概念
Cloud Manager 3.7

NetApp
March 25, 2024

目錄

概念

Cloud Manager與Cloud Volumes ONTAP 概述

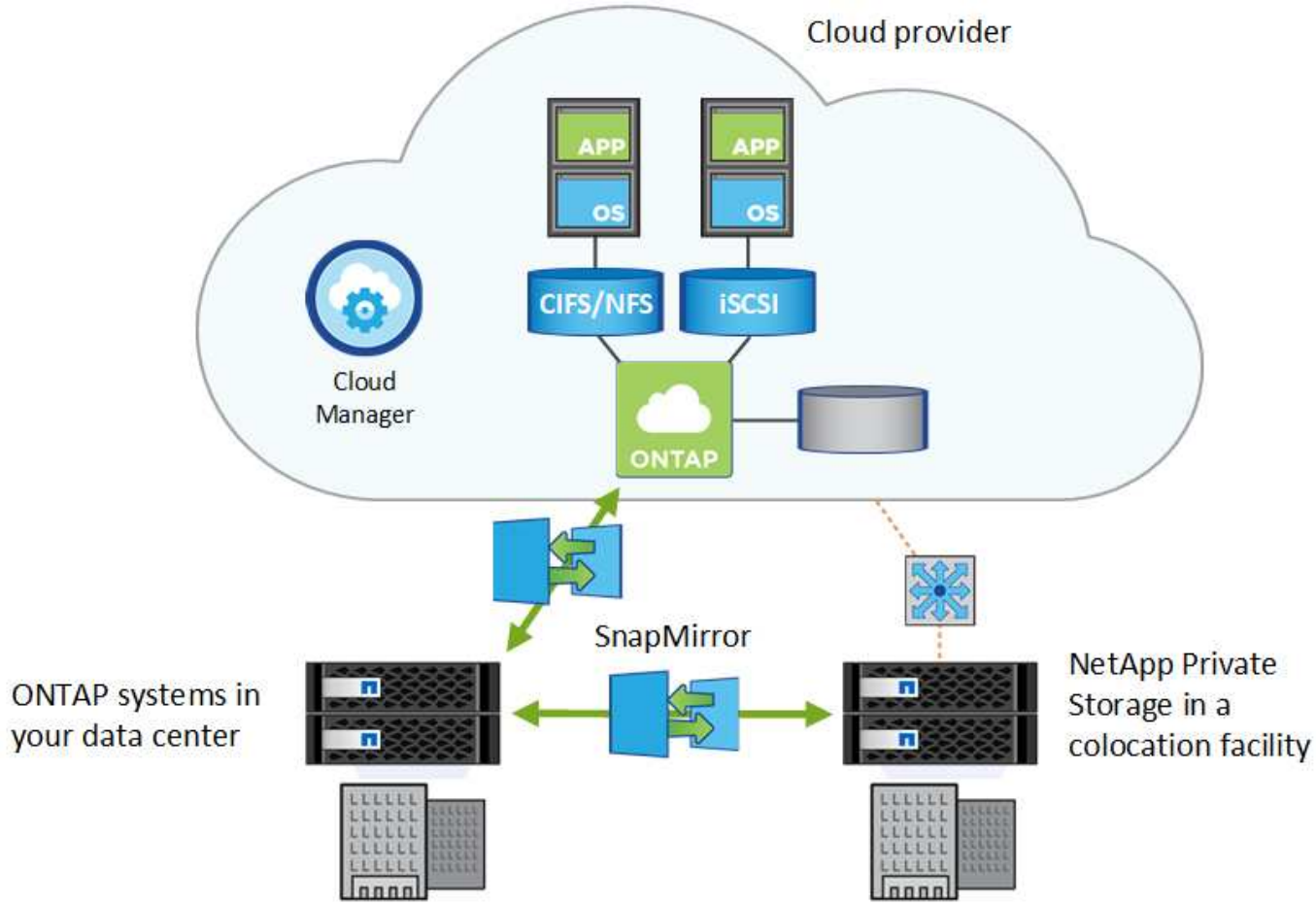
Cloud Manager可讓您部署Cloud Volumes ONTAP 支援企業級雲端儲存功能的功能、並可在NetApp建置的混合雲之間輕鬆複寫資料。

Cloud Manager

Cloud Manager的建置考量十分簡單。本指南將引導您完成Cloud Volumes ONTAP 功能完善的設定、提供簡化的儲存資源配置與自動化容量管理、並可在混合雲之間進行拖放式資料複寫等功能、進而簡化資料管理。

Cloud Manager需要部署和管理Cloud Volumes ONTAP 功能、但也可以探索及配置內部部署ONTAP 的內部部署式叢集儲存設備。這可為您的雲端和內部部署儲存基礎架構提供集中控管點。

您可以在雲端或網路上執行Cloud Manager、只需連線至您要部署Cloud Volumes ONTAP 的網路即可。下圖顯示Cloud Manager與Cloud Volumes ONTAP 在雲端供應商中執行的功能。同時也顯示混合雲之間的資料複寫。



"深入瞭解 Cloud Manager"

Cloud Volumes ONTAP

僅有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您可以使

用Cloud Volumes ONTAP 支援功能來執行正式作業工作負載、災難恢復、DevOps、檔案共享和資料庫管理。

利用下列主要功能、將企業儲存設備延伸至雲端：Cloud Volumes ONTAP

- 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。
- 高可用度可確保在雲端環境發生故障時、企業的可靠性和持續營運。
- 資料複寫Cloud Volumes ONTAP 功能利用NetApp領先業界的SnapMirror複寫技術、將內部部署資料複寫到雲端、因此可輕鬆將次要複本用於多種使用案例。
- 在高效能與低效能儲存資源池之間進行資料分層切換、無需讓應用程式離線。
- 應用程式一致性可確保使用NetApp SnapCenter 功能的NetApp Snapshot複本一致性。

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"

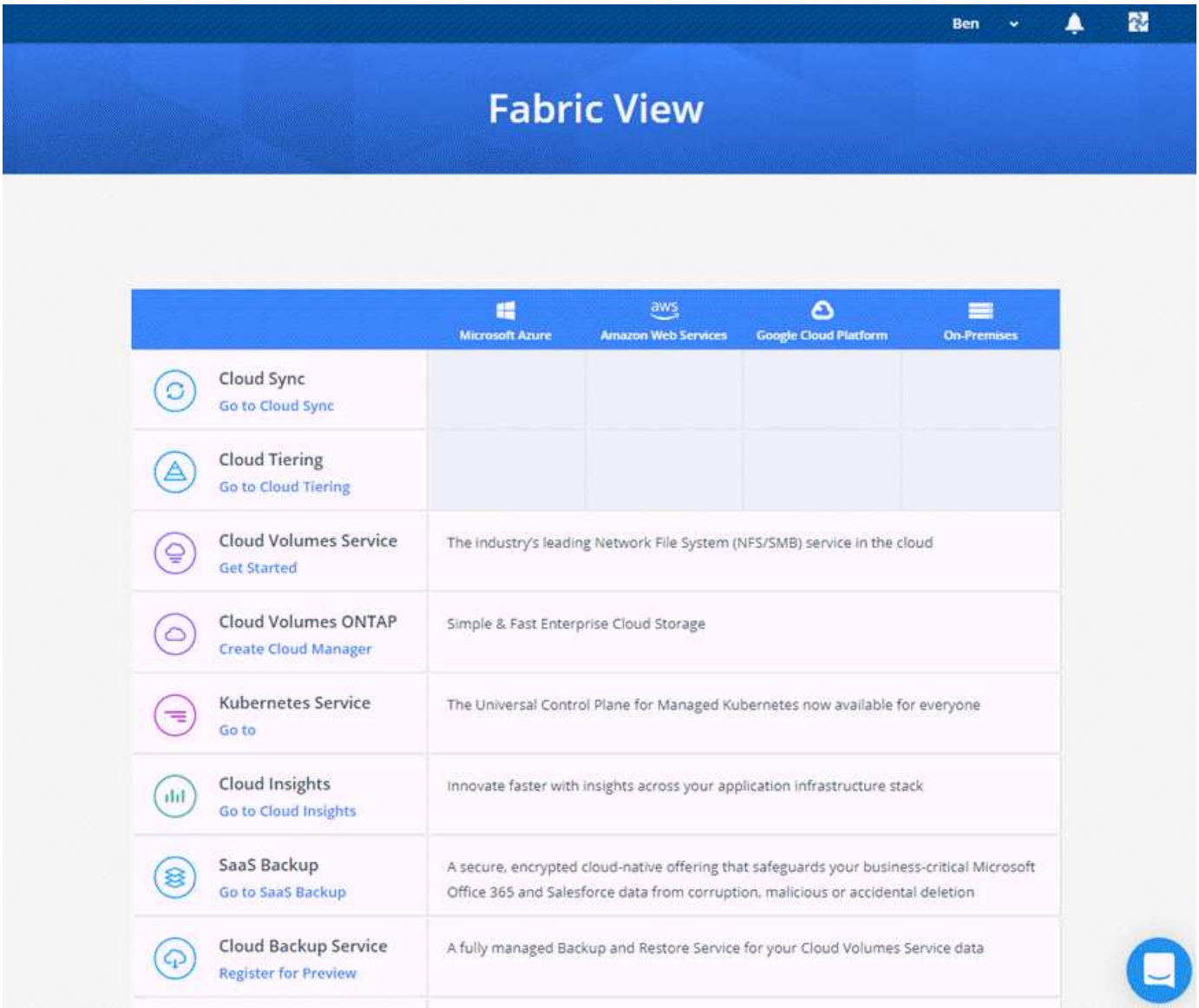
"深入瞭 Cloud Volumes ONTAP 解功能"

NetApp Cloud Central

"NetApp Cloud Central" 提供集中位置以存取及管理NetApp雲端資料服務。這些服務可讓您在雲端上執行關鍵應用程式、建立自動化的DR站台、備份SaaS資料、以及在多個雲端之間有效地移轉和控制資料。

Cloud Manager與NetApp Cloud Central的整合提供多項優點、包括簡化部署體驗、單一位置即可檢視及管理多個Cloud Manager系統、以及集中式使用者驗證。

透過集中式使用者驗證、您可以在Cloud Manager系統之間、Cloud Manager與Cloud Sync 其他資料服務（例如：）之間使用相同的認證資料集。如果您忘記密碼、也很容易重設密碼。



Cloud Central帳戶

每個Cloud Manager系統都會與_NetApp Cloud Central帳戶建立關聯。Cloud Central帳戶提供多租戶共享、可讓您在隔離的工作區中組織使用者和資源。

Cloud Central帳戶可實現多租戶共享：

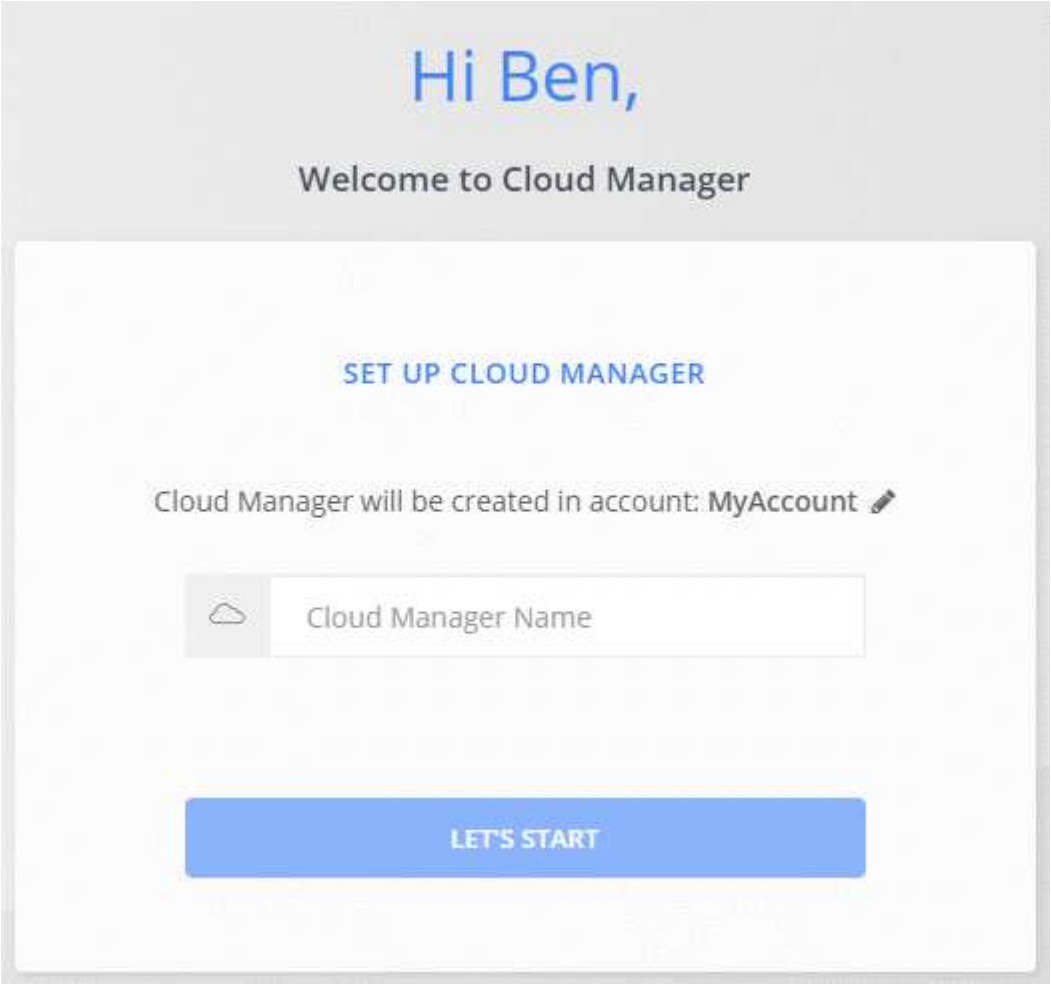
- 單一Cloud Central帳戶可包含多個Cloud Manager系統、以滿足不同的業務需求。

  由於使用者與Cloud Central帳戶相關聯、因此不需要為每個Cloud Manager系統設定使用者。

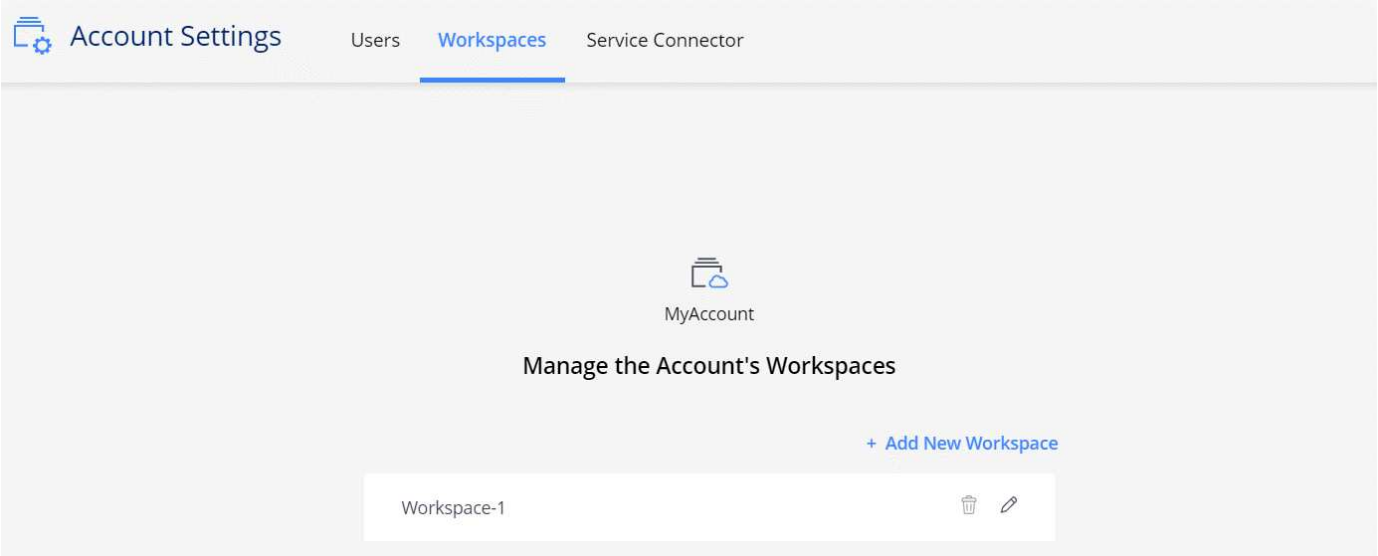
- 在每個Cloud Manager系統中、有多位使用者可以在Cloud Volumes ONTAP 稱為工作區的隔離環境中部署及管理功能完善的系統。

  除非共用這些工作區、否則其他使用者無法看到這些工作區。

部署Cloud Manager時、您可以選取要與系統建立關聯的Cloud Central帳戶：



接著、帳戶管理員可以管理使用者、工作區和服務連接器、藉此修改此帳戶的設定：



如需逐步指示、請參閱 "設定 Cloud Central 帳戶"。

> Cloud Manager需要存取_\https://cloudmanager.cloud.netapp.com_才能連線至Cloud Central帳戶服務。在防火牆上開啟此URL、以確保Cloud Manager可以聯絡該服務。

使用者、工作區和服務連接器

Cloud Manager 中的「帳戶設定」小工具可讓帳戶管理員管理 Cloud Central 帳戶。如果您剛建立帳戶、就會從頭開始。但如果您已經設定帳戶、您會看到_所有_與帳戶相關聯的使用者、工作區和服務連接器。

使用者

這些是您與Cloud Central帳戶建立關聯的NetApp Cloud Central使用者。將使用者與該帳戶中的帳戶和一或多個工作區建立關聯、可讓這些使用者在 Cloud Manager 中建立及管理工作環境。

當您建立使用者關聯時、您會指派一個角色給他們：

- *Account admin* ：可在 Cloud Manager 中執行任何動作。
- _Workspace 管理 _ ：可在指派的工作區中建立及管理資源。

工作區

在 Cloud Manager 中、工作區會將任何數量的工作環境與其他工作環境隔離。除非帳戶管理員將該管理員與該工作區建立關聯、否則 Workspace 系統管理員無法存取工作區中的工作環境。

工作環境代表儲存系統：

- 單節點 Cloud Volumes ONTAP 的不完整系統或 HA 配對
- 您網路中的內部部署 ONTAP 式叢集
- NetApp 私有儲存組態中的一個叢集 ONTAP

服務連接器

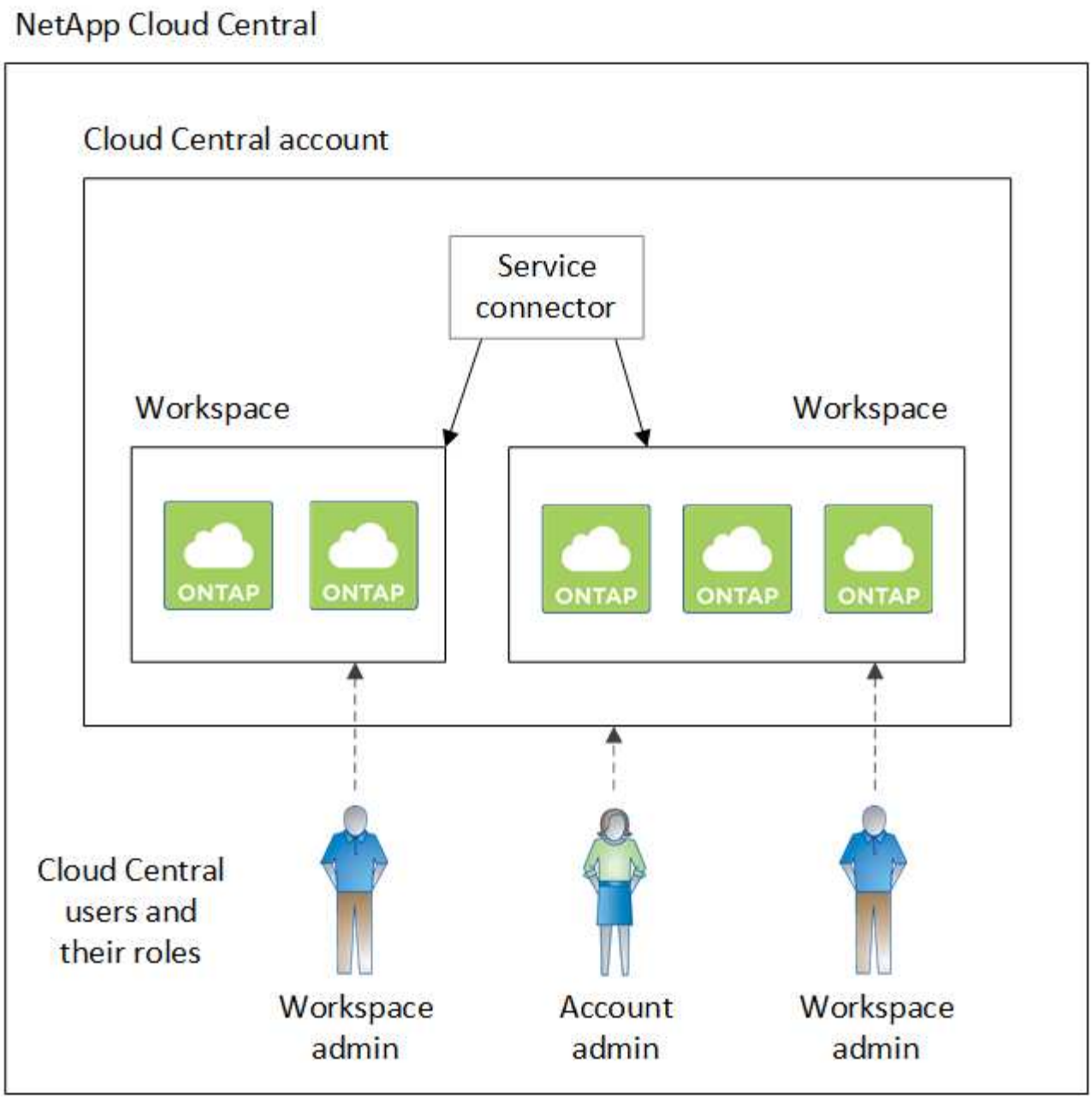
服務連接器是Cloud Manager的一部分。它執行大部分的Cloud Manager軟體（例如使用者介面）、除了它所連線的幾項Cloud Central服務（auth0和Cloud Central帳戶）。服務連接器可在部署於雲端供應商的虛擬機器執行個體上執行、或是在您設定的內部部署主機上執行。

您可以將服務連接器與多個NetApp雲端資料服務搭配使用。例如、如果您已經有Cloud Manager的服務連接器、則可在設定Cloud Tiering服務時加以選取。

範例

以下範例顯示使用兩個工作區來建立孤立環境Cloud Volumes ONTAP 的帳戶。例如、其中一個工作區可能用於接移環境、另一個工作區則用於正式作業環境。

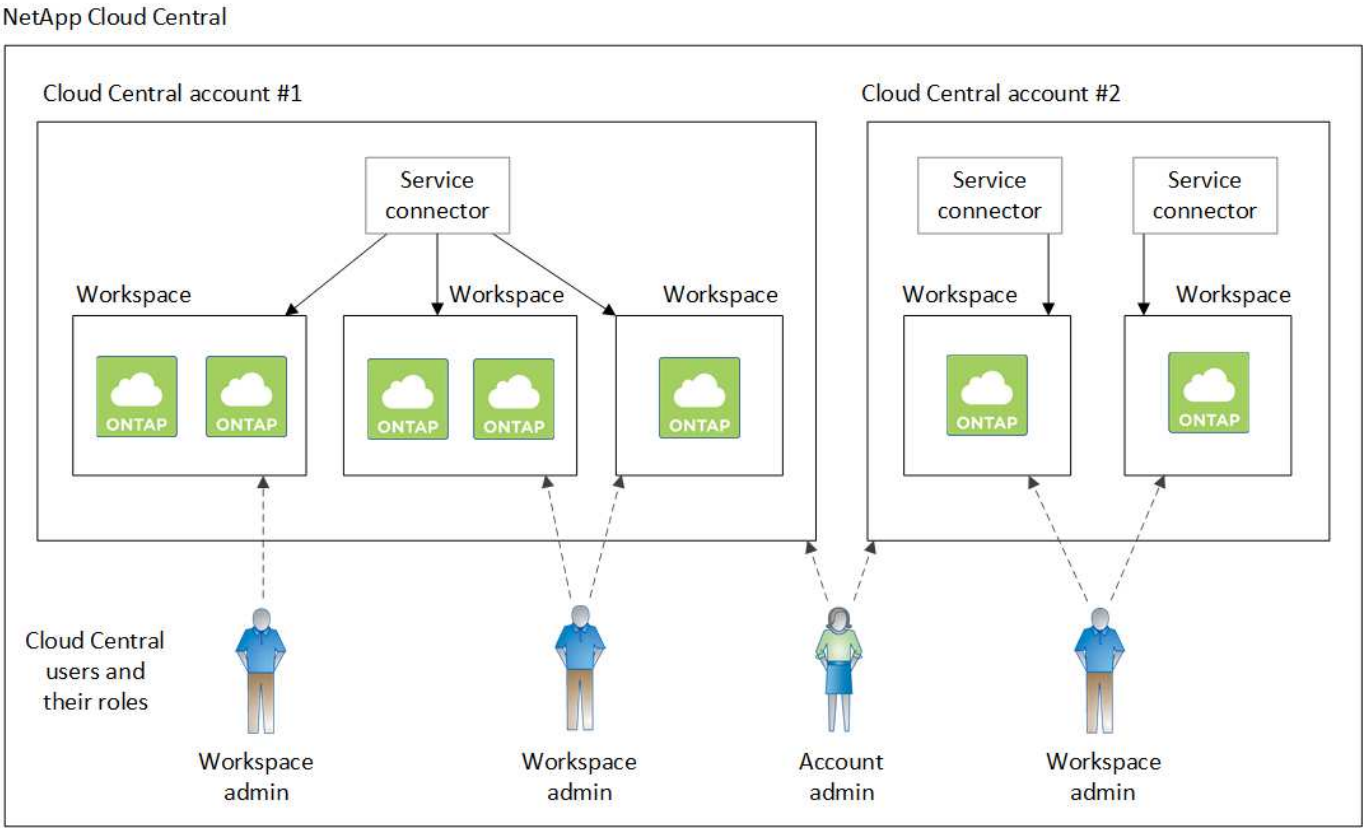
> Cloud Manager和Cloud Volumes ONTAP 這個功能不屬於NetApp Cloud Central帳戶、而是在雲端供應商中執行。這是每個元件之間關係的概念呈現。



以下是使用兩個獨立 Cloud Central 帳戶、顯示最高層級的多租戶共享的另一個範例。例如、服務供應商可能會在一個Cloud Central帳戶中使用Cloud Manager來為客戶提供服務、而使用另一個帳戶來為其中一個業務單位提供災難恢復。

請注意、帳戶2包含兩個獨立的服務連接器。如果您的系統位於不同的地區、或是位於不同的雲端供應商、就可能發生這種情況。

> 同樣地、Cloud Manager和Cloud Volumes ONTAP 整個系統並未真正位於NetApp Cloud Central帳戶中、而是在雲端供應商中執行。這是每個元件之間關係的概念呈現。



與Cloud Central帳戶整合的常見問題集

在您升級至Cloud Manager 3.7之後的一段時間內、NetApp會選擇特定的Cloud Manager系統來與Cloud Central帳戶整合。此常見問題集可回答您對此程序可能有的問題。

程序需要多久時間？

只需幾分鐘。

Cloud Manager是否無法使用？

否、您仍可存取Cloud Manager系統。

關於此功能呢 **Cloud Volumes ONTAP** ？

您的整個系統不會中斷運作Cloud Volumes ONTAP 。

在此過程中會發生什麼事？

NetApp會在整合程序中執行下列作業：

1. 建立新的Cloud Central帳戶、並將其與Cloud Manager系統建立關聯。
2. 指派新角色給每位現有使用者：
    - Cloud Manager管理員成為帳戶管理員
    - 租戶管理員和工作環境管理員會成為Workspace Admins

3. 建立取代現有租戶的工作區。
4. 將您的工作環境放在這些工作區中。
5. 將服務連接器與所有工作區建立關聯。

我的**Cloud Manager**系統安裝位置是否重要？

不可以無論系統位於AWS、Azure或內部部署環境、NetApp都能將其與Cloud Central帳戶整合。

雲端供應商帳戶

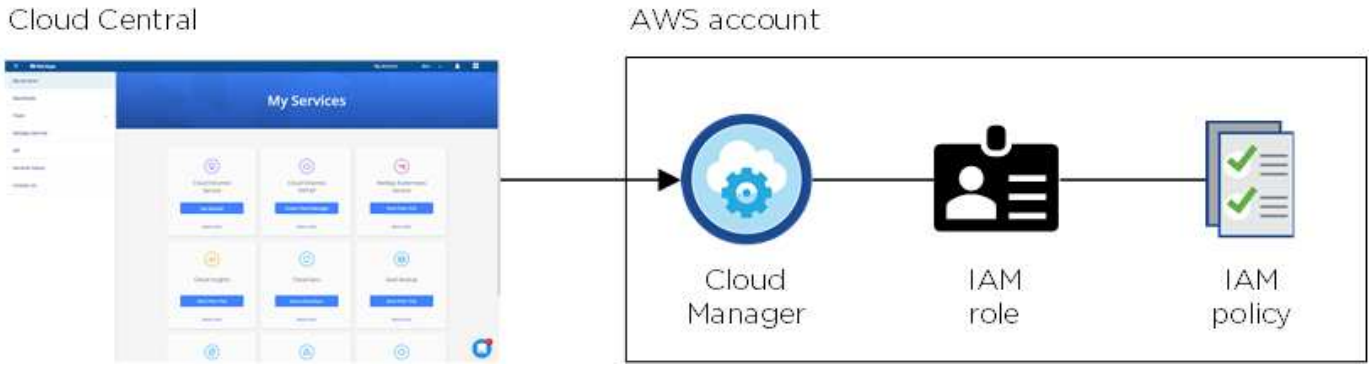
AWS帳戶和權限

Cloud Manager可讓您選擇想要部署Cloud Volumes ONTAP 的AWS帳戶。您可以在Cloud Volumes ONTAP 初始AWS帳戶中部署所有的整套系統、也可以設定其他帳戶。

初始**AWS**帳戶

從NetApp Cloud Central部署Cloud Manager時、您需要使用具有啟動Cloud Manager執行個體權限的AWS帳戶。所需權限列於 "適用於AWS的NetApp Cloud Central原則"。

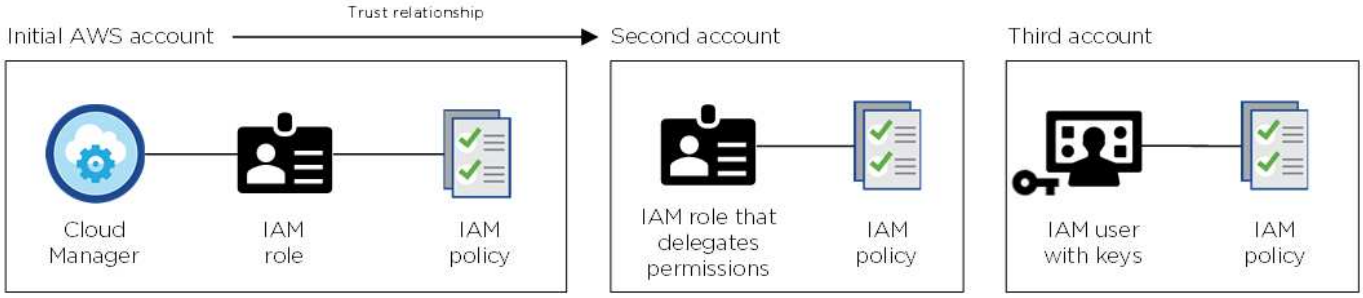
Cloud Central在AWS中啟動Cloud Manager執行個體時、會為執行個體建立IAM角色和執行個體設定檔。它也附加原則、讓Cloud Manager有權限在Cloud Volumes ONTAP 該AWS帳戶中部署及管理功能。 "檢閱 Cloud Manager 如何使用權限"。



Cloud Manager會在您建立新的工作環境時、依預設選取此雲端供應商帳戶：

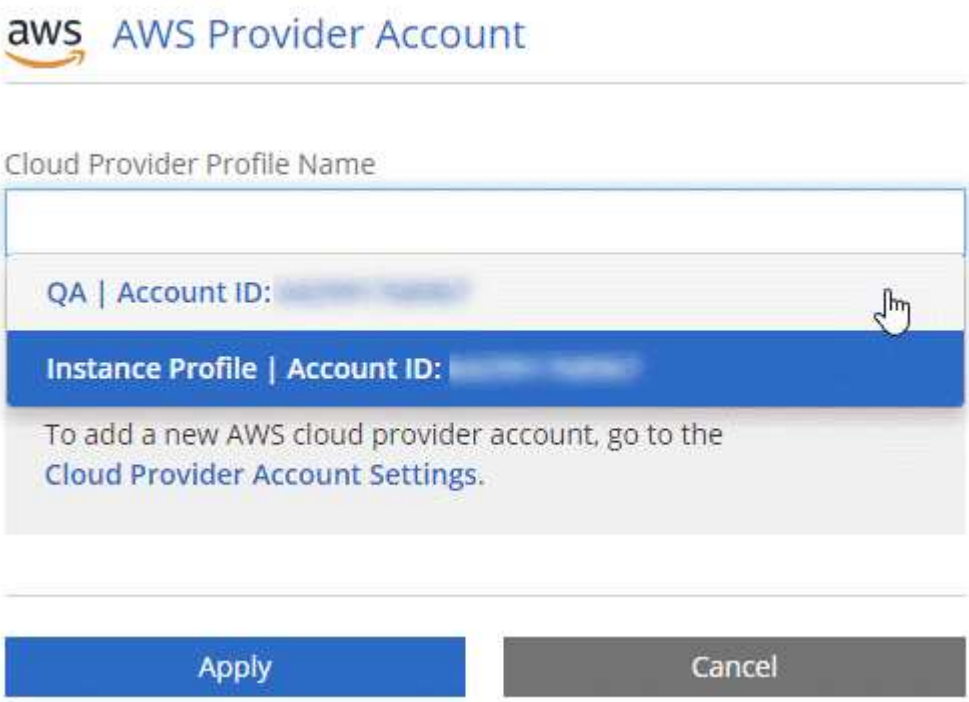
其他**AWS**帳戶

如果您想要在 Cloud Volumes ONTAP 不同的 AWS 帳戶中啟動功能、您也可以選擇 "為 IAM 使用者或信任帳戶中角色的 ARN 提供 AWS 金鑰"。下圖顯示兩個額外的帳戶、一個透過信任帳戶中的 IAM 角色提供權限、另一個則透過 IAM 使用者的 AWS 金鑰提供權限：



您可以 "將雲端供應商帳戶新增至Cloud Manager" 指定 IAM 角色的 Amazon 資源名稱（ARN）或 IAM 使用者的 AWS 金鑰。

新增其他帳戶之後、您可以在建立新的工作環境時切換至該帳戶：



Marketplace 部署和內部部署呢？

以上各節說明NetApp Cloud Central建議的部署方法。您也可以從部署Cloud Manager至AWS "AWS Marketplace" 您也可以 "在內部部署中安裝Cloud Manager"。

如果您使用 Marketplace 、則會以相同方式提供權限。您只需要手動建立和設定 IAM 角色、然後為任何其他帳戶提供權限。

對於內部部署、您無法為 Cloud Manager 系統設定 IAM 角色、但您可以像提供額外 AWS 帳戶一樣提供權限。

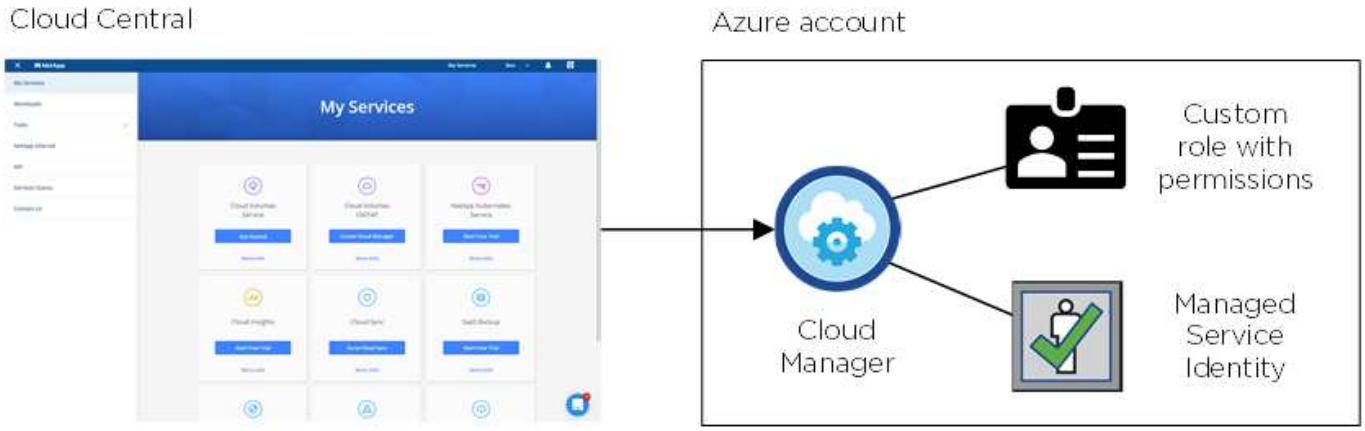
Azure帳戶與權限

Cloud Manager可讓您選擇要部署Cloud Volumes ONTAP 的Azure帳戶。您可以在Cloud Volumes ONTAP 初始Azure帳戶中部署所有的整套系統、也可以設定其他帳戶。

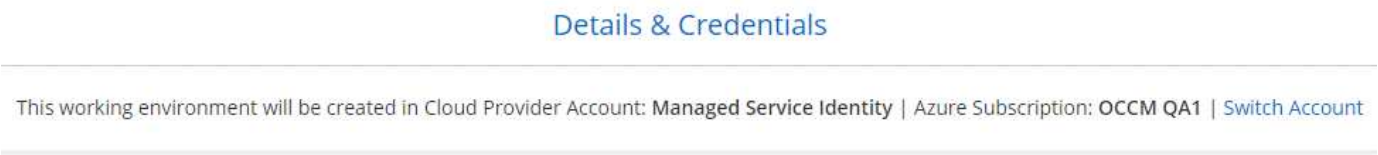
初始Azure帳戶

從NetApp Cloud Central部署Cloud Manager時、您需要使用具備部署Cloud Manager虛擬機器權限的Azure帳戶。所需權限列於 "適用於Azure的NetApp Cloud Central原則"。

當Cloud Central在Azure中部署Cloud Manager虛擬機器時 "系統指派的託管身分識別" 在Cloud Manager虛擬機器上、建立自訂角色、並將其指派給虛擬機器。此角色可讓Cloud Manager在Cloud Volumes ONTAP 該Azure訂閱中部署及管理功能。 "檢閱 Cloud Manager 如何使用權限"。



Cloud Manager會在您建立新的工作環境時、依預設選取此雲端供應商帳戶：

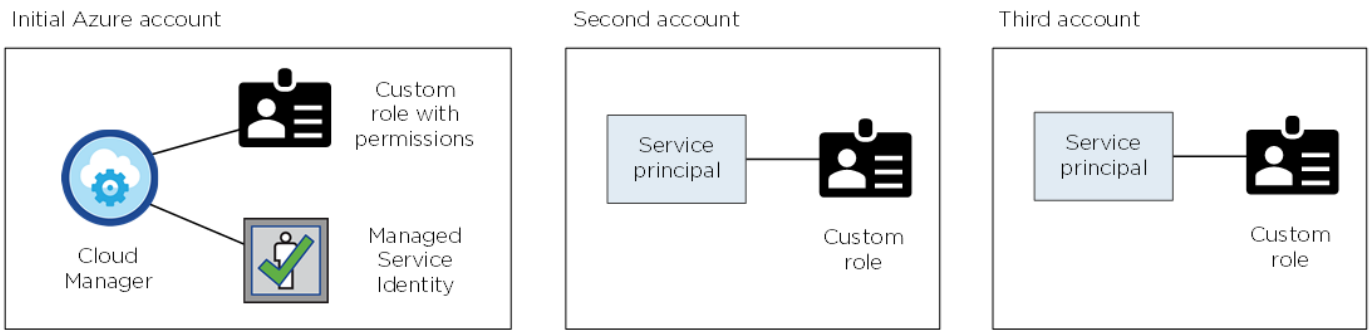


初始帳戶的額外Azure訂閱

託管身分識別與您啟動Cloud Manager的訂閱相關。如果您想要選擇不同的 Azure 訂閱、則需要 "將託管身分識別與這些訂閱建立關聯"。

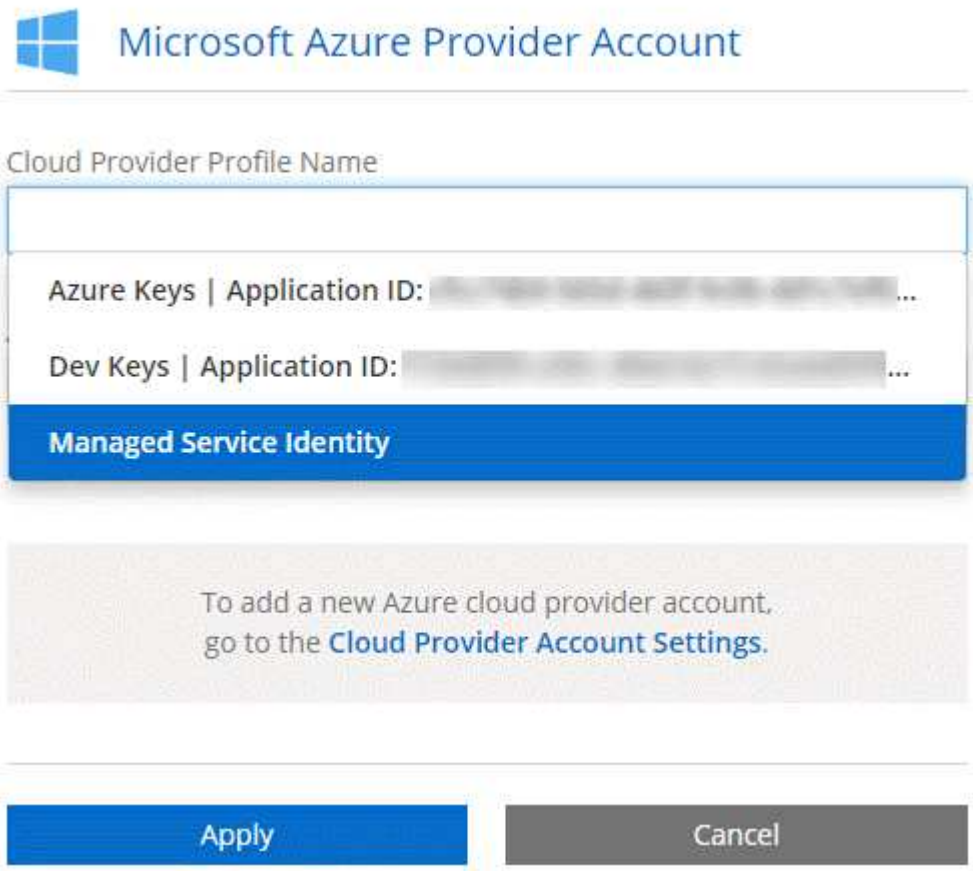
其他Azure帳戶

如果您想要在Cloud Volumes ONTAP 不同的Azure帳戶中部署功能、則必須授予所需的權限 "在 Azure Active Directory 中建立及設定服務主體" 針對每個 Azure 帳戶。下圖顯示兩個額外的帳戶、每個帳戶都設有提供權限的服務主體和自訂角色：



您可以 "將雲端供應商帳戶新增至Cloud Manager" 提供 AD 服務主體的詳細資料。

新增其他帳戶之後、您可以在建立新的工作環境時切換至該帳戶：



Marketplace 部署和內部部署呢？

以上各節說明NetApp Cloud Central建議的部署方法。您也可以從部署Cloud Manager至Azure "Azure Marketplace"您也可以 "在內部部署中安裝Cloud Manager"。

如果您使用 Marketplace 、則會以相同方式提供權限。您只需要手動建立及設定Cloud Manager的託管身分識別、然後為任何其他帳戶提供權限。

對於內部部署、您無法為Cloud Manager系統設定託管身分識別、但您可以像提供其他帳戶一樣提供權限。

Google Cloud 專案、權限和帳戶

服務帳戶可讓 Cloud Manager 在 Cloud Volumes ONTAP Cloud Manager 的同一個專案中、或在不同專案中、擁有部署和管理這些系統的權限。您新增至 Cloud Manager 的 Google Cloud 帳戶可用於進行資料分層。

Cloud Manager 的專案與權限

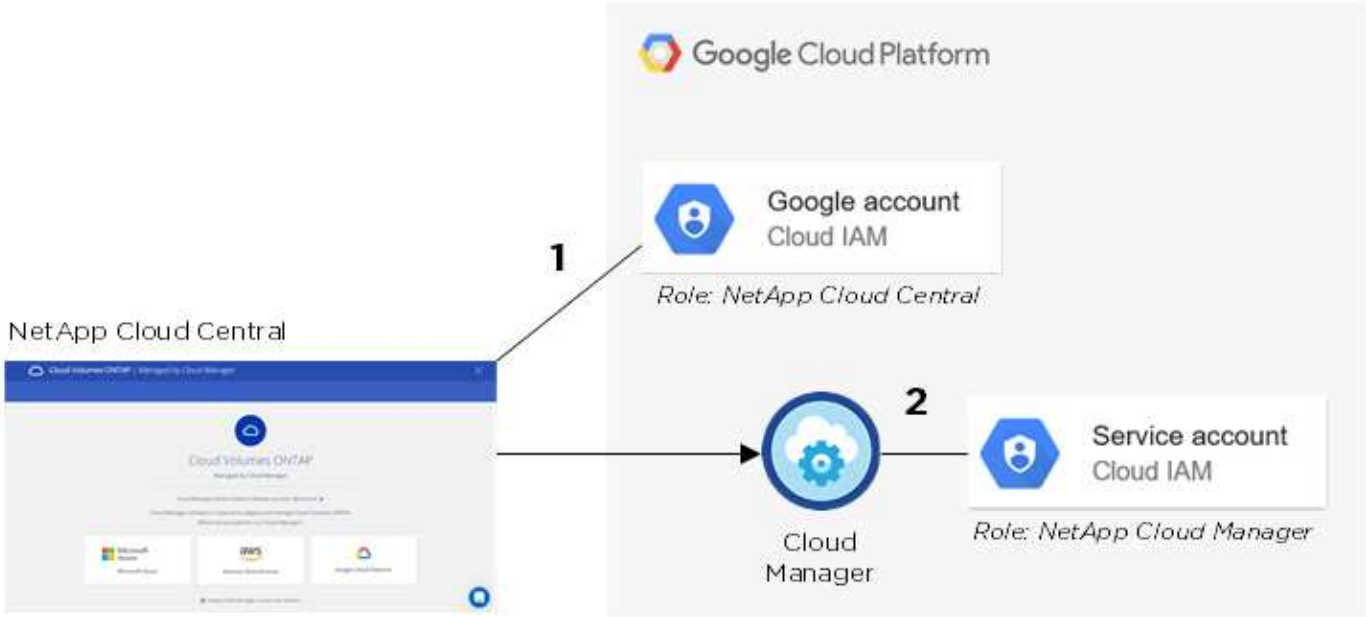
在Cloud Volumes ONTAP Google Cloud中部署時、您必須先在Google Cloud專案中部署Cloud Manager。Cloud Manager無法在您的內部部署環境或其他雲端供應商中執行。

部署Cloud Manager之前、必須先設定兩組權限 "NetApp Cloud Central"：

1. 您需要使用具有從Cloud Central啟動Cloud Manager VM執行個體權限的Google帳戶來部署Cloud Manager。
2. 部署Cloud Manager時、系統會提示您選取 "服務帳戶" 適用於 VM 執行個體。Cloud Manager 可從服務帳戶取得權限 Cloud Volumes ONTAP 、代表您建立及管理各種系統。將自訂角色附加至服務帳戶、即可提供權限。

我們已設定兩個 Y反 洗錢檔案、其中包含使用者和服務帳戶所需的權限。 "瞭解如何使用 Yaml 檔案來設定權限"。

下圖說明上述第 1 和第 2 項所述的權限要求：



適用於此產品的專案 Cloud Volumes ONTAP

可與Cloud Manager位於同一個專案中、或是位於不同的專案中。Cloud Volumes ONTAP若要在Cloud Volumes ONTAP 不同的專案中部署功能、您必須先將Cloud Manager服務帳戶和角色新增至該專案。

- "瞭解如何設定Cloud Manager服務帳戶（請參閱步驟4）"。
- "瞭解如何在 Cloud Volumes ONTAP GCP 中部署功能、並選擇專案"。

負責資料分層

需要在Cloud Manager中新增Google Cloud帳戶、才能在Cloud Volumes ONTAP 支援資料的系統上分層處理資料。資料分層會自動將冷資料分層至低成本的物件儲存設備、讓您回收主儲存設備的空間、並縮減二線儲存設備。

新增帳戶時、您必須為具有 Storage Admin 權限的服務帳戶、提供 Cloud Manager 儲存設備存取金鑰。Cloud Manager 使用存取金鑰來設定及管理雲端儲存庫、以利資料分層。

新增 Google Cloud 帳戶之後、您就可以在建立、修改或複寫個別磁碟區時、在這些磁碟區上啟用資料分層功能。

- "瞭解如何設定 GCP 帳戶、並將其新增至 Cloud Manager"。
- "瞭解如何將非作用中資料分層至低成本物件儲存設備"。

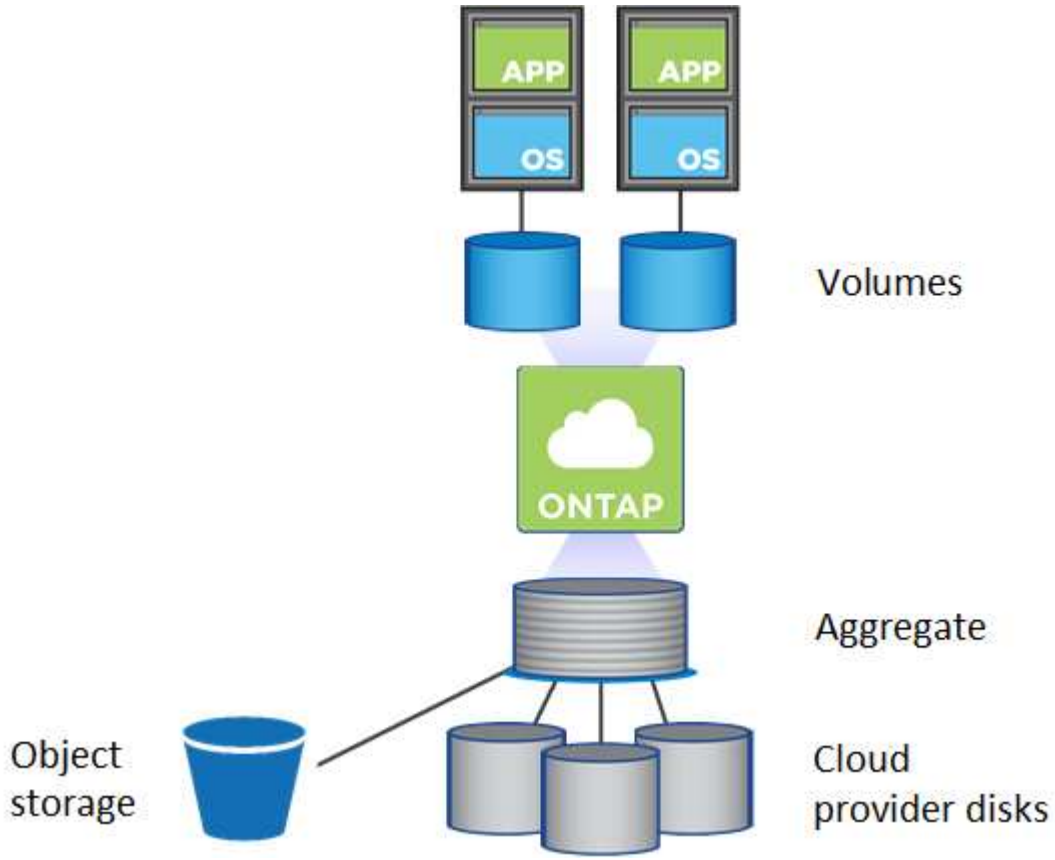
儲存設備

磁碟與集合體

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

總覽

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



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

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

AWS 儲存設備

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

EBS 儲存設備

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

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

EBS 磁碟類型的差異較高、如下所示：

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

> HA 組態和資料分層不支援冷 HDD 磁碟。

本機 **NVMe** 儲存設備

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

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

Azure 儲存設備

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

單一節點系統

單一節點系統可使用三種 Azure 託管磁碟：

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

  每種託管磁碟類型的磁碟大小上限為 32 TB 。

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

HA 配對

HA 配對使用 Premium 分頁區、磁碟大小上限為 8 TB 。

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

GCP 儲存設備

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

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

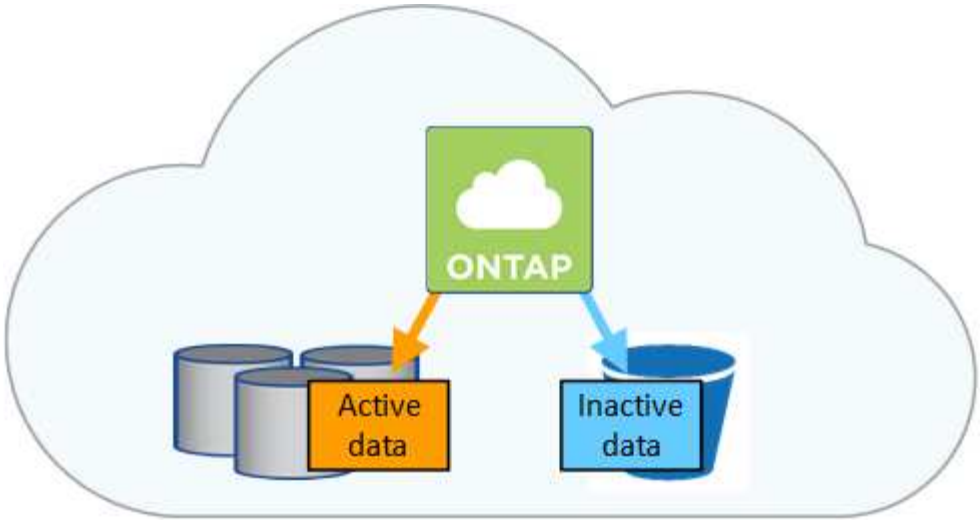
- 相關連結 *
- "Google Cloud Platform 文件：儲存選項"
- "檢閱 Cloud Volumes ONTAP GCP 中的儲存限制"

RAID 類型

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

資料分層總覽

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



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

您不需要安裝功能授權、就能啟用資料分層FabricPool （例如、）。

AWS 中的資料分層

當您在 AWS 中啟用資料分層功能時、 Cloud Volumes ONTAP VMware 會使用 EBS 做為熱資料的效能層、而 AWS S3 則是非作用中資料的容量層。變更系統分層層級可讓您選擇不同的S3儲存類別。

效能層級

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

容量層

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

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

分層層級

如果您不打算存取非作用中資料、您可以將系統的分層層級變更為下列其中一項、藉此降低儲存成本：*Intelligent Tiering* _、_*One Zone Inoti*頻頻 存取_或_*Standard-in*頻繁 存取。當您變更分層層級時、非作用中的資料會從Standard儲存類別開始、並移至您選取的儲存類別、如果資料在30天後仍未存取。

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

建立系統之後、就可以變更分層層級。如需詳細資訊、請參閱 "將非作用中資料分層至低成本物件儲存設備"。

分層層級是全系統層級、並非每個Volume。

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。變更系統分層層級可讓您選擇不同的Azure儲存層。

效能層級

效能層可以是 SSD 或 HDD 。

容量層

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

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

分層層級

如果您不打算存取非作用中資料、可以將系統的分層層級變更為Azure _cool儲存層、藉此降低儲存成本。當您變更分層層級時、非作用中的資料會從熱儲存層開始、並移至冷卻儲存層（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、因此在變更分層層級之前、請先將此納入考量。 "深入瞭解 Azure Blob 儲存設備存取層"。

建立系統之後、就可以變更分層層級。如需詳細資訊、請參閱 "將非作用中資料分層至低成本物件儲存設備"。

分層層級是全系統層級、並非每個Volume。

GCP 中的資料分層

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

效能層級

效能層可以是 SSD 或 HDD （標準磁碟）。

容量層

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

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

分層層級

目前不支援其他GCP儲存類別。

資料分層和容量限制

如果您啟用資料分層、系統的容量限制會維持不變。此限制分佈於效能層和容量層。

Volume 分層原則

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

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

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

僅適用於 **Snapshot**

當 Aggregate 達到 50% 容量後、 Cloud Volumes ONTAP 將不會與作用中檔案系統相關聯的 Snapshot 複本的 Cold 使用者資料分層至容量層。冷卻期約為 2 天。

如果讀取、容量層上的冷資料區塊會變熱、並移至效能層。

自動

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

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

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

無

將磁碟區的資料保留在效能層中、避免移至容量層。

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

關閉 Cloud Volumes ONTAP 此功能會影響冷卻期間

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

- 自動： 31 天
- 僅 Snapshot ： 2 天

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

設定資料分層

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

儲存管理

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

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

儲存資源配置

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

簡化資源配置

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

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

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

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

帳戶管理員可從 * 設定 * 頁面修改可用空間臨界值。

AWS 中集合體的磁碟大小選擇

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

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

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

您可以使用進階配置選項自行選擇磁碟大小。

進階分配

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

容量管理

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

自動容量管理

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

下列範例說明此模式的運作方式：

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

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

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

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

利用自動容量管理來管理 **inode**

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

手動容量管理

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

WORM 儲存設備

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

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

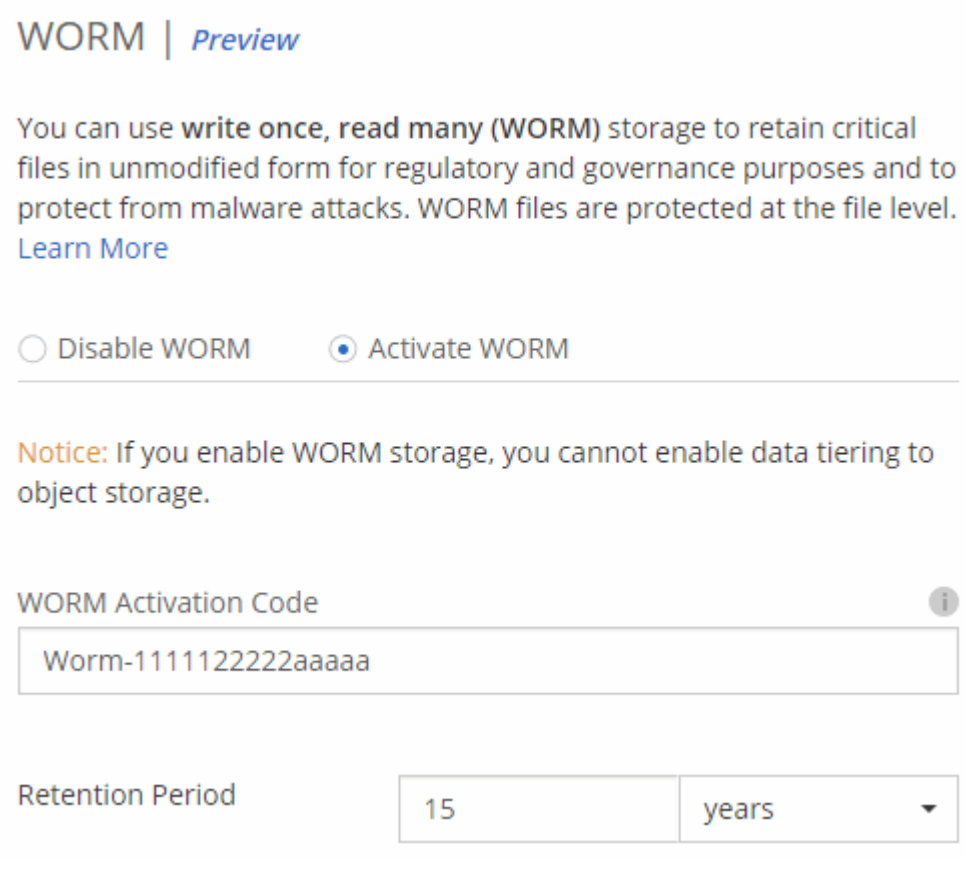
保留期間結束後、您必須負責刪除不再需要的任何檔案。

啟動 **WORM** 儲存設備

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

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

下圖顯示如何在建立工作環境時啟動 WORM 儲存設備：



將檔案提交至 **WORM**

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

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

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

限制

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

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。

總覽

在 AWS 中 Cloud Volumes ONTAP 、不含下列元件：

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

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

儲存設備接管與恢復

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

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

RPO 和 RTO

HA 組態可維持資料的高可用度、如下所示：

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

HA 部署模式

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

多個可用度區域中的可用度Cloud Volumes ONTAP

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

NFS 與 CIFS 資料存取

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

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

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

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

iSCSI 資料存取

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

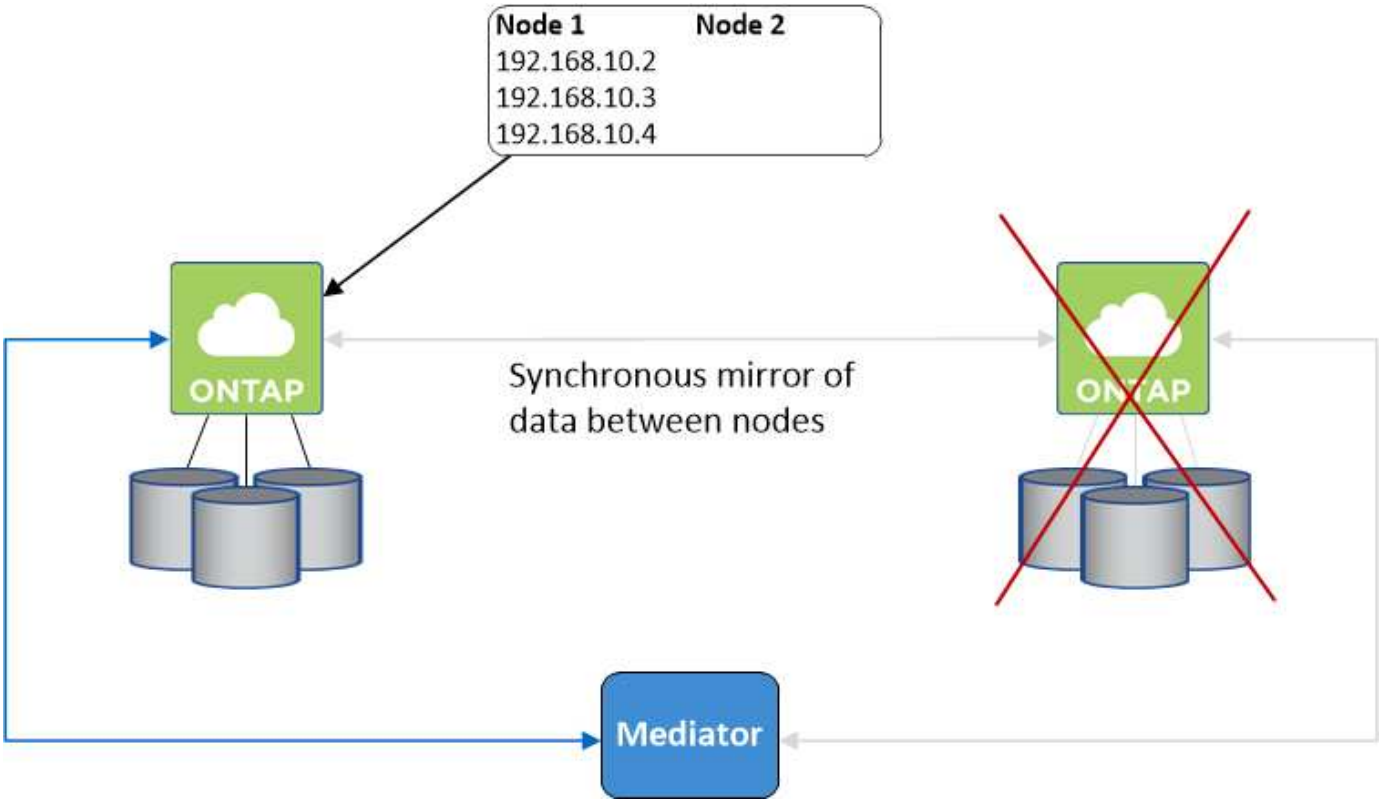
iSCSI的儲存接管與恢復

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

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

NAS的儲存接管與恢復

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



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

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

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

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

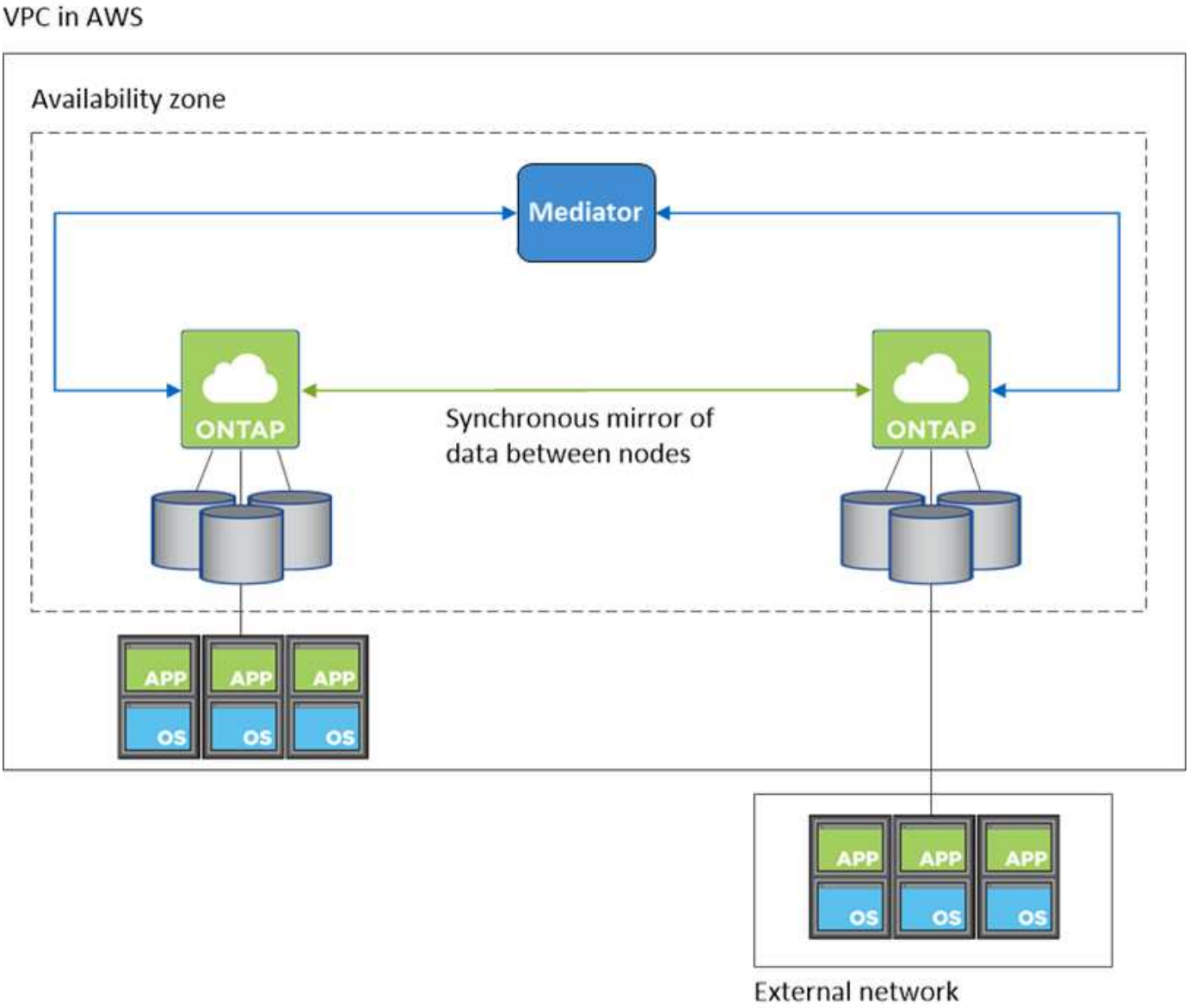
在單一可用度區域（AZ）中部署 HA 組態、可確保執行 Cloud Volumes ONTAP 此節點的執行個體故障時、資料的高可用度。所有資料均可從 VPC 外部原生存取。

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

資料存取

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

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



儲存設備接管與恢復

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

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

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

儲存設備如何在 **HA** 配對中運作

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

儲存配置

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

儲存組態

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

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

HA 組態的效能期望

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

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

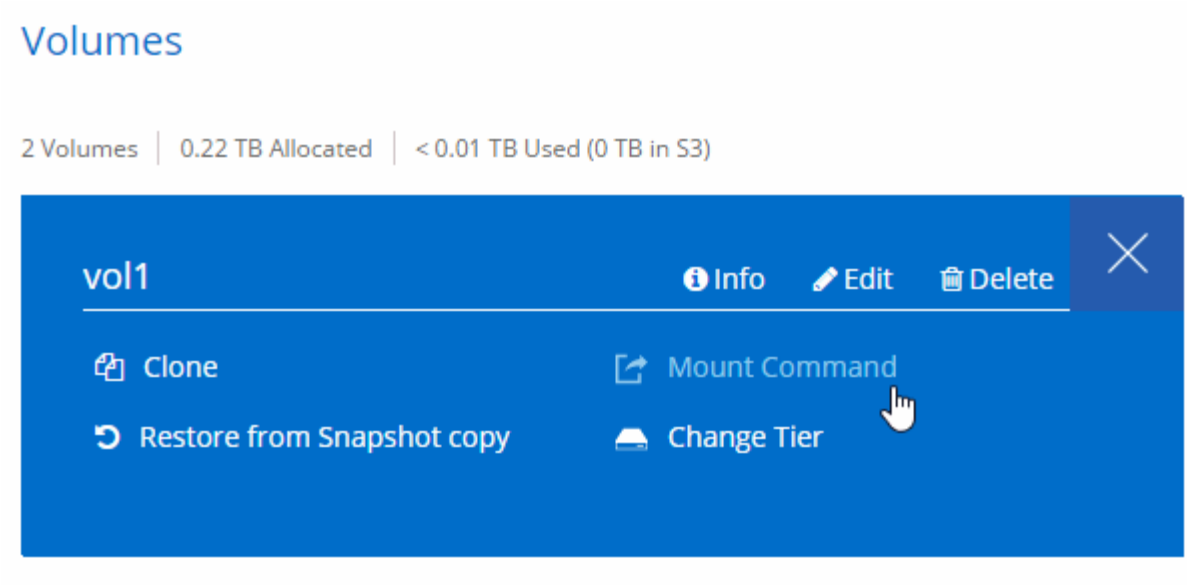
如需 Cloud Volumes ONTAP 更多關於效能的詳細資訊、請參閱 "效能"。

用戶端存取儲存設備

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

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

您可以從 Cloud Manager 輕鬆識別正確的 IP 位址：

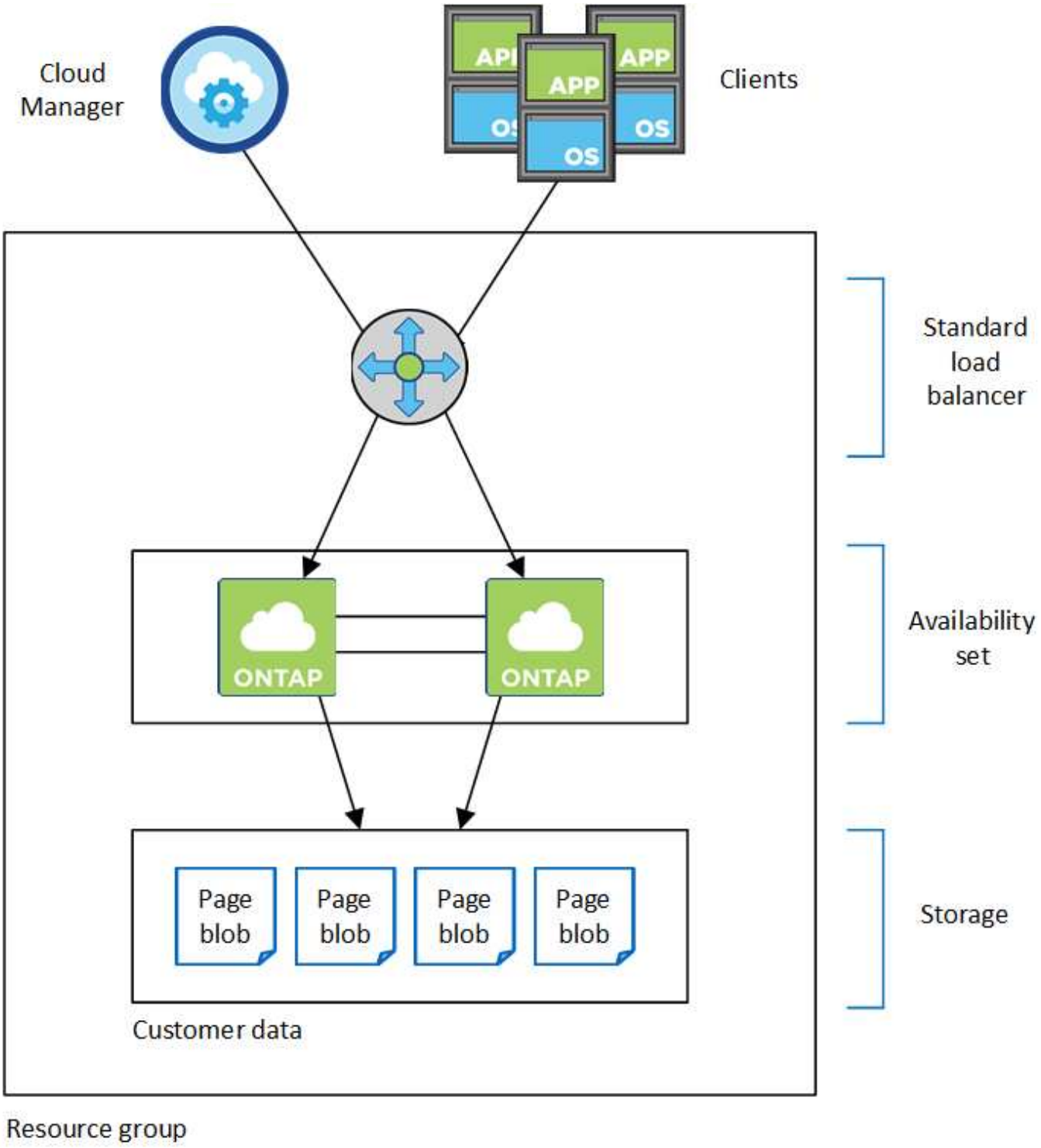


Azure 中的高可用度配對

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

HA 元件

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



請注意 Cloud Manager 為您部署的 Azure 元件：

Azure 標準負載平衡器

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

可用度設定

可用度集可確保節點位於不同的故障和更新網域中。

磁碟

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

- 兩個90 GB Premium SSD磁碟用於開機磁碟區（每個節點一個）
- 兩個 140 GB Premium Storage 頁面、用於根磁碟區（每個節點一個）
- 兩個128 GB標準HDD磁碟、可節省核心（每個節點一個）

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。

RPO 和 RTO

HA 組態可維持資料的高可用度、如下所示：

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

儲存設備接管與恢復

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

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

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

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

儲存組態

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

HA 限制

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

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

- 某些地區不支援 HA 配對。

  "請參閱支援的 Azure 地區清單"。

"瞭解如何在 Azure 中部署 HA 系統"。

評估

您可以在 Cloud Volumes ONTAP 購買軟體前先評估其功能。

如需單節點Cloud Volumes ONTAP 的免費試用30天、請參閱 "NetApp Cloud Central"。不收取每小時軟體費用、但基礎架構費用仍需支付。免費試用版會在到期時自動轉換為付費的每小時訂閱。

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

授權

每Cloud Volumes ONTAP 個BYOL系統都必須安裝有效訂閱的授權。如果未安裝使用中的授權、Cloud Volumes ONTAP 則在30天後、無法自行關閉。Cloud Manager 可為您管理授權、並在授權到期前通知您、藉此簡化程序。

新系統的授權管理

當您建立BYOL系統時、Cloud Manager會提示您輸入NetApp支援網站帳戶。Cloud Manager 使用帳戶從 NetApp 下載授權檔案、並將其安裝在 Cloud Volumes ONTAP 整個作業系統上。

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

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

授權過期

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

您可以選取工作環境來檢閱訊息。

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

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

授權續約

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

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

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 Volume Encryption（從Cloud Volumes ONTAP 推出時起）
- 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 Volume Encryption搭配原生AWS、Azure或GCP加密、以加密Hypervisor層級的資料。

NetApp Volume Encryption

NetApp Volume Encryption（NVE）是一項軟體技術、可一次加密閒置一個磁碟區的資料。資料、Snapshot複本和中繼資料都會加密。資料的存取權是由唯一的XTS-AES-256金鑰提供、每個磁碟區一個金鑰。

支援NetApp Volume Encryption搭配外部金鑰管理伺服器。Cloud Volumes ONTAP不支援Onboard Key Manager。您可以在中找到支援的金鑰管理程式 "NetApp 互通性對照表工具" 在*關鍵經理*解決方案下。

您可以使用CLI或System Manager、在新的或現有的磁碟區上啟用NetApp Volume Encryption。Cloud Manager不支援NetApp Volume Encryption。如需相關指示、請參閱 "使用NetApp Volume Encryption加密磁碟區"。

AWS 金鑰管理服務

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

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

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

Azure 儲存服務加密

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

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

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

執行防毒掃描 **ONTAP**

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

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

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

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

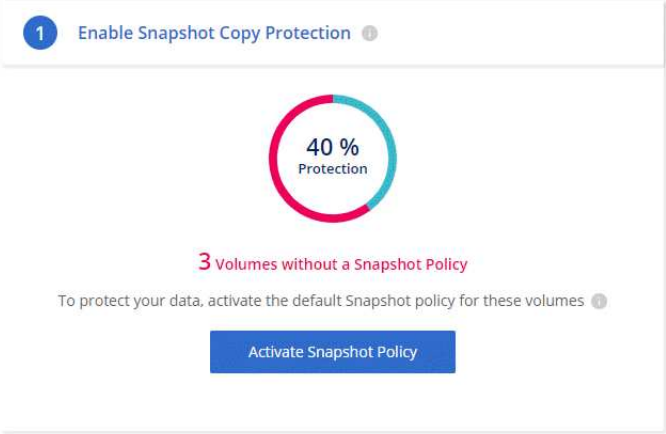
勒索軟體保護

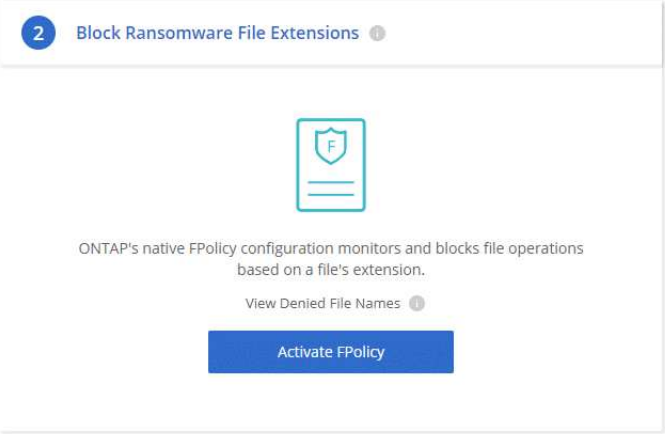
勒索軟體攻擊可能會耗費一定的時間、資源和商譽。Cloud Manager 可讓您針對勒索軟體實作 NetApp 解決方案、提供有效的可見度、偵測及補救工具。

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

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

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





"瞭解如何實作 NetApp 勒索軟體解決方案"。

效能

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

如需Cloud Volumes ONTAP AWS的相關資訊、請參閱 "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"。

如需Cloud Volumes ONTAP Microsoft Azure適用的功能、請參閱 "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"。