開始使用 **Amazon Web Services**

Cloud Volumes ONTAP

NetApp
February 13, 2026

目錄

開始使用 Amazon Web Services

AWS 中的Cloud Volumes ONTAP快速入門

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

1 建立控制台代理

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

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

2 規劃您的配置

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

3 設定網路

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

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

3. 設定到 Amazon Simple Storage Service（Amazon S3）服務的 VPC 端點。

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

"了解有關網絡要求的更多信息" 。

4 設定 **AWS KMS**

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

5 使用控制台啟動**Cloud Volumes ONTAP**

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

相關連結

- "為 AWS 建立控制台代理"
- "從 AWS Marketplace 建立控制台代理"

- "在本機安裝並設定控制台代理"
- "控制台代理的 AWS 權限"

在 AWS 中規劃您的Cloud Volumes ONTAP配置

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

選擇Cloud Volumes ONTAP許可證

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

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

選擇支援的區域

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

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

選擇受支援的本地區域

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

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

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

"AWS 文件：AWS 本機區域入門" 。

選擇支援的實例

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

"AWS 中Cloud Volumes ONTAP支援的配置"

了解儲存限制

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

"AWS 中Cloud Volumes ONTAP的儲存限制"

在 AWS 中調整系統大小

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

實例類型

- 將您的工作負載要求與每個 EC2 執行個體類型的最大吞吐量和 IOPS 相符。
- 如果多個使用者同時向系統寫入數據，請選擇具有足夠 CPU 來管理請求的執行個體類型。
- 如果您有一個主要用於讀取的應用程序，那麼請選擇具有足夠 RAM 的系統。
  - "AWS 文件：Amazon EC2 執行個體類型"
  - "AWS 文件：Amazon EBS 優化實例"

EBS 磁碟類型

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

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

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

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

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

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

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

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

EBS 磁碟大小

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

- 聚合中的所有磁碟必須具有相同的大小。
- EBS 磁碟的效能與磁碟大小相關。此大小決定了 SSD 磁碟的基線 IOPS 和最大突發持續時間以及 HDD 磁碟的基線和突發吞吐量。
- 最終，您應該選擇能夠提供您所需的_持續效能_的磁碟大小。

- 即使您確實選擇了更大的磁碟（例如，六個 4 TiB 磁碟），您可能無法獲得所有的 IOPS，因為 EC2 執行個體可能會達到其頻寬限制。

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

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

查看預設系統磁碟

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

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

控制台代理還需要係統磁碟。 "查看控制台代理預設配置的詳細信息" 。

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

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

需要指出的是，存在一些限制：

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

收集網路資訊

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

單一可用區中的單一節點或 **HA** 對

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

多個可用區中的 **HA** 對

AWS 資訊	你的價值
地區	
專有網絡	
安全群組（如果使用您自己的）	
節點 1 可用區	
節點 1 子網	
節點 2 可用區	
節點 2 子網	
中介可用區域	
調解器子網	
中介者的金鑰對	
叢集管理口浮動IP位址	
節點 1 上資料的浮動 IP 位址	
節點 2 上資料的浮動 IP 位址	
浮動 IP 位址的路由表	

選擇寫入速度

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

選擇卷使用情況設定檔

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

NetApp儲存效率功能有以下優勢：

精簡配置

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

重複資料刪除

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

壓縮

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

設定網路

為Cloud Volumes ONTAP設定 AWS 網路

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

一般要求

確保您已滿足 AWS 中的以下要求。

Cloud Volumes ONTAP節點的出站互聯網訪問

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

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

Cloud Volumes ONTAP端點

Cloud Volumes ONTAP使用這些端點與各種服務進行通訊。

端點	適用於	目的	部署模式	端點不可用時的影響
\ https://netapp-cloud-account.auth0.com	驗證	用於控制台中的身份驗證。	標準和限制模式。	用戶身份驗證失敗，以下服務仍然不可用： • Cloud Volumes ONTAP服務 • ONTAP服務 • 協定和代理服務
\ https://api.bluexp.netapp.com/tenancy	租賃	用於從控制台檢索Cloud Volumes ONTAP資源以授權資源和使用者。	標準和限制模式。	Cloud Volumes ONTAP資源和使用者未獲得授權。
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	用於將AutoSupport遙測資料傳送給NetApp支援。	標準和限制模式。	AutoSupport資訊仍未送達。

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

HA 中介器的出站互聯網訪問

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

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

NetApp Console代理程式的網路代理程式配置

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

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

"ONTAP CLI：安全性憑證安裝"命令。

有關配置代理伺服器的信息，請參閱 "配置控制台代理以使用代理伺服器"。

私人 **IP** 位址

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

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

單節點系統的 **IP** 位址

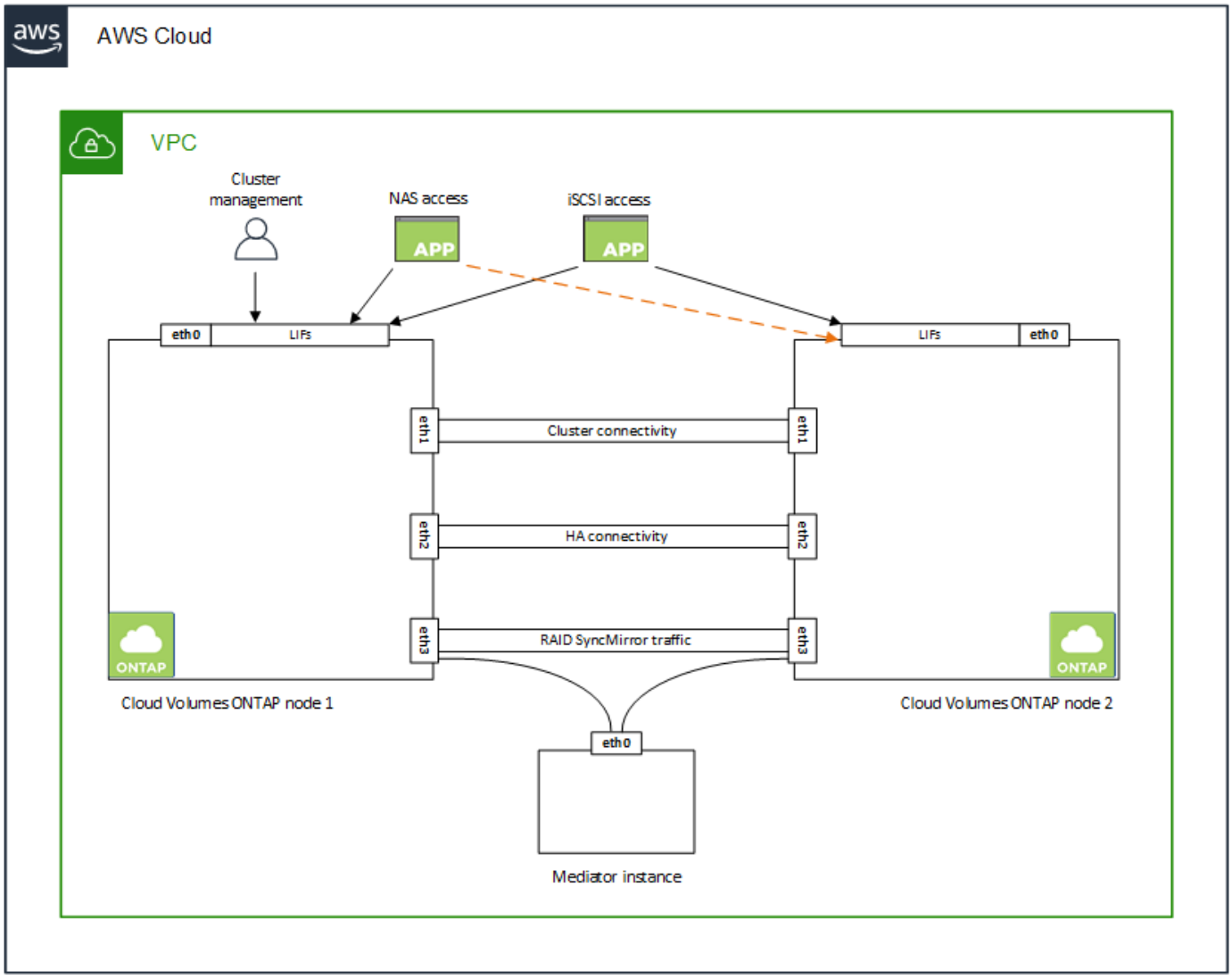
NetApp Console 為單節點系統指派 6 個 IP 位址。

下表提供了與每個私人 IP 位址關聯的 LIF 的詳細資訊。

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

HA 對的 **IP** 位址

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



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

下表提供了與每個私人 IP 位址關聯的 LIF 的詳細資訊。

雷射誘導螢光	介面	節點	目的
叢集管理	eth0	節點 1	整個集群（HA 對）的行政管理。
節點管理	eth0	節點 1 和節點 2	節點的行政管理。
集群間	eth0	節點 1 和節點 2	跨叢集通訊、備份和複製。
NAS數據	eth0	節點 1	透過 NAS 協定進行客戶端存取。
iSCSI 數據	eth0	節點 1 和節點 2	透過 iSCSI 協定進行客戶端存取。系統也將其用於其他重要的網路工作流程。這些 LIF 是必需的，不應刪除。
集群連接	eth1	節點 1 和節點 2	使節點能夠相互通訊並在叢集內移動資料。
HA 連接	eth2	節點 1 和節點 2	發生故障轉移時兩個節點之間的通訊。

雷射誘導螢光	介面	節點	目的
RSM iSCSI 流量	eth3	節點 1 和節點 2	RAID SyncMirror iSCSI 流量，以及兩個Cloud Volumes ONTAP節點和中介之間的通訊。
調解員	eth0	調解員	節點和中介之間的通訊通道，用於協助儲存接管和歸還過程。

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

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

安全群組

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

正在尋找有關控制台代理的資訊？ "查看控制台代理程式的安全性群組規則"

資料分層連接

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

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

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

與**ONTAP**系統的連接

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

CIFS 的 DNS 和 Active Directory

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

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

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

VPC共享

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

"了解如何在共享子網路中部署 HA 對" 。

多可用區中 HA 對的要求

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

要了解 HA 對的工作原理，請參閱"高可用性對"。

可用區域

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

每個可用區都應該有一個子網路。

用於 NAS 資料和叢集/SVM 管理的浮動 IP 位址

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

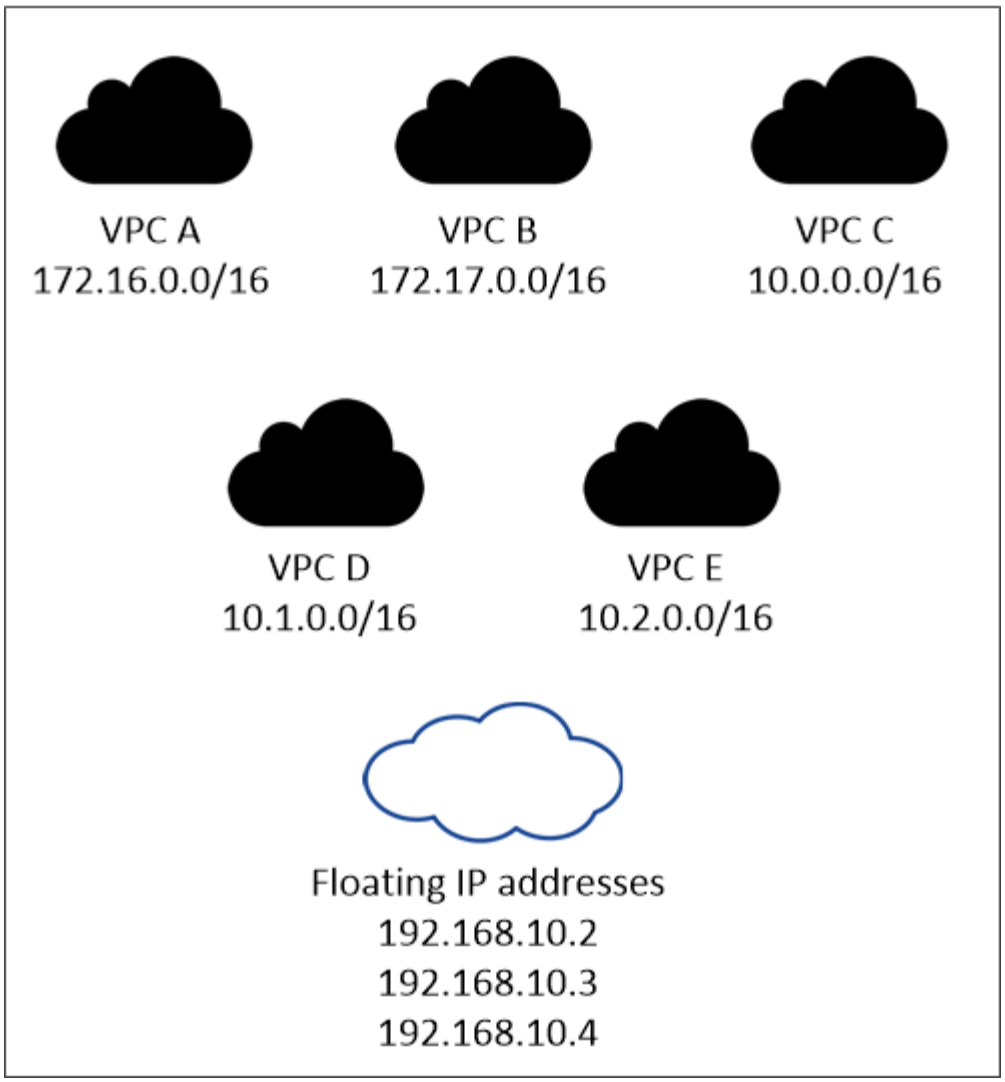
一個浮動 IP 位址用於叢集管理，一個用於節點 1 上的 NFS/CIFS 數據，一個用於節點 2 上的 NFS/CIFS 資料。用於 SVM 管理的第四個浮動 IP 位址是可選的。

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

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

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

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



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

中轉網關，用於從 **VPC** 外部啟用浮動 **IP** 訪問

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

路由表

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

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

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

有關路由表的更多信息，請參閱 "AWS 文件：路由表"。

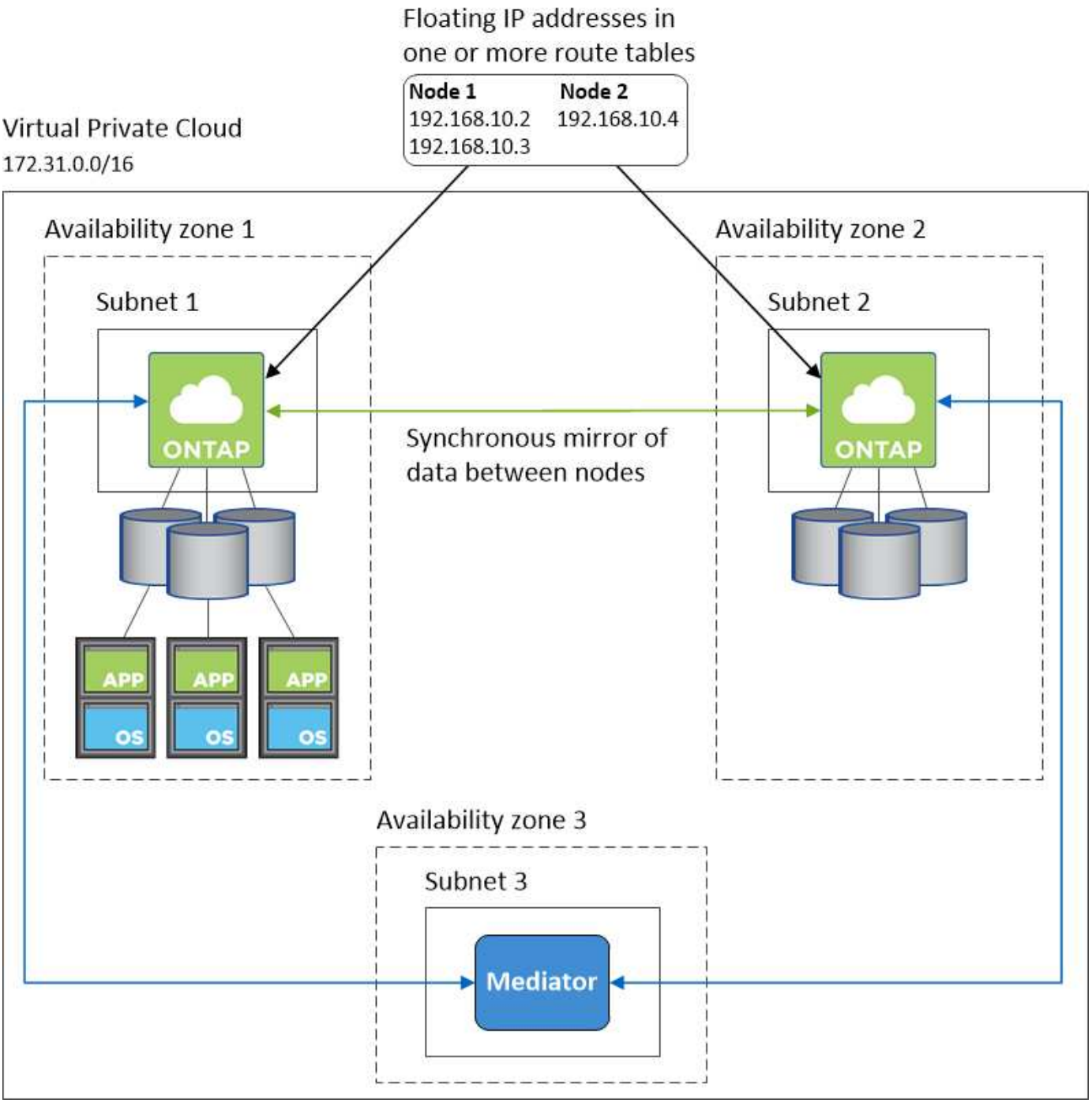
連接到NetApp管理工具

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

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

HA 設定範例

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



控制台代理的要求

如果您尚未建立控制台代理，則應查看網路需求。

- "查看控制台代理程式的網路要求"
- "AWS 中的安全群組規則"

相關主題

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

為**Cloud Volumes ONTAP HA** 設定 **AWS** 傳輸網關

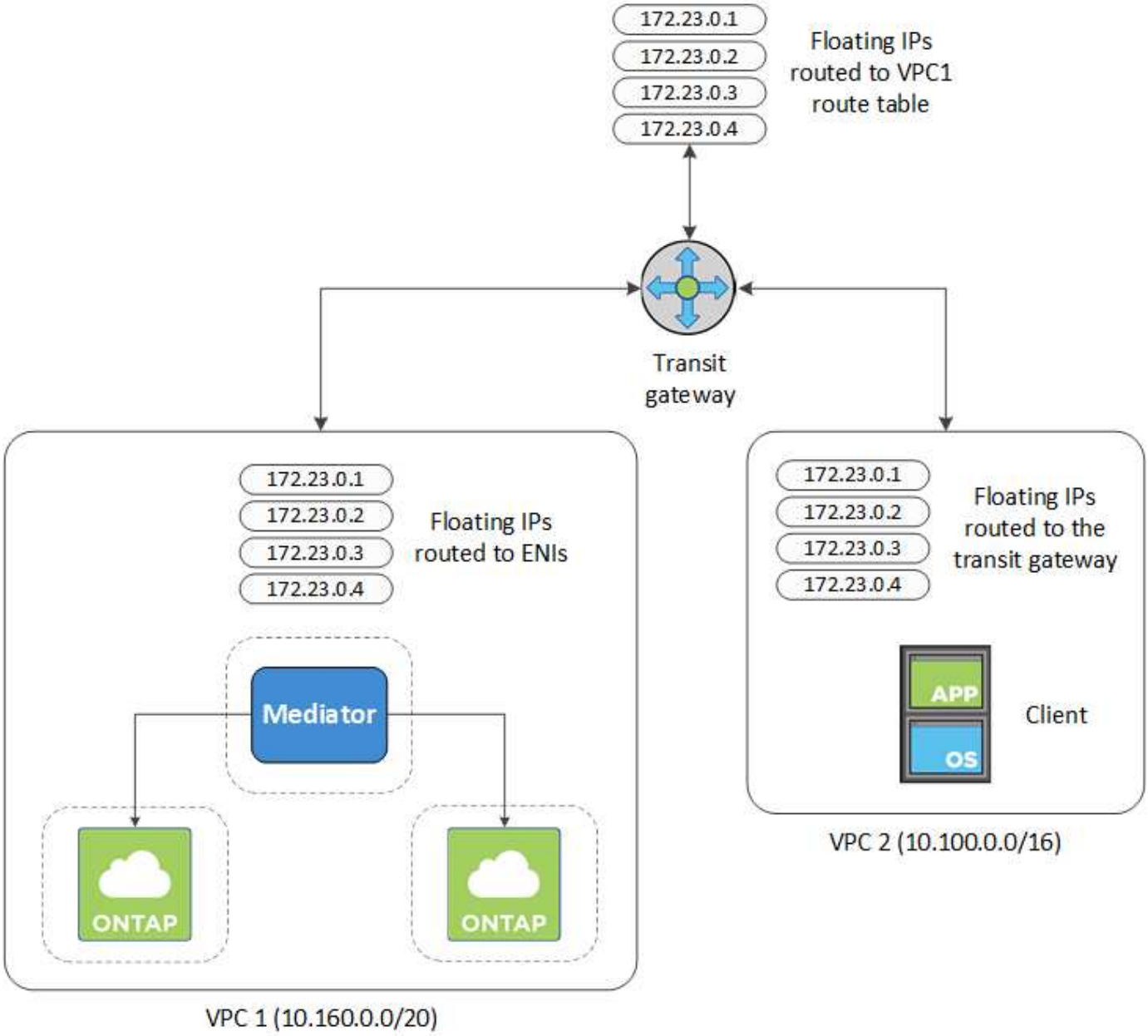
設定 AWS 中轉網關以允許存取 HA 對的"浮動IP位址"來自 HA 對所在的 VPC 外部。

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

叢集管理介面和可選的 SVM 管理 LIF 也需要浮動 IP 位址。

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

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

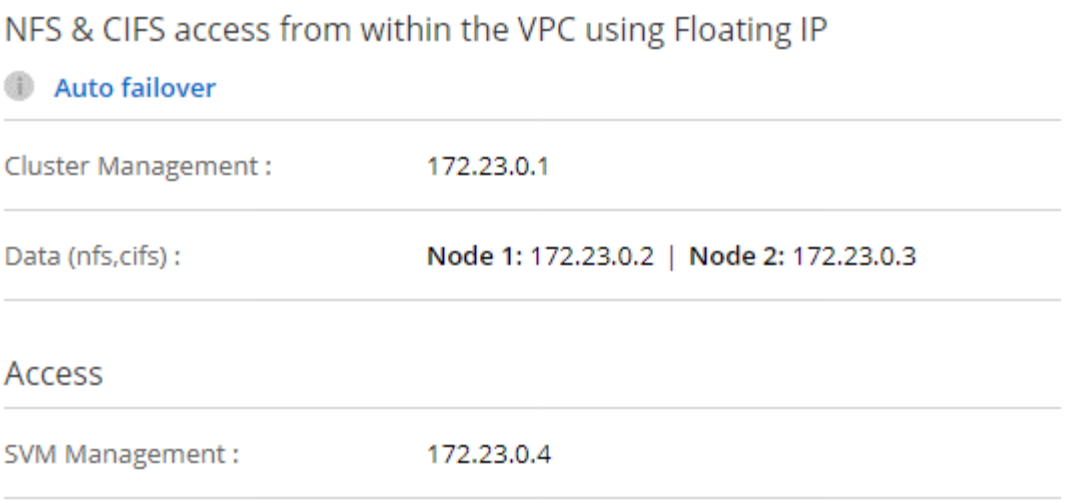


以下步驟說明如何設定類似的配置。

步驟

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

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



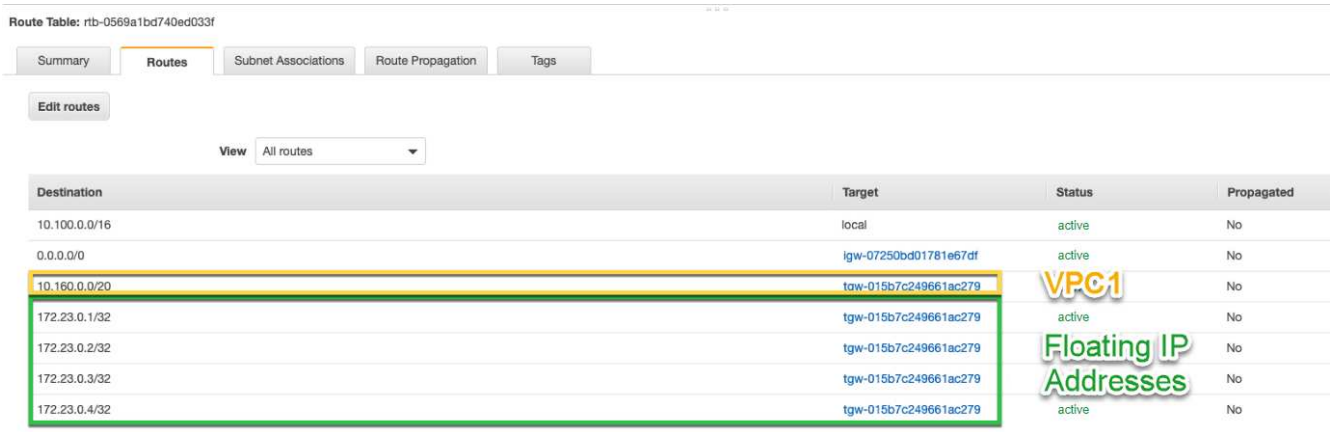
以下範例圖顯示了中轉網關的路由表。它包括到兩個 VPC 的 CIDR 區塊的路由和Cloud Volumes ONTAP使用的四個浮動 IP 位址。

4. 修改需要存取浮動IP位址的VPC的路由表。

   a. 為浮動IP位址新增路由條目。

   b. 將路由條目新增至 HA 對所在 VPC 的 CIDR 區塊。

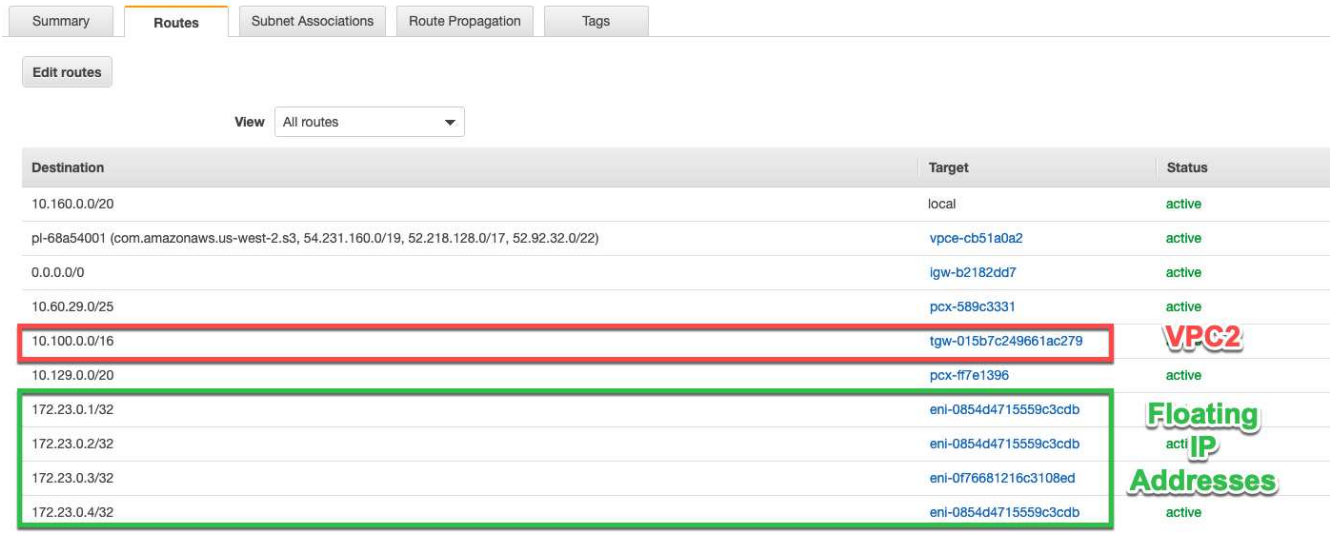
      下面的範例圖顯示了 VPC 2 的路由表，其中包含到 VPC 1 的路由和浮動 IP 位址。



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

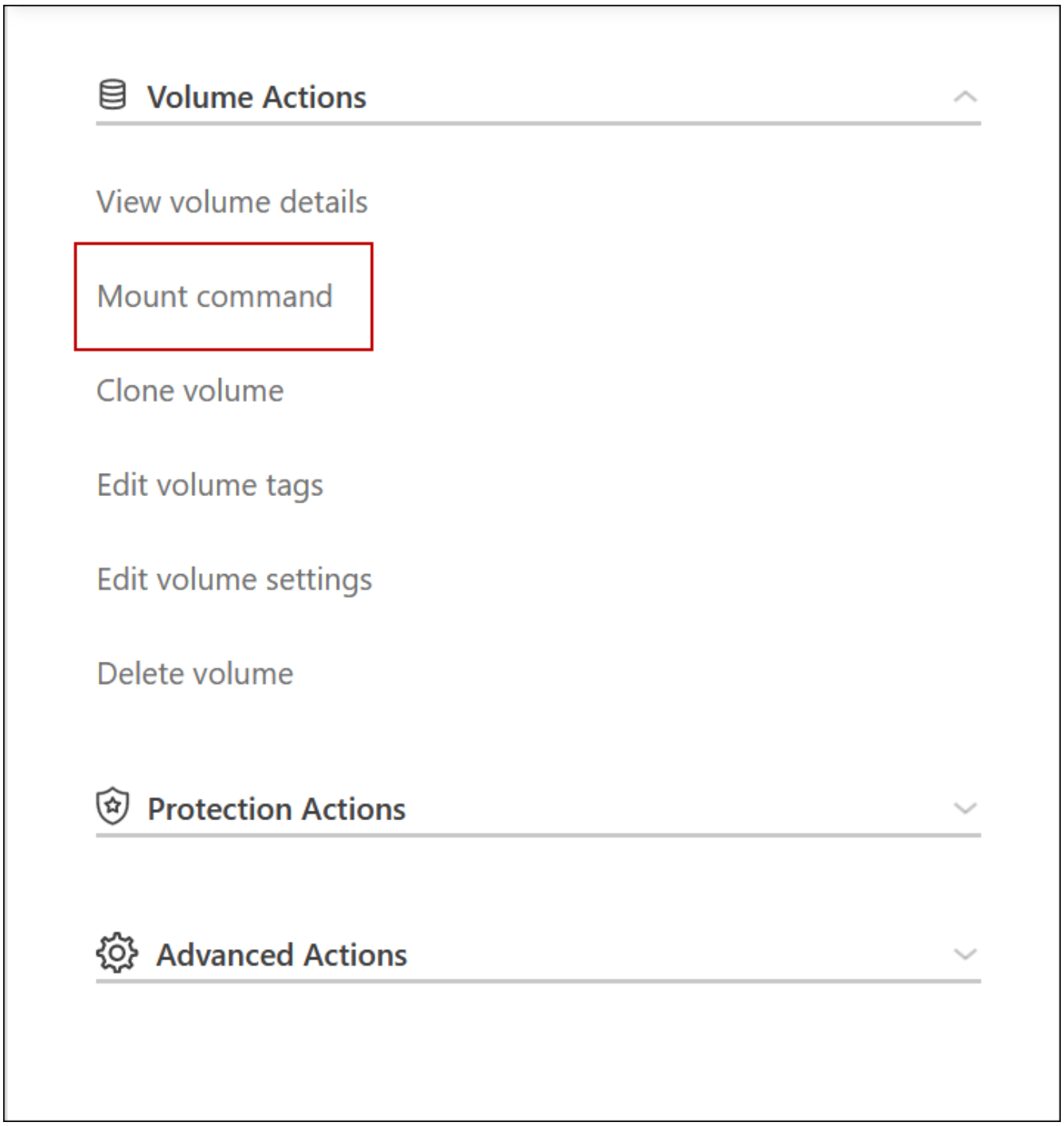
   這一步很重要，因為它完成了 VPC 之間的路由。

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



6. 將安全性群組設定更新為 VPC 的所有流量。
   a. 在虛擬私有雲下，點選*子網路*。
   b. 按一下「路由表」選項卡，為 HA 對的其中一個浮動 IP 位址選擇所需的環境。
   c. 按一下“安全性群組”。
   d. 選擇*編輯入站規則*。
   e. 按一下“新增規則”。
   f. 在類型下，選擇*所有流量*，然後選擇 VPC IP 位址。
   g. 按一下“儲存規則”以套用變更。
7. 使用浮動 IP 位址將磁碟區掛載到客戶端。

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



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

   "了解如何編輯卷" 。

相關連結

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

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

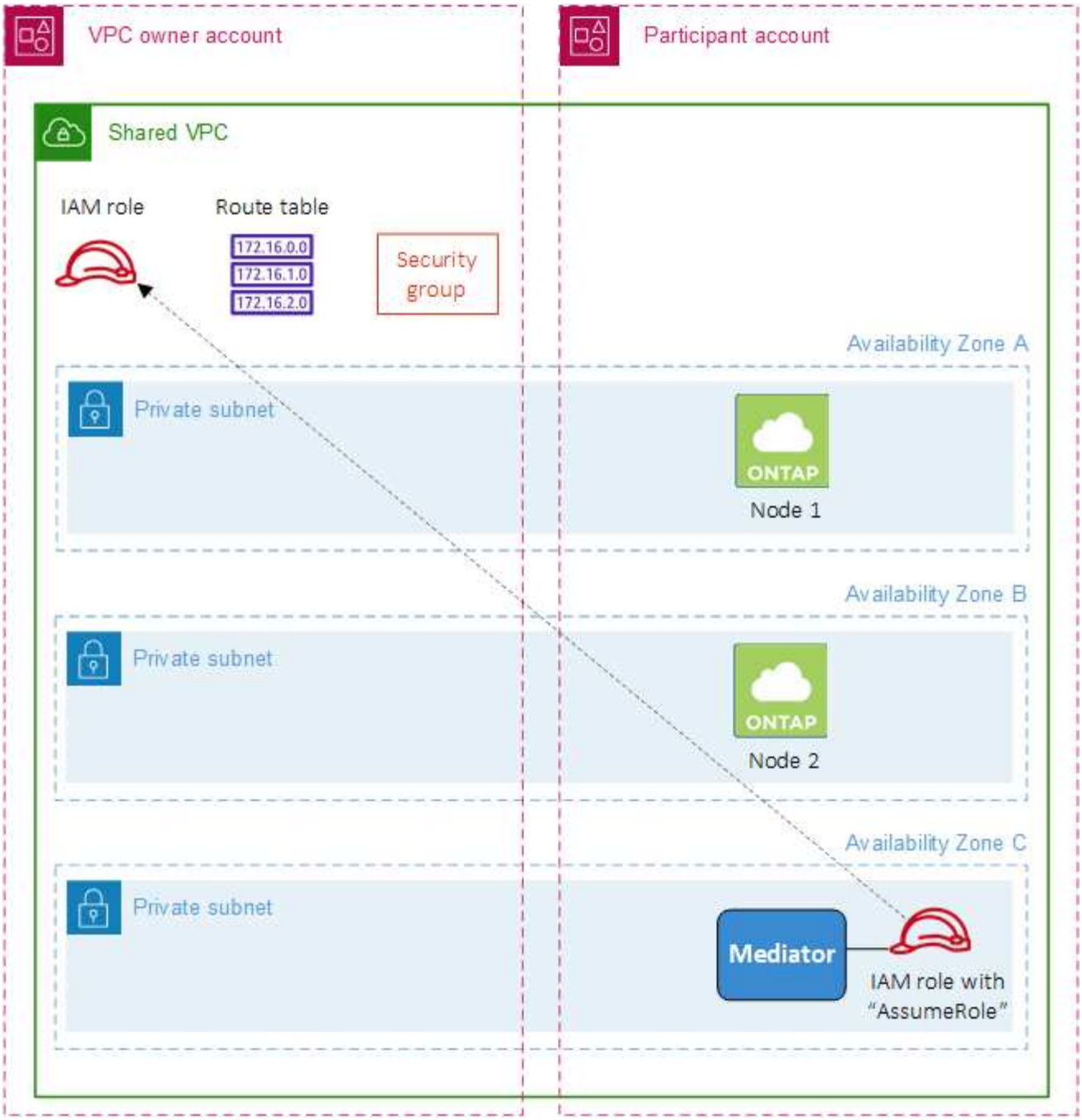
從 9.11.1 版本開始，AWS 透過 VPC 共享支援Cloud Volumes ONTAP HA 對。 VPC 共用可讓您的組織與其他 AWS 帳戶共用子網路。若要使用此配置，您必須設定您的 AWS 環境，然後使用 API 部署 HA 對。

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

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

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

下圖顯示了此部署所涉及的元件：



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

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

步驟

1. 與參與者帳戶共用 VPC 所有者帳戶中的子網路。

   此步驟是在共用子網路中部署 HA 對所必需的。

   "AWS 文件：共享子網"

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

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

3. 在 VPC 擁有者帳戶中，建立一個包含下列權限的 IAM 角色：

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

4. 使用 API 建立新的Cloud Volumes ONTAP系統。

   請注意，您必須指定以下欄位：

   - “安全群組 ID”

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

   - “haParams”物件中的“assumeRoleArn”

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

     例如：

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

+
"了解Cloud Volumes ONTAP API"

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

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

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

步驟

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

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

4. 儲存檔案並登出控制台代理程式。您不需要重新啟動控制台代理。

Cloud Volumes ONTAP的 AWS 安全群組入站和出站規則

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

Cloud Volumes ONTAP規則

Cloud Volumes ONTAP的安全群組需要入站和出站規則。

入站規則

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

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

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

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

出站規則

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

基本出站規則

Cloud Volumes ONTAP的預設安全群組包括以下出站規則。

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

高級出站規則

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

來源是Cloud Volumes ONTAP系統上的介面（IP 位址）。

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

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

HA 調解器外部安全群組的規則

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

入站規則

HA 中介的預定義安全群組包括以下入站規則。

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

出站規則

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

基本出站規則

HA 中介的預定義安全群組包括以下出站規則。

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

高級出站規則

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

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

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

HA 設定內部安全群組的規則

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

控制台始終建立此安全性群組。您沒有選擇使用自己的。

入站規則

預定義安全性群組包括以下入站規則。

協定	港口	目的
所有流量	全部	HA 中介器與 HA 節點之間的通信

出站規則

預定義安全性群組包括以下出站規則。

協定	港口	目的
所有流量	全部	HA 中介器與 HA 節點之間的通信

"查看控制台代理程式的安全性群組規則"

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

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

步驟

1. 確保存在有效的客戶主金鑰 (CMK)。

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

   "AWS 文件：客戶主金鑰 (CMK)"

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

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

   "AWS 文件：編輯金鑰"

3. 如果 CMK 位於不同的 AWS 帳戶中，請完成下列步驟：

   a. 從 CMK 所在的帳戶進入 KMS 控制台。

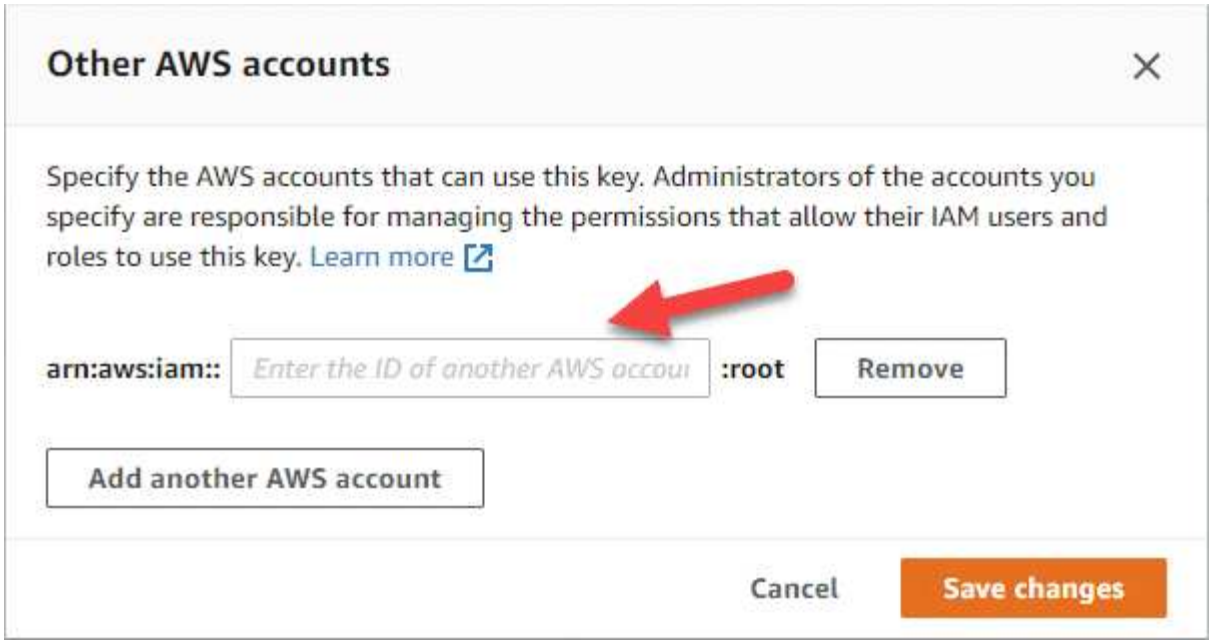
   b. 選擇鍵。

   c. 在「常規配置」窗格中，複製金鑰的 ARN。

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

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

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



e. 現在切換到為控制台提供權限的 AWS 帳戶並開啟 IAM 控制台。

f. 建立包含下面列出的權限的 IAM 策略。

g. 將政策附加到向控制台提供權限的 IAM 角色或 IAM 使用者。

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

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

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

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

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

Service（Amazon S3）儲存貯體中的資料，則需要執行此步驟。

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

"AWS 文件：編輯金鑰"

為Cloud Volumes ONTAP節點設定 AWS IAM 角色

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

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

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

步驟

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

標準區域

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

GovCloud（美國）區域

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

絕密地區

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

秘密區域

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

- Cloud Volumes ONTAP節點的備份策略

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

標準區域

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

GovCloud（美國）區域

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

絕密地區

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

秘密區域

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

- HA介導者

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

3. 建立一個 IAM 角色並將您建立的策略附加到該角色。

結果

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

更多資訊

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

在 AWS 中設定Cloud Volumes ONTAP許可

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

免費增值

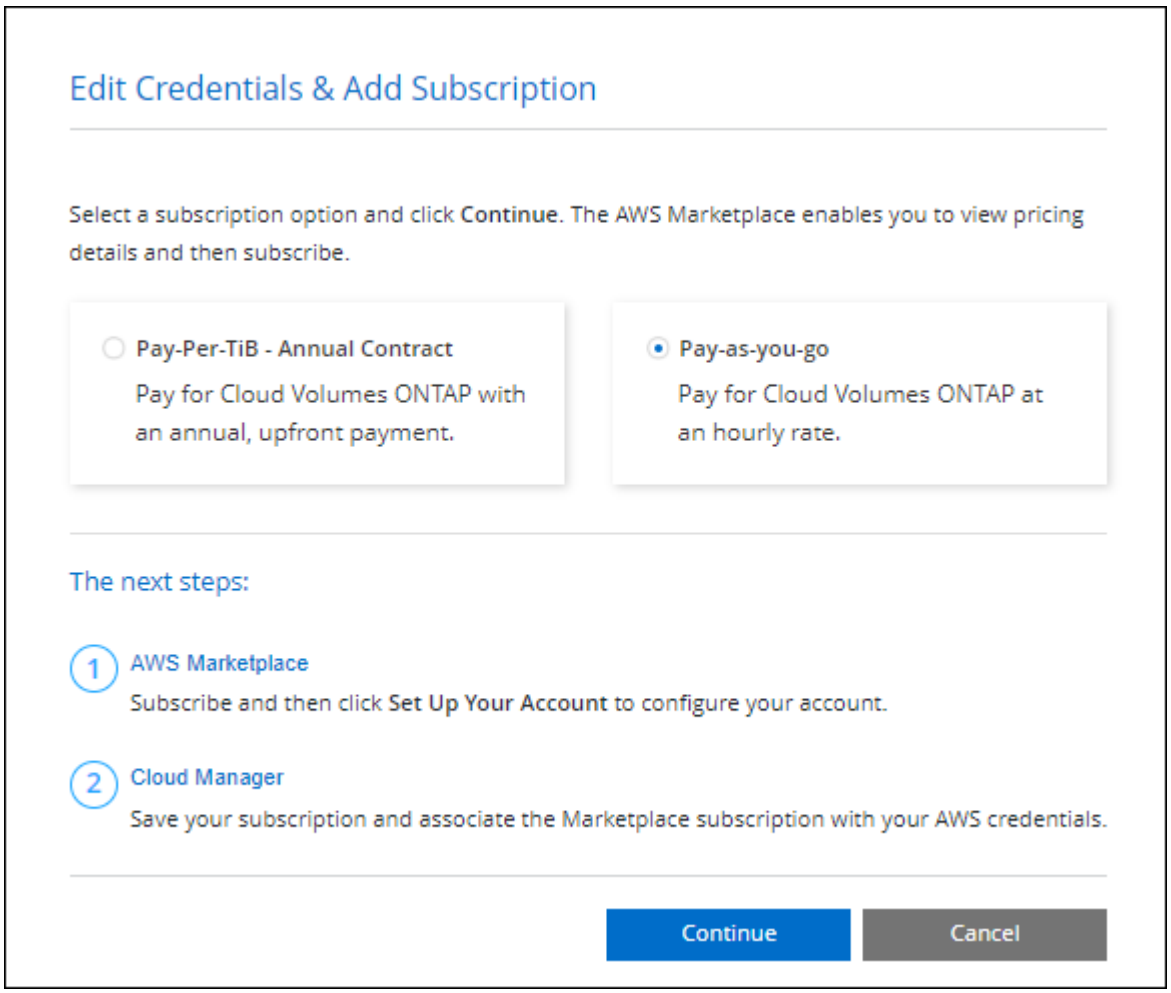
選擇免費加值服務，免費使用Cloud Volumes ONTAP，最高可提供 500 GiB 的設定容量。"了解有關免費增值服務的更多信息" 。

步驟

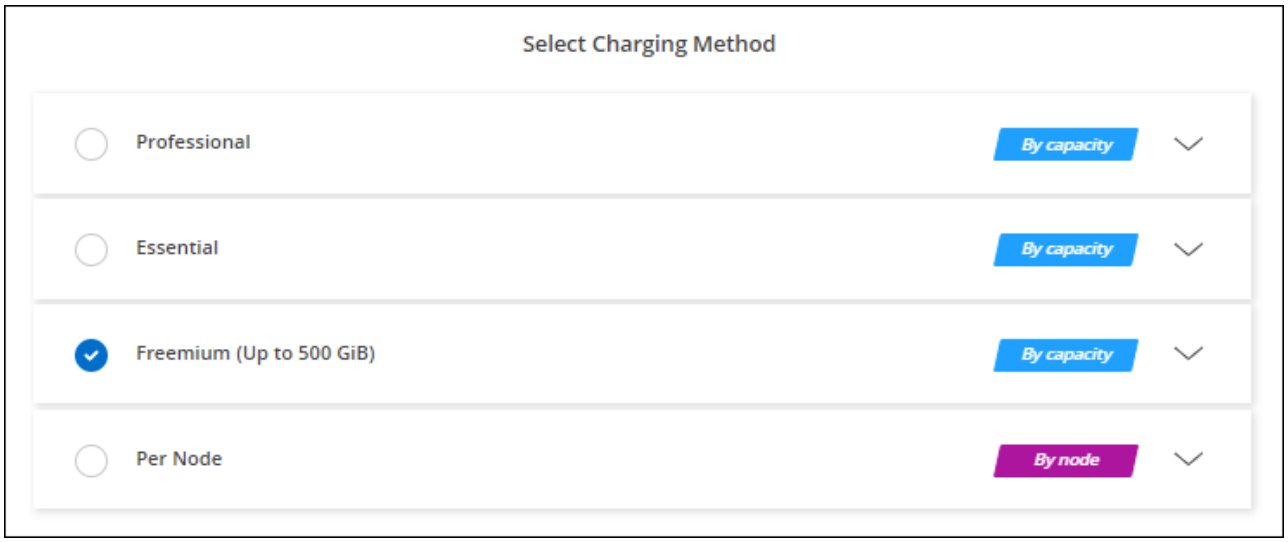
1. 從NetApp Console的左側導覽功能表中，選擇「儲存」>「管理」。
2. 在*系統*頁面上，按一下*新增系統*並依照步驟操作。

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

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



a. 返回控制台後，到達收費方式頁面時選擇「免費增值」。



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

基於容量的許可證

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

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

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

"了解有關基於容量的許可的更多信息" 。

以下部分介紹如何開始使用每種消費模型。

BYOL

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

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

步驟

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

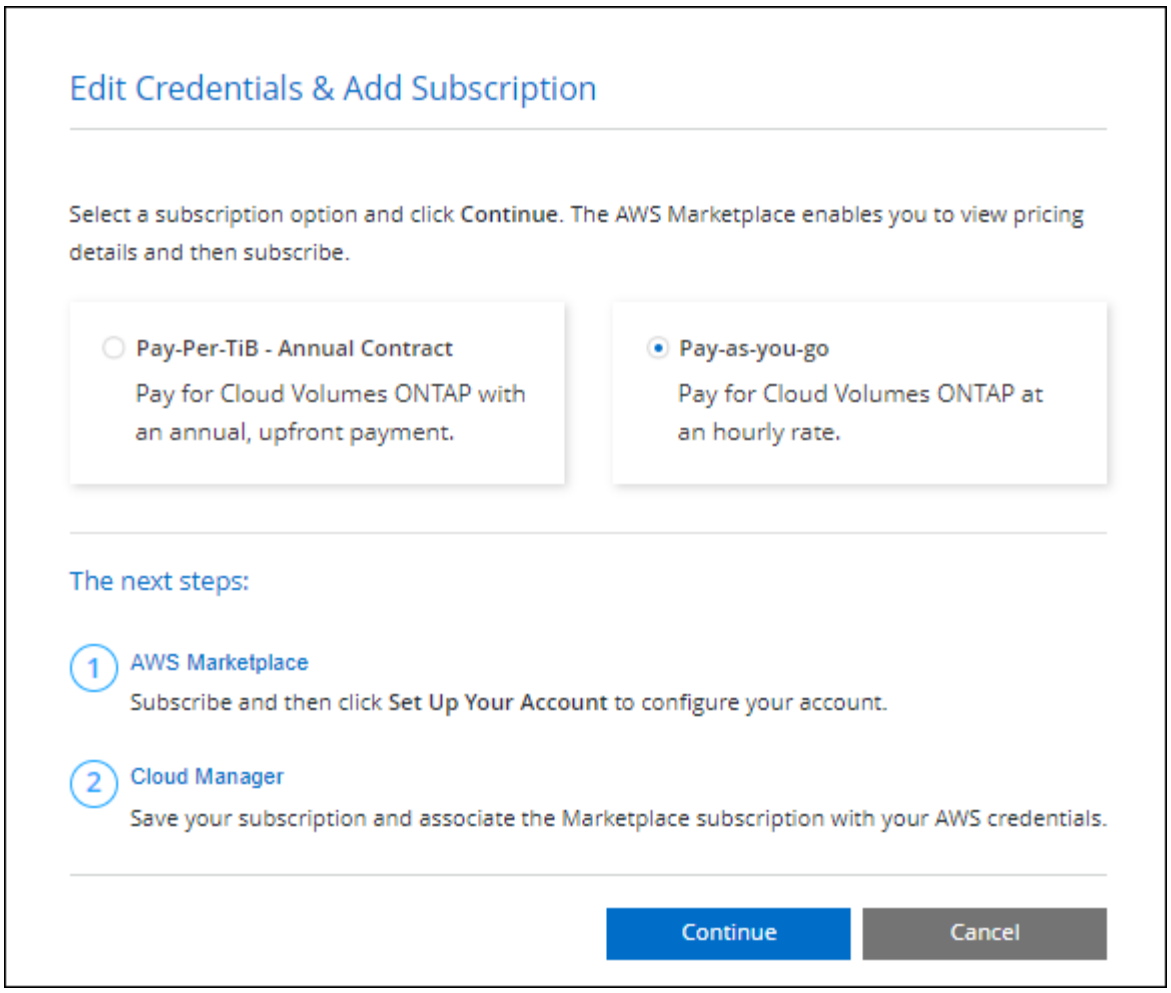
   控制台會自動查詢 NetApp 的授權服務，以取得與您的NetApp支援網站帳戶相關的授權的詳細資訊。如果沒有錯誤，控制台會自動將許可證新增至控制台。

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

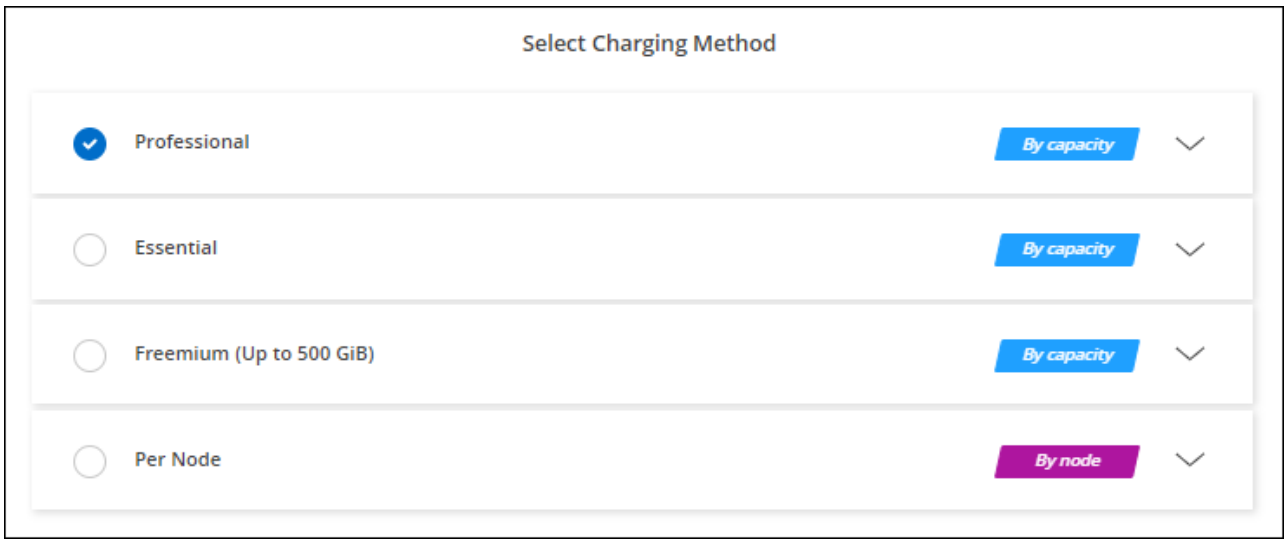
3. 在控制台的「系統」頁面上，按一下「新增系統」並依照步驟操作。

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

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



a. 返回控制台後，在到達收費方式頁面時選擇基於容量的套餐。



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

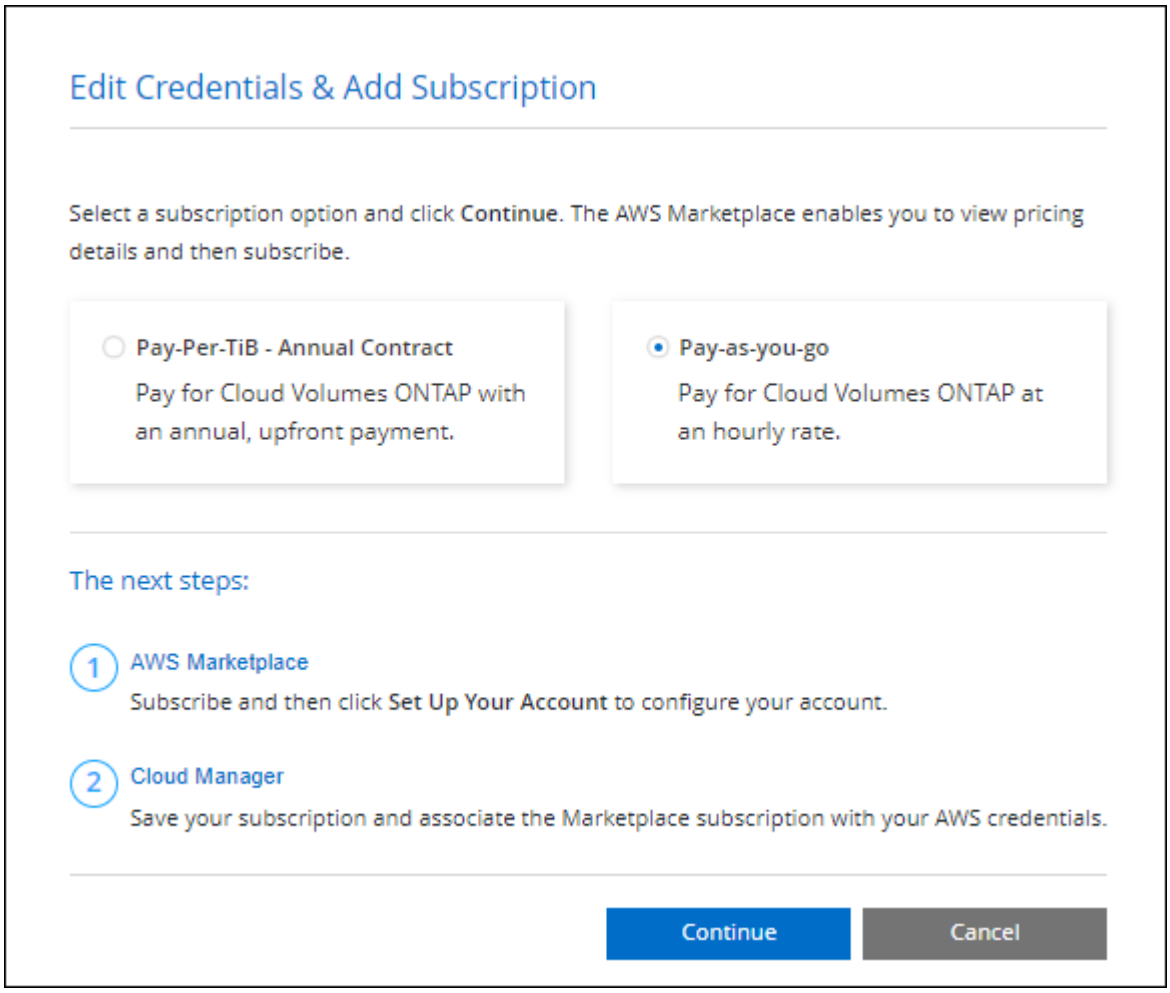
PAYGO 訂閱

透過訂閱雲端供應商市場提供的服務按小時付費。

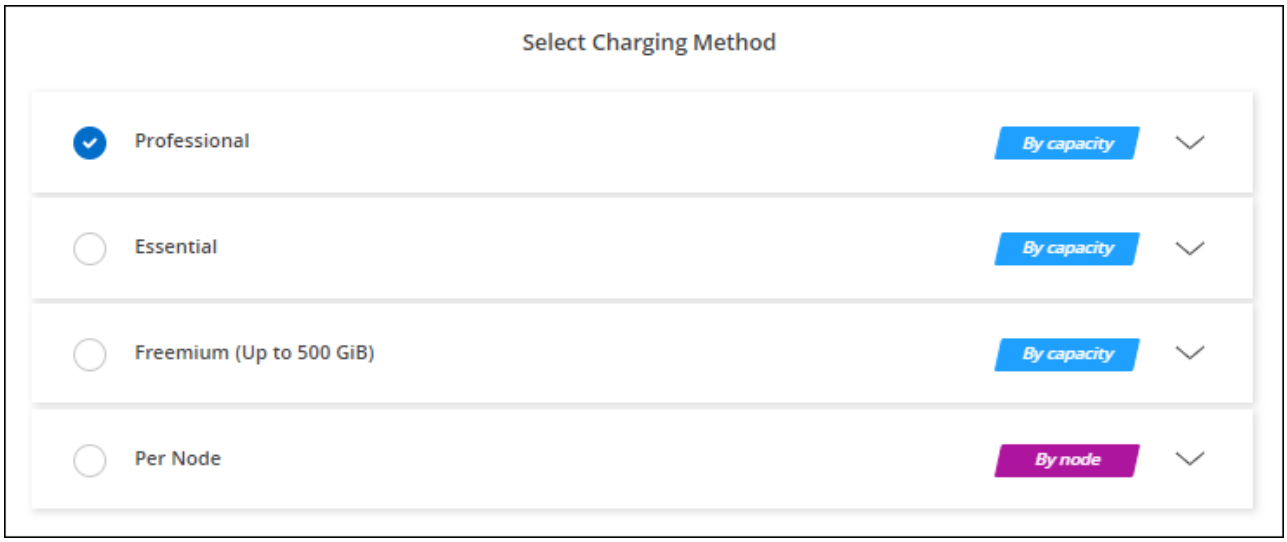
當您建立Cloud Volumes ONTAP系統時，控制台會提示您訂閱 AWS Marketplace 中提供的協定。然後將該訂閱與系統關聯以進行收費。您可以使用相同的訂閱來取得其他Cloud Volumes ONTAP系統。

步驟

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



   b. 返回控制台後，在到達收費方式頁面時選擇基於容量的套餐。



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

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

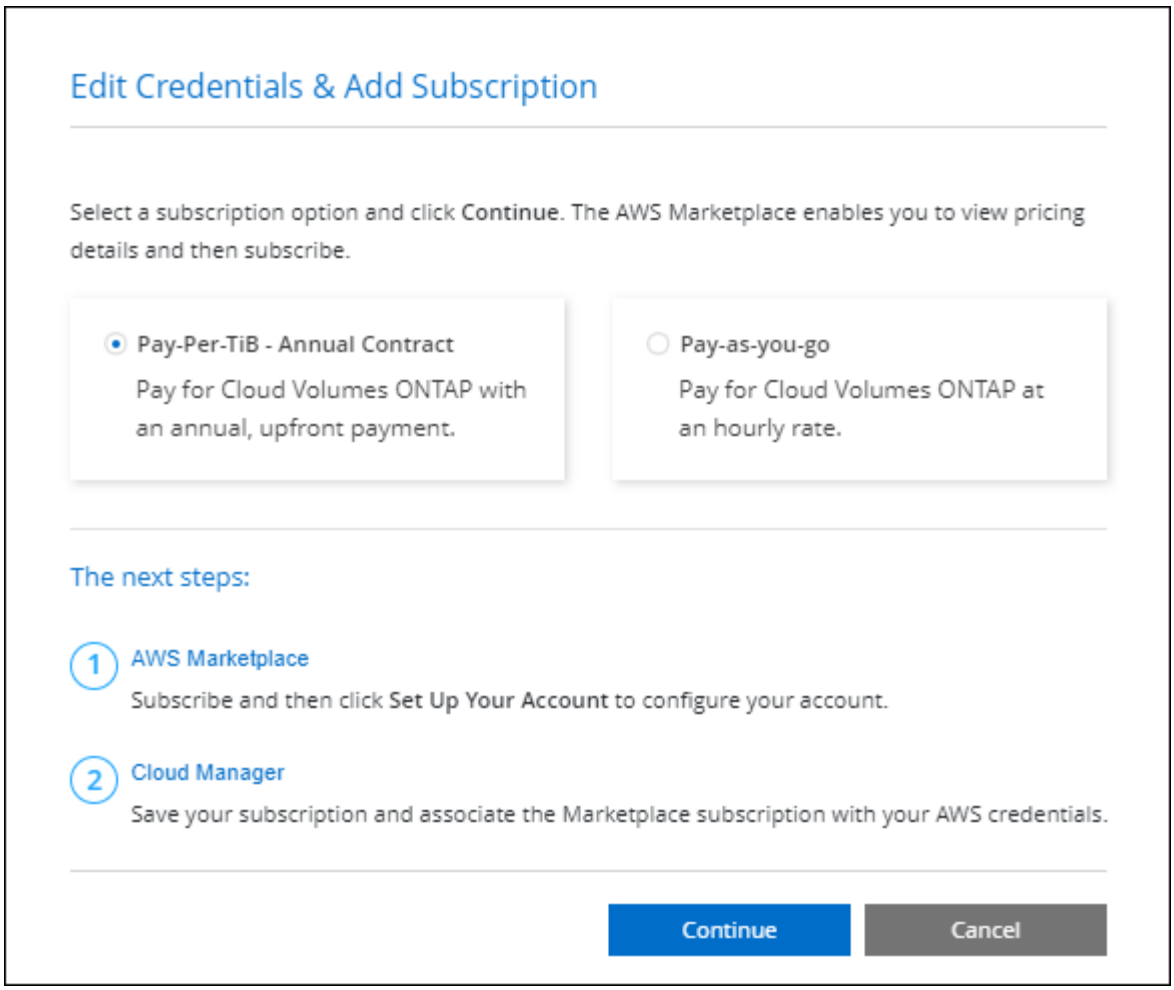
年度合約

從雲端提供者的市場購買年度合同，按年付款。

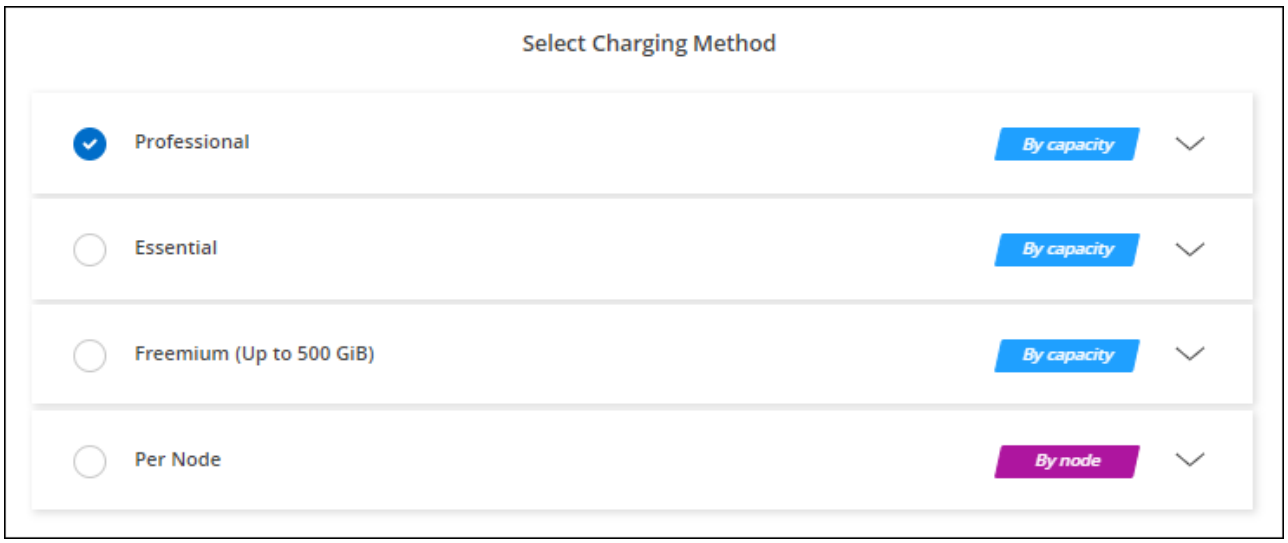
與按小時訂閱類似，控制台會提示您訂閱 AWS Marketplace 中提供的年度合約。

步驟

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



b. 返回控制台後，在到達收費方式頁面時選擇基於容量的套餐。



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

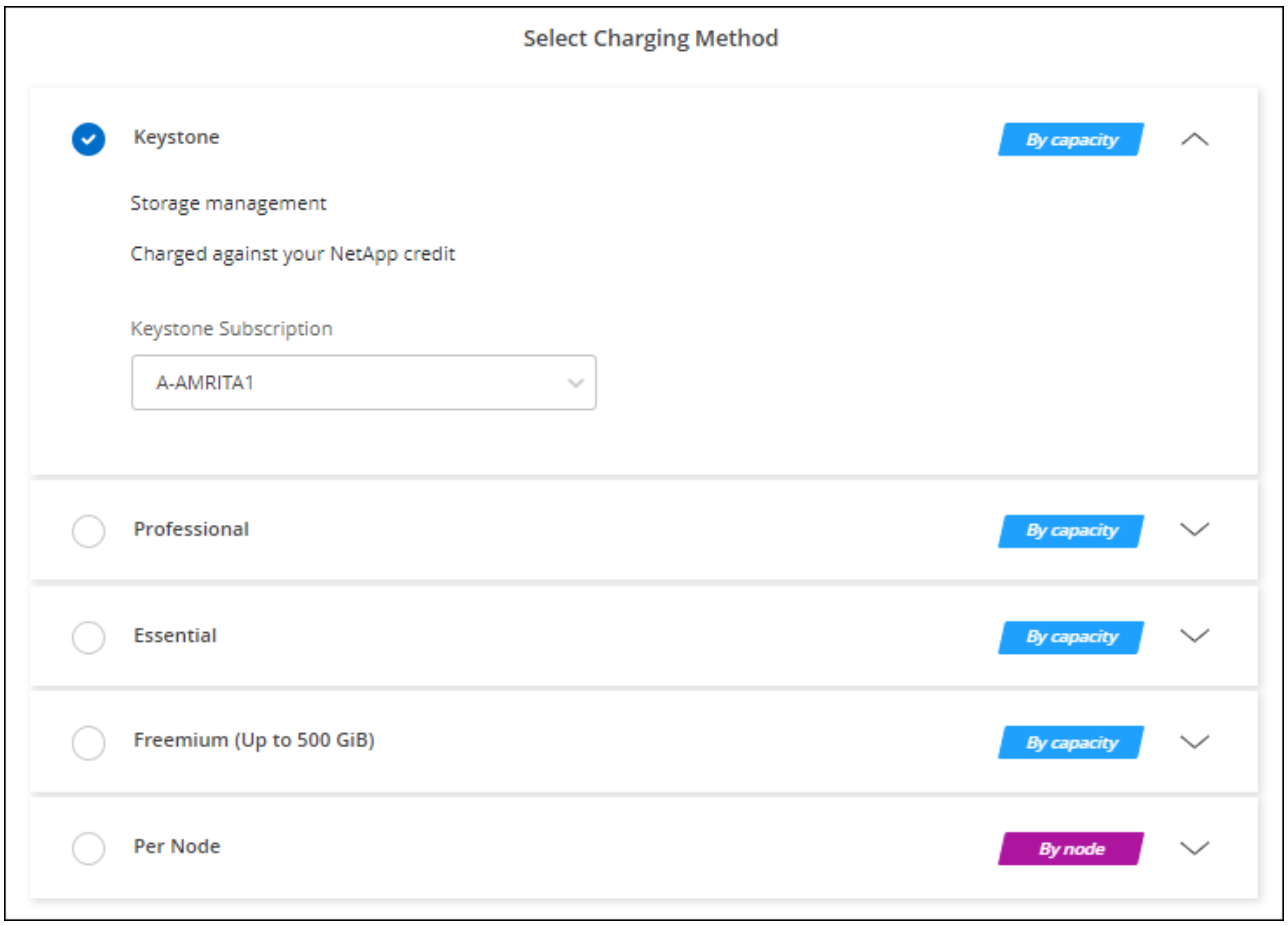
Keystone訂閱

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

步驟

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

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



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

基於節點的許可證

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

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

使用快速部署在 AWS 中部署Cloud Volumes ONTAP

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

開始之前

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

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

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

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

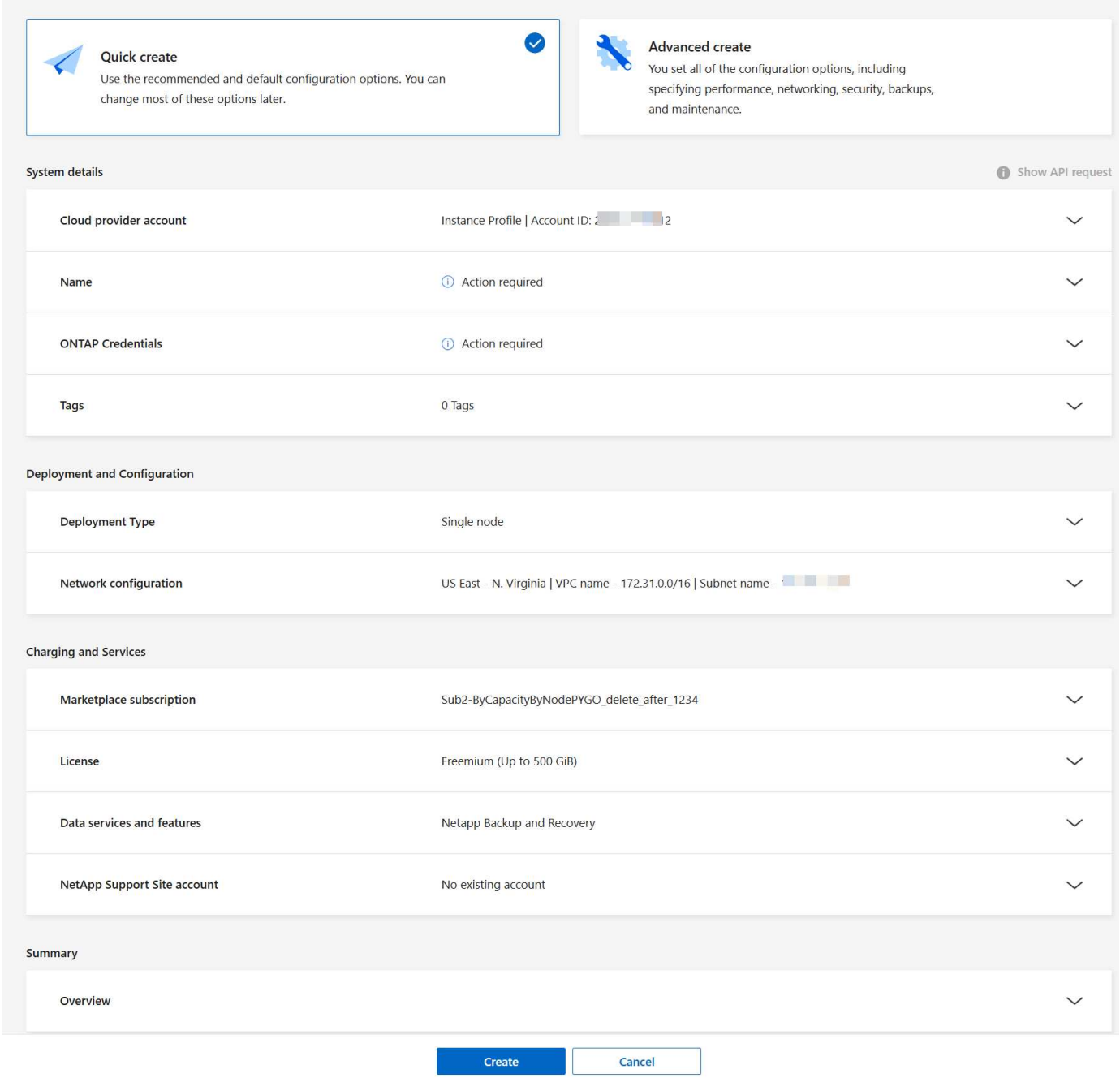
  有關詳細信息，請參閱"AWS 中Cloud Volumes ONTAP的網路需求"。

關於此任務

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

步驟

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



系統詳細信息

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

部署和配置

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

高可用性

如果您選擇了 HA 配置，請輸入以下資訊：

單可用區高可用性

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

多個可用區中的高可用性

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

充電和服務

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

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

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

總結

檢查或編輯您輸入的詳細信息，然後點擊*建立*。

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

相關連結

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

在 AWS 中啟動Cloud Volumes ONTAP

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

開始之前

開始之前您需要以下內容。

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

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

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

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

在 AWS 中啟動單節點Cloud Volumes ONTAP系統

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

關於此任務

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

步驟

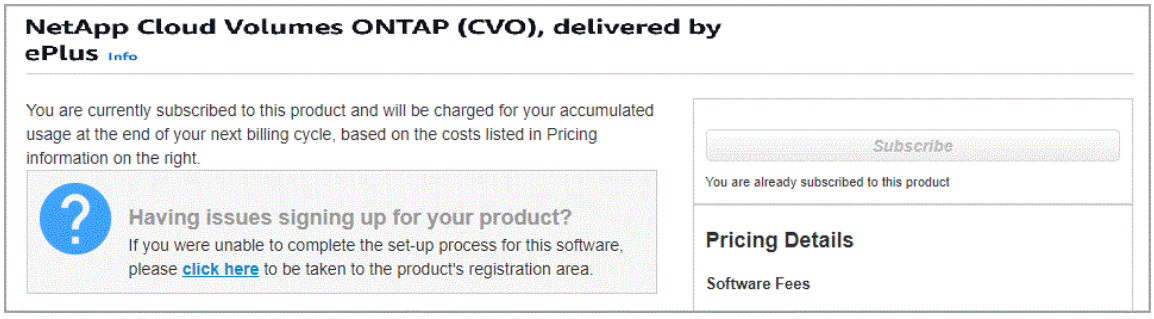
1. 從左側導覽功能表中，選擇“儲存”>“管理”。

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

   此頁面中的某些欄位是不言自明的。下表描述了您可能需要指導的欄位：

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

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



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

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

8. 位置和連接：輸入您在 "AWS 工作表"。

   下表描述了您可能需要指導的欄位：

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

9. 資料加密：選擇無資料加密或 AWS 管理加密。

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

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

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

   "了解有關受支援的加密技術的更多信息" 。

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

    如果保留預設配置，則只需要指定一個卷，然後審核並批准該配置。

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

    如果您選擇其中一個包，那麼您只需要指定一個卷，然後審核並批准配置。

13. **IAM** 角色：最好保留預設選項，讓控制台為您建立角色。

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

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

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

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

    請注意以下事項：

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

      "了解資料分層的工作原理" 。

16. 寫入速度與 **WORM**：

    a. 如有需要，請選擇*正常*或*高*寫入速度。

       "了解有關寫入速度的更多信息" 。

    b. 如果需要，請啟動一次寫入、多次讀取 (WORM) 儲存。

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

    "了解有關 WORM 存儲的更多信息" 。

    a. 如果您啟動 WORM 存儲，請選擇保留期限。

17. 建立磁碟區：輸入新磁碟區的詳細資料或點選*跳過*。

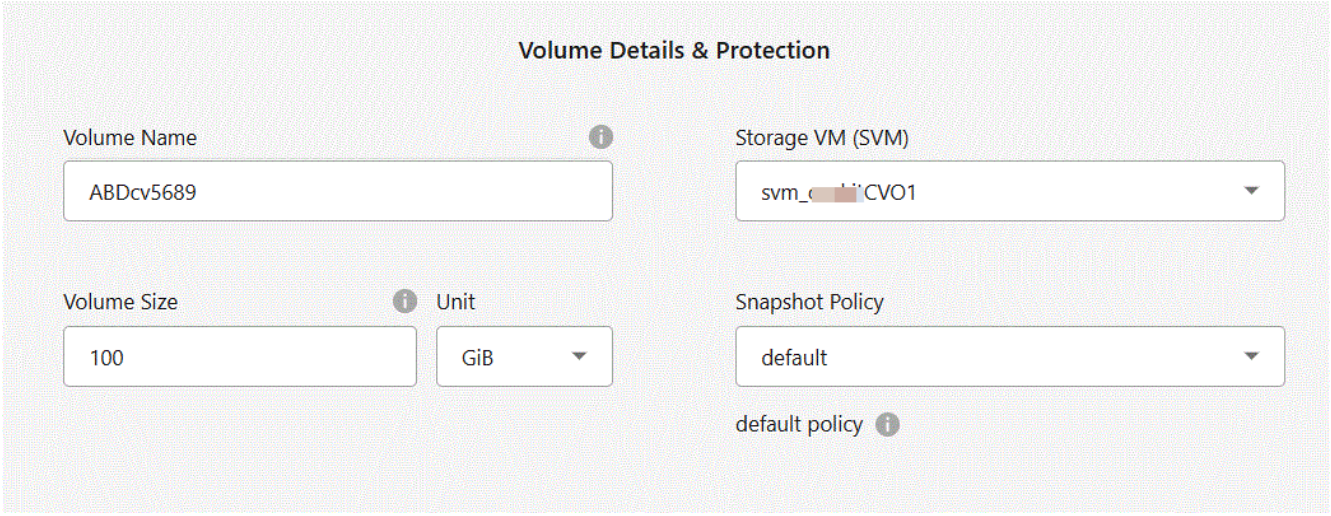
    "了解支援的客戶端協定和版本" 。

    此頁面中的某些欄位是不言自明的。下表描述了您可能需要指導的欄位：

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

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

下圖顯示了磁碟區建立精靈的第一頁：



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

場地	描述
DNS 主 IP 位址和輔助 IP 位址	為 CIFS 伺服器提供名稱解析的 DNS 伺服器的 IP 位址。所列的 DNS 伺服器必須包含定位 CIFS 伺服器將加入的網域的 Active Directory LDAP 伺服器和網域控制站所需的服務位置記錄 (SRV)。
要加入的 Active Directory 網域	您希望 CIFS 伺服器加入的 Active Directory (AD) 網域的 FQDN。
授權加入網域的憑證	具有足夠權限將電腦新增至 AD 網域內指定組織單位 (OU) 的 Windows 帳戶的名稱和密碼。
CIFS 伺服器 NetBIOS 名稱	AD 網域中唯一的 CIFS 伺服器名稱。
組織單位	AD 網域內與 CIFS 伺服器關聯的組織單位。預設值為 CN=Computers。如果將 AWS Managed Microsoft AD 配置為Cloud Volumes ONTAP 的AD 伺服器，則應在此欄位中輸入 **OU=Computers,OU=corp**。

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

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

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

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

結果

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

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

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

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

完成後

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

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

在 AWS 中啟動Cloud Volumes ONTAP HA 對

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

限制

目前，AWS Outposts 不支援 HA 對。

關於此任務

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

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

步驟

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

   一些 AWS 本地區域可用。

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

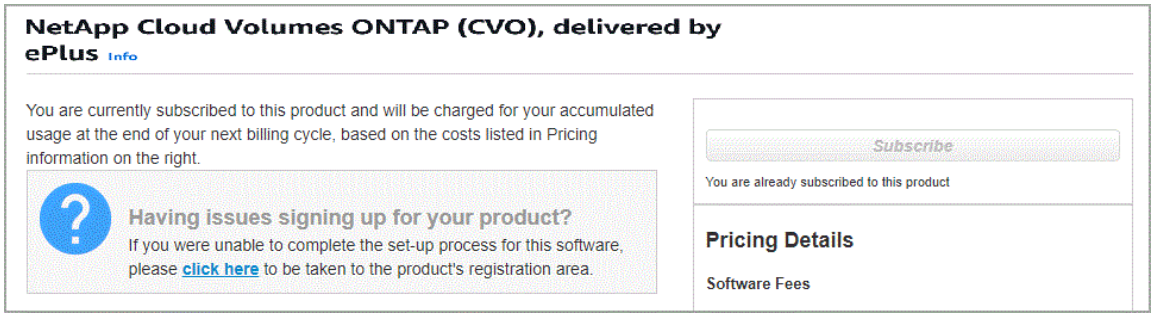
   如果您執行的是控制台代理 3.9.36 或更低版本，則需要新增 `DescribeAvailabilityZones`AWS EC2 控制台中 AWS 角色的權限。

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

   此頁面中的某些欄位是不言自明的。下表描述了您可能需要指導的欄位：

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

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



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

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

6. **HA** 部署模型：選擇 HA 配置。

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

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

   下表描述了您可能需要指導的欄位：

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

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

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

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

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

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

11. 資料加密：選擇無資料加密或 AWS 管理加密。

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

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

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

    "了解有關受支援的加密技術的更多信息" 。

12. 收費方式和 **NSS** 帳戶：指定您想要在此系統中使用的收費選項，然後指定NetApp支援網站帳戶。
    - "了解Cloud Volumes ONTAP的授權選項" 。
    - "了解如何設定許可" 。

13. * Cloud Volumes ONTAP配置*（僅限年度 AWS Marketplace 合約）：查看預設配置並點擊*繼續*或點擊*更改配置*以選擇您自己的配置。

    如果保留預設配置，則只需要指定一個卷，然後審核並批准該配置。

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

    如果您選擇其中一個包，那麼您只需要指定一個卷，然後審核並批准配置。

15. **IAM** 角色：最好保留預設選項，讓控制台為您建立角色。

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

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

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

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

    請注意以下事項：

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

"了解資料分層的工作原理" 。

18. 寫入速度與 **WORM**：

    a. 如有需要，請選擇*正常*或*高*寫入速度。

       "了解有關寫入速度的更多信息" 。

    b. 如果需要，請啟動一次寫入、多次讀取 (WORM) 儲存。

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

    "了解有關 WORM 存儲的更多信息" 。

    a. 如果您啟動 WORM 存儲，請選擇保留期限。

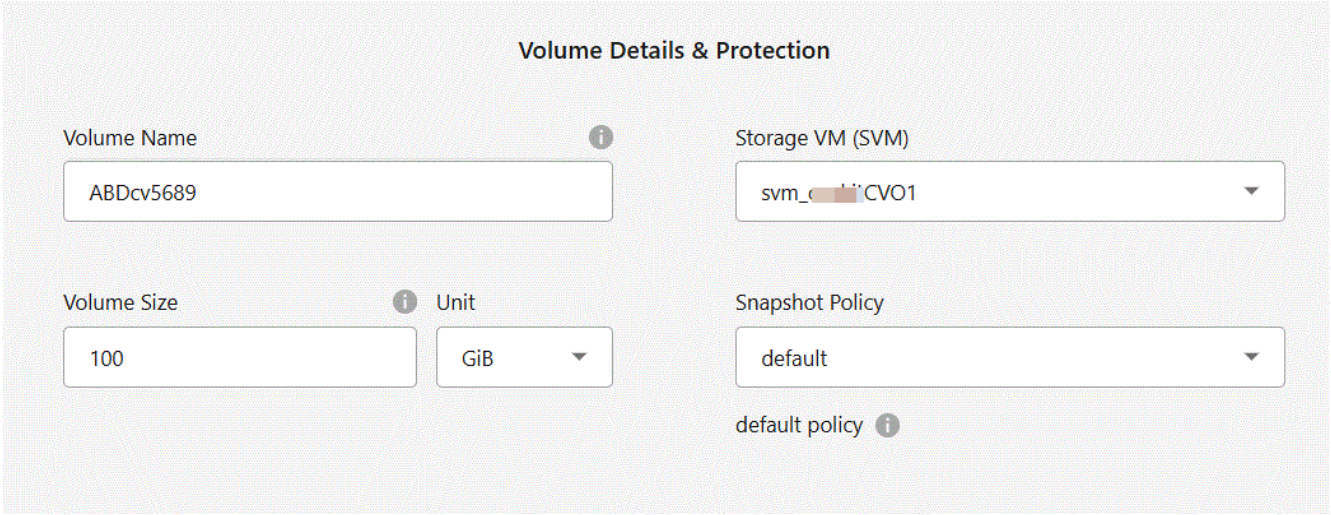
19. 建立磁碟區：輸入新磁碟區的詳細資料或點選*跳過*。

    "了解支援的客戶端協定和版本" 。

    此頁面中的某些欄位是不言自明的。下表描述了您可能需要指導的欄位：

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

    下圖顯示了磁碟區建立精靈的第一頁：



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

場地	描述
DNS 主 IP 位址和輔助 IP 位址	為 CIFS 伺服器提供名稱解析的 DNS 伺服器的 IP 位址。所列的 DNS 伺服器必須包含定位 CIFS 伺服器將加入的網域的 Active Directory LDAP 伺服器和網域控制站所需的服務位置記錄 (SRV)。
要加入的 Active Directory 網域	您希望 CIFS 伺服器加入的 Active Directory (AD) 網域的 FQDN。
授權加入網域的憑證	具有足夠權限將電腦新增至 AD 網域內指定組織單位 (OU) 的 Windows 帳戶的名稱和密碼。
CIFS 伺服器 NetBIOS 名稱	AD 網域中唯一的 CIFS 伺服器名稱。
組織單位	AD 網域內與 CIFS 伺服器關聯的組織單位。預設值為 CN=Computers。如果將 AWS Managed Microsoft AD 配置為Cloud Volumes ONTAP 的AD 伺服器，則應在此欄位中輸入 **OU=Computers,OU=corp**。
DNS 網域	Cloud Volumes ONTAP儲存虛擬機器 (SVM) 的 DNS 網域。大多數情況下，該域與 AD 域相同。
NTP 伺服器	選擇「使用 Active Directory 網域」以使用 Active Directory DNS 設定 NTP 伺服器。如果您需要使用不同的位址來設定 NTP 伺服器，那麼您應該使用 API。請參閱 "NetApp Console自動化文檔"了解詳情。請注意，只有在建立 CIFS 伺服器時才能設定 NTP 伺服器。建立 CIFS 伺服器後，它不可配置。

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

    更多信息，請參閱"選擇卷使用情況設定檔"和"資料分層概述"。

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

結果

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

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

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

完成後

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

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

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

相關連結

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

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

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

開始之前

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

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

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

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

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

步驟 1：設定網絡

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

步驟

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

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

步驟 2：設定權限

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

您需要針對以下各項制定 IAM 策略和 IAM 角色：

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

步驟

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

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

秘密區域

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

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

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

絕密地區

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

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

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

```
        ]
}
```

3. 為Cloud Volumes ONTAP建立策略。

秘密區域

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

絕密地區

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

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

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

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

   創建角色：

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

   選擇角色：

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

步驟 3：設定 AWS KMS

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

步驟

1. 確保您的帳戶或其他 AWS 帳戶中存在有效的客戶主金鑰 (CMK)。

   CMK 可以是 AWS 管理的 CMK 或客戶管理的 CMK。

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

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

3. 將執行個體的 IAM 角色新增至 CMK 的金鑰使用者清單。

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

步驟 4：安裝控制台代理程式並設定控制台

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

步驟

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

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

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

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

      配置實例時請注意以下事項：

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

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

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

步驟 5：（可選）安裝私有模式憑證

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

步驟

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

   ```
   docker ps
   ```

   b. 若要進入 occm 容器，請執行下列命令：

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

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

   ```
   env
   ```

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

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

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

   ```
   docker ps
   ```

   b. 若要進入 occm 容器，請執行下列命令：

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

   將新的證書文件保存在裡面。

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

   ```
   env
   ```

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

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

e. 若要檢查憑證是否已安裝，請執行以下命令：

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

f. 若要退出 occm 容器，請執行下列命令：

```
exit
```

g. 若要重設 occm 容器，請執行下列命令：

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

步驟 6：向控制台新增許可證

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

步驟

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

結果

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

步驟 7：從控制台啟動Cloud Volumes ONTAP

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

開始之前

對於 HA 對，需要金鑰對來啟用對 HA 中介的基於金鑰的 SSH 驗證。

步驟

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

   對於 HA：在 建立 下，選擇Cloud Volumes ONTAP或Cloud Volumes ONTAP HA。
3. 完成精靈中的步驟以啟動Cloud Volumes ONTAP系統。

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

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

完成 HA 對嚮導時請注意以下事項。

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

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

完成精靈時請注意以下事項：

- 您應該保留預設選項以使用產生的安全性群組。

  預先定義的安全性群組包含Cloud Volumes ONTAP成功運作所需的規則。如果您有使用自己的需求，可以參考下面的安全群組部分。
- 您必須選擇在準備 AWS 環境時所建立的 IAM 角色。
- 底層 AWS 磁碟類型適用於初始Cloud Volumes ONTAP磁碟區。

  您可以為後續磁碟區選擇不同的磁碟類型。
- AWS 磁碟的效能與磁碟大小相關。

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

- 磁碟大小是系統上所有磁碟的預設大小。

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

結果

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

步驟 8：安裝資料分層的安全性證書

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

開始之前

1. 建立 S3 儲存桶。

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

2. 保留您安裝的根證書 `step 4`便利。

步驟

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

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

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

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

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

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