設定用戶端連線
StorageGRID

NetApp
November 04, 2025

目錄

設定用戶端連線 1
設定 S3 和 Swift 用戶端連線：總覽 1
組態工作流程 1
將 StorageGRID 附加至用戶端應用程式所需的資訊 2
S3 或 Swift 用戶端的安全性 4
摘要 4
StorageGRID 如何為用戶端應用程式提供安全性 4
TLS程式庫支援的雜湊和加密演算法 5
使用 S3 設定精靈 5
使用 S3 設定精靈：考量與需求 5
存取並完成 S3 設定精靈 6
管理 HA 群組 15
管理高可用度（HA）群組：總覽 15
如何使用HA群組？ 17
HA群組的組態選項 18
設定高可用度群組 20
管理負載平衡 25
負載平衡考量 25
設定負載平衡器端點 28
設定 S3 端點網域名稱 37
新增 S3 端點網域名稱 38
重新命名 S3 端點網域名稱 38
刪除 S3 端點網域名稱 38
摘要：用於用戶端連線的IP位址和連接埠 39
URL 範例 39
何處可以找到 IP 位址 39

設定用戶端連線

設定 S3 和 Swift 用戶端連線：總覽

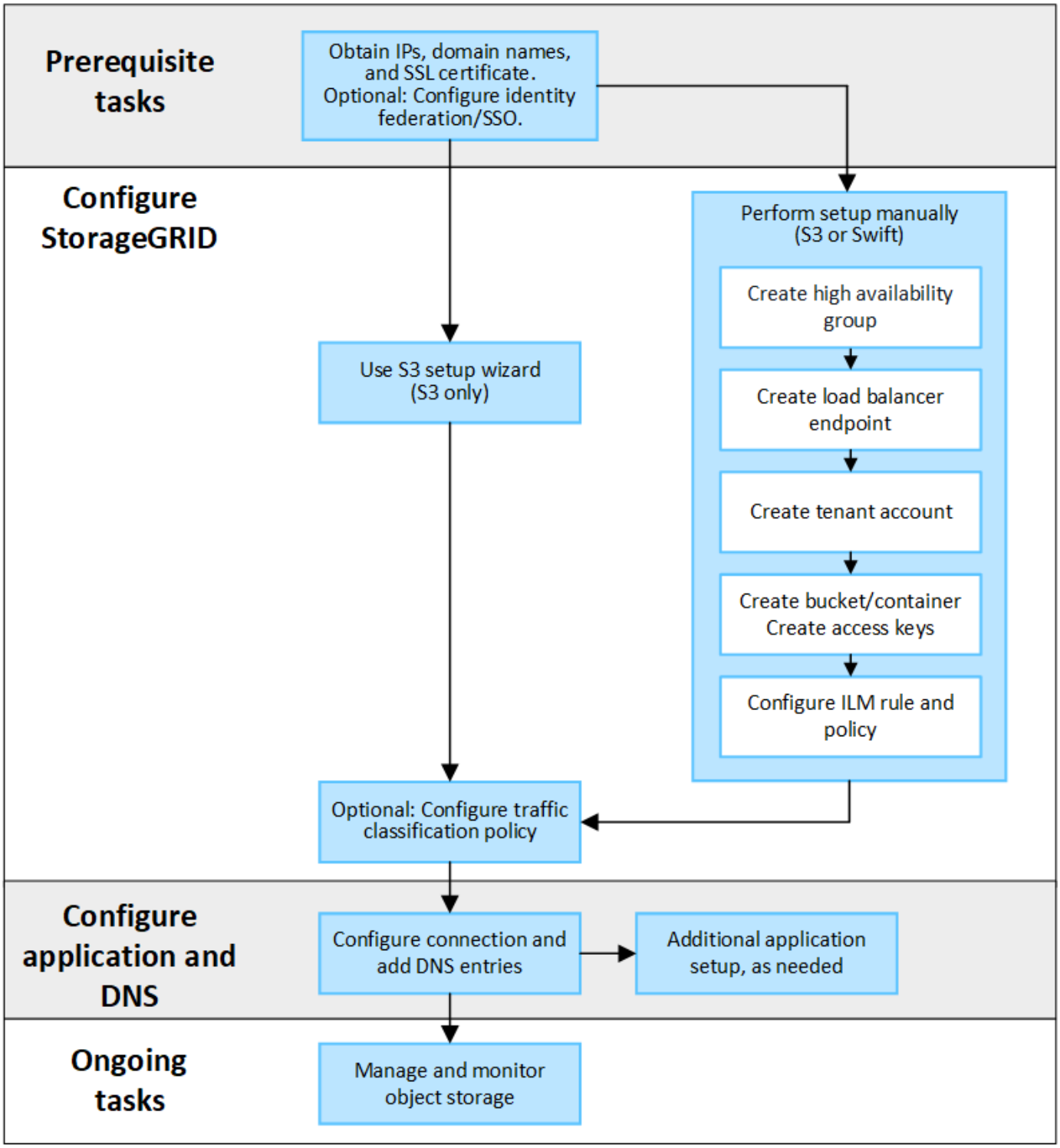
身為網格管理員、您可以管理組態選項、以控制 S3 和 Swift 用戶端應用程式如何連線至 StorageGRID 系統、以儲存和擷取資料。

Swift 用戶端應用程式的支援已過時、未來版本將會移除。

組態工作流程

如工作流程圖所示、將 StorageGRID 連接至任何 S3 或 Swift 應用程式有四個主要步驟：

1. 根據用戶端應用程式與 StorageGRID 的連線方式、在 StorageGRID 中執行必要工作。
2. 使用 StorageGRID 取得應用程式連線至網格所需的值。您可以使用 S3 設定精靈、或手動設定每個 StorageGRID 實體。
3. 使用 S3 或 Swift 應用程式完成 StorageGRID 連線。建立 DNS 項目、將 IP 位址與您打算使用的任何網域名稱建立關聯。
4. 在應用程式和 StorageGRID 中執行持續的工作、以隨時間而管理和監控物件儲存。



將 StorageGRID 附加至用戶端應用程式所需的資訊

在您將 StorageGRID 附加到 S3 或 Swift 用戶端應用程式之前、您必須先在 StorageGRID 中執行組態步驟、並取得特定值。

我需要什麼價值？

下表顯示您必須在 StorageGRID 中設定的值、以及 S3 或 Swift 應用程式和 DNS 伺服器使用這些值的位置。

價值	其中已設定值	使用值的位置
虛擬 IP （ VIP ）位址	StorageGRID > HA 群組	DNS 項目
連接埠	StorageGRID > 負載平衡器端點	用戶端應用程式
SSL 憑證	StorageGRID > 負載平衡器端點	用戶端應用程式
伺服器名稱（ FQDN ）	StorageGRID > 負載平衡器端點	• 用戶端應用程式 • DNS 項目
S3 存取金鑰 ID 和秘密存取金鑰	StorageGRID > 租戶與貯體	用戶端應用程式
貯體 / 容器名稱	StorageGRID > 租戶與貯體	用戶端應用程式

如何取得這些價值？

視您的需求而定、您可以執行下列任一動作來取得所需資訊：

- * 使用 "S3 設定精靈"*。S3 安裝精靈可協助您快速設定 StorageGRID 中的必要值、並輸出一個或兩個檔案、供您在設定 S3 應用程式時使用。精靈會引導您完成必要步驟、並協助確保您的設定符合 StorageGRID 最佳實務做法。

  如果您正在設定 S3 應用程式、建議您使用 S3 安裝精靈、除非您知道自己有特殊需求、否則實作將需要大量自訂。

- * 使用 "FabricPool 設定精靈"*。與 S3 設定精靈類似、 FabricPool 設定精靈可協助您快速設定所需的值、並輸出可在 ONTAP 中設定 FabricPool 雲端層時使用的檔案。

  如果您計畫將 StorageGRID 作為 FabricPool 雲端層的物件儲存系統、建議您使用 FabricPool 設定精靈、除非您知道自己有特殊需求、否則實作將需要大量自訂。

- * 手動設定項目 * 。如果您要連線至 Swift 應用程式（或是連線至 S3 應用程式、而不想使用 S3 安裝精靈）、您可以手動執行組態來取得所需的值。請遵循下列步驟：

  a. 設定您要用於 S3 或 Swift 應用程式的高可用度（ HA ）群組。請參閱 "設定高可用度群組"。

  b. 建立 S3 或 Swift 應用程式將使用的負載平衡器端點。請參閱 "設定負載平衡器端點"。

  c. 建立 S3 或 Swift 應用程式將使用的租戶帳戶。請參閱 "建立租戶帳戶"。

  d. 對於 S3 租戶、請登入租戶帳戶、然後為每個存取應用程式的使用者產生存取金鑰 ID 和秘密存取金鑰。請參閱 "建立您自己的存取金鑰"。

  e. 在租戶帳戶內建立一或多個 S3 貯體或 Swift 容器。如需 S3 的詳細資訊、請參閱 "建立S3儲存區"。若要使用 Swift 、請使用 "提交容器要求"。

  f. 若要為屬於新租戶或貯體 / 容器的物件新增特定放置指示、請建立新的 ILM 規則、並啟動新的 ILM 原則以使用該規則。請參閱 "建立ILM規則" 和 "建立ILM原則"。

S3 或 Swift 用戶端的安全性

StorageGRID 租戶帳戶使用 S3 或 Swift 用戶端應用程式、將物件資料儲存至 StorageGRID 。您應該檢閱為用戶端應用程式實作的安全性措施。

摘要

下表摘要說明如何為 S3 和 Swift REST API 實作安全性：

安全問題	**REST API**的實作
連線安全性	TLS
伺服器驗證	由系統CA或系統管理員提供的自訂伺服器憑證簽署的X・509伺服器憑證
用戶端驗證	**S3** S3 帳戶（存取金鑰 ID 和秘密存取金鑰） **Swift** Swift 帳戶（使用者名稱和密碼）
用戶端授權	**S3** 貯體擁有權及所有適用的存取控制原則 **Swift** 系統管理員角色存取

StorageGRID 如何為用戶端應用程式提供安全性

S3 和 Swift 用戶端應用程式可以連線至 Gateway 節點或管理節點上的負載平衡器服務、或直接連線至 Storage Node 。

- 連線至負載平衡器服務的用戶端可以根據您的方式使用 HTTPS 或 HTTP "設定負載平衡器端點"。

  HTTPS 提供安全的 TLS 加密通訊、建議使用。您必須將安全性憑證附加至端點。

  HTTP 提供較不安全的未加密通訊、只能用於非正式作業或測試網格。

- 連線至儲存節點的用戶端也可以使用 HTTPS 或 HTTP 。

  HTTPS 是預設值、建議使用。

  HTTP 提供較不安全、未加密的通訊、但可選擇性使用 "已啟用" 適用於非正式作業或測試網格。

- 支援使用TLS加密支援不支援的客戶端與StorageGRID 之通訊。
- 無論負載平衡器端點是設定為接受HTTP或HTTPS連線、網格內負載平衡器服務與儲存節點之間的通訊都會加密。

- 用戶端必須提供HTTP驗證標頭StorageGRID 給才能執行REST API作業。請參閱 "驗證要求" 和 "支援的Swift API端點"。

安全性憑證與用戶端應用程式

在任何情況下、用戶端應用程式都可以使用網格管理員上傳的自訂伺服器憑證或StorageGRID 由該系統產生的憑證來建立TLS連線：

- 當用戶端應用程式連線到負載平衡器服務時、會使用為負載平衡器端點設定的憑證。每個負載平衡器端點都有自己的憑證 &#8212 ；網格管理員上傳的自訂伺服器憑證、或是網格管理員在設定端點時在 StorageGRID 中產生的憑證。

  請參閱 "負載平衡考量"。

- 當用戶端應用程式直接連線至儲存節點時、它們會使用安裝 StorageGRID 系統（由系統憑證授權單位簽署）時為儲存節點產生的系統產生的伺服器憑證、 或是由網格管理員提供給網格的單一自訂伺服器憑證。請參閱 "新增自訂 S3 或 Swift API 憑證"。

用戶端應設定為信任已簽署其用於建立TLS連線之任何憑證的憑證授權單位。

TLS程式庫支援的雜湊和加密演算法

StorageGRID 系統支援一組加密套件、用戶端應用程式可在建立 TLS 工作階段時使用這些套件。要配置加密算法，請轉至 * 配置 * > * 安全性 * > * 安全性設置 * ，然後選擇 *TLS 和 SSH 策略 * 。

支援的**TLS**版本

支援TLS 1.2和TLS 1.3。StorageGRID

> 不再支援SSLv3和TLS 1.1（或更早版本）。

使用 S3 設定精靈

使用 S3 設定精靈：考量與需求

您可以使用 S3 設定精靈、將 StorageGRID 設定為 S3 應用程式的物件儲存系統。

何時使用 **S3** 設定精靈

S3 安裝精靈會引導您完成每個步驟、設定 StorageGRID 以搭配 S3 應用程式使用。在完成精靈的過程中、您可以下載檔案、以便在 S3 應用程式中輸入值。使用精靈可更快速地設定您的系統、並確保您的設定符合 StorageGRID 最佳實務做法。

如果您有 "root 存取權限"、您可以在開始使用 StorageGRID Grid Manager 時完成 S3 設定精靈、也可以隨時存取並完成精靈。視您的需求而定、您也可以手動設定部分或全部必要項目、然後使用精靈來組合 S3 應用程式所需的值。

使用精靈之前

使用精靈之前、請確認您已完成這些先決條件。

取得 **IP** 位址並設定 **VLAN** 介面

如果您要設定高可用度（ HA ）群組、就會知道 S3 應用程式將連線到哪些節點、以及將使用哪個 StorageGRID 網路。您也知道要輸入哪些子網路 CIDR 、閘道 IP 位址和虛擬 IP （ VIP ）位址值。

如果您打算使用虛擬 LAN 來分隔 S3 應用程式的流量、則表示您已經設定了 VLAN 介面。請參閱 "設定VLAN介面"。

設定身分識別聯盟和 **SSO**

如果您計畫在 StorageGRID 系統上使用身分識別聯盟或單一登入（ SSO ）、則表示您已啟用這些功能。您也知道 S3 應用程式將使用哪個同盟群組的租戶帳戶擁有 root 存取權。請參閱 "使用身分識別聯盟" 和 "設定單一登入"。

取得及設定網域名稱

您知道 StorageGRID 要使用哪個完整網域名稱（ FQDN ）。網域名稱伺服器（ DNS ）項目會將此 FQDN 對應到您使用精靈建立的 HA 群組的虛擬 IP （ VIP ）位址。

如果您計畫使用 S3 虛擬託管式要求、您應該要有 "已設定 S3 端點網域名稱"。建議使用虛擬託管式要求。

檢閱負載平衡器和安全性憑證需求

如果您計畫使用 StorageGRID 負載平衡器、您已檢閱負載平衡的一般考量事項。您擁有要上傳的憑證或產生憑證所需的值。

如果您打算使用外部（第三方）負載平衡器端點、則該負載平衡器具有完整網域名稱（ FQDN ）、連接埠和憑證。

設定任何網格同盟連線

如果您想要允許 S3 租戶複製帳戶資料、並使用網格同盟連線將貯體物件複寫到其他網格、請在啟動精靈之前確認下列事項：

- 您有 "已設定網格同盟連線"。
- 連線狀態為 * 已連線 * 。
- 您擁有root存取權限。

存取並完成 **S3** 設定精靈

您可以使用 S3 設定精靈來設定 StorageGRID 、以便搭配 S3 應用程式使用。安裝精靈提供應用程式存取 StorageGRID 儲存區和儲存物件所需的值。

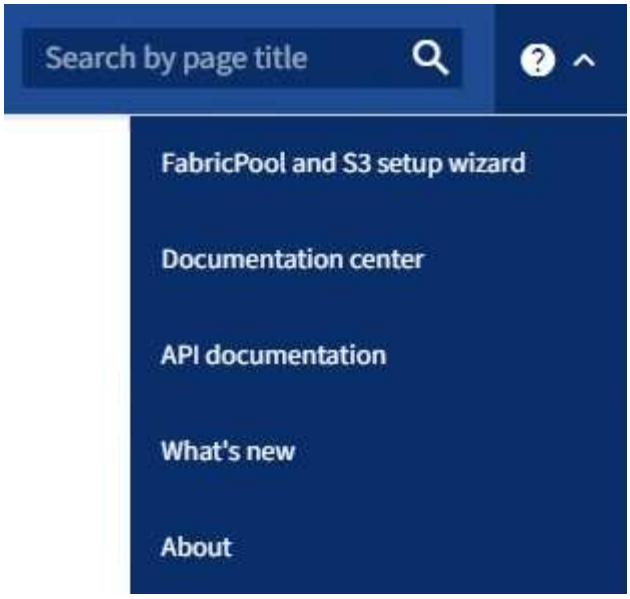
開始之前

- 您擁有 "root 存取權限"。
- 您已檢閱 "考量與要求" 以使用精靈。

存取精靈

步驟

1. 使用登入Grid Manager "支援的網頁瀏覽器"。
2. 如果儀表板上出現 * FabricPool 和 S3 設定精靈 * 橫幅、請選取橫幅中的連結。如果橫幅不再出現、請從 Grid Manager 的標題列中選取說明圖示、然後選取 * FabricPool 和 S3 設定精靈 * 。



3. 在 FabricPool and S3 安裝精靈頁面的 S3 應用程式區段中、選取 * 立即設定 * 。

步驟 **6** 之 **1** ：設定 **HA** 群組

HA 群組是每個節點包含 StorageGRID 負載平衡器服務的集合。HA 群組可以包含閘道節點、管理節點或兩者。

您可以使用 HA 群組來協助保持 S3 資料連線可用。如果 HA 群組中的作用中介面發生故障、備份介面就能管理工作負載、對 S3 作業幾乎沒有影響。

如需此工作的詳細資訊、請參閱 "管理高可用度群組"。

步驟

1. 如果您打算使用外部負載平衡器、則不需要建立 HA 群組。選取 * 略過此步驟 * 並前往 步驟 2 、共 6 步：設定負載平衡器端點。
2. 若要使用 StorageGRID 負載平衡器、您可以建立新的 HA 群組或使用現有的 HA 群組。

建立**HA**群組

a. 若要建立新的 HA 群組、請選取 * 建立 HA 群組 * 。

b. 如需 * 輸入詳細資料 * 步驟、請填寫下列欄位。

欄位	說明
HA 群組名稱	此 HA 群組的唯一顯示名稱。
說明（選用）	此 HA 群組的描述。

c. 在 * 新增介面 * 步驟中、選取您要在此 HA 群組中使用的節點介面。

使用欄標題來排序列、或輸入搜尋詞彙以更快找到介面。

您可以選取一或多個節點、但每個節點只能選取一個介面。

d. 對於「介面優先順序」步驟、請判斷此 HA 群組的主要介面和任何備份介面。

拖曳列以變更 * 優先順序 * 欄中的值。

清單中的第一個介面是主要介面。主介面是作用中介面、除非發生故障。

如果 HA 群組包含多個介面、且作用中介面故障、則虛擬 IP （ VIP ）位址會依照優先順序移至第一個備份介面。如果該介面故障、VIP位址會移至下一個備份介面、依此類推。解決故障時、 VIP 位址會移回可用的最高優先順序介面。

e. 在 * 輸入 IP 位址 * 步驟中、請填寫下列欄位。

欄位	說明
子網路 CIDR	以 CIDR 表示法和 #8212 表示的 VIP 子網路位址； IPv4 位址後面接著斜線和子網路長度（ 0-32 ）。 網路位址不得設定任何主機位元。例如、 `192.16.0.0/22`。
閘道 IP 位址（選用）	如果用於存取 StorageGRID 的 S3 IP 位址與 StorageGRID VIP 位址不在同一子網路上、請輸入 StorageGRID VIP 本機閘道 IP 位址。本機閘道IP位址必須位於VIP子網路內。
虛擬 IP 位址	為 HA 群組中的作用中介面輸入至少一個且不超過十個 VIP 位址。所有 VIP 位址都必須位於 VIP 子網路內。 至少一個位址必須是 IPv4 。您也可以指定其他的IPv6位址。

f. 選取 * 建立 HA 群組 * 、然後選取 * 完成 * 以返回 S3 設定精靈。

g. 選取 * 繼續 * 以移至負載平衡器步驟。

使用現有 **HA** 群組

a. 若要使用現有的 HA 群組、請從 * 選取 HA 群組 * 中選取 HA 群組名稱。

b. 選取 * 繼續 * 以移至負載平衡器步驟。

步驟 **2** 、共 **6** 步：設定負載平衡器端點

StorageGRID 使用負載平衡器從用戶端應用程式管理工作負載。負載平衡可將多個儲存節點的速度和連線容量最大化。

您可以使用 StorageGRID 負載平衡器服務（存在於所有閘道和管理節點上）、也可以連線至外部（第三方）負載平衡器。建議使用 StorageGRID 負載平衡器。

如需此工作的詳細資訊、請參閱 "負載平衡考量"。

若要使用 StorageGRID 負載平衡器服務、請選取 * StorageGRID 負載平衡器 * 索引標籤、然後建立或選取您要使用的負載平衡器端點。若要使用外部負載平衡器、請選取 * 外部負載平衡器 * 索引標籤、並提供您已設定之系統的詳細資料。

建立端點

步驟

1. 若要建立負載平衡器端點、請選取 * 建立端點 * 。
2. 如需 * 輸入端點詳細資料 * 步驟、請填寫下列欄位。

欄位	說明
名稱	端點的描述性名稱。
連接埠	您要用於負載平衡的選用功能。StorageGRID此欄位預設為您建立的第一個端點為 10433 、但您可以輸入任何未使用的外部連接埠。如果您輸入 80 或 443 、則端點只能在 Gateway 節點上設定、因為這些連接埠是保留在管理節點上。 • 注意： * 不允許其他網格服務使用的連接埠。請參閱 "網路連接埠參考"。
用戶端類型	必須是 *S3 * 。
網路傳輸協定	選擇* HTTPS *。 • 注意 * ：支援與 StorageGRID 通訊、但不建議使用 TLS 加密。

3. 對於 *Select 綁定模式 * 步驟，請指定綁定模式。繫結模式可控制使用任何 IP 位址或使用特定 IP 位址和網路介面存取端點的方式。

模式	說明
全域（預設）	用戶端可以使用任何閘道節點或管理節點的 IP 位址、任何網路上任何 HA 群組的虛擬 IP （ VIP ）位址、或對應的 FQDN 來存取端點。 除非您需要限制此端點的存取能力、否則請使用* Global *設定（預設）。
HA群組的虛擬IP	用戶端必須使用 HA 群組的虛擬 IP 位址（或對應的 FQDN ）才能存取此端點。 具有此繫結模式的端點都可以使用相同的連接埠編號、只要您為端點選取的 HA 群組不會重疊。
節點介面	用戶端必須使用所選節點介面的 IP 位址（或對應的 FQDN ）來存取此端點。
節點類型	根據您選取的節點類型、用戶端必須使用任何管理節點的 IP 位址（或對應的 FQDN ）或任何閘道節點的 IP 位址（或對應的 FQDN ）來存取此端點。

4. 對於租戶存取步驟、請選取下列其中一項：

欄位	說明
允許所有租戶（預設）	所有租戶帳戶都可以使用此端點來存取他們的貯體。
允許選取的租戶	只有選取的租戶帳戶才能使用此端點存取其貯體。
封鎖選取的租戶	選取的租戶帳戶無法使用此端點存取其儲存區。所有其他租戶都可以使用此端點。

5. 對於 * 附加憑證 * 步驟、請選取下列其中一項：

欄位	說明
上傳憑證（建議）	使用此選項可上傳 CA 簽署的伺服器憑證、憑證私密金鑰及選用的 CA 套件組合。
產生憑證	使用此選項可產生自我簽署的憑證。請參閱 "設定負載平衡器端點" 以取得詳細的輸入內容。
使用 StorageGRID S3 和 Swift 憑證	只有在您已上傳或產生 StorageGRID 通用憑證的自訂版本時、才可使用此選項。請參閱 "設定S3和Swift API憑證" 以取得詳細資料。

6. 選擇 * 完成 * 返回 S3 設定精靈。
7. 選擇 * 繼續 * 以前往租戶和貯體步驟。

對端點憑證所做的變更、可能需要15分鐘才能套用至所有節點。

使用現有負載平衡器端點

步驟

1. 若要使用現有的端點、請從 * 選取負載平衡器端點 * 中選取其名稱。
2. 選擇 * 繼續 * 以前往租戶和貯體步驟。

使用外部負載平衡器

步驟

1. 若要使用外部負載平衡器、請填寫下列欄位。

欄位	說明
FQDN	外部負載平衡器的完整網域名稱（ FQDN ）。
連接埠	S3 應用程式用來連線到外部負載平衡器的連接埠編號。

欄位	說明
憑證	複製外部負載平衡器的伺服器憑證、然後貼到此欄位。

2. 選擇 * 繼續 * 以前往租戶和貯體步驟。

步驟 **3** 、共 **6** 步：建立租戶和貯體

租戶是可以使用 S3 應用程式在 StorageGRID 中儲存及擷取物件的實體。每個租戶都有自己的使用者、存取金鑰、貯體、物件和一組特定功能。您必須先建立租戶、然後才能建立 S3 應用程式用來儲存物件的貯體。

貯體是用來儲存租戶物件和物件中繼資料的容器。雖然有些租戶可能有許多貯體、但精靈可協助您以最快且最簡單的方式建立租戶和貯體。您可以稍後使用租戶管理器來新增任何您需要的額外貯體。

您可以為此 S3 應用程式建立新的租戶、以便使用。或者、您也可以為新租戶建立貯體。最後、您可以允許精靈為租戶的根使用者建立 S3 存取金鑰。

如需此工作的詳細資訊、請參閱 "建立租戶帳戶" 和 "建立S3儲存區"。

步驟

1. 選取*建立租戶*。
2. 如需輸入詳細資料步驟、請輸入下列資訊。

欄位	說明
名稱	租戶帳戶的名稱。租戶名稱不一定是唯一的。建立租戶帳戶時、會收到唯一的數字帳戶ID。
說明（選用）	協助識別租戶的說明。
用戶端類型	此租戶將使用的用戶端傳輸協定類型。對於 S3 設定精靈、會選取 **S2** 、且欄位會停用。
儲存配額（選用）	如果您想要此租用戶擁有儲存配額、則需要配額和單位的數值。

3. 選擇*繼續*。
4. 或者、選取您想要此租用戶擁有的任何權限。

其中有些權限有額外的需求。如需詳細資料、請選取每個權限的說明圖示。

權限	如果選取 ...
允許平台服務	租戶可以使用 S3 平台服務、例如 CloudMirror 。請參閱 "管理S3租戶帳戶的平台服務"。

權限	如果選取 ...
使用自己的身分識別來源	租戶可以為同盟群組和使用者設定及管理自己的身分識別來源。如果您有、此選項會停用 "已設定 SSO" 適用於您的 StorageGRID 系統。
允許 S3 Select	租戶可以發出 S3 SelectObjectContent API 要求、以篩選及擷取物件資料。請參閱 "管理用戶帳戶的S3 Select"。 • 重要 * ： SelectObjectContent 要求可降低所有 S3 用戶端和所有租戶的負載平衡器效能。只有在必要時才啟用此功能、而且僅適用於信任的租戶。
使用網格同盟連線	租戶可以使用網格同盟連線。 選取此選項： • 使此租用戶和新增至帳戶的所有租戶群組和使用者、從這個網格（ _ 來源網格 _ ）複製到所選連線（ _ 目的地網格 _ ）的其他網格。 • 允許此租戶在每個網格上對應的儲存格之間設定跨網格複寫。 請參閱 "管理 Grid Federation 的允許租戶"。

5. 如果您選取 * 使用網格同盟連線 * 、請選取其中一個可用的網格同盟連線。
6. 根據您的 StorageGRID 系統是否使用、定義租戶帳戶的根存取權 "身分識別聯盟"、 "單一登入（ SSO ）"或兩者。

選項	請這麼做
如果未啟用身分識別聯盟	指定當以本機根使用者身分登入租戶時所使用的密碼。
如果已啟用身分識別聯盟	a. 選取現有的同盟群組以擁有租用戶的根存取權限。 b. 您也可以選擇指定當以本機根使用者身分登入租用戶時要使用的密碼。
如果同時啟用身分識別聯盟和單一登入（ SSO ）	選取現有的同盟群組以擁有租用戶的根存取權限。沒有本機使用者可以登入。

7. 如果您希望精靈為 root 使用者建立存取金鑰 ID 和秘密存取金鑰、請選取 * 自動建立 root 使用者 S3 存取金鑰 * 。

如果租戶的唯一使用者是 root 使用者、請選取此選項。如果其他使用者將使用此租戶、請使用 Tenant Manager 來設定金鑰和權限。

8. 選擇*繼續*。
9. 針對「建立貯體」步驟、您可以選擇性地為租戶物件建立貯體。否則、請選取 * 建立不含貯體的租戶 * 以移至 下載資料步驟。

如果已啟用網格的 S3 物件鎖定功能、則在此步驟建立的儲存格並未啟用 S3 物件鎖定功能。如果您需要為此 S3 應用程式使用 S3 物件鎖定貯體、請選取 * 建立不含 Bucket 的租戶 * 。然後、使用 Tenant Manager "建立貯體" 而是。

a. 輸入 S3 應用程式將使用的儲存區名稱。例如、 `S3-bucket`。

   您無法在建立貯體之後變更貯體名稱。

b. 為此貯體選取 * 區域 * 。

   使用預設區域 (`us-east-1`）除非您預期未來會使用 ILM 來根據貯體的區域篩選物件。

c. 如果您要儲存此貯體中每個物件的每個版本、請選取 * 啟用物件版本管理 * 。

d. 選取 * 建立租戶和貯體 * 、然後前往下載資料步驟。

步驟 **4** 、共 **6** 步：下載資料

在下載資料步驟中、您可以下載一或兩個檔案、以儲存您剛設定的詳細資料。

步驟

1. 如果您選取 * 自動建立 root 使用者 S3 存取金鑰 * 、請執行下列其中一項或兩項操作：
   - 選取 * 下載存取金鑰 * 下載 `.csv` 包含租戶帳戶名稱、存取金鑰 ID 和秘密存取金鑰的檔案。
   - 選取複製圖示（）將存取金鑰 ID 和秘密存取金鑰複製到剪貼簿。
2. 選擇 * 下載組態值 * 下載 `.txt` 包含負載平衡器端點、租戶、貯體和根使用者設定的檔案。
3. 將此資訊儲存至安全的位置。

   在複製兩個存取金鑰之前、請勿關閉此頁面。關閉此頁面後、金鑰將無法使用。請務必將此資訊儲存在安全的位置、因為此資訊可用於從 StorageGRID 系統取得資料。

4. 如果出現提示、請選取核取方塊、確認您已下載或複製金鑰。
5. 選取 * 繼續 * 以移至 ILM 規則和原則步驟。

第 **5** 步、共 **6** 步：審查 **S3** 的 **ILM** 規則和 **ILM** 原則

資訊生命週期管理（ ILM ）規則可控制 StorageGRID 系統中所有物件的放置、持續時間和擷取行為。StorageGRID 隨附的 ILM 原則會為所有物件建立兩個複寫複本。此原則會生效、直到您至少啟動一個新原則為止。

步驟

1. 檢閱頁面上提供的資訊。
2. 如果您要新增屬於新租戶或貯體之物件的特定指示、請建立新規則和新原則。請參閱 "建立ILM規則" 和 "ILM 原則：概觀"。
3. 請選擇 * 我已檢閱這些步驟、並瞭解我需要做什麼 * 。
4. 選取核取方塊、表示您瞭解接下來該怎麼做。

5. 選擇 * 繼續 * 前往 * 摘要 * 。

步驟 **6** 之 **6** ：檢視摘要

步驟

1. 檢閱摘要。
2. 請記下後續步驟中的詳細資料、其中說明在連線到 S3 用戶端之前可能需要的其他組態。例如、選取 * 以 root 身分登入 * 會將您帶到租戶管理員、您可以在其中新增租戶使用者、建立其他貯體、以及更新貯體設定。
3. 選擇*完成*。
4. 使用您從 StorageGRID 下載的檔案或手動取得的值來設定應用程式。

管理 HA 群組

管理高可用度（HA）群組：總覽

您可以將多個管理節點和閘道節點的網路介面分組為高可用度（HA）群組。如果HA群組中的作用中介面故障、備份介面就能管理工作負載。

什麼是HA群組？

您可以使用高可用度（HA）群組、為S3和Swift用戶端提供高可用度的資料連線、或提供高可用度的Grid Manager和Tenant Manager連線。

每個HA群組均可存取所選節點上的共享服務。

- 包含閘道節點、管理節點或兩者的HA群組、可為S3和Swift用戶端提供高可用度的資料連線。
- 僅包含管理節點的HA群組可提供高可用度的網格管理程式和租戶管理程式連線。
- 只包含服務應用裝置和 VMware 型軟體節點的 HA 群組、可為提供高可用度的連線 "使用S3 Select的S3租戶"。 使用S3 Select時建議使用HA群組、但不需要。

如何建立HA群組？

1. 您可以為一個或多個管理節點或閘道節點選取網路介面。您可以使用Grid Network（eth0）介面、用戶端網路（eth2）介面、VLAN介面、或是新增至節點的存取介面。

   如果 HA 群組具有 DHCP 指派的 IP 位址、則無法將介面新增至 HA 群組。

2. 您可以指定一個介面做為主要介面。主介面是作用中介面、除非發生故障。
3. 您可以決定任何備份介面的優先順序。
4. 您可以為群組指派一到10個虛擬IP（VIP）位址。用戶端應用程式可以使用這些VIP位址來連線StorageGRID至

如需相關指示、請參閱 "設定高可用度群組"。

什麼是作用中介面？

正常運作期間、HA群組的所有VIP位址都會新增至主要介面、這是優先順序中的第一個介面。只要主介面仍可用、當用戶端連線至群組的任何VIP位址時、就會使用該介面。也就是說、在正常作業期間、主要介面是群組的「作用中」介面。

同樣地、在正常作業期間、 HA 群組的任何低優先順序介面都會做為「備份」介面。除非主要（目前使用中）介面無法使用、否則不會使用這些備份介面。

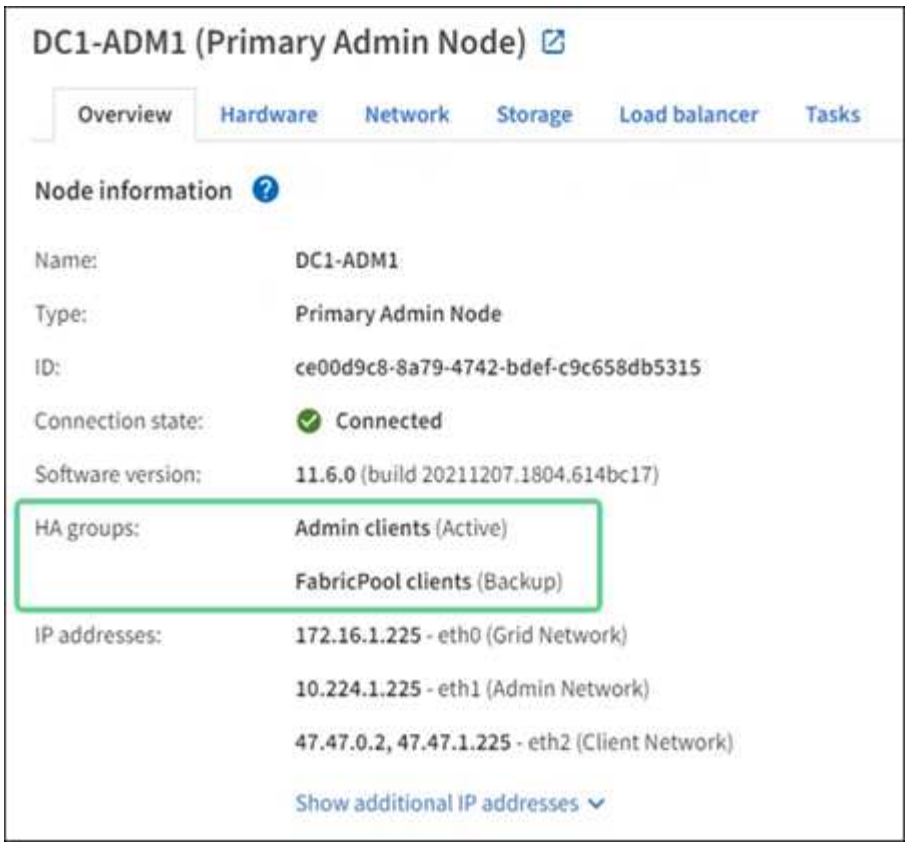
檢視節點的目前**HA**群組狀態

若要查看節點是否指派給HA群組並判斷其目前狀態、請選取* nodes **>***節點_。

如果「總覽」索引標籤包含* HA群組*的項目、則該節點會指派給列出的HA群組。群組名稱後面的值是HA群組中節點的目前狀態：

- * Active*：HA群組目前裝載於此節點上。
- 備份：HA群組目前未使用此節點、這是備份介面。
- * 停止 * ：由於已手動停止高可用度（ keepalive ）服務、因此無法在此節點上裝載 HA 群組。
- * 故障 * ：由於下列一項或多項原因、因此無法在此節點上裝載 HA 群組：
  - 。負載平衡器（Ngine-GW）服務未在節點上執行。
  - 。節點的eth0或VIP介面關閉。
  - 。節點當機。

在此範例中、主要管理節點已新增至兩個HA群組。此節點目前是管理用戶端群組的作用中介面、FabricPool 也是適用於「支援客戶」群組的備份介面。



當作用中介面故障時會發生什麼事？

目前裝載VIP位址的介面是作用中介面。如果HA群組包含多個介面、且作用中介面故障、VIP位址會依照優先順序移至第一個可用的備份介面。如果該介面故障、VIP位址會移至下一個可用的備份介面、依此類推。

容錯移轉可因下列任一原因觸發：

- 介面設定所在的節點會停機。
- 介面設定所在的節點至少失去與所有其他節點的連線2分鐘。
- 作用中介面關閉。
- 負載平衡器服務會停止。
- 高可用度服務停止。

主控作用中介面的節點外部網路故障可能不會觸發容錯移轉。同樣地、 Grid Manager 或 Tenant Manager 的服務也不會觸發容錯移轉。

容錯移轉程序通常只需幾秒鐘、而且速度足夠快、用戶端應用程式只會遇到些微影響、而且可以仰賴正常的重試行為來繼續作業。

當故障得以解決且優先順序較高的介面再次可用時、VIP位址會自動移至可用的最高優先順序介面。

如何使用**HA**群組？

您可以使用高可用度（HA）群組、為StorageGRID 物件資料和管理用途提供高可用度的連接至物件資料。

- HA群組可提供高可用度的管理連線至Grid Manager或Tenant Manager。
- HA群組可為S3和Swift用戶端提供高可用度的資料連線。
- 僅包含一個介面的HA群組可讓您提供多個VIP位址、並明確設定IPv6位址。

只有當群組中包含的所有節點都提供相同的服務時、HA群組才能提供高可用度。建立HA群組時、請從提供所需服務的節點類型新增介面。

- 管理節點：包括負載平衡器服務、並可存取Grid Manager或租戶管理程式。
- * 閘道節點 * ：包括負載平衡器服務。

HA群組的用途	將此類型的節點新增至**HA**群組
存取Grid Manager	• 主管理節點（主） • 非主要管理節點 *附註：*主要管理節點必須是主要介面。部分維護程序只能從主要管理節點執行。
僅限租戶管理程式存取	• 主要或非主要管理節點
S3或Swift用戶端存取-負載平衡器服務	• 管理節點 • 閘道節點
的S3用戶端存取 "S3 Select"	• 服務應用裝置 • VMware軟體節點 附註：使用S3 Select時建議使用HA群組、但不需要。

搭配**Grid Manager**或**Tenant Manager**使用**HA**群組的限制

如果Grid Manager或Tenant Manager服務失敗、HA群組容錯移轉就不會觸發。

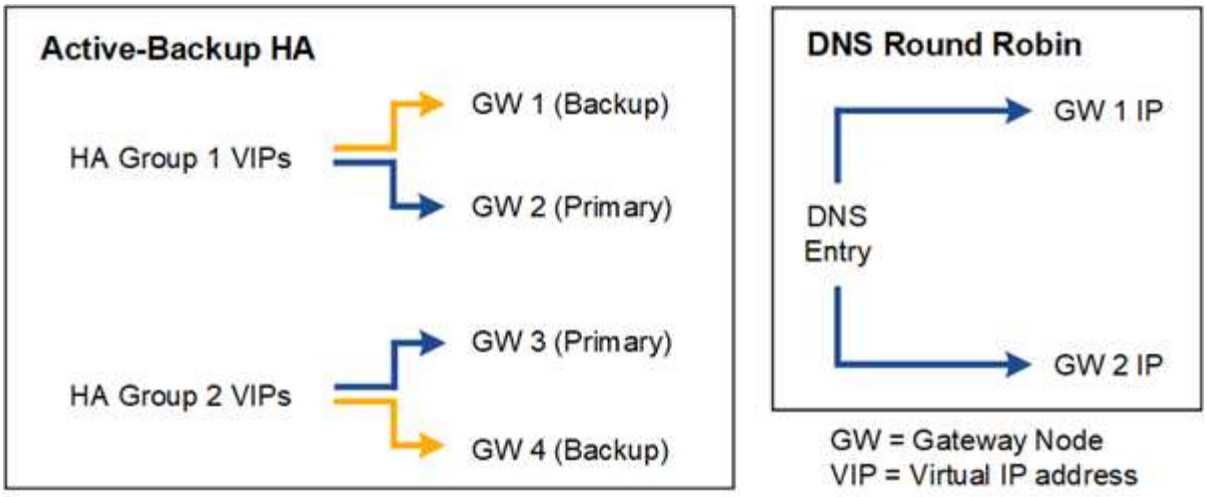
如果您在容錯移轉發生時登入Grid Manager或租戶管理程式、系統將會登出、您必須再次登入才能繼續執行工作。

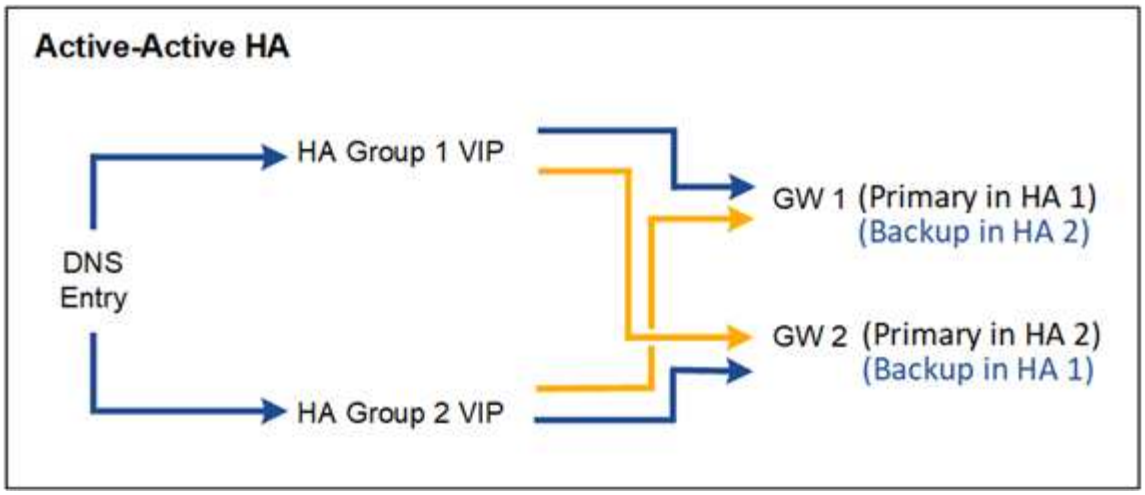
當主要管理節點無法使用時、無法執行某些維護程序。容錯移轉期間、您可以使用Grid Manager監控StorageGRID 您的作業系統。

HA群組的組態選項

下圖提供不同的HA群組設定方式範例。每個選項都有優點和缺點。

在圖中、藍色表示HA群組中的主要介面、黃色表示HA群組中的備份介面。





下表摘要說明各HA組態的優點、如圖所示。

組態	優勢	缺點
主動備份HA	• 由不需依賴外部資源的不受依賴的功能執行管理StorageGRID 。 • 快速容錯移轉：	• HA群組中只有一個節點處於作用中狀態。每個HA群組至少有一個節點處於閒置狀態。
DNS循環配置資源	• 增加Aggregate處理量。 • 無閒置主機。	• 慢速容錯移轉、可能取決於用戶端行為。 • 需要在StorageGRID 不屬於此功能的情況下組態硬體。 • 需要客戶實作的健全狀況檢查。
主動式HA	• 流量分散於多個HA群組。 • 高Aggregate處理量、可隨HA群組數量而擴充。 • 快速容錯移轉：	• 更複雜的設定。 • 需要在StorageGRID 不屬於此功能的情況下組態硬體。 • 需要客戶實作的健全狀況檢查。

設定高可用度群組

您可以設定高可用度（HA）群組、以提供對管理節點或閘道節點上服務的高可用度存取。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限"。
- 如果您打算在HA群組中使用VLAN介面、則表示您已建立VLAN介面。請參閱 "設定VLAN介面"。
- 如果您打算針對HA群組中的節點使用存取介面、則已建立介面：
  - * Red Hat Enterprise Linux （安裝節點之前） * ： "建立節點組態檔"
  - * Ubuntu或DEBIAN*（安裝節點之前）*： "建立節點組態檔"
  - * Linux（安裝節點之後）*： "Linux：新增主幹或存取介面至節點"
  - * VMware（安裝節點之後）*： "VMware：新增主幹或存取介面至節點"

建立高可用度群組

當您建立高可用度群組時、請選取一或多個介面、然後依優先順序加以組織。然後、您將一個或多個VIP位址指派給群組。

介面必須是要納入HA群組的閘道節點或管理節點。HA群組只能將一個介面用於任何指定節點、但同一個節點的其他介面可用於其他HA群組。

存取精靈

步驟

1. 選擇*組態*>*網路*>*高可用度群組*。
2. 選擇* Create （建立）。

輸入**HA**群組的詳細資料

步驟

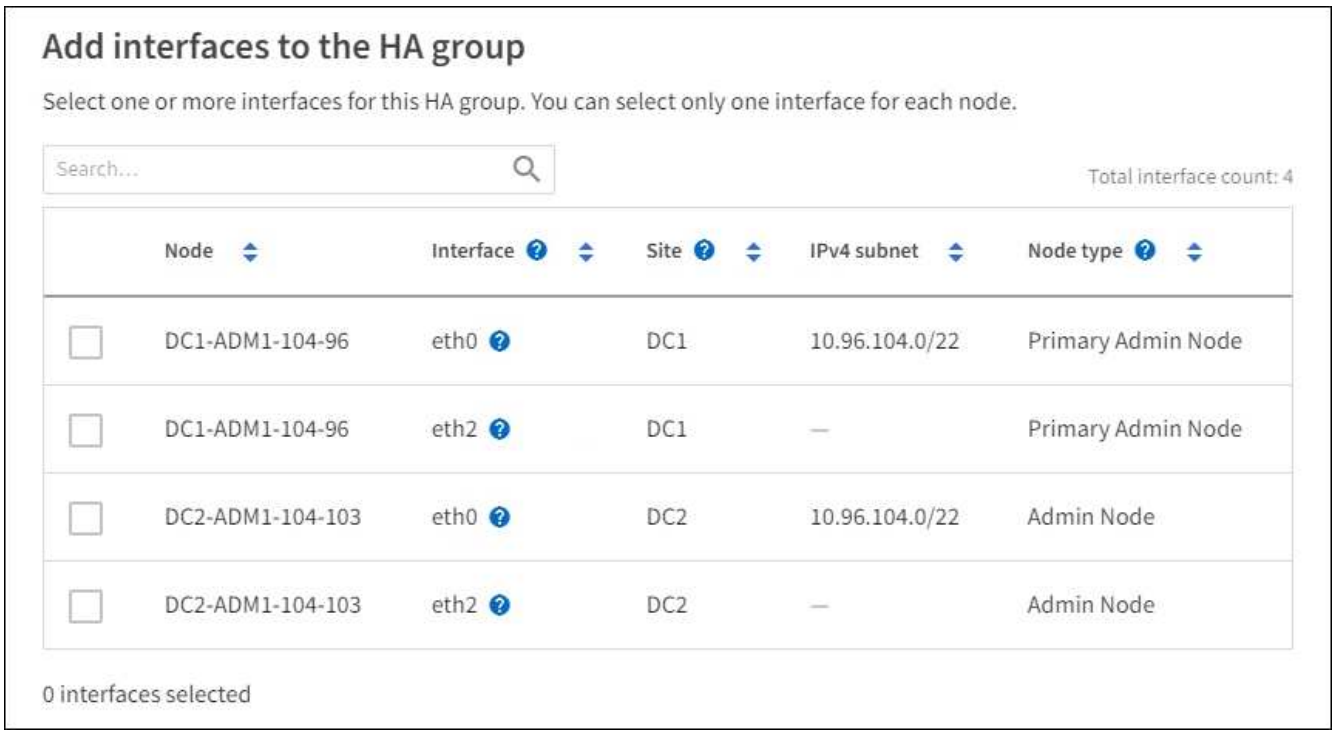
1. 為HA群組提供唯一名稱。
2. （可選）輸入HA群組的說明。
3. 選擇*繼續*。

新增介面至**HA**群組

步驟

1. 選取一或多個介面以新增至此HA群組。

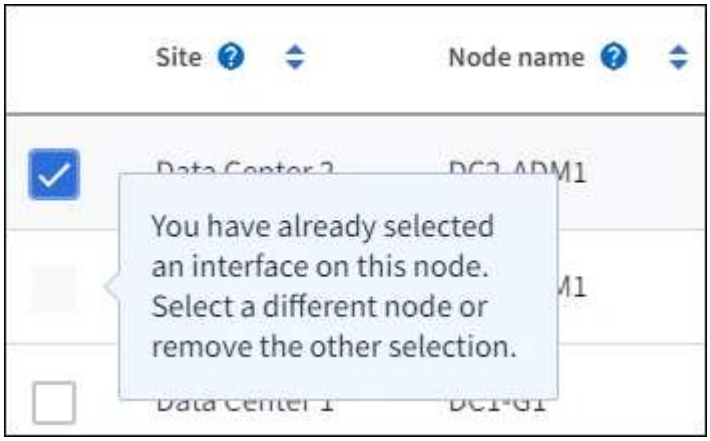
   使用欄標題來排序列、或輸入搜尋詞彙以更快找到介面。



建立VLAN介面之後、請等待5分鐘、讓新介面出現在表格中。

選擇介面的準則

- 您必須選取至少一個介面。
- 您只能為節點選取一個介面。
- 如果HA群組用於管理節點服務的HA保護（包括Grid Manager和Tenant Manager）、請選取「僅管理節點上的介面」。
- 如果HA群組用於HA保護S3或Swift用戶端流量、請選取管理節點、閘道節點或兩者上的介面。
- 如果您在不同類型的節點上選取介面、則會顯示資訊注意事項。系統會提醒您、如果發生容錯移轉、先前作用中節點所提供的服務可能無法在新作用中節點上使用。例如、備份閘道節點無法提供管理節點服務的 HA 保護。同樣地、備份管理節點也無法執行主要管理節點所能提供的所有維護程序。
- 如果您無法選取介面、則其核取方塊會停用。工具提示提供更多資訊。



- 如果介面的子網路值或閘道與其他選取的介面衝突、則無法選取介面。

。如果設定的介面沒有靜態 IP 位址、則無法選取該介面。

2. 選擇*繼續*。

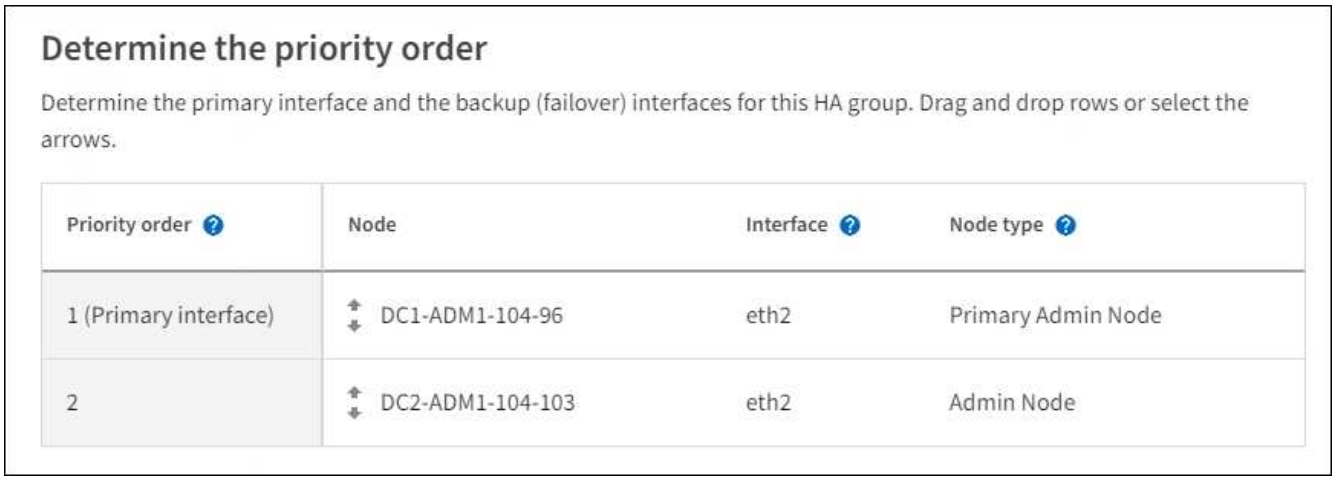
決定優先順序

如果 HA 群組包含多個介面、您可以判斷哪個是主要介面、哪些是備份（容錯移轉）介面。 如果主要介面故障、 VIP 位址會移至可用的最高優先順序介面。如果該介面故障、VIP位址會移至下一個可用的最高優先順序介面、依此類推。

步驟

1. 在 * 優先順序 * 欄中拖曳列、以決定主要介面和任何備份介面。

   清單中的第一個介面是主要介面。主介面是作用中介面、除非發生故障。



   如果HA群組可存取Grid Manager、則您必須在主要管理節點上選取介面作為主要介面。部分維護程序只能從主要管理節點執行。

2. 選擇*繼續*。

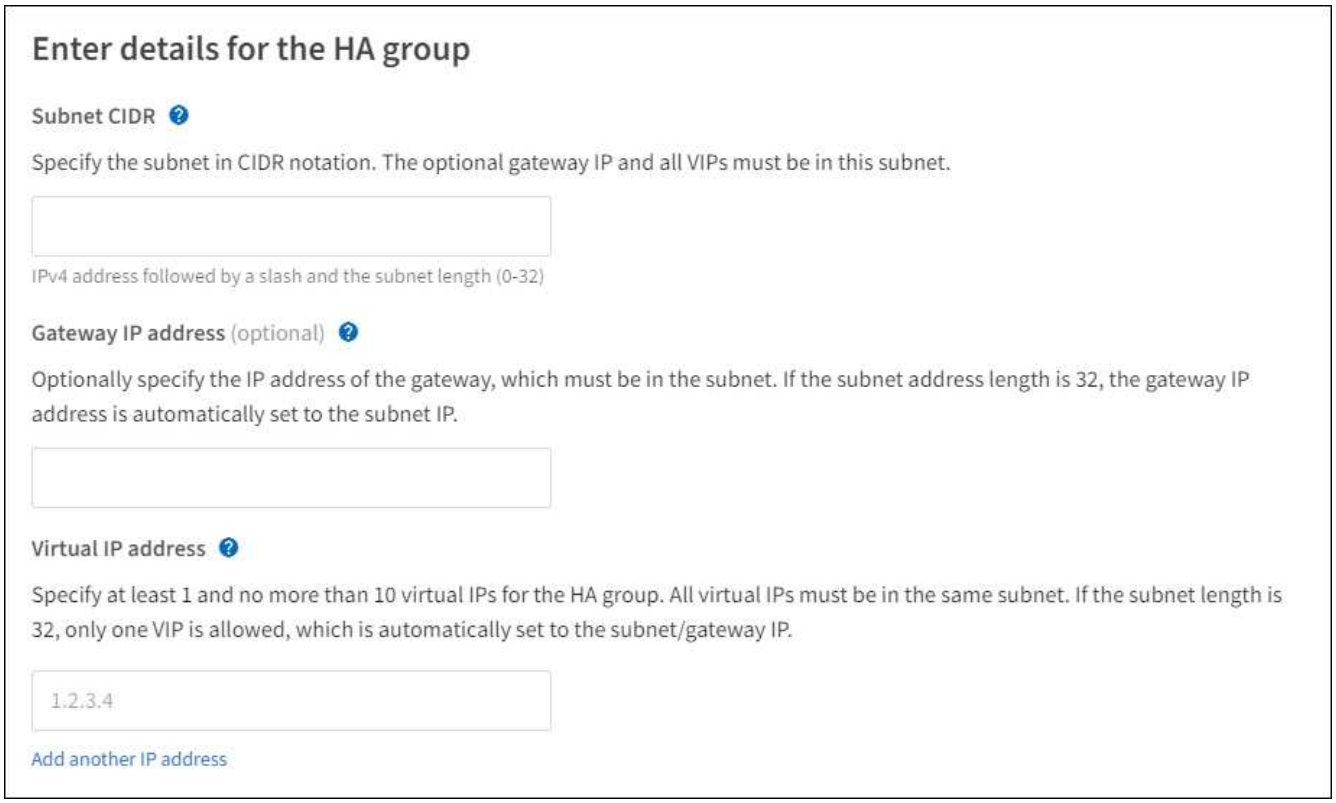
輸入**IP**位址

步驟

1. 在*子網路CID*欄位中、以CIDR表示法指定VIP子網路、即一種IPV4位址、後面接著一條斜槓和子網路長度（0-32）。

   網路位址不得設定任何主機位元。例如、 `192.16.0.0/22`。

   如果您使用32位元前置碼、VIP網路位址也會做為閘道位址和VIP位址。



2. 或者、如果任何S3、Swift、管理用戶端或租戶用戶端將從不同的子網路存取這些VIP位址、請輸入*閘道IP位址*。閘道位址必須位於VIP子網路內。

   用戶端和管理使用者將使用此閘道來存取虛擬IP位址。

3. 為 HA 群組中的作用中介面輸入至少一個且不超過十個 VIP 位址。所有 VIP 位址都必須位於 VIP 子網路內、而且所有位址都會同時在作用中介面上作用。

   您必須至少提供一個IPV4位址。您也可以指定其他的IPv6位址。

4. 選擇* Create HA group（建立HA群組）、然後選取 Finish（完成）*。

   HA群組隨即建立、您現在可以使用已設定的虛擬IP位址。

後續步驟

如果您要使用此HA群組進行負載平衡、請建立負載平衡器端點、以判斷連接埠和網路傳輸協定、並附加任何必要的憑證。請參閱 "設定負載平衡器端點"。

編輯高可用度群組

您可以編輯高可用度（HA）群組、以變更其名稱和說明、新增或移除介面、變更優先順序、或新增或更新虛擬IP位址。

例如、如果您想要在站台或節點取消委任程序中移除與所選介面相關聯的節點、則可能需要編輯HA群組。

步驟

1. 選擇*組態*>*網路*>*高可用度群組*。

「高可用度群組」頁面會顯示所有現有的HA群組。

2. 選取您要編輯之 HA 群組的核取方塊。
3. 根據您要更新的內容、執行下列其中一項：
   - 選取*「動作*」>*「編輯虛擬IP位址*」以新增或移除VIP位址。
   - 選取*「動作*」>*「編輯HA群組*」以更新群組的名稱或說明、新增或移除介面、變更優先順序、或新增或移除VIP位址。
4. 如果您選取*編輯虛擬IP位址*：
   a. 更新HA群組的虛擬IP位址。
   b. 選擇*保存*。
   c. 選擇*完成*。
5. 如果您選取*編輯HA群組*：
   a. 或者、請更新群組的名稱或說明。
   b. 或者、選取或清除核取方塊以新增或移除介面。

      如果HA群組可存取Grid Manager、則您必須在主要管理節點上選取介面作為主要介面。部分維護程序只能從主要管理節點執行

   c. 您也可以拖曳資料列來變更此 HA 群組的主要介面和任何備份介面的優先順序。
   d. 或者、更新虛擬IP位址。
   e. 選取*「Save（儲存）」、然後選取「Finish（完成）」*。

移除高可用度群組

您可以一次移除一或多個高可用度（HA）群組。

如果 HA 群組繫結至負載平衡器端點、則無法移除該群組。若要刪除 HA 群組、您必須將其從任何使用它的負載平衡器端點中移除。

若要避免用戶端中斷、請先更新任何受影響的S3或Swift用戶端應用程式、再移除HA群組。更新每個用戶端以使用其他IP位址進行連線、例如、不同HA群組的虛擬IP位址、或是安裝期間為介面設定的IP位址。

步驟

1. 選擇*組態*>*網路*>*高可用度群組*。
2. 檢閱您要移除之每個 HA 群組的 * 負載平衡器端點 * 欄。如果列出任何負載平衡器端點：
   a. 移至 * 組態 * > * 網路 * > * 負載平衡器端點 * 。
   b. 選取端點的核取方塊。
   c. 選取*「動作*」>*「編輯端點繫結模式*」。
   d. 更新繫結模式以移除 HA 群組。
   e. 選取*儲存變更*。
3. 如果未列出負載平衡器端點、請選取您要移除的每個 HA 群組的核取方塊。

4. 選取 * 動作 * > * 移除 HA 群組 * 。
5. 檢閱訊息並選擇*刪除HA群組*以確認您的選擇。

   您選取的所有HA群組都會移除。「高可用度群組」頁面上會出現綠色的成功橫幅。

管理負載平衡

負載平衡考量

您可以使用負載平衡來處理來自 S3 和 Swift 用戶端的擷取和擷取工作負載。

什麼是負載平衡？

當用戶端應用程式從 StorageGRID 系統儲存或擷取資料時、 StorageGRID 會使用負載平衡器來管理擷取和擷取工作負載。負載平衡可在多個儲存節點之間分配工作負載、以最大化速度和連線容量。

此功能可在所有管理節點和所有閘道節點上安裝支援程式、並提供第7層負載平衡功能。StorageGRID它會對用戶端要求執行傳輸層安全性（TLS）終止、檢查要求、並建立新的安全連線至儲存節點。

將用戶端流量轉送至儲存節點時、每個節點上的負載平衡器服務都會獨立運作。透過加權程序、負載平衡器服務會將更多要求路由傳送至CPU可用度較高的儲存節點。

> 雖然推薦使用「VMware負載平衡器」服務、但StorageGRID 您可能想要改為整合協力廠商負載平衡器。如需相關資訊、請聯絡您的NetApp客戶代表或參閱 "TR-4626：StorageGRID 不包括第三方和全域負載平衡器"。

我需要多少個負載平衡節點？

一般最佳實務做法StorageGRID 是、您的一套系統應該在負載平衡器服務中包含兩個或多個節點。例如、站台可能包含兩個閘道節點、或同時包含一個管理節點和一個閘道節點。無論您使用的是服務應用裝置、裸機節點或虛擬機器（ VM ）型節點、請確定每個負載平衡節點都有足夠的網路、硬體或虛擬化基礎架構。

什麼是負載平衡器端點？

負載平衡器端點會定義傳入和傳出用戶端應用程式要求用來存取包含負載平衡器服務之節點的連接埠和網路傳輸協定（ HTTPS 或 HTTP ）。端點也會定義用戶端類型（ S3 或 Swift ）、繫結模式、以及選擇性的允許或封鎖租戶清單。

若要建立負載平衡器端點、請選取 * 組態 * > * 網路 * > * 負載平衡器端點 * 、或完成 FabricPool 和 S3 設定精靈。如需相關指示：

- "設定負載平衡器端點"
- "使用 S3 設定精靈"
- "使用 FabricPool 設定精靈"

連接埠的考量事項

對於您建立的第一個端點、負載平衡器端點的連接埠預設為 10433 、但您可以指定介於 1 到 65535 之間的任何

未使用的外部連接埠。如果您使用連接埠 80 或 443 、端點將僅使用 Gateway 節點上的負載平衡器服務。這些連接埠保留在管理節點上。如果您對多個端點使用相同的連接埠、則必須為每個端點指定不同的繫結模式。

不允許其他網格服務使用的連接埠。請參閱 "網路連接埠參考"。

網路傳輸協定的考量事項

在大多數情況下、用戶端應用程式與 StorageGRID 之間的連線應該使用傳輸層安全性（ TLS ）加密。支援但不建議連線至無 TLS 加密的 StorageGRID 、尤其是在正式作業環境中。當您選取 StorageGRID 負載平衡器端點的網路傳輸協定時、應該選取 **HTTPS** 。

負載平衡器端點憑證的考量事項

如果選擇 **HTTPS** 作爲負載平衡器端點的網絡協議，則必須提供安全證書。建立負載平衡器端點時、您可以使用以下三個選項中的任何一個：

- * 上傳簽署的憑證（建議） * 。此憑證可由公開信任或私有憑證授權單位（ CA ）簽署。最佳做法是使用公開信任的 CA 伺服器憑證來保護連線安全。與產生的憑證不同、 CA 簽署的憑證可以不中斷地旋轉、有助於避免過期問題。

  您必須先取得下列檔案、才能建立負載平衡器端點：

  - 自訂伺服器憑證檔案。
  - 自訂伺服器憑證私密金鑰檔案。
  - 或者、每個中繼發行憑證授權單位的憑證 CA 套裝組合。
- * 產生自我簽署的憑證 * 。
- * 使用全球 StorageGRID S3 和 Swift 認證 * 。您必須上傳或產生此憑證的自訂版本、才能為負載平衡器端點選取該憑證。請參閱 "設定S3和Swift API憑證"。

我需要什麼價值？

若要建立憑證、您必須知道 S3 或 Swift 用戶端應用程式用來存取端點的所有網域名稱和 IP 位址。

憑證的 * 主體 DN* （辨別名稱）項目必須包含用戶端應用程式將用於 StorageGRID 的完整網域名稱。例如：

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

必要時、憑證可以使用萬用字元來代表執行負載平衡器服務的所有管理節點和閘道節點的完整網域名稱。例如、 `*.storagegrid.example.com` 使用*萬用字元表示 `adm1.storagegrid.example.com` 和 `gn1.storagegrid.example.com`。

如果您打算使用 S3 虛擬託管式要求、則該憑證也必須為每個要求提供 * 替代名稱 * 項目 "S3 端點網域名稱" 您已設定、包括任何萬用字元名稱。例如：

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

如果您在網域名稱中使用萬用字元、請參閱 "伺服器憑證的強化準則"。

您也必須為安全性憑證中的每個名稱定義 DNS 項目。

如何管理過期的憑證？

如果用於保護 S3 應用程式與 StorageGRID 之間連線的憑證過期、應用程式可能會暫時失去對 StorageGRID 的存取權。

若要避免憑證過期問題、請遵循下列最佳實務做法：

- 請仔細監控任何警告即將到期的憑證、例如 * 負載平衡器端點憑證到期 * 、以及 * S3 和 Swift API* 警示的通用伺服器憑證到期日。
- 請務必讓 StorageGRID 和 S3 應用程式的憑證版本保持同步。如果您更換或更新用於負載平衡器端點的憑證、則必須更換或更新 S3 應用程式所使用的同等憑證。
- 使用公開簽署的 CA 憑證。如果您使用由 CA 簽署的憑證、您可以不中斷地更換即將過期的憑證。
- 如果您已產生自我簽署的 StorageGRID 憑證、且該憑證即將過期、則必須在現有憑證過期之前、手動在 StorageGRID 和 S3 應用程式中置換憑證。

綁定模式的注意事項

繫結模式可讓您控制哪些 IP 位址可用於存取負載平衡器端點。如果端點使用繫結模式、則用戶端應用程式只有在使用允許的 IP 位址或其對應的完整網域名稱（ FQDN ）時、才能存取端點。使用任何其他 IP 位址或 FQDN 的用戶端應用程式無法存取端點。

您可以指定下列任何一種繫結模式：

- * 通用 * （預設）：用戶端應用程式可以使用任何閘道節點或管理節點的 IP 位址、任何網路上任何 HA 群組的虛擬 IP （ VIP ）位址、或對應的 FQDN 來存取端點。除非您需要限制端點的存取、否則請使用此設定。
- * HA 群組的虛擬 IP * 。用戶端應用程式必須使用 HA 群組的虛擬 IP 位址（或對應的 FQDN ）。
- * 節點介面 * 。用戶端必須使用所選節點介面的 IP 位址（或對應的 FQDN ）。
- * 節點類型 * 。根據您選取的節點類型、用戶端必須使用任何管理節點的 IP 位址（或對應的 FQDN ）、或任何閘道節點的 IP 位址（或對應的 FQDN ）。

租戶存取的考量事項

租戶存取是一項選擇性的安全功能、可讓您控制哪些 StorageGRID 租戶帳戶可以使用負載平衡器端點來存取他們的貯體。您可以允許所有租戶存取端點（預設）、也可以指定每個端點的允許或封鎖租戶清單。

您可以使用此功能、在租戶與其端點之間提供更好的安全隔離。例如、您可以使用此功能來確保某個租戶擁有的最高機密或高度機密資料、不會被其他租戶完全存取。

為了進行存取控制、如果在要求中未提供存取金鑰（例如匿名存取）、則租戶會根據用戶端要求中使用的存取金鑰來決定租戶。

租戶存取範例

若要瞭解此安全功能的運作方式、請考慮下列範例：

1. 您已建立兩個負載平衡器端點、如下所示：
   - * 公有 * 端點：使用連接埠 10443 並允許存取所有租戶。
   - *Top secret * 端點：使用連接埠 10444 、僅允許存取 *Top secret * 租戶。所有其他租戶都會被封鎖、無法存取此端點。
2. 。 `top-secret.pdf` 位於 *Top Secret * 租戶擁有的貯體內。

存取 `top-secret.pdf`、 * 上秘密 * 租戶中的使用者可以向發出 GET 要求 `https://w.x.y.z:10444/top-secret.pdf`。由於此租戶可以使用 10444 端點、因此使用者可以存取物件。不過、如果屬於任何其他租戶的使用者向相同的 URL 發出相同的要求、他們就會收到立即存取遭拒訊息。即使認證和簽章有效、存取仍會遭到拒絕。

CPU可用度

將S3或Swift流量轉送至儲存節點時、每個管理節點和閘道節點上的負載平衡器服務都會獨立運作。透過加權程序、負載平衡器服務會將更多要求路由傳送至CPU可用度較高的儲存節點。節點CPU負載資訊會每隔幾分鐘更新一次、但加權可能會更頻繁地更新。所有儲存節點都會被指派最低的基本權重值、即使節點回報100%使用率或無法報告使用率亦然。

在某些情況下、CPU可用度的相關資訊僅限於負載平衡器服務所在的站台。

設定負載平衡器端點

負載平衡器端點決定連接StorageGRID 至閘道和管理節點上的S3和Swift用戶端可使用的連接埠和網路傳輸協定。您也可以使用端點來存取 Grid Manager 、 Tenant Manager 或兩者。

Swift 用戶端應用程式的支援已過時、未來版本將會移除。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您擁有 "root 存取權限"。
- 您已檢閱 "負載平衡考量"。
- 如果您先前已重新對應要用於負載平衡器端點的連接埠、您就擁有了 "已移除連接埠重新對應"。
- 您已建立任何打算使用的高可用度（HA）群組。建議使用HA群組、但不需要。請參閱 "管理高可用度群組"。
- 如果將使用負載平衡器端點 "S3租戶選擇"、不得使用任何裸機節點的IP位址或FQDN。S3 Select 所使用的負載平衡器端點僅允許使用服務應用裝置和 VMware 型軟體節點。
- 您已設定任何打算使用的VLAN介面。請參閱 "設定VLAN介面"。
- 如果您要建立HTTPS端點（建議）、您就有伺服器憑證的資訊。

對端點憑證所做的變更、可能需要15分鐘才能套用至所有節點。

- 若要上傳憑證、您需要伺服器憑證、憑證私密金鑰、以及選擇性的CA套裝組合。
- 若要產生憑證、您需要S3或Swift用戶端用來存取端點的所有網域名稱和IP位址。您也必須知道主旨（辨別名稱）。
- 如果您想要使用StorageGRID Sfor S3和Swift API認證（也可用於直接連線至儲存節點）、則您已使用由外部憑證授權單位簽署的自訂認證來取代預設認證。請參閱 "設定S3和Swift API憑證"。

建立負載平衡器端點

每個 S3 或 Swift 用戶端負載平衡器端點都會指定連接埠、用戶端類型（ S3 或 Swift ）、以及網路傳輸協定（ HTTP 或 HTTPS ）。管理介面負載平衡器端點會指定連接埠、介面類型和不受信任的用戶端網路。

存取精靈

步驟

1. 選擇*組態*>*網路*>*負載平衡器端點*。
2. 若要為 S3 或 Swift 用戶端建立端點、請選取 *S3 或 Swift 用戶端 * 標籤。
3. 若要建立端點以存取 Grid Manager 、 Tenant Manager 或兩者、請選取 * 管理介面 * 索引標籤。
4. 選擇* Create （建立）。

輸入端點詳細資料

步驟

1. 選取適當的指示、以輸入您要建立的端點類型的詳細資料。

S3 或 **Swift** 用戶端

欄位	說明
名稱	端點的描述性名稱、會出現在「負載平衡器端點」頁面的表格中。
連接埠	您要用於負載平衡的選用功能。StorageGRID此欄位預設為 10433 、表示您建立的第一個端點、但您可以輸入 1 到 65535 之間的任何未使用的外部連接埠。 如果您輸入 **80** 或 **8443** ，則端點僅在網關節點上配置，除非您已釋放端口 8443 。然後、您可以使用連接埠 8443 做為 S3 端點、而且連接埠將同時在 Gateway 和 Admin Node 上設定。
用戶端類型	將使用此端點的用戶端應用程式類型：* S3 或 Swift *。
網路傳輸協定	用戶端連線至此端點時所使用的網路傳輸協定。 • 選擇* HTTPS *進行安全的TLS加密通訊（建議）。您必須先附加安全性憑證、才能儲存端點。 • 選擇「* HTTP *」以獲得較不安全且未加密的通訊。僅將HTTP用於非正式作業網格。

管理介面

欄位	說明
名稱	端點的描述性名稱、會出現在「負載平衡器端點」頁面的表格中。
連接埠	您要用來存取 Grid Manager 、 Tenant Manager 或兩者的 StorageGRID 連接埠。 • 網格管理器： **8443** • 租戶經理： **9443** • Grid Manager 和 Tenant Manager ： **443** • 注意 * ：您可以使用這些預設連接埠或其他可用的連接埠。
介面類型	選取您要使用此端點存取的 StorageGRID 介面選項按鈕。
不受信任的用戶端網路	如果不受信任的用戶端網路應該可以存取此端點、請選取 * 是 * 。否則、請選取 * 否 * 。 當您選取 * 是 * 時、連接埠會在所有不受信任的用戶端網路上開啟。 • 注意 * ：當您建立負載平衡器端點時、您只能將連接埠設定為開放或關閉給不受信任的用戶端網路。

1. 選擇*繼續*。

選取繫結模式

步驟

1. 選取端點的繫結模式、以控制使用任何 IP 位址或使用特定 IP 位址和網路介面存取端點的方式。

   有些繫結模式適用於用戶端端端點或管理介面端點。此處列出兩種端點類型的所有模式。

模式	說明
全域（用戶端端端點的預設值）	用戶端可以使用任何閘道節點或管理節點的 IP 位址、任何網路上任何 HA 群組的虛擬 IP （ VIP ）位址、或對應的 FQDN 來存取端點。 除非您需要限制此端點的存取、否則請使用 * 全域 * 設定。
HA群組的虛擬IP	用戶端必須使用 HA 群組的虛擬 IP 位址（或對應的 FQDN ）才能存取此端點。 具有此繫結模式的端點都可以使用相同的連接埠編號、只要您為端點選取的 HA 群組不會重疊。
節點介面	用戶端必須使用所選節點介面的 IP 位址（或對應的 FQDN ）來存取此端點。
節點類型（僅限用戶端端端點）	根據您選取的節點類型、用戶端必須使用任何管理節點的 IP 位址（或對應的 FQDN ）或任何閘道節點的 IP 位址（或對應的 FQDN ）來存取此端點。
所有管理節點（管理介面端點的預設值）	用戶端必須使用任何管理節點的 IP 位址（或對應的 FQDN ）來存取此端點。

   如果多個端點使用相同的連接埠、 StorageGRID 會使用此優先順序來決定要使用的端點： * HA 群組的虛擬 IP * > * 節點介面 * > * 節點類型 * > * 全域 * 。

   如果您要建立管理介面端點、則只允許使用管理節點。

2. 如果您選取* HA群組的虛擬IP *、請選取一或多個HA群組。

   如果您要建立管理介面端點、請選取僅與管理節點相關聯的 VIP 。

3. 如果您選取*節點介面*、請針對您要與此端點建立關聯的每個管理節點或閘道節點、選取一或多個節點介面。
4. 如果您選取 * 節點類型 * 、請選取管理節點（包括主要管理節點和任何非主要管理節點）或閘道節點。

控制租戶存取

> 管理介面端點只有在端點具有時、才能控制租戶存取 租戶管理器的介面類型。

步驟

1. 對於 * 租戶存取 * 步驟、請選取下列其中一項：

欄位	說明
允許所有租戶（預設）	所有租戶帳戶都可以使用此端點來存取他們的貯體。 如果您尚未建立任何租戶帳戶、則必須選取此選項。新增租戶帳戶之後、您可以編輯負載平衡器端點、以允許或封鎖特定帳戶。
允許選取的租戶	只有選取的租戶帳戶才能使用此端點存取其貯體。
封鎖選取的租戶	選取的租戶帳戶無法使用此端點存取其儲存區。所有其他租戶都可以使用此端點。

2. 如果您要建立 **HTTP** 端點、則不需要附加憑證。選取*「Create」（建立）*以新增負載平衡器端點。然後前往 完成後。否則、請選取*繼續*以附加憑證。

附加憑證

步驟

1. 如果您要建立* HTTPS *端點、請選取要附加到端點的安全性憑證類型。

   憑證可保護S3和Swift用戶端與管理節點或閘道節點上的負載平衡器服務之間的連線。

   - 上傳認證。如果您有要上傳的自訂憑證、請選取此選項。
   - 產生憑證。如果您有產生自訂憑證所需的值、請選取此選項。
   - 使用**StorageGRID SS3**和**Swift**認證。如果您想要使用全域S3和Swift API憑證、也可以直接用於儲存節點的連線、請選取此選項。

     除非您已使用外部憑證授權單位簽署的自訂憑證取代由網格 CA 簽署的預設 S3 和 Swift API 憑證、否則無法選取此選項。請參閱 "設定S3和Swift API憑證"。

   - * 使用管理介面憑證 * 。如果您想要使用通用管理介面憑證、也可用於直接連線至管理節點、請選取此選項。

2. 如果您沒有使用 StorageGRID S3 和 Swift 憑證、請上傳或產生憑證。

上傳憑證

a. 選擇*上傳憑證*。

b. 上傳所需的伺服器憑證檔案：

   - 伺服器憑證：自訂伺服器憑證檔案（以PEM編碼）。
   - * 憑證私密金鑰 * ：自訂伺服器憑證私密金鑰檔案 (`.key`）。

     EC 私密金鑰必須大於 224 位元。RSA私密金鑰必須大於或等於2048位元。

   - * CA套裝組合*：單一選用檔案、內含來自每個中繼發行憑證授權單位（CA）的憑證。檔案應包含以憑證鏈順序串聯的每個由PEE編碼的CA憑證檔案。

c. 展開*憑證詳細資料*、即可查看您上傳之每個憑證的中繼資料。如果您上傳了選用的CA套件、每個憑證都會顯示在其各自的索引標籤上。

   - 選取*下載憑證*以儲存憑證檔案、或選取*下載CA套件*以儲存憑證套件組合。

     指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 選擇*複製憑證PEP*或*複製CA套裝組合PEP*、即可複製憑證內容以貼到其他位置。

d. 選擇* Create （建立）。+ 隨即建立負載平衡器端點。自訂憑證用於 S3 和 Swift 用戶端之間的所有後續新連線、或是管理介面和端點之間的所有新連線。

產生憑證

a. 選擇*產生憑證*。

b. 指定憑證資訊：

欄位	說明
網域名稱	要包含在憑證中的一或多個完整網域名稱。使用*作為萬用字元來代表多個網域名稱。
IP	要包含在憑證中的一或多個 IP 位址。
主旨（選用）	憑證擁有者的 X.509 主體或辨別名稱（ DN ）。 如果在此欄位中未輸入任何值、則產生的憑證會使用第一個網域名稱或 IP 位址做為主體一般名稱（ CN ）。
有效天數	憑證建立後過期的天數。

欄位	說明
新增金鑰使用方式擴充功能	如果選取（預設和建議）、金鑰使用方式和延伸金鑰使用方式延伸會新增至產生的憑證。 這些延伸定義了憑證中所含金鑰的用途。 • 附註 * ：除非您在憑證包含這些副檔名時遇到舊版用戶端的連線問題、否則請保留此核取方塊。

c. 選取*產生*。

d. 選取 * 憑證詳細資料 * 以查看所產生憑證的中繼資料。

   ▪ 選取*下載憑證*以儲存憑證檔案。

   指定憑證檔案名稱和下載位置。以副檔名儲存檔案 `.pem`。

   例如： `storagegrid_certificate.pem`

   ▪ 選取*複製憑證PEP*以複製憑證內容以貼到其他位置。

e. 選擇* Create （建立）。

   隨即建立負載平衡器端點。自訂憑證用於 S3 與 Swift 用戶端之間的所有後續新連線、或是管理介面與此端點之間的所有新連線。

完成後

步驟

1. 如果您使用 DNS 、請確定 DNS 包含一筆記錄、將 StorageGRID 完整網域名稱（ FQDN ）與用戶端用來建立連線的每個 IP 位址建立關聯。

   您在DNS記錄中輸入的IP位址取決於您是否使用HA負載平衡節點群組：

   ◦ 如果您已設定 HA 群組、用戶端將會連線至該 HA 群組的虛擬 IP 位址。

   ◦ 如果您不使用 HA 群組、用戶端將使用閘道節點或管理節點的 IP 位址連線至 StorageGRID 負載平衡器服務。

   您也必須確保DNS記錄會參考所有必要的端點網域名稱、包括任何萬用字元名稱。

2. 提供S3和Swift用戶端連線至端點所需的資訊：

   ◦ 連接埠號碼

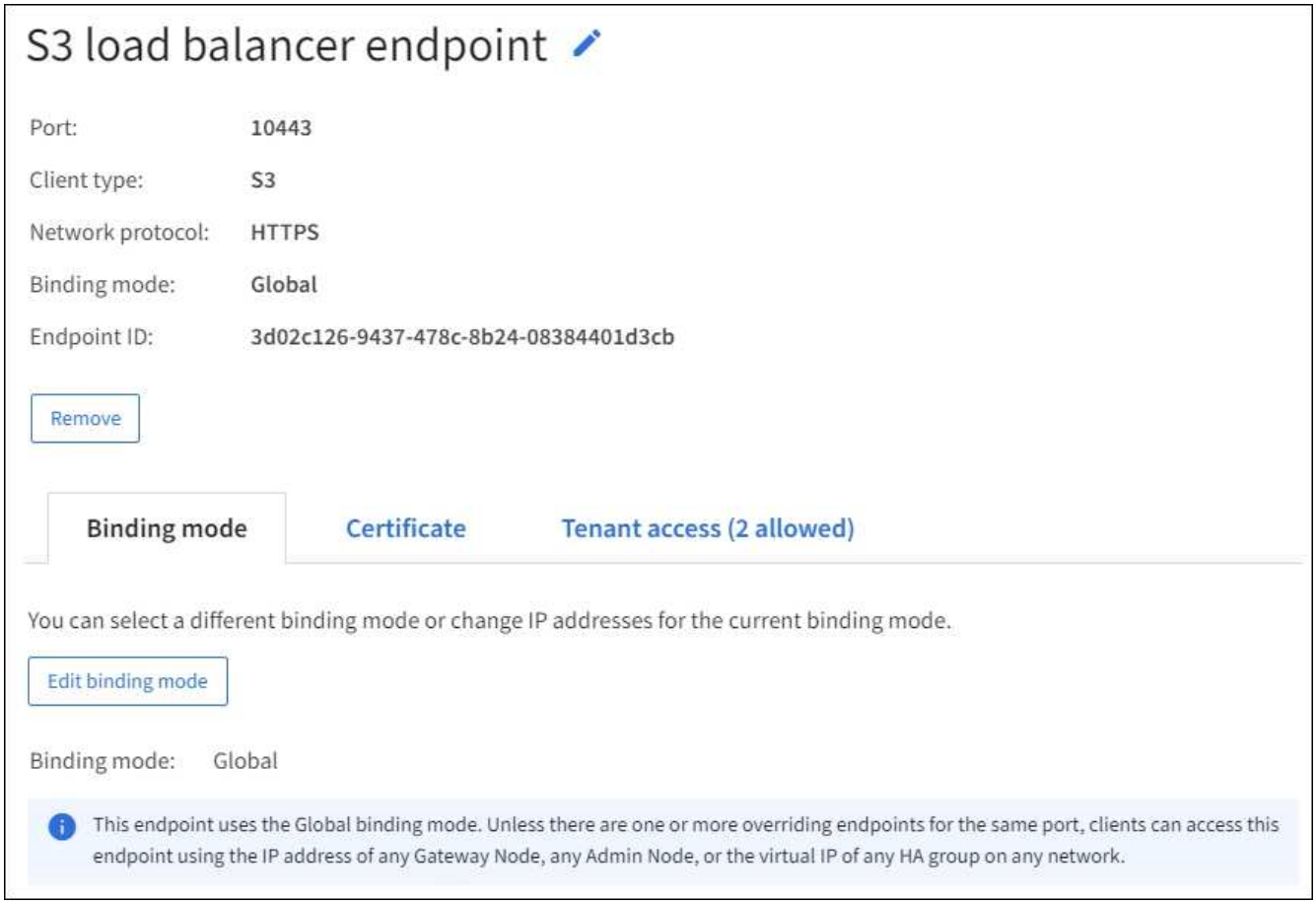
   ◦ 完整網域名稱或IP位址

   ◦ 任何必要的憑證詳細資料

檢視及編輯負載平衡器端點

您可以檢視現有負載平衡器端點的詳細資料、包括安全端點的憑證中繼資料。您可以變更端點的特定設定。

- 若要檢視所有負載平衡器端點的基本資訊、請檢閱「負載平衡器端點」頁面上的表格。
- 若要檢視特定端點的所有詳細資料、包括憑證中繼資料、請在表格中選取端點的名稱。顯示的資訊會因端點類型及其設定方式而異。



- 若要編輯端點、請使用負載平衡器端點頁面上的 * 動作 * 功能表。

如果您在編輯管理介面端點的連接埠時、無法存取 Grid Manager 、請更新 URL 和連接埠以重新取得存取權。

編輯端點之後、您可能需要等待15分鐘、才能將變更套用至所有節點。

工作	「行動」功能表	詳細資料頁面
編輯端點名稱	a. 選取端點的核取方塊。 b. 選取*「動作*」>*「編輯端點名稱*」。 c. 輸入新名稱。 d. 選擇*保存*。	a. 選取端點名稱以顯示詳細資料。 b. 選取編輯圖示 。 c. 輸入新名稱。 d. 選擇*保存*。

工作	「行動」功能表	詳細資料頁面
編輯端點連接埠	a. 選取端點的核取方塊。 b. 選取 * 動作 * > * 編輯端點連接埠 * c. 輸入有效的連接埠號碼。 d. 選擇*保存*。	*n*
編輯端點繫結模式	a. 選取端點的核取方塊。 b. 選取*「動作*」>*「編輯端點繫結模式*」。 c. 視需要更新連結模式。 d. 選取*儲存變更*。	a. 選取端點名稱以顯示詳細資料。 b. 選擇*編輯綁定模式*。 c. 視需要更新連結模式。 d. 選取*儲存變更*。
編輯端點憑證	a. 選取端點的核取方塊。 b. 選取*「動作*」>*「編輯端點憑證*」。 c. 視需要上傳或產生新的自訂憑證、或開始使用全域S3和Swift憑證。 d. 選取*儲存變更*。	a. 選取端點名稱以顯示詳細資料。 b. 選擇*認證*標籤。 c. 選取*編輯憑證*。 d. 視需要上傳或產生新的自訂憑證、或開始使用全域S3和Swift憑證。 e. 選取*儲存變更*。
編輯租戶存取	a. 選取端點的核取方塊。 b. 選取 * 動作 * > * 編輯租戶存取 * 。 c. 選擇不同的存取選項、從清單中選取或移除租戶、或兩者都執行。 d. 選取*儲存變更*。	a. 選取端點名稱以顯示詳細資料。 b. 選擇 * 租戶存取 * 標籤。 c. 選取 * 編輯租戶存取 * 。 d. 選擇不同的存取選項、從清單中選取或移除租戶、或兩者都執行。 e. 選取*儲存變更*。

移除負載平衡器端點

您可以使用* Actions（動作）*功能表移除一或多個端點、也可以從詳細資料頁面移除單一端點。

若要避免用戶端中斷、請先更新任何受影響的S3或Swift用戶端應用程式、再移除負載平衡器端點。使用指派給另一個負載平衡器端點的連接埠、更新每個用戶端以進行連線。請務必同時更新任何必要的憑證資訊。

如果您在移除管理介面端點時失去對 Grid Manager 的存取權、請更新 URL 。

- 若要移除一或多個端點：
  a. 在「負載平衡器」頁面中、選取您要移除的每個端點的核取方塊。
  b. 選擇*「Actions」（動作）>「Remove*」（移除

c. 選擇*確定*。

- 若要從詳細資料頁面移除一個端點：
  a. 從「負載平衡器」頁面。選取端點名稱。
  b. 在詳細資料頁面上選取*移除*。
  c. 選擇*確定*。

設定 S3 端點網域名稱

若要支援 S3 虛擬代管型要求、您必須使用 Grid Manager 來設定 S3 用戶端所連線的 S3 端點網域名稱清單。

不支援將 IP 位址用於端點網域名稱。未來的版本將會阻止此組態。

開始之前

- 您將使用登入Grid Manager "支援的網頁瀏覽器"。
- 您有 "特定存取權限"。
- 您已確認網格升級尚未進行。

網格升級進行中時、請勿變更網域名稱組態。

關於這項工作

若要讓用戶端使用S3端點網域名稱、您必須執行下列所有動作：

- 使用Grid Manager將S3端點網域名稱新增StorageGRID 至整個系統。
- 請確定 "用戶端用於 StorageGRID HTTPS 連線的憑證" 針對用戶端所需的所有網域名稱進行簽署。

  例如、如果端點是 `s3.company.com`、您必須確保用於HTTPS連線的憑證包含 `s3.company.com` 端點和端點的萬用字元主體替代名稱（SAN）： `*.s3.company.com`。

- 設定用戶端使用的DNS伺服器。為用戶端用來建立連線的 IP 位址加入 DNS 記錄、並確保記錄會參照所有必要的 S3 端點網域名稱、包括任何萬用字元名稱。

用戶端可以StorageGRID 使用閘道節點、管理節點或儲存節點的IP位址、或是連線至高可用度群組的虛擬IP位址、來連線至功能區。您應該瞭解用戶端應用程式如何連線至網格、以便在DNS記錄中包含正確的IP位址。

使用HTTPS連線（建議）到網格的用戶端可使用下列任一憑證：

- 連線到負載平衡器端點的用戶端可以使用該端點的自訂憑證。每個負載平衡器端點都可設定為辨識不同的 S3 端點網域名稱。
- 連線至負載平衡器端點或直接連線至儲存節點的用戶端可以自訂全域 S3 和 Swift API 憑證、以包含所有必要的 S3 端點網域名稱。

如果您沒有新增 S3 端點網域名稱、而且清單是空的、則會停用 S3 虛擬託管樣式要求的支援。

新增 S3 端點網域名稱

步驟

1. 選擇 * 組態 * > * 網路 * > * S3 端點網域名稱 * 。
2. 在 * 網域名稱 1* 欄位中輸入網域名稱。選取 * 新增其他網域名稱 * 以新增更多網域名稱。
3. 選擇*保存*。
4. 確定用戶端使用的伺服器憑證符合所需的 S3 端點網域名稱。
   - 如果用戶端連線到使用其本身憑證的負載平衡器端點、 "更新與端點相關的憑證"。
   - 如果用戶端連線到使用全域 S3 和 Swift API 憑證的負載平衡器端點、或直接連線到儲存節點、 "更新全域 S3 和 Swift API 憑證"。
5. 新增必要的DNS記錄、以確保端點網域名稱要求能夠解析。

結果

現在、當用戶端使用端點時 `bucket.s3.company.com`、DNS伺服器會解析為正確的端點、而且憑證會依照預期驗證端點。

重新命名 S3 端點網域名稱

如果您變更 S3 應用程式使用的名稱、虛擬代管樣式的要求將會失敗。

步驟

1. 選擇 * 組態 * > * 網路 * > * S3 端點網域名稱 * 。
2. 選取您要編輯的網域名稱欄位、然後進行必要的變更。
3. 選擇*保存*。
4. 選擇 * 是 * 以確認您的變更。

刪除 S3 端點網域名稱

如果您移除 S3 應用程式使用的名稱、虛擬代管樣式的要求將會失敗。

步驟

1. 選擇 * 組態 * > * 網路 * > * S3 端點網域名稱 * 。
2. 選取刪除圖示 ✕ 在網域名稱旁。
3. 選擇 * 是 * 以確認刪除。

相關資訊

- "使用S3 REST API"
- "檢視IP位址"
- "設定高可用度群組"

摘要：用於用戶端連線的IP位址和連接埠

若要儲存或擷取物件、 S3 和 Swift 用戶端應用程式會連線到負載平衡器服務（包含在所有管理節點和閘道節點上）、或是連接到所有儲存節點上的本機分配路由器（ LDR ）服務。

用戶端應用程式可以使用網格節點的 IP 位址和該節點上服務的連接埠號碼、來連線至 StorageGRID 。您也可以建立高可用度（ HA ）負載平衡節點群組、以提供使用虛擬 IP （ VIP ）位址的高可用度連線。如果您想要使用完整網域名稱（ FQDN ）而非 IP 或 VIP 位址連線至 StorageGRID 、您可以設定 DNS 項目。

下表摘要說明用戶端連線StorageGRID 至靜態的不同方式、以及每種連線類型所使用的IP位址和連接埠。如果您已經建立負載平衡器端點和高可用度（ HA ）群組、請參閱 何處可以找到 IP 位址 在 Grid Manager 中找出這些值。

連線位置	用戶端連線的服務	**IP** 位址	連接埠
HA 群組	負載平衡器	HA群組的虛擬IP位址	指派給負載平衡器端點的連接埠
管理節點	負載平衡器	管理節點的IP位址	指派給負載平衡器端點的連接埠
閘道節點	負載平衡器	閘道節點的IP位址	指派給負載平衡器端點的連接埠
儲存節點	LdR	儲存節點的IP位址	預設S3連接埠： • HTTPS ： 18082 • HTTP ： 18084 預設Swift連接埠： • HTTPS ： 18083 • HTTP ： 18085

URL 範例

若要將用戶端應用程式連線至 HA 群組的閘道節點負載平衡器端點、請使用如下所示的 URL 結構：

`https://VIP-of-HA-group:LB-endpoint-port`

例如、如果 HA 群組的虛擬 IP 位址為 192.0.2.5 、而負載平衡器端點的連接埠號碼為 10443 、則應用程式可以使用下列 URL 連線至 StorageGRID ：

`https://192.0.2.5:10443`

何處可以找到 IP 位址

1. 使用登入Grid Manager "支援的網頁瀏覽器"。

2. 若要尋找網格節點的IP位址：
   a. 選擇*節點*。
   b. 選取您要連線的管理節點、閘道節點或儲存節點。
   c. 選擇* Overview（概述）*選項卡。
   d. 在「節點資訊」區段中、記下節點的IP位址。
   e. 選取*顯示更多*以檢視IPv6位址和介面對應。

      您可以從用戶端應用程式建立連線至清單中的任何IP位址：

      - * eth0：* Grid Network
      - * eth1：*管理網路（選用）
      - * eth2：*用戶端網路（選用）

      如果您正在檢視管理節點或閘道節點、且該節點是高可用度群組中的作用中節點、則HA群組的虛擬IP位址會顯示在eth2上。

3. 若要尋找高可用度群組的虛擬IP位址：
   a. 選擇*組態*>*網路*>*高可用度群組*。
   b. 在表中、記下HA群組的虛擬IP位址。
4. 若要尋找負載平衡器端點的連接埠號碼：
   a. 選擇*組態*>*網路*>*負載平衡器端點*。
   b. 記下您要使用的端點連接埠編號。

      如果連接埠號碼為 80 或 443 、則端點只能在 Gateway 節點上設定、因為這些連接埠是保留在管理節點上。所有其他連接埠都在閘道節點和管理節點上設定。

   c. 從表格中選取端點名稱。
   d. 確認 * 用戶端類型 * （ S3 或 Swift ）符合將使用端點的用戶端應用程式。