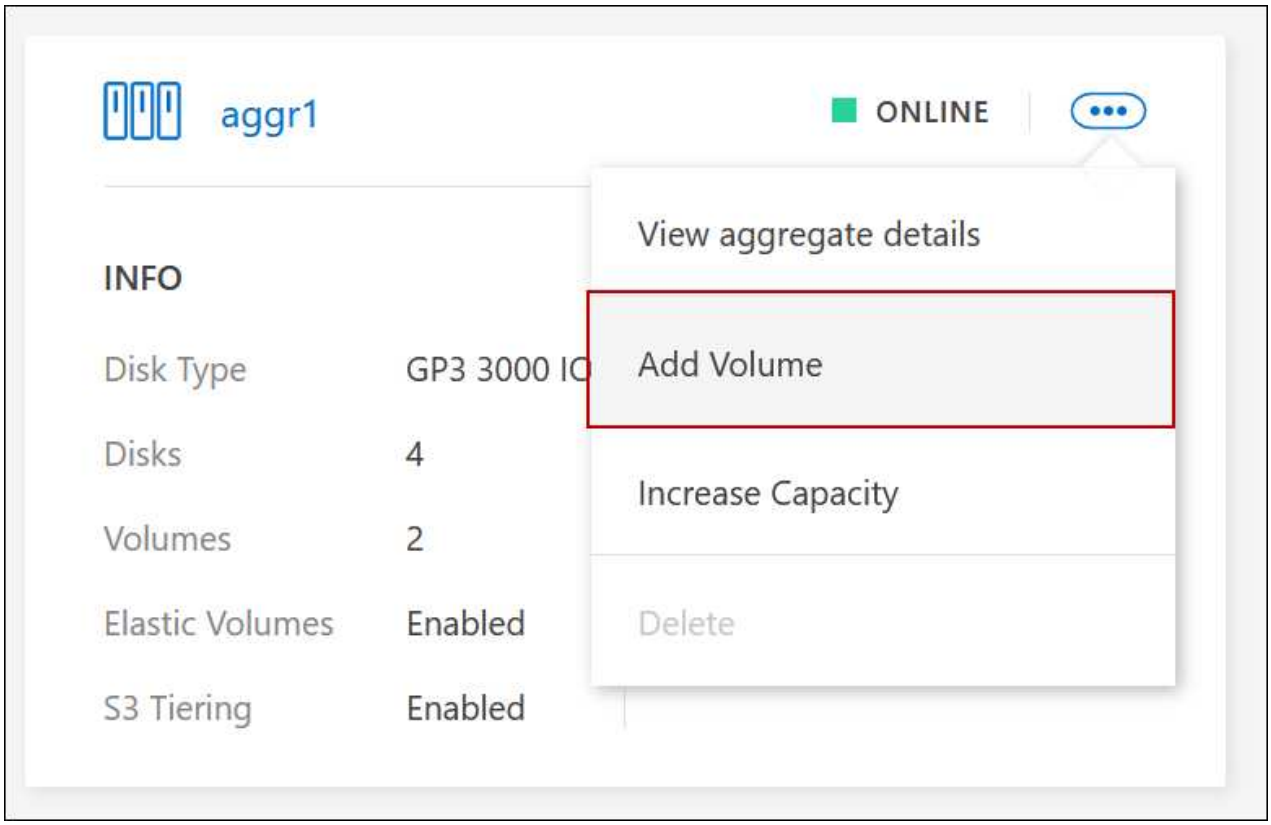
任何**Aggregate**

在「概觀」標籤上、瀏覽至「 Volume 」磚、然後按一下「 * 新增 Volume * 」。



特定**Aggregate**

在 Aggregate 索引標籤上、瀏覽至所需的 Aggregate 動態磚。按一下功能表圖示、然後按一下 * 新增 Volume * 。



4. 依照精靈中的步驟建立磁碟區。

   a. 詳細資料、保護及標記：輸入有關磁碟區的基本詳細資料、然後選取Snapshot原則。

      此頁面上的部分欄位是不知自明的。下列清單說明您可能需要指引的欄位：

欄位	說明
Volume名稱	您可以為新磁碟區輸入的可識別名稱。
Volume大小	您可以輸入的最大大小、主要取決於您是否啟用精簡配置、這可讓您建立比目前可用實體儲存容量更大的磁碟區。
儲存 VM （ SVM ）	儲存虛擬機器是 ONTAP 執行於支援內部的虛擬機器、可為您的用戶端提供儲存與資料服務。您可能知道這是 SVM 或 Vserver 。根據預設、系統會設定一個儲存 VM 、但部分組態會支援額外的儲存 VM 。 Cloud Volumes ONTAP 您可以為新的 Volume 指定儲存 VM 。
Snapshot 原則	Snapshot 複製原則會指定自動建立的 NetApp Snapshot 複本的頻率和數量。NetApp Snapshot 複本是一種不影響效能的時間點檔案系統映像、需要最少的儲存容量。您可以選擇預設原則或無。您可以針對暫時性資料選擇「無」：例如、 Microsoft SQL Server 的 Tempdb 。

   b. 傳輸協定：為磁碟區（NFS、CIFS或iSCSI）選擇傳輸協定、然後提供所需的資訊。

      如果您選取CIFS、但未設定伺服器、則在您按一下*「下一步」*之後、BlueXP會提示您設定CIFS連線功能。

      "瞭解支援的用戶端傳輸協定和版本"。

      以下各節將說明您可能需要指引的欄位。說明會依傳輸協定加以組織。

NFS

存取控制

選擇自訂匯出原則、讓用戶端可以使用磁碟區。

匯出原則

定義子網路中可存取磁碟區的用戶端。根據預設、BlueXP會輸入一個值、以供存取子網路中的所有執行個體。

CIFS

權限與使用者/群組

可讓您控制使用者和群組存取SMB共用區的層級（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。如果您指定網域Windows使用者名稱、則必須使用網域\使用者名稱格式來包含使用者的網域。

DNS 主要和次要 **IP** 位址

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

如果您要設定Google Managed Active Directory、AD預設可透過169.254.169.254 IP位址存取。

要加入的 **Active Directory** 網域

您要 CIFS 伺服器加入之 Active Directory （ AD ）網域的 FQDN 。

授權加入網域的認證資料

具有足夠權限的 Windows 帳戶名稱和密碼、可將電腦新增至 AD 網域內的指定組織單位（ OU ）。

CIFS 伺服器 **NetBios** 名稱

AD 網域中唯一的 CIFS 伺服器名稱。

組織單位

AD 網域中與 CIFS 伺服器相關聯的組織單位。預設值為「 CN= 電腦」。

- 若要將AWS託管Microsoft AD設定為Cloud Volumes ONTAP AD伺服器以供使用、請在此欄位中輸入* OID=computers,O=corp*。
- 若要將Azure AD網域服務設定為Cloud Volumes ONTAP AD伺服器以供使用、請在此欄位中輸入* OID=AADDC computers*或* OID=AADDC使用者*。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 說明文件：在 Azure AD 網域服務託管網域中建立組織單位（ OU ）"^]
- 若要將Google託管Microsoft AD設定為Cloud Volumes ONTAP AD伺服器以供使用、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託管Microsoft AD的組織單位"^]

DNS 網域

適用於整個儲存虛擬 Cloud Volumes ONTAP 機器（ SVM ）的 DNS 網域。在大多數情況下、網域與 AD 網域相同。

NTP 伺服器

選擇 * 使用 Active Directory 網域 * 來使用 Active Directory DNS 設定 NTP 伺服器。如果您需要使用不同的位址來設定 NTP 伺服器、則應該使用 API 。請參閱 "藍圖XP自動化文件" 以取得詳細資料。

請注意、您只能在建立CIFS伺服器時設定NTP伺服器。您建立CIFS伺服器之後、就無法進行設定。

iSCSI

LUN

iSCSI 儲存目標稱為 LUN （邏輯單元）、以標準區塊裝置的形式呈現給主機。建立iSCSI磁碟區時、BlueXP會自動為您建立LUN。我們只要在每個磁碟區建立一個LUN、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 "使用 IQN 從主機連線至 LUN"。

啟動器群組

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 目標可透過標準乙太網路介面卡（ NIC ）、 TCP 卸載引擎（ TOE ）卡（含軟體啟動器）、整合式網路介面卡（ CNA ）或專用主機匯流排介面卡（ HBA ）連線至網路、並由 iSCSI 合格名稱（ IQN ）識別。

a. 磁碟類型：根據您的效能需求和成本需求、為磁碟區選擇基礎磁碟類型。

   - "在 AWS 中調整系統規模"
     - "在 Azure 中調整系統規模"
     - "在Google Cloud中調整系統規模"

5. 使用率設定檔與分層原則：選擇是否啟用或停用磁碟區上的儲存效率功能、然後選取 "Volume分層原則"。

   包含多項儲存效率功能、可減少您所需的總儲存容量。 ONTAPNetApp 儲存效率功能提供下列效益：

   資源隨需配置

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

   重複資料刪除

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

   壓縮

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

6. 審查：檢閱磁碟區的詳細資料、然後按一下*新增*。

結果

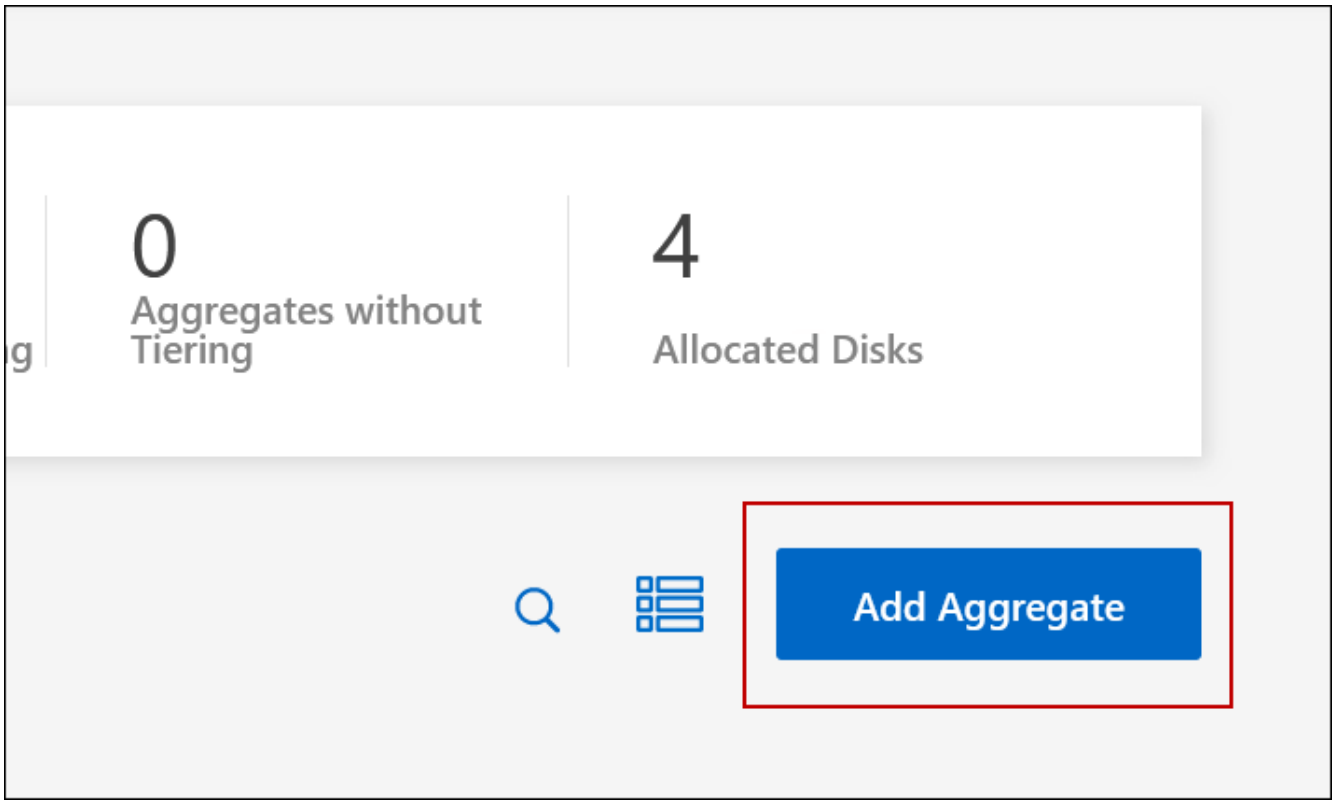
BlueXP會在Cloud Volumes ONTAP 整個系統上建立磁碟區。

在HA組態的第二個節點上建立磁碟區

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

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按兩下 Cloud Volumes ONTAP 您要管理集合體的運作環境名稱。
3. 在 Aggregate 索引標籤上、按一下 * 新增 Aggregate * 。
4. 從 _ 新增 Aggregate _ 畫面建立 Aggregate 。



5. 對於主節點、請在 HA 配對中選擇第二個節點。
6. 在BlueXP建立Aggregate之後、選取該集合體、然後按一下「*建立Volume *」。
7. 輸入新磁碟區的詳細資料、然後按一下「 * 建立 * 」。

結果

BlueXP會在HA配對的第二個節點上建立磁碟區。

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

建立Volume之後

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

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

管理現有磁碟區

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

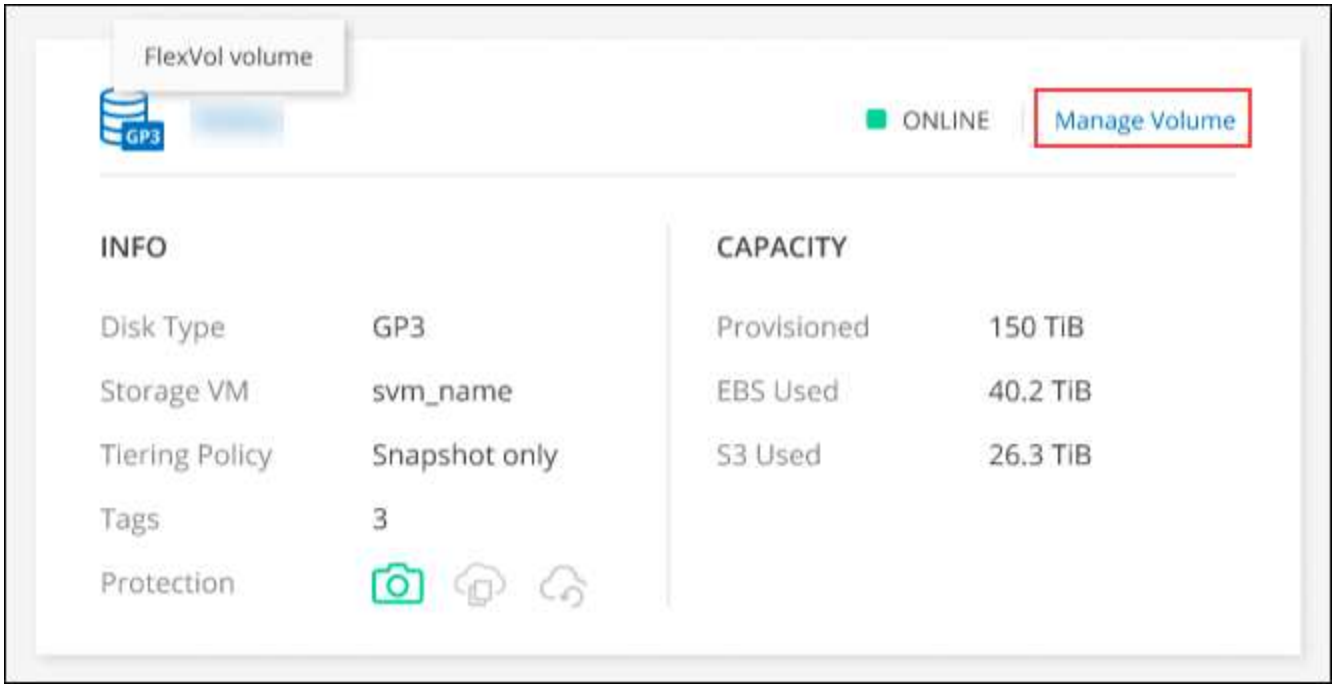
您可以在 BlueXP 標準檢視或進階檢視中管理磁碟區。「標準檢視」提供一組有限的選項來修改您的磁碟區。進階檢視提供進階管理層級、例如複製、調整大小、變更反勒索軟體的設定、分析、保護和活動追蹤、以及跨階層移動磁碟區。請參閱 "使用進階檢視來管理Cloud Volumes ONTAP"。

管理磁碟區

透過 BlueXP 標準檢視、您可以根據儲存需求來管理磁碟區。您可以檢視、編輯、複製、還原及刪除磁碟區。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按兩下 Cloud Volumes ONTAP 您要管理磁碟區的「功能區」工作環境。
3. 在工作環境中、按一下 * Volumes （磁碟區） * 標籤。



4. 在 Volumes （磁碟區）索引標籤上、瀏覽至所需的磁碟區標題、然後按一下 * Manage Volumes （管理磁碟區） * 以存取 Manage Volumes （管理磁碟區）右側面板。

工作	行動
檢視磁碟區的相關資訊	在「管理磁碟區」面板的「 Volume Actions 」（ Volume 動作）下、按一下「 * 檢視磁碟區詳細資料 * 」

工作	行動
取得 NFS 掛載命令	a. 在「管理磁碟區」面板的「 Volume Actions 」（ Volume 動作）下、按一下「 * 掛載命令 * 」。 b. 按一下 * 複本 * 。
複製磁碟區	a. 在「管理磁碟區」面板的「 Volume Actions 」（磁碟區動作）下、按一下「 * Clone the volume * 」（ b. 視需要修改複本名稱、然後按一下 * Clone （複製） * 。 此程序會建立 FlexClone Volume 。FlexClone Volume 是可寫入的時間點複本、空間效率極高、因為它會使用少量的空間作為中繼資料、然後只會在資料變更或新增時耗用額外空間。 若要深入瞭解 FlexClone Volume 、請參閱 "《 9 邏輯儲存管理指南》 ONTAP"。
編輯磁碟區（僅限讀寫磁碟區）	a. 在「管理磁碟區」面板的「 Volume Actions 」（磁碟區動作）下、按一下 * 「 Edit Volume settings* 」（ b. 修改磁碟區的 Snapshot 原則、 NFS 傳輸協定版本、 NFS 存取控制清單（匯出原則）或共用權限、然後按一下 * 套用 * 。 如果您需要自訂 Snapshot 原則、可以使用 System Manager 來建立。
刪除 Volume	a. 在「管理磁碟區」面板的「 Volume Actions 」（磁碟區動作）下、按一下「 * 刪除磁碟區 * 」 b. 在「刪除 Volume 」視窗下、輸入您要刪除的 Volume 名稱。 c. 再按一下 * 刪除 * 以確認。
隨需建立 Snapshot 複本	a. 在「管理磁碟區」面板的「保護動作」下、按一下 * 建立 Snapshot 複本 * 。 b. 視需要變更名稱、然後按一下「 * 建立 * 」。
將資料從 Snapshot 複本還原至新的 Volume	a. 在「管理磁碟區」面板的「保護動作」下、按一下 * 從 Snapshot 複本還原 * 。 b. 選取 Snapshot 複本、輸入新磁碟區的名稱、然後按一下 * 還原 * 。
變更基礎磁碟類型	a. 在「管理磁碟區」面板的「進階動作」下、按一下 * 變更磁碟類型 * 。 b. 選取磁碟類型、然後按一下 * 變更 * 。 BlueXP會將磁碟區移至使用所選磁碟類型的現有Aggregate、或為磁碟區建立新的Aggregate。

工作	行動
變更分層原則	a. 在「管理磁碟區」面板的「進階動作」下、按一下 * 變更階層原則 * 。 b. 選取不同的原則、然後按一下 * 變更 * 。 BlueXP會將磁碟區移至現有的Aggregate、該集合體使用所選的磁碟類型進行分層、或是為磁碟區建立新的Aggregate。
刪除 Volume	a. 選取磁碟區、然後按一下 * 刪除 * 。 b. 在對話方塊中輸入磁碟區的名稱。 c. 再按一下 * 刪除 * 以確認。

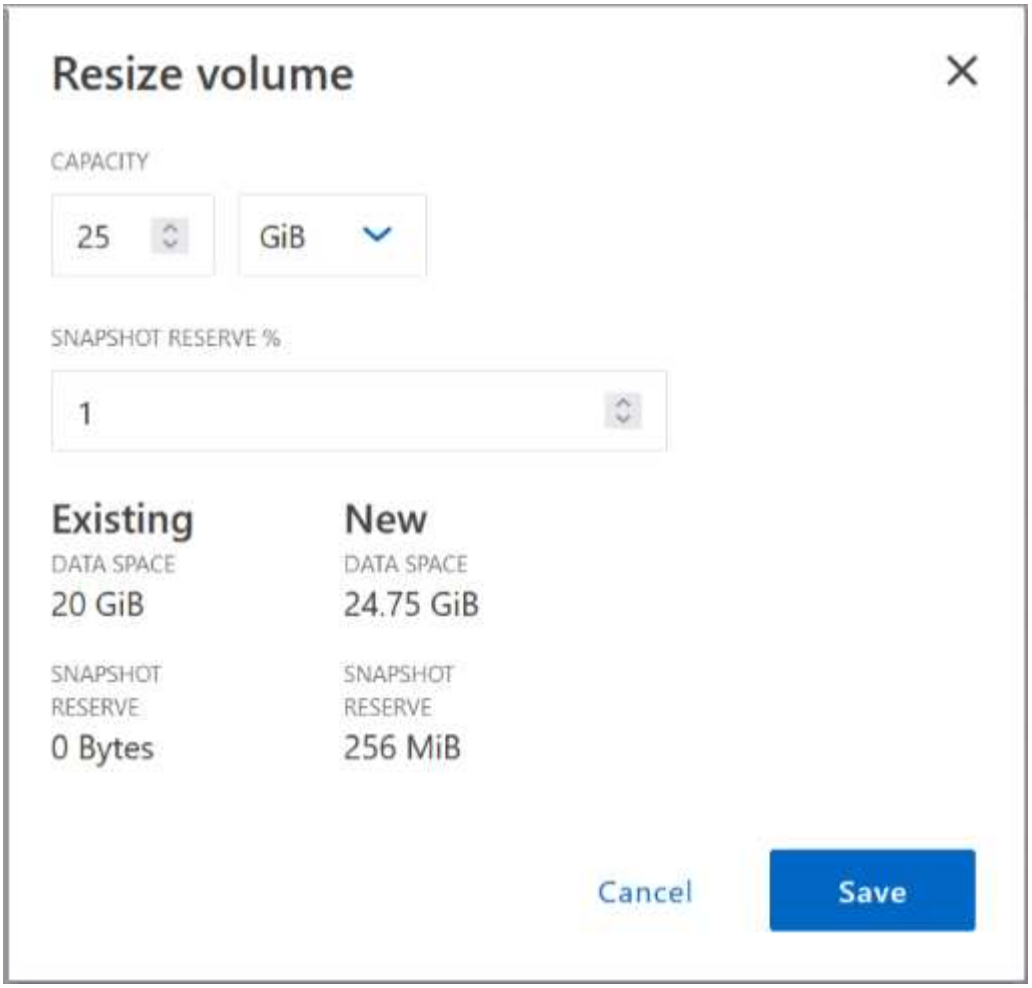
調整磁碟區大小

根據預設、當磁碟區空間不足時、它會自動增加至最大大小。預設值為 1 、 000 、這表示磁碟區的大小可增加至 11 倍。此值可在 Connector 的設定中設定。

如果您需要調整磁碟區大小、可以從 BlueXP 的「進階檢視」進行調整。

步驟

1. 開啟「進階檢視」、透過 System Manager 調整磁碟區大小。請參閱 "如何開始使用"。
2. 從左側導覽功能表中、選取 * 儲存 > 磁碟區 * 。
3. 從磁碟區清單中、找出您應該調整大小的磁碟區。
4. 按一下選項圖示 。
5. 選取 * 調整大小 * 。
6. 在 * 調整 Volume 大小 * 畫面上、視需要編輯容量和 Snapshot 保留百分比。您可以將現有的可用空間與修改後的容量進行比較。
7. 按一下「 * 儲存 * 」。



調整磁碟區大小時、請務必將系統的容量限制列入考量。前往 "發行說明 Cloud Volumes ONTAP" 以取得更多詳細資料。

修改**CIFS**伺服器

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

步驟

1. 在工作環境的「總覽」標籤中、按一下右側面板下方的「功能」標籤。
2. 在 "CIFS Setup （ CIFS 設置） " 字段下，單擊 *p鉛筆 圖標 * 以顯示 "CIFS Setup （ CIFS 設置） " 窗口。
3. 指定 CIFS 伺服器的設定：

工作	行動
選取儲存 VM （ SVM ）	選取 Cloud Volume ONTAP 儲存虛擬機器（ SVM ）會顯示其已設定的 CIFS 資訊。
要加入的 Active Directory 網域	您要 CIFS 伺服器加入之 Active Directory （ AD ）網域的 FQDN 。
授權加入網域的認證資料	具有足夠權限的 Windows 帳戶名稱和密碼、可將電腦新增至 AD 網域內的指定組織單位（ OU ）。

工作	行動
DNS 主要和次要 IP 位址	提供 CIFS 伺服器名稱解析的 DNS 伺服器 IP 位址。列出的 DNS 伺服器必須包含所需的服務位置記錄（ SRV), 才能找到 CIFS 伺服器要加入之網域的 Active Directory LDAP 伺服器和網域控制器。ifdef：：GCP[]如果您正在設定Google Managed Active Directory、則AD預設可透過169.254.169.254 IP位址存取。endif::GCP[]
DNS 網域	適用於整個儲存虛擬 Cloud Volumes ONTAP 機器（ SVM ）的 DNS 網域。在大多數情況下、網域與 AD 網域相同。
CIFS 伺服器 NetBios 名稱	AD 網域中唯一的 CIFS 伺服器名稱。
組織單位	AD 網域中與 CIFS 伺服器相關聯的組織單位。預設值為「 CN= 電腦」。 • 若要將AWS託管Microsoft AD設定為Cloud Volumes ONTAP AD伺服器以供使用、請在此欄位中輸入* OID=computers,O=corp*。 • 若要將Azure AD網域服務設定為Cloud Volumes ONTAP AD伺服器以供使用、請在此欄位中輸入* OID=AADDC computers*或* OID=AADDC使用者*。"Azure 說明文件：在 Azure AD 網域服務託管網域中建立組織單位（ OU ）" • 若要將Google託管Microsoft AD設定為Cloud Volumes ONTAP AD伺服器以供使用、請在此欄位中輸入* OU=computers,OU=Cloud *。"Google Cloud文件：Google託管Microsoft AD的組織單位"

4. 按一下 * 設定 * 。

結果

利用變更更新 CIFS 伺服器。 Cloud Volumes ONTAP

移動Volume

移動磁碟區以提高容量使用率、改善效能、並達成服務層級協議。

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

步驟

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

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

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

當BlueXP顯示「需要採取行動」訊息時、請移動磁碟區

BlueXP可能會顯示「必要行動」訊息、指出移動磁碟區是避免容量問題的必要條件、但您必須自行修正問題。如果發生這種情況、您需要找出如何修正問題、然後移動一或多個磁碟區。

當Aggregate已達到90%使用容量時、BlueXP會顯示這些必要行動訊息。如果啟用資料分層、則當Aggregate達到80%已使用容量時、訊息會顯示。根據預設、10%的可用空間會保留給資料分層。 "深入瞭解資料分層的可用空間比率"。

步驟

1. [找出如何修正容量問題]。
2. 根據您的分析、移動磁碟區以避免容量問題：
   - [將磁碟區移至其他系統、以避免發生容量問題]。
   - 將磁碟區移至其他Aggregate、以避免容量問題。

找出如何修正容量問題

如果BlueXP無法提供移動磁碟區以避免容量問題的建議、您必須識別需要移動的磁碟區、以及是否應該將它們移到同一個系統上的其他Aggregate或其他系統上。

步驟

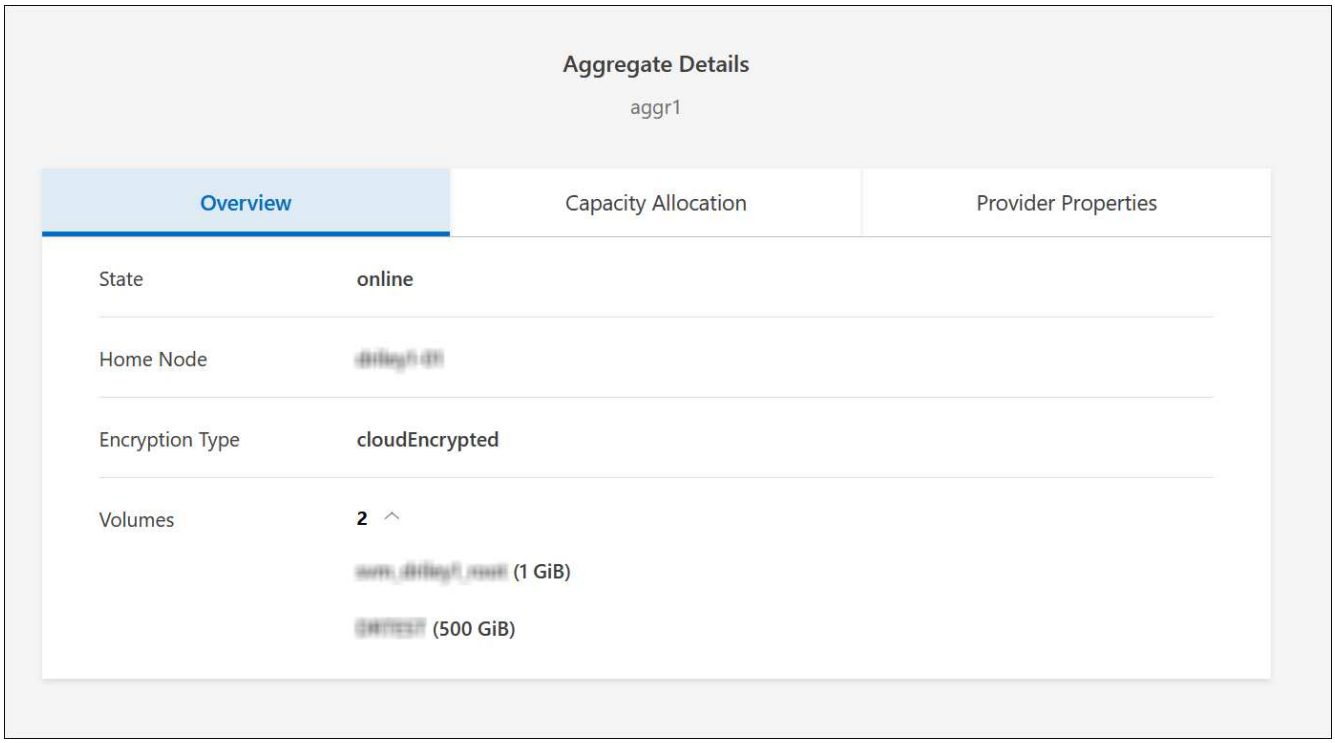
1. 檢視必要行動訊息中的進階資訊、以識別已達到容量上限的集合體。

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

2. 識別一個或多個要從集合體移出的磁碟區：

   a. 在工作環境中、按一下 * Aggregate 標籤 * 。
   b. 瀏覽至所需的 Aggregate 方塊、然後按一下 * 。 （省略符號圖示） > 檢視 Aggregate 詳細資料 * 。
   c. 在 Aggregate Details 畫面的 Overview （概觀）索引標籤下、檢閱每個 Volume 的大小、然後選擇一個或多個要移出 Aggregate 的 Volume 。

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



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

   如需詳細資訊、請參閱 將磁碟區移至其他Aggregate、以避免容量問題。

4. 如果系統已達到磁碟限制、請執行下列任何一項：
   a. 刪除所有未使用的磁碟區。
   b. 重新排列磁碟區、以釋放集合體上的空間。

      如需詳細資訊、請參閱 將磁碟區移至其他Aggregate、以避免容量問題。

   c. 將兩個或多個磁碟區移至另一個有空間的系統。

      如需詳細資訊、請參閱 將磁碟區移至其他Aggregate、以避免容量問題。

將磁碟區移至其他系統、以避免發生容量問題

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

關於這項工作

您可以依照此工作中的步驟來修正下列必要行動訊息：

> 移動磁碟區是避免容量問題的必要步驟、不過、由於系統已達到磁碟限制、因此BlueXP無法為您執行此動作。

步驟

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

2. 將來源工作環境拖放到目標工作環境、以執行磁碟區的一次性資料複寫。

   如需詳細資訊、請參閱 "在系統之間複寫資料"。

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

   如需詳細資訊、請參閱 "管理資料複寫排程和關係"。

4. 設定磁碟區以進行資料存取。

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

5. 刪除原始 Volume 。

   如需詳細資訊、請參閱 "管理磁碟區"。

將磁碟區移至其他**Aggregate**、以避免容量問題

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

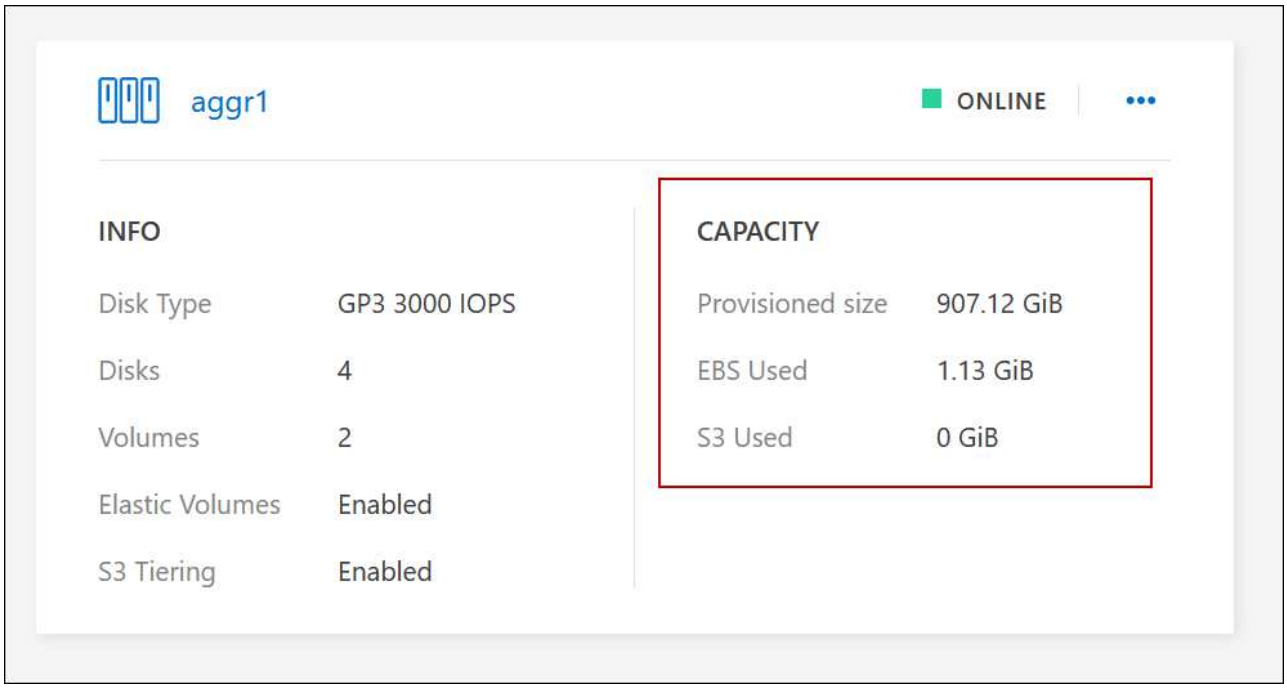
關於這項工作

您可以依照此工作中的步驟來修正下列必要行動訊息：

> 為了避免容量問題、必須移動兩個以上的磁碟區；不過、BlueXP無法為您執行此動作。

步驟

1. 驗證現有的 Aggregate 是否具有您需要移動的磁碟區可用容量：
   a. 在工作環境中、按一下 * Aggregate 標籤 * 。
   b. 瀏覽至所需的 Aggregate 方塊、然後按一下 * 。 （省略符號圖示） > 檢視 Aggregate 詳細資料 * 。
   c. 在 Aggregate 方塊下、檢視可用容量（資源配置大小減去使用的 Aggregate 容量）。



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

   如需詳細資訊、請參閱 "建立 Aggregate"。
4. 使用 System Manager 或 CLI 將磁碟區移至 Aggregate 。
5. 在大多數情況下、您可以使用 System Manager 來移動磁碟區。

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

磁碟區移動可能會緩慢執行的原因

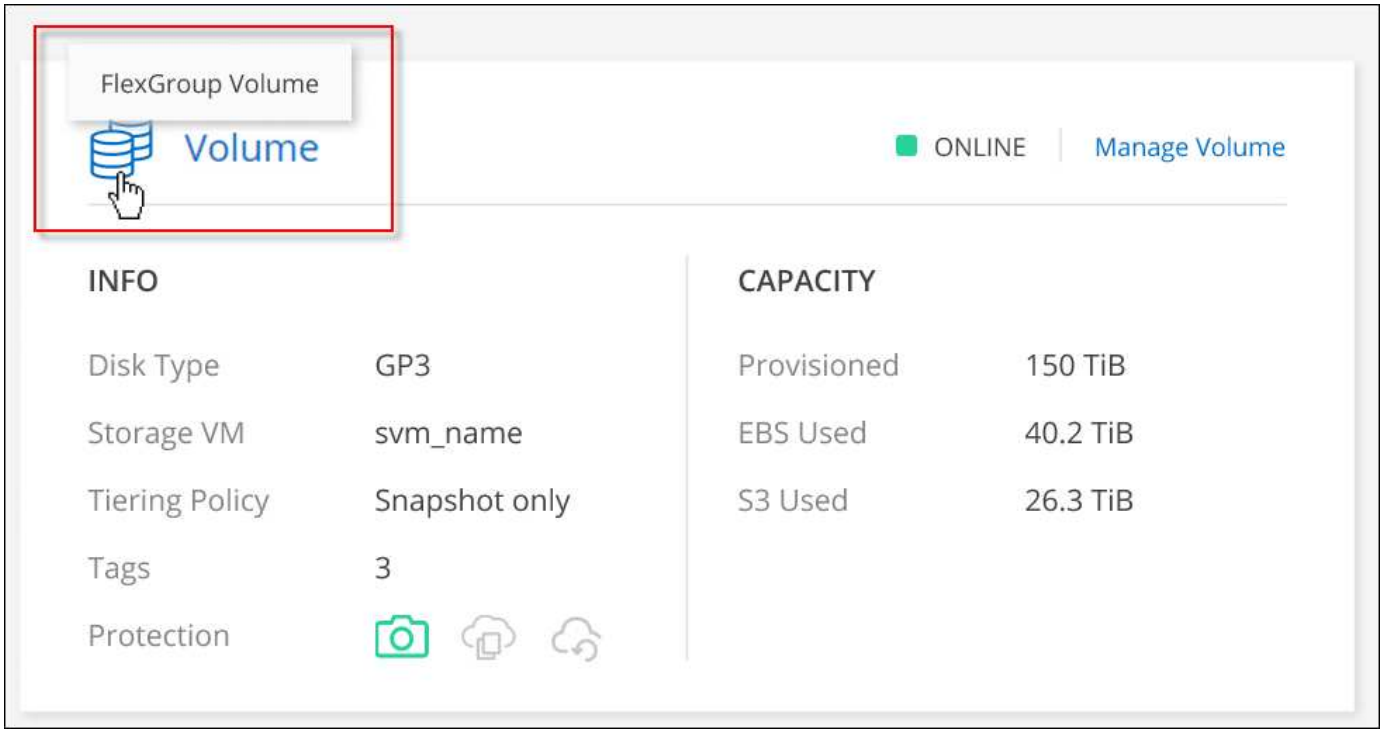
如果 Cloud Volumes ONTAP 下列任一情況屬實、則移動 Volume 所需時間可能比預期更長：

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

  如果在 9.4 版或更早版本的 Aggregate 上啟用資料分層、則會使用較舊的命名配置。
- 來源與目的地集合體上的加密設定不相符、或是正在進行重新金鑰。
- 在移動磁碟區時指定了 _ 分層原則 _ 選項、以變更分層原則。
- 磁碟區移動時指定了「 -generation-destination-key_ 」選項。

檢視 **FlexGroup Volume**

您可以直接透過 BlueXP 中的 Volumes （磁碟區）標籤、檢視透過 CLI 或系統管理員建立的 FlexGroup 磁碟區。BlueXP 與提供給 FlexVol Volume 的資訊相同、透過專用的 Volumes 方塊、提供建立的 FleGroup Volume 的詳細資訊。在「 Volume （磁碟區）」磚下方、您可以透過圖示的暫留文字來識別每個 FlexGroup 磁碟區群組。此外、您也可以透過 Volume 樣式欄、在 Volume 清單檢視下識別及排序 FlexGroup Volume 。



目前、您只能在 BlueXP 下檢視現有的 FlexGroup 磁碟區。在 BlueXP 中建立 FlexGroup 磁碟區的功能無法使用、但已計畫在未來版本中使用。

將非作用中資料分層至低成本物件儲存設備

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

若要設定資料分層、您需要執行下列動作：

1 選擇支援的組態

支援大部分的組態。如果Cloud Volumes ONTAP 您的系統執行的是最新版本、那麼您應該會很滿意。 "深入瞭解"。

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

- 對於 AWS 、您需要 VPC 端點對 S3 。 深入瞭解。
- 對於Azure而言、只要BlueXP具備必要的權限、您就不需要執行任何操作。 深入瞭解。

- 若為Google Cloud、您需要設定私有Google Access的子網路、並設定服務帳戶。 深入瞭解。

3 請確定您已啟用分層功能、並有一個 **Aggregate**

必須在集合體上啟用資料分層、才能在磁碟區上啟用資料分層。您應該瞭解新磁碟區和現有磁碟區的需求。 深入瞭解。

4 建立、修改或複寫磁碟區時、請選擇分層原則

在建立、修改或複寫磁碟區時、BlueXP會提示您選擇分層原則。

- "在讀寫磁碟區上分層資料"
- "在資料保護磁碟區上分層資料"

什麼是資料分層不需要的？ **#8217** ？

- 您不需要安裝功能授權、就能進行資料分層。
- 您不需要為容量層建立物件存放區。BlueXP能為您實現這項目標。
- 您不需要在系統層級啟用資料分層。

  在系統建立時、BlueXP會為Cold資料建立物件存放區、 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功能（在某些情況下、 在 Aggregate 上）。

支援資料分層的組態

您可以在使用特定組態和功能時啟用資料分層。

AWS支援

- AWS支援資料分層功能、從Cloud Volumes ONTAP 功能表9.2開始。
- 效能層可以是通用SSD（GP3或gp2）或已配置的IOPS SSD（IO1）。

使用處理量最佳化的HDD（ST1）時、不建議將資料分層至物件儲存設備。

支援**Azure**

- Azure支援下列資料分層：
  - 9.4版、搭配單一節點系統
  - 9.6版、搭配HA配對
- 效能層可以是優質SSD託管磁碟、標準SSD託管磁碟或標準HDD託管磁碟。

支援**Google Cloud**

- Google Cloud支援資料分層功能、從Cloud Volumes ONTAP 推出的功能僅支援32個9.6個。
- 效能層可以是SSD持續磁碟、平衡持續磁碟或標準持續磁碟。

功能互通性

- 加密技術支援資料分層。
- 必須在磁碟區上啟用精簡配置。

需求

視您的雲端供應商而定、必須設定特定的連線和權限、 Cloud Volumes ONTAP 以便讓效益管理系統將冷資料分層處理至物件儲存設備。

將冷資料分層至 **AWS S3** 的需求

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

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

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

將冷資料分層至 **Azure Blob** 儲存設備的需求

只要BlueXP具備必要的權限、您就不需要在效能層與容量層之間建立連線。如果Connector的自訂角色具有下列權限、則BlueXP會為您啟用vnet服務端點：

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

根據預設、權限會包含在自訂角色中。 "檢視Azure對Connector的權限"

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

- 駐留的子網路 Cloud Volumes ONTAP 必須設定為私有 Google Access 。如需相關指示、請參閱 "Google Cloud 文件：設定私有 Google Access"。
- 服務帳戶必須附加Cloud Volumes ONTAP 至

  "瞭解如何設定此服務帳戶"。

  當您建立Cloud Volumes ONTAP 一個運作環境時、系統會提示您選擇此服務帳戶。

  如果您在部署期間未選擇服務帳戶、則必須關閉Cloud Volumes ONTAP 該服務帳戶、前往Google Cloud主控台、然後將該服務帳戶附加至Cloud Volumes ONTAP 該故障。然後、您可以依照下一節所述、啟用資料分層。

- 若要使用客戶管理的加密金鑰來加密儲存區、請啟用Google Cloud儲存區使用金鑰。

  "瞭解如何搭配Cloud Volumes ONTAP 使用客戶管理的加密金鑰"。

只要沒有連線或權限問題、在建立系統時、BlueXP就會建立Cold資料的物件存放區。如果您在建立系統之後才實作上述需求、則需要透過建立物件存放區的 API 或系統管理員手動啟用分層功能。

未來的 Cloud Volumes ONTAP 版本將提供透過 BlueXP 使用者介面進行分層的功能。

確保在 **Aggregate** 上啟用分層

必須在集合體上啟用資料分層、才能在磁碟區上啟用資料分層。您應該瞭解新磁碟區和現有磁碟區的需求。

- * 新磁碟區 *

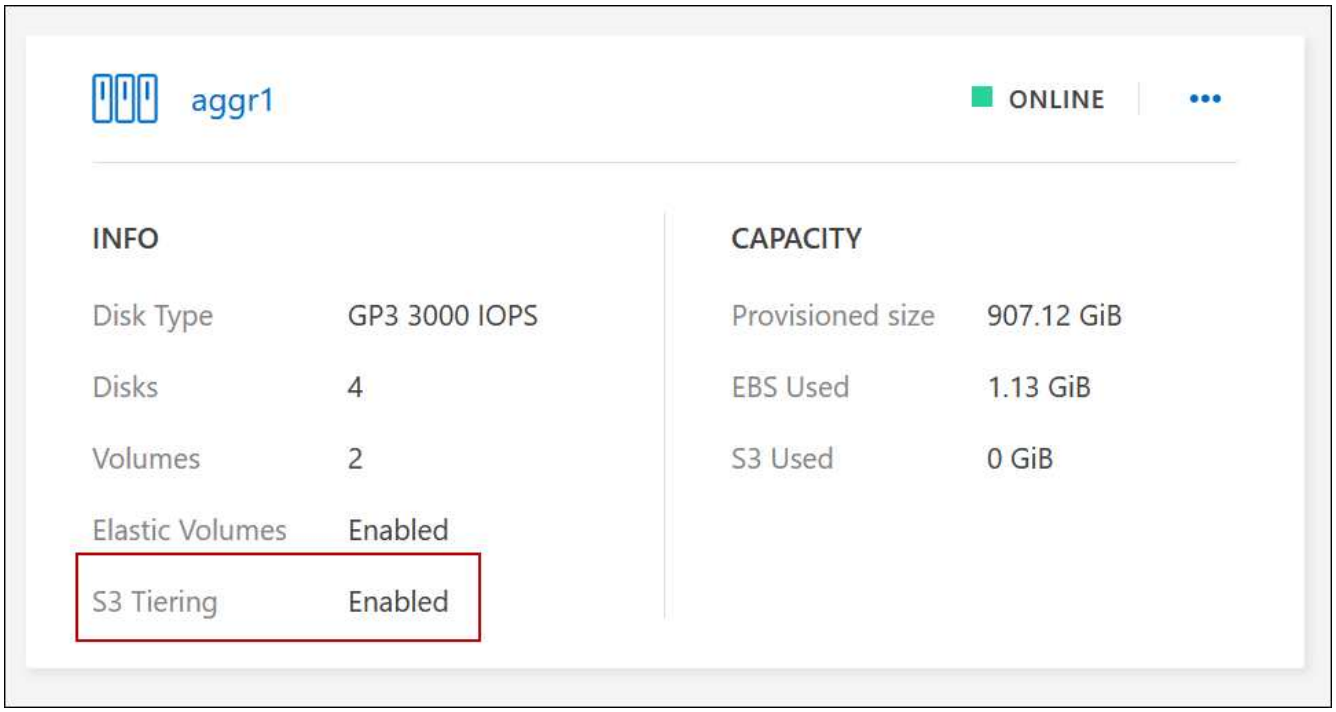
  如果您要在新磁碟區上啟用資料分層功能、就不需要擔心在集合體上啟用資料分層功能。BlueXP會在已啟用分層功能的現有Aggregate上建立磁碟區、或是在啟用資料分層功能的Aggregate不存在的情況下、為磁碟區建立新的Aggregate。

- * 現有磁碟區 *

  如果您想要在現有磁碟區上啟用資料分層、則必須確保已在基礎 Aggregate 上啟用資料分層。如果在現有的 Aggregate 上未啟用資料分層、則需要使用 System Manager 將現有的 Aggregate 附加至物件存放區。

確認是否在 **Aggregate** 上啟用分層的步驟

1. 在BlueXP中開啟工作環境。
2. 按一下 Aggregate 索引標籤。
3. 瀏覽至所需的方塊、並驗證是否已在 Aggregate 上啟用或停用分層。



在集合體上啟用分層的步驟

1. 在 System Manager 中、按一下 * Storage > Tiers* 。

2. 按一下 Aggregate 的動作功能表、然後選取 * 附加 Cloud Tiers* 。
3. 選取要附加的雲端層、然後按一下「 * 儲存 * 」 。

接下來呢？

您現在可以在新的和現有的磁碟區上啟用資料分層、如下一節所述。

從讀寫磁碟區分層資料

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

步驟

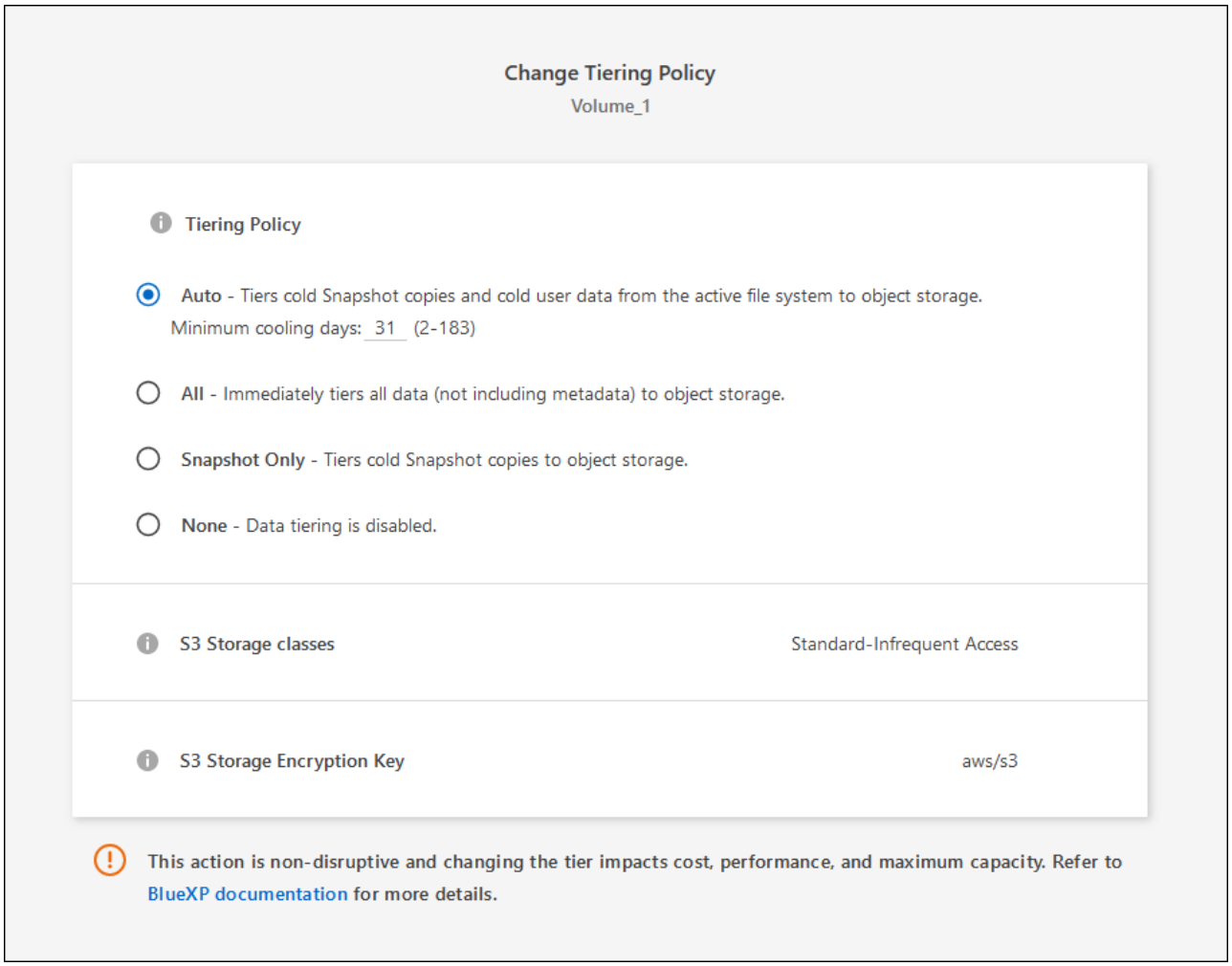
1. 在工作環境下的 Volumes （磁碟區）標籤中、建立新的磁碟區或變更現有磁碟區的層級：

工作	行動
建立新的 Volume	按一下「 * 新增 Volume * 」 。
修改現有的 Volume	選取所需的磁碟區方塊、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 * 進階動作 * 和 * 變更分層原則 * 。

2. 選取分層原則。

   如需這些原則的說明、請參閱 "資料分層總覽"。

   ◦ 範例 *



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

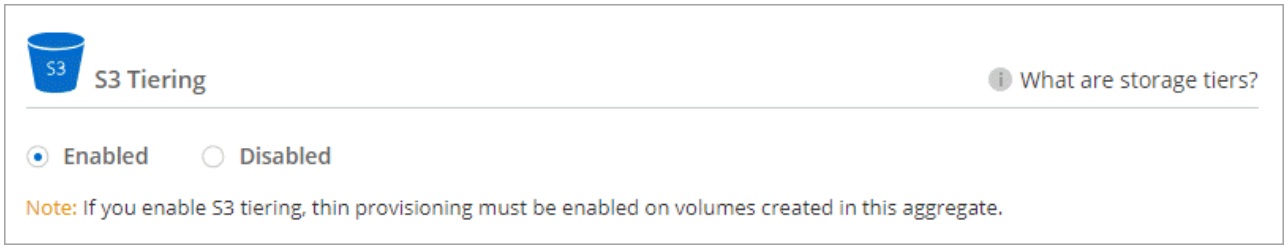
從資料保護磁碟區分層資料

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

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、選取包含來源磁碟區的工作環境、然後將其拖曳至您要複寫磁碟區的工作環境。
3. 依照提示操作、直到您到達分層頁面、並啟用資料分層以供物件儲存使用。

    ◦ 範例 *



如需複寫資料的說明、請參閱 "在雲端之間複寫資料"。

變更階層式資料的儲存類別

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

階層式資料的儲存類別是全系統的、並非每個 Volume 都有。

如需支援的儲存類別資訊、請參閱 "資料分層總覽"。

步驟

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

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Cloud Volumes ONTAP 將資料分層儲存至物件儲存時、需要多少空間才能在物件SSD/HDD上使用。預設設定為10%可用空間、但您可以根據需求調整設定。

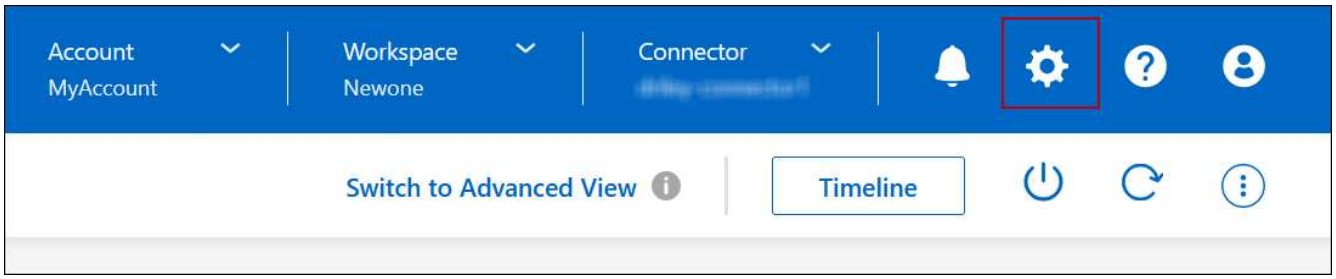
例如、您可以選擇少於10%的可用空間、以確保您使用購買的容量。然後、當需要額外容量時、BlueXP可以為您購買額外的磁碟（直到達到Aggregate的磁碟限制為止）。

如果空間不足、Cloud Volumes ONTAP 則無法移動資料、可能會導致效能降低。任何變更都應謹慎進行。如果您不確定、請聯絡NetApp支援部門以取得指引。

此比率對災難恢復案例非常重要、因為Cloud Volumes ONTAP 當資料從物件儲存區讀取時、將資料移至SSD/HDD以提供更好的效能。如果空間不足、Cloud Volumes ONTAP 則無法移動資料。在變更比率時、請將此納入考量、以便符合您的業務需求。

步驟

1. 在 BlueXP 主控台的右上角、按一下 * 設定 * 圖示、然後選取 * Cloud Volumes ONTAP 設定 * 。



2. 在* Capacity 下、按一下 Aggregate Capacity臨界值- Free Space Ratio for Data Tiering *。
3. 根據您的需求變更可用空間比率、然後按一下「儲存」。

變更自動分層原則的冷卻週期

如果Cloud Volumes ONTAP 您使用_auto_分層原則在某個SURFVolume上啟用資料分層、您可以根據業務需求調整預設的冷卻時間。此動作僅支援使用 API 和 CLI 。

冷卻期間是指磁碟區中的使用者資料在被視為「冷」並移至物件儲存設備之前、必須保持非作用中狀態的天數。

自動分層原則的預設冷卻期間為31天。您可以變更冷卻期間、如下所示：

- 9.8或更新版本：2天至183天
- 9.7或更早：2天至63天

步驟

1. 建立磁碟區或修改現有磁碟區時、請將_mirumCoolingDays參數與API要求搭配使用。

將**LUN**連接至主機

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

請注意下列事項：

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

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按兩下 Cloud Volumes ONTAP 您要管理磁碟區的「功能區」工作環境。
3. 在工作環境中、按一下 * Volumes （磁碟區） * 標籤。
4. 在 Volumes （磁碟區）索引標籤上、瀏覽至所需的磁碟區標題、然後按一下 * Manage Volumes （管理磁碟區） * 以存取 Manage Volumes （管理磁碟區）右側面板。
5. 按一下 * 目標 IQN* 。
6. 按一下「 * 複製 * 」以複製 IQN 名稱。
7. 設定從主機到 LUN 的 iSCSI 連線。
    - "適用於 Red Hat Enterprise Linux 的支援 9 iSCSI Express 組態：啟動目標的 iSCSI 工作階段 ONTAP"
    - "適用於 Windows 的 S89 iSCSI Express 組態：以目標啟動 iSCSI 工作階段 ONTAP"
    - "SAN主機組態ONTAP"

利用**NetApp**功能加速資料存取**FlexCache**

FlexCache Volume 是一種儲存磁碟區、可從來源（或來源）磁碟區快取 SMB 和 NFS 讀取資料。後續讀取快取資料會加快該資料的存取速度。

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

BlueXP 提供 FlexCache 磁碟區的管理功能 "BlueXP Volume 快取" 服務：

您也可以使用 ONTAP CLI 或 ONTAP 系統管理員來建立及管理 FlexCache 磁碟區：

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

BlueXP 會為所有新的 Cloud Volumes ONTAP 系統產生 FlexCache 授權。授權包含500 GiB使用限制。

Aggregate管理

建立Aggregate

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

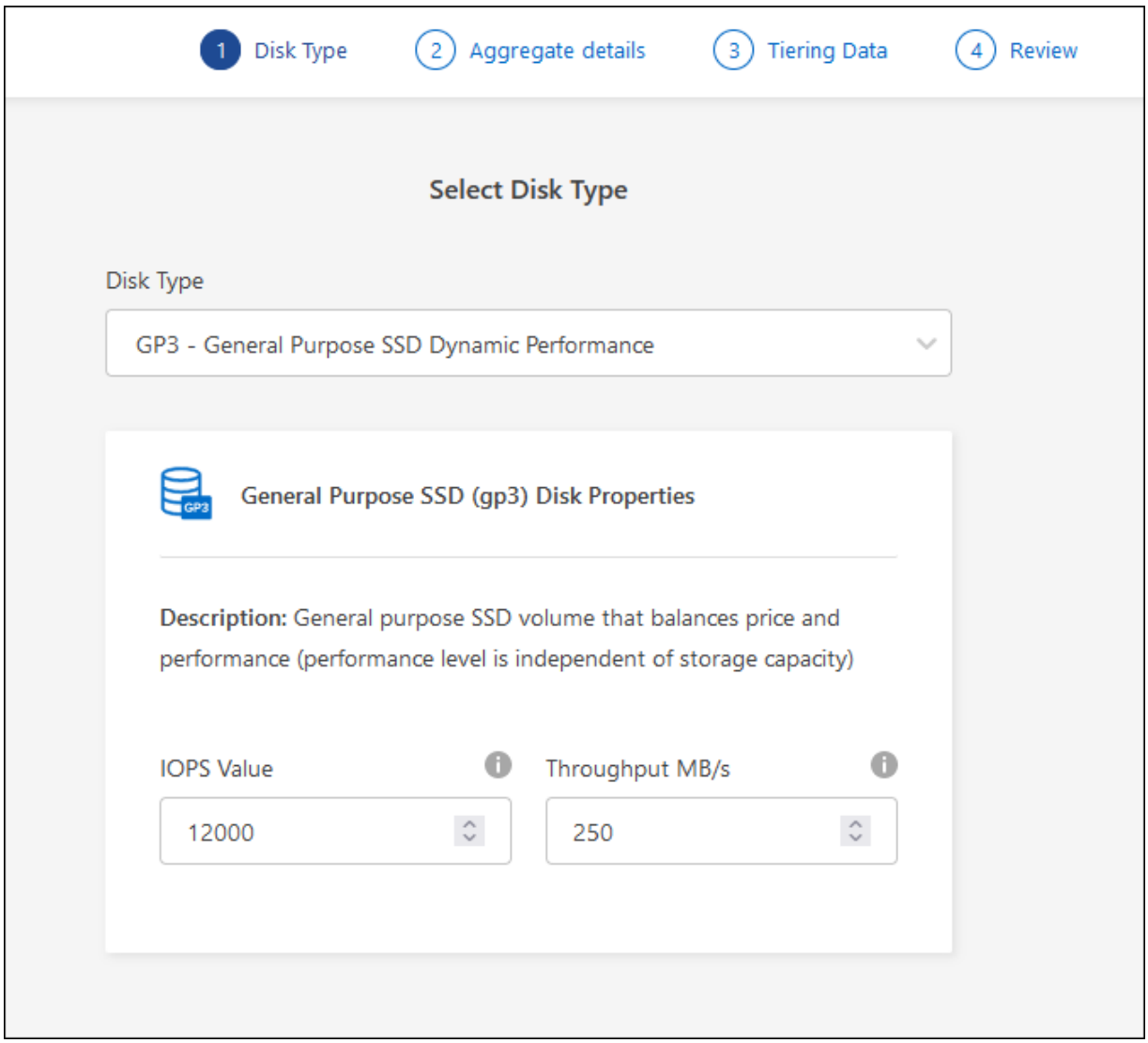
所有磁碟和集合體都必須直接從BlueXP建立和刪除。您不應從其他管理工具執行這些動作。這樣做可能會影響系統穩定性、阻礙未來新增磁碟的能力、並可能產生備援雲端供應商費用。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按兩下 Cloud Volumes ONTAP 您要管理集合體的實例名稱。
3. 在 Aggregate 索引標籤上、按一下 * 新增 Aggregate * 、然後指定 Aggregate 的詳細資料。

AWS

- 如果系統提示您選擇磁碟類型和磁碟大小、請參閱 "在Cloud Volumes ONTAP AWS中規劃您的不一樣組態"。
- 如果系統提示您輸入Aggregate的容量大小、則表示您要在支援Amazon EBS彈性磁碟區功能的組態上建立Aggregate。下列螢幕快照顯示由GP3磁碟組成的新Aggregate範例。



"深入瞭解彈性磁碟區的支援"。

Azure

如需磁碟類型與磁碟大小的說明、請參閱 "在Cloud Volumes ONTAP Azure中規劃您的不一樣組態"。

Google Cloud

如需磁碟類型與磁碟大小的說明、請參閱 "在Cloud Volumes ONTAP Google Cloud規劃您的不一樣組態"。

4. 按一下「 * 執行 * 」、然後按一下「 * 核准並購買 * 」。

管理集合體

新增磁碟、檢視有關集合體的資訊、以及刪除這些磁碟來管理集合體。

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

開始之前

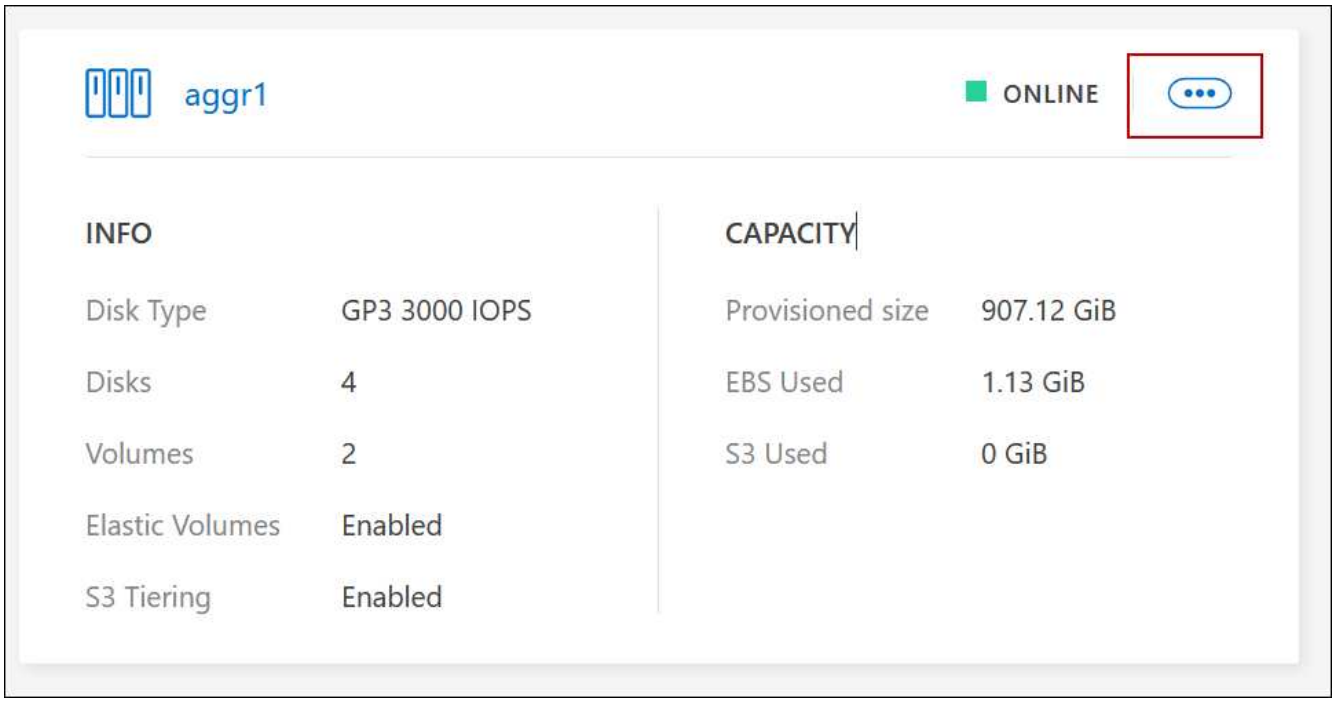
如果您要刪除 Aggregate 、則必須先刪除 Aggregate 中的磁碟區。

關於這項工作

如果Aggregate空間不足、您可以使用System Manager將磁碟區移至其他Aggregate。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按兩下 Cloud Volumes ONTAP 您要管理集合體的功能性工作環境。
3. 在工作環境中、按一下 * Aggregate * 標籤。
4. 在 Aggregate 索引標籤上、瀏覽至所需標題、然後按一下 * 。 （省略符號圖示） * 。



5. 管理您的 Aggregate ：

工作	行動
檢視有關 Aggregate 的資訊	在 … （省略符號圖示）功能表下、按一下 * 檢視 Aggregate details* 。
在特定 Aggregate 上建立磁碟區	在 … （省略號圖示）功能表下、按一下 * 新增 Volume * 。

工作	行動
將磁碟新增至 Aggregate	a. 在 … （省略號圖示）功能表下、按一下 * 新增磁碟 * 。 b. 選取您要新增的磁碟數目、然後按一下「 * 新增 * 」。 集合體中的所有磁碟大小必須相同。
增加支援Amazon EBS彈性Volume的Aggregate容量	a. 在 … （省略符號圖示）功能表下、按一下 * 增加容量 * 。 b. 輸入您要新增的額外容量、然後按一下 * 增加 * 。 請注意、您必須將Aggregate的容量增加至少256 GiB或集合體大小的10%。 例如、如果您有1.77 TiB Aggregate、則10%為181 GiB。此值低於256 GiB、因此集合體的大小必須至少增加256 GiB。
刪除 Aggregate	a. 選取不包含任何磁碟區的 Aggregate tile 按一下 * 。 （省略符號圖示） > 刪除 * 。 b. 再按一下 * 刪除 * 以確認。

管理**Connector**上的容量設定

每個Connector都有設定、可決定其如何管理Cloud Volumes ONTAP 用於實現效益的Aggregate容量。

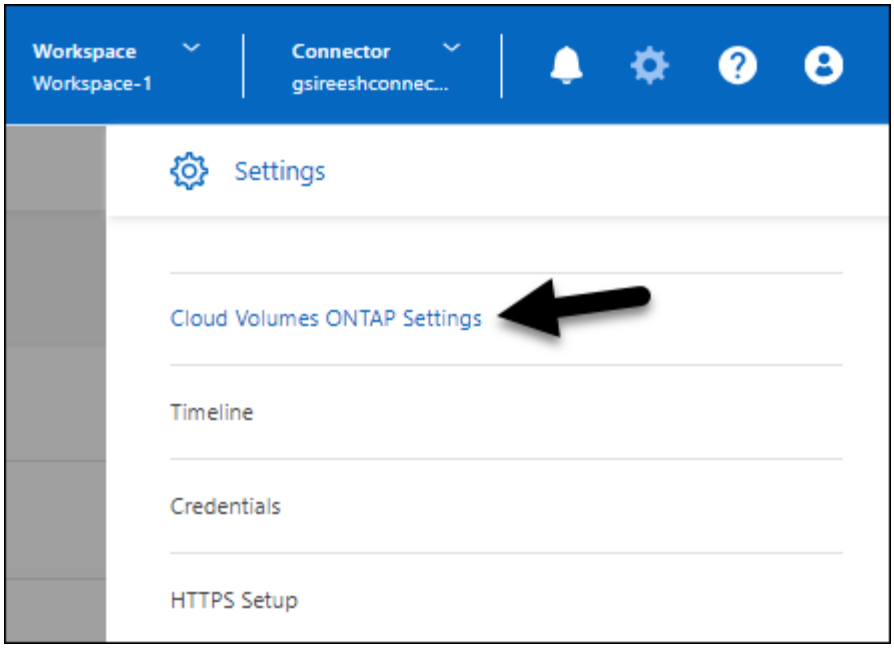
這些設定會影響Cloud Volumes ONTAP 由Connector管理的所有功能不全系統。如果您有另一個Connector、則可以以不同的方式設定。

必要權限

修改 Cloud Volumes ONTAP 設定需要帳戶管理權限。

步驟

1. 在 BlueXP 主控台的右上角、按一下「設定」圖示、然後選取 * 「 Cloud Volumes ONTAP 設定 * 」。



2. 在* Capacity *下、修改下列任何設定：

容量管理模式

選擇BlueXP是否通知您儲存容量決策、或是BlueXP是否自動為您管理容量需求。

"瞭解容量管理模式的運作方式"。

Aggregate Capacity 臨界值 **-** 可用空間比率

此比率是容量管理決策的關鍵參數、無論您是處於自動或手動的容量管理模式、瞭解其影響都是不可或缺的。建議您根據您的特定儲存需求和預期成長來設定此臨界值、以在資源使用率和成本之間維持平衡。

在手動模式中、如果集合體上的可用空間比率降至低於指定臨界值、就會觸發通知、提醒您應採取行動來解決可用空間比率過低的問題。請務必監控這些通知、並手動管理彙總容量、以避免服務中斷並確保最佳效能。

可用空間比率的計算方式如下：
（Aggregate capcap處理 能力- Aggregate上的總使用容量）/ Aggregate cap處理 能力

請參閱 "自動容量管理" 若要立即瞭解、容量會自動在 Cloud Volumes ONTAP 中管理。

Aggregate Capacity 臨界值 **-** 資料分層的可用空間比率

定義將資料分層至容量層（物件儲存）時、效能層（磁碟）需要多少可用空間。

這種比率對於災難恢復方案非常重要。從容量層讀取資料時Cloud Volumes ONTAP 、將資料移至效能層、以提供更好的效能。如果空間不足、Cloud Volumes ONTAP 則無法移動資料。

3. 按一下「 * 儲存 * 」 。

儲存VM管理

在BlueXP中管理儲存VM

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

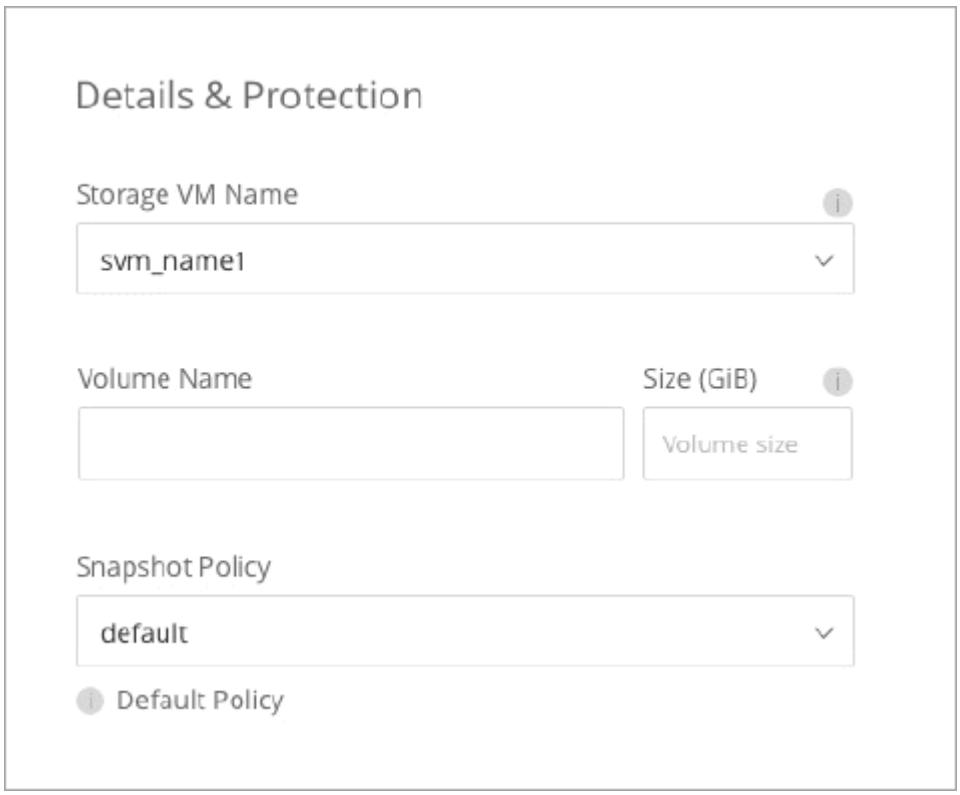
支援的儲存 VM 數量

某些組態支援多個儲存VM。前往 "發行說明 Cloud Volumes ONTAP" 驗證Cloud Volumes ONTAP 支援的儲存VM數量是否適用於您的版本的支援。

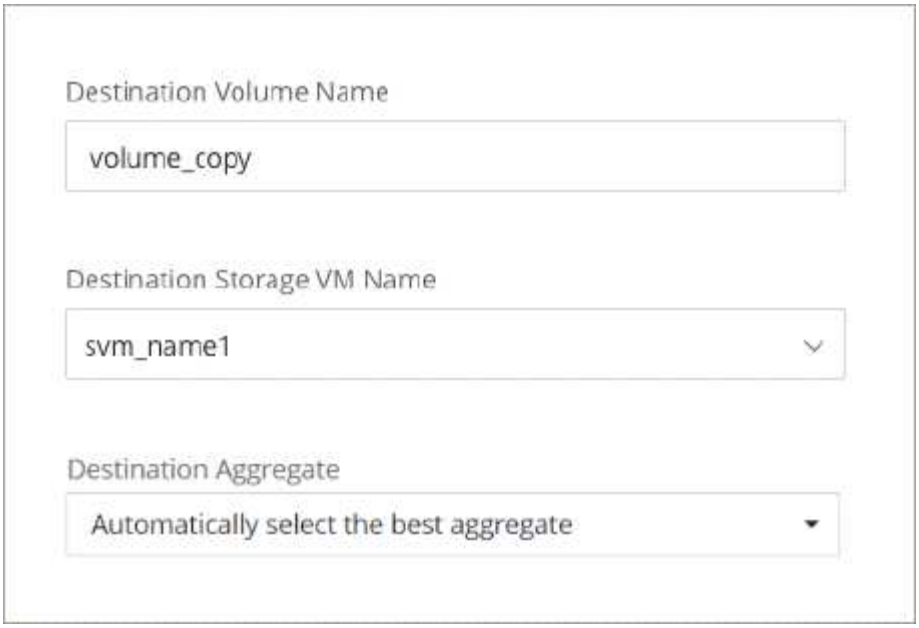
使用多個儲存VM

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

例如、下圖顯示如何在建立 Volume 時選擇儲存 VM 。



下圖顯示如何在將磁碟區複寫至其他系統時、選擇儲存 VM 。



修改預設儲存**VM**的名稱

BlueXP會自動命名為其所建立的Cloud Volumes ONTAP 單一儲存VM、以利執行效能。如果您有嚴格的命名標準、則可以從 System Manager 、 CLI 或 API 修改儲存 VM 的名稱。例如、您可能希望名稱與您為 ONTAP 自己的叢集命名儲存虛擬機器的方式相符。

在**Cloud Volumes ONTAP AWS**中建立資料服務儲存**VM**以供其使用

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

若要建立額外的資料服務儲存VM、您需要在AWS中分配IP位址、然後根據ONTAP 您的靜態組態執行支援功能指令。Cloud Volumes ONTAP

支援的儲存 **VM** 數量

從9.7版開始、特定Cloud Volumes ONTAP 的支援功能可支援多個儲存VM。前往 "發行說明 Cloud Volumes ONTAP" 驗證Cloud Volumes ONTAP 支援的儲存VM數量是否適用於您的版本的支援。

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

驗證組態的限制

每個EC2執行個體都支援每個網路介面的私有IPv4位址數目上限。在AWS中為新的儲存VM分配IP位址之前、您必須先確認限制。

步驟

1. 請選擇 "《不知》中的「儲存限制」區段Cloud Volumes ONTAP"。
2. 識別執行個體類型的每個介面IP位址數目上限。

3. 請記下這個數字、因為您在AWS中分配IP位址時、會在下一節中需要這個數字。

在**AWS**中分配**IP**位址

在為新的儲存VM建立生命期之前、必須先將私有的IPv4位址指派給AWS中的連接埠e0a。

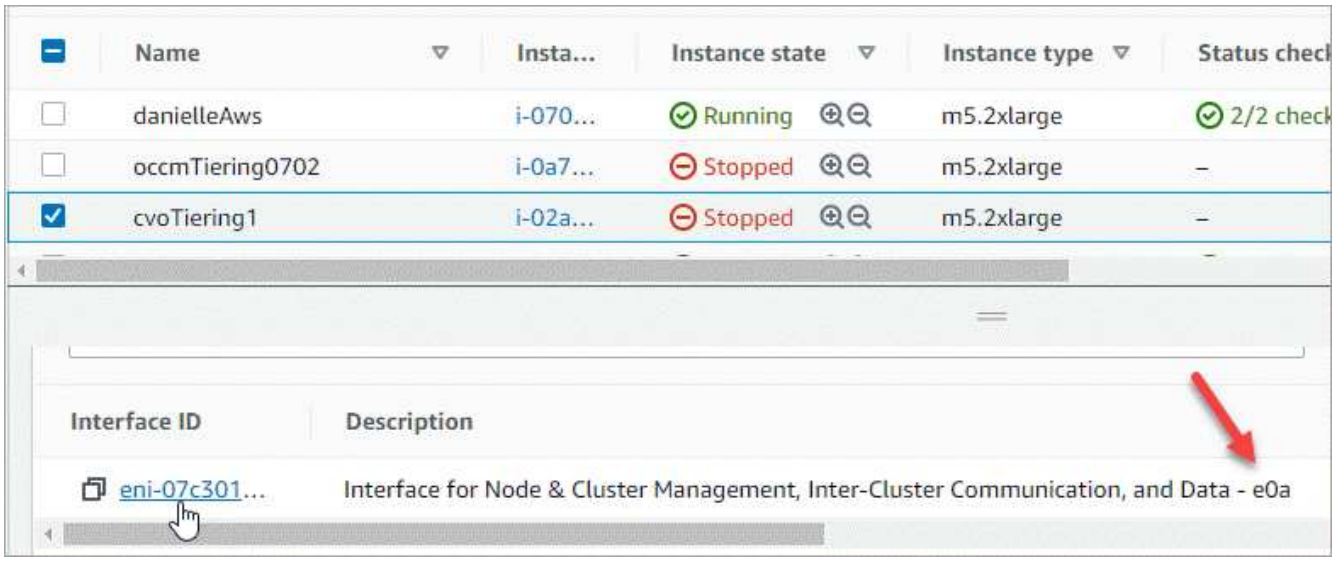
請注意、儲存VM的選用管理LIF需要在單一節點系統和單一AZ的HA配對上使用私有IP位址。此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

步驟

1. 登入AWS並開啟EC2服務。
2. 選取Cloud Volumes ONTAP 「這個實例」、然後按一下「網路」。

   如果您要在HA配對上建立儲存VM、請選取節點1。

3. 向下捲動至*網路介面*、然後按一下*介面ID*以取得連接埠e0a。



4. 選取網路介面、然後按一下*「動作」>「管理IP位址」*。
5. 展開e0a的IP位址清單。
6. 驗證IP位址：
   a. 計算已分配IP位址的數量、以確認連接埠是否有空間可用於其他IP。

      您應該已經在本頁上一節中找出每個介面支援的IP位址上限。

   b. 選用：前往CLI Cloud Volumes ONTAP 執行*網路介面show*以確認每個IP位址都在使用中。

      如果IP位址未在使用中、您可以將其與新的儲存VM搭配使用。

7. 回到AWS主控台、按一下*指派新的IP位址*、根據新儲存VM所需的容量來指派額外的IP位址。
   - 單節點系統：需要一個未使用的次要私有IP。

     若要在儲存VM上建立管理LIF、則需要選用的次要私有IP。

- 單一AZ中的HA配對：節點1上需要一個未使用的次要私有IP。

  若要在儲存VM上建立管理LIF、則需要選用的次要私有IP。

- 多個AZs中的HA配對：每個節點需要一個未使用的次要私有IP。

8. 如果您要在單一AZ中分配HA配對的IP位址、請啟用*允許重新指派次要私有IPV4位址*。
9. 按一下「 * 儲存 * 」。
10. 如果您在多個AZs中有HA配對、則必須針對節點2重複這些步驟。

在單一節點系統上建立儲存**VM**

這些步驟可在單一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、如果您想要建立管理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通往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上未使用的次要私有IP。

3. 選用：建立儲存VM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是e0a上另一個未使用的次要私有IP。

4. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

在單一**AZ**的**HA**配對上建立儲存**VM**

這些步驟可在單一AZ的HA配對上建立新的儲存VM。建立NAS LIF需要一個私有IP位址、如果您想要建立管理LIF、則需要另一個選用的私有IP位址。

這兩個生命點都會分配到節點1上。如果發生故障、私有IP位址可以在節點之間移動。

步驟

1. 建立儲存虛擬機器和通往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節點1 e0a上未使用的次要私有IP。在接管時、此IP位址可重新定位至CVO-node2的e0a、因為服務原則的預設資料檔表示IP可移轉至合作夥伴節點。

3. 選用：在節點1上建立儲存VM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是e0a上另一個未使用的次要私有IP。

4. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

5. 如果您執行Cloud Volumes ONTAP 的是版本不含更新版本的版本、請修改儲存VM的網路服務原則。

   需要修改服務、因為Cloud Volumes ONTAP 這樣可確保支援功能可將iSCSI LIF用於傳出管理連線。

```
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**AZs**的**HA**配對上建立儲存**VM**

這些步驟可在多個AZs的HA配對上建立新的儲存VM。

NAS LIF需要_浮動_ IP位址、管理LIF則為選用。這些浮動IP位址不需要您在AWS中分配私有IP。而是會在AWS路由表中自動設定浮動IP、以指向同一個VPC中的特定節點ENI。

為了讓浮動IP能夠搭配ONTAP 使用、必須在每個節點上的每個儲存VM上設定私有IP位址。這反映在以下步驟中、其中iSCSI LIF是在節點1和節點2上建立。

步驟

1. 建立儲存虛擬機器和通往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
```

   - 在部署HA組態的AWS區域中、所有VPC的浮動IP位址必須位於CIDR區塊之外。192・168・0・27是一個浮動IP地址的例子。 "深入瞭解如何選擇浮動IP位址"。
   - 「服務原則預設資料檔案」表示IP可以移轉至合作夥伴節點。

3. 選用：在節點1上建立儲存VM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是支援儲存VM中浮動IP的LIF移轉所必需的。它不一定是iSCSI LIF、但無法設定在節點之間移轉。
   - 「服務原則預設資料區塊」表示IP位址不會在節點之間移轉。
   - _Private IP是CVO節點1的eth0（e0a）上未使用的次要私有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是支援儲存VM中浮動IP的LIF移轉所必需的。它不一定是iSCSI LIF、但無法設定在節點之間移轉。
- 「服務原則預設資料區塊」表示IP位址不會在節點之間移轉。
- _Private IP是CVO節點2的eth0（e0a）上未使用的次要私有IP位址。

6. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

7. 如果您執行Cloud Volumes ONTAP 的是版本不含更新版本的版本、請修改儲存VM的網路服務原則。

需要修改服務、因為Cloud Volumes ONTAP 這樣可確保支援功能可將iSCSI LIF用於傳出管理連線。

```
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Cloud Volumes ONTAP Azure中建立資料服務儲存VM以供其使用

儲存虛擬機器是 ONTAP 執行於支援內部的虛擬機器、可為您的用戶端提供儲存與資料服務。您可能知道這是 *SVM* 或 *vserver* 。根據預設、系統會設定一個儲存VM、但在Azure上執行時、則支援其他儲存VM。Cloud Volumes ONTAP Cloud Volumes ONTAP

若要建立額外的資料服務儲存VM、您必須在Azure中配置IP位址、然後執行ONTAP 支援功能指令、以建立儲存VM和資料LIF。

若要執行其他 NIC 相關工作、您可以在 Azure 中指派具有適當權限的網路參與者角色或自訂角色。如需這些 NIC 相關權限的詳細資訊、請參閱 "Microsoft Azure 文件"。

支援的儲存 **VM** 數量

從9.9.0版本開始、特定Cloud Volumes ONTAP 的支援功能可支援多個儲存VM。前往 "發行說明 Cloud Volumes ONTAP" 驗證Cloud Volumes ONTAP 支援的儲存VM數量是否適用於您的版本的支援。

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

在**Azure**中配置**IP**位址

您必須先在Azure中配置IP位址、才能建立儲存VM並分配LIF。

單一節點系統

在您建立儲存VM並分配LIF之前、必須先將IP位址指派給Azure中的nic0。

您需要為資料LIF存取建立IP位址、並為儲存VM（SVM）管理LIF建立另一個選用的IP位址。此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

步驟

1. 登入Azure入口網站、然後開啟*虛擬機器*服務。
2. 按一下Cloud Volumes ONTAP 「不完整虛擬機器」的名稱。
3. 按一下*網路*。
4. 按一下nic0的網路介面名稱。
5. 在*設定*下、按一下* IP組態*。
6. 按一下「 * 新增 * 」 。
7. 輸入IP組態的名稱、選取*動態*、然後按一下*確定*。
8. 按一下您剛才建立的IP組態名稱、將*指派*變更為*靜態*、然後按一下*儲存*。

   最好使用靜態IP位址、因為靜態IP可確保IP位址不會變更、有助於避免不必要的應用程式中斷運作。

如果您要建立SVM管理LIF、請重複這些步驟以建立其他IP位址。

完成後

複製您剛建立的私有IP位址。當您為新的儲存VM建立生命期時、必須指定這些IP位址。

HA配對

如何為HA配對分配IP位址、取決於您使用的儲存傳輸協定。

iSCSI

在您建立儲存VM並分配LIF之前、必須先將iSCSI IP位址指派給Azure中的nic0。iSCSI的IPS會指派給nic0而非負載平衡器、因為iSCSI會使用ALUA進行容錯移轉。

您需要建立下列IP位址：

- 從節點1存取iSCSI資料LIF的IP位址
- 從節點2存取iSCSI資料LIF的IP位址
- 儲存VM（SVM）管理LIF的選用IP位址

  此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

步驟

1. 登入Azure入口網站、然後開啟*虛擬機器*服務。
2. 按一下Cloud Volumes ONTAP 節點1的「支援不支援虛擬機器」名稱。
3. 按一下*網路*。
4. 按一下nic0的網路介面名稱。
5. 在*設定*下、按一下* IP組態*。
6. 按一下「 * 新增 * 」。
7. 輸入IP組態的名稱、選取*動態*、然後按一下*確定*。
8. 按一下您剛才建立的IP組態名稱、將*指派*變更為*靜態*、然後按一下*儲存*。

   最好使用靜態IP位址、因為靜態IP可確保IP位址不會變更、有助於避免不必要的應用程式中斷運作。

9. 在節點2上重複這些步驟。
10. 如果您要建立SVM管理LIF、請在節點1上重複這些步驟。

NFS

您用於NFS的IP位址會配置在負載平衡器中、以便在發生容錯移轉事件時、IP位址可以移轉到其他節點。

您需要建立下列IP位址：

- 單一IP位址、可從節點1存取NAS資料LIF
- 單一IP位址、可從節點2存取NAS資料LIF
- 儲存VM（SVM）管理LIF的選用IP位址

  DNS通訊需要iSCSI LIF。iSCSI LIF用於此用途、因為它不會在容錯移轉時移轉。

  此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

步驟

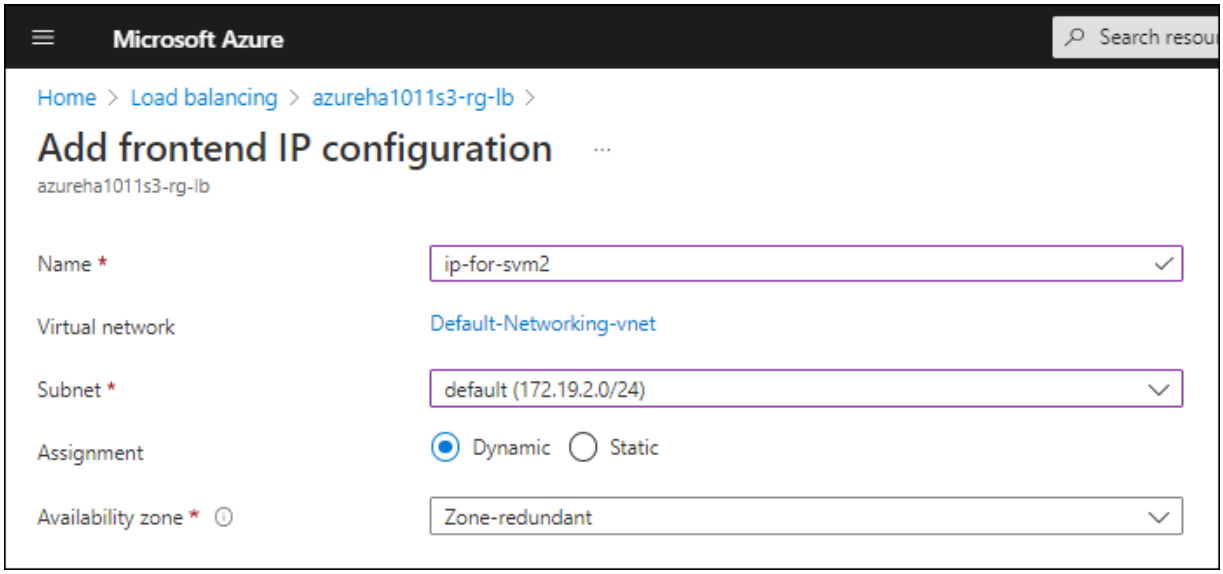
1. 在Azure入口網站中、開啟*負載平衡器*服務。
2. 按一下HA配對的負載平衡器名稱。

3. 從節點1建立資料LIF存取的前端IP組態、從節點2存取資料LIF的前端IP組態、以及儲存VM（SVM）管理LIF的另一個選用前端IP。

   a. 在*設定*下、按一下*前端IP組態*。

   b. 按一下「 * 新增 * 」。

   c. 輸入前端IP的名稱、選取Cloud Volumes ONTAP 該子網路做為「靜態HA配對」、保留「動態」選項、並在「可用區域」中保留「區域-備援」選項、以確保區域故障時IP位址仍可繼續使用。



   d. 按一下您剛才建立的前端IP組態名稱、將*指派*變更為*靜態*、然後按一下*儲存*。

      最好使用靜態IP位址、因為靜態IP可確保IP位址不會變更、有助於避免不必要的應用程式中斷運作。

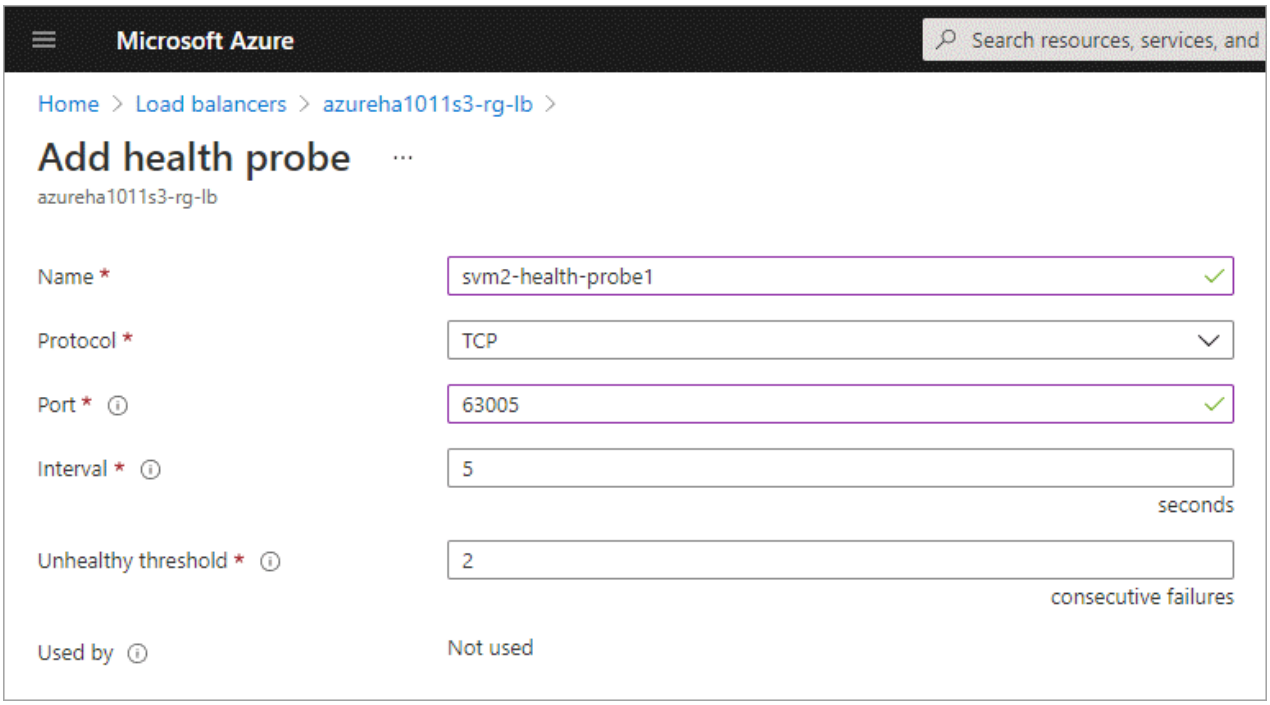
4. 為您剛建立的每個前端IP新增健全狀況探查。

   a. 在負載平衡器的*設定*下、按一下*健全狀況探查*。

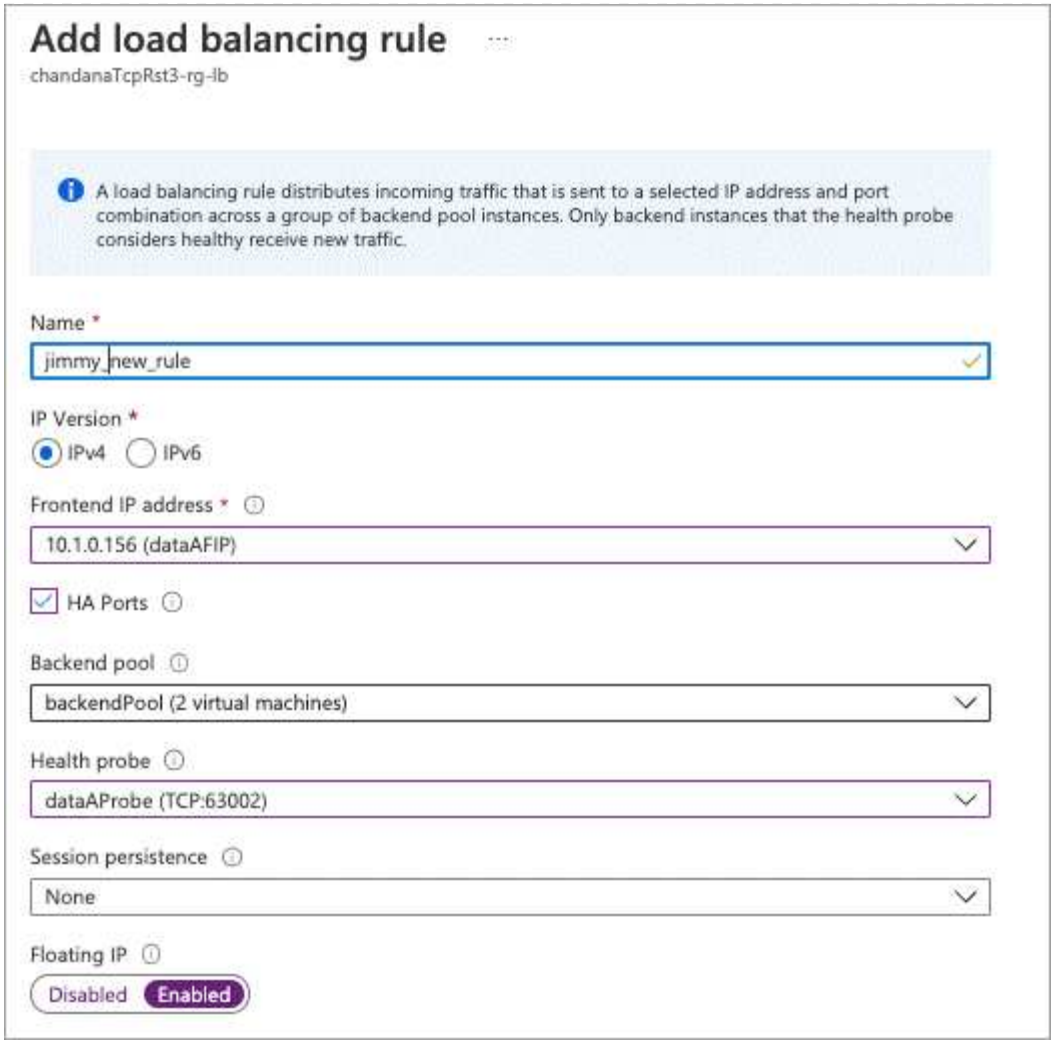
   b. 按一下「 * 新增 * 」。

   c. 輸入健全狀況探針的名稱、然後輸入介於63005和65000之間的連接埠號碼。保留其他欄位的預設值。

      連接埠號碼必須介於63005和65000之間。例如、如果您要建立三個健全狀況探針、可以輸入使用連接埠編號63005、63006和63007的探針。



5. 為每個前端IP建立新的負載平衡規則。
   a. 在負載平衡器的*設定*下、按一下*負載平衡規則*。
   b. 按一下*「Add*（新增*）」、然後輸入所需資訊：
      - 名稱：輸入規則的名稱。
      - * IP Version ：選取 IPV*。
      - 前端**IP**位址：選取您剛建立的前端IP位址之一。
      - * HA連接埠*：啟用此選項。
      - 後端集區：保留已選取的預設後端集區。
      - 健全狀況探查：選取您為所選前端IP所建立的健全狀況探查。
      - 工作階段持續性：選取*無*。
      - 浮動**IP**：選擇*已啟用*。



6. 確認Cloud Volumes ONTAP 適用於此功能的網路安全群組規則可讓負載平衡器針對上述步驟4所建立的健全狀況探查傳送TCP探查。請注意、這是預設允許的。

中小企業

用於SMB資料的IP位址會配置在負載平衡器中、以便在發生容錯移轉事件時、IP位址可以移轉到其他節點。

您需要在負載平衡器中建立下列IP位址：

- 單一IP位址、可從節點1存取NAS資料LIF
- 單一IP位址、可從節點2存取NAS資料LIF
- 每個VM各自的NIC 0中節點1上iSCSI LIF的一個IP位址
- 節點2上iSCSI LIF的一個IP位址

  DNS和SMB通訊需要iSCSI LIF。iSCSI LIF用於此用途、因為它不會在容錯移轉時移轉。

- 儲存VM（SVM）管理LIF的選用IP位址

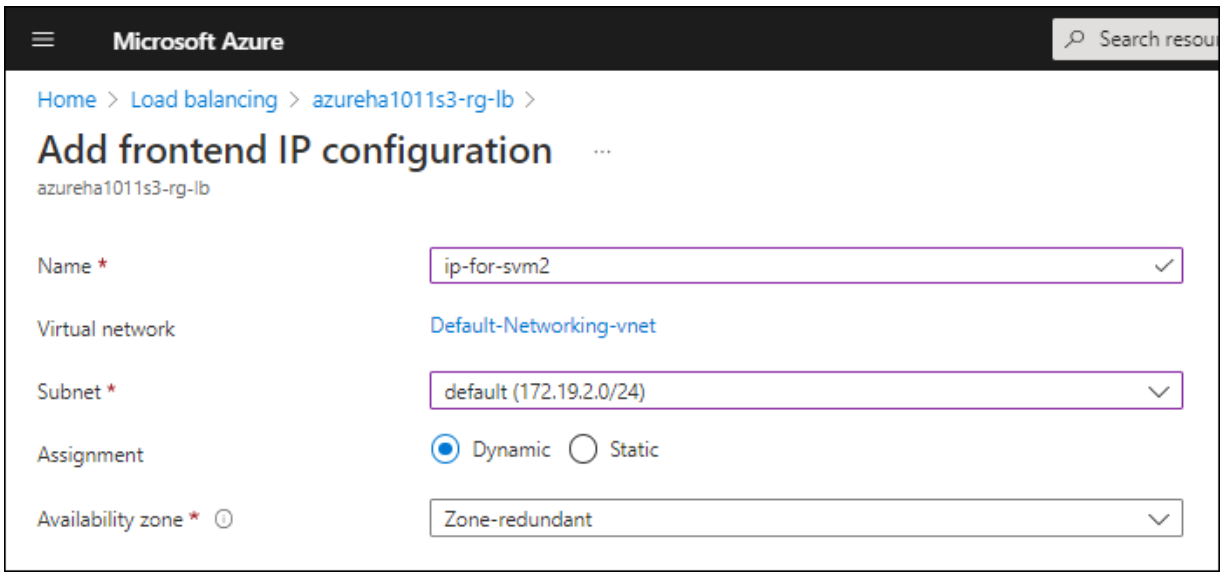
  此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

步驟

1. 在Azure入口網站中、開啟*負載平衡器*服務。
2. 按一下HA配對的負載平衡器名稱。
3. 僅為資料和SVM LIF建立所需的前端IP組態數目：

   前端IP只能在每個對應SVM的NIC 0下建立。如需如何將IP位址新增至SVM NIC 0的詳細資訊、請參閱「步驟7 [hyperlink]」

   a. 在*設定*下、按一下*前端IP組態*。
   b. 按一下「 * 新增 * 」。
   c. 輸入前端IP的名稱、選取Cloud Volumes ONTAP 該子網路做為「靜態HA配對」、保留「動態」選項、並在「可用區域」中保留「區域-備援」選項、以確保區域故障時IP位址仍可繼續使用。



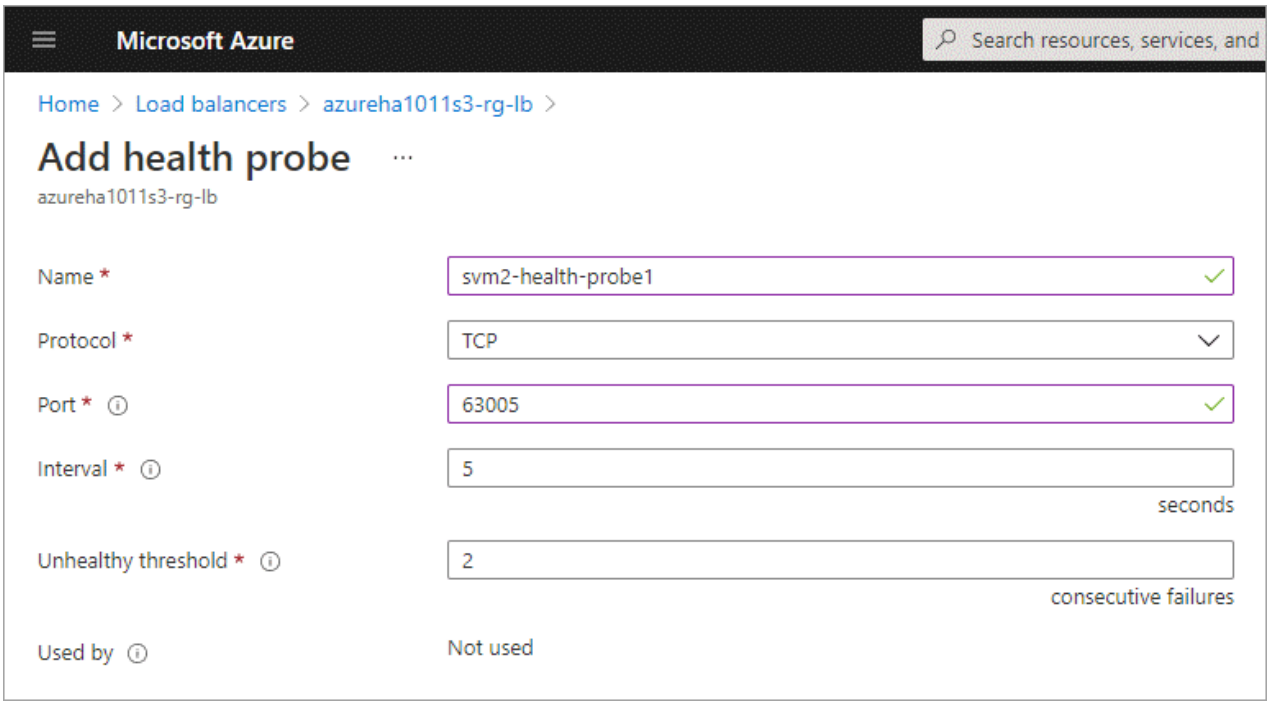
   d. 按一下您剛才建立的前端IP組態名稱、將*指派*變更為*靜態*、然後按一下*儲存*。

      最好使用靜態IP位址、因為靜態IP可確保IP位址不會變更、有助於避免不必要的應用程式中斷運作。

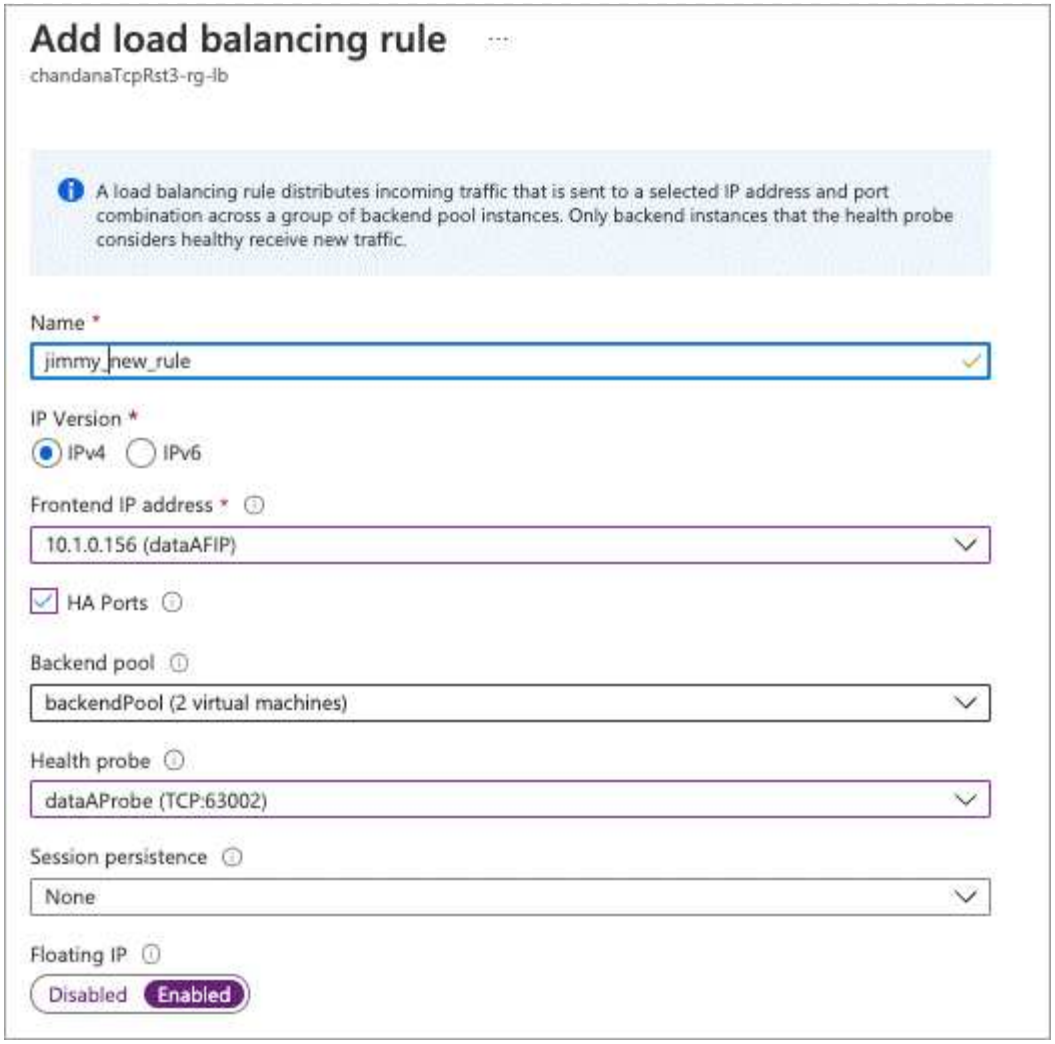
4. 為您剛建立的每個前端IP新增健全狀況探查。

   a. 在負載平衡器的*設定*下、按一下*健全狀況探查*。
   b. 按一下「 * 新增 * 」。
   c. 輸入健全狀況探針的名稱、然後輸入介於63005和65000之間的連接埠號碼。保留其他欄位的預設值。

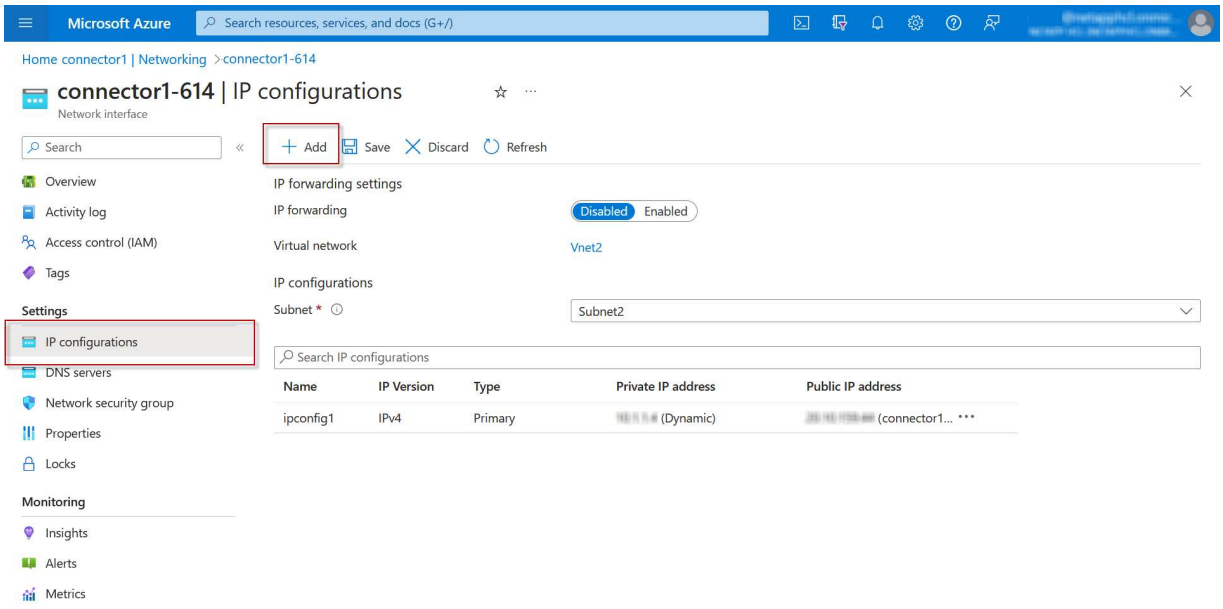
      連接埠號碼必須介於63005和65000之間。例如、如果您要建立三個健全狀況探針、可以輸入使用連接埠編號63005、63006和63007的探針。



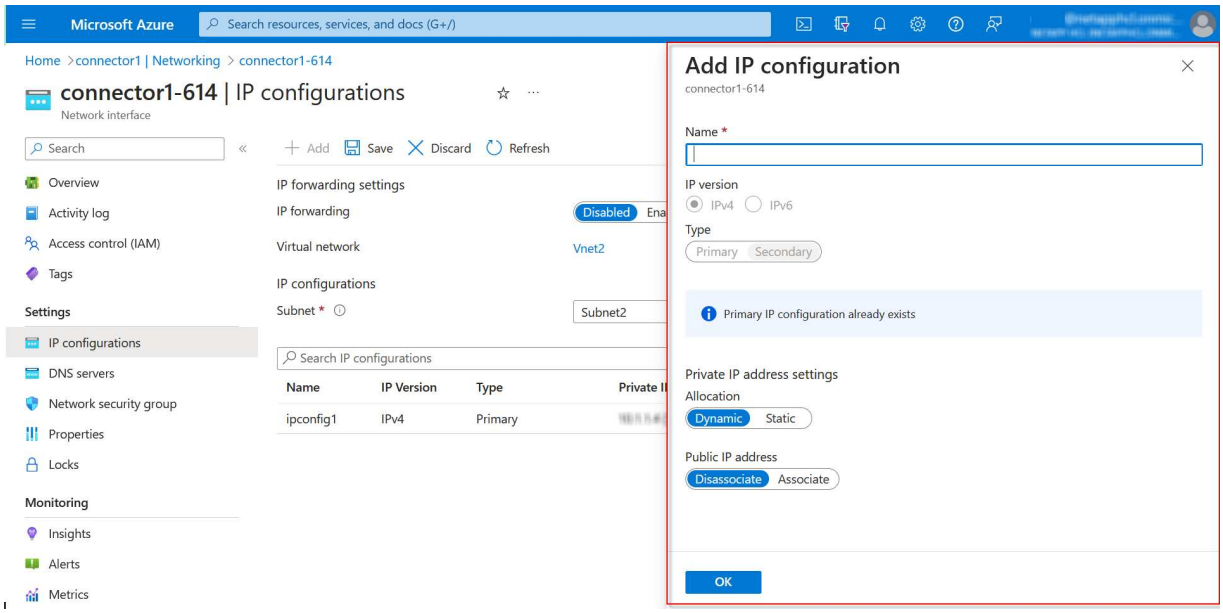
5. 為每個前端IP建立新的負載平衡規則。
   a. 在負載平衡器的*設定*下、按一下*負載平衡規則*。
   b. 按一下*「Add*（新增*）」、然後輸入所需資訊：
      - 名稱：輸入規則的名稱。
      - * IP Version ：選取 IPV*。
      - 前端**IP**位址：選取您剛建立的前端IP位址之一。
      - * HA連接埠*：啟用此選項。
      - 後端集區：保留已選取的預設後端集區。
      - 健全狀況探查：選取您為所選前端IP所建立的健全狀況探查。
      - 工作階段持續性：選取*無*。
      - 浮動**IP**：選擇*已啟用*。



6. 確認Cloud Volumes ONTAP 適用於此功能的網路安全群組規則可讓負載平衡器針對上述步驟4所建立的健全狀況探查傳送TCP探查。請注意、這是預設允許的。
7. 對於iSCSI LIF、請新增NIC 0的IP位址。
   a. 按一下Cloud Volumes ONTAP 「不完整虛擬機器」的名稱。
   b. 按一下*網路*。
   c. 按一下nic0的網路介面名稱。
   d. 在「設定」下、按一下「* IP組態*」。
   e. 按一下「 * 新增 * 」。



f. 輸入IP組態的名稱、選取動態、然後按一下*確定*。



g. 按一下您剛才建立的IP組態名稱、將指派變更為靜態、然後按一下*儲存*。

最好使用靜態IP位址、因為靜態IP可確保IP位址不會變更、有助於避免不必要的應用程式中斷運作。

完成後

複製您剛建立的私有IP位址。當您為新的儲存VM建立生命期時、必須指定這些IP位址。

建立儲存VM和LIF

在Azure中配置IP位址之後、您可以在單一節點系統或HA配對上建立新的儲存VM。

如何在單一節點系統上建立儲存VM和LIF、取決於您使用的儲存傳輸協定。

iSCSI

請依照下列步驟建立新的儲存VM、以及所需的LIF。

步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -vserver <svm-name> -destination 0.0.0.0/0
-gateway <ip-of-gateway-server>
```

2. 建立資料LIF：

```
network interface create -vserver <svm-name> -home-port e0a -address
<iscsi-ip-address> -netmask-length <# of mask bits> -lif <lif-name>
-home-node <name-of-node1> -data-protocol iscsi
```

3. 選用：建立儲存VM管理LIF。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

4. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

NFS

請依照下列步驟建立新的儲存VM、以及所需的LIF。

步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -vserver <svm-name> -destination 0.0.0.0/0
-gateway <ip-of-gateway-server>
```

2. 建立資料LIF：

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nas-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

3. 選用：建立儲存VM管理LIF。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

4. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

中小企業

請依照下列步驟建立新的儲存VM、以及所需的LIF。

步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -vserver <svm-name> -destination 0.0.0.0/0
-gateway <ip-of-gateway-server>
```

2. 建立資料LIF：

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nas-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

3. 選用：建立儲存VM管理LIF。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

4. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

HA配對

如何在HA配對上建立儲存VM和LIF、取決於您使用的儲存傳輸協定。

iSCSI

請依照下列步驟建立新的儲存VM、以及所需的LIF。

步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -vserver <svm-name> -destination 0.0.0.0/0
-gateway <ip-of-gateway-server>
```

2. 建立資料生命量：

   a. 使用下列命令在節點1上建立iSCSI LIF。

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

   b. 使用下列命令在節點2上建立iSCSI LIF。

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

3. 選用：在節點1上建立儲存VM管理LIF。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

   此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

4. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

5. 如果您執行Cloud Volumes ONTAP 的是版本不含更新版本的版本、請修改儲存VM的網路服務原則。

   a. 輸入下列命令以存取進階模式。

      ```
      ::> set adv -con off
      ```

      需要修改服務、因為Cloud Volumes ONTAP 這樣可確保支援功能可將iSCSI LIF用於傳出管理連線。

```
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
```

NFS

請依照下列步驟建立新的儲存VM、以及所需的LIF。

步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -vserver <svm-name> -destination 0.0.0.0/0
-gateway <ip-of-gateway-server>
```

2. 建立資料生命量：

   a. 使用下列命令在節點1上建立NAS LIF。

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node1> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe1>
```

   b. 使用下列命令在節點2上建立NAS LIF。

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node2> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe2>
```

3. 建立iSCSI LIF以提供DNS通訊：

   a. 使用下列命令在節點1上建立iSCSI LIF。

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

   b. 使用下列命令在節點2上建立iSCSI LIF。

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

4. 選用：在節點1上建立儲存VM管理LIF。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

5. 選用：在節點1上建立儲存VM管理LIF。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

6. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

7. 如果您執行Cloud Volumes ONTAP 的是版本不含更新版本的版本、請修改儲存VM的網路服務原則。

   a. 輸入下列命令以存取進階模式。

```
::> set adv -con off
```

需要修改服務、因為Cloud Volumes ONTAP 這樣可確保支援功能可將iSCSI LIF用於傳出管理連線。

```
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
```

中小企業

請依照下列步驟建立新的儲存VM、以及所需的LIF。

步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -vserver <svm-name> -destination 0.0.0.0/0
-gateway <ip-of-gateway-server>
```

2. 建立NAS資料生命量：
   a. 使用下列命令在節點1上建立NAS LIF。

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node1> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe1>
```

   b. 使用下列命令在節點2上建立NAS LIF。

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node2> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe2>
```

3. 建立iSCSI LIF以提供DNS通訊：
   a. 使用下列命令在節點1上建立iSCSI LIF。

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

   b. 使用下列命令在節點2上建立iSCSI LIF。

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

4. 選用：在節點1上建立儲存VM管理LIF。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

5. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

6. 如果您執行Cloud Volumes ONTAP 的是版本不含更新版本的版本、請修改儲存VM的網路服務原則。

   a. 輸入下列命令以存取進階模式。

```
::> set adv -con off
```

需要修改服務、因為Cloud Volumes ONTAP 這樣可確保支援功能可將iSCSI LIF用於傳出管理連線。

```
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
```

接下來呢？

在HA配對上建立儲存VM之後、最好先等待12小時、再在該SVM上配置儲存設備。從發行版的《21》開始、BlueXP會以12小時的時間間隔掃描HA配對負載平衡器的設定。Cloud Volumes ONTAP如果有新的SVM、則BlueXP會啟用可縮短非計畫性容錯移轉的設定。

在**Cloud Volumes ONTAP Google Cloud**中建立資料服務儲存**VM**以供其使用

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

支援的儲存 **VM** 數量

從9.11.1版開始、Cloud Volumes ONTAP Google Cloud中的特定支援功能可支援多個儲存VM。前往 "發行說明 Cloud Volumes ONTAP" 驗證Cloud Volumes ONTAP 支援的儲存VM數量是否適用於您的版本的支援。

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

建立儲存**VM**

如果授權支援、您可以在單一節點系統或HA配對上建立多個儲存VM。請注意、您必須使用BlueXP API在HA配對上建立儲存VM、而您可以使用CLI或System Manager在單一節點系統上建立儲存VM。

單一節點系統

這些步驟使用CLI在單一節點系統上建立新的儲存VM。建立資料LIF需要一個私有IP位址、如果您想要建立管理LIF、則需要另一個選用的私有IP位址。

步驟

1. 在Google Cloud中、移至Cloud Volumes ONTAP 「實例」、並為每個LIF新增一個IP位址至nic0。

如果您想在儲存VM上建立管理LIF、則需要一個IP位址用於資料LIF、另一個選用IP位址。

"Google Cloud文件：新增別名IP範圍至現有執行個體"

2. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-
volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name> -gateway
<ip-of-gateway-server>
```

3. 指定您在Google Cloud中新增的IP位址、以建立資料LIF。

iSCSI

```
network interface create -vserver <svm-name> -home-port e0a -address
<iscsi-ip-address> -lif <lif-name> -home-node <name-of-node1> -data
-protocol iscsi
```

NFS或SMB

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

4. 選用：指定您在Google Cloud中新增的IP位址、以建立儲存VM管理LIF。

```
network interface create -vserver <svm-name> -lif <lif-name> -role data
-data-protocol none -address <svm-mgmt-ip-address> -netmask-length
<length> -home-node <name-of-node1> -status-admin up -failover-policy
system-defined -firewall-policy mgmt -home-port e0a -auto-revert false
-failover-group Default
```

5. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver <svm-name> -aggregates <aggr1,aggr2>
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

HA配對

您必須使用BlueXP API在Cloud Volumes ONTAP Google Cloud的某個系統上建立儲存VM。由於BlueXP會使用所需的LIF服務來設定儲存VM、以及輸出SMB/CIFS通訊所需的iSCSI LIF、因此需要使用API（而非System Manager或CLI）。

請注意、BlueXP會在Google Cloud中配置所需的IP位址、並使用資料LIF來建立儲存VM、以進行SMB/NFS存取、並使用iSCSI LIF來進行傳出SMB通訊。

必要的Google Cloud權限

Connector需要特定權限、才能建立及管理Cloud Volumes ONTAP 儲存VM、以利執行各種HA配對。所需權限包含在中 "NetApp 提供的原則"。

步驟

1. 使用下列API呼叫建立儲存VM：

「POST /occm/api/gcp/ha/辦公 環境/ ｛we_ID｝ /svm/」

申請機構應包括下列項目：

```
{ "svmName": "myNewSvm1" }
```

管理**HA**配對上的儲存**VM**

BlueXP API也支援在HA配對上重新命名及刪除儲存VM。

重新命名儲存**VM**

如有需要、您可以隨時變更儲存VM的名稱。

步驟

1. 使用下列API呼叫重新命名儲存VM：

   「PPUT /occm/API/GCP / ha /工作環境/ ｛we ID｝ /SVM」

   申請機構應包括下列項目：

```
{
"svmNewName": "newSvmName",
"svmName": "oldSvmName"
}
```

刪除儲存**VM**

如果您不再需要儲存VM、可以從Cloud Volumes ONTAP 停止功能中刪除。

步驟

1. 使用下列API呼叫來刪除儲存VM：

   「刪除/occm/api/gcp/ha/工作 環境/ ｛we_ID｝ /Svm/ ｛Svm_name｝ 」

設定 **SVM** 災難恢復

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

如果在兩個 Cloud Volumes ONTAP 系統之間設定 SnapMirror SVM 複寫、複寫必須介於兩個 HA 配對系統或兩個單一節點系統之間。您無法在 HA 配對和單一節點系統之間設定 SnapMirror SVM 複寫。

如需 CLI 指示、請參閱下列文件。

- "SVM 災難恢復準備快速指南"

- "SVM Disaster Recovery Express 指南"

安全性與資料加密

使用 **NetApp** 加密解決方案加密磁碟區

支援NetApp Volume Encryption（NVE）和NetApp Aggregate Encryption（NAE）Cloud Volumes ONTAP 。NVE和NAE是軟體型解決方案、可啟用FIPS 140-2標準的磁碟區閒置資料加密功能。 "深入瞭解這些加密解決方案"。

外部金鑰管理程式支援NVE和NAE。

使用 **AWS** 金鑰管理服務管理金鑰

您可以使用 "AWS 的金鑰管理服務（ KMS ）" 保護 AWS 部署應用程式中的 ONTAP 加密金鑰。

您可以使用 CLI 或 ONTAP REST API 來啟用 AWS KMS 的金鑰管理。

使用 KMS 時、請注意、根據預設、資料 SVM 的 LIF 會用於與雲端金鑰管理端點通訊。節點管理網路用於與 AWS 的驗證服務進行通訊。如果叢集網路設定不正確、叢集將無法正確使用金鑰管理服務。

開始之前

- Cloud Volumes ONTAP 必須執行 9.12.0 版或更新版本
- 您必須已安裝 Volume Encryption （ VE ）授權和
- 您必須已安裝多租戶加密金鑰管理（ 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

您只能設定資料 SVM 的金鑰。

組態

AWS

1. 您必須建立 "授予" 適用於管理加密的 IAM 角色所使用的 AWS KMS 金鑰。IAM 角色必須包含允許下列作業的原則：
   - `DescribeKey`
   - `Encrypt`
   - `Decrypt`
     若要建立授予、請參閱 "AWS文件"。
2. "將原則新增至適當的 IAM 角色。" 原則應支援 `DescribeKey`、 `Encrypt`和 `Decrypt` 營運：

Cloud Volumes ONTAP

1. 切換至您的 Cloud Volumes ONTAP 環境。

2. 切換至進階權限等級：「et -priv榮幸 進階」
3. 啟用 AWS 金鑰管理程式：
   `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、請輸入秘密金鑰。
5. 確認 AWS KMS 已正確設定：
   `security key-manager external aws show -vserver svm_name`

使用Azure Key Vault管理金鑰

您可以使用 "Azure Key Vault（AKV）" 在ONTAP Azure部署的應用程式中保護您的不加密金鑰。

AKV可用於保護 "NetApp Volume Encryption（NVE）金鑰" 僅適用於資料SVM。

使用AKV的金鑰管理可透過CLI或ONTAP REST API來啟用。

使用AKV時、請注意、預設會使用資料SVM 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供應商的驗證服務（login.microsoftonline.com）進行通訊。如果叢集網路設定不正確、叢集將無法正確使用金鑰管理服務。

開始之前

- 必須執行9.10.1版或更新版本Cloud Volumes ONTAP
- 已安裝Volume Encryption（VE）授權（NetApp Volume Encryption授權會自動安裝在Cloud Volumes ONTAP 向NetApp支援註冊的每個支援系統上）
- 您必須擁有多租戶加密金鑰管理（MT_EK-Mgmt）授權
- 您必須是叢集或SVM管理員
- 現用Azure訂閱

限制

- AKV只能在資料SVM上設定
- Nae 不可使用 AKV 。Nae 需要外部支援的 KMIP 伺服器。

組態程序

概述的步驟將說明如何向Cloud Volumes ONTAP Azure註冊您的「還原組態」、以及如何建立Azure Key Vault和金鑰。如果您已經完成這些步驟、請確定您擁有正確的組態設定、尤其是在中 建立Azure Key Vault，然後繼續 組態Cloud Volumes ONTAP。

- 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）

- 組態Cloud Volumes ONTAP

Azure應用程式註冊

1. 您必須先在Azure訂閱中註冊您的應用程式Cloud Volumes ONTAP 、才能使用此功能來存取Azure Key Vault。在Azure入口網站中、選取「應用程式註冊」。
2. 選擇「**新登錄」。
3. 提供應用程式名稱、並選取支援的應用程式類型。Azure Key Vault使用預設的單一租戶即可滿足需求。選擇「註冊」。
4. 在Azure Overview（Azure總覽）視窗中、選取您已註冊的應用程式。將應用程式（用戶端）ID *和*目錄（租戶）ID *複製到安全位置。在稍後的註冊程序中、將會需要這些工具。

建立**Azure**用戶端機密

1. 在Azure入口網站中註冊Azure Key Vault應用程式、選取「**憑證與機密」窗格。
2. 選取「**新用戶端密碼」。輸入有意義的用戶端機密名稱。NetApp建議使用24個月到期日、不過您的特定雲端治理原則可能需要不同的設定。
3. 按一下「新增」以建立用戶端機密。複製「Value*」欄中所列的秘密字串、並將其儲存在安全的位置以供稍後使用 組態Cloud Volumes ONTAP。在您離開頁面後、不會再顯示機密值。

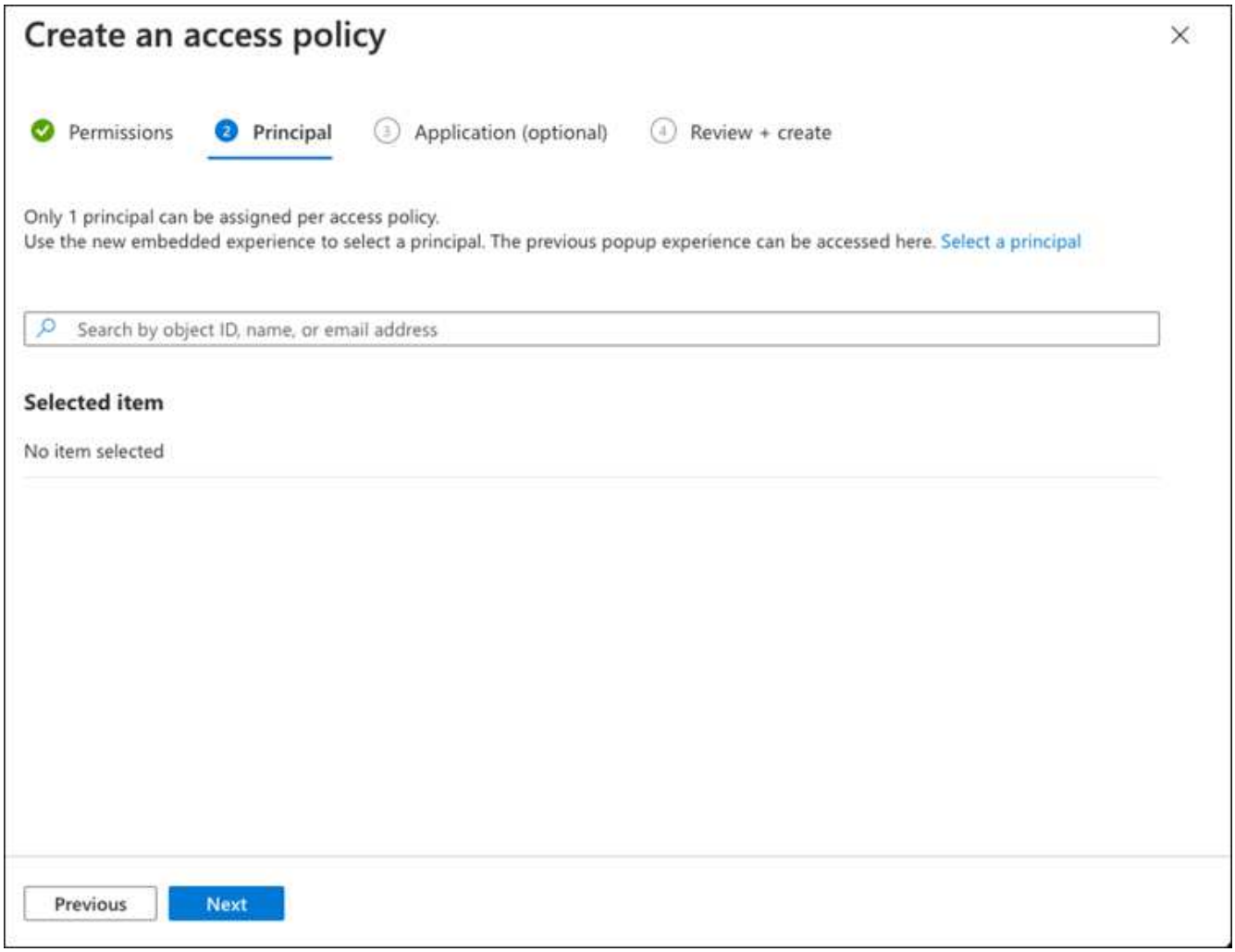
建立**Azure Key Vault**

1. 如果您有現有的Azure Key Vault、您可以將其連線至Cloud Volumes ONTAP 您的整套組態；不過、您必須根據此程序中的設定來調整存取原則。
2. 在Azure入口網站中、瀏覽至「**關鍵故障」區段。
3. 按一下「*+建立」、然後輸入所需資訊、包括資源群組、地區及價格層級。此外、請輸入保留刪除的保存庫的天數、然後在金鑰保存庫中選取「*啟用清除保護」。
4. 選擇「*下一步」以選擇存取原則。
5. 選取下列選項：
   a. 在「存取組態*」下、選取「資料庫存取原則*」。
   b. 在「資源存取*」下、選取「 Azure磁碟加密」以進行Volume加密*。
6. 選取「**+建立」以新增存取原則。
7. 在「從範本*設定」下、按一下下拉式功能表、然後選取「**金鑰、秘密及憑證管理」範本。
8. 選擇每個下拉式權限功能表（金鑰、秘密、憑證）、然後在功能表清單頂端選擇所有*、以選取所有可用的權限。您應該擁有：
   - 關鍵權限：已選取20項
   - **機密權限：選擇8項
   - 認證權限：16項已選取


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」以選取您在其中建立的「*主要」* Azure註冊應用程式 Azure應用程式註冊。選擇「下一步」。

   每個原則只能指派一個主體。



10. 按兩次「下一步」、直到您抵達「審查並建立」為止。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「審查+建立」來建立金鑰保存庫。（網路存取方法可能由治理原則或您的企業雲端安全團隊規定。）
13. 記錄金鑰庫URI：在您建立的金鑰庫中、瀏覽至「總覽」功能表、然後從右側欄複製「** Vault URI」。您需要此功能、以便稍後進行。

建立加密金鑰

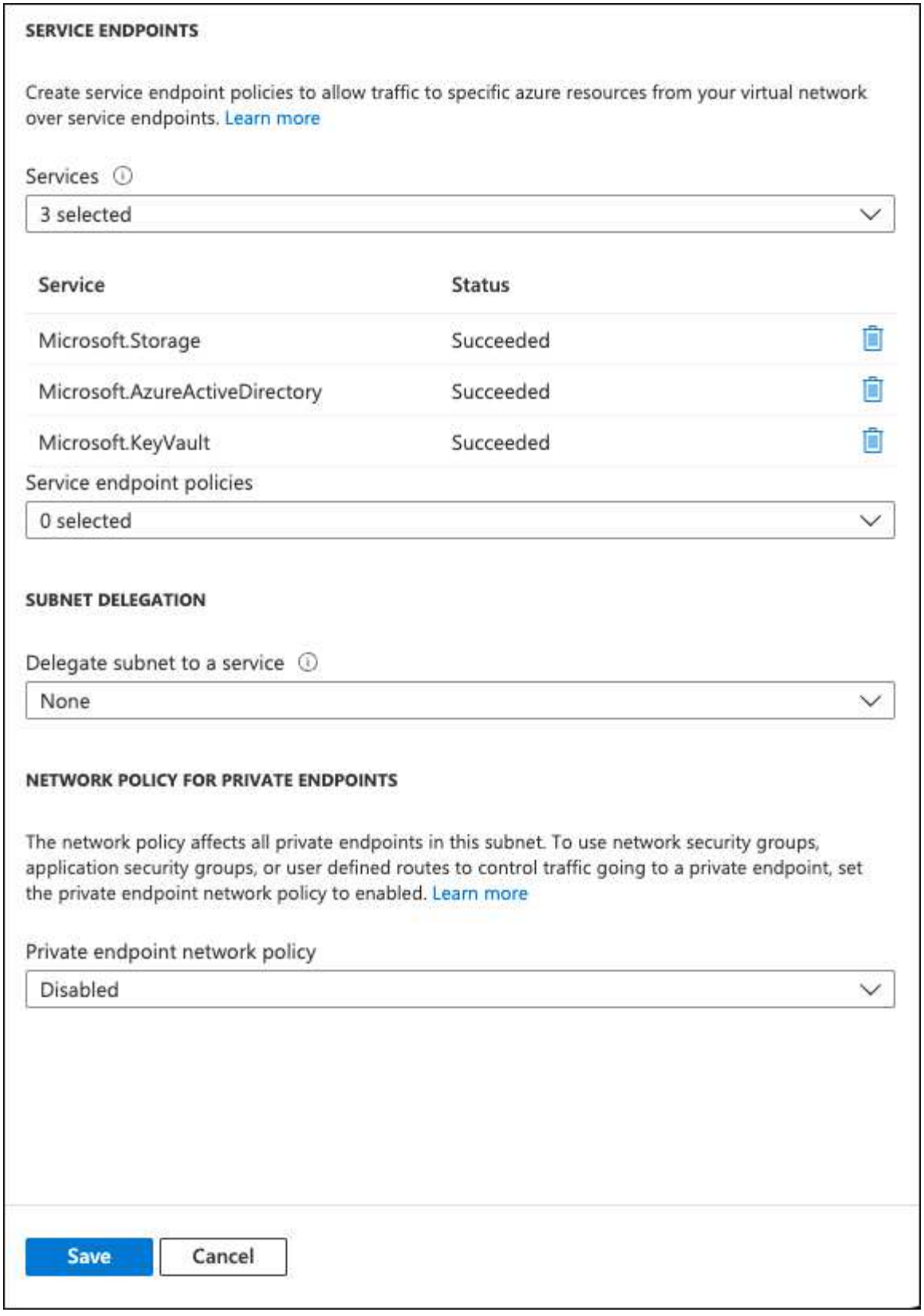
1. 在您為Cloud Volumes ONTAP 之建立的Key Vault功能表中、瀏覽至「** Keys」選項。
2. 選取「產生/匯入」以建立新的金鑰。
3. 將預設選項設為「**產生」。
4. 提供下列資訊：
   - 加密金鑰名稱

- 金鑰類型：RSA
- RSA金鑰大小：2048
- 已啟用：是

5. 選取「建立」以建立加密金鑰。
6. 返回「**按鍵」功能表、然後選取您剛建立的按鍵。
7. 在「目前版本」下方選取金鑰ID、即可檢視金鑰內容。
8. 找到「**金鑰識別碼」欄位。將URI複製到但不包括十六進位字串。

建立**Azure Active Directory**端點（僅限**HA**）

1. 只有在您將Azure Key Vault設定為HA Cloud Volumes ONTAP 功能環境時、才需要執行此程序。
2. 在Azure入口網站中、瀏覽至「**虛擬網路」。
3. 選取部署Cloud Volumes ONTAP 了整個功能區的虛擬網路、然後選取頁面左側的「**Subnets」（子網路）功能表。
4. 從Cloud Volumes ONTAP 清單中選取要部署的子網路名稱。
5. 瀏覽至「*服務端點」標題。在下拉式功能表中、選取下列項目：
   - **Microsoft.AzureActiveDirectory
   - **Microsoft.KeyVault**
   - ***Microsoft.Storage**（選用）



6. 選取「**儲存」以擷取您的設定。

組態**Cloud Volumes ONTAP**

1. 使用您偏好的SSH用戶端連線至叢集管理LIF。
2. 進入進階權限模式ONTAP ：

```
set advanced -con off
```

3. 識別所需的資料SVM、並驗證其DNS組態：「vserver services name-service DNS show」

   a. 如果所需資料SVM的DNS項目存在、且其中包含Azure DNS項目、則不需要採取任何行動。如果沒有、請為資料SVM新增DNS伺服器項目、以指向Azure DNS、私有DNS或內部部署伺服器。這應該符合叢集管理SVM的項目：「vserver services name-service DNS create -vserver *svm_name*-domain_-name -servers *ip_address*」

   b. 確認已為資料SVM建立DNS服務：「vserver services name-service DNS show」

4. 使用應用程式登錄後儲存的用戶端ID和租戶ID來啟用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_`

   ⓘ ◦ `_full_key_URI` 價值必須運用 `<https:// <key vault host name>/keys/<key label>` 格式。

5. 成功啟用 Azure Key Vault 後、請輸入 `client secret value` 出現提示時。

6. 檢查金鑰管理程式的狀態：「安全金鑰管理程式外部azure檢查」輸出內容如下：

```
::*> 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.
```

   如果是 `service_reachability` 狀態不是 `OK`、SVM無法以所有必要的連線和權限來連線至Azure Key Vault服務。請確保您的Azure網路原則和路由不會封鎖您的私有vNet、使其無法到達Azure KeyVault Public端點。如果有、請考慮使用Azure私有端點、從vNet內存取金鑰庫。您可能還需要在SVM上新增靜態主機項目、以解析端點的私有IP位址。

   ◦ `kms_wrapped_key_status` 將會報告 `UNKNOWN` 初始組態時。其狀態將變更為 `OK` 加密第一個磁碟區之後。

7. 選用：建立測試Volume以驗證NVE的功能。

「vol create -vserver *Svm_name*-volume *volVolume _name*-Aggregate *aggr _-size _size*-state online -policy default」

如果設定正確、Cloud Volumes ONTAP 則會自動建立Volume並啟用Volume加密。

8. 確認磁碟區已正確建立並加密。如果是的話、「-is-Encrypted」參數會顯示為「true」。「vol show -vserver *svm_name*-Fields is加密」

利用Google的雲端金鑰管理服務來管理金鑰

您可以使用 "Google Cloud Platform的金鑰管理服務（雲端KMS）" 在ONTAP Google Cloud Platform部署的應用程式中保護您的不加密金鑰。

雲端KMS的金鑰管理可透過CLI或ONTAP REST API啟用。

使用 Cloud KMS 時、請注意、根據預設、會使用 Data SVM 的 LIF 與雲端金鑰管理端點通訊。節點管理網路用於與雲端供應商的驗證服務（oauth2.googleapis.com）進行通訊。如果叢集網路設定不正確、叢集將無法正確使用金鑰管理服務。

開始之前

- 必須執行9.10.1版或更新版本Cloud Volumes ONTAP
- 已安裝Volume Encryption（VE）授權
- 安裝多租戶加密金鑰管理（MTEKM）授權、從Cloud Volumes ONTAP 版本號為E59.12.1 GA開始。
- 您必須是叢集或SVM管理員
- 現用Google Cloud Platform訂閱

限制

- 雲端KMS只能在資料SVM上設定

組態

Google Cloud

1. 在您的Google Cloud環境中、 "建立對稱的GCP金鑰環和金鑰"。
2. 為Cloud Volumes ONTAP 您的服務帳戶建立自訂角色。

```
gcloud iam roles create kmsCustomRole
    --project=<project_id>
    --title=<kms_custom_role_name>
    --description=<custom_role_description>

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
tions.get,cloudkms.locations.list,resourcemanager.projects.get
    --stage=GA
```

3. 將自訂角色指派給Cloud KMS金鑰與Cloud Volumes ONTAP 更新服務帳戶：「gCloud kms金鑰add-iam-policy-binding *key_name*-keyring *key_ring_name*-location *-member ServiceAccount*：*_service_Account_Name*-role專案/*customer_project _id*/ros/ros/kmsCustomrole」
4. 下載服務帳戶Json金鑰：「gCloud iam服務帳戶金鑰可建立金鑰檔案-iam-account=*sa-name@project-id*.iam.gserviceaccount.com」

Cloud Volumes ONTAP

1. 使用您偏好的SSH用戶端連線至叢集管理LIF。
2. 切換至進階權限等級：「et -priv榮幸 進階」
3. 為資料SVM建立DNS。「建立網域C_<project >_.internal -name-servers *server_address*-vserver *Svm_name*」
4. 建立CMEK項目：「安全金鑰管理程式外部GCP啟用-vserver *Svm_name*-project -id *project _-key-ring_name _key_ring_name*-key-ring_location *key_ring_stip*-key-name *key_name*」
5. 出現提示時、請從GCP帳戶輸入服務帳戶Json金鑰。
6. 確認啟用的程序成功：「安全金鑰管理程式外部GCP檢查-vserver *svm_name*」
7. 選用：建立磁碟區以測試加密「volvol create *volvolvole_name*-Aggregate *Aggregate _-vserver _vserver_name*-size 10G」

疑難排解

如果您需要疑難排解、可以跳接上述最後兩個步驟中的原始REST API記錄：

1. "以d為準"
2. "ystemShell -node_node_-command tail -f /mroot/etc/log/mlog/kmip2_client.log"

改善防範勒索軟體的能力

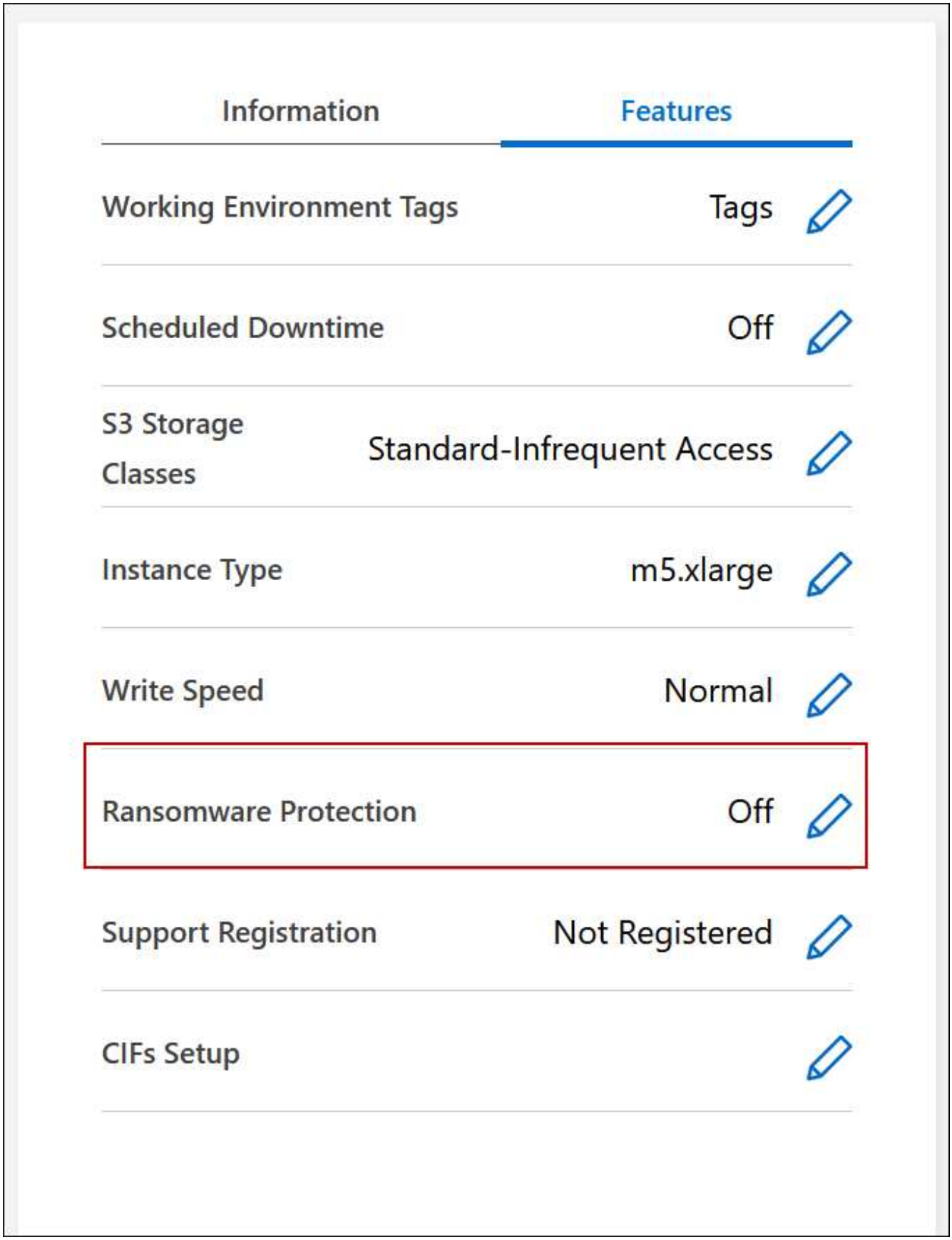
勒索軟體攻擊可能會耗費一定的時間、資源和商譽。BlueXP 可讓您針對勒索軟體實作兩種 NetApp 解決方案：防範常見的勒索軟體副檔名和自動勒索軟體保護（ ARP ）。這些解決方案可提供有效的工具、以利可見度、偵測和補救。

防止常見勒索軟體檔案副檔名

透過 BlueXP 、勒索軟體保護設定可讓您利用 ONTAP FPolicy 功能來防範常見的勒索軟體檔案副檔名類型。

步驟

1. 在 Canvas 頁面上、按兩下您設定為勒索軟體保護的系統名稱。
2. 在「概述」索引標籤上、按一下「功能」面板、然後按一下 * 勒索軟體保護 * 旁的鉛筆圖示。



3. 實作 NetApp 勒索軟體解決方案：

   a. 如果您的磁碟區未啟用 Snapshot 原則、請按一下「 * 啟動 Snapshot Policy* 」。

NetApp Snapshot 技術提供業界最佳的勒索軟體補救解決方案。成功還原的關鍵在於從未受感染的備份還原。Snapshot 複本為唯讀、可防止勒索軟體毀損。他們也能提供精細度、以建立單一檔案複本或完整災難恢復解決方案的映像。

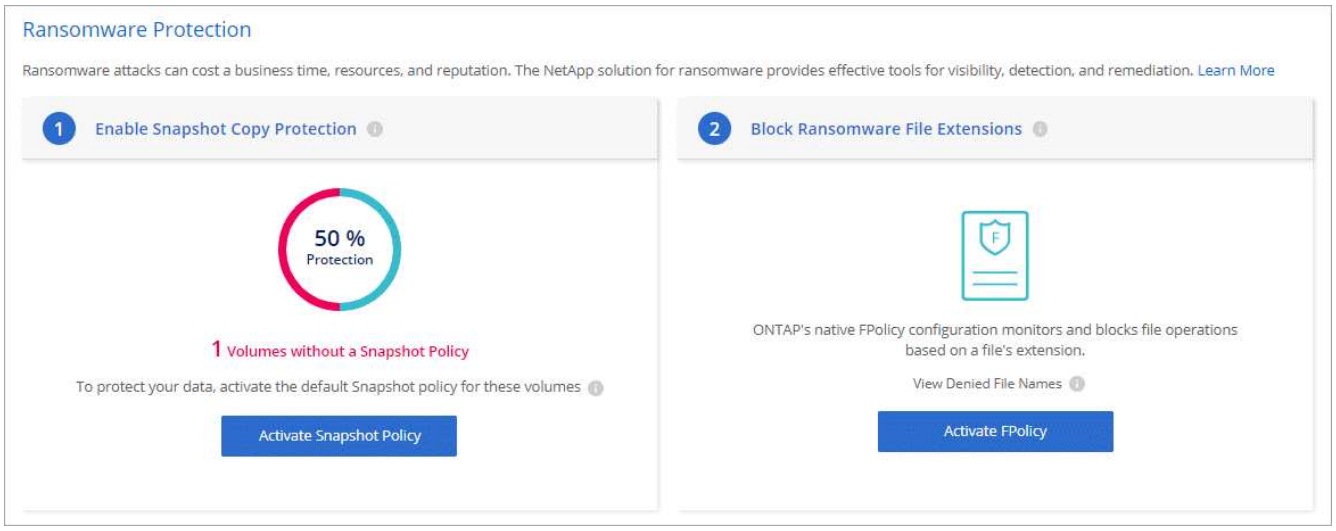
b. 按一下「 * 啟動 FPolicy* 」以啟用 ONTAP 的 FPolicy 解決方案、此解決方案可根據檔案副檔名來封鎖檔案作業。

這項預防解決方案可封鎖常見的勒索軟體檔案類型、藉此改善保護、避免勒索軟體攻擊。

預設FPolicy範圍會封鎖下列副檔名的檔案：

微、加密、鎖定、加密、加密、 crinf, r5a、XRNT, XDBL、R16M01D05、 Pzdc、好、好！、天哪！、RDM、 RRK、加密RS、crjoker、EnCipErEd、LeChiffre

當您啟動Cloud Volumes ONTAP 有關功能的FPolicy時、BlueXP就會建立這個範圍。此清單是根據常見的勒索軟體檔案類型。您可以使用Cloud Volumes ONTAP 來自於整個CLI的_vserver fpolicy scoon__命令來自訂封鎖的副檔名。



自主勒索軟體保護

Cloud Volumes ONTAP 支援「自動勒索軟體保護」（ARP ）功能、可對工作負載執行分析、主動偵測並警告可能表示勒索軟體攻擊的異常活動。

與透過提供的檔案副檔名保護分開 "勒索軟體保護設定"、 ARP 功能會使用工作負載分析、根據偵測到的「異常活動」來警示使用者可能遭受的攻擊。勒索軟體保護設定和 ARP 功能均可搭配使用、以提供全面的勒索軟體保護。

ARP 功能僅適用於以節點為基礎的授權模式和以容量為基礎的授權模式、且僅適用於 BYOL 授權（ 1 至 36 個月期限）。您必須聯絡您的 NetApp 銷售代表、以購買新的獨立附加授權、以搭配 Cloud Volumes ONTAP 中的 ARP 功能使用。

ARP 授權被視為「浮動」授權、這表示它不受限於單一 Cloud Volumes ONTAP 執行個體、而且可以套用至多個 Cloud Volumes ONTAP 環境。

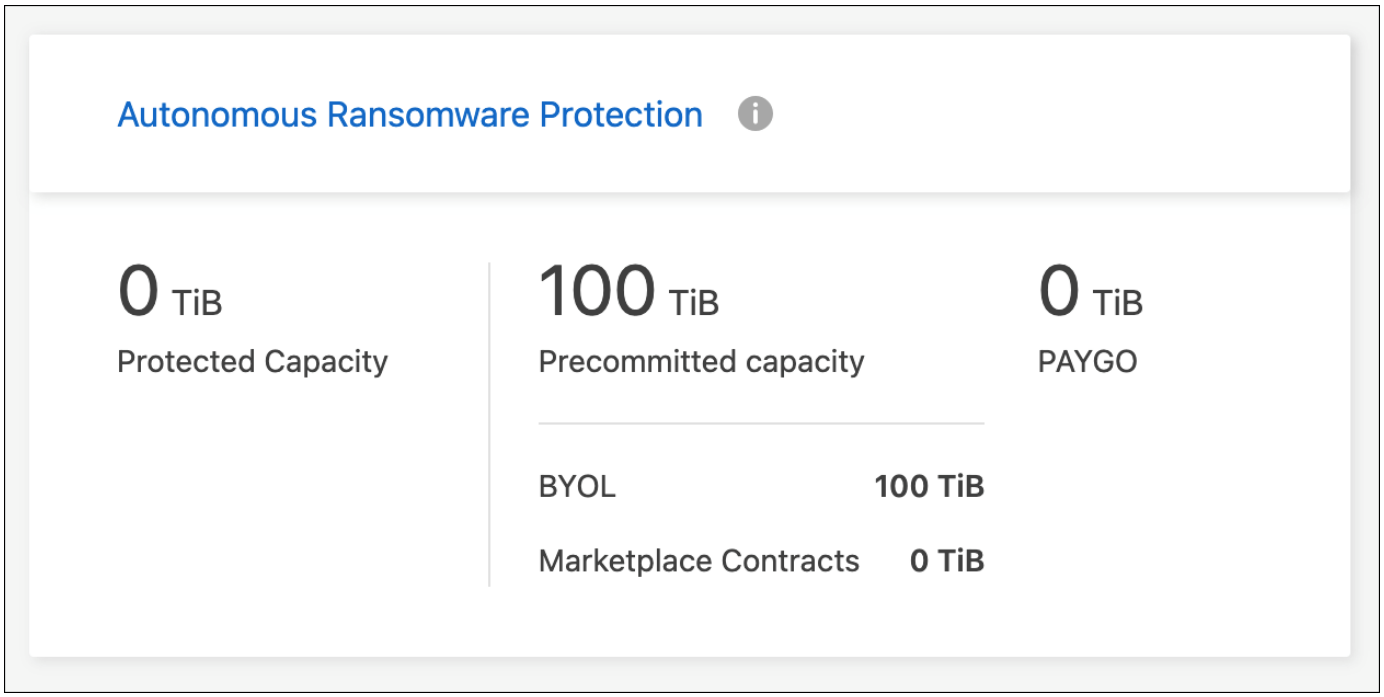
在節點型 Cloud Volumes ONTAP 授權中使用 ARP 功能的情況、目前並未反映在 Digital Wallet 中。未來版本的 Digital Wallet 將提供檢視節點型 ARP 使用率的功能。

購買附加授權並將其新增至 Digital Wallet 後、您可以使用 Cloud Volumes ONTAP 以每個磁碟區為基礎來啟用 ARP 。ARP 的收費是根據已啟用 ARP 功能的已配置磁碟區總容量、以磁碟區層級計量。最低授權容量為 1TB 。不過、 ARP 功能沒有最低容量充電量。

已啟用 ARP 的磁碟區具有「學習模式」或「作用中」的指定狀態。任何 ARP 狀態為「已停用」的磁碟區都會排除在充電之外。例如、具有 30 TiB 已配置容量的 Cloud Volumes ONTAP 環境、可選擇僅擁有 15 個 TiB 磁碟區的子集、並啟用 ARP 。

磁碟區的 ARP 組態是透過 ONTAP 系統管理員和 ONTAP CLI 執行。

如需如何使用 ONTAP 系統管理員和 CLI 啟用 ARP 的詳細資訊、請參閱 "啟用自發勒索軟體保護"。



若未取得授權、則無法使用授權功能。

系統管理

升級Cloud Volumes ONTAP 版軟體

從Cloud Volumes ONTAP BlueXP升級以取得最新的新功能與增強功能。升級軟體之前、您應該先準備 Cloud Volumes ONTAP 好用的不一樣系統。

升級總覽

在開始Cloud Volumes ONTAP 進行還原升級程序之前、您應該注意下列事項。

僅從**BlueXP**升級

必須從BlueXP完成升級。Cloud Volumes ONTAP您不應 Cloud Volumes ONTAP 使用 System Manager 或 CLI 來升級功能。這樣做可能會影響系統穩定性。

如何升級

BlueXP提供兩種升級Cloud Volumes ONTAP 途徑：

- 在工作環境中顯示升級通知之後
- 將升級映像放在HTTPS位置、然後提供URL給BlueXP

支援的升級途徑

您可以升級的版本取決於您目前執行的版本。Cloud Volumes ONTAP Cloud Volumes ONTAP

目前版本	您可以直接升級至的版本
9.14.1.	9.15.0
9.14.0%	9.14.1.
9.13.1.12.9.12.9.	9.14.1.
	9.14.0%
9.13.0	9.13.1.12.9.12.9.
9.12.1%	9.13.1.12.9.12.9.
	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
9.0	9.1

目前版本	您可以直接升級至的版本
8.3	9.0

請注意下列事項：

- 支援的升級途徑Cloud Volumes ONTAP 與內部部署ONTAP 的內部部署的更新途徑不同。
- 如果您依照工作環境中顯示的升級通知進行升級、則BlueXP會提示您升級至遵循這些支援升級途徑的版本。
- 如果您將升級映像放在HTTPS位置進行升級、請務必遵循這些支援的升級途徑。
- 在某些情況下、您可能需要升級數次才能達到目標版本。

  例如、如果您執行的是9.8版、而且想要升級至9.10.1版、則必須先升級至9.9.1版、然後再升級至9.10.1版。

修補程式版本

自 2024 年 1 月起、只有在 BlueXP 中、如果是三個最新版 Cloud Volumes ONTAP 的修補程式版本、才能進行修補程式升級。我們使用最新的 GA 版本來判斷在 BlueXP 中顯示的三個最新版本。例如、如果目前的 GA 版本為 9.13.1 、則 BlueXP 中會出現 9.11.1.9.13.1 的修補程式。如果您想要升級至 9.11.1 版或更低版本的修補程式版本、您需要使用手動升級程序 下載 ONTAP 映像。

根據補充程式（ P ）版本的一般規則、您可以從一個版本版本升級至目前執行版本或下一個版本的任何 P 版本。

以下是幾個範例：

- 9.13.0 > 9.13.1P15
- 9.12.1 > 9.13.1P2

還原或降級

不Cloud Volumes ONTAP 支援還原或降級至先前版本的功能。

支援註冊

必須向 NetApp 支援部門註冊、才能使用本頁所述的任何方法來升級軟體。 Cloud Volumes ONTAP這適用於 PAYGO 和 BYOL 。您需要 "手動登錄 PAYGO 系統"、但 BYOL 系統預設為註冊。

尚未註冊支援的系統仍會在新版本推出時收到在BlueXP中顯示的軟體更新通知。但您必須先註冊系統、才能升級軟體。

HA中介程序的升級

BlueXP也會在Cloud Volumes ONTAP 更新過程中視需要更新中介執行個體。

使用 C4 、 M4 和 R4 EC2 執行個體類型在 AWS 中升級

Cloud Volumes ONTAP 不再支援 C4 、 M4 和 R4 EC2 執行個體類型。您可以使用這些執行個體類型、將現有部署升級至 Cloud Volumes ONTAP 9.89.12.1 版。在您升級之前、我們建議您 變更執行個體類型。如果您無法變更執行個體類型、則需要 啟用增強的網路功能 升級之前。請閱讀下列各節、深入瞭解如何變更執行個體類型及啟用增強網路功能。

在執行 9.13.0 版及更新版本的 Cloud Volumes ONTAP 中、您無法使用 C4 、 M4 及 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、然後再減少 變更執行個體類型 或是使用 C5 、 m5 和 R5 EC2 執行個體類型部署新的 HA 配對組態、然後移轉資料。

變更執行個體類型

相較於 C5 、 m5 和 R5 EC2 執行個體類型、 C4 、 M4 和 R4 EC2 執行個體類型、每個節點的磁碟數量都會增加。如果您執行的 C4 、 M4 或 R4 EC2 執行個體的每個節點磁碟數低於 C5 、 m5 和 R5 執行個體的每個節點磁碟可用量上限、您可以將 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EC2執行個體類型Cloud Volumes ONTAP 以供使用"

如果您無法變更執行個體類型、請遵循中的步驟 [啟用增強的網路功能]。

啟用增強的網路功能

若要升級至 Cloud Volumes ONTAP 9.8 版及更新版本、您必須在執行 C4 、 M4 或 R4 執行個體類型的叢集上啟用 *Enhanced networking* 。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 等增強型網路"。

準備升級

執行升級之前、您必須先確認系統已就緒、並進行任何必要的組態變更。

- [計畫停機時間]
- [確認自動恢復功能仍啟用]
- 暫停SnapMirror傳輸
- 驗證Aggregate是否在線上
- [確認所有的生命都在主連接埠上]

計畫停機時間

當您升級單節點系統時、升級程序會使系統離線長達 25 分鐘、在此期間 I/O 會中斷。

在許多情況下、升級 HA 配對不會中斷營運、 I/O 也不會中斷。在此不中斷營運的升級程序中、會同時升級每個節點、以繼續為用戶端提供 I/O 服務。

工作階段導向的通訊協定可能會在升級期間對某些區域的用戶端和應用程式造成不良影響。如需詳細資訊、 "請參閱 ONTAP 文件"

確認自動恢復功能仍啟用

自動恢復必須在 Cloud Volumes ONTAP 一個「無法恢復的 HA 配對」上啟用（這是預設設定）。如果沒有、則作業將會失敗。

"供應說明文件：設定自動恢復的命令 ONTAP"

暫停SnapMirror傳輸

如果 Cloud Volumes ONTAP 某個不活躍的 SnapMirror 關係、最好在更新 Cloud Volumes ONTAP 該軟件之前暫停傳輸。暫停傳輸可防止 SnapMirror 故障。您必須暫停來自目的地系統的傳輸。

雖然 BlueXP 備份與還原使用 SnapMirror 實作來建立備份檔案（稱為 SnapMirror Cloud ）、但系統升級時不需要暫停備份。

關於這項工作

這些步驟說明如何使用系統管理程式來執行 9.3 版及更新版本。

步驟

1. 從目的地系統登入System Manager。

   您可以將網頁瀏覽器指向叢集管理LIF的IP位址、以登入System Manager。您可以在Cloud Volumes ONTAP不工作環境中找到IP位址。

   您要從哪個電腦存取BlueXP、必須有連到Cloud Volumes ONTAP 該系統的網路連線。例如、您可能需要從雲端供應商網路中的跨接主機登入BlueXP。

2. 按一下 * 保護 > 關係 * 。
3. 選取關係、然後按一下 * 作業 > 靜止 * 。

驗證Aggregate是否在線上

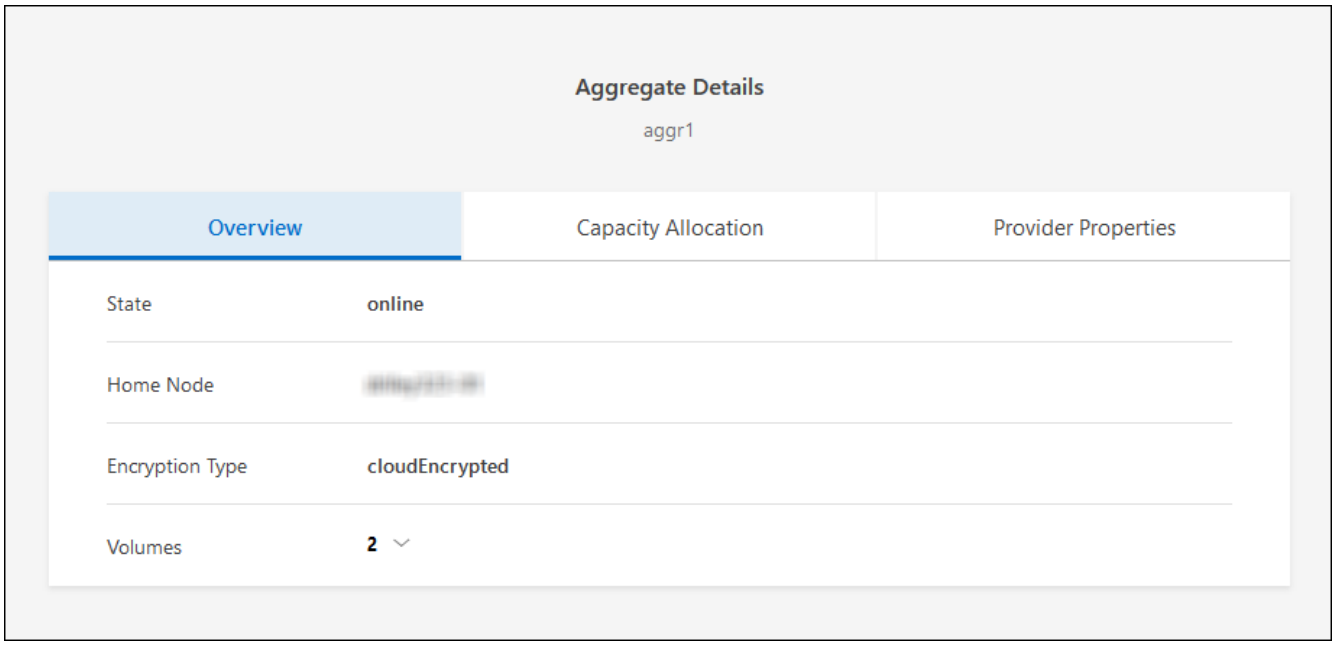
更新軟體之前、必須先在線上安裝適用於 Cloud Volumes ONTAP 此功能的 Aggregate 。在大多數的組態中、Aggregate 都應該處於線上狀態、但如果沒有、則應該將其上線。

關於這項工作

這些步驟說明如何使用系統管理程式來執行 9.3 版及更新版本。

步驟

1. 在工作環境中、按一下 * Aggregate * 標籤。
2. 按一下 Aggregate 標題下的省略符號按鈕、然後選取 * 檢視 Aggregate details* 。



3. 如果 Aggregate 離線、請使用 System Manager 將 Aggregate 上線：
   a. 按一下「 * 儲存設備 > 集合體與磁碟 > Aggregate * 」。
   b. 選取 Aggregate 、然後按一下 * 更多動作 > 狀態 > 線上 * 。

確認所有的生命都在主連接埠上

在升級之前、所有的生命體都必須位於主連接埠上。請參閱的 ONTAP 文件 "確認所有的生命都在主連接埠上"。

如果發生升級失敗錯誤、請參閱 "知識庫文章「 Cloud Volumes ONTAP 升級失敗」"。

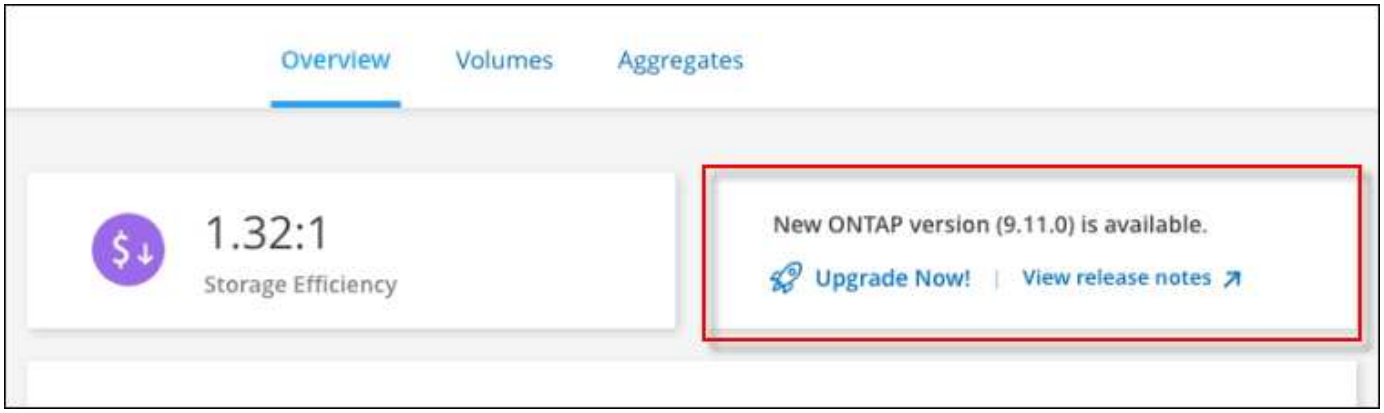
升級**Cloud Volumes ONTAP**

當有新版本可供升級時、BlueXP會通知您。您可以從此通知開始升級程序。如需詳細資訊、請參閱 從BlueXP通知升級。

使用外部URL上的映像執行軟體升級的另一種方法。如果BlueXP無法存取S3儲存區來升級軟體、或是您已獲得修補程式、此選項很有幫助。如需詳細資訊、請參閱 從URL提供的映像升級。

從**BlueXP**通知升級

當Cloud Volumes ONTAP 有新版Cloud Volumes ONTAP 的功能時、BlueXP會在不工作環境中顯示通知：



您可以從此通知開始升級程序、從 S3 儲存區取得軟體映像、安裝映像、然後重新啟動系統、藉此自動化程序。

開始之前

在Cloud Volumes ONTAP 這個系統上、不能進行諸如Volume或Aggregate建立等BlueXP作業。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 選取工作環境。

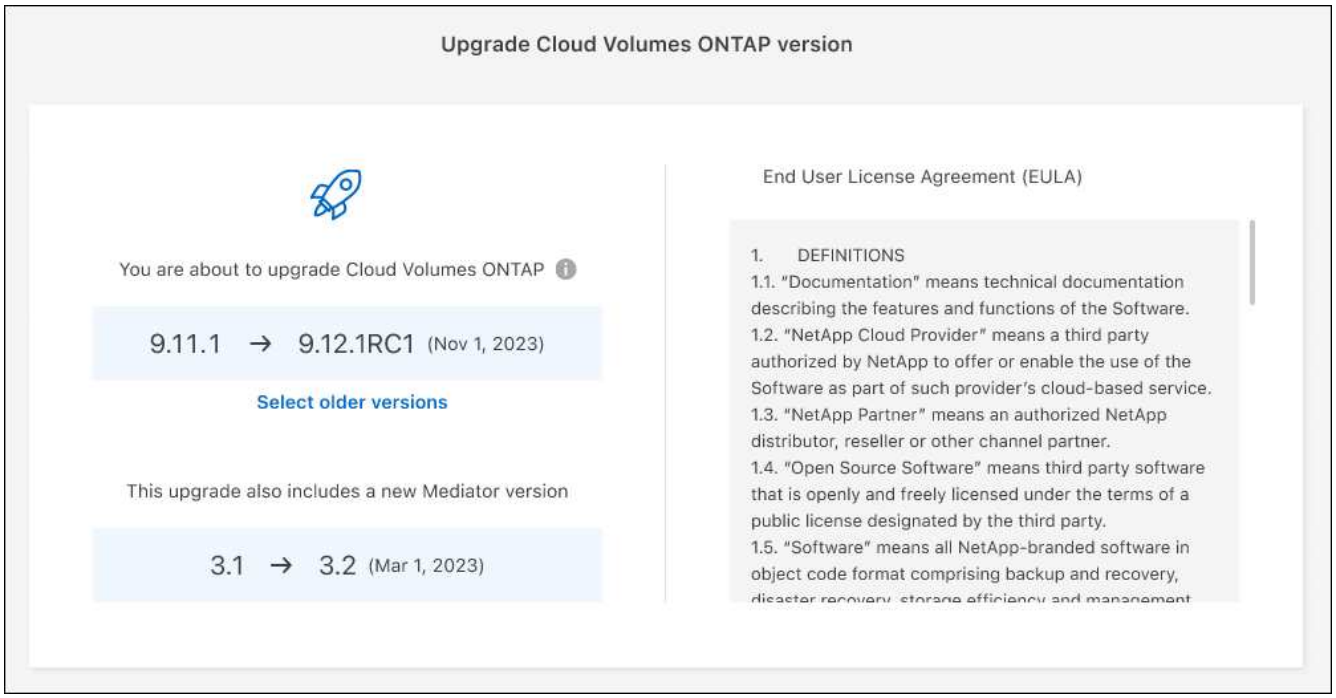
   如果有新版本可用、則會在「概觀」索引標籤中顯示通知：

3. 如果有新版本可用、請按一下 * 立即升級！ *

   您必須先擁有 NetApp 支援網站 帳戶、才能透過 BlueXP 通知升級 Cloud Volumes ONTAP 。

4. 在「升級 Cloud Volumes ONTAP 」頁面中、閱讀 EULA 、然後選取 * 我閱讀並核准 EULA * 。
5. 按一下*升級*。

   「升級 Cloud Volumes ONTAP 」頁面預設會選取最新可用的 Cloud Volumes ONTAP 版本進行升級。如果有舊版 Cloud Volumes ONTAP 、您可以按一下 * 選擇舊版 * 來選擇升級版本。請參閱 "支援的升級路徑清單" 根據您目前的 Cloud Volumes ONTAP 版本、取得適當的升級路徑。



6. 若要檢查升級狀態、請按一下「設定」圖示、然後選取 * 時間表 * 。

結果

BlueXP會啟動軟體升級。軟體更新完成後、您可以在工作環境中執行動作。

完成後

如果您暫停 SnapMirror 傳輸、請使用 System Manager 繼續傳輸。

從**URL**提供的映像升級

您可以將Cloud Volumes ONTAP 「更新」軟體映像放在Connector或HTTP伺服器上、然後從BlueXP開始軟體升級。如果BlueXP無法存取S3儲存區來升級軟體、您可以使用此選項。

開始之前

- 在Cloud Volumes ONTAP 這個系統上、不能進行諸如Volume或Aggregate建立等BlueXP作業。
- 如果您使用HTTPS來裝載ONTAP 資訊影像、升級可能會因為SSL驗證問題而失敗、因為遺失憑證。因應措施是產生並安裝CA簽署的憑證、以用於ONTAP 在EXP和BlueXP之間進行驗證。

  前往NetApp知識庫檢視逐步指示：

  "NetApp KB：如何將BlueXP設定為HTTPS伺服器、以裝載升級映像"

步驟

1. 選用：設定HTTP伺服器、以裝載Cloud Volumes ONTAP 支援此功能的軟體映像。

   如果您有虛擬網路的VPN連線、您可以將Cloud Volumes ONTAP 該Imagesoftware映像放在您自己網路中的HTTP伺服器上。否則、您必須將檔案放在雲端的HTTP伺服器上。

2. 如果您使用自己的安全群組Cloud Volumes ONTAP 來執行功能、請確定傳出規則允許HTTP連線Cloud Volumes ONTAP 、以便讓畫面能夠存取軟體映像。

預設情況下、預先定義Cloud Volumes ONTAP 的「支援HTTP連線」安全群組會允許傳出HTTP連線。

3. 從取得軟體映像 "NetApp 支援網站"。
4. 將軟體映像複製到Connector上的目錄、或是將從其中提供檔案的HTTP伺服器上。

   有兩種路徑可供使用。正確的路徑取決於您的Connector版本。

   - 「/opt/application/netapp/cloudmanager/dock_occm/data/ontap / imes/」
   - /op/application/NetApp/cloudmanager/ontONTAP /映像/
5. 在 BlueXP 的工作環境中、按一下 * 。 （省略號圖示） * 、然後按一下 * 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 * 變更映像 * 。

   如果您將軟體映像複製到上述路徑中的Connector、請輸入下列URL：

   http://<Connector-private-IP-address>/ontap/images/<image-file-name>

   在 URL 中， * image-file-name* 必須遵循格式 "cot.image.9.13.1p2.tgz" 。
7. 按 * Proceed* 確認。

結果

BlueXP會啟動軟體更新。軟體更新完成後、即可在工作環境中執行動作。

完成後

如果您暫停 SnapMirror 傳輸、請使用 System Manager 繼續傳輸。

修正使用**Google Cloud NAT**閘道時的下載失敗

Connector會自動下載Cloud Volumes ONTAP 適用於更新的軟體。如果您的組態使用Google Cloud NAT閘道、下載可能會失敗。您可以限制軟體映像分成的零件數量來修正此問題。此步驟必須使用BlueXP API完成。

步驟

1. 將PUT要求提交至/occm/config、並以下列Json做為本文：

```
{
  "maxDownloadSessions": 32
}
```

_MaxDownloadSseds_的值可以是1或任何大於1的整數。如果值為1、則下載的映像不會分割。

請注意、32為範例值。您應該使用的值取決於NAT組態和可同時使用的工作階段數目。

"深入瞭解/occm/config API呼叫"。

註冊隨用隨付系統

NetApp提供的支援包含Cloud Volumes ONTAP 在整個過程中、但您必須先向NetApp註冊系統、才能啟動支援。

向 NetApp 註冊 PAYGO 系統時、必須 ONTAP 使用任何方法來升級 __LW_NETAPP 軟體 "本頁說明"。

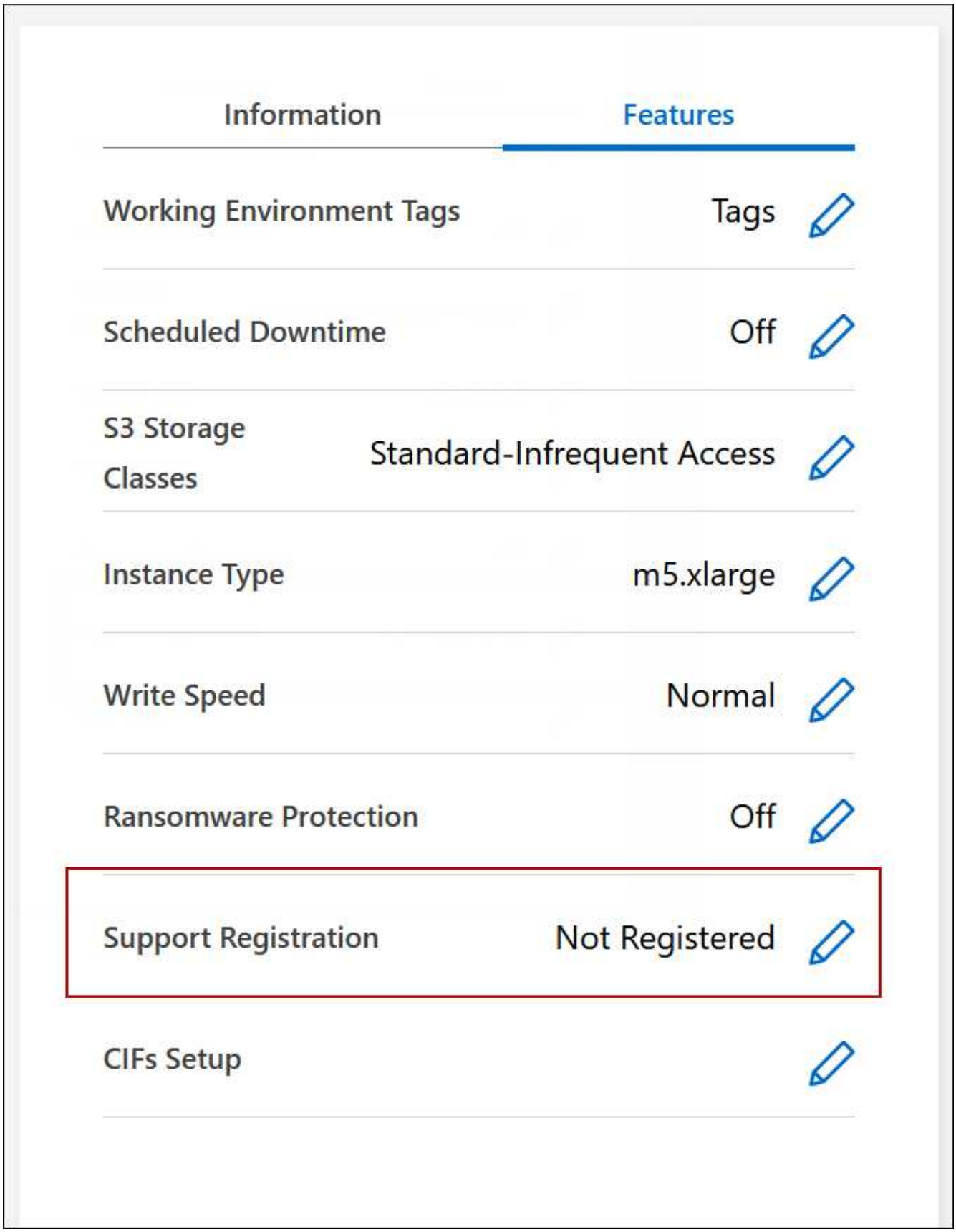
尚未註冊支援的系統仍會在新版本推出時收到在BlueXP中顯示的軟體更新通知。但您必須先註冊系統、才能升級軟體。

步驟

1. 如果NetApp 支援網站 您尚未將您的支援帳戶新增至藍圖XP、請前往*帳戶設定*、立即新增。

   "瞭解如何新增 NetApp 支援網站帳戶"。

2. 在「 Canvas 」頁面上、按兩下您要登錄的系統名稱。
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 支援網站帳戶、然後按一下 * 註冊 * 。

結果

BlueXP向NetApp註冊系統。

管理 **Cloud Volumes ONTAP** 功能不全

您可以從Cloud Volumes ONTAP BlueXP停止並開始執行功能、以管理雲端運算成本。

排程 **Cloud Volumes ONTAP** 自動關閉功能

您可能想要在 Cloud Volumes ONTAP 特定時間間隔內關閉此功能、以降低運算成本。您可以將BlueXP設定為自動關機、然後在特定時間重新啟動系統、而非手動執行此動作。

關於這項工作

- 當您排程自動關閉Cloud Volumes ONTAP 您的作業系統時、如果正在進行作用中的資料傳輸、則BlueXP會將關機時間延後。

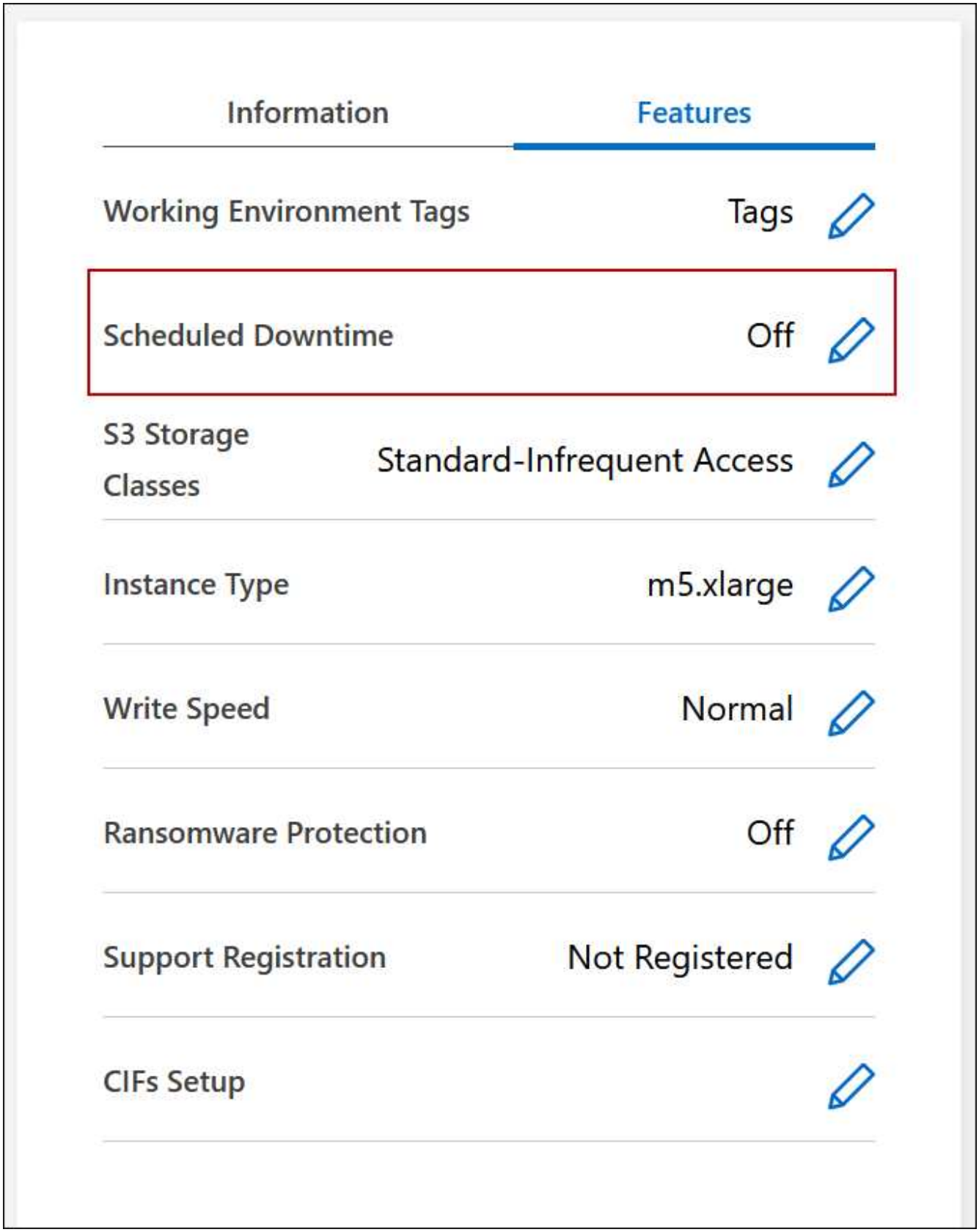
  在傳輸完成後、BlueXP會關閉系統。

- 此工作會排程 HA 配對中兩個節點的自動關機。
- 透過Cloud Volumes ONTAP 排定的關機功能關閉功能時、不會建立開機和根磁碟的快照。

  只有在執行手動關機時、才會自動建立快照、如下一節所述。

步驟

1. 在 Canvas 頁面上、按兩下所需的工作環境。
2. 在「總覽」索引標籤上、按一下「功能」面板、然後按一下 * 排程停機 * 旁的鉛筆圖示。



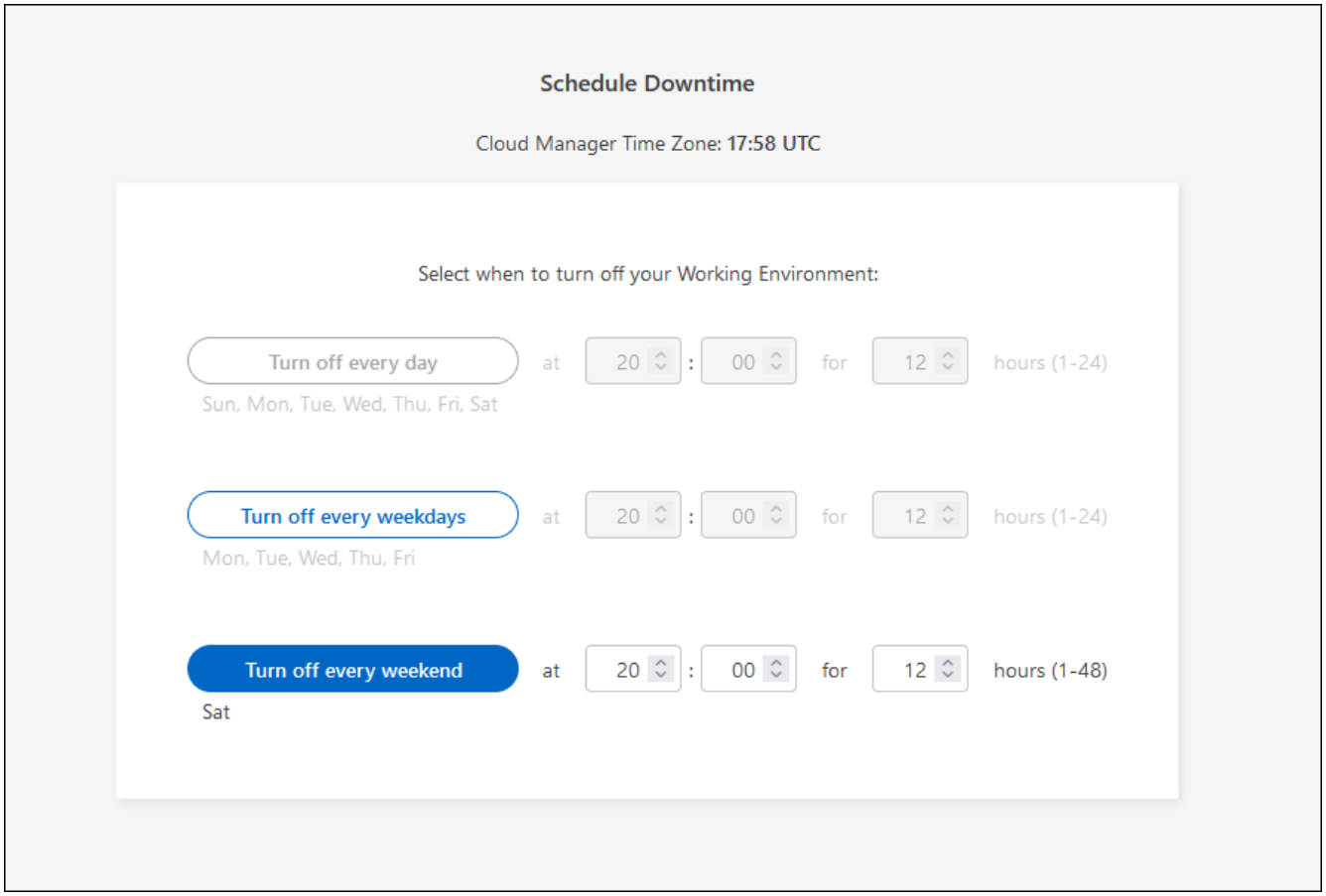
3. 指定關機排程：

   a. 選擇您要每天、每個工作日、每個週末或三種選項的任意組合來關閉系統。

   b. 指定您要關閉系統的時間、以及關閉系統的時間長度。

- 範例 *

下圖顯示一個排程、指示 BlueXP 每週六下午 20 ： 00 關閉系統（下午 8 ： 00 ） 12 小時。每週一上午12：00、BlueXP會重新啟動系統



4. 按一下「 * 儲存 * 」。

結果

BlueXP會儲存排程。「功能」面板下方的對應排程停機項目會顯示為「開啟」。

停止 **Cloud Volumes ONTAP**

停止 Cloud Volumes ONTAP 使用功能可節省運算成本、並建立根磁碟和開機磁碟的快照、有助於疑難排解。

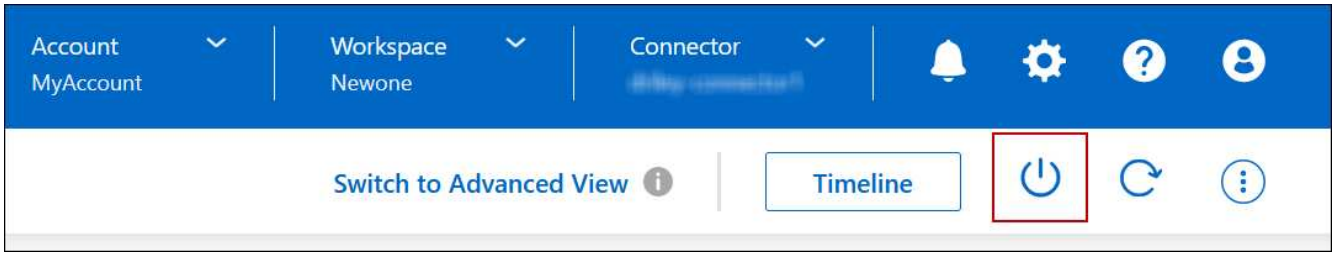
為降低成本、BlueXP會定期刪除較舊的根磁碟和開機磁碟快照。根磁碟和開機磁碟只會保留兩個最新的快照。

關於這項工作

當您停止HA配對時、BlueXP會關閉兩個節點。

步驟

1. 在工作環境中、按一下 * 關閉 * 圖示。



2. 保留建立快照的選項、因為快照可以啟用系統還原。
3. 按一下 * 關閉 * 。

   停止系統可能需要幾分鐘的時間。您可以稍後從工作環境頁面重新啟動系統。

   快照會在重新開機時自動建立。

使用 NTP 同步系統時間

指定 NTP 伺服器可同步處理網路中系統之間的時間、有助於避免時間差異所造成的問題。

使用指定NTP伺服器 "BlueXP API" 或從使用者介面進行 "建立CIFS伺服器"。

修改系統寫入速度

BlueXP可讓您選擇Cloud Volumes ONTAP 一般或高速寫入速度來執行功能。預設寫入速度為正常。如果工作負載需要快速寫入效能、您可以改為高速寫入。

所有類型的單一節點系統和部分HA配對組態均支援高速寫入。檢視中支援的組態 "發行說明 Cloud Volumes ONTAP"

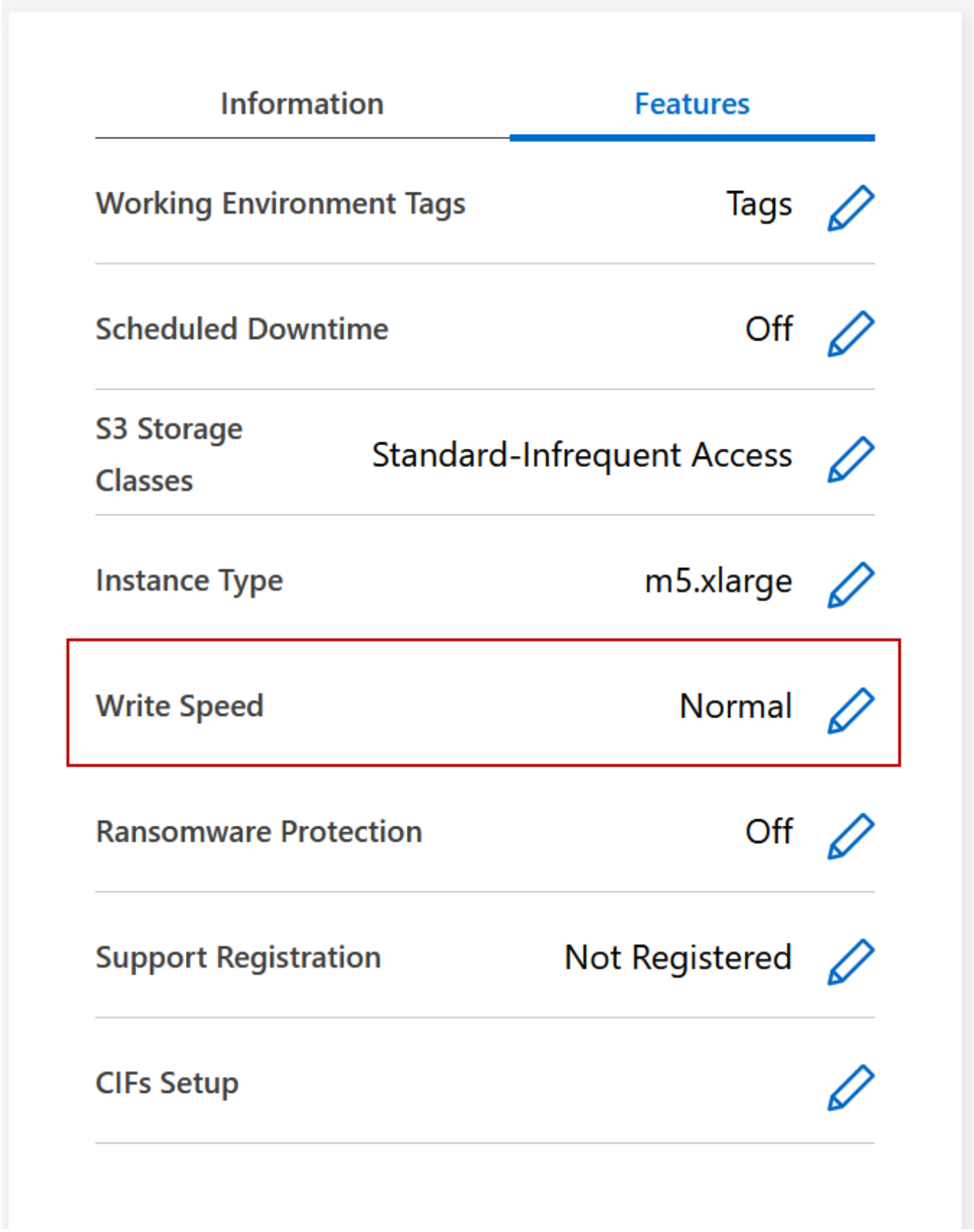
在變更寫入速度之前、您應該先進行 "瞭解一般與高設定之間的差異"。

關於這項工作

- 確保磁碟區或集合體建立等作業未在進行中。
- 請注意、這項變更會重新啟動Cloud Volumes ONTAP 整個系統。這是一項中斷營運的程序、需要整個系統停機。

步驟

1. 在「 Canvas 」頁面上、按兩下您設定為寫入速度的系統名稱。
2. 在「總覽」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」、則必須閱讀「我瞭解 … 」聲明、並勾選方塊以確認。

從9.13.0版開始、Google Cloud中的「*高速*寫入速度Cloud Volumes ONTAP 」選項可搭配支援。

4. 按一下 * 儲存 * 、檢閱確認訊息、然後按一下 * 核准 * 。

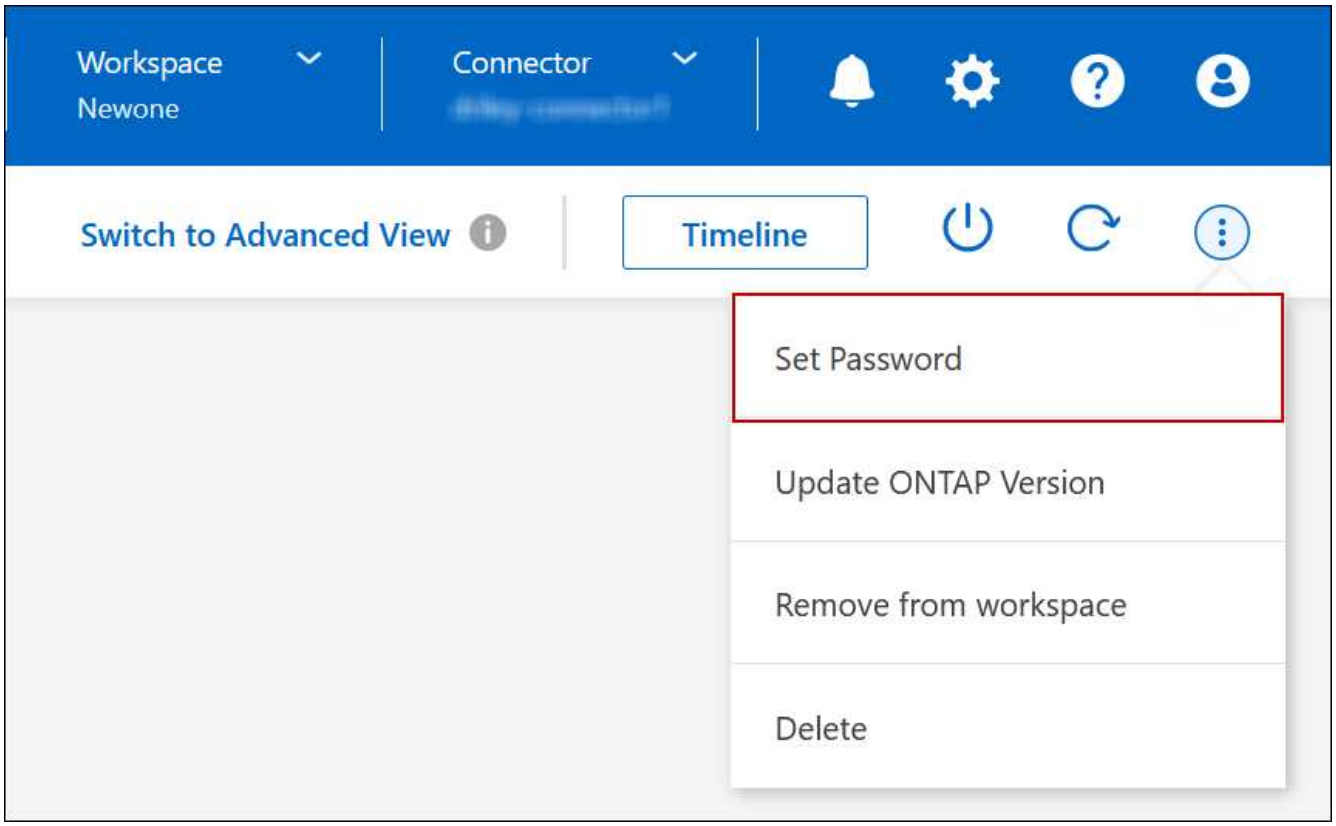
變更Cloud Volumes ONTAP 密碼以供使用

包含叢集管理帳戶。 Cloud Volumes ONTAP如有需要、您可以從BlueXP變更此帳戶的密碼。

您不應透過 System Manager 或 CLI 變更管理帳戶的密碼。此密碼不會反映在BlueXP中。因此、BlueXP無法正確監控執行個體。

步驟

1. 在「畫布」頁面上、按兩下 Cloud Volumes ONTAP 工作環境的名稱。
2. 在 BlueXP 主控台的右上角、按一下省略符號圖示、然後選取 * 設定密碼 * 。



新密碼必須與您最近使用的六個密碼之一不同。

新增、移除或刪除系統

將現有Cloud Volumes ONTAP 的不只是系統新增至藍圖XP

您可以探索並新增Cloud Volumes ONTAP 現有的元件系統至藍圖XP。如果您部署了新

的BlueXP系統、您可能會這麼做。

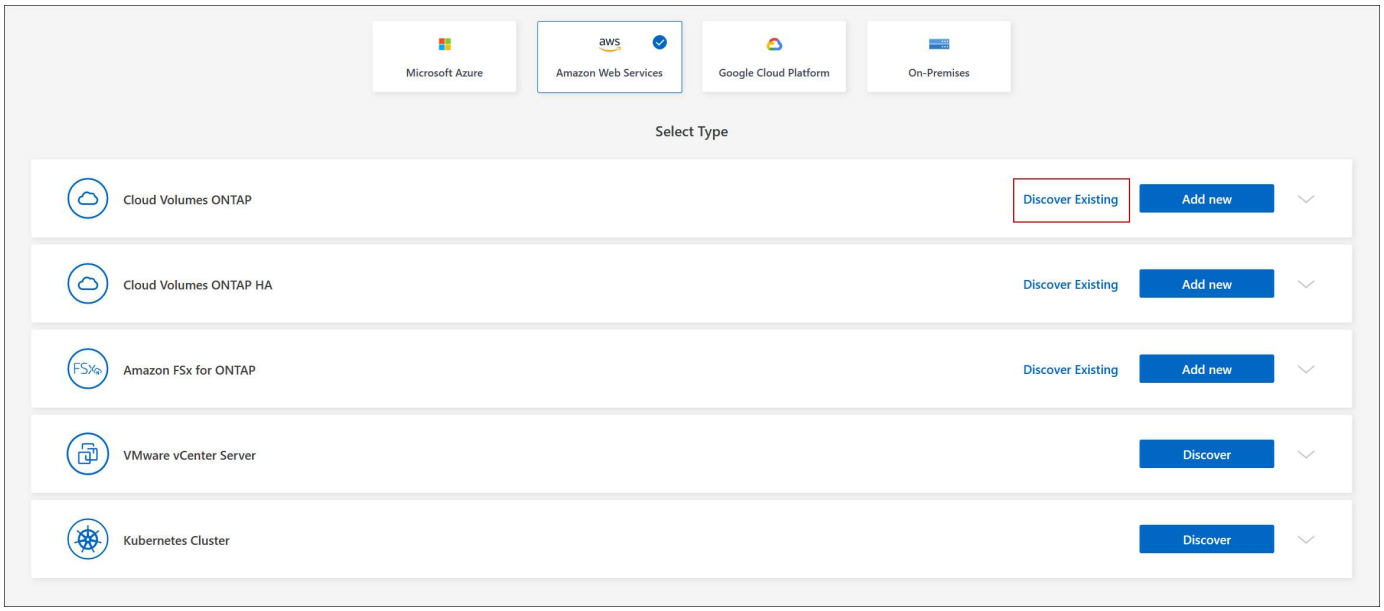
開始之前

您必須知道 Cloud Volumes ONTAP 該密碼才能使用此功能。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按一下「 * 新增工作環境 * 」 。
3. 選取系統所在的雲端供應商。
4. 選擇 Cloud Volumes ONTAP 哪種類型的系統。
5. 按一下連結以探索現有系統。

+



1. 在「區域」頁面上、選擇執行個體所在的區域、然後選取執行個體。
2. 在「認證資料」頁面上、輸入 Cloud Volumes ONTAP for the fu位 管理員使用者的密碼、然後按一下「 * 執行 * 」 。

結果

BlueXP會將Cloud Volumes ONTAP 這個實例新增到工作區。

移除 **Cloud Volumes ONTAP** 運作環境

帳戶管理員可移除 Cloud Volumes ONTAP 運作中的環境、將其移至其他系統、或疑難排解探索問題。

關於這項工作

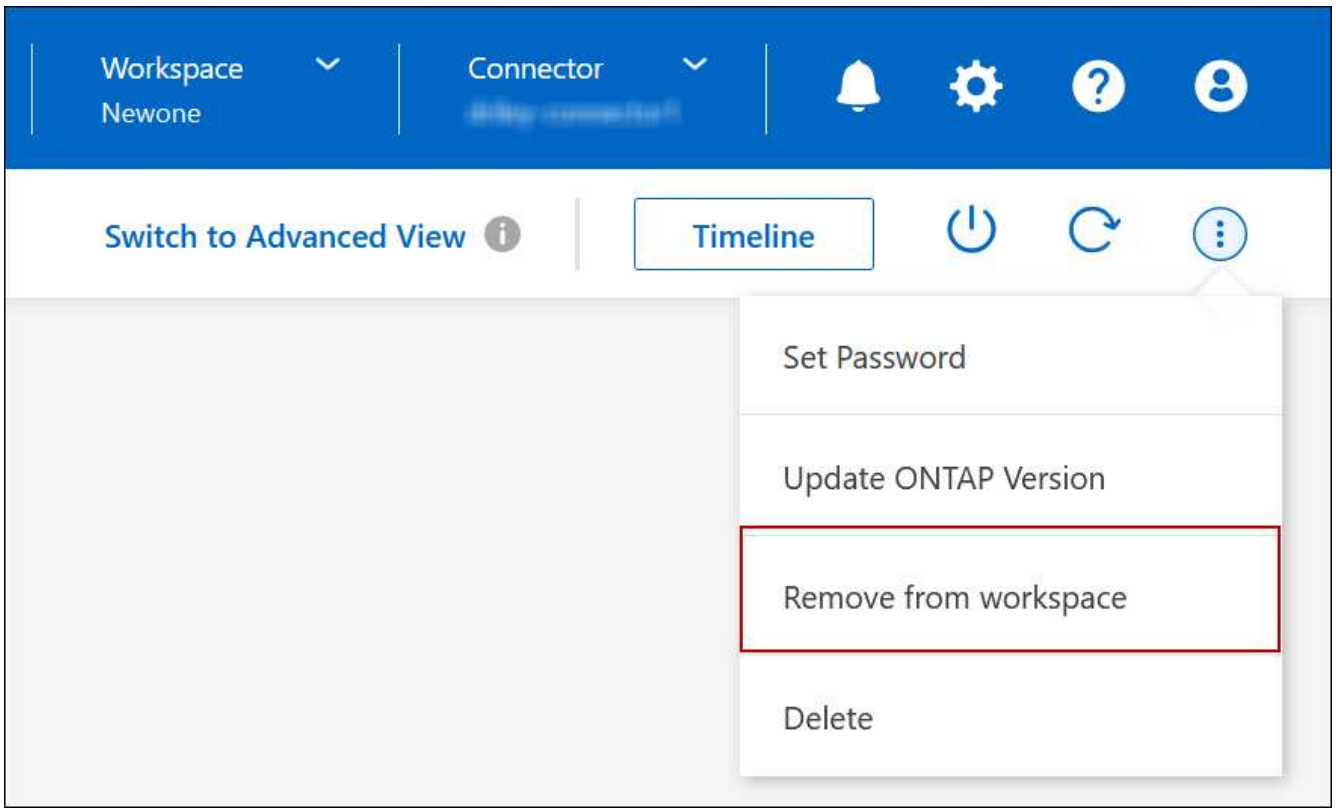
移除Cloud Volumes ONTAP 功能不正常的環境、將其從藍圖XP移除。它不會刪除 Cloud Volumes ONTAP 此作業系統。您稍後可以重新探索工作環境。

從BlueXP移除工作環境可讓您執行下列動作：

- 在另一個工作區重新探索
- 從另一個BlueXP系統重新探索
- 如果在初始探索期間發生問題、請重新探索

步驟

1. 在 Canvas 頁面上、按兩下您要移除的工作環境。
2. 在 BlueXP 主控台的右上角、按一下省略符號圖示、然後選取 * 從工作區移除 * 。



3. 在「從工作區檢閱」視窗中、按一下 * 移除 * 。

結果

BlueXP移除工作環境。使用者可隨時從「畫版」頁面重新探索此工作環境。

刪除**Cloud Volumes ONTAP** 一個系統

您應該一律從Cloud Volumes ONTAP BlueXP刪除不適用的系統、而不要從雲端供應商的主控台刪除。例如、如果您從Cloud Volumes ONTAP 雲端供應商處終止授權的樣例、則無法將授權金鑰用於其他執行個體。您必須從BlueXP刪除工作環境、才能釋出授權。

當您刪除工作環境時、BlueXP會終止Cloud Volumes ONTAP 執行個體、並刪除磁碟和快照。

當您刪除工作環境時、其他服務所管理的資源、例如 BlueXP 備份和還原的備份、以及 BlueXP 分類的執行個體、都不會被刪除。您必須自行手動刪除。如果您沒有、您將繼續收取這些資源的費用。

當您Cloud Volumes ONTAP 的雲端供應商部署了支援功能時、就能在執行個體上提供終止保護。此選項有助於防止意外終止。

步驟

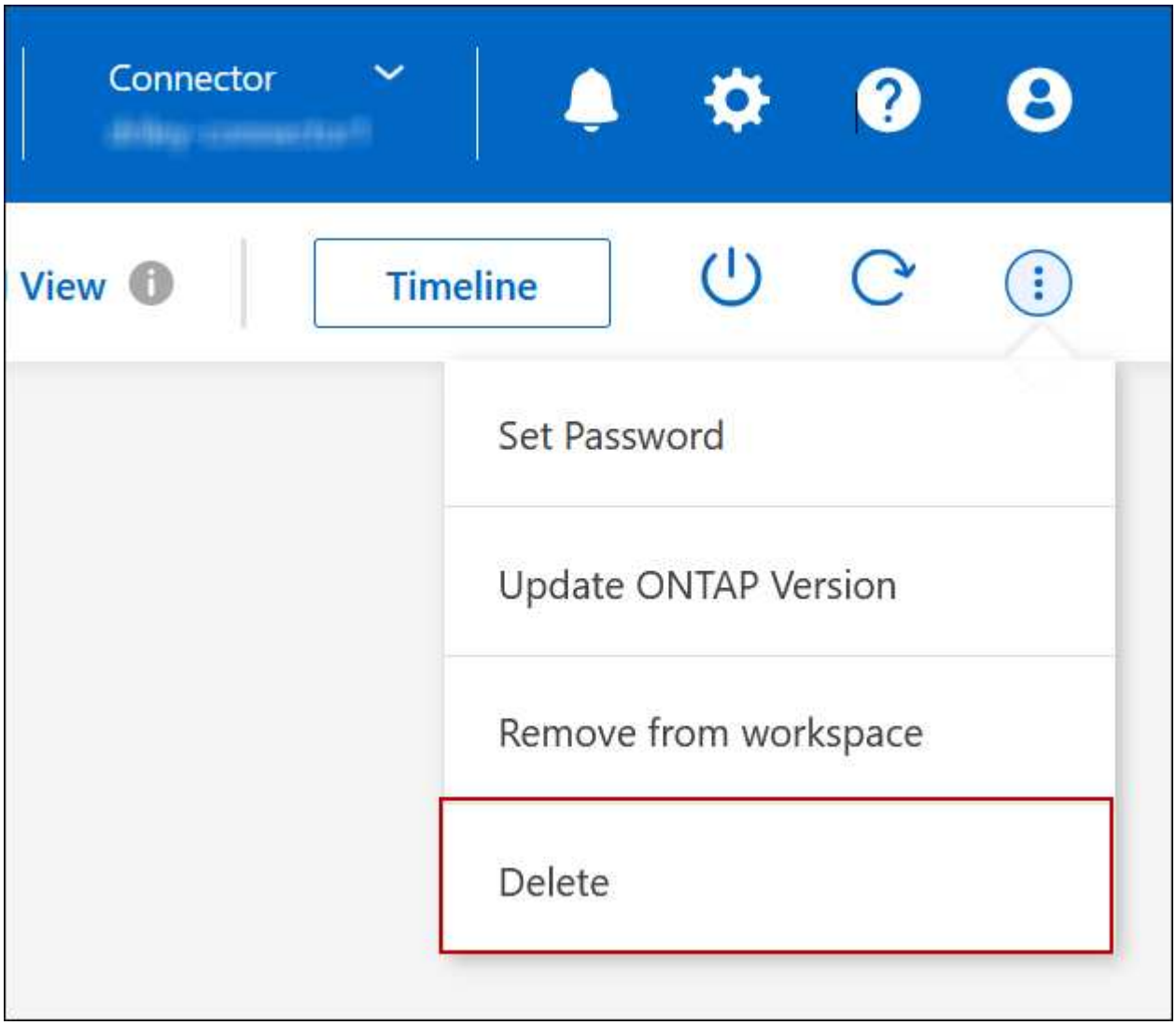
1. 如果您在工作環境中啟用 BlueXP 備份與還原、請先判斷是否仍需要備份資料、然後再決定 "如有必要、請刪除備份"。

   BlueXP 備份與還原在設計上不受 Cloud Volumes ONTAP 的保護。BlueXP 備份與還原不會在您刪除 Cloud Volumes ONTAP 系統時自動刪除備份、而且在刪除系統之後、 UI 目前不支援刪除備份。

2. 如果您在此工作環境中啟用 BlueXP 分類、且沒有其他工作環境使用此服務、則您必須刪除該服務的執行個體。

   "深入瞭解 BlueXP 分類執行個體"。

3. 刪除Cloud Volumes ONTAP 這個作業環境。
   a. 在「畫版」頁面上、按兩下Cloud Volumes ONTAP 您要刪除的「紙張工作環境」名稱。
   b. 在 BlueXP 主控台的右上角、按一下省略符號圖示、然後選取 * 刪除 * 。



c. 在刪除工作環境視窗下、輸入工作環境的名稱、然後按一下 * 刪除 * 。

刪除工作環境最多可能需要 5 分鐘。

AWS管理

變更EC2執行個體類型Cloud Volumes ONTAP 以供使用

在Cloud Volumes ONTAP AWS中啟動時、您可以從多個執行個體或類型中進行選擇。如果判斷執行個體的大小過小或過大、您可以隨時變更執行個體類型。

關於這項工作

- 自動恢復必須在 Cloud Volumes ONTAP 一個「無法恢復的 HA 配對」上啟用（這是預設設定）。如果沒有、則作業將會失敗。

  "供應說明文件：設定自動恢復的命令 ONTAP"

- 變更執行個體類型可能會影響AWS服務費用。
- 此作業會重新啟動 Cloud Volumes ONTAP 。

  對於單一節點系統、 I/O 會中斷。

  對於 HA 配對、變更不中斷營運。HA 配對可繼續提供資料。

BlueXP會主動啟動接管並等待回饋、一次只能正常變更一個節點。NetApp 的 QA 團隊在這段過程中測試了寫入和讀取檔案的能力、並未發現客戶端有任何問題。隨著連線變更、我們確實看到 I/O 層級的重試次數、但應用程式層卻取代了 NFS/CIFS 連線的這些短「重新連線」。

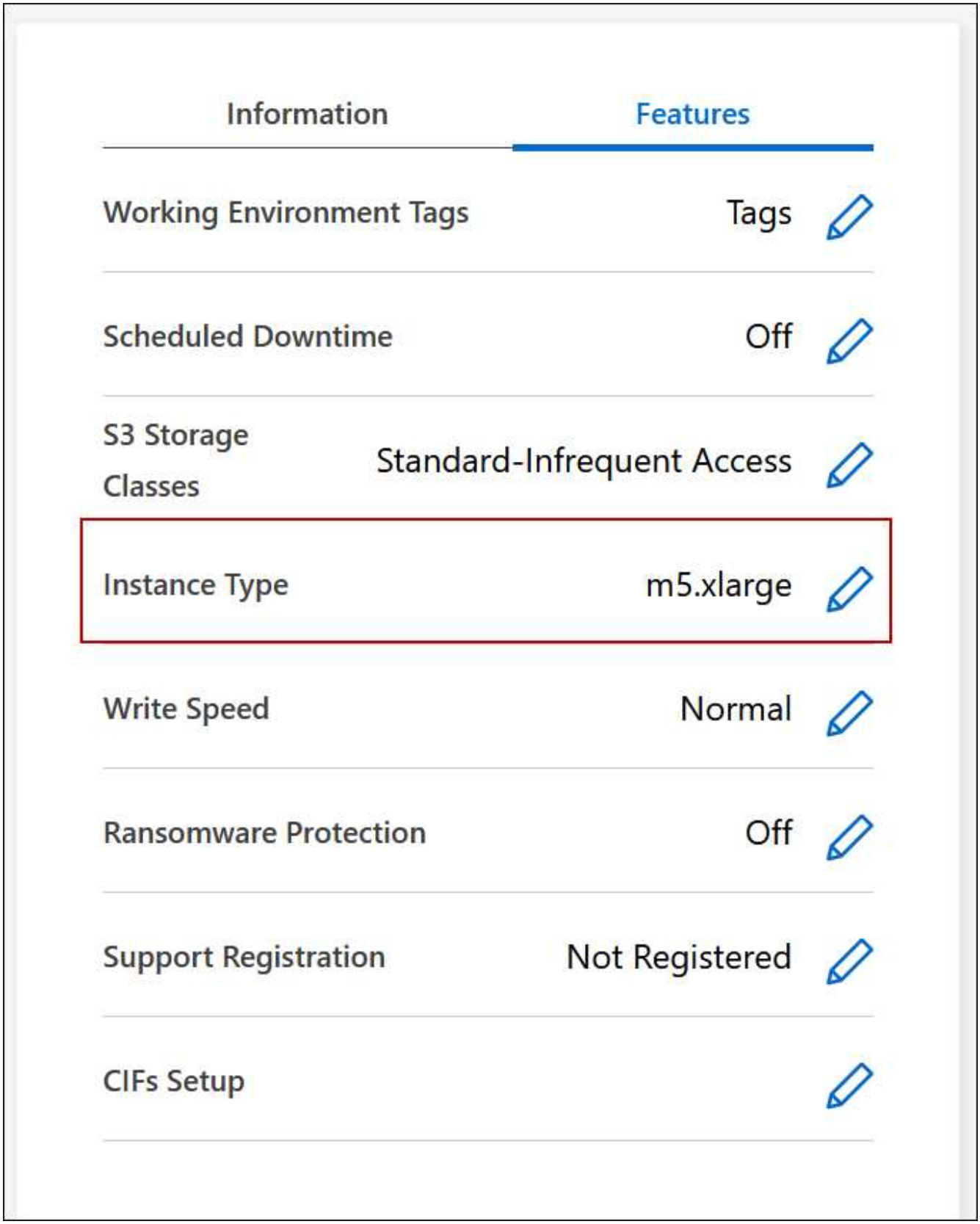
參考資料

如需 AWS 中支援的執行個體類型清單、請參閱 "支援的 EC2 執行個體"。

如果您無法從 C4 、 M4 或 R4 執行個體變更執行個體類型、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 Canvas 頁面上、選取工作環境。
2. 在「概述」標籤上、按一下「功能」面板、然後按一下「 * 執行個體類型 * 」旁邊的鉛筆圖示。



a. 如果您使用的是節點型 PAYGO 授權、您可以選擇不同的授權和執行個體類型、方法是按一下 * 授權類型 * 旁的鉛筆圖示。

3. 選擇執行個體類型、選取核取方塊以確認您瞭解變更的影響、然後按一下 * 變更 * 。

結果

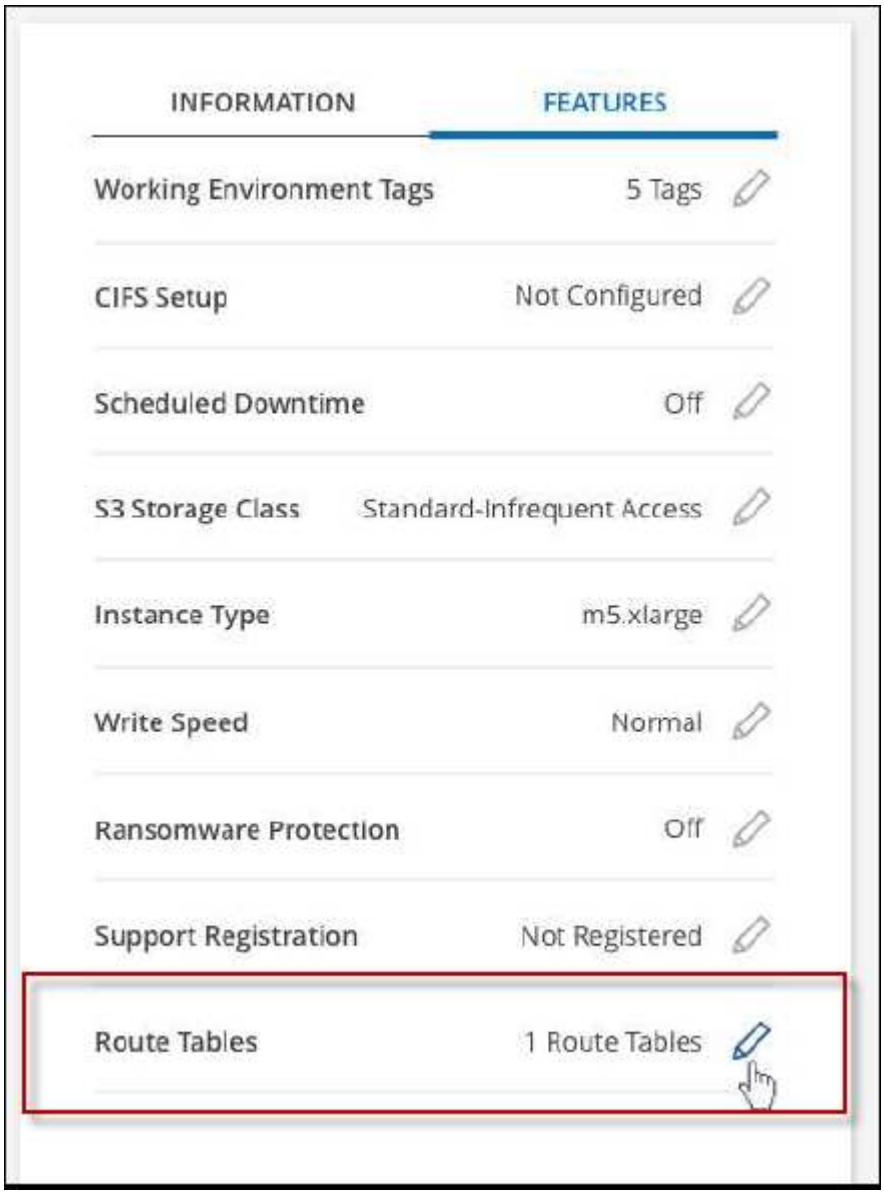
以新組態重新開機。 Cloud Volumes ONTAP

在多個**AZs**中變更**HA**配對的路由表

您可以修改AWS路由表、其中包含部署在多個AWS可用性區域（AZs）中之HA配對的浮動IP位址路由。如果新的 NFS 或 CIFS 用戶端需要存取 AWS 中的 HA 配對、您可以這麼做。

步驟

1. 在 Canvas 頁面上、選取工作環境。
2. 在「總覽」標籤上、按一下「功能」面板、然後按一下「 * 路由表 * 」旁邊的鉛筆圖示。



3. 修改所選路由表的清單、然後按一下「 * 儲存 * 」。

結果

BlueXP會傳送AWS要求來修改路由表。

Azure管理

變更Azure VM類型Cloud Volumes ONTAP 以供使用

在Cloud Volumes ONTAP Microsoft Azure中啟動時、您可以從多種VM類型中進行選擇。您可以隨時變更VM類型、只要判斷其規模過小或過大、就能滿足您的需求。

關於這項工作

- 自動恢復必須在 Cloud Volumes ONTAP 一個「無法恢復的 HA 配對」上啟用（這是預設設定）。如果沒有、則作業將會失敗。

  "供應說明文件：設定自動恢復的命令 ONTAP"

- 變更VM類型可能會影響Microsoft Azure服務費用。
- 此作業會重新啟動 Cloud Volumes ONTAP 。

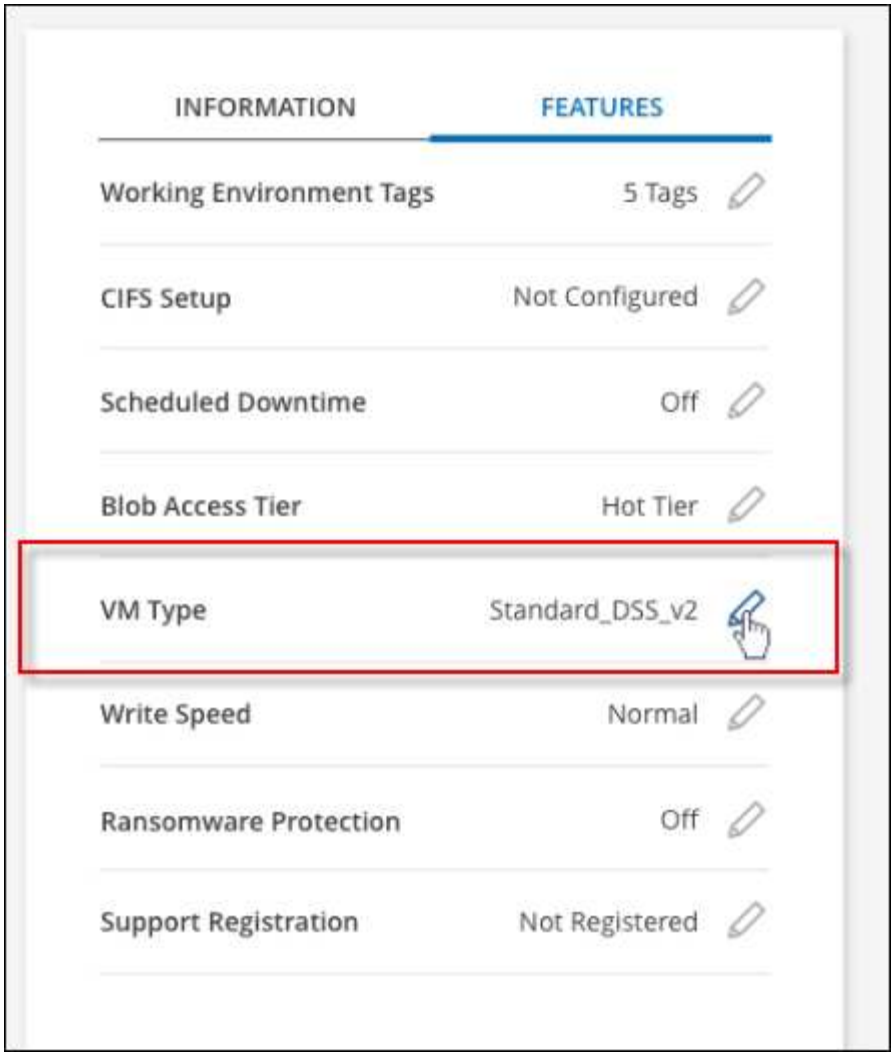
  對於單一節點系統、 I/O 會中斷。

  對於 HA 配對、變更不中斷營運。HA 配對可繼續提供資料。

  BlueXP會主動啟動接管並等待回饋、一次只能正常變更一個節點。NetApp 的 QA 團隊在這段過程中測試了寫入和讀取檔案的能力、並未發現客戶端有任何問題。隨著連線變更、我們確實看到 I/O 層級的重試次數、但應用程式層卻取代了 NFS/CIFS 連線的這些短「重新連線」。

步驟

1. 在 Canvas 頁面上、選取工作環境。
2. 按一下 [概觀] 索引標籤上的 [功能] 面板，然後按一下 *VM 類型 * 旁邊的鉛筆圖示。



a. 如果您使用的是節點型 PAYGO 授權、您可以選擇不同的授權和 VM 類型、方法是按一下 * 授權類型 * 旁的鉛筆圖示。

3. 選取 VM 類型、選取核取方塊以確認您瞭解變更的影響、然後按一下 * 變更 * 。

結果

以新組態重新開機。 Cloud Volumes ONTAP

在**Cloud Volumes ONTAP Azure**中覆寫**CIFS**鎖、以利執行不需使用的功能

帳戶管理員可在BlueXP中啟用一項設定、以防止Cloud Volumes ONTAP 在Azure維護活動期間發生有關還原儲存設備的問題。啟用此設定時 Cloud Volumes ONTAP 、不支援 CIFS 會鎖定並重設作用中的 CIFS 工作階段。

關於這項工作

Microsoft Azure 會排程在其虛擬機器上定期進行維護活動。當某個維護事件發生在Cloud Volumes ONTAP 一個不支援的HA配對上時、HA配對會啟動儲存設備接管。如果在此維護事件期間有作用中的CIFS工作階段、則CIFS檔案上的鎖定功能可能會妨礙儲存設備恢復。

如果啟用此設定、 Cloud Volumes ONTAP 則會取消鎖定並重設作用中的 CIFS 工作階段。因此、HA配對可在這些維護事件期間完成儲存恢復。

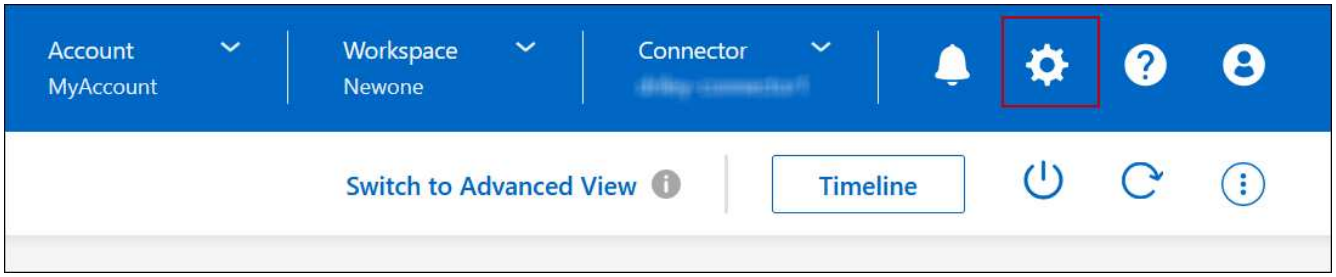
此程序可能會對 CIFS 用戶端造成破壞。未從 CIFS 用戶端提交的資料可能會遺失。

您需要的產品

您必須先建立連接器、才能變更BlueXP設定。 "瞭解方法"。

步驟

1. 在 BlueXP 主控台的右上角、按一下「設定」圖示、然後選取 * 「 Cloud Volumes ONTAP 設定 * 」 。



2. 在* Azure 下、按一下 Azure CIFS Locks for Azure HA工作環境*。
3. 按一下核取方塊以啟用此功能、然後按一下「儲存」 。

使用**Azure**私有連結或服務端點

使用Azure Private Link連線至相關儲存帳戶。Cloud Volumes ONTAP如有需要、您可以停用Azure私有連結、改用服務端點。

總覽

根據預設、BlueXP會啟用Azure Private Link、以便Cloud Volumes ONTAP 在支援的各個儲存帳戶之間建立連線。Azure Private Link可保護Azure中端點之間的連線安全、並提供效能優勢。

如有需要、您可以設定Cloud Volumes ONTAP 使用服務端點、而非Azure Private Link。

無論是哪一種組態、BlueXP都會限制Cloud Volumes ONTAP 存取網路、以利連接到各個儲存帳戶。網路存取僅限於Cloud Volumes ONTAP 部署了下列項目的vnet和部署Connector的vnet。

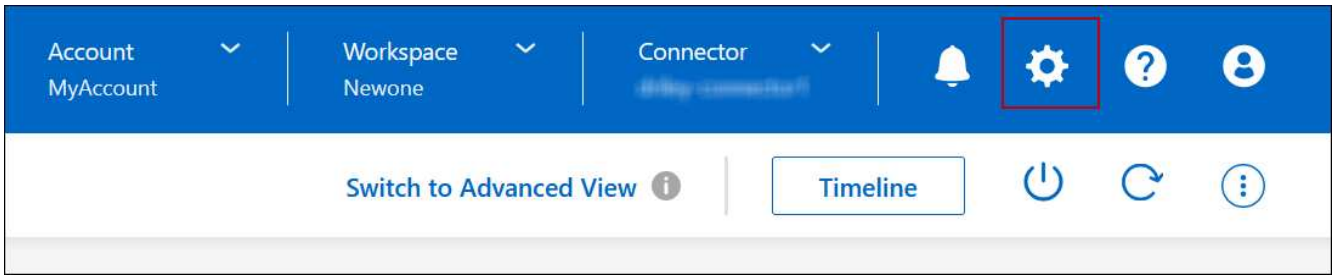
停用**Azure**私有連結、改用服務端點

如果貴企業需要、您可以變更BlueXP中的設定、使Cloud Volumes ONTAP 其設定使用服務端點、而非Azure私有連結。變更此設定會套用Cloud Volumes ONTAP 至您所建立的新版資訊系統。服務端點僅在中受支援 "Azure區域配對" 連接器與Cloud Volumes ONTAP 胎心之間。

連接器應部署在Cloud Volumes ONTAP 其所管理的或所管理的各個系統所在的Azure區域 "Azure區域配對" 適用於整個系統。Cloud Volumes ONTAP

步驟

1. 在 BlueXP 主控台的右上角、按一下「設定」圖示、然後選取 * 「 Cloud Volumes ONTAP 設定 * 」 。



2. 在* Azure 下、按一下*使用**Azure Private Link**。
3. 取消選擇* Cloud Volumes ONTAP 在不同時使用*私有連結的情況下、連接到儲存帳戶*。
4. 按一下「 * 儲存 * 」 。

完成後

如果您停用Azure私有連結、且Connector使用Proxy伺服器、則必須啟用直接API流量。

"瞭解如何在Connector上啟用直接API流量"

使用**Azure**私有連結

在大多數情況下、您不需要做任何事、就能使用Cloud Volumes ONTAP 下列功能來設定Azure私有連結：BlueXP會為您管理Azure私有連結。但如果您使用現有的Azure私有DNS區域、則必須編輯組態檔。

自訂**DNS**的需求

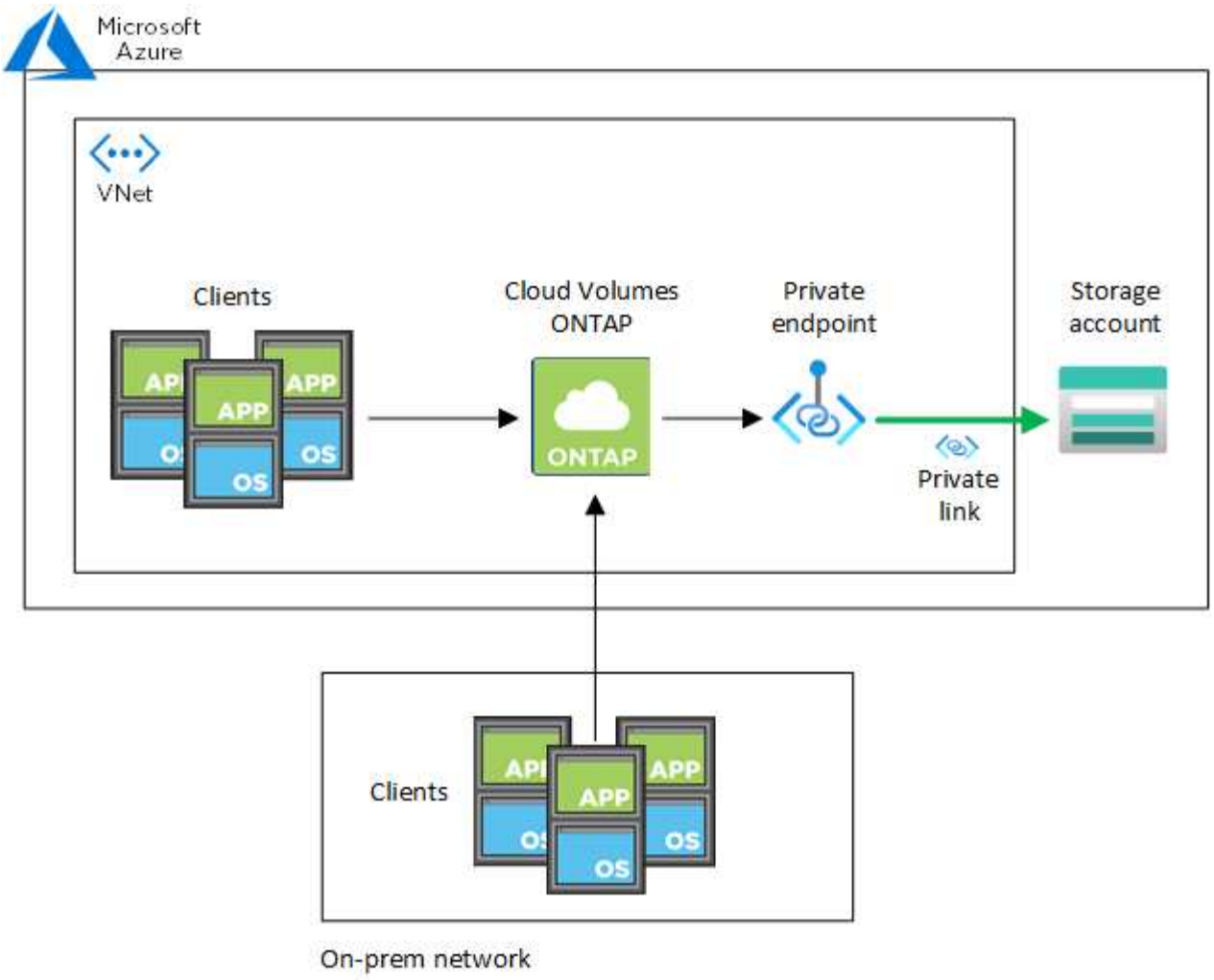
或者、如果您使用自訂DNS、則需要從自訂DNS伺服器建立條件轉寄站、以前往Azure私有DNS區域。若要深入瞭解、請參閱 "Azure關於使用DNS轉寄站的文件"。

私有連結連線的運作方式

當BlueXP在Cloud Volumes ONTAP Azure中部署時、它會在資源群組中建立一個私有端點。私有端點與Cloud Volumes ONTAP 用於實現功能不均的儲存帳戶相關聯。因此Cloud Volumes ONTAP 、存取資料可透過Microsoft主幹網路存取。

當用戶端與Cloud Volumes ONTAP S時 位於相同的vnet內、在連接VNets的對等網路內、或在使用私有VPN或ExpressRoute連線至vnet的內部部署網路中、用戶端存取會透過私有連結進行。

以下範例顯示用戶端透過私有連結從同一個Vnet存取、以及從內部網路存取具有私有VPN或ExpressRoute連線的權限。



如果連接器和Cloud Volumes ONTAP 物件系統部署在不同的VNets中、則您必須在部署連接器的vnet和Cloud Volumes ONTAP 部署了該系統的vnet之間設定vnet對等關係。

提供您**Azure**私有**DNS**的詳細資料給**BlueXP**

如果您使用 "Azure 私有 DNS"然後您需要修改每個 Connector 上的組態檔。否則、BlueXP無法在Cloud Volumes ONTAP 支援的儲存帳戶之間啟用Azure Private Link連線。

請注意、 DNS 名稱必須符合 Azure DNS 命名需求 "如 Azure 文件所示"。

步驟

1. SSH 連接至 Connector 主機並登入。
2. 瀏覽至下列目錄：/opp/application/netapp/cloudmanager/docker_occm/data
3. 使用下列關鍵字-值配對新增「user-Private - DNS"區域設定參數、以編輯app.conf：

```
"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
}
```

此參數應與「system-id」輸入的層級相同、如下所示：

```
"system-id" : "<system ID>",
"user-private-dns-zone-settings" : {
```

請注意、只有當私有DNS區域的訂閱與Connector不同時、才需要訂購關鍵字。

4. 儲存檔案並登出 Connector 。

   不需要重新開機。

在故障時啟用復原功能

如果BlueXP無法建立Azure私有連結做為特定行動的一部分、則在不使用Azure私有連結連線的情況下完成此動作。當建立新的工作環境（單一節點或HA配對）、或是HA配對上發生下列動作時、就會發生這種情況：建立新的Aggregate、新增磁碟至現有的Aggregate、或是在超過32 TiB時建立新的儲存帳戶。

如果BlueXP無法建立Azure私有連結、您可以啟用復原功能來變更此預設行為。這有助於確保您完全符合貴公司的安全法規。

如果您啟用復原、則BlueXP會停止動作、並回溯作為行動一部分所建立的所有資源。

您可以透過API或更新app.conf檔案來啟用復原功能。

*透過API*啟用復原功能

步驟

1. 請使用「PUT /occm/config（放入/occm/config）API呼叫與下列要求內容：

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

更新**app.conf**以啟用復原功能

步驟

1. SSH 連接至 Connector 主機並登入。
2. 瀏覽至下列目錄：/opp/application/netapp/cloudmanager/docker_occm/data
3. 新增下列參數和值以編輯 app.conf ：

```
 "rollback-on-private-link-failure": true
```
. 儲存檔案並登出 Connector 。

不需要重新開機。

正在移動資源群組

支援Azure資源群組移動、但工作流程僅發生在Azure主控台。Cloud Volumes ONTAP

您可以在同一Azure訂閱中、將工作環境從一個資源群組移至Azure中的其他資源群組。不支援在不同Azure訂閱之間移動資源群組。

步驟

1. 從* Canvas*移除工作環境。

   若要瞭解如何移除工作環境、請參閱 "移除 Cloud Volumes ONTAP 運作環境"。

2. 在Azure主控台執行資源群組搬移。

   若要完成移動、請參閱 "將資源移至新的資源群組或訂閱Microsoft Azure文件中"。

3. 在* Canvas*中、探索工作環境。
4. 在工作環境的資訊中尋找新的資源群組。

結果

工作環境及其資源（VM、磁碟、儲存帳戶、網路介面、快照）位於新的資源群組中。

分離 **Azure** 中的 **SnapMirror** 流量

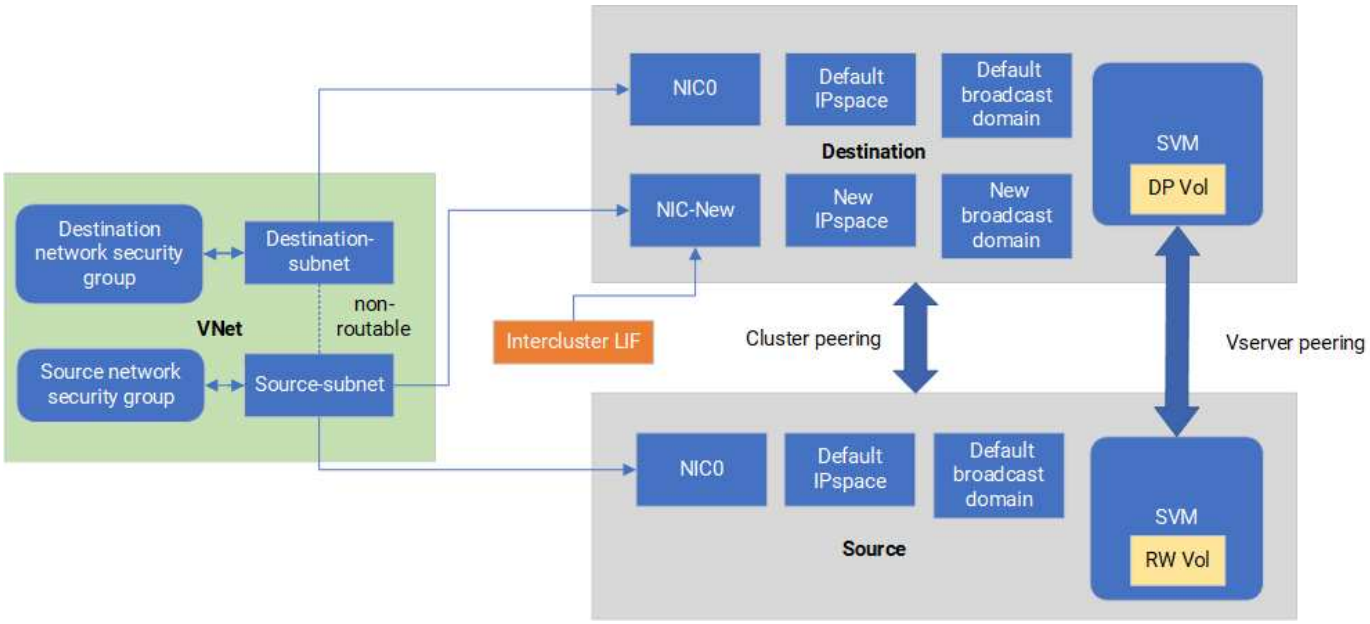
有了 Azure 中的 Cloud Volumes ONTAP 、您可以將 SnapMirror 複寫流量與資料和管理流量區隔。若要將 SnapMirror 複寫流量與資料流量區隔、您需要新增網路介面卡（ NIC ）、相關的叢集間 LIF 和不可路由的子網路。

關於 **Azure** 中的 **SnapMirror** 流量分隔

根據預設、 BlueXP 會在相同子網路上的 Cloud Volumes ONTAP 部署中設定所有 NIC 和生命。在此類組態中、 SnapMirror 複寫流量和資料與管理流量使用相同的子網路。分離 SnapMirror 流量會利用無法路由傳送至現有子網路的額外子網路、用於資料和管理流量。

圖 **1.**

下圖顯示 SnapMirror 複寫流量與其他 NIC 、相關的叢集間 LIF 和單一節點部署中不可路由的子網路之間的分隔。HA 配對部署稍有不同。



開始之前

請檢閱下列考量事項：

- 您只能將單一 NIC 新增至 Cloud Volumes ONTAP 單一節點或 HA 配對部署（ VM 執行個體）、以進行 SnapMirror 流量分隔。
- 若要新增 NIC 、您部署的 VM 執行個體類型必須有未使用的 NIC 。
- 來源叢集和目的地叢集應可存取相同的虛擬網路（ vnet ）。目的地叢集是 Azure 中的 Cloud Volumes ONTAP 系統。來源叢集可以是 Azure 中的 Cloud Volumes ONTAP 系統、也可以是 ONTAP 系統。

步驟 **1** ：建立額外的 **NIC** 並附加至目的地 **VM**

本節提供如何建立其他 NIC 並將其附加至目的地 VM 的說明。目的地 VM 是 Azure 中 Cloud Volumes ONTAP 的單一節點或 HA 配對系統、您可以在其中設定額外的 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 環境來停止節點。
   a. 停止節點。

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

b. 取消分配節點。

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-vm>
```

4. 設定網路安全性群組規則、使兩個子網路（來源叢集子網路和目的地叢集子網路）無法彼此路由。
   a. 在目的地 VM 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. 在目的 VM 上建立新的 NIC 、並提供來源叢集子網路的子網路 ID 。在此輸入新 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. 儲存私有 IP 位址。此 IP 位址 <new_added_nic_primary_addr> 用於在中建立叢集間 LIF 廣播網域、新 NIC 的叢集間 LIF。
5. 將新的 NIC 連接至 VM 。

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics <dest_node-vm-nic-new>
```

6. 啟動 VM （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 新的）存在且已啟用加速網路連線。

```
az network nic list --resource-group azure-59806175-60147103-azure-rg --query "[].{NIC: name, VM: virtualMachine.id}"
```

對於 HA 配對部署、請針對合作夥伴節點重複這些步驟。

步驟 2 ：為新 NIC 建立新的 IPspace 、廣播網域和叢集間 LIF

叢集間生命體的獨立 IPspace 可在叢集之間進行複寫的網路功能之間提供邏輯分隔。

請使用 ONTAP CLI 執行下列步驟。

步驟

1. 建立新的 IPspace （ new_IPSpace ）。

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. 在新的 IPspace （ new_IPSpace ）上建立廣播網域、然後新增 NIC 新連接埠。

```
dest::> network port show
```

3. 對於單節點系統、新增的連接埠為 *e0b* 。對於具有託管磁碟的 HA 配對部署、新增的連接埠為 *e0d* 。對於具有頁面 Blobs 的 HA 配對部署、新增的連接埠為 *e0e* 。使用節點名稱而非 VM 名稱。執行即可找到節點名稱 `node show`。

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. 在新的廣播網域（ new_bd ）和新的 NIC （ NIC 新）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. 驗證新叢集間 LIF 的建立。

```
dest::> net int show
```

對於 HA 配對部署、請針對合作夥伴節點重複這些步驟。

步驟 3 ：驗證來源和目的地系統之間的叢集對等關係

本節提供如何驗證來源和目的地系統之間對等關係的指示。

請使用 ONTAP CLI 執行下列步驟。

步驟

1. 確認目的地叢集的叢集間 LIF 可以 ping 通來源叢集的叢集間 LIF 。由於目的地叢集執行此命令、因此目的

地 IP 位址是來源上的叢集間 LIF IP 位址。

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
-destination <10.161.189.6>
```

2. 確認來源叢集的叢集間 LIF 可以 ping 通目的地叢集的叢集間 LIF 。目的地是在目的地上建立的新 NIC 的 IP 位址。

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
<10.161.189.18>
```

對於 HA 配對部署、請針對合作夥伴節點重複這些步驟。

步驟 4 ：在來源與目的地系統之間建立 SVM 對等關係

本節提供如何在來源與目的地系統之間建立 SVM 對等關係的指示。

請使用 ONTAP CLI 執行下列步驟。

步驟

1. 使用來源叢集間 LIF IP 位址做為、在目的地上建立叢集對等關係 `-peer-addrs`。對於 HA 配對、請將兩個節點的來源叢集間 LIF IP 位址列為 `-peer-addrs`。

```
dest::> cluster peer create -peer-addrs <10.161.189.6> -ipspace
<new_ipspace>
```

2. 輸入並確認通行密碼。
3. 使用目的地叢集 LIF IP 位址做為、在來源上建立叢集對等關係 `peer-addrs`。對於 HA 配對、請將兩個節點的目的地叢集間 LIF IP 位址列為 `-peer-addrs`。

```
src::> cluster peer create -peer-addrs <10.161.189.18>
```

4. 輸入並確認通行密碼。
5. 檢查叢集是否已對等連接。

```
src::> cluster peer show
```

在可用度欄位中成功的對等顯示 * 可用 * 。

6. 在目的地上建立 SVM 對等關係。來源和目的地 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 對等關係。

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. 請檢查 SVM 是否有問題。

```
dest::> vserver peer show
```

對等狀態顯示 **peered** 並顯示對等應用程式 **snapmirror**。

步驟 5 ：在來源與目的地系統之間建立 SnapMirror 複寫關係

本節提供如何在來源與目的地系統之間建立 SnapMirror 複寫關係的指示。

若要移動現有的 SnapMirror 複寫關係、您必須先中斷現有的 SnapMirror 複寫關係、然後再建立新的 SnapMirror 複寫關係。

請使用 ONTAP CLI 執行下列步驟。

步驟

1. 在目的地 SVM 上建立資料保護的 Volume 。

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. 在目的地上建立 SnapMirror 複寫關係、其中包括 SnapMirror 原則和複寫排程。

```
dest::> snapmirror create -source-path src_svm:src_vol  -destination
-path  dest_svm:new_dest_vol -vserver dest_svm -policy
MirrorAllSnapshots -schedule 5min
```

3. 初始化目的地上的 SnapMirror 複寫關係。

```
dest::> snapmirror initialize -destination-path  <dest_svm:new_dest_vol>
```

4. 在 ONTAP CLI 中、執行下列命令以驗證 SnapMirror 關係狀態：

```
dest::> snapmirror show
```

關係狀態為 `Snapmirrored` 而關係的健全狀況就是 `true`。

5. 可選：在 ONTAP CLI 中，運行以下命令查看 SnapMirror 關係的操作歷史記錄。

```
dest::> snapmirror show-history
```

或者、您可以掛載來源和目的地磁碟區、將檔案寫入來源磁碟區、並驗證磁碟區是否正在複寫到目的地。

Google Cloud管理

變更Google Cloud機器類型Cloud Volumes ONTAP 以供使用

在Cloud Volumes ONTAP Google Cloud上啟動時、您可以從多種機器類型中進行選擇。如果判斷執行個體的大小過小或過大、您可以隨時變更執行個體或機器類型。

關於這項工作

- 自動恢復必須在 Cloud Volumes ONTAP 一個「無法恢復的 HA 配對」上啟用（這是預設設定）。如果沒有、則作業將會失敗。

  "供應說明文件：設定自動恢復的命令 ONTAP"

- 變更機器類型可能會影響Google Cloud服務費用。
- 此作業會重新啟動 Cloud Volumes ONTAP 。

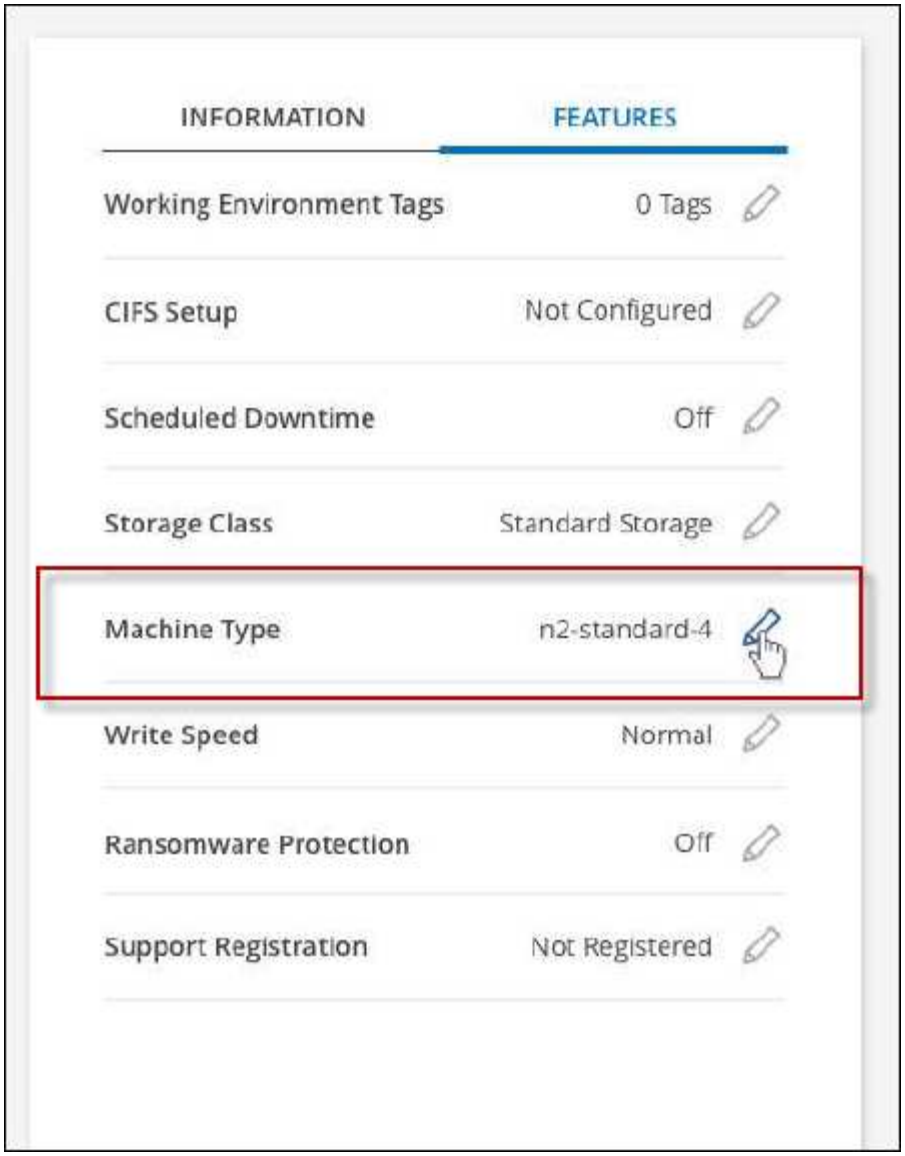
  對於單一節點系統、 I/O 會中斷。

  對於 HA 配對、變更不中斷營運。HA 配對可繼續提供資料。

> BlueXP會主動啟動接管並等待回饋、一次只能正常變更一個節點。NetApp 的 QA 團隊在這段過程中測試了寫入和讀取檔案的能力、並未發現客戶端有任何問題。隨著連線變更、我們確實看到 I/O 層級的重試次數、但應用程式層卻取代了 NFS/CIFS 連線的這些短「重新連線」。

步驟

1. 在 Canvas 頁面上、選取工作環境。
2. 在「概述」索引標籤上、按一下「功能」面板、然後按一下「 * 機器類型 * 」旁邊的鉛筆圖示。



a. 如果您使用的是節點型 PAYGO 授權、您可以選擇不同的授權和機器類型、方法是按一下 * 授權類型 * 旁的鉛筆圖示。

3. 選擇機器類型、勾選核取方塊以確認您瞭解變更的影響、然後按一下 * 變更 * 。

結果

以新組態重新開機。 Cloud Volumes ONTAP

使用進階檢視來管理Cloud Volumes ONTAP

如果您需要執行Cloud Volumes ONTAP 進階的支援管理功能、可以使用ONTAP 支援ONTAP 此功能的支援功能、這個功能是隨附於一個系統的管理介面。我們已將System Manager介面直接納入BlueXP、因此您不需要離開BlueXP進行進階管理。

功能

BlueXP的進階檢視可讓您存取其他管理功能：

- 進階儲存管理

  管理一致性群組、共用區、qtree、配額和儲存VM。

- 網路管理

  管理IPspace、網路介面、連接埠集和乙太網路連接埠。

- 活動與工作

  檢視事件記錄、系統警示、工作和稽核記錄。

- 進階資料保護

  保護儲存VM、LUN及一致性群組。

- 主機管理

  設定SAN啟動器群組和NFS用戶端。

支援的組態

透過System Manager進階管理功能、Cloud Volumes ONTAP 可在標準雲端區域中以支援使用支援的版本為0、10.0及更新版本。

不支援在GovCloud區域或沒有外傳網際網路存取的區域整合System Manager。

限制

下列功能不支援出現在System Manager介面中Cloud Volumes ONTAP 的部分功能：

- BlueXP 分層

  Cloud Volumes ONTAP 不支援 BlueXP 分層服務。建立磁碟區時、必須直接從BlueXP的標準檢視畫面設定將資料分層至物件儲存設備。

- 階層

  System Manager不支援集合管理（包括本機層級和雲端層）。您必須直接從BlueXP的「標準檢視」管理集合體。

- 韌體升級

  不支援Cloud Volumes ONTAP 從*叢集>設定*頁面自動更新韌體。

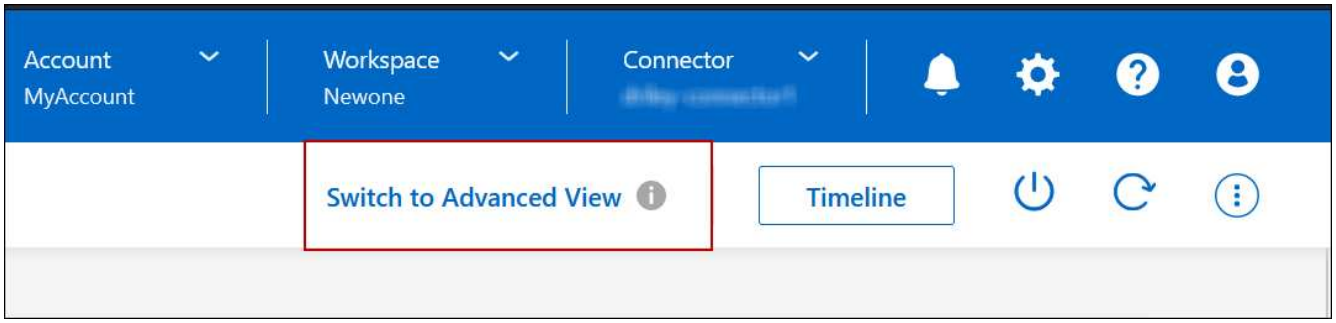
此外、不支援System Manager的角色型存取控制。

如何開始使用

開啟Cloud Volumes ONTAP 一個運作環境、然後按一下「進階檢視」選項。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按兩下Cloud Volumes ONTAP 某個系統的名稱。
3. 在右上角、按一下*切換至進階檢視*。



4. 如果出現確認訊息、請仔細閱讀、然後按一下*關閉*。
5. 使用System Manager來管理Cloud Volumes ONTAP 功能。
6. 如有需要、請按一下*切換至標準檢視*、透過BlueXP返回標準管理。

協助使用**System Manager**

如果您需要協助、請Cloud Volumes ONTAP 參閱《System Manager with》（搭配使用系統管理程式） "本文檔ONTAP" 以取得逐步指示。以下是幾個可能有幫助的連結：

- "Volume與LUN管理"
- "網路管理"
- "資料保護"

從**Cloud Volumes ONTAP CLI**管理

利用此功能、您可以執行所有的管理命令、這是進階工作或使用CLI時的最佳選擇。Cloud Volumes ONTAP您可以使用 Secure Shell （ SSH ）連線至 CLI 。

開始之前

您使用 SSH 連線 Cloud Volumes ONTAP 到 Suse 的主機必須有連至 Cloud Volumes ONTAP Suse 的網路連線。例如、您可能需要從雲端供應商網路中的跨接主機執行SSH。

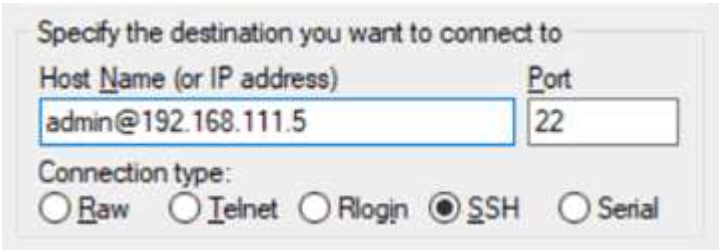
當部署於多個 AZs 時 Cloud Volumes ONTAP 、使用浮動 IP 位址進行叢集管理介面、這表示外部路由無法使用。您必須從屬於同一個路由網域的主機連線。

步驟

1. 在BlueXP中、識別叢集管理介面的IP位址：
   a. 從左側導覽功能表中、選取*儲存設備> Canvas*。
   b. 在「畫版」頁面上、選取 Cloud Volumes ONTAP 「系統」。
   c. 複製右窗格中顯示的叢集管理 IP 位址。
2. 使用 SSH 連線至使用管理帳戶的叢集管理介面 IP 位址。

◦ 範例 *

下圖顯示使用 Putty 的範例：



3. 在登入提示下、輸入 admin 帳戶的密碼。

◦ 範例 *

```
Password: ********
COT2::>
```

系統健全狀況與事件

驗**AutoSupport** 證此設定

可主動監控系統健全狀況、並傳送訊息給NetApp技術支援部門。AutoSupport根據預設、AutoSupport 每個節點上都會啟用支援功能、以便使用HTTPS傳輸傳輸傳輸協定將訊息傳送給技術支援。最好驗證AutoSupport 此資訊是否能傳送。

唯一必要的組態步驟是確保Cloud Volumes ONTAP 使用者能夠連線到傳出的網際網路。如需詳細資料、請參閱雲端供應商的網路需求。

需求**AutoSupport**

支援NetApp功能的支援節點需要外傳網際網路存取功能、此功能可主動監控系統健全狀況、並將訊息傳送給NetApp技術支援部門。Cloud Volumes ONTAP AutoSupport

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

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

如果傳出的網際網路連線無法傳送AutoSupport 功能性訊息、則BlueXP會自動將Cloud Volumes ONTAP 您的功能性更新系統設定為使用Connector做為Proxy伺服器。唯一的需求是確保連接器的安全性群組允許連接埠3128上的傳入連線。部署Connector之後、您需要開啟此連接埠。

如果您定義了Cloud Volumes ONTAP 嚴格的傳出規則以供支援、那麼Cloud Volumes ONTAP 您也必須確保支援透過連接埠3128建立_Outbound _連線的安全性群組。

在您確認可以存取傳出網際網路之後、您可以測試AutoSupport 以確保能夠傳送訊息。如需相關指示、請參閱 "

文件：設定檔ONTAP AutoSupport"。

疑難排解**AutoSupport** 您的**VMware**組態

如果傳出連線無法使用、且BlueXP無法將Cloud Volumes ONTAP 您的作業系統設定為使用Connector做為Proxy伺服器、您將會收到來自BlueXP的通知、標題為「<工作環境名稱>無法傳送AutoSupport 靜態訊息」。

您很可能因為網路問題而收到此訊息。

請依照下列步驟來解決此問題。

步驟

1. SSH到Cloud Volumes ONTAP 支援系統、以便從CLI管理系統。

   "瞭解如何從SSH到Cloud Volumes ONTAP 功能"。

2. 顯示AutoSupport 資訊子系統的詳細狀態：

   《不知詳情》AutoSupport

   回應應類似下列內容：

```
    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類別的狀態為「ok」、表示AutoSupport 已正確設定、並可傳送訊息。

3. 如果狀態不正常、請驗證每Cloud Volumes ONTAP 個節點的Proxy URL：

   《AutoSupport 鏈接：字段proxy-url'》

4. 如果Proxy URL參數是空的、請設定Cloud Volumes ONTAP 使用連接器做為Proxy：

   《AutoSupport 支援：modify -proxy-URL http://<connector Private IP>:3128》

5. 再次驗AutoSupport 證此狀態：

   《不知詳情》AutoSupport

6. 如果狀態仍然失敗、請驗證Cloud Volumes ONTAP 透過連接埠3128驗證顯示的是在連接埠之間與連接器之

間是否有連線。

7. 如果狀態ID在驗證是否有連線後仍失敗、請使用SSH連線至連接器。

   "深入瞭解連接至Linux VM for the Connector的相關資訊"

8. 請前往「/opt/sapplication/netapp/cloudmanager/dock_occm/data/`」

9. 開啟Proxy組態檔「shquid.conf」

   檔案的基本結構如下：

```
        http_port 3128
        acl localnet src 172.31.0.0/16
        acl azure_aws_metadata dst 169.254.169.254

        http_access allow localnet
        http_access deny azure_aws_metadata
        http_access allow localhost
        http_access deny all
```

   localnet src值是Cloud Volumes ONTAP 指整個過程中的CIDR。

10. 如果Cloud Volumes ONTAP 無法在檔案中指定的範圍內更新整個系統的CIDR區塊、請更新該值或新增下列項目：

    「ACL cv網 卡來源<CIDR >」

    如果您新增此新項目、請別忘了新增允許項目：

    "http存取允許cvonet"

    範例如下：

```
        http_port 3128
        acl localnet src 172.31.0.0/16
        acl cvonet src 172.33.0.0/16
        acl azure_aws_metadata dst 169.254.169.254

        http_access allow localnet
        http_access allow cvonet
        http_access deny azure_aws_metadata
        http_access allow localhost
        http_access deny all
```

11. 編輯組態檔之後、請重新啟動Proxy容器作為Sudo：

    「Docker重新啟動sid」

12. 返回Cloud Volumes ONTAP 到還原CLI、確認Cloud Volumes ONTAP 功能不只能傳送AutoSupport 功能不實的訊息：

    《不知詳情》AutoSupport

設定EMS

事件管理系統（EMS）會收集ONTAP 並顯示有關發生在故障系統上的事件資訊。若要接收事件通知、您可以針對特定事件嚴重性設定事件目的地（電子郵件地址、 SNMP 設陷主機或 syslog 伺服器）和事件路由。

您可以使用 CLI 設定 EMS 。如需相關指示、請參閱 "文件：EMS組態總覽ONTAP"。

概念

提供授權Cloud Volumes ONTAP

有多種授權選項可供Cloud Volumes ONTAP 選擇。每個選項都能讓您選擇符合需求的消費模式。

授權總覽

下列授權選項適用於新客戶。

容量型授權
: 根據Cloud Volumes ONTAP 資源配置的容量、在NetApp帳戶中支付多個支援系統的費用。包括購買附加雲端資料服務的能力。

Keystone訂閱
: 以隨成長付費訂閱為基礎的服務、為HA配對提供無縫的混合雲體驗。

先前的個別節點授權模式仍適用於已購買授權或正在訂閱市場的現有客戶。

以下各節提供這些選項的詳細資訊。

若未取得授權、則無法使用授權功能。

容量型授權

容量型授權套件可讓您針對Cloud Volumes ONTAP 每TiB的容量付費。授權與您的NetApp帳戶相關聯、只要授權有足夠的容量可用、您就能根據授權向多個系統收取費用。

例如、您可以購買單一20 TiB授權、部署四Cloud Volumes ONTAP 個作業系統、然後將5個TiB磁碟區分配給每個系統、總共20 TiB。容量可用於Cloud Volumes ONTAP 該帳戶中部署的每個作業系統上的磁碟區。

容量型授權的形式為_package_。當您部署Cloud Volumes ONTAP 一套解決方案時、您可以根據業務需求、從多個授權套件中進行選擇。

雖然 BlueXP 管理的產品和服務的實際使用量和計量都是以 GiB 和 TiB 計算、但是會交替使用「 GB/GiB 」和「 TB/TiB 」這兩個詞彙。這會反映在 Cloud Marketplace 清單、價格報價、上市說明及其他支援文件中。

套件

下列容量型套件可供Cloud Volumes ONTAP 使用。

如需下列容量型套件支援的 VM 類型清單、請參閱：

- "Azure支援的組態"
- "Google Cloud支援的組態"

Freemium

NetApp Cloud Volumes ONTAP 免費提供所有的支援功能（仍需支付雲端供應商費用）。

- 不需要授權或合約。
- 不包括NetApp的支援。
- 每Cloud Volumes ONTAP 個系統的資源配置容量上限為500 GiB。
- 您可以在Cloud Volumes ONTAP 任何雲端供應商中、使用最多10個包含每個NetApp帳戶的Freemium產品的NetApp系統。
- 如果Cloud Volumes ONTAP 供應的資料系統容量超過500 GiB、則BlueXP會將系統轉換成Essentials套件。

  一旦系統轉換成Essentials套件 最低收費 適用。

  任何其他配置容量低於500 GiB的系統、都會留在Freemium上（只要使用Freemium產品進行部署）。

最佳化

單獨支付已配置的容量和I/O作業費用。

- 單一節點或HA Cloud Volumes ONTAP
- 充電是以兩個成本元件為基礎：儲存與使用（ I/O ）。

  與資料複寫（ SnapMirror ）、備份（ SnapVault ）或 NDMP 相關的 I/O 將不會收取費用。

- 您可在Azure Marketplace以隨用隨付方案或年度合約形式取得
- 可在Google Cloud Marketplace以隨用隨付方案或年度合約形式提供
- 以額外成本附加任何NetApp的雲端資料服務

基礎知識

依容量付費Cloud Volumes ONTAP 、以供各種不同組態使用。

- 選擇Cloud Volumes ONTAP 您的需求組態：
  - 單一節點或HA系統
  - 用於災難恢復（DR）的檔案與區塊儲存或次要資料
- 以額外成本附加任何NetApp的雲端資料服務

專業人員

以容量支付Cloud Volumes ONTAP 任何類型的不受限制的還原組態。

- 提供Cloud Volumes ONTAP 任何功能組態的授權

  單一節點或HA、以相同速率為主要和次要磁碟區充電

- 包括使用 BlueXP 備份與還原的不限數量的 Volume 備份、但僅適用於使用專業版套件的 Cloud Volumes ONTAP 系統。

BlueXP 備份與還原需要 PAYGO 訂閱、但使用此服務不會產生任何費用。如需設定 BlueXP 備份與還原授權的詳細資訊、請參閱 "設定 BlueXP 備份與還原的授權"。

- 以額外成本附加任何NetApp的雲端資料服務

邊際快取

提供Cloud Volumes Edge Cache授權。

- 與Professional套件相同的功能、可為分散式企業提供營運不中斷和資料保護
- 智慧型邊緣快取功能、可透過每個位置佔用空間較小的Windows VM進行快取
- 每購買3個Tib容量、就有一個邊緣節點
- 您可在Azure Marketplace以隨用隨付方案或年度合約形式取得
- 可在Google Cloud Marketplace以隨用隨付方案或年度合約形式提供

"深入瞭解Cloud Volumes Edge Cache如何協助您的企業發展"

消費模式

下列消費模式提供容量型授權套件：

- * BYOL*：向NetApp購買的授權、可用於在Cloud Volumes ONTAP 任何雲端供應商中部署

+請注意、最佳化和邊緣快取套件無法搭配BYOL使用。

- * PAYGO*：每小時向雲端供應商的市場訂購一次。
- 年度：雲端供應商市場的年度合約。

請注意下列事項：

- 如果您向NetApp（BYOL）購買授權、也必須向雲端供應商的市場訂閱PAYGO產品。

  您的授權一律會先收取費用、但在下列情況下、您將會從市場的每小時費率中收取費用：

  - 如果您超過授權容量
  - 如果授權期限已到期
- 如果您有市場的年度合約、Cloud Volumes ONTAP 您所部署的_all_系統將根據該合約付費。您無法與BYOL混搭一年一度的市場合約。
- 中國地區僅支援具有BYOL的單一節點系統。

變更套件

部署完成後、您可以變更Cloud Volumes ONTAP 使用容量型授權的一套功能、以利執行一套功能。例如、如果您部署Cloud Volumes ONTAP 的是含有Essentials套件的功能完善的系統、則當您的業務需求改變時、可以將其變更為Professional套件。

"瞭解如何變更充電方法"。

定價

如需定價的詳細資訊、請前往 "NetApp BlueXP網站"。

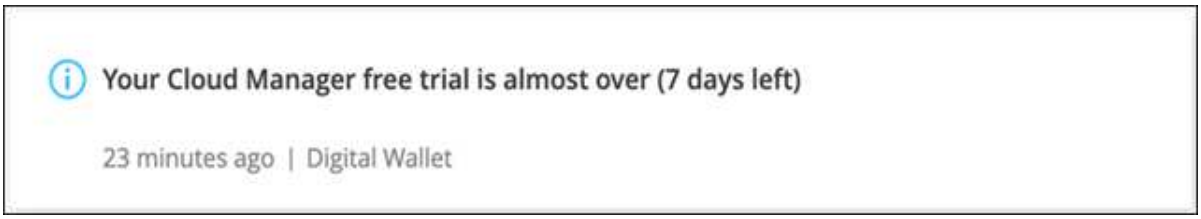
免費試用

您可以在雲端供應商的市場中、透過隨用隨付訂閱取得30天的免費試用版。免費試用包括 Cloud Volumes ONTAP 和 BlueXP 備份與還原。試用版會在您訂閱市場上的產品項目時開始。

沒有執行個體或容量限制。您可以任意部署Cloud Volumes ONTAP 多個不需付費的功能、並視需要配置多餘的容量、30天內即可免費部署。免費試用版會在30天後自動轉換為付費的每小時訂閱。

雖然不收取Cloud Volumes ONTAP 每小時的軟體授權費用、但您的雲端供應商仍需支付基礎架構費用。

您將會在BlueXP中收到一則通知、告知免費試用開始、剩餘7天、以及剩餘1天。例如：



支援的組態

以容量為基礎的授權套件可搭配Cloud Volumes ONTAP 使用於NetApp 9.7及更新版本。

容量限制

有了這種授權模式、每Cloud Volumes ONTAP 個個別的支援系統都能透過磁碟和分層到物件儲存設備、支援最多2 PIB的容量。

授權本身並無最大容量限制。

最大系統數

透過容量型授權、Cloud Volumes ONTAP 每個NetApp帳戶最多可有20個不限數量的不二元系統。_system_是Cloud Volumes ONTAP 一個EsireHA配對、Cloud Volumes ONTAP 一個僅供支援的節點系統、或是您所建立的任何其他儲存VM。預設的儲存VM不會計入限制。此限制適用於所有授權模式。

例如、假設您有三種工作環境：

- 單一節點Cloud Volumes ONTAP 的不完整系統、只需一個儲存VM（這是部署Cloud Volumes ONTAP 時建立的預設儲存VM）

  這種工作環境是單一系統的重要關鍵。

- 單一節點Cloud Volumes ONTAP 的不完整系統、含兩個儲存VM（預設儲存VM、加上您所建立的一個額外儲存VM）

  此工作環境可視為兩個系統：一個用於單一節點系統、另一個用於額外的儲存VM。

- 包含三個儲存VM（預設儲存VM、加上您所建立的兩個額外儲存VM）的支援功能Cloud Volumes ONTAP

  此工作環境可算為三個系統：一個用於HA配對、兩個用於額外的儲存VM。

總共有六個系統。之後您的帳戶就有額外14個系統的空間。

如果您的大型部署需要20個以上的系統、請聯絡您的客戶代表或銷售團隊。

"深入瞭解NetApp客戶"。

充電注意事項

下列詳細資料可協助您瞭解充電方式如何搭配容量型授權使用。

最低收費

每個資料服務儲存VM至少要有一個主要（讀寫）磁碟區、至少需支付4 TiB的最低費用。如果主要磁碟區的總和低於4 TiB、則BlueXP會將4 TiB最低收費套用至該儲存VM。

如果您尚未配置任何磁碟區、則不適用最低收費。

對於 Essentials 套件、 4 TiB 最低容量費用不適用於僅包含次要（資料保護）磁碟區的儲存 VM 。例如、如果您的儲存虛擬機器擁有1個二線資料的TiB、則只需支付1個TiB的資料費用。對於所有其他非 Essentials 套件類型（最佳化、專業版和邊緣快取）、無論磁碟區類型為何、都會套用 4 TiB 的最低容量充電。

過度使用

如果您超過BYOL容量、或授權過期、系統會根據您的市場訂閱、按每小時費率收取超額費用。

Essentials套件

有了Essentials套件、您將依照部署類型（HA或單一節點）和Volume類型（主要或次要）收費。從高到低的定價順序如下： *Essentials Primary HA* 、 *Essentials Primary Single Node* 、 *Essentials Secondary HHA _* 和 *_Essentials Secondary Single Nod* 。或者、當您購買市場合約或接受私人優惠時、任何部署或 Volume 類型的容量費用都相同。

BYOL

如果您向 NetApp （ BYOL ）購買 Essentials 授權、且超過該部署和 Volume 類型的授權容量、則 BlueXP 數位錢包會因價格較高的 Essentials 授權（如果您有此授權且有可用容量）而收取超額費用。這是因為我們會先使用您已購買的可用容量作為預付容量、然後再針對市場進行充電。如果您的 BYOL 授權沒有可用容量、則超出的容量將以市場隨選時數費率（ PAYGO ）收取、並將增加每月帳單的成本。

以下是範例。假設您擁有下列Essentials套件授權：

- 500 TiB _Essentials二線HA授權、擁有500 TiB的承諾容量
- 500 TiB _Essentials單一節點_授權、僅擁有100 TiB的已認可容量

另有50個TiB配置在與次要Volume的HA配對上。BlueXP 數位錢包不需向 PAYGO 收取 50 TiB 費用、而是根據 *Essentials Single Node* 授權收取 50 TiB 超額費用。該授權的價格高於 _Essentials 次要 HHA 、但它是使用您已購買的授權、不會在您的每月帳單中增加成本。

在 BlueXP 數位錢包中、 50 TiB 將根據 *Essentials Single Nodon* 授權收費。

以下是另一個範例。假設您擁有下列Essentials套件授權：

- 500 TiB _Essentials二線HA授權、擁有500 TiB的承諾容量
- 500 TiB _Essentials單一節點_授權、僅擁有100 TiB的已認可容量

另有 100 TiB 是在具有主要磁碟區的 HA 配對上進行佈建。您購買的授權沒有 *Essentials* 主要 *HA* 承諾容量。*_Essentials* 主要 *HA* 授權的價格高於 *Essentials* 主要單一節點 _ 和 *_Essentials* 次要 *HA* 授權。

在此範例中、 BlueXP 數位錢包會以額外 100 TiB 的市場費率收取超額費用。超額費用會顯示在您的每月帳單上。

市場合約或私人優惠

如果您購買的 Essentials 授權屬於市場合約或私有方案的一部分、則 BYOL 邏輯將不適用、而且您必須擁有正確的使用授權類型。授權類型包括 Volume 類型（主要或次要）和部署類型（ HA 或單一節點）。

例如、假設您使用 Essentials 授權部署 Cloud Volumes ONTAP 執行個體。接著、您可以配置讀寫磁碟區（主要單一節點）和唯讀（次要單一節點）磁碟區。您的市場合約或私有方案必須包含 _Essentials 單一節點 _ 和 _Essentials 次要單一節點 _ 的容量、以涵蓋已配置的容量。任何不屬於您市場合約或私人優惠的資源配置容量、都會以隨選時數費率（ PAYGO ）收取費用、並將成本加到您的每月帳單中。

儲存**VM**

- 額外的資料服務儲存VM（SVM）無需額外授權成本、但每個資料服務SVM的最低容量費用為4 TiB。
- 災難恢復SVM是根據已配置的容量來收費的。

HA 配對

對於HA配對、您只需支付節點上已配置容量的費用。您不需支付同步鏡射至合作夥伴節點的資料費用。

FlexClone與**FlexCache** 功能

- FlexClone磁碟區所使用的容量不需付費。
- 來源FlexCache 和目的地的資料不只是主要資料、而且會根據已配置的空間進行收費。

如何開始使用

瞭解如何開始使用容量型授權：

- "在Cloud Volumes ONTAP AWS中設定適用於此功能的授權"
- "在Cloud Volumes ONTAP Azure中設定for NetApp的授權"
- "在Cloud Volumes ONTAP Google Cloud中設定適用於此技術的授權"

Keystone訂閱

以隨成長付費訂閱為基礎的服務、可為偏好營運成本使用模式的使用者、提供無縫的混合雲體驗、以供預先支付資本支出或租賃之用。

充電是根據 Keystone 訂閱中一或多個 Cloud Volumes ONTAP HA 配對的承諾容量大小而定。

系統會定期彙總每個 Volume 的已配置容量、並將其與 Keystone 訂閱上的已認可容量進行比較、而任何超額資料都會在 Keystone 訂閱上以暴增方式收費。

"深入瞭解 NetApp Keystone"。

支援的組態

HA 配對支援 Keystone 訂閱。目前單一節點系統不支援此授權選項。

容量限制

每Cloud Volumes ONTAP 個個別的支援透過磁碟和分層至物件儲存設備、最多可支援2個PIB容量。

如何開始使用

瞭解如何開始使用 Keystone 訂閱：

- "在Cloud Volumes ONTAP AWS中設定適用於此功能的授權"
- "在Cloud Volumes ONTAP Azure中設定for NetApp的授權"
- "在Cloud Volumes ONTAP Google Cloud中設定適用於此技術的授權"

節點型授權

節點型授權是前一代的授權模式、可讓您依Cloud Volumes ONTAP 節點授權使用。此授權模式不適用於新客戶、也不提供免費試用。副節點充電已由上述的副容量充電方法取代。

現有客戶仍可使用節點型授權：

- 如果您擁有有效授權、BYOL僅適用於授權續約。
- 如果您有有效的市場訂閱、仍可透過該訂閱付費。

授權轉換

不Cloud Volumes ONTAP 支援將現有的支援系統轉換成其他授權方法。目前的三種授權方法是容量型授權、基礎概念訂閱和節點型授權。例如、您無法將系統從節點型授權轉換成容量型授權（反之亦然）。

如果您想要轉換至其他授權方法、可以購買授權、使用Cloud Volumes ONTAP 該授權部署新的一套作業系統、然後將資料複寫到新系統。

請注意、不支援將系統從PAYGO節點授權轉換成BYOL節點授權（反之亦然）。您需要部署新系統、然後將資料複寫到該系統。 "瞭解如何在PAYGO和BYOL之間切換"。

儲存設備

用戶端傳輸協定

支援iSCSI、NFS、SMB、NVMe-TCP及S3用戶端傳輸協定Cloud Volumes ONTAP 。

iSCSI

iSCSI是一種區塊傳輸協定、可在標準乙太網路上執行。大多數用戶端作業系統都提供軟體啟動器、可透過標準乙太網路連接埠執行。

NFS

NFS是UNIX和Linux系統的傳統檔案存取傳輸協定。用戶端可以ONTAP 使用NFSv3、NFSv4和NFSv4.1傳輸協定來存取S16 Volume中的檔案。您可以使用UNIX型權限、NTFS型權限或兩者的組合來控制檔案存取。

用戶端可以使用NFS和SMB傳輸協定存取相同的檔案。

中小企業

SMB是Windows系統的傳統檔案存取傳輸協定。用戶端可以ONTAP 使用SMB 2.0、SMB 2.1、SMB 3.0和SMB 3.1.1傳輸協定來存取位於支援區內的檔案。就像NFS一樣、支援各種權限樣式。

S3

支援S3作為橫向擴充儲存的選項Cloud Volumes ONTAP 。S3傳輸協定支援可讓您設定S3用戶端存取儲存VM（SVM）中儲存區段內的物件。

"瞭解S3多重傳輸協定的運作方式"。"瞭解如何在ONTAP 功能區中設定及管理S3物件儲存服務"。

NVMe TCP

如果您使用Cloud Volumes ONTAP 的是版本為9.12.1或更新版本、則支援適用於雲端供應商的NVMe-TCP。BlueXP不提供任何適用於NVMe TCP的管理功能。

如需透過ONTAP NVMe設定NVMe的詳細資訊、請參閱 "設定NVMe的儲存VM"。

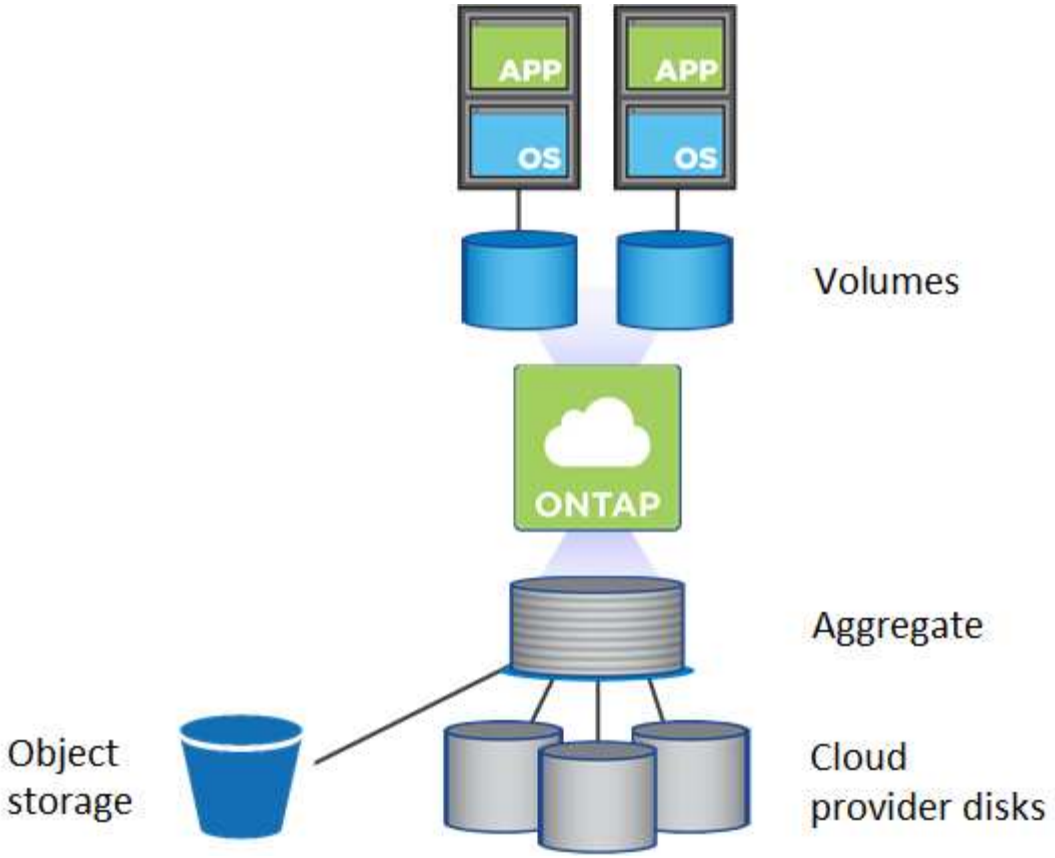
磁碟與集合體

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

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

總覽

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



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

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

AWS 儲存設備

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

EBS 儲存設備

在 AWS 中、 Aggregate 最多可包含 6 個大小相同的磁碟。但是如果您的組態支援Amazon EBS彈性Volume功能、則Aggregate最多可包含8個磁碟。 "深入瞭解彈性磁碟區的支援"。

磁碟大小上限為16 TiB。

基礎EBS磁碟類型可以是一般用途SSD（GP3或gp2）、已配置的IOPS SSD（IO1）或處理量最佳化HDD（ST1）。您可以將 EBS 磁碟與 Amazon S3 配對至 "將非作用中資料分層至低成本物件儲存設備"。

使用處理量最佳化的HDD（ST1）時、不建議將資料分層至物件儲存設備。

本機 **NVMe** 儲存設備

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

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

Azure 儲存設備

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

單一節點系統

單一節點系統可使用三種 Azure 託管磁碟：

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

  每種託管磁碟類型的磁碟大小上限為32 TiB。

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

HA 配對

HA配對使用兩種磁碟、以較高的成本為I/O密集型工作負載提供高效能：

- *Premium*頁面*Blobs*、磁碟大小上限為8 TiB
- *Managed disks*、磁碟大小上限為32 TiB

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

Google Cloud儲存設備

在Google Cloud中、Aggregate最多可包含6個大小相同的磁碟。磁碟大小上限為64 TiB。

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

- 相關連結 *
- "Google Cloud文件：儲存選項"
- "檢閱Cloud Volumes ONTAP Google Cloud中的功能不均儲存限制"

RAID 類型

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

熱備援

RAID0不支援使用熱備援磁碟來提供備援。

建立連接Cloud Volumes ONTAP 到某個實例的未使用磁碟（熱備援）是不必要的費用、可能會使您無法視需要配置額外的空間。因此不建議這麼做。

AWS中的彈性Volume

支援Amazon EBS Elastic Volumes功能搭配Cloud Volumes ONTAP 使用支援的不只能提供更好的效能和額外容量、還能讓BlueXP自動視需要增加基礎磁碟容量。

效益

- 動態磁碟成長

  在Cloud Volumes ONTAP 執行過程中、當執行了不同時磁碟仍連接時、BlueXP可以動態增加磁碟大小。

- 更優異的效能

  使用彈性磁碟區啟用的集合體最多可有八個磁碟、在兩個RAID群組中平均使用。此組態可提供更高的處理量和一致的效能。

- 較大的集合體

  支援八個磁碟、可提供最多128 TiB的集合體容量。對於未啟用「彈性磁碟區」功能的集合體、這些限制高於六個磁碟限制和96個TiB限制。

  請注意、系統總容量限制維持不變。

"深入瞭解AWS的彈性磁碟區"

支援的組態

Amazon EBS彈性磁碟區功能支援特定Cloud Volumes ONTAP 的版本、以及特定的EBS磁碟類型。

版本**Cloud Volumes ONTAP**

從Cloud Volumes ONTAP 9.11.0版或更新版本建立的_new _支援彈性磁碟區功能。此功能不支援Cloud Volumes ONTAP 在9.11.0之前部署的現有支援功能。

例如、如果您建立Cloud Volumes ONTAP 了一個版本不支援彈性磁碟區功能、之後又將該系統升級至版本9.11.0、則不支援彈性磁碟區功能。必須是使用9.11.0版或更新版本部署的新系統。

使用通用SSD（GP3）或已配置的IOPS SSD（IO1）時、會在Aggregate層級自動啟用彈性磁碟區功能。使用任何其他磁碟類型的Aggregate不支援彈性磁碟區功能。

必要的AWS權限

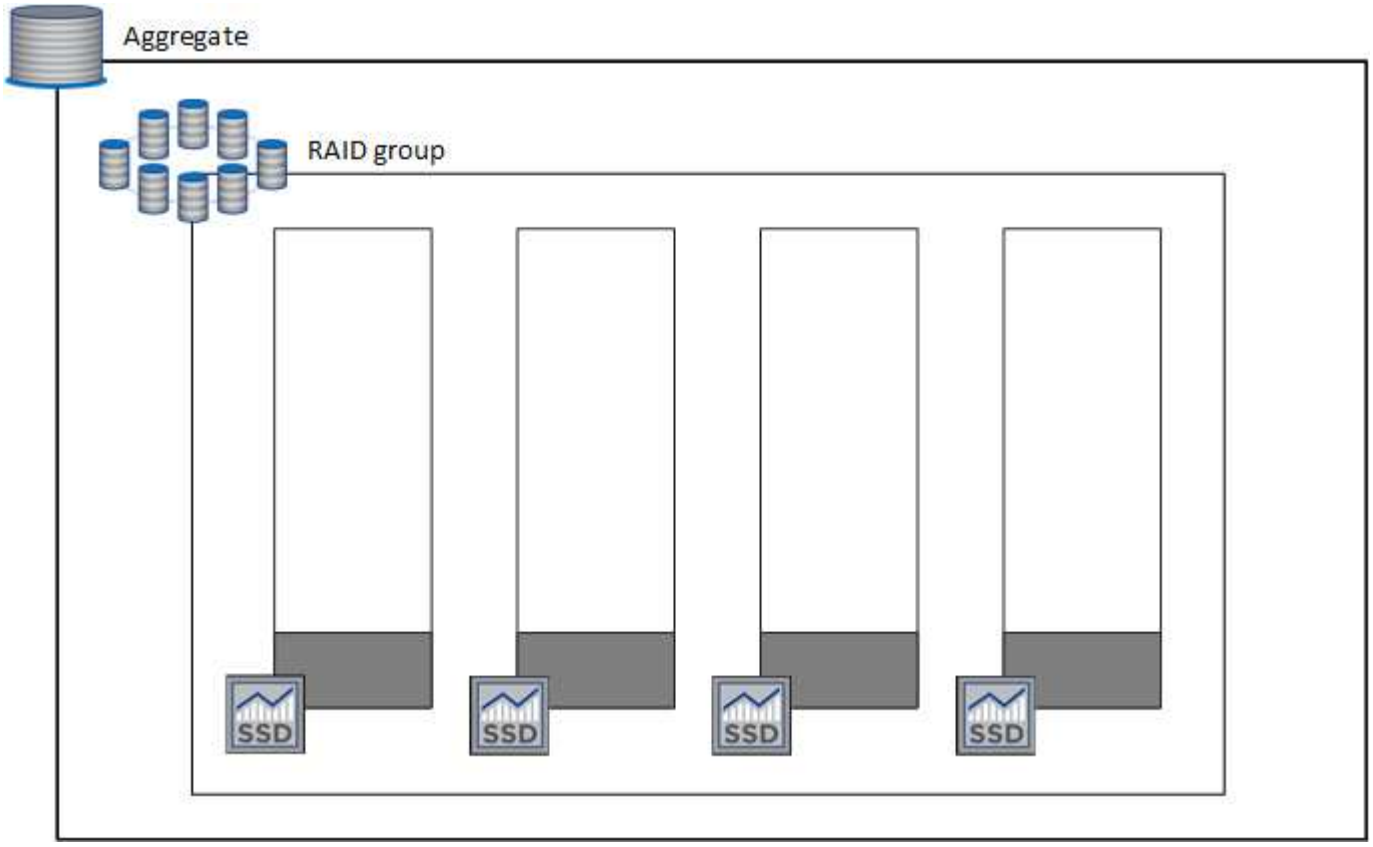
從3.9.19版本開始、連接器需要下列權限、才能啟用Cloud Volumes ONTAP 及管理資訊區上的「彈性Volume」功能：

- EC2：說明體積修改
- EC2：修改Volume

這些權限包含在中 "NetApp 提供的原則"

彈性磁碟區的支援運作方式

啟用「彈性磁碟區」功能的Aggregate由一或兩個RAID群組組成。每個RAID群組都有四個容量相同的磁碟。以下是10 TiB Aggregate的範例、每個集合體有四個2.5 TiB的磁碟：



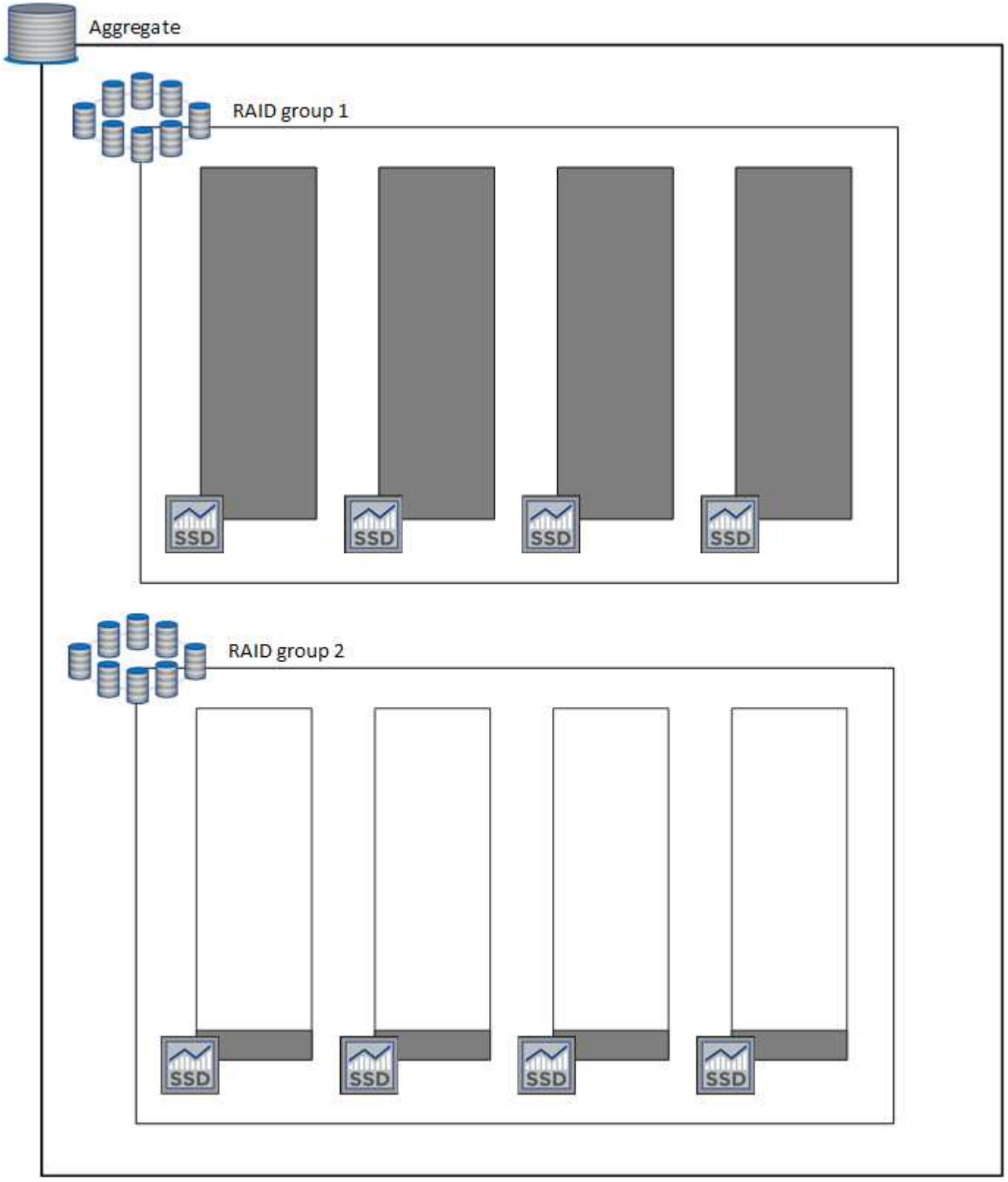
當BlueXP建立Aggregate時、它會從一個RAID群組開始。如果需要額外的容量、則BlueXP會將RAID群組中所有磁碟的容量增加相同數量、以擴充集合體。容量增加至少為256 GiB或集合體大小的10%。

例如、如果您有1個TiB Aggregate、則每個磁碟為250 GiB。集合體容量的10%為100 GiB。這低於256 GiB、因此集合體的大小會增加至少256 GiB（每個磁碟64 GiB）。

在Cloud Volumes ONTAP 執行更新時、由於磁碟仍在連接中、因此BlueXP可增加磁碟的大小。變更不中斷營運。

如果某個Aggregate達到64 TiB（或每個磁碟上有16 TiB）、則BlueXP會建立第二個RAID群組來增加容量。第二個RAID群組的運作方式與第一個相同：它有四個磁碟具有完全相同的容量、最多可擴充至64 TiB。這表示集合體的最大容量可達128 TiB。

以下是兩個RAID群組的集合體範例。第一個RAID群組已達到容量上限、第二個RAID群組中的磁碟則有足夠的可用空間。



建立Volume時會發生什麼事

如果您建立的磁碟區使用GP3或IO1磁碟、則BlueXP會在集合上建立磁碟區、如下所示：

- 如果現有GP3或IO1 Aggregate已啟用彈性磁碟區、則BlueXP會在該Aggregate上建立磁碟區。
- 如果有多個已啟用彈性磁碟區的GP3或IO1集合體、則BlueXP會在需要最少資源量的集合體上建立磁碟區。
- 如果系統只有GP3或IO1 Aggregate未啟用彈性磁碟區、則會在該Aggregate上建立磁碟區。

> 雖然這種情況不太可能發生、但可能發生兩種情況：
>
> - 從API建立Aggregate時、您明確停用了彈性磁碟區功能。
> - 您Cloud Volumes ONTAP 從使用者介面建立了一個新的功能區、在這種情況下、彈性磁碟區功能會在初始Aggregate上停用。檢閱 [限制] 請參閱下方以瞭解更多資訊。

- 如果現有的Aggregate沒有足夠的容量、則BlueXP會在啟用彈性磁碟區的情況下建立Aggregate、然後在新的Aggregate上建立該磁碟區。

  Aggregate的大小取決於所要求的磁碟區大小加上額外10%的容量。

容量管理模式

連接器的容量管理模式可與彈性磁碟區搭配運作、類似於它與其他類型的集合體搭配運作的方式：

- 啟用自動模式（這是預設設定）時、如果需要額外的容量、BlueXP會自動增加集合體的大小。
- 如果您將容量管理模式變更為手動、則BlueXP會要求您核准購買額外容量。

"深入瞭解容量管理模式"。

限制

增加Aggregate的大小最多需要6小時。在此期間、BlueXP無法要求該Aggregate的任何額外容量。

如何使用彈性磁碟區

您可以在BlueXP中使用彈性磁碟區、如下所示：

- 使用GP3或IO1磁碟時、請建立在初始Aggregate上啟用「彈性磁碟區」的新系統

  "瞭解如何建立Cloud Volumes ONTAP 一套功能完善的系統"

- 在已啟用「彈性磁碟區」的集合體上建立新的磁碟區

  如果您建立的磁碟區使用GP3或IO1磁碟、則BlueXP會自動在已啟用彈性磁碟區的集合體上建立磁碟區。如需詳細資料、請參閱 建立Volume時會發生什麼事。

  "瞭解如何建立Volume"。

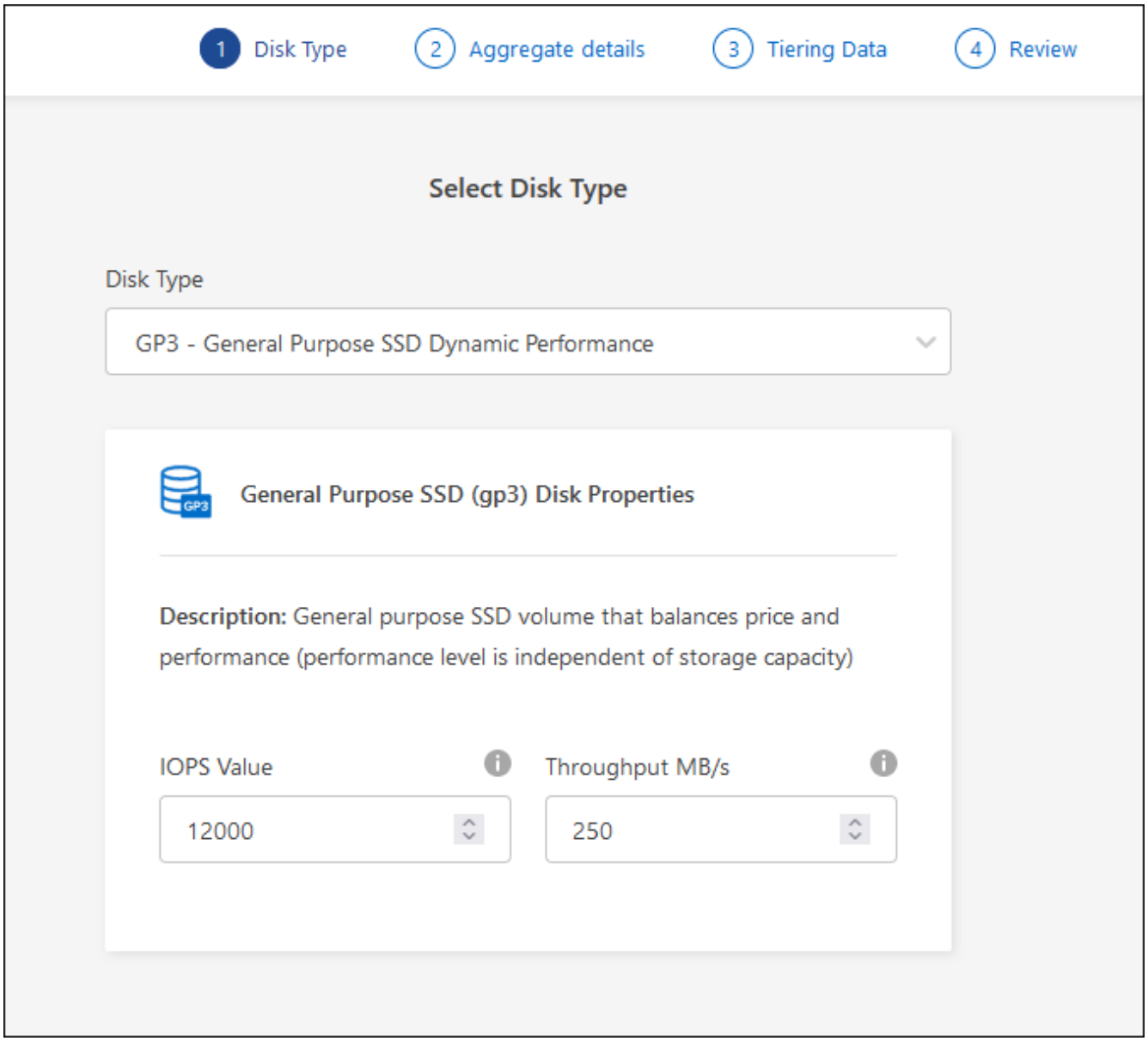
- 建立已啟用彈性磁碟區的新Aggregate

  只要Cloud Volumes ONTAP 使用GP3或IO1磁碟的新Aggregate系統是從9.11.0版或更新版本建立、就會在

新的Aggregate上自動啟用「彈性Volume」。

建立Aggregate時、BlueXP會提示您輸入Aggregate的容量大小。這與您選擇磁碟大小和磁碟數目的其他組態不同。

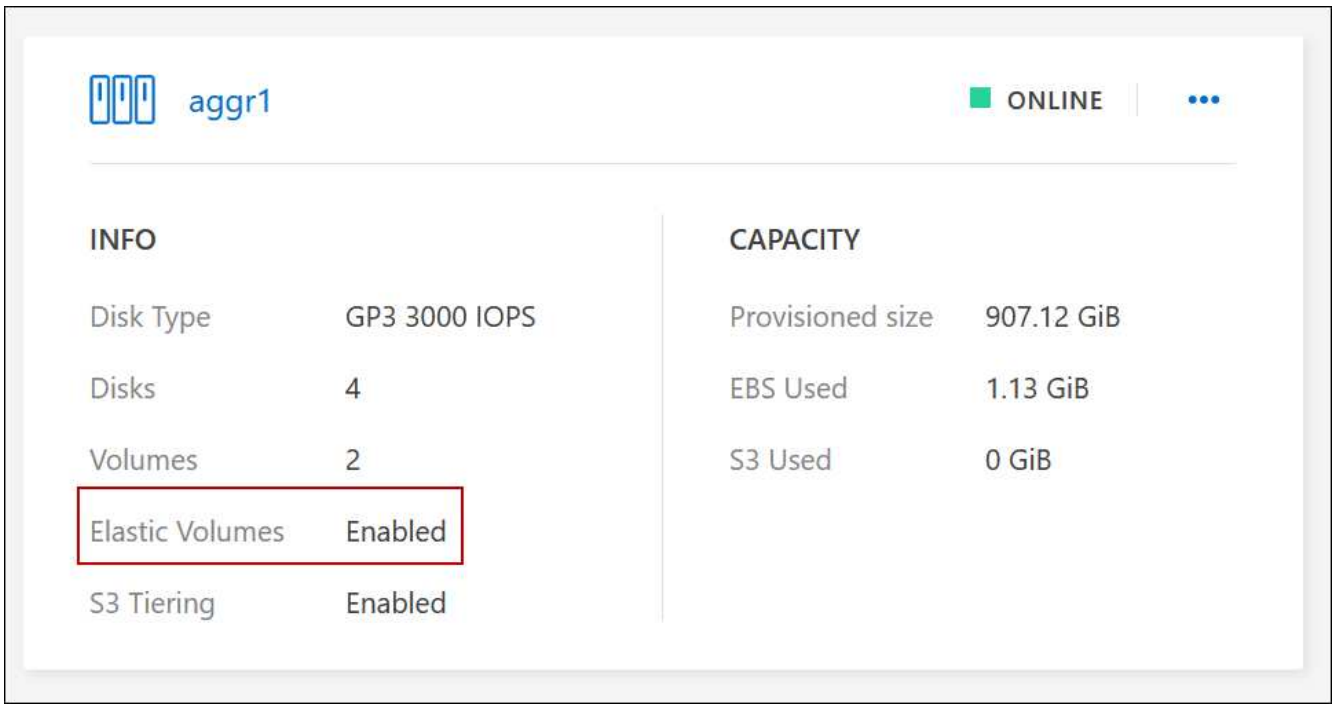
下列螢幕快照顯示由GP3磁碟組成的新Aggregate範例。



"瞭解如何建立Aggregate"。

- 識別已啟用彈性磁碟區的集合體

前往「進階配置」頁面時、您可以識別是否已在集合體上啟用「彈性磁碟區」功能。在下列範例中、 Aggr1 已啟用彈性 Volume 。



- 新增容量至Aggregate

  雖然BlueXP會視需要自動新增容量來集合體、但您可以自行手動增加容量。

  "瞭解如何增加Aggregate容量"。

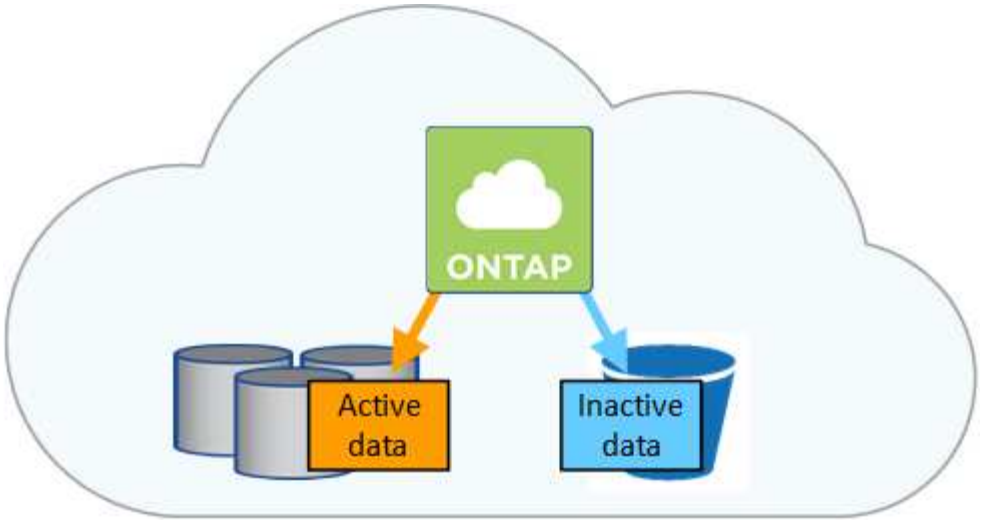
- 將資料複寫到已啟用彈性磁碟區的集合體

  如果目的地Cloud Volumes ONTAP 支援彈性Volume、則目的地Volume會放置在已啟用彈性Volume的集合體上（只要您選擇GP3或IO1磁碟）。

  "瞭解如何設定資料複寫"

資料分層總覽

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



資料分層是 FabricPool 以不同步技術為後盾。Cloud Volumes ONTAP 為所有 Cloud Volumes ONTAP 叢集提供資料分層功能、無需額外授權。當您啟用資料分層時、資料階層至物件儲存設備會產生費用。如需物件儲存成本的詳細資訊、請參閱雲端供應商的文件。

AWS 中的資料分層

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

效能層級

效能層可以是通用SSD（GP3或gp2）或已配置的IOPS SSD（IO1）。

使用處理量最佳化的HDD（ST1）時、不建議將資料分層至物件儲存設備。

容量層

這個系統會將非作用中的資料分層至單一S3儲存區。Cloud Volumes ONTAP

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

當BlueXP建立S3儲存區時、會使用下列預設設定：

- 儲存等級：標準
- 預設加密：停用
- 封鎖公開存取：封鎖所有公開存取
- 物件擁有權：啟用ACL
- 儲存區版本設定：已停用
- 物件鎖定：已停用

儲存類別

AWS 中階層式資料的預設儲存類別為 *Standard* 。Standard 適用於儲存在多個可用度區域中的常用資料。

如果您不打算存取非作用中資料、可以將儲存類別變更為下列其中一項、藉此降低儲存成本：*Intelligent Tiering*、*_One Zone In*頻率 存取、_Standard-in頻繁 存取_或_S3 Glacier即時擷取。當您變更儲存類別時、

非作用中的資料會從 Standard 儲存類別開始、並轉換至您選取的儲存類別（如果 30 天後仍未存取資料）。

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

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

資料分層的儲存類別是全系統範圍、並非每個磁碟區。

Azure 中的資料分層

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

效能層級

效能層可以是 SSD 或 HDD 。

容量層

將非作用中資料分層至單一Blob容器。Cloud Volumes ONTAP

BlueXP會建立一個新的儲存帳戶、並為每Cloud Volumes ONTAP 個運作環境建立一個容器。儲存帳戶名稱為隨機。並不會針對每個 Volume 建立不同的容器。

BlueXP會建立具有下列設定的儲存帳戶：

- 存取層：Hot
- 效能：標準
- 備援：本機備援儲存設備（LRS）
- 帳戶：StorageV2（通用v2）
- 需要安全傳輸以執行REST API作業：已啟用
- 儲存帳戶金鑰存取：已啟用
- 最低TLS版本：1.2版
- 基礎架構加密：已停用

儲存存取層

Azure 中階層式資料的預設儲存存取層為 *hot* 層。熱層是容量層中經常存取資料的理想選擇。

如果您不打算存取容量層中的非作用中資料、可以改用_cle__儲存層來降低儲存成本。當您將儲存層變更為冷卻時、非作用中的容量層資料會直接移至冷卻儲存層。

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

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

資料分層的儲存存取層是全系統的、並非每個磁碟區。

Google Cloud中的資料分層

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

效能層級

效能層可以是SSD持續磁碟、平衡持續磁碟或標準持續磁碟。

容量層

這個系統會將非作用中的資料分層至單一Google Cloud Storage儲存庫。Cloud Volumes ONTAP

BlueXP會為每個工作環境建立一個儲存區、並將其命名為「網路資源池」、「叢集唯一識別碼」。並不會針對每個 Volume 建立不同的儲存區。

當BlueXP建立儲存區時、會使用下列預設設定：

- 位置類型：地區
- 儲存等級：標準
- 公共存取：受物件ACL限制
- 存取控制：精細的
- 保護：無
- 資料加密：Google管理的金鑰

儲存類別

階層式資料的預設儲存類別為 *Standard Storage* 類別。如果資料不常存取、您可以改用 *Nearline Storage* 或 *Coldline Storage* 來降低儲存成本。當您變更儲存類別時、後續的非作用中資料會直接移至您選取的類別。

> ⓘ 當您變更儲存類別時、任何現有的非使用中資料都會維持預設的儲存類別。若要變更現有非使用中資料的儲存類別、您必須手動執行指定。

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

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

資料分層的儲存類別是全系統範圍、並非每個磁碟區。

資料分層和容量限制

如果您啟用資料分層、系統的容量限制會維持不變。此限制分佈於效能層和容量層。

Volume 分層原則

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

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

您可以將最小冷卻週期和預設Aggregate臨界值變更為50%（以下詳細資訊）。 "瞭解如何變更冷卻週期" 和 "瞭解如何變更臨界值"。

在建立或修改磁碟區時、您可以使用BlueXP從下列磁碟區分層原則中進行選擇：

僅適用於 **Snapshot**

當 Aggregate 達到 50% 容量後、 Cloud Volumes ONTAP 將不會與作用中檔案系統相關聯的 Snapshot 複本的 Cold 使用者資料分層至容量層。冷卻期約為 2 天。

如果讀取、容量層上的冷資料區塊會變熱、並移至效能層。

全部

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

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

自動

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

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

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

無

將磁碟區的資料保留在效能層中、避免移至容量層。

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

關閉 **Cloud Volumes ONTAP** 此功能會影響冷卻期間

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

- 自動： 31 天
- 僅 Snapshot ： 2 天

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

關閉動作時、會保留每個區塊的溫度、直到您重新啟動系統為止。Cloud Volumes ONTAP例如、當您關閉系統時、如果區塊的溫度為5、則當您重新開啟系統時、溫度仍為5。

設定資料分層

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

儲存管理

BlueXP提供Cloud Volumes ONTAP 簡化且進階的功能、可管理各種不支援的儲存設備。

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

儲存資源配置

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

簡化資源配置

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

建立磁碟區時、BlueXP會執行以下三項操作之一：

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

+在AWS中支援彈性磁碟區的集合體、BlueXP也會增加RAID群組中磁碟的大小。 "深入瞭解彈性磁碟區的支援"。

- 它會為新的 Aggregate 購買磁碟、並將該磁碟區放在該 Aggregate 上。

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

帳戶管理員可從 * 設定 * 頁面修改可用空間臨界值。

AWS 中集合體的磁碟大小選擇

當BlueXP在Cloud Volumes ONTAP AWS中建立新的Aggregate以供其使用時、它會隨著系統中的Aggregate數量增加、逐漸增加集合體中的磁碟大小。這樣做是為了確保您可以在系統達到AWS允許的最大資料磁碟數量之前、先使用系統的最大容量。

例如、BlueXP可能會選擇下列磁碟大小：

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

此行為不適用於支援Amazon EBS彈性磁碟區功能的集合體。啟用彈性磁碟區的集合體由一或兩個RAID群組組成。每個RAID群組都有四個容量相同的磁碟。 "深入瞭解彈性磁碟區的支援"。

您可以使用進階配置選項自行選擇磁碟大小。

進階分配

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

容量管理

客戶管理員可以選擇是否要由BlueXP通知您儲存容量決策、或是由BlueXP自動管理您的容量需求。

此行為由連接器上的_Capacity Management Mode_決定。容量管理模式會影響Cloud Volumes ONTAP 由該Connector管理的所有不完整系統。如果您有另一個Connector、則可以以不同的方式設定。

自動容量管理

容量管理模式預設為自動。在此模式中、 BlueXP 會每 15 分鐘檢查一次可用空間比率、以判斷可用空間比率是否低於指定的臨界值。如果需要更多容量、 BlueXP 會自動開始購買新磁碟、刪除未使用的磁碟集合（集合體）、視需要在集合體之間移動磁碟區、並嘗試防止磁碟故障。

下列範例說明此模式的運作方式：

- 如果某個Aggregate達到容量臨界值、而且有空間容納更多磁碟、則BlueXP會自動為該Aggregate購買新的磁碟、讓磁碟區持續成長。

如果 AWS 中支援彈性磁碟區的集合體、 BlueXP 也會增加 RAID 群組中磁碟的大小。 "深入瞭解彈性磁碟區的支援"。

+
* 如果集合體達到容量臨界值、而且無法支援任何其他磁碟、 BlueXP 會自動將該集合體的磁碟區移至具有可用容量的集合體、或移至新的集合體。

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

+
請注意、可用空間現在可在原始 Aggregate 上使用。現有磁碟區或新磁碟區可以使用該空間。在此案例中、空間無法傳回給雲端供應商。

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

利用自動容量管理來管理 **LUN**

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

手動容量管理

如果帳戶管理員將容量管理模式設為手動、則必須決定容量時、BlueXP會顯示必要行動訊息。自動模式中所述的相同範例適用於手動模式、但您必須接受這些動作。

深入瞭解

"瞭解如何修改容量管理模式"。

寫入速度

BlueXP可讓您針對大多數Cloud Volumes ONTAP 的功能組態、選擇一般或高速寫入速度。在您選擇寫入速度之前、您應該先瞭解一般與高設定之間的差異、以及使用高速寫入速度時的風險與建議。

正常寫入速度

當您選擇正常寫入速度時、資料會直接寫入磁碟。當資料直接寫入磁碟時、可降低發生非計畫性系統中斷或因非計畫性系統中斷而發生串聯故障的資料遺失可能性（僅限 HA 配對）。

正常寫入速度為預設選項。

高速寫入

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

發生非計畫性系統中斷時可能遺失的資料量、是最後兩個一致點的範圍。一致點是將緩衝資料寫入磁碟的行為。寫入日誌已滿或 10 秒後（以先到者為準）、就會出現一致點。不過、雲端供應商所提供的儲存設備效能、可能會影響一致點處理時間。

何時使用高速寫入

如果您的工作負載需要快速寫入效能、而且在發生非計畫性系統中斷或發生非計畫性系統中斷的串聯故障時、您可以承受資料遺失的風險（僅限 HA 配對）、那麼高速寫入速度是很好的選擇。

使用高速寫入速度時的建議事項

如果您啟用高速寫入速度、則應確保應用程式層的寫入保護、或是應用程式在發生資料遺失時仍能承受。

使用**AWS**中的**HA**配對來高速寫入

如果您計畫在AWS中啟用HA配對的高速寫入速度、您應該瞭解多個可用度區域（AZ）部署與單一AZ部署之間的保護層級差異。在多個AZs之間部署HA配對可提供更多恢復能力、並有助於降低資料遺失的機率。

"深入瞭解AWS中的HA配對"。

支援高速寫入的組態

並非所有 Cloud Volumes ONTAP 的不支援高速寫入的組態。這些組態預設會使用正常寫入速度。

AWS

如果您使用單一節點系統、 Cloud Volumes ONTAP 則支援所有執行個體類型的高速寫入速度。

從9.8版開始、Cloud Volumes ONTAP 當使用幾乎所有支援的EC2執行個體類型（m5.xlarge和r5.xlarge除外）時、支援HA配對的高速寫入速度。

"深入瞭解Cloud Volumes ONTAP 支援的Amazon EC2執行個體"。

Azure

如果您使用單一節點系統、 Cloud Volumes ONTAP 則支援所有 VM 類型的高速寫入速度。

如果您使用HA配對、Cloud Volumes ONTAP 從9.8版開始、支援多種VM類型的高速寫入速度。前往 "發行說明 Cloud Volumes ONTAP" 可查看支持高速寫入速度的VM類型。

Google Cloud

如果您使用單一節點系統、 Cloud Volumes ONTAP 則支援所有機器類型的高速寫入速度。

如果您使用HA配對、Cloud Volumes ONTAP 從9.13.0版開始、支援多種VM類型的高速寫入速度。前往 "發行說明 Cloud Volumes ONTAP" 可查看支持高速寫入速度的VM類型。

"深入瞭解Cloud Volumes ONTAP 支援的Google Cloud機器類型"。

如何選擇寫入速度

您可以在建立新的工作環境時選擇寫入速度、而且可以 "變更現有系統的寫入速度"。

發生資料遺失時的預期結果

如果資料因高速寫入而遺失、事件管理系統（EMS）會報告下列兩個事件：

- 更新版本Cloud Volumes ONTAP

```
 NOTICE nv.data.loss.possible: An unexpected shutdown occurred while in
high write speed mode, which possibly caused a loss of data.
* 從9.11.0到9.11.1 Cloud Volumes ONTAP
```

```
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..
* 零點9.8到9.10.1 Cloud Volumes ONTAP
```

```
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.
```

發生這種情況時Cloud Volumes ONTAP 、無需使用者介入、即可啟動及繼續提供資料。

如何在資料遺失時停止資料存取

如果您擔心資料遺失、希望應用程式在資料遺失時停止執行、並在資料遺失問題妥善解決後恢復資料存取、您可以從 CLI 使用 NVFIL 選項來達成此目標。

啟用 **NVFIL** 選項

「 vol modify -volume <vol-name> -nv故障 開啟」

檢查 **NVFIL** 設定

「 vol show -volume <vol-name> -功能 變數 nv失敗 」

停用 **NVFIL** 選項

「 volvol modify -volume <vol-name> -nvail off' 」

發生資料遺失時、啟用 NVFIL 的 NFS 或 iSCSI 磁碟區應停止提供資料（不影響無狀態傳輸協定的 CIFS ）。如需詳細資料、請參閱 "NVFIL 如何影響 NFS 磁碟區或 LUN 的存取"。

以檢查 **NVFIL** 狀態

「 vol show -功能 變數 in -nvfaile-state 」

正確解決資料遺失問題之後、您可以清除 NVFIL 狀態、磁碟區將可供資料存取。

清除 **NVFIL** 狀態

「 vol modify -volume <vol-name> -in nvfaile-state 假」

Flash 快取

部分Cloud Volumes ONTAP 支援的組態包括本機NVMe儲存設備、Cloud Volumes ONTAP 這些儲存設備可作為_Flash Cache使用、以獲得更好的效能。

什麼是**Flash Cache**？

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

支援的組態

Flash Cache支援特定Cloud Volumes ONTAP 的支援功能。檢視中支援的組態 "發行說明 Cloud Volumes ONTAP"

限制

- 所有磁碟區都必須停用壓縮功能、才能充分發揮Flash Cache效能提升功能Cloud Volumes ONTAP 、直到更新至VMware版。當您部署或升級Cloud Volumes ONTAP 至盡力9.12.1時、就不需要停用壓縮功能。

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

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

WORM 儲存設備

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

WORM儲存設備的運作方式

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

保留期間結束後、您必須負責刪除不再需要的任何檔案。

充電

WORM儲存設備的充電時數是每小時一次、視WORM磁碟區的總配置容量而定。

僅適用於 PAYGO 或年度承諾條款、 WORM 授權可透過雲端供應商的市場購買。WORM 支援節點型和容量型授權模式。

BYOL 授權不適用於 Cloud Volumes ONTAP 上的 WORM 儲存設備。

您應該瞭解Cloud Volumes ONTAP 下列使用支援功能的充電行為：

- 從ONTAP S59.10.1開始、WORM磁碟區和非WORM磁碟區可以存在於同一個集合體上。
- 如果您在建立Cloud Volumes ONTAP 一個功能不全的環境時啟用WORM、那麼您從BlueXP建立的每個磁碟區都會啟用WORM。不過ONTAP 、您可以使用「功能性CLI」或「系統管理程式」來建立已停用WORM的磁碟區。這些磁碟區不會以WORM速率收費。
- 如果您在建立工作環境時未啟用WORM、則從BlueXP建立的每個Volume都會停用WORM。這些磁碟區不會以WORM速率收費。

"瞭解WORM儲存設備的定價"

啟動 WORM 儲存設備

如何啟動WORM儲存取決於Cloud Volumes ONTAP 您所使用的版本。

9.10.1版及更新版本

從功能部件支援的版本起、您可以選擇在Volume層級啟用或停用WORM Cloud Volumes ONTAP 。

當您建立Cloud Volumes ONTAP 全新的支援環境時、系統會提示您啟用或停用WORM儲存設備：

- 如果您在建立工作環境時啟用WORM儲存、則您從BlueXP建立的每個Volume都會啟用WORM。但您可以使用System Manager或CLI來建立已停用WORM的磁碟區。
- 如果您在建立工作環境時停用WORM儲存設備、則從BlueXP、System Manager或CLI建立的每個Volume都會停用WORM。如果您想要在Cloud Volumes ONTAP 建立期間未啟用的支援環境中啟用WORM、您必須建立支援票證、並提供NetApp支援以取得協助。

無論選擇哪一項、您都應該這樣做 瞭解充電的運作方式。

9.10.0版及更早版本

您可以在 Cloud Volumes ONTAP 建立新的工作環境時、在一個可靠的系統上啟動 WORM 儲存設備。您從BlueXP建立的每個磁碟區都已啟用WORM。您無法停用個別磁碟區上的WORM儲存設備。

將檔案提交至 **WORM**

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

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

刪除 **WORM** 檔案

您可以在保留期間使用權限刪除功能刪除 WORM 檔案。

如需相關指示、請參閱 "本文檔 ONTAP"

WORM與資料分層

當您建立全新Cloud Volumes ONTAP 的版本的更新版本時、可以同時啟用資料分層和WORM儲存。利用WORM儲存設備進行資料分層、可將資料分層至雲端的物件存放區。

您應該瞭解下列關於啟用資料分層和WORM儲存設備的資訊：

- 分層至物件儲存的資料不含ONTAP 「支援WORM」功能。為了確保端點對端點WORM功能、您必須正確設定儲存區權限。
- 分層至物件儲存的資料並不具備WORM功能、這意味著從技術上而言、任何擁有完整儲存區和容器存取權的人、都能移除由ONTAP 實物分級的物件。
- 啟用WORM和分層後、將Cloud Volumes ONTAP 會封鎖還原或降級至物件9.8。

限制

- WORM儲存在Cloud Volumes ONTAP 「受信任的儲存管理員」模式下運作。儘管WORM檔案受到保護、不會遭到竄改或修改、但即使這些磁碟區包含未過期的WORM資料、叢集管理員仍可刪除這些磁碟區。
- 除了值得信賴的儲存管理員模式之外Cloud Volumes ONTAP 、在「值得信賴的雲端管理員」模式下、WORM儲存設備也會以隱含方式運作。雲端管理員可以直接從雲端供應商移除或編輯雲端儲存設備、在WORM資料到期日前刪除。

高可用度配對

AWS 中的高可用度配對

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

HA 元件

在 AWS 中 Cloud Volumes ONTAP 、不含下列元件：

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

中介者

以下是AWS中有關中介執行個體的一些重要詳細資料：

執行個體類型
: T3-micro

磁碟
: 兩個 ST1 磁碟、 8 GiB 和 4 GiB

作業系統
: DEBIAN11

  對於版本更新的版本、在中介器上安裝了DEBIAN10。Cloud Volumes ONTAP

升級
: 升級Cloud Volumes ONTAP 時、BlueXP也會視需要更新中介執行個體。

存取執行個體
: 當Cloud Volumes ONTAP 您從BlueXP建立一套功能不全的HA配對時、系統會提示您提供一個用於中介執行個體的金鑰配對。您可以使用該金鑰配對來進行SSH存取 `admin` 使用者：

第三方代理程式
: 中介執行個體不支援協力廠商代理程式或VM延伸。

儲存設備接管與恢復

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

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

儲存設備接管、重新同步及還原均為預設自動執行。不需要使用者採取任何行動。

RPO 和 RTO

HA 組態可維持資料的高可用度、如下所示：

- 恢復點目標（ RPO ）為 0 秒。您的資料交易一致、不會遺失任何資料。
- 恢復時間目標（ RTO ）為 120 秒。萬一發生停電、資料應在 120 秒或更短時間內可用。

HA 部署模式

您可以跨多個可用性區域（ AZs ）或單一可用性區域（ AZ ）部署 HA 組態、確保資料的高可用度。您應該檢閱每個組態的詳細資料、以選擇最符合您需求的組態。

多個可用性區域

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

NFS 與 CIFS 資料存取

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

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

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

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

iSCSI 資料存取

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

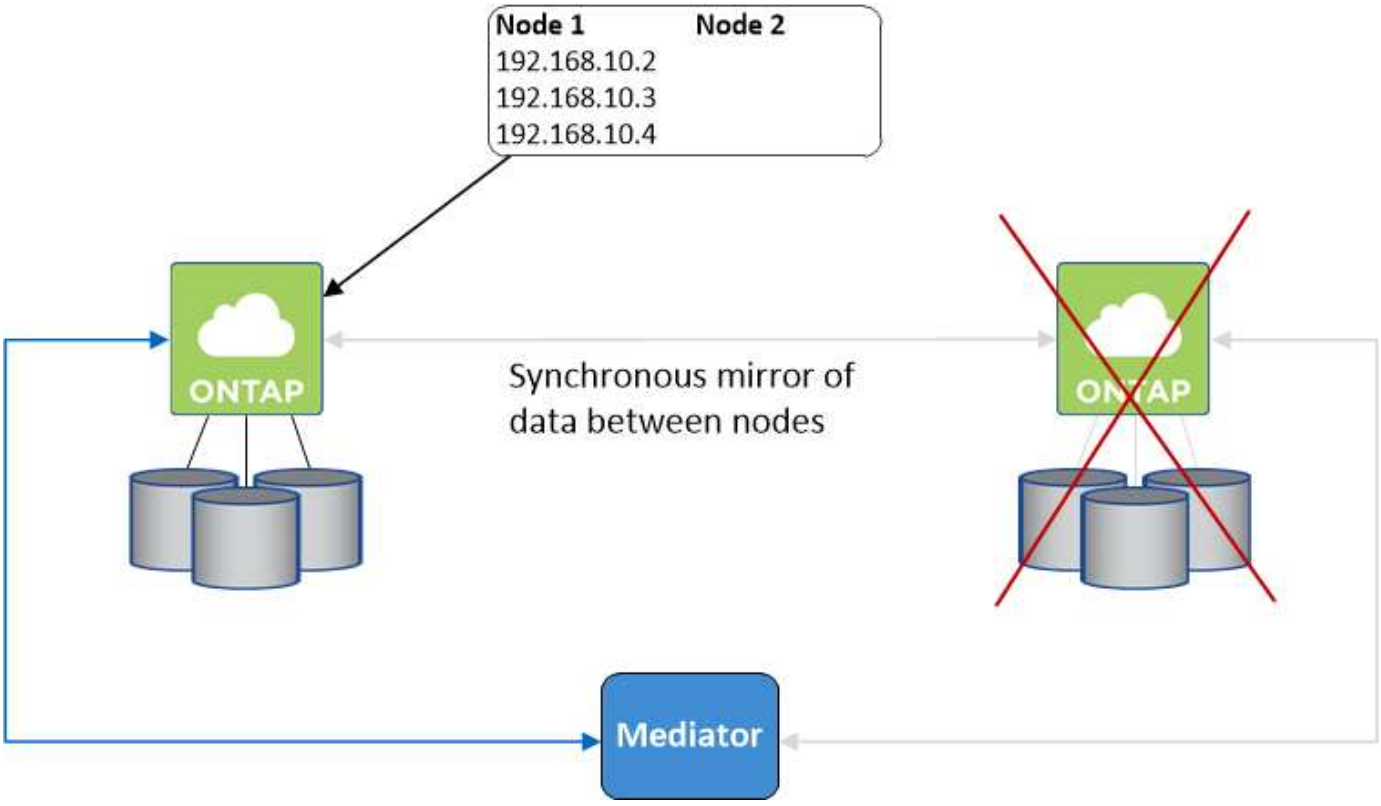
iSCSI 的接管與恢復

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

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

NAS 的接管與恢復

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



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

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

選取磁碟區並按一下*掛載Command*、即可從BlueXP輕鬆識別正確的IP位址。

單一可用性區域

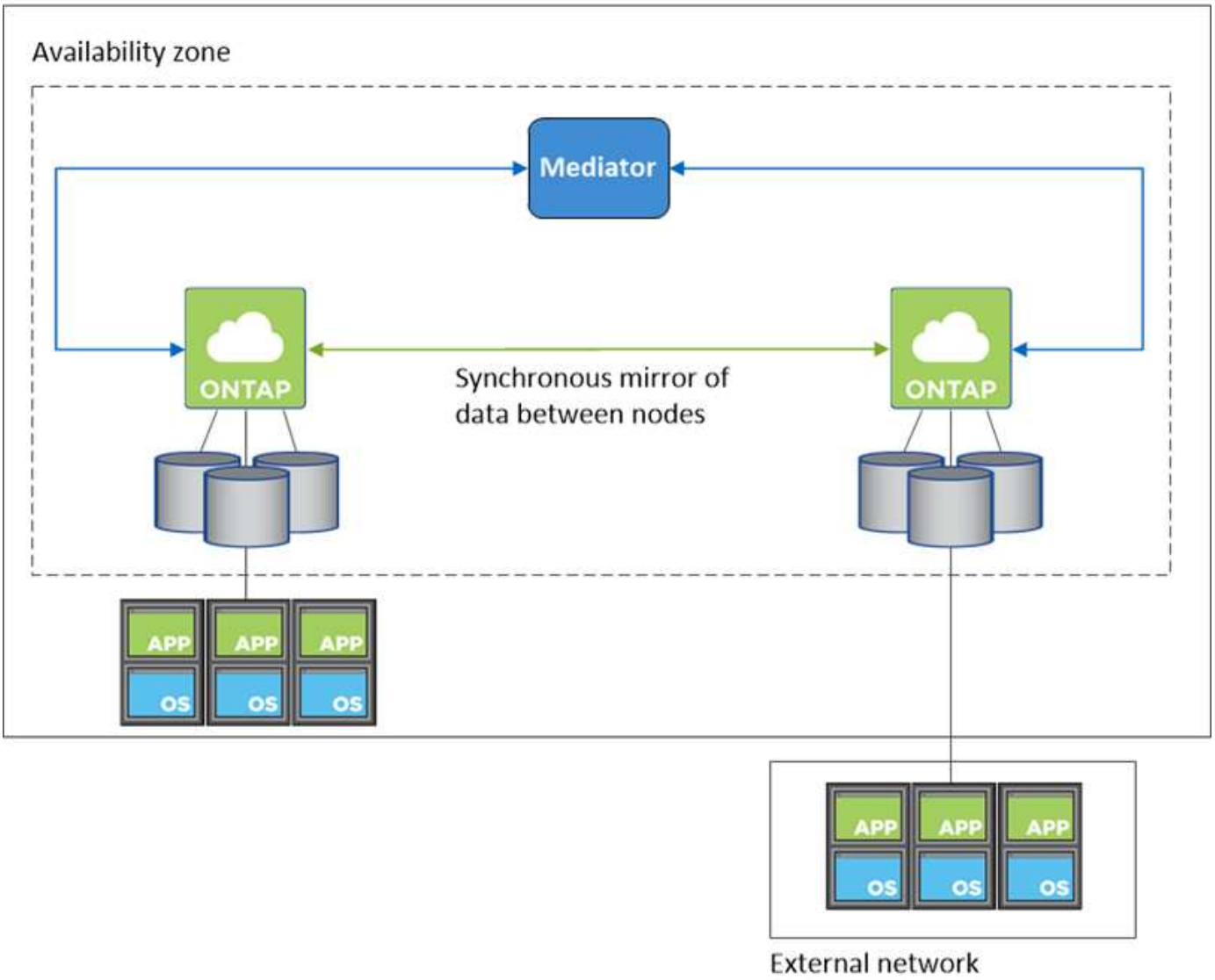
在單一可用性區域（ AZ ）中部署 HA 組態、可確保執行 Cloud Volumes ONTAP 節點的執行個體發生故障時、資料的高可用度。所有資料均可從 VPC 外部原生存取。

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

資料存取

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

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



接管與恢復

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

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

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

AWS 本機區域

AWS 本機區域是一種基礎架構部署、其中儲存、運算、資料庫和其他精選 AWS 服務都位於大城市和產業區域附近。有了 AWS 本機區域、您就能讓 AWS 服務更接近您、進而改善工作負載的延遲、並在本機維護資料庫。

您可以在 AWS 本機區域中部署單一 AZ 或多個 AZ 組態。

在標準模式下使用 BlueXP 時、支援 AWS 本機區域。目前、在受限模式或私有模式下使用 BlueXP 時、並不支援 AWS 本機區域。

AWS 本機區域組態範例

以下為範例組態：

- 單一可用性區域：叢集節點和介面位於同一個本機區域。
- 多個可用性區域
  在多個可用性區域組態中、有三個執行個體、兩個節點和一個中介器。三個執行個體中的一個執行個體必須位於個別的區域中。您可以選擇設定方式。

  以下是三種組態範例：

  - 每個叢集節點位於不同的本機區域、而介面位於公用可用性區域中。
  - 本機區域中的一個叢集節點、本機區域中的中介節點、以及第二個叢集節點位於可用性區域中。
  - 每個叢集節點和介面位於不同的本機區域中。

支援的磁碟和執行個體類型

唯一支援的磁碟類型是 GP2 。

目前支援下列 EC2 執行個體類型系列、其大小為 xlarge 到 4xlarge ：

- M5
- c5
- C5d
- R5
- R5d

"您應該參閱 AWS 、以取得本機區域中支援的 EC2 執行個體類型的最新完整詳細資料"。

儲存設備如何在 **HA** 配對中運作

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

儲存配置

當您建立新的磁碟區並需要額外的磁碟時、BlueXP會將相同數量的磁碟分配給兩個節點、建立鏡射的Aggregate、然後建立新的磁碟區。例如、如果磁碟區需要兩個磁碟、則BlueXP會在每個節點上配置兩個磁碟、總共四個磁碟。

儲存組態

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

只有在儲存系統檢視中使用BluXP時、才能設定雙主動式組態。

效能期望

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

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

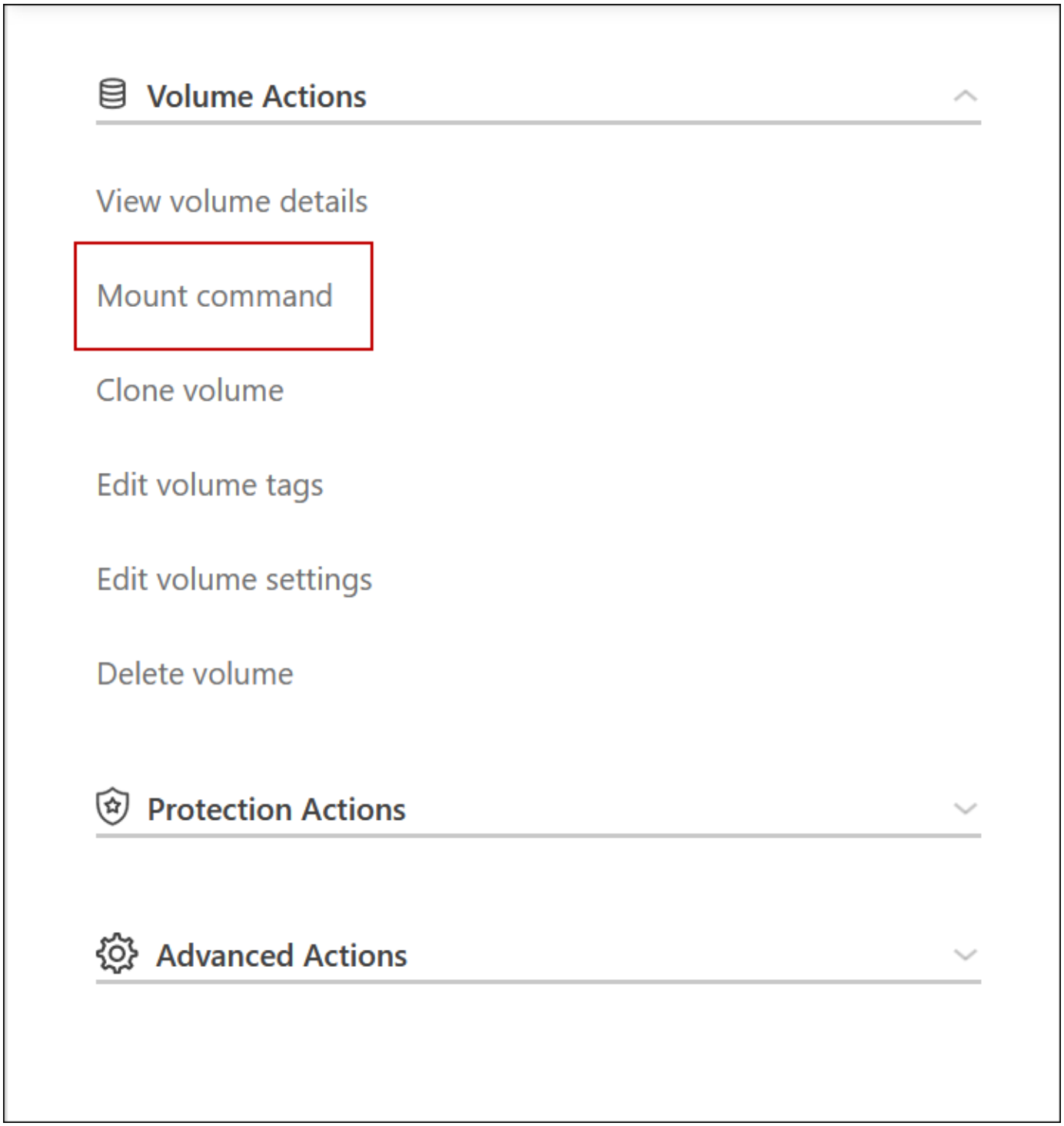
如需 Cloud Volumes ONTAP 更多關於效能的詳細資訊、請參閱 "效能"。

用戶端存取儲存設備

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

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

您可以透過 BlueXP 「管理磁碟區」面板下的 *Mount Command* 選項、輕鬆識別正確的 IP 位址。

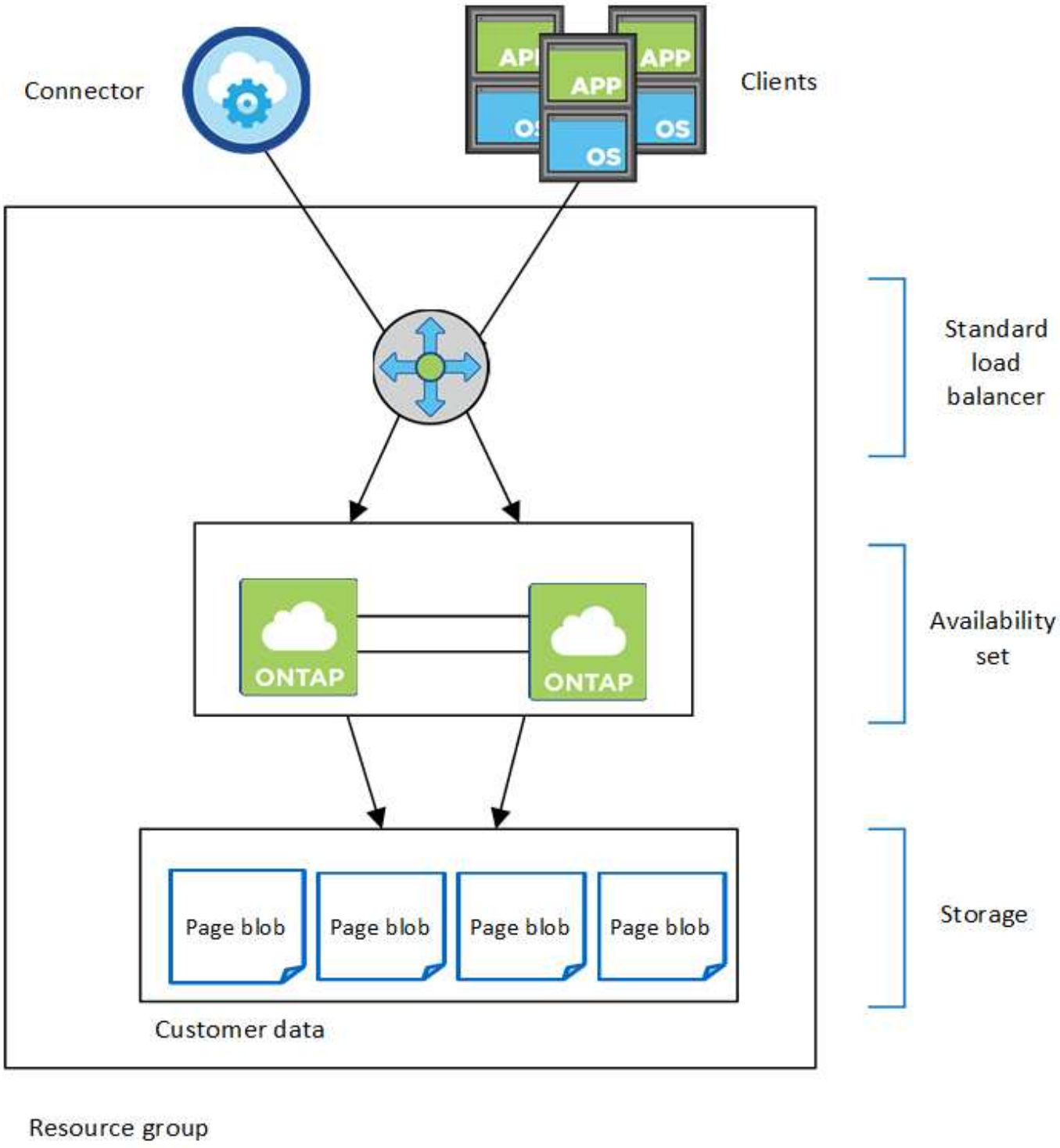


Azure 中的高可用度配對

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

HA 元件

Azure中的一套「功能」頁面Blob組態包括下列元件Cloud Volumes ONTAP ：



請注意以下關於BlueXP部署給您的Azure元件：

Azure 標準負載平衡器

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

可用度設定

Azure可用度集是Cloud Volumes ONTAP 一個由各個節點組成的邏輯群組。可用度集可確保節點處於不同的故障狀態、並更新網域以提供備援和可用度。 "如需可用度集的詳細資訊、請參閱Azure文件"。

磁碟

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

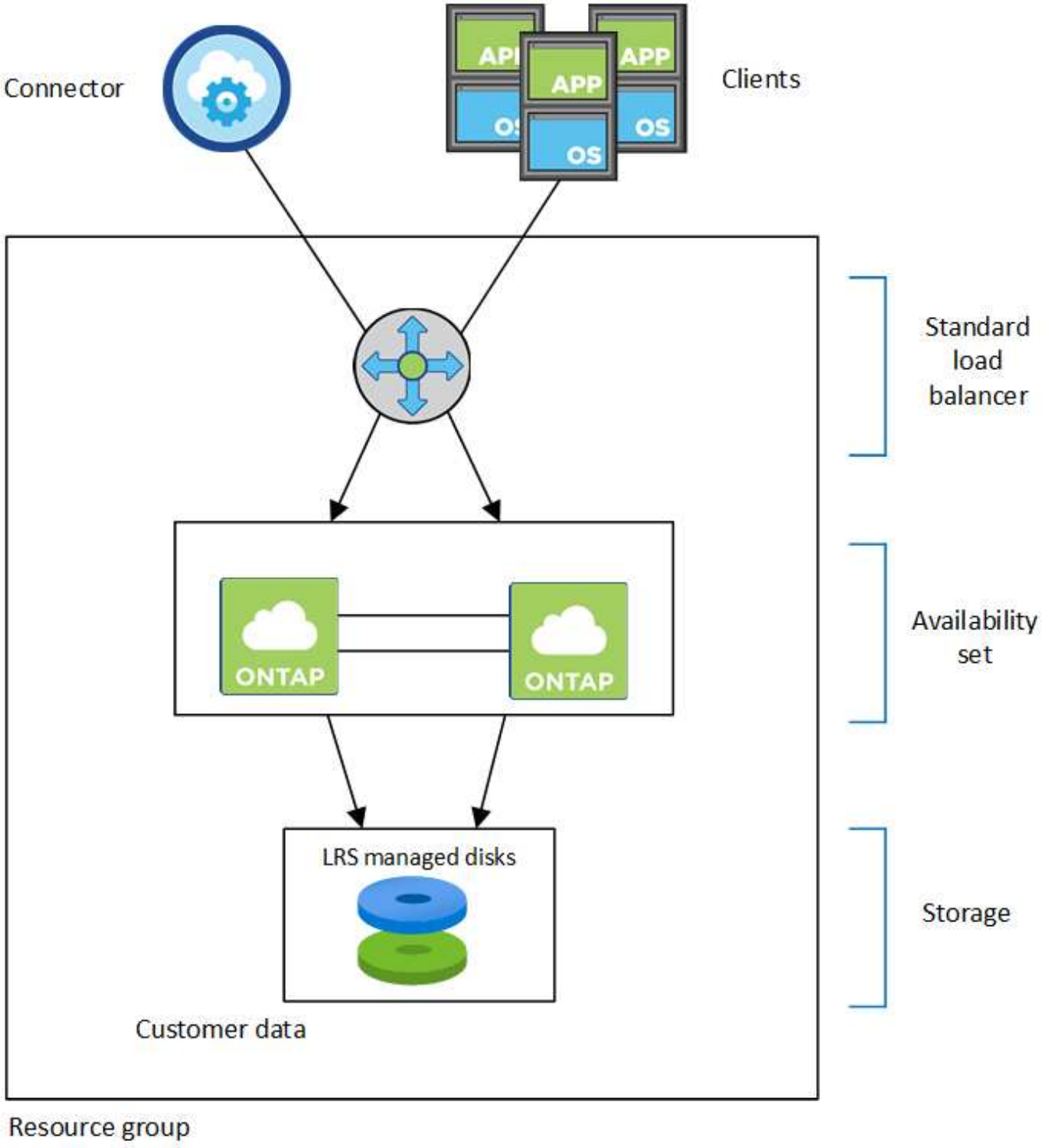
儲存帳戶

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

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

HA單一可用度區域組態與共享的託管磁碟

在共享託管磁碟上執行的一個僅有一個可用度區域組態包含下列元件Cloud Volumes ONTAP ：



請注意以下關於BlueXP部署給您的Azure元件：

Azure 標準負載平衡器

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

可用度設定

Azure可用度集是Cloud Volumes ONTAP 一個由各個節點組成的邏輯群組。可用度集可確保節點處於不同的故障狀態、並更新網域以提供備援和可用度。 "如需可用度集的詳細資訊、請參閱Azure文件"。

磁碟

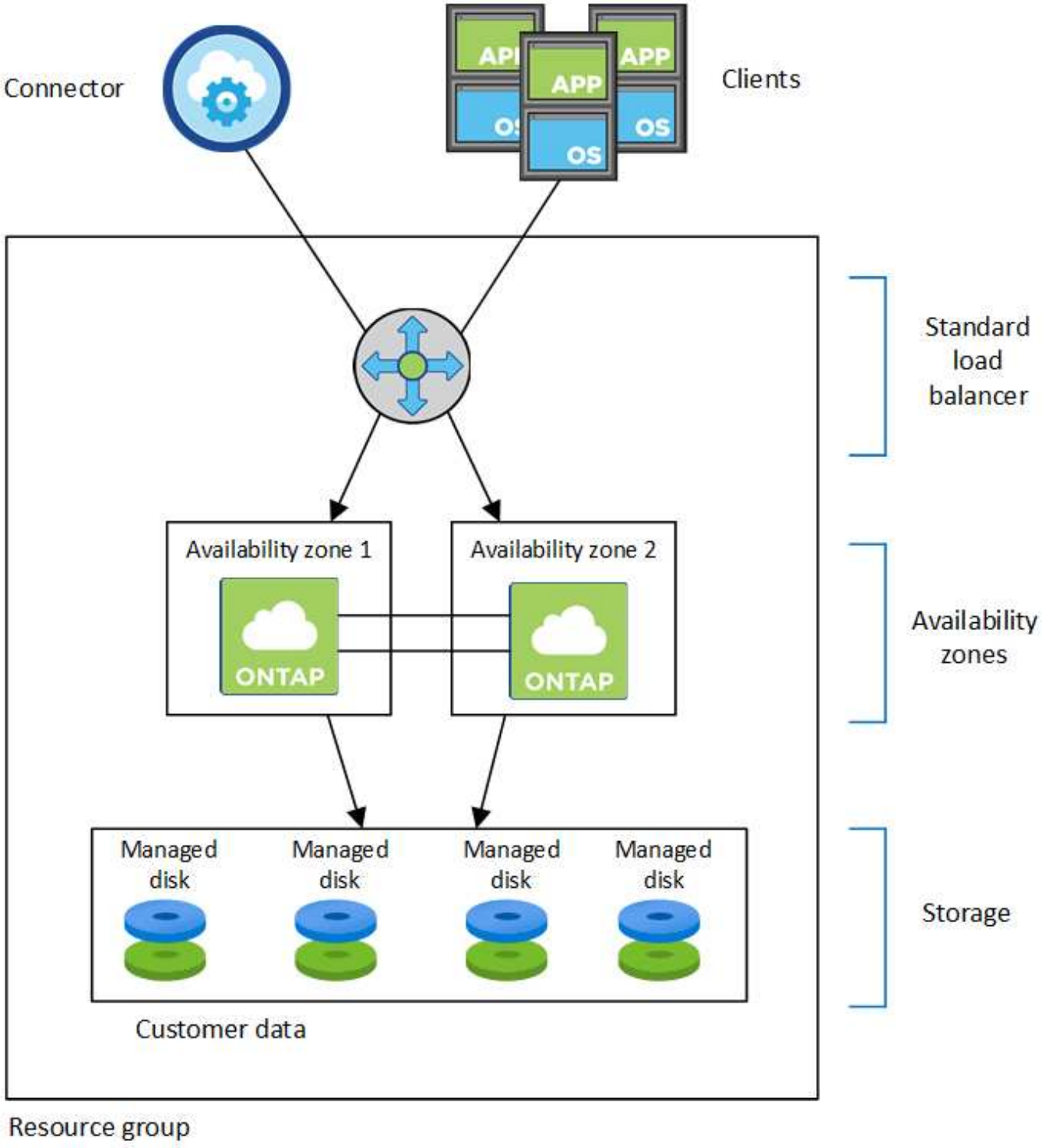
客戶資料位於本機備援儲存設備（LRS）託管磁碟上。每個節點均可存取其他節點的儲存設備。也需要額外的儲存空間 "開機、root、合作夥伴root、核心和NVRAM資料"。

儲存帳戶

儲存帳戶用於託管式磁碟型部署、以處理診斷記錄並分層處理至blob儲存設備。

HA多重可用度區域組態

Azure中的一個支援多種可用度的區域組態包括下列元件Cloud Volumes ONTAP ：



請注意以下關於BlueXP部署給您的Azure元件：

Azure 標準負載平衡器

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

可用度區域

將兩Cloud Volumes ONTAP 個靜態節點部署至不同的可用度區域。可用度區域可確保節點位於不同的故障網域中。 "如需Azure區域備援儲存設備的詳細資訊、請參閱Azure文件"。

磁碟

客戶資料位於區域備援儲存設備（ZRS）託管磁碟上。每個節點均可存取其他節點的儲存設備。也需要額外的儲存空間 "開機、root、合作夥伴root及核心資料"。

儲存帳戶

儲存帳戶用於託管式磁碟型部署、以處理診斷記錄並分層處理至blob儲存設備。

RPO 和 RTO

HA 組態可維持資料的高可用度、如下所示：

- 恢復點目標（ RPO ）為 0 秒。您的資料交易一致、不會遺失任何資料。
- 恢復時間目標（ RTO ）為 120 秒。萬一發生停電、資料應在 120 秒或更短時間內可用。

儲存設備接管與恢復

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

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

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

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

儲存設備接管、重新同步及還原均為預設自動執行。不需要使用者採取任何行動。

儲存組態

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

Google Cloud的高可用度配對

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

HA 元件

Google Cloud的NetApp HA組態包括下列元件：Cloud Volumes ONTAP

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

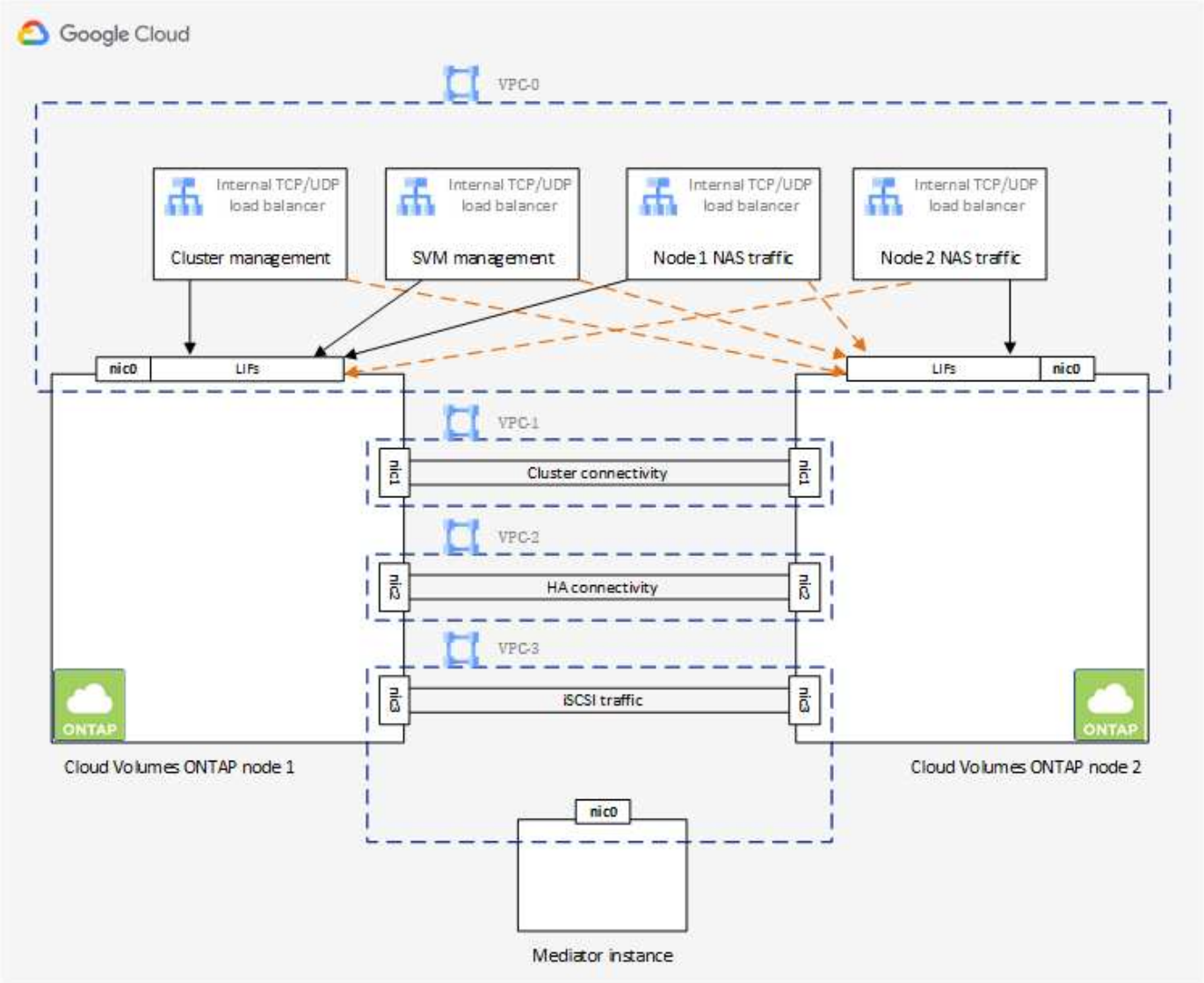
- 四個虛擬私有雲端（VPC）。

  由於 GCP 要求每個網路介面位於獨立的 VPC 網路、因此組態使用四個 VPC 。

- 四個 Google Cloud 內部負載平衡器（ TCP/IP / udp ）、可管理 Cloud Volumes ONTAP 傳入至該「叢集 HA 配對」的流量。

"深入瞭解網路需求"，包括有關負載平衡器、VPC、內部IP位址、子網路等的詳細資訊。

下列概念性影像顯示Cloud Volumes ONTAP 出一套功能不整的HA配對及其元件：



中介者

以下是Google Cloud中介執行個體的一些重要詳細資料：

執行個體類型

E2-Micro（先前使用F1-Micro執行個體）

磁碟

兩個標準持續磁碟、每個10 GiB

作業系統

DEBIAN11

對於版本更新的版本、在中介器上安裝了DEBIAN10。Cloud Volumes ONTAP

升級

升級Cloud Volumes ONTAP 時、BlueXP也會視需要更新中介執行個體。

存取執行個體

對於Debian、預設的雲端使用者是「admin」。當透過Google Cloud主控台或gCloud命令列要求SSH存取時、Google Cloud會建立並新增「admin」使用者的憑證。您可以指定「show」以取得root權限。

第三方代理程式

中介執行個體不支援協力廠商代理程式或VM延伸。

儲存設備接管與恢復

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

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

儲存設備接管、重新同步及還原均為預設自動執行。不需要使用者採取任何行動。

RPO 和 RTO

HA 組態可維持資料的高可用度、如下所示：

- 恢復點目標（ RPO ）為 0 秒。

  您的資料交易一致、不會遺失任何資料。

- 恢復時間目標（ RTO ）為 120 秒。

  萬一發生停電、資料應在 120 秒或更短時間內可用。

HA 部署模式

您可以在多個區域或單一區域中部署 HA 組態、確保資料的高可用度。

多個區域（建議）

跨三個區域部署 HA 組態、可確保在區域內發生故障時、仍能持續提供資料。請注意、與使用單一區域相比、寫入效能略低、但卻是最低的。

單一區域

當部署在單一區域時、 Cloud Volumes ONTAP 使用分散配置原則的即可實現不受限制的 HA 組態。此原則可確保 HA 組態不會在區域內發生單點故障、而無需使用個別區域來實現故障隔離。

此部署模式可降低成本、因為各區域之間不需支付任何資料出口費用。

儲存設備如何在 **HA** 配對中運作

不像 ONTAP 是一個叢集、 Cloud Volumes ONTAP 在 GCP 中使用的不二線 HA 配對儲存設備不會在節點之間共享。相反地、資料會在節點之間同步鏡射、以便在發生故障時能夠使用資料。

儲存配置

當您建立新的磁碟區並需要額外的磁碟時、BlueXP會將相同數量的磁碟分配給兩個節點、建立鏡射的Aggregate、然後建立新的磁碟區。例如、如果磁碟區需要兩個磁碟、則BlueXP會在每個節點上配置兩個磁碟、總共四個磁碟。

儲存組態

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

HA 組態的效能期望

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

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

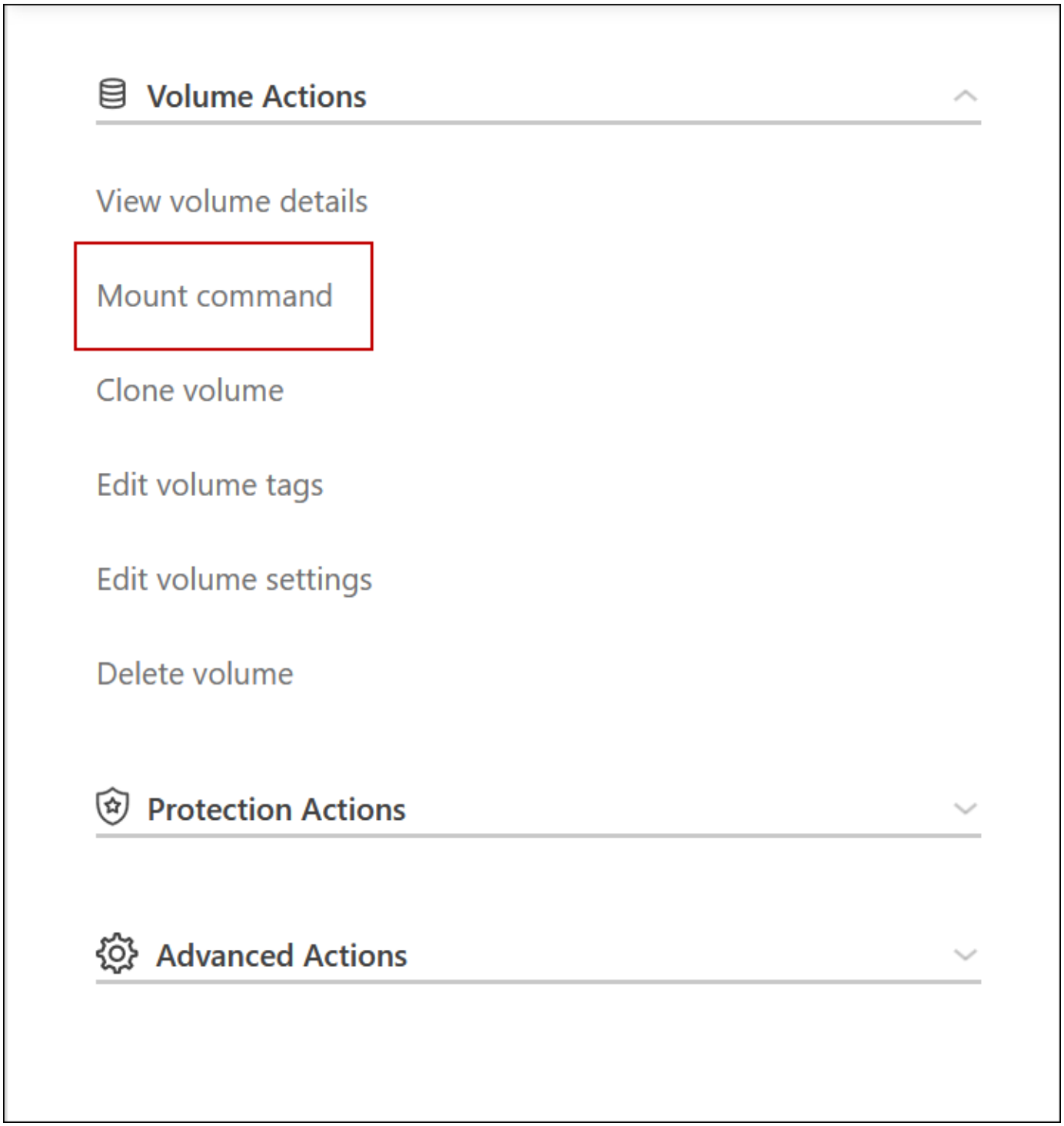
如需 Cloud Volumes ONTAP 更多關於效能的詳細資訊、請參閱 "效能"。

用戶端存取儲存設備

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

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

您可以透過 BlueXP 「管理磁碟區」面板下的 *Mount Command* 選項、輕鬆識別正確的 IP 位址。



相關連結

- "深入瞭解網路需求"
- "瞭解如何開始使用 GCP"

接管期間無法使用的動作

當HA配對中的某個節點無法使用時、另一個節點會為其合作夥伴提供資料、以提供持續的資料服務。這稱為_storage takeover。在儲存恢復完成之前、數個動作都無法使用。

當HA配對中的節點無法使用時、BlueXP中的工作環境狀態為_Degraded。

下列動作無法從BlueXP儲存設備接管中使用：

- 支援註冊
- 授權變更
- 執行個體或VM類型變更
- 寫入速度變更
- CIFS設定
- 變更組態備份的位置
- 設定叢集密碼
- 管理磁碟與集合體（進階分配）

儲存恢復完成、工作環境狀態恢復正常之後、這些動作就會再次可用。

安全性

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

加密閒置的資料

支援下列加密技術： Cloud Volumes ONTAP

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

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

NetApp 加密解決方案（ **NVE** 和 **NAE** ）

支援Cloud Volumes ONTAP "NetApp Volume Encryption（NVE）與NetApp Aggregate Encryption（NAE）"。NVE 和 NAE 是軟體型解決方案、可對磁碟區進行（ FIPS ） 140-2 相容的閒置資料加密。NVE 和 NAE 都使用 AES 256 位元加密。

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

外部金鑰管理程式支援NVE和NAE。

新的Aggregate在您設定外部金鑰管理程式之後、預設會啟用NetApp Aggregate Encryption（NAE）。非 NAE

Aggregate 一部分的新磁碟區、預設會啟用 NetApp Volume Encryption （ NVE ）（例如、如果您有在設定外部金鑰管理程式之前建立的現有 Aggregate ）。

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

AWS 金鑰管理服務

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

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

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

Azure 儲存服務加密

資料會使用在Cloud Volumes ONTAP Azure中的功能自動加密 "Azure 儲存服務加密" 使用Microsoft管理的金鑰。

您可以視需要使用自己的加密金鑰。 "瞭解如何在Cloud Volumes ONTAP Azure中設定使用客戶管理的金鑰"。

Google Cloud Platform 預設加密

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

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

執行防毒掃描 **ONTAP**

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

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

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

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

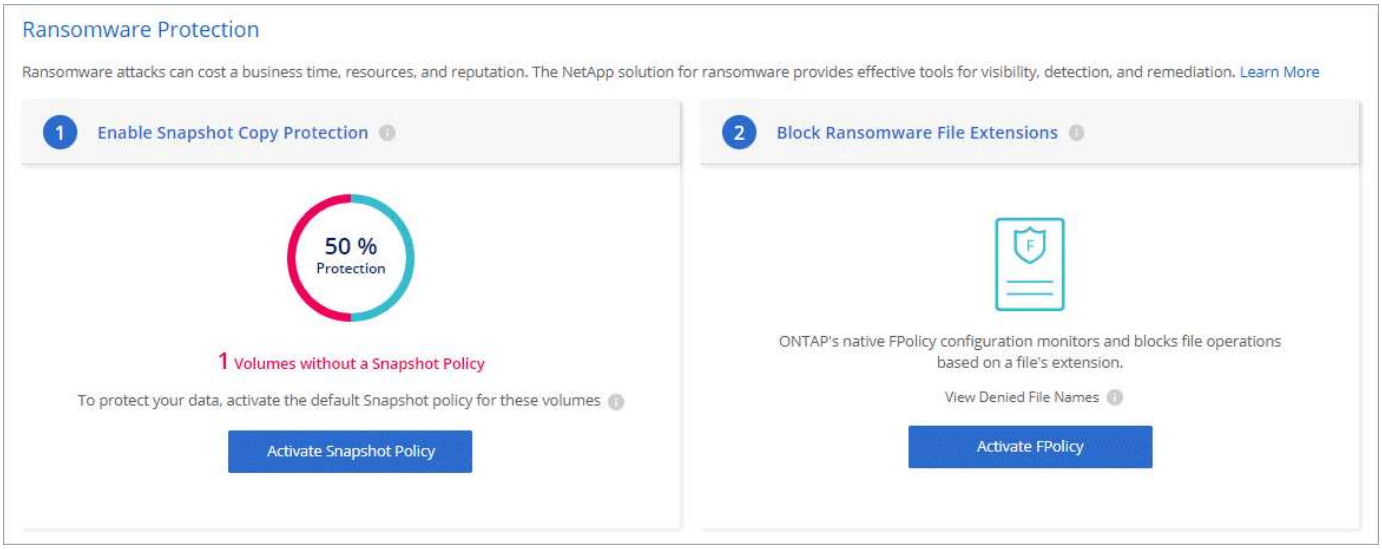
勒索軟體保護

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

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

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

- 此外、您也可以啟用ONTAP的FPolicy解決方案、封鎖常見的勒索軟體副檔名。



"瞭解如何實作 NetApp 勒索軟體解決方案"。

效能

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

效能技術報告

- AWS 適用的 Cloud Volumes ONTAP

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

- 適用於 Microsoft Azure 的 Cloud Volumes ONTAP

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

- 適用於 Google Cloud Cloud Volumes ONTAP

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

CPU效能

從雲端供應商的監控工具中、顯示出使用率極高（超過90%）的節點。Cloud Volumes ONTAP這是因為ONTAP、當需要時、支援的所有vCPU都會保留在虛擬機器上。

如需協助、請參閱 "NetApp知識庫文章、說明如何ONTAP 使用CLI監控不實的CPU使用率"

節點型BYOL的授權管理

每個採用節點型BYOL的系統都必須安裝有效訂閱的系統授權。Cloud Volumes ONTAPBlueXP可管理您的授權、並在授權到期前顯示警告、藉此簡化程序。

節點型授權是前一代Cloud Volumes ONTAP 的BYOL for the節點型授權僅適用於授權續約。

"深入瞭Cloud Volumes ONTAP 解有關功能多樣的授權選項"。

"深入瞭解如何管理節點型授權"。

BYOL 系統授權

節點型授權最多可為單一節點或HA配對提供368TiB容量。

您可以購買Cloud Volumes ONTAP 多個適用於某個不含資料的BYOL系統授權、以分配超過368TiB的容量。例如、您可能會購買兩份授權、以配置多達736 TiB的容量來Cloud Volumes ONTAP 供使用。您也可以購買四份授權、最多可取得1.4 PIB。

單一節點系統或 HA 配對可購買的授權數量不受限制。

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

新系統的授權管理

當您建立節點型BYOL系統時、BlueXP會提示您輸入授權的序號和NetApp 支援網站 您的效益帳戶。BlueXP使用帳戶從NetApp下載授權檔案、並將其安裝在Cloud Volumes ONTAP 整個作業系統上。

"瞭解如何在NetApp 支援網站 BlueXP中新增功能不一的帳戶"。

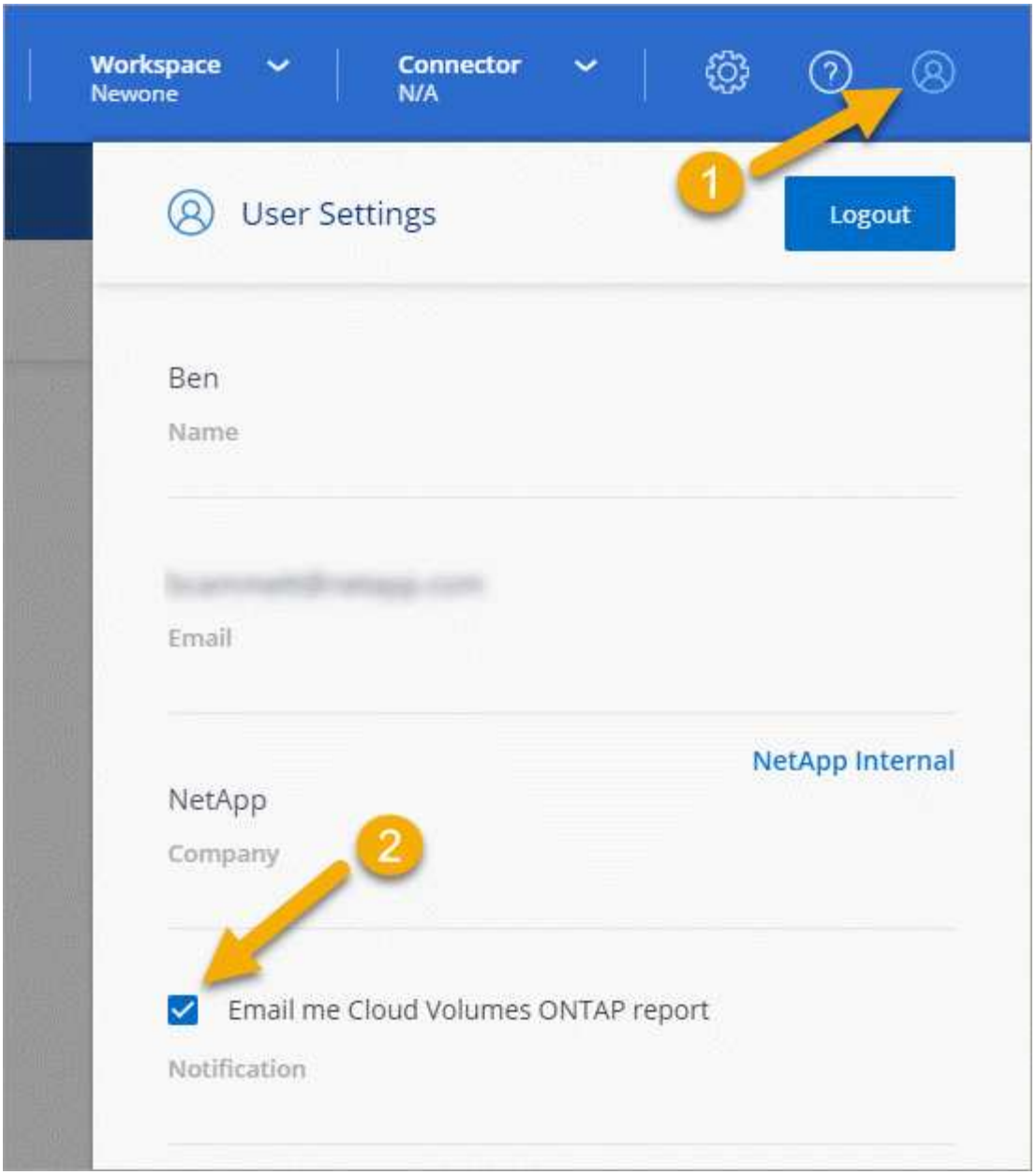
如果BlueXP無法透過安全的網際網路連線存取授權檔案、您可以這麼做 "自行取得檔案、然後手動將檔案上傳至BlueXP"。

授權過期

在節點型授權即將到期的30天之前、BlueXP會顯示警告、並在授權到期時再次顯示警告。下圖顯示使用者介面中顯示的30天到期警告：

您可以選取工作環境來檢閱訊息。

如果Cloud Volumes ONTAP 您是帳戶管理員、且啟用下列選項、則BlueXP會在以電子郵件寄送給您的《支援報告》中包含授權到期警告：



電子郵件報告每2週會顯示授權到期警告。

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

授權續約

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

如果BlueXP無法透過安全的網際網路連線存取授權檔案、您可以這麼做 "自行取得檔案、然後手動將檔案上傳至BlueXP"。

授權移轉至新系統

當您刪除現有系統、然後使用相同授權建立新系統時、節點型BYOL授權可在Cloud Volumes ONTAP 各個版本之間傳輸。

例如、您可能想要刪除現有的授權系統、然後在不同的VPC/vnet或雲端供應商中、將授權用於新的BYOL系統。請注意、任何雲端供應商都只能使用不受雲端限制的序號。不受雲端限制的序號開頭為_908xxxx_字首。

請務必注意、您的BYOL授權與貴公司及一組特定的NetApp支援網站認證資料有關。

不再是不知道的數位顧問AutoSupport Active IQ

這個功能的元件會收集遙測資料並傳送給分析人員。AutoSupport ONTAP支援以支援技術分析資料、並提供主動式的照護與最佳化功能。Active IQ AutoSupport利用人工智慧、Active IQ 即可識別潛在問題、並在問題影響企業之前協助您解決問題。

透過雲端型入口網站和行動應用程式、提供可據以行動的預測分析和主動式支援、讓您能夠在全球混合雲中最佳化資料基礎架構。Active IQ所有擁有有效的NetApp客戶都能從NetApp獲得資料導向的見解和建議Active IQ （功能因產品和支援層而異）SupportEdge 。

以下是Active IQ 您可以利用下列功能來執行的作業：

- 規劃升級。

  可識別環境中的問題、這些問題可透過升級至更新版本的VMware知識來解決、而升級顧問元件則可協助您規劃成功的升級方案。Active IQ ONTAP

- 檢視系統健全狀況。

  您的「不健全狀況」儀表板會回報任何問題、並協助您修正這些問題。Active IQ監控系統容量、確保儲存空間永遠不會耗盡。檢視系統的支援案例。

- 管理效能：

  顯示系統效能的時間比您在《VMware系統管理程式》中看到的更長。Active IQ ONTAP找出影響您效能的組態和系統問題。最大化效率。檢視儲存效率指標、找出在更少空間中儲存更多資料的方法。

- 檢視庫存與組態。

  顯示完整的庫存、軟體和硬體組態資訊。Active IQ查看服務合約何時到期並續約、以確保您仍享有支援。

相關資訊

- "NetApp文件：Active IQ 《Data Advisor》"
- "產品Active IQ 發表"
- "部門服務SupportEdge"

的預設組態 Cloud Volumes ONTAP

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

預設設定

- 在部署Cloud Volumes ONTAP 時、BlueXP會建立一個資料服務儲存VM。部分組態支援額外的儲存 VM 。 "深入瞭解管理儲存 VM"。

  從BlueXP 3.9.5版本開始、系統會在初始儲存VM上啟用邏輯空間報告功能。以邏輯方式回報空間時ONTAP、此功能會報告磁碟區空間、讓儲存效率功能所節省的所有實體空間也會報告為已使用。

- BlueXP會自動在ONTAP 下列功能授權上安裝Cloud Volumes ONTAP 到更新版本：
  - CIFS
  - FlexCache
  - FlexClone
  - iSCSI
  - 多租戶加密金鑰管理（MTEKM）、從Cloud Volumes ONTAP 版本號為E9.12.1 GA開始
  - NetApp Volume Encryption （僅適用於 BYOL 或註冊的 PAYGO 系統）
  - NFS
- SnapMirror
- SnapRestore
- SnapVault
  - 預設會建立多個網路介面：
- 叢集管理 LIF
- 叢集間 LIF
- Azure HA系統上的SVM管理LIF
- Google Cloud HA系統上的SVM管理LIF
- AWS單一節點系統上的SVM管理LIF
- 節點管理 LIF

+在Google Cloud中、此LIF與叢集間LIF結合使用。

- iSCSI 資料 LIF
- CIFS 與 NFS 資料 LIF

> 根據Cloud Volumes ONTAP 雲端供應商的需求、根據預設、LIF容錯移轉功能會停用以供使用。將 LIF 移轉至其他連接埠會中斷執行個體上 IP 位址與網路介面的外部對應、使 LIF 無法存取。

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

    可從http://ipaddress/occm/offboxconfig/存取備份、其中_ipaddress_是Connector主機的IP位址。

  - BlueXP會設定一些不同於其他管理工具的Volume屬性（例如System Manager或CLI）。

    下表列出BlueXP設定的Volume屬性與預設值不同：

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

+
請參閱 "SUR_volume cre__手冊頁ONTAP" 以取得這些屬性的相關資訊。

用於系統資料的內部磁碟

除了儲存使用者資料之外、BlueXP也購買雲端儲存設備來儲存系統資料。

AWS

- 每個節點有三個磁碟用於開機、根和核心資料：
  - 用於開機資料的 47 GB IO1 磁碟
  - 140 GiB GP3磁碟用於根資料
  - 540 GiB gp2磁碟用於核心資料
- 對於 HA 配對、介面執行個體的兩個 ST1 EBS 磁碟區約為 8 GiB 和 4 GiB 、以及每個節點額外的 140 GiB GP3 磁碟、以包含另一個節點的根資料複本。

  在某些區域中、可用的 EBS 磁碟類型只能是 gp2 。
- 每個開機磁碟和根磁碟各一份 EBS 快照

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

在AWS中、NVRAM位於開機磁碟上。

Azure （單一節點）

- 三個優質 SSD 磁碟：
  - 一個10 GiB磁碟用於開機資料

- 一個140 GiB磁碟用於根資料
- 一個512 GiB磁碟用於NVRAM

  如果您選擇Cloud Volumes ONTAP 的虛擬機器支援Ultra SSD、則系統會使用32 GiB Ultra SSD來執行NVRAM、而非使用Premium SSD。

- 一張1024 GiB標準HDD磁碟、可節省核心
- 每個開機磁碟和根磁碟各一份 Azure 快照
- Azure中的每個磁碟預設都會在閒置時加密。

Azure（**HA**配對）

HA與頁面**blob**配對

- 兩個10 GiB Premium SSD磁碟用於開機磁碟區（每個節點一個）
- 兩個140 GiB Premium Storage頁面、用於根磁碟區（每個節點一個）
- 兩個1024 GiB標準HDD磁碟、可節省核心（每個節點一個）
- 兩個512 GiB Premium SSD磁碟用於NVRAM（每個節點一個）
- 每個開機磁碟和根磁碟各一份 Azure 快照

  快照會在重新開機時自動建立。

- Azure中的每個磁碟預設都會在閒置時加密。

HA 可與多個可用性區域中的共享託管磁碟配對

- 兩個10 GiB Premium SSD磁碟用於開機磁碟區（每個節點一個）
- 兩個512 GiB Premium Storage頁面、用於根磁碟區（每個節點一個）
- 兩個1024 GiB標準HDD磁碟、可節省核心（每個節點一個）
- 兩個512 GiB Premium SSD磁碟用於NVRAM（每個節點一個）
- 每個開機磁碟和根磁碟各一份 Azure 快照

  快照會在重新開機時自動建立。

- Azure中的每個磁碟預設都會在閒置時加密。

Google Cloud（單一節點）

- 一個10 GiB SSD持續磁碟用於開機資料
- 一個64 GiB SSD持續磁碟用於根資料
- 一個500 GiB SSD持續磁碟用於NVRAM
- 一個315 GiB標準持續磁碟、用於儲存核心
- 用於開機和根資料的快照

快照會在重新開機時自動建立。

- 開機磁碟和根磁碟預設為加密。

Google Cloud（HA配對）

- 兩個10 GiB SSD持續磁碟、用於開機資料
- 四個64 GiB SSD持續磁碟用於根資料
- 兩個500 GiB SSD持續磁碟用於NVRAM
- 兩個315 GiB標準持續磁碟、用於儲存核心
- 一個10 GiB標準持續磁碟、用於中介資料
- 一個10 GiB標準持續磁碟、用於中介開機資料
- 用於開機和根資料的快照

快照會在重新開機時自動建立。

- 開機磁碟和根磁碟預設為加密。

磁碟所在位置

BlueXP將儲存設備配置如下：

- 開機資料位於附加至執行個體或虛擬機器的磁碟上。

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

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

知識與支援

註冊以取得支援

需要註冊支援、才能獲得 BlueXP 及其儲存解決方案與服務專屬的技術支援。也需要註冊支援、才能啟用 Cloud Volumes ONTAP 系統的重要工作流程。

註冊支援並不會啟用雲端供應商檔案服務的 NetApp 支援。如需雲端供應商檔案服務、其基礎架構或任何使用服務的解決方案的相關技術支援、請參閱該產品的 BlueXP 文件中的「取得說明」。

- "Amazon FSX for ONTAP Sf"
- "Azure NetApp Files"
- "適用於 Google Cloud Cloud Volumes Service"

支援登錄總覽

有兩種登錄形式可啟動支援服務權利：

- 註冊您的BlueXP帳戶ID支援訂閱（您的20位數960xxxxxxx序號位於BlueXP的「Support Resources（支援資源）」頁面）。

  這是您在BlueXP內任何服務的單一支援訂閱ID。每個BlueXP帳戶層級的支援訂閱都必須註冊。

- 在Cloud Volumes ONTAP 雲端供應商的市場中註冊與訂閱相關的支援服務序號（這些序號為20位數909601xxxxxxxx序號）。

  這些序號通常稱為「_PAYGO」序號、並在Cloud Volumes ONTAP 部署時由BlueXP產生。

註冊這兩種類型的序號、即可開啟支援服務單和自動建立個案。如下列所述、將 NetApp 支援網站 （ NSS ）帳戶新增至 BlueXP 即可完成登錄。

註冊您的 **BlueXP** 帳戶以取得 **NetApp** 支援

若要註冊以取得支援並啟動支援授權、 BlueXP 帳戶中的一位使用者必須將 NetApp 支援網站 帳戶與其 BlueXP 登入建立關聯。您如何註冊NetApp支援取決於您是否已擁有NetApp 支援網站 一個NetApp（NSS）帳戶。

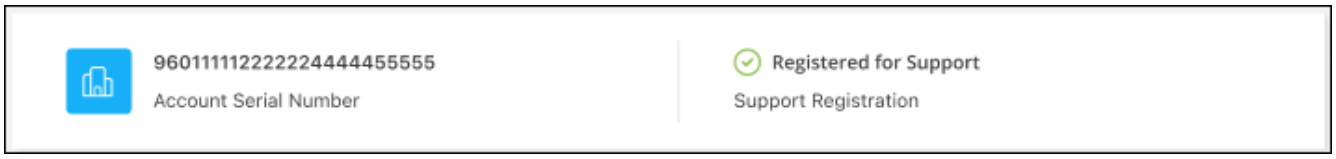
現有的客戶、擁有一個新服務客戶帳戶

如果您是擁有NSS帳戶的NetApp客戶、您只需透過BlueXP註冊即可獲得支援。

步驟

1. 在 BlueXP 主控台的右上角、選取「設定」圖示、然後選取 * 認證 * 。
2. 選取 * 使用者認證 * 。
3. 選取 * 新增 NSS 認證 * 、然後遵循 NetApp 支援網站 （ NSS ）驗證提示。
4. 若要確認註冊程序是否成功、請選取「說明」圖示、然後選取 * 「支援 * 」 。

   「 * 資源 * 」頁面應顯示您的帳戶已註冊以取得支援。



請注意、如果其他 BlueXP 使用者尚未將 NetApp 支援網站 帳戶與 BlueXP 登入建立關聯、則不會看到此相同的支援登錄狀態。不過、這並不表示您的 BlueXP 帳戶尚未註冊支援。只要帳戶中有一位使用者已遵循這些步驟、您的帳戶就已登錄。

現有客戶、但無**NSS.**帳戶

如果您是現有的 NetApp 客戶、擁有現有的授權和序號、但沒有 NSS_ 帳戶、則需要建立一個 NSS 帳戶、並將其與您的 BlueXP 登入建立關聯。

步驟

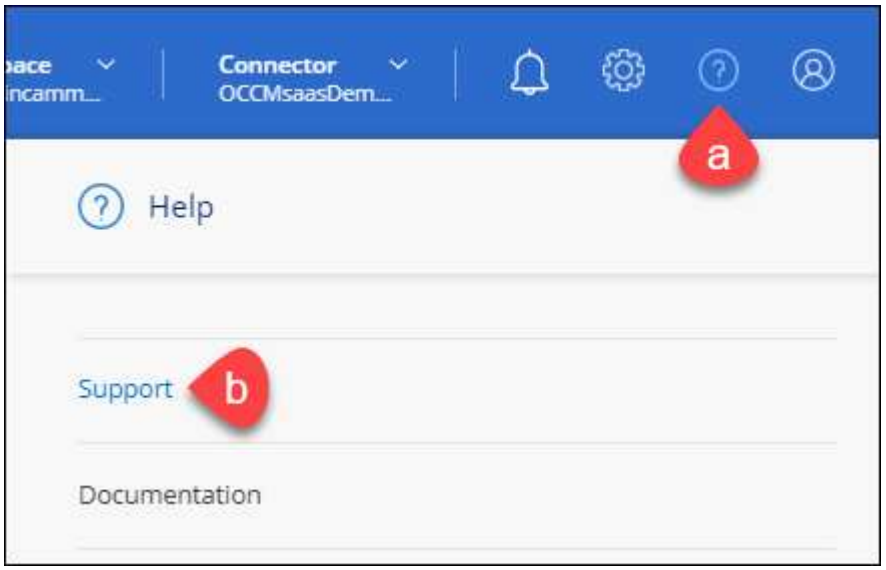
1. 完成建立NetApp 支援網站 一個不完善的帳戶 "《使用者登錄表》NetApp 支援網站"
   a. 請務必選擇適當的使用者層級、通常為* NetApp客戶/終端使用者*。
   b. 請務必複製上述序號欄位使用的BlueXP帳戶序號（960xxxx）。這將加速帳戶處理。
2. 完成下的步驟、將新的 NSS 帳戶與 BlueXP 登入建立關聯 [現有的客戶、擁有一個新服務客戶帳戶]。

NetApp全新推出

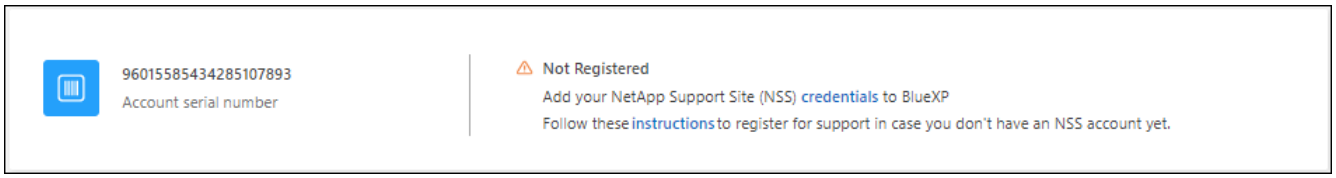
如果您是NetApp的新客戶、而且您沒有新的NSS帳戶、請依照下列每個步驟操作。

步驟

1. 在 BlueXP 主控台的右上角、選取「說明」圖示、然後選取 * 「支援 * 」 。



2. 從「Support Registration（支援註冊）」頁面找到您的帳戶ID序號。



3. 瀏覽至 "NetApp的支援註冊網站" 並選擇*我不是NetApp註冊客戶*。
4. 填寫必填欄位（紅色星號）。
5. 在*產品系列*欄位中、選取* Cloud Manager*、然後選取適用的帳單供應商。
6. 複製上述步驟2的帳戶序號、完成安全性檢查、然後確認您已閱讀NetApp的全球資料隱私權政策。

   系統會立即將電子郵件傳送至提供的信箱、以完成此安全交易。如果驗證電子郵件在幾分鐘內未送達、請務必檢查您的垃圾郵件資料夾。

7. 確認電子郵件中的行動。

   確認將您的申請提交給NetApp、並建議您建立NetApp 支援網站 一個申請表。

8. 完成建立NetApp 支援網站 一個不完善的帳戶 "《使用者登錄表》NetApp 支援網站"
   a. 請務必選擇適當的使用者層級、通常為* NetApp客戶/終端使用者*。
   b. 請務必複製上述序號欄位使用的帳戶序號（960xxxx）。這將加速帳戶處理。

完成後

在此過程中、NetApp應與您聯絡。這是新使用者的一次性就職練習。

擁有 NetApp 支援網站 帳戶後、請完成下的步驟、將帳戶與 BlueXP 登入建立關聯 [現有的客戶、擁有一個新服務客戶帳戶]。

建立 NSS 認證的關聯、以取得 Cloud Volumes ONTAP 支援

若要為 Cloud Volumes ONTAP 啟用下列關鍵工作流程、必須將 NetApp 支援網站 認證與 BlueXP 帳戶建立關聯：

- 註冊隨用隨付 Cloud Volumes ONTAP 系統以取得支援

  您必須提供您的NSS帳戶、才能啟動系統支援、並取得NetApp技術支援資源的存取權。

- 自帶授權（Cloud Volumes ONTAP BYOL）即可部署

  您必須提供您的NSS帳戶、才能讓BlueXP上傳授權金鑰、並啟用您所購買期間的訂閱。這包括定期續約的自動更新。

- 升級Cloud Volumes ONTAP 更新版的更新版

將 NSS 認證與 BlueXP 帳戶建立關聯、與 BlueXP 使用者登入相關的 NSS 帳戶不同。

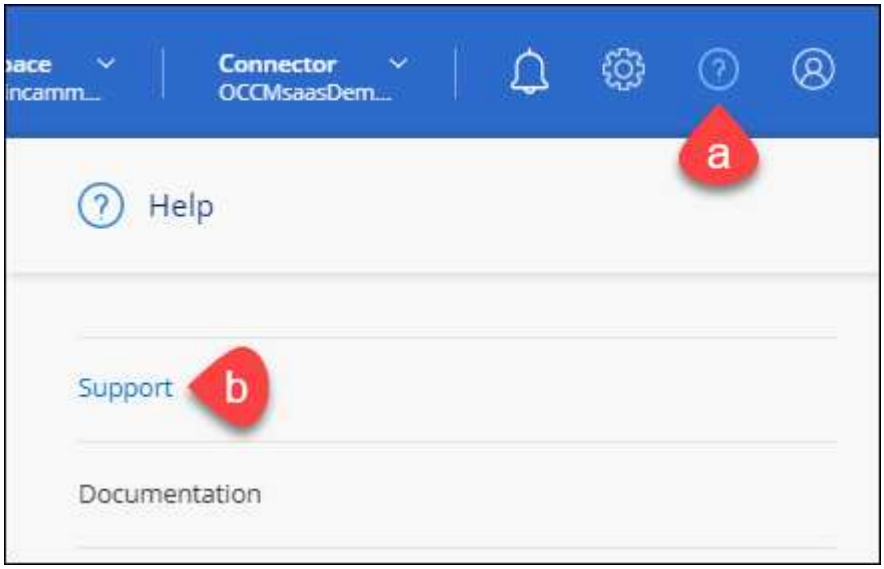
這些 NSS 認證會與您的特定 BlueXP 帳戶 ID 相關聯。屬於BlueXP帳戶的使用者可以從*支援> nss管理*存取這些認證資料。

- 如果您有客戶層級的帳戶、可以新增一或多個NSS帳戶。

- 如果您有合作夥伴或經銷商帳戶、您可以新增一或多個NSS帳戶、但這些帳戶無法與客戶層級帳戶一起新增。

步驟

1. 在 BlueXP 主控台的右上角、選取「說明」圖示、然後選取 * 「支援 * 」 。



2. 選取 **NSS Management > Add NSS Account** 。
3. 系統提示時、請選取 * 繼續 * 以重新導向至 Microsoft 登入頁面。

   NetApp 使用 Microsoft Entra ID 做為身分識別提供者、提供專為支援與授權所設計的驗證服務。

4. 在登入頁面上、提供您的NetApp支援網站註冊電子郵件地址和密碼、以執行驗證程序。

   這些行動可讓BlueXP將您的nssa帳戶用於授權下載、軟體升級驗證、以及未來的支援註冊等項目。

   請注意下列事項：

   - NSS-帳戶必須是客戶層級的帳戶（而非來賓帳戶或暫存帳戶）。您可以擁有多個客戶層級的NSS帳戶。
   - 如果該帳戶是合作夥伴層級帳戶、則只能有一個NSS帳戶。如果您嘗試新增客戶層級的NSS帳戶、但有合作夥伴層級的帳戶存在、您會收到下列錯誤訊息：

     「此帳戶不允許使用新增服務客戶類型、因為已經有不同類型的新增服務使用者。」

   如果您擁有預先存在的客戶層級的NSS帳戶、並嘗試新增合作夥伴層級的帳戶、情況也是如此。

   - 成功登入後、NetApp會儲存NSS.使用者名稱。

     這是系統產生的ID、會對應至您的電子郵件。在「* nssn*管理*」頁面上、您可以從顯示電子郵件 ••• 功能表。

   - 如果您需要重新整理登入認證憑證權杖、也可以在中使用*更新認證*選項 ••• 功能表。

     使用此選項會提示您重新登入。請注意、這些帳戶的權杖會在90天後過期。系統會張貼通知、提醒您注意此點。

取得協助

NetApp以多種方式支援BlueXP及其雲端服務。我們全年無休提供豐富的免費自助支援選項、例如知識庫（KB）文章和社群論壇。您的支援註冊包括透過網路票證提供遠端技術支援。

取得雲端供應商檔案服務的支援

如需雲端供應商檔案服務、其基礎架構或任何使用服務的解決方案的相關技術支援、請參閱該產品的 BlueXP 文件中的「取得說明」。

- "Amazon FSX for ONTAP Sf"
- "Azure NetApp Files"
- "適用於 Google Cloud Cloud Volumes Service"

若要獲得 BlueXP 及其儲存解決方案與服務的專屬技術支援、請使用下列支援選項。

使用自我支援選項

這些選項可供免費使用、一天24小時、一週7天：

- 文件

  您目前正在檢視的BlueXP文件。

- "知識庫"

  請搜尋BlueXP知識庫、找出有助於疑難排解問題的文章。

- "社群"

  歡迎加入BlueXP社群、以追蹤後續討論或建立新討論。

利用**NetApp**支援建立案例

除了上述的自我支援選項、您也可以在啟動支援之後、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 NetApp 支援網站 認證與 BlueXP 登入建立關聯。 "瞭解如何管理與 BlueXP 登入相關的認證"。
- 如果您要為具有序號的 ONTAP 系統開啟案例、則您的 NSS 帳戶必須與該系統的序號相關聯。

步驟

1. 在 BlueXP 中、選取 * 說明 > 支援 * 。
2. 在「資源」頁面上、選擇「技術支援」下的其中一個可用選項：

   a. 如果您想與電話上的某人通話、請選取 * 致電 * 。您將會被導向netapp.com上的頁面、其中列出您可以撥打的電話號碼。

b. 選擇 * 建立案例 * 、與 NetApp 支援專家一起開啟 Ticket ：

- 服務：選取問題相關的服務。例如、特定於服務工作流程或功能的技術支援問題的BlueXP。
- 工作環境：如果適用於儲存設備、請選取* Cloud Volumes ONTAP 《》或《內部部署*》、然後選取相關的工作環境。

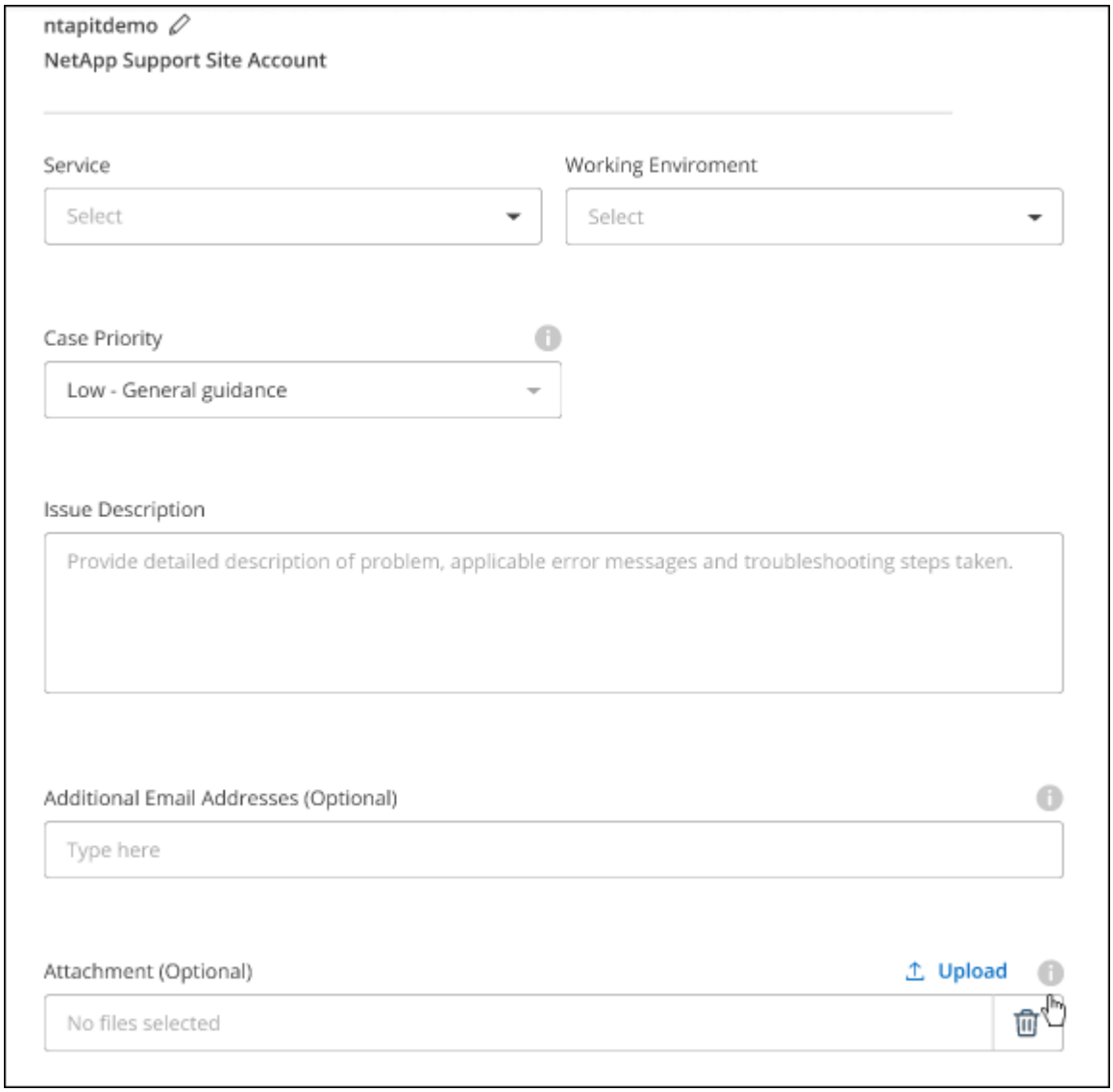
  工作環境清單位於您在服務的最上層橫幅中所選的BlueXP帳戶、工作區和Connector範圍內。

- 案例優先順序：選擇案例的優先順序、可以是低、中、高或嚴重。

  若要深入瞭解這些優先順序、請將滑鼠游標暫留在欄位名稱旁的資訊圖示上。

- 問題說明：提供問題的詳細說明、包括任何適用的錯誤訊息或您執行的疑難排解步驟。
- 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（選填） * ：上傳最多五個附件、一次上傳一個。

  每個檔案的附件上限為 25 MB 。支援下列副檔名： txt 、 log 、 pdf 、 jpg/jpeg 、 rtf 、 doc/dox 、 xls/xlsx 和 csv 。



完成後

您的支援案例編號會出現快顯視窗。NetApp支援專家將會審查您的案例、並盡快回覆您。

如需支援案例的記錄、您可以選取 * 設定 > 時間軸 * 、然後尋找名為「建立支援案例」的動作。 最右側的按鈕可讓您展開動作以查看詳細資料。

嘗試建立案例時、可能會遇到下列錯誤訊息：

"您無權針對所選服務建立案例"

此錯誤可能表示、與該帳戶相關聯的NSS帳戶及記錄公司與BlueXP帳戶序號的記錄公司不同（例如960xxxx)或工作環境序號。您可以使用下列其中一個選項尋求協助：

- 使用產品內對談
- 請至提交非技術案例 https://mysupport.netapp.com/site/help

管理支援案例（預覽）

您可以直接從BlueXP檢視及管理作用中和已解決的支援案例。您可以管理與您的NSS帳戶和貴公司相關的個案。

案例管理可透過預覽取得。我們計畫改善這項體驗、並在即將推出的版本中加入增強功能。請使用產品內建聊天功能、向我們傳送意見反應。

請注意下列事項：

- 頁面頂端的案例管理儀表板提供兩種檢視：
  - 左側檢視顯示您所提供的使用者nssc帳戶在過去3個月內開啟的個案總數。
  - 右側檢視顯示過去3個月內、貴公司層級根據您的使用者nssc帳戶所開啟的個案總數。

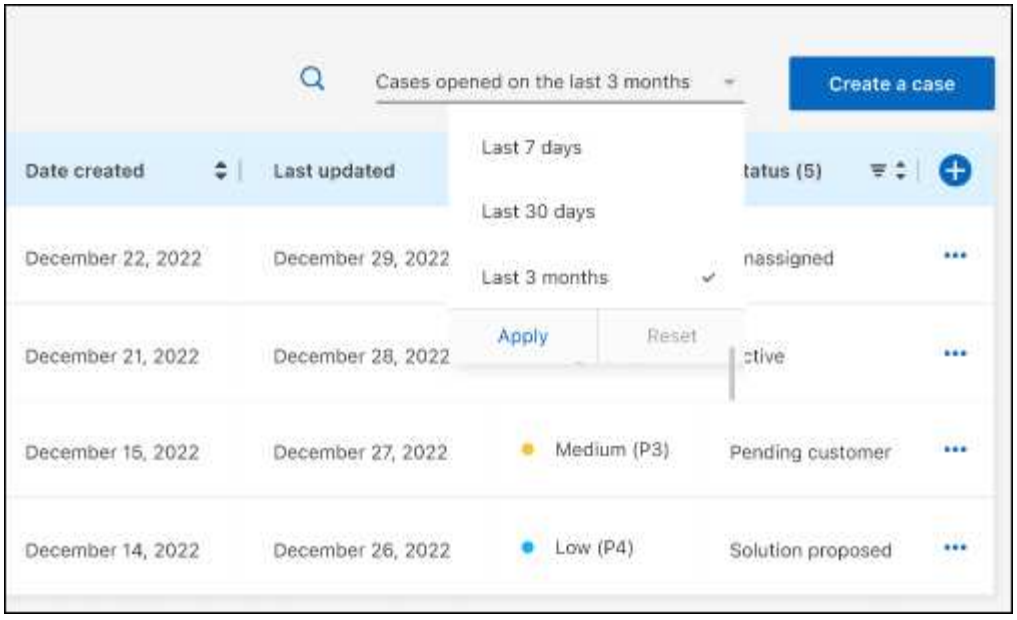
  表格中的結果會反映您所選檢視的相關個案。
- 您可以新增或移除感興趣的欄、也可以篩選優先順序和狀態等欄的內容。其他欄則只提供排序功能。

  如需詳細資料、請參閱下列步驟。
- 在個別案例層級、我們提供更新案例附註或關閉尚未處於「已結案」或「待結案」狀態的案例的功能。

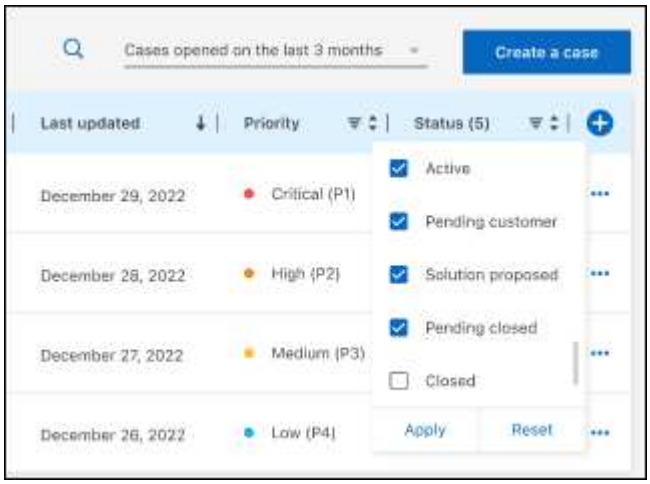
步驟

1. 在 BlueXP 中、選取 * 說明 > 支援 * 。
2. 選取 * 個案管理 * 、如果出現提示、請將您的 NSS 帳戶新增至 BlueXP 。

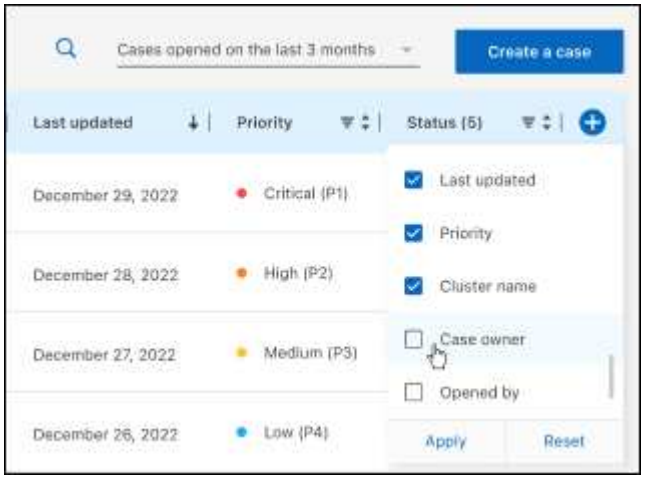
   「個案管理」頁面會顯示與您的BlueXP使用者帳戶相關聯的與NSS帳戶相關的未決個案。這是顯示在「* nssnmanagement *」頁面頂端的相同nss.帳戶。
3. （可選）修改表格中顯示的資訊：
   - 在 * 組織案例 * 下、選取 * 檢視 * 以檢視與貴公司相關的所有案例。
   - 選擇確切的日期範圍或選擇不同的時間範圍、以修改日期範圍。



◦ 篩選欄的內容。



◦ 選取以變更表格中顯示的欄 ⊕ 然後選擇您要顯示的欄。

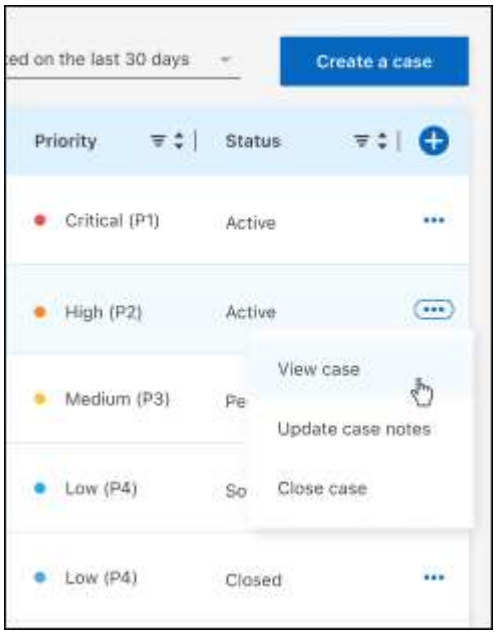


4. 選取以管理現有案例 ••• 並選擇其中一個可用選項：

- 檢視案例：檢視特定案例的完整詳細資料。
- * 更新案例附註 * ：提供問題的其他詳細資料、或選擇 * 上傳檔案 * 最多附加五個檔案。

  每個檔案的附件上限為 25 MB 。支援下列副檔名： txt 、 log 、 pdf 、 jpg/jpeg 、 rtf 、 doc/dox 、 xls/xlsx 和 csv 。

- * 結案案例 * ：提供結案原因的詳細資料、並選取 * 結案案例 * 。



法律聲明

法律聲明提供版權聲明、商標、專利等存取權限。

版權

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp 、 NetApp 標誌及 NetApp 商標頁面上列出的標章均為 NetApp 、 Inc. 的商標。其他公司與產品名稱可能為其各自所有者的商標。

"https://www.netapp.com/company/legal/trademarks/"

專利

如需最新的 NetApp 擁有專利清單、請參閱：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隱私權政策

"https://www.netapp.com/company/legal/privacy-policy/"

開放原始碼

通知檔案提供有關 NetApp 軟體所使用之協力廠商版權與授權的資訊。

- "藍圖XP注意事項"
- "關於此問題的聲明Cloud Volumes ONTAP"
- "關於本產品的注意事項ONTAP"