



採用Epic的混合雲Cloud Volumes ONTAP FlexPod

FlexPod

NetApp
November 04, 2025

目錄

採用Epic的混合雲Cloud Volumes ONTAP FlexPod	1
TR-4960：FlexPod 《以Cloud Volumes ONTAP Epic為基礎的混合雲》	1
目標對象	2
解決方案效益	2
解決方案拓撲	3
解決方案元件	3
FlexPod	3
EHR	4
NetApp Console	4
控制台代理	4
NetApp Cloud Volumes ONTAP	5
NetApp Active IQ Unified Manager	5
Cisco Intersight	5
VMware vSphere 7.0	6
VMware vCenter Server	6
硬體與軟體版本	6
安裝與組態	7
NetApp Cloud Volumes ONTAP 產品部署	7
內部部署FlexPod 的內部部署	8
內部部署ONTAP 的不整儲存組態	8
將本機FlexPod儲存加入到NetApp Console	10
SAN組態	11
NetApp主機公用程式套件	11
探索ONTAP 功能	11
設定多重路徑	12
建立實體磁碟區	13
建立Volume群組	13
建立邏輯Volume	14
建立檔案系統	14
建立要掛載的資料夾	15
掛載檔案系統	15
資料產生	15
設定內部部署ONTAP 的SnapMirror與Cloud Volumes ONTAP 功能不全的SnapMirror複寫	16
解決方案驗證	17
應用程式開發與測試（開發/測試）	17
災難恢復	20
驗證正式作業站台上的資料	23
結論	25
何處可找到其他資訊	25

採用Epic的混合雲Cloud Volumes ONTAP FlexPod

TR-4960：FlexPod 《以Cloud Volumes ONTAP Epic為基礎的混合雲》



與下列合作夥伴合作：

NetApp的Kamini Singh

數位化轉型的關鍵、就是利用資料做更多工作。醫院會產生大量資料、並需要大量資料來管理組織、有效服務病患。在治療病患及管理員工排程和醫療資源時、會收集並處理資訊。

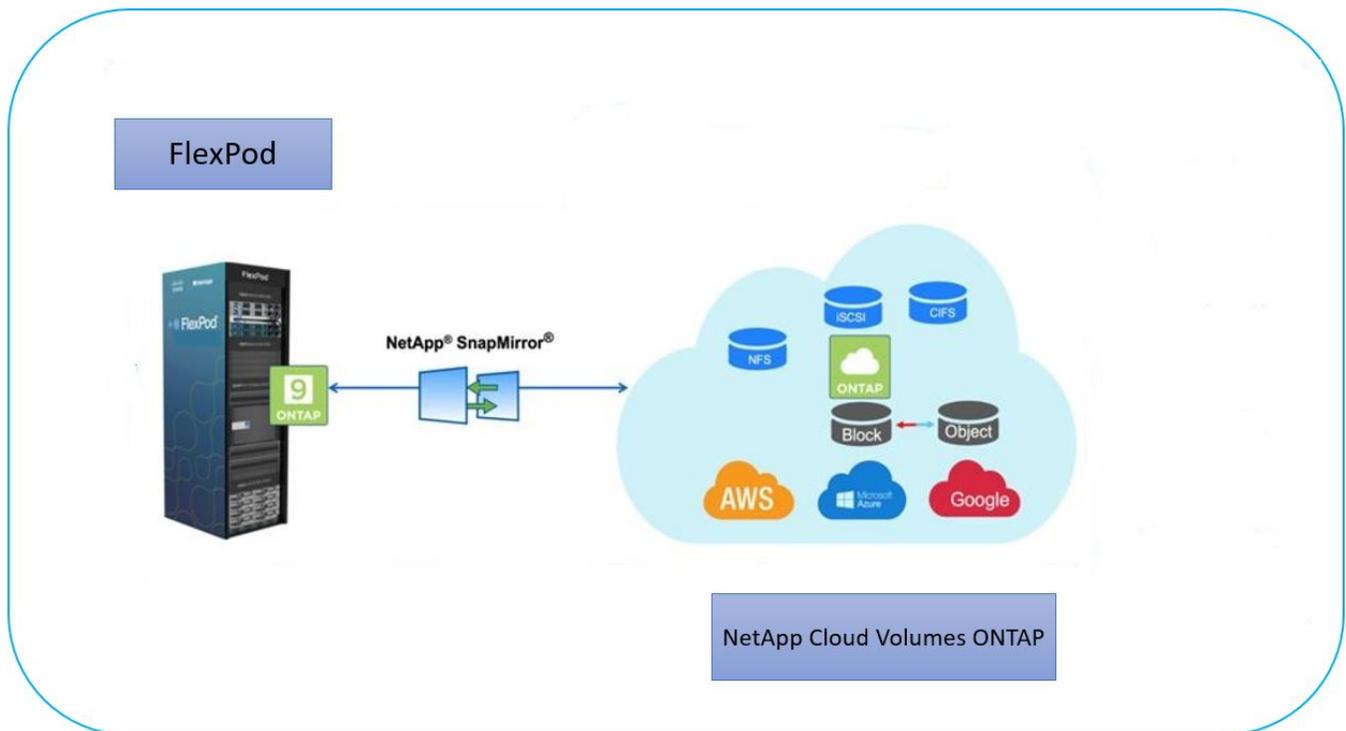
醫療資料的大小不斷增加、這些資料所提供的寶貴見解、使醫療資料服務和資料保護成為關鍵與挑戰。首先、醫療資料必須同時可用並受到保護、才能符合資料恢復、醫療業務持續性或法規遵循要求。

第二、醫療資料必須隨時可供分析。此分析通常使用人工智慧（AI）和機器學習（ML）方法、協助醫療企業改善解決方案並創造商業價值。

第三、隨著醫療業務成長、資料服務基礎架構和資料保護方法必須能夠因應醫療資料的成長。此外、資料移動性也日益重要、因為需要將資料從建立資料的邊緣移至核心和雲端、以便將可用的資源用於資料分析或歸檔用途。

NetApp為企業應用程式（包括醫療）提供單一資料管理解決方案、我們能夠引導醫院完成數位轉型的過程。NetApp Cloud Volumes ONTAP 支援醫療資料管理解決方案、可將資料從FlexPod 「支援資料中心」有效率地複寫到Cloud Volumes ONTAP 部署在AWS等公有雲上的「支援中心」。

利用具成本效益且安全的公有雲資源、Cloud Volumes ONTAP 利用高效率的資料複寫、內建的儲存效率、以及簡單的災難恢復測試、讓基於雲端的災難恢復（DR）更為出色。這些系統均以統一化的控制和拖放簡易性進行管理、提供具成本效益且防範項目的保護、避免發生任何錯誤、故障或災難。NetApp SnapMirror技術是區塊層級資料複寫的解決方案、可透過遞增式更新、讓目的地保持最新狀態Cloud Volumes ONTAP。



目標對象

本文件適用於NetApp與合作夥伴解決方案工程師（SE）及專業服務人員。NetApp假設讀者具備下列背景知識：

- 深入瞭解SAN和NAS概念
- 熟悉NetApp ONTAP 功能儲存系統的技術知識
- 熟悉ONTAP 組態及管理功能的技術知識

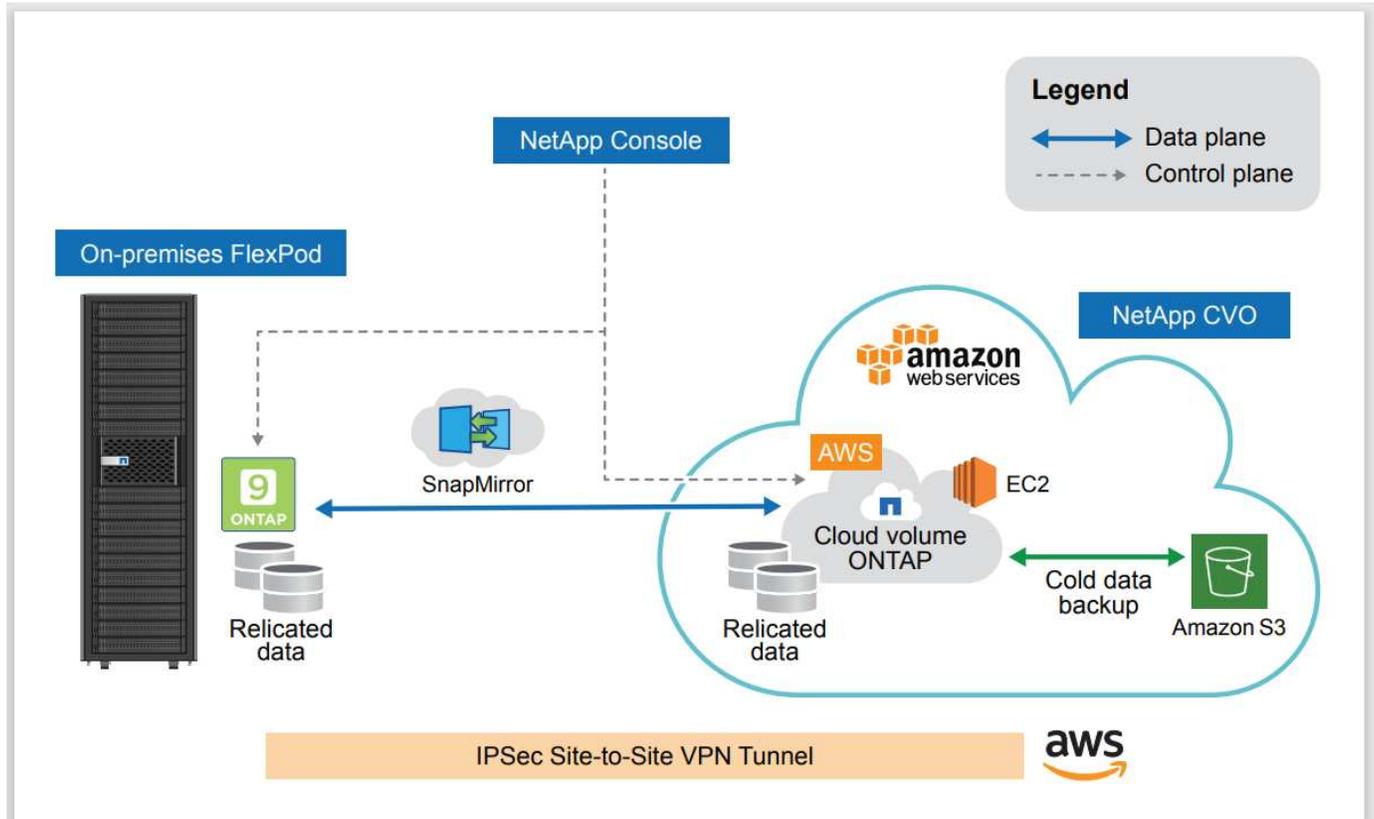
解決方案效益

與NetApp支援整合的Datacenter可為醫療工作負載提供下列優勢Cloud Volumes ONTAP FlexPod：

- ***自訂的保護。** Cloud Volumes ONTAP *支援區塊層級的資料複寫功能、可透過ONTAP 遞增式更新、將目的地保持在最新狀態。使用者可以指定同步排程、以決定何時傳輸來源的變更。這可為各種醫療資料提供自訂的保護。
- ***容錯移轉與容錯回復。** *發生災難時、儲存管理員可以快速設定容錯移轉至雲端磁碟區。當主要站台恢復時、DR環境中建立的新資料會同步回來源磁碟區、以便重新建立次要資料複寫。如此一來、便能輕鬆恢復醫療資料而不中斷營運。
- ***效率。** *二線雲端複本的儲存空間和成本、是使用資料壓縮、精簡配置和重複資料刪除技術最佳化的。醫療資料會以壓縮和重複資料刪除的形式、在區塊層級傳輸、以提升傳輸速度。資料也會自動分層至低成本的物件儲存設備、而且只有在存取時才會恢復至高效能儲存設備、例如在DR案例中。如此可大幅降低持續儲存成本。
- **勒索軟體防護** NetApp Console勒索軟體防護功能可掃描本地和雲端環境中的資料來源，偵測安全漏洞，並提供其當前的安全狀態和風險評分。然後它會提供可操作的建議，您可以進一步調查並遵循這些建議進行補救。這可以幫助您保護關鍵的醫療保健資料免受勒索軟體攻擊。

解決方案拓撲

本節描述解決方案的邏輯拓撲結構。下圖表示由FlexPod本地環境、運行在 Amazon Web Services (AWS) 上的NetApp Cloud Volumes ONTAP (CVO) 和NetApp Console SaaS 平台組成的解決方案拓撲。



端點之間的控制平面和資料平面會清楚標示出來。資料平面會在ONTAP 執行於FAS All Flash的整個過程中執行、並FlexPod 透過安全的站台對站台VPN連線、在AWS中執行NetApp CVO執行個體之間執行。將醫療工作負載資料從內部部署FlexPod 的「支援資料中心」複寫到NetApp Cloud Volumes ONTAP 解決方案、是由NetApp SnapMirror複寫來處理。此解決方案也支援選擇性備份及分層保存在NetApp CVO執行個體中的冷資料至AWS S3。

["下一步：解決方案元件。"](#)

解決方案元件

["上一篇：解決方案總覽。"](#)

FlexPod

支援針對虛擬化與非虛擬化解決方案、提供一套明確定義的硬體與軟體、為兩者提供整合式基礎。FlexPod包括NetApp的不二儲存設備、Cisco Nexus網路、Cisco MDS儲存網路、以及Cisco Unified Computing System (Cisco UCS) ONTAP FlexPod。

醫療組織正在尋求解決方案、以簡化數位轉型、並改善病患體驗與成果。有了這個功能、您就能獲得一個安全且可擴充的平台、來提升效率、並讓員工更快做出更明智的決策、以便提供更好的病患照護FlexPod。

支援下列優點、因此支援各種醫療工作負載需求的理想平台FlexPod：

- 最佳化營運、以獲得更快的洞見和更好的病患結果。
- 利用可擴充且可靠的基礎架構來簡化映像應用程式。
- 以備受肯定的方法快速有效地部署醫療應用程式、例如EHR。

EHR

電子健康記錄 (EHRs) 為中型和大型醫療組織、醫院和整合式醫療組織製作軟體。客戶也包括社區醫院、學術機構、兒童組織、安全網供應商及多醫院系統。EHR整合式軟體涵蓋臨床、存取和營收功能、並延伸至家中。

醫療業者組織仍面臨著壓力、必須在領先業界的EHRs上、充分發揮其大量投資所帶來的效益。客戶在設計EHR解決方案和關鍵任務應用程式的資料中心時、通常會針對其資料中心架構找出下列目標：

- EHR應用程式的高可用度
- 高效能
- 在資料中心內輕鬆實作EHR
- 靈活度與擴充性、可透過新的EHR版本或應用程式來實現成長
- 成本效益
- 管理能力、穩定性及支援簡易性
- 健全的資料保護、備份、還原及業務持續運作

FlexPod已獲得 EHR 認證，並支援包含Cisco UCS、Intel Xeon 處理器、Red Hat Enterprise Linux (RHEL) 和 VMware ESXiCisco化的平台。該平台，加上 EHR 對運行ONTAP的NetApp存儲的高舒適度評級，使您能夠通過FlexPod在完全託管的私有雲中運行您的醫療保健應用程序，該私有雲還可以連接到任何公共雲提供商。

NetApp Console

NetApp Console是一個企業級的、基於 SaaS 的管理平台，它使 IT 專家和雲端架構師能夠使用NetApp雲端解決方案集中管理其混合多雲基礎架構。它提供了一個集中式系統，用於查看和管理您的本地和雲端存儲，支援混合雲、多雲提供者和帳戶。有關詳細信息，請參閱 ["NetApp Console文檔"](#)。

控制台代理

控制台代理實例使控制台能夠管理公有雲環境中的資源和程序。控制台提供的許多功能都需要控制台代理，它可以部署在雲端或本地網路中。

控制台代理在以下位置受支援：

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- 內部部署

["了解有關控制台代理的更多信息"](#)。

NetApp Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP 解決方案是軟體定義的儲存產品、可在ONTAP 雲端上執行支援功能的資料管理軟體、為檔案和區塊工作負載提供進階的資料管理功能。有了VMware、您就能最佳化雲端儲存成本並提升應用程式效能、同時強化資料保護、安全性和法規遵循。Cloud Volumes ONTAP

主要效益包括：

- *儲存效率。*運用內建的重複資料刪除技術、資料壓縮、精簡配置及即時複製功能、將儲存成本降至最低。
- *高可用性。*在雲端環境發生故障時、提供企業級的可靠性和持續運作。
- *資料保護。*Cloud Volumes ONTAP *此功能使用領先業界的NetApp複寫技術SnapMirror、將內部部署資料複寫至雲端、以便在多種使用案例中輕鬆取得次要複本。此外、還能與Cloud Backup整合、提供備份與還原功能、以保護雲端資料、並長期歸檔Cloud Volumes ONTAP。
- *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 技術提供NetApp Snapshot複本的一致性。
- 資料安全 Cloud Volumes ONTAP。*支援資料加密、並提供防範病毒和勒索軟體的功能。
- *隱私法規遵循控管措施。*與Cloud Data Sense整合可協助您瞭解資料內容、並識別敏感資料。

更多詳細信息，請參閱["Cloud Volumes ONTAP"](#)。

NetApp Active IQ Unified Manager

NetApp Active IQ Unified Manager 支援透過ONTAP 單一、重新設計且直覺化的介面、監控您的不只是單一儲存叢集、還能提供社群智慧和AI分析的情報。它可針對儲存環境及其上執行的虛擬機器、提供全方位的作業、效能及主動深入見解。當儲存基礎架構發生問題時、Unified Manager可通知您有關問題的詳細資料、以協助識別根本原因。虛擬機器儀表板可讓您檢視虛擬機器的效能統計資料、以便從vSphere主機到網路、最後到儲存設備的整個I/O路徑進行調查。

有些事件也提供補救行動、可用來修正問題。您可以設定事件的自訂警示、以便在發生問題時、透過電子郵件和SNMP設陷通知您。利用此功能、您可以預測容量和使用趨勢、以便在發生問題之前採取行動、避免因應短期決策而導致長期的額外問題、藉此規劃使用者的儲存需求Active IQ Unified Manager。

有關詳細信息，請參閱 ["Active IQ Unified Manager"](#)。

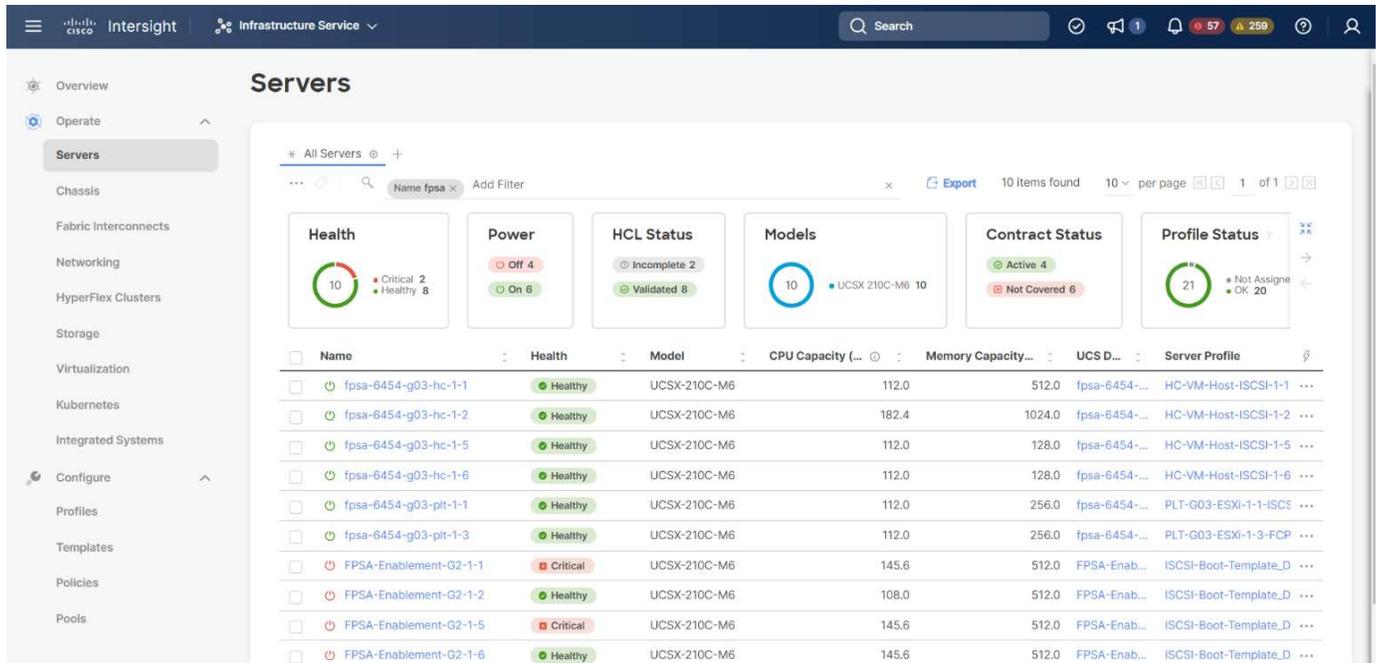
Cisco Intersight

Cisco Intersight是SaaS平台、可針對傳統和雲端原生的應用程式和基礎架構、提供智慧型自動化、監控及最佳化功能。此平台可協助IT團隊推動變革、並提供專為混合雲設計的營運模式。Cisco Intersight提供下列優點：

- 更快的交付速度。Intersight是以雲端或客戶資料中心的服務形式提供、因為它採用敏捷的軟體開發模式、所以能頻繁更新並持續創新。如此一來、客戶就能專注於支援關鍵業務需求。
- 簡化營運。Intersight使用單一、安全的SaaS交付工具、搭配通用的庫存、驗證及API、可在整個堆疊和所有位置上運作、消除跨團隊的封閉環境、藉此簡化營運。這可讓您在內部部署、VM、K8s、無伺服器、自動化、在內部部署和公有雲中都能進行最佳化和成本控管。
- *持續最佳化。*您可以使用Cisco Intersight提供的智慧功能、跨越每個層面、以及Cisco技術支援中心、持續最佳化您的環境。這項情報會轉換成建議的可自動執行的行動、讓您能夠即時因應任何變更：從移動工作負載、監控實體伺服器的健全狀況、到為您使用的公有雲提供降低成本的建議。

Cisco Intersight有兩種管理作業模式：UCSM託管模式（UMM）和Intersight託管模式（IMMM）。在Fabric互連

的初始設定期間、您可以針對光纖附加的Cisco UCS系統、選取原生的UCSM託管模式 (Umm) 或Intersight託管模式 (IMMM)。在此解決方案中、使用原生的IMM. 下圖顯示Cisco Intersight儀表板。



VMware vSphere 7.0

VMware vSphere是一種虛擬化平台、可將大量的基礎架構（包括CPU、儲存設備和網路）整體管理為無縫、多功能且動態的作業環境。與管理個別機器的傳統作業系統不同、VMware vSphere會將整個資料中心的基礎架構集合在一起、建立一個資源強大的單一儲存設備、以便快速動態地分配給任何需要的應用程式。

有關 VMware vSphere 及其組件的更多信息，請參閱["VMware vSphere"](#)。

VMware vCenter Server

VMware vCenter Server可從單一主控台統一管理所有主機和VM、並集合叢集、主機和VM的效能監控。VMware vCenter Server可讓系統管理員深入瞭解運算叢集、主機、VM、儲存設備、來賓作業系統、以及虛擬基礎架構的其他重要元件。VMware vCenter可管理VMware vSphere環境中的豐富功能集。

詳細資訊請參見["VMware vCenter"](#)。

硬體與軟體版本

這種混合雲解決方案可以擴展到任何運行支援版本的軟體、韌體和硬體的FlexPod環境，具體定義見：["NetApp互通性對照表工具"](#)，["UCS硬體與軟體相容性"](#)，和["VMware相容性指南"](#)。

下表顯示內部部署FlexPod 的更新版軟硬體。

元件	產品	版本
運算	Cisco UCS X210 c M6.	5.0 (1b)
	Cisco UCS Fabric Interconnects 6454.	4.2 (2a)

元件	產品	版本
網路	Cisco Nexus 9336C-FX2 NX-OS	9.3 (9)
儲存設備	NetApp AFF 產品-A400	零點9.11.1P2 ONTAP
	適用於VMware vSphere的NetApp ONTAP 產品開發工具	9.11.
	適用於VMware VAAI的NetApp NFS 外掛程式	2.0
	NetApp Active IQ Unified Manager	9.11p1
軟體	VMware vSphere	7.0 (U3)
	VMware ESXi Nenic乙太網路驅動程式	1.0.35.0
	VMware vCenter應用裝置	7.0.3
	Cisco Intersight輔助虛擬應用裝置	1.0.9-342.

下表顯示了控制台和Cloud Volumes ONTAP版本。

廠商	產品	版本
NetApp	安慰	3.9.24
	Cloud Volumes ONTAP	零點9.11. ONTAP

["下一步：安裝與組態。"](#)

安裝與組態

["先前版本：解決方案元件。"](#)

NetApp Cloud Volumes ONTAP 產品部署

完成下列步驟以設定Cloud Volumes ONTAP 您的實例：

1. 準備公有雲服務供應商環境。

您必須擷取公有雲服務供應商的環境詳細資料、才能進行解決方案組態。例如、針對Amazon Web Services (AWS) 環境準備、您需要AWS存取金鑰、AWS密碼金鑰、以及其他網路詳細資料、例如區域、VPC、子網路等。

2. 設定VPC端點閘道。

VPC端點閘道是啟用VPC與AWS S3服務之間連線的必要條件。這是用來在CVO（具有閘道類型的端點）上啟用備份。

3. 存取NetApp Console。

要存取控制台和其他雲端服務，您需要註冊。["NetApp Console"](#)。有關在控制台帳戶中設定工作區和使用者的信息，請參閱 ["NetApp Console設定與管理"](#)。您需要一個具有權限的帳戶，才能直接從控制台在您的雲

端提供者部署控制台代理程式。若要取得所需的權限，請參閱 ["NetApp Console的權限摘要"](#)。

4. 部署控制台代理程式。

在新增 Cloud Volumes ONTAP系統之前，必須先部署控制台代理程式。如果您嘗試在沒有安裝控制台代理的情況下建立第一個Cloud Volumes ONTAP系統，控制台會提示您。若要從控制台在 AWS 中部署控制台代理，請參閱下列內容：["AWS 中的控制台代理安裝選項"](#)。

5. 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。["請閱讀逐步指示"](#)。

如需這些步驟的詳細資訊、請參閱 ["AWS的功能快速入門指南Cloud Volumes ONTAP"](#)。

在這個解決方案中，我們在 AWS 上部署了一個單節點Cloud Volumes ONTAP系統。

內部部署FlexPod 的內部部署

若要瞭解FlexPod UCS X系列、VMware及NetApp ONTAP 的功能不全、請參閱 ["採用Cisco UCS X系列的資料中心FlexPod"](#) 設計指南：本文件提供設計指南、可將Cisco Intersight託管UCS X系列平台整合到FlexPod 「支援資料中心」基礎架構中。

如需部署內部部署FlexPod 的資訊實例、請參閱 ["本部署指南"](#)。

本文件提供部署指南、可將Cisco Intersight託管UCS X系列平台整合到FlexPod 一套Datacenter基礎架構中。本文件涵蓋成功部署的組態和最佳實務做法。

可在UCS託管模式和Cisco Intersight託管模式（IMMM）中部署FlexPod。如果您要以FlexPod UCS託管模式部署功能、請參閱此 ["設計指南"](#) 以及這項功能 ["部署指南"](#)。

使用Ansible、可利用基礎架構做為程式碼來自動化部署FlexPod。以下是GitHub儲存庫的端點對端FlexPod 點支援連結：

- 可在UCS託管模式、NetApp功能和VMware vSphere中使用Cisco UCS進行的FlexPod 可行組態ONTAP ["請按這裡"](#)。
- 可在IMM, NetApp功能和VMware vSphere中看到Cisco UCS的FlexPod 可執行組態ONTAP ["請按這裡"](#)。

內部部署ONTAP 的不整儲存組態

本節說明ONTAP 本解決方案特有的一些重要的資訊功能組態步驟。

1. 設定執行iSCSI服務的SVM。

```
1. vservers create -vservers Healthcare_SVM -rootvolume
Healthcare_SVM_root -aggregate aggr1_A400_G0312_01 -rootvolume-security
-style unix
2. vservers add-protocols -vservers Healthcare_SVM -protocols iscsi
3. vservers iscsi create -vservers Healthcare_SVM
```

To verify:

```
A400-G0312::> vservers iscsi show -vservers Healthcare_SVM
Vserver: Healthcare_SVM
Target Name:
iqn.1992-08.com.netapp:sn.1fbf00f438c111ed866cd039ea91fb56:vs.3
Target Alias: Healthcare_SVM
Administrative Status: up
```

如果在叢集組態期間未安裝iSCSI授權、請務必先安裝授權、再建立iSCSI服務。

2. 建立FlexVol 一個流通量。

```
1. volume create -vservers Healthcare_SVM -volume hc_iscsi_vol -aggregate
aggr1_A400_G0312_01 -size 500GB -state online -policy default -space
guarantee none
```

3. 新增iSCSI存取介面。

```
1. network interface create -vservers Healthcare_SVM -lif iscsi-lif-01a
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node01-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> -status-admin up
2. network interface create -vservers Healthcare_SVM -lif iscsi-lif-01b
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node01-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> -status-admin up
3. network interface create -vservers Healthcare_SVM -lif iscsi-lif-02a
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node02-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> -status-admin up
4. network interface create -vservers Healthcare_SVM -lif iscsi-lif-02b
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node02-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> -status-admin up
```

在此解決方案中、我們建立了四個iSCSI邏輯介面 (I生命週期)、每個節點上各有兩個。

在部署vCenter並將所有ESXi主機新增至該執行個體的情況下、我們需要FlexPod 部署Linux VM、做為連線至及存取NetApp ONTAP 等位儲存設備的伺服器。在此解決方案中、我們已在vCenter中安裝CentOS 8執行個體。

4. 建立LUN。

```
1. lun create -vserver Healthcare_SVM -path /vol/hc_iscsi_vol/iscsi_lun1  
-size 200GB -ostype linux -space-reserve disabled
```

對於EHR作業資料庫 (odb)、日誌和應用程式工作負載、EHR建議將儲存設備呈現給iSCSI LUN。如果您的AIX版本和RHEL作業系統能夠增強效能、則NetApp也支援使用FCP和NVMe/FC。FCP和NVMe / FC可共存於同一個架構上。

5. 建立igroup。

```
1. igroup create -vserver Healthcare_SVM -igroup ehr -protocol iscsi  
-ostype linux -initiator iqn.1994-05.com.redhat:8e91e9769336
```

igroup用於允許伺服器存取LUN。若為Linux主機、可在檔案中找到伺服器IQN
/etc/iscsi/initiatorname.iscsi。

6. 將LUN對應至igroup。

```
1. lun mapping create -vserver Healthcare_SVM -path  
/vol/hc_iscsi_vol/iscsi_lun1 -igroup ehr -lun-id 0
```

將本機FlexPod儲存加入到NetApp Console

使用控制台完成以下步驟，將FlexPod儲存新增至系統中。

1. 從導覽選單中，選擇“儲存”>“系統”。
2. 在“系統”頁面上，按一下“新增系統”，然後選擇“本機部署”。
3. 選取*內部部署ONTAP 的S--。單擊 * 下一步 * 。
4. 在「叢集詳細資料」頁面上、輸入叢集管理IP位址和管理員使用者帳戶的密碼ONTAP。然後按一下「新增」。
5. 在「詳細資料與認證」頁面上、輸入工作環境的名稱與說明、然後按一下「執行」。

控制台發現ONTAP集群，並將其作為系統添加到「系統」頁面。

如需詳細資訊、請參閱頁面 ["探索內部部署ONTAP 的叢集"](#)。

["下一步：SAN組態。"](#)

SAN組態

"先前：安裝與組態。"

本節說明EHR所需的主機端組態、以使軟體能與NetApp儲存設備最佳整合。在此區段中、我們特別討論Linux作業系統的主機整合。使用 "[NetApp互通性對照表工具IMT \(不含\)](#)" 驗證所有軟體與韌體版本。



下列組態步驟是本解決方案中使用的CentOS 8主機專屬的設定步驟。

NetApp主機公用程式套件

NetApp建議您在連線至及存取NetApp儲存系統的主機作業系統上安裝NetApp主機公用程式套件（主機公用程式）。支援原生Microsoft多重路徑I/O（MPIO）。作業系統必須支援非對稱邏輯單元存取（ALUA）、才能執行多重路徑作業。安裝主機公用程式會設定NetApp儲存設備的主機匯流排介面卡（HBA）設定。

NetApp主機公用程式可下載 "[請按這裡](#)"。在此解決方案中、我們已在主機上安裝Linux Host Utilities 7.1。

```
[root@hc-cloud-secure-1 ~]# rpm -ivh netapp_linux_unified_host_utilities-7-1.x86_64.rpm
```

探索ONTAP 功能

請確定iSCSI服務在應登入時執行。若要為目標上的特定入口網站或目標上的所有入口網站設定登入模式、請使用 `iscsiadm` 命令。

```
[root@hc-cloud-secure-1 ~]# rescan-scsi-bus.sh
[root@hc-cloud-secure-1 ~]# iscsiadm -m discovery -t sendtargets -p
<iscsi-lif-ip>
[root@hc-cloud-secure-1 ~]# iscsiadm -m node -L all
```

現在您可以使用了 `sanlun` 可顯示有關連接主機LUN的信息。請確定您以root身分登入主機。

```
[root@hc-cloud-secure-1 ~]# sanlun lun show
controller(7mode/E-Series)/
                                device      host          lun
vserver(cDOT/FlashRay) lun-pathname filename adapter protocol size
product
-----
---
Healthcare_SVM                /dev/sdb host33   iSCSI    200g
cDOT
                                /vol/hc_iscsi_vol/iscsi_lun1

Healthcare_SVM                /dev/sdc host34   iSCSI    200g
cDOT
                                /vol/hc_iscsi_vol/iscsi_lun1
```

設定多重路徑

Device Mapper多路徑（DM-多路徑）是Linux中的原生多重路徑公用程式。它可用於備援和改善效能。它會彙總或合併伺服器與儲存設備之間的多重I/O路徑、因此在作業系統層級建立單一裝置。

1. 在系統上設定DM-MultiPath之前、請先確認系統已更新且已包含 device-mapper-multipath 套件：

```
[root@hc-cloud-secure-1 ~]# rpm -qa|grep multipath
device-mapper-multipath-libs-0.8.4-31.el8.x86_64
device-mapper-multipath-0.8.4-31.el8.x86_64
```

2. 組態檔是 /etc/multipath.conf 檔案：如下所示更新組態檔。

```
[root@hc-cloud-secure-1 ~]# cat /etc/multipath.conf
defaults {
    path_checker      readsector0
    no_path_retry     fail
}
devices {
    device {
        vendor        "NETAPP  "
        product        "LUN.*"
        no_path_retry  queue
        path_checker   tur
    }
}
```

3. 啟用並啟動多重路徑服務。

```
[root@hc-cloud-secure-1 ~]# systemctl enable multipathd.service
[root@hc-cloud-secure-1 ~]# systemctl start multipathd.service
```

4. 新增可載入的核心模組 `dm-multipath` 並重新啟動多重路徑服務。最後、請檢查多重路徑狀態。

```
[root@hc-cloud-secure-1 ~]# modprobe -v dm-multipath
insmod /lib/modules/4.18.0-408.el8.x86_64/kernel/drivers/md/dm-
multipath.ko.xz

[root@hc-cloud-secure-1 ~]# systemctl restart multipathd.service

[root@hc-cloud-secure-1 ~]# multipath -ll
3600a09803831494c372b545a4d786278 dm-2 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
|+-+ policy='service-time 0' prio=50 status=active
|  `-- 33:0:0:0 sdb 8:16 active ready running
`-+-+ policy='service-time 0' prio=10 status=enabled
  `-- 34:0:0:0 sdc 8:32 active ready running
```



如需這些步驟的詳細資訊、請參閱 ["請按這裡"](#)。

建立實體磁碟區

使用 `pvcreate` 初始化區塊裝置以做為實體磁碟區的命令。初始化類似於格式化檔案系統。

```
[root@hc-cloud-secure-1 ~]# pvcreate /dev/sdb
Physical volume "/dev/sdb" successfully created.
```

建立Volume群組

若要從一或多個實體磁碟區建立磁碟區群組、請使用 `vgcreate` 命令。此命令會依名稱建立新的磁碟區群組、並至少新增一個實體磁碟區。

```
[root@hc-cloud-secure-1 ~]# vgcreate datavg /dev/sdb
Volume group "datavg" successfully created.
```

◦ `vgdisplay` 命令可用於以固定形式顯示Volume群組內容（例如大小、範圍、實體磁碟區數量等）。

```
[root@hc-cloud-secure-1 ~]# vdisplay datavg
--- Volume group ---
VG Name                datavg
System ID
Format                 lvm2
Metadata Areas        1
Metadata Sequence No  1
VG Access              read/write
VG Status              resizable
MAX LV                 0
Cur LV                0
Open LV                0
Max PV                 0
Cur PV                1
Act PV                 1
VG Size                <200.00 GiB
PE Size                4.00 MiB
Total PE               51199
Alloc PE / Size        0 / 0
Free PE / Size         51199 / <200.00 GiB
VG UUID                C7jmI0-J0SS-Cq91-t6b4-A9xw-nTfi-RXcy28
```

建立邏輯Volume

當您建立邏輯Volume時、邏輯Volume會使用組成Volume群組的實體磁碟區上的可用範圍、從Volume群組中進行切分。

```
[root@hc-cloud-secure-1 ~]# lvcreate -l 100%FREE -n datalv datavg
Logical volume "datalv" created.
```

此命令會建立一個稱為的邏輯Volume `datalv` 這會使用Volume群組中所有未配置的空間 `datavg`。

建立檔案系統

```
[root@hc-cloud-secure-1 ~]# mkfs.xfs -K /dev/datavg/datalv
meta-data=/dev/datavg/datalv      isize=512    agcount=4, agsize=13106944
blks
        =                          sectsz=4096   attr=2, projid32bit=1
        =                          crc=1        finobt=1, sparse=1, rmapbt=0
        =                          reflink=1    bigtime=0 inobtcount=0
data      =                          bsize=4096   blocks=52427776, imaxpct=25
        =                          sunit=0      swidth=0 blks
naming    =version 2                 bsize=4096   ascii-ci=0, ftype=1
log        =internal log             bsize=4096   blocks=25599, version=2
        =                          sectsz=4096   sunit=1 blks, lazy-count=1
realtime  =none                       extsz=4096   blocks=0, rtextents=0
```

建立要掛載的資料夾

```
[root@hc-cloud-secure-1 ~]# mkdir /file1
```

掛載檔案系統

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1
```

```
[root@hc-cloud-secure-1 ~]# df -k
```

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
devtmpfs	8072804	0	8072804	0%	/dev
tmpfs	8103272	0	8103272	0%	/dev/shm
tmpfs	8103272	9404	8093868	1%	/run
tmpfs	8103272	0	8103272	0%	/sys/fs/cgroup
/dev/mapper/cs-root	45496624	5642104	39854520	13%	/
/dev/sda2	1038336	258712	779624	25%	/boot
/dev/sda1	613184	7416	605768	2%	/boot/efi
tmpfs	1620652	12	1620640	1%	/run/user/42
tmpfs	1620652	0	1620652	0%	/run/user/0
/dev/mapper/datavg-datalv	209608708	1494520	208114188	1%	/file1

如需這些工作的詳細資訊、請參閱頁面 ["使用CLI命令進行LVM管理"](#)。

資料產生

`Dgen.pl` 是一個用於 EHR I/O 模擬器 (GenerateIO) 的 perl 腳本資料產生器。LUN 內的資料由 EHR 產生。`Dgen.pl` 腳本。該腳本旨在創建與 EHR 資料庫中的數據類似的數據。

```

[root@hc-cloud-secure-1 ~]# cd GenerateIO-1.17.3/

[root@hc-cloud-secure-1 GenerateIO-1.17.3]# ./dgen.pl --directory /file1
--jobs 80

[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37
dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38
dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39
dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40
dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80

[root@hc-cloud-secure-1 file1]# df -k .

```

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
/dev/mapper/datavg-datalv	209608708	178167156	31441552	85%	/file1

執行時 Dgen.pl 指令碼預設會使用85%的檔案系統來產生資料。

設定內部部署ONTAP的SnapMirror與Cloud Volumes ONTAP 功能不全的SnapMirror複寫

NetApp SnapMirror可透過LAN或WAN高速複寫資料、因此您可以在虛擬與傳統環境中同時獲得高資料可用度與快速資料複寫。當您將資料複寫到NetApp儲存系統並持續更新次要資料時、資料會保持最新狀態、並在需要時隨時保持可用。不需要外部複寫伺服器。

完成下列步驟、在內部部署ONTAP的整套系統和CVO之間設定SnapMirror複寫。

1. 從導覽選單中，選擇“儲存”>“系統”。
 2. 在「系統」中，選擇包含來源磁碟區的系統，將其拖曳到要將磁碟區複製到的系統，然後選擇「複製」。
- 其餘步驟說明如何在Cloud Volumes ONTAP 不同時執行的ONTAP 功能叢集之間建立同步關係。
3. *來源與目的地對等關係設定。*如果出現此頁面、請選取叢集對等關係的所有叢集間生命體。
 4. *來源Volume選擇。*選取您要複寫的磁碟區。
 5. *目的地磁碟類型與分層。*如果目標Cloud Volumes ONTAP 是一個支援系統、請選取目的地磁碟類型、然後選擇是否要啟用資料分層。
 6. *目的地Volume名稱：*指定目的地Volume名稱、然後選擇目的地Aggregate。如果目的地是ONTAP 一個不必要的叢集、您也必須指定目的地儲存VM。
 7. *最大傳輸率。*指定資料傳輸的最大傳輸率（以百萬位元組/秒為單位）。
 8. 複寫原則。*選擇預設原則或按一下*其他原則、然後選取其中一個進階原則。如需協助、["深入瞭解複寫原](#)

則"。

9. *排程。*選擇一次性複本或週期性排程。有多個預設排程可供使用。如果您想要不同的排程、則必須在上建立新的排程 destination cluster 使用System Manager。

10. 檢閱*檢閱*檢閱您的選擇、然後按一下*執行。

如需這些組態步驟的詳細資訊、請參閱 ["請按這裡"](#)。

控制台啟動資料複製過程。在此階段，您可以看到在本機ONTAP系統和Cloud Volumes ONTAP之間建立的 複製服務。

在這個叢集中、您可以看到新建立的Volume Cloud Volumes ONTAP。

您也可以確認內部部署Volume與雲端Volume之間已建立SnapMirror關係。

如需複寫工作的詳細資訊、請參閱* Replication（複寫）索引標籤。

["下一步：解決方案驗證。"](#)

解決方案驗證

["先前版本：SAN組態。"](#)

在本節中、我們會複習一些解決方案使用案例。

- SnapMirror的主要使用案例之一是資料備份。SnapMirror可透過複寫同一個叢集內的資料或遠端目標、作為主要備份工具。
- 使用DR環境執行應用程式開發測試（開發/測試）。
- 災難發生時的災難恢復。
- 資料發佈與遠端資料存取。

值得注意的是、本解決方案中驗證的使用案例相對較少、並不代表SnapMirror複寫的完整功能。

應用程式開發與測試（開發/測試）

若要加速應用程式開發、您可以在DR站台快速複製複寫的資料、並將其用於開發/測試應用程式。災難恢復與開發/測試環境的主機代管可大幅改善備份或災難恢復設備的使用率、而隨需開發/測試複本則可提供所需數量的資料複本、讓您更快上線。

NetApp FlexClone技術可用於快速建立SnapMirror目的地FlexVol SnapMirror Volume的讀寫複本、以便您擁有次要複本的讀寫存取權、以確認所有正式作業資料是否可用。

請完成下列步驟、以使用DR環境執行應用程式開發/測試：

1. 製作正式作業資料的複本。若要這麼做、請執行內部部署磁碟區的應用程式快照。應用程式快照建立包含三個步驟：Lock、Snap`和 `Unlock。
 - a. 靜止檔案系統、使I/O暫停、應用程式維持一致性。在步驟C中發出unquiesce命令之前、任何寫入檔案系統的應用程式都會保持在等待狀態步驟a、b和c是透過透明的程序或工作流程執行、不會影響應用程式SLA。

```
[root@hc-cloud-secure-1 ~]# fsfreeze -f /file1
```

此選項會要求將指定的檔案系統從新的修改中凍結。任何嘗試寫入凍結檔案系統的程序都會遭到封鎖、直到檔案系統解除凍結為止。

- b. 建立內部部署Volume的快照。

```
A400-G0312::> snapshot create -vserver Healthcare_SVM -volume  
hc_iscsi_vol -snapshot kamini
```

- c. 取消靜止檔案系統以重新啟動I/O

```
[root@hc-cloud-secure-1 ~]# fsfreeze -u /file1
```

此選項用於解除檔案系統凍結、並允許繼續作業。凍結所封鎖的任何檔案系統修改都會解除封鎖、並允許完成。

應用程式一致的快照功能也可以使用NetApp SnapCenter 解決方案來執行、NetApp解決方案能夠完整協調上述流程SnapCenter、作為上述流程的一部分。如需詳細資訊、請參閱 ["請按這裡"](#)。

2. 執行SnapMirror更新作業、使正式作業和DR系統保持同步。

```
singlecvoaws::> snapmirror update -destination-path  
svm_singlecvoaws:hc_iscsi_vol_copy -source-path  
Healthcare_SVM:hc_iscsi_vol  
  
Operation is queued: snapmirror update of destination  
"svm_singlecvoaws:hc_iscsi_vol_copy".
```

也可以透過NetApp ConsoleGUI 的「複製」標籤執行SnapMirror更新。

3. 根據先前擷取的應用程式快照建立FlexClone執行個體。

```
singlecvoaws::> volume clone create -flexclone kamini_clone -type RW  
-parent-vserver svm_singlecvoaws -parent-volume hc_iscsi_vol_copy  
-junction-active true -foreground true -parent-snapshot kamini  
  
[Job 996] Job succeeded: Successful
```

對於先前的工作、也可以建立新的快照、但您必須依照上述步驟進行、以確保應用程式一致性。

4. 啟動FlexClone Volume以在雲端上顯示EHR執行個體。

```
singlecvoaws::> lun mapping create -vserver svm_singlecvoaws -path
/vol/kamini_clone/iscsi_lun1 -igroup ehr-igroup -lun-id 0

singlecvoaws::> lun mapping show
Vserver      Path                                Igroup      LUN ID
Protocol
-----
-----
svm_singlecvoaws
                /vol/kamini_clone/iscsi_lun1    ehr-igroup  0    iscsi
```

5. 在雲端的EHR執行個體上執行下列命令、以存取資料或檔案系統。

a. 探索ONTAP 功能：檢查多重路徑狀態。

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show

Output:
controller(7mode/E-Series)/          device      host          lun
vserver(cDOT/FlashRay) lun-pathname filename adapter protocol size
product
-----
-----
svm_singlecvoaws                      /dev/sda    host2        iSCSI        200g
cDOT
                /vol/kamini_clone/iscsi_lun1
sudo multipath -ll

Output:
3600a09806631755a452b543041313053 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

b. 啟動Volume群組。

```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

c. 掛載檔案系統並顯示檔案系統資訊摘要。

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                1K-blocks  Used    Available  Use%
Mounted on
/dev/mapper/datavg-datalv 209608708 183987096 25621612   88%
/file1
```

這會驗證您是否可以使用DR環境進行應用程式開發/測試。在災難恢復儲存設備上執行應用程式開發/測試、可讓您更充分地利用資源、否則可能會佔用大量時間。

災難恢復

SnapMirror技術也可作為災難恢復計畫的一部分。如果將關鍵資料複寫到不同的實體位置、嚴重的災難就不需要延長關鍵業務應用程式的資料不可用時間。用戶端可透過網路存取複寫的資料、直到正式作業站台從毀損、意外刪除、自然災害等狀況中恢復為止。

在對主站台進行容錯回復的情況下、SnapMirror提供一種有效率的方法來重新同步災難恢復站台與主站台、只要反轉SnapMirror關係、就能將變更的或新的資料從災難恢復站台傳輸回主站台。在主正式作業站台恢復正常的應用程式作業之後、SnapMirror會繼續傳輸至DR站台、而不需要進行其他基礎傳輸。

若要驗證成功的DR案例、請完成下列步驟：

1. 停止裝載內部部署ONTAP 的SVM、模擬來源（正式作業）端的災難 (hc_iscsi_vol) 。

The screenshot shows the ONTAP System Manager interface. The main content area displays a table of Storage VMs. The table has columns for Name, State, Subtype, Configured Protocols, IPspace, and Protection. Three rows are visible: CL_CIFS_SVM, CL_SVM, and Healthcare_SVM. The Healthcare_SVM row is selected, and a context menu is open over it, showing options: Edit, Delete, Stop (highlighted with a red box), Trace File Access, and Login Banner Message. The left sidebar shows the navigation menu with categories like DASHBOARD, INSIGHTS, STORAGE, NETWORK, EVENTS & JOBS, PROTECTION, HOSTS, and CLUSTER. The top navigation bar includes the ONTAP System Manager logo and a search bar.

Name	State	Subtype	Configured Protocols	IPspace	Protection
CL_CIFS_SVM	running	default	SMB/CIFS	Default	Shield
CL_SVM	running	default	NFS, ISCSI, FC	Default	Shield
Healthcare_SVM	running	default	NFS, ISCSI	Default	Shield

請確定SnapMirror複寫已設定在ONTAP 內部部署的支援範FlexPod 圍內、以供執行個體使用、Cloud

Volumes ONTAP 並在AWS中設定為可建立常用的應用程式快照。

SVM停止運作後，`hc_iscsi_vol` 控制台中不顯示音量。

2. 在CVO中啟動DR。

- a. 打破內部ONTAP 環境的SnapMirror與Cloud Volumes ONTAP 內部環境的複寫關係、並推廣CVO目的地Volume (hc_iscsi_vol_copy) 上線。

SnapMirror關係中斷後、目的地Volume類型會從資料保護 (DP) 變更為讀取/寫入 (RW)。

```
singlecvoaws::> volume show -volume hc_iscsi_vol_copy -fields typev
server          volume          type
-----
svm_singlecvoaws hc_iscsi_vol_copy RW
```

- b. 啟動Cloud Volumes ONTAP 目的地Volume in the目的地、在雲端的EC2執行個體上顯示EHR執行個體。

```
singlecvoaws::> lun mapping create -vserver svm_singlecvoaws -path
/vol/hc_iscsi_vol_copy/iscsi_lun1 -igroup ehr-igroup -lun-id 0

singlecvoaws::> lun mapping show
Vserver      Path                                     Igroup      LUN ID
Protocol
-----
svm_singlecvoaws
          /vol/hc_iscsi_vol_copy/iscsi_lun1  ehr-igroup  0          iscsi
```

- c. 若要存取雲端EHR執行個體上的資料和檔案系統、請先探索ONTAP 此解決方案的功能、並驗證多重路徑狀態。

```

sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show
Output:
controller(7mode/E-Series)/          device      host          lun
vserver(cDOT/FlashRay) lun-pathname filename adapter protocol size
product
-----
-----
svm_singlecvoaws                      /dev/sda  host2      iSCSI      200g
cDOT

                               /vol/hc_iscsi_vol_copy/iscsi_lun1
sudo multipath -ll
Output:
3600a09806631755a452b543041313051 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running

```

- d. 然後啟動Volume群組。

```

sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active

```

- e. 最後、掛載檔案系統並顯示檔案系統資訊。

```

sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                1K-blocks  Used    Available  Use%
Mounted on
/dev/mapper/datavg-datalv 209608708 183987096 25621612   88%
/file1

```

此輸出顯示使用者可透過網路存取複寫的資料、直到正式作業站台從災難中恢復為止。

- f. 反轉SnapMirror關係。此作業會反轉來源與目的地磁碟區的角色。

執行此作業時、來自原始來源Volume的內容會被目的地Volume的內容覆寫。當您想要重新啟動離線的來源 Volume 時、這很有幫助。

現在是CVO Volume (hc_iscsi_vol_copy) 成為來源磁碟區、內部部署磁碟區 (hc_iscsi_vol) 成為目的地Volume。

在上次資料複寫與停用來源磁碟區之間寫入原始來源磁碟區的任何資料都不會保留。

- a. 若要驗證CVO磁碟區的寫入存取權、請在雲端的EHR執行個體上建立新檔案。

```
cd /file1/  
sudo touch newfile
```

當正式作業站台當機時、用戶端仍可存取資料、也可寫入Cloud Volumes ONTAP 目前為來源Volume的靜態Volume。

在對主站台進行容錯回復的情況下、SnapMirror提供一種有效率的方法來重新同步災難恢復站台與主站台、只要反轉SnapMirror關係、就能將變更的或新的資料從災難恢復站台傳輸回主站台。在主正式作業站台恢復正常的應用程式作業之後、SnapMirror會繼續傳輸至DR站台、而不需要進行其他基礎傳輸。

本節說明當正式作業站台遭受災難時、災難恢復案例的成功解決方法。現在、當來源站台完成還原時、應用程式可以安全地為用戶端提供服務。

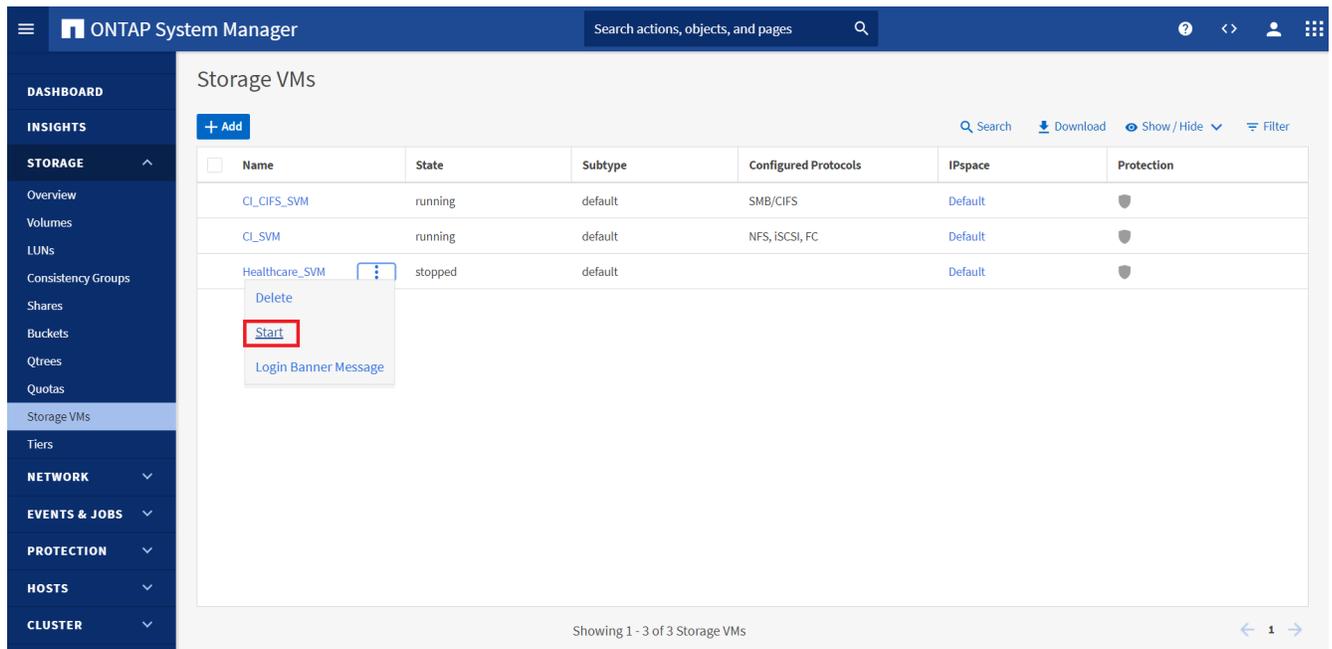
驗證正式作業站台上的資料

正式作業站台還原之後、您必須確保還原原始組態、而且用戶端能夠從來源站台存取資料。

在本節中、我們將討論如何建立來源站台、恢復內部部署ONTAP 的SnapMirror與Cloud Volumes ONTAP 還原之間的SnapMirror關係、最後在來源端執行資料完整性檢查

下列程序可用於驗證正式作業站台上的資料：

1. 請確定來源網站已啟動。若要這麼做、請啟動裝載內部部署ONTAP 的SVM (hc_iscsi_vol) 。



- 打破Cloud Volumes ONTAP 內部部署ONTAP 的SnapMirror複寫關係、並推廣內部部署的Volume (hc_iscsi_vol) 回歸正式作業。

SnapMirror關係中斷之後、內部部署磁碟區類型會從資料保護 (DP) 變更為讀取/寫入 (RW) 。

```
A400-G0312::> volume show -volume hc_iscsi_vol -fields type
vserver          volume          type
-----
Healthcare_SVM hc_iscsi_vol RW
```

- 反轉SnapMirror關係。現在、內部部署ONTAP 的《The On-One-Volume》 (內部部署) (hc_iscsi_vol) 會像以前一樣變成來源Volume、Cloud Volumes ONTAP 也會變成《The》的《The》 (來源) Volume (hc_iscsi_vol_copy) 成為目的地Volume。

依照這些步驟、我們已成功還原原始組態。

- 重新啟動內部部署的EHR執行個體。掛載檔案系統、並確認 newfile 您在雲端的EHR執行個體上建立的正式作業中斷時、現在也存在於此處。

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1
[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01 dir05 dir09 dir13 dir17 dir21 dir25 dir29 dir33 dir37 dir41 dir45 dir49 dir53 dir57 dir61 dir65 dir69 dir73 dir77 kamini
dir02 dir06 dir10 dir14 dir18 dir22 dir26 dir30 dir34 dir38 dir42 dir46 dir50 dir54 dir58 dir62 dir66 dir70 dir74 dir78 latest_file
dir03 dir07 dir11 dir15 dir19 dir23 dir27 dir31 dir35 dir39 dir43 dir47 dir51 dir55 dir59 dir63 dir67 dir71 dir75 dir79 newfile
dir04 dir08 dir12 dir16 dir20 dir24 dir28 dir32 dir36 dir40 dir44 dir48 dir52 dir56 dir60 dir64 dir68 dir72 dir76 dir80
```

我們可以推斷、從來源到目的地的資料複寫作業已成功完成、而且資料完整性也已維持不變。如此即可完成正式作業站台上的資料驗證。

"下一步：結論。"

結論

["先前版本：解決方案驗證。"](#)

建置混合雲是大多數醫療組織隨時提供資料可用度的目標。在這個解決方案中、我們實作FlexPod 了一套採用Cloud Volumes ONTAP NetApp SnapMirror複寫技術的混合雲解決方案、以驗證某些使用案例來備份及恢復醫療應用程式和工作負載。

由Cisco與NetApp的策略合作夥伴關係、提供經過嚴格測試與預先驗證的融合式基礎架構、可提供可預測的低延遲系統效能與高可用度FlexPod。這種方法可讓EHR達到高舒適度、最終為EHR系統的使用者提供最佳回應時間。

有了NetApp、您就能在雲端上執行EHR正式作業、災難恢復、備份或分層、就像在內部部署資料中心執行NetApp儲存功能一樣。有了NetApp Cloud Volumes ONTAP 功能、NetApp就能提供企業級的功能和效能、以便在雲端上有效執行EHR。NetApp雲端選項可提供區塊over iSCSI、檔案over NFS或SMB。

此解決方案能滿足醫療組織的需求、讓他們邁出數位轉型的步伐。它也能協助他們以有效率的方式管理應用程式和工作負載。

["下一步：何處可找到其他資訊。"](#)

何處可找到其他資訊

["上一篇：結論。"](#)

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

- 首頁FlexPod

["https://www.flexpod.com"](https://www.flexpod.com)

- Cisco驗證FlexPod 的《設計與部署指南》、適用於

["https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"](https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html)

- NetApp Console

["https://console.netapp.com/"](https://console.netapp.com/)

- NetApp Cloud Volumes ONTAP

["https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html"](https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html)

- 在AWS中快速入門Cloud Volumes ONTAP

["https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html"](https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html)

- SnapMirror複寫

["https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html"](https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html)

- TR-3928：NetApp Epic最佳實務做法
<https://www.netapp.com/pdf.html?item=/media/17137-tr3928pdf.pdf>
- TR-4693：FlexPod 《Epic EHR資料中心部署指南》
["https://www.netapp.com/media/10658-tr-4693.pdf"](https://www.netapp.com/media/10658-tr-4693.pdf)
- Epic適用的解決方案FlexPod
["https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmw_epic.html"](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmw_epic.html)
- NetApp 互通性對照表工具
["http://support.netapp.com/matrix/"](http://support.netapp.com/matrix/)
- Cisco UCS硬體與軟體互通性工具
["http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"](http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html)
- VMware相容性指南
["http://www.vmware.com/resources/compatibility/search.php"](http://www.vmware.com/resources/compatibility/search.php)

版本歷程記錄

版本	日期	文件版本歷程記錄
1.0版	2023年3月	初始版本

版權資訊

Copyright © 2025 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。