



VMware vSphere 的角色型存取控制 (RBAC)

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

目錄

VMware vSphere 的角色型存取控制 (RBAC)	1
vCenter Server RBAC 如何與 ONTAP tools 協同工作	1
vCenter Server 權限示意圖	1
vCenter Server 權限的組成部分	1
vCenter Server 對 ONTAP 工具的 RBAC 注意事項	2
vCenter 角色和系統管理員帳戶	2
vSphere 物件階層	2
ONTAP tools for VMware vSphere 10 隨附的角色	3
vSphere 物件和 ONTAP 儲存設備後端	6
使用 vCenter Server RBAC	6

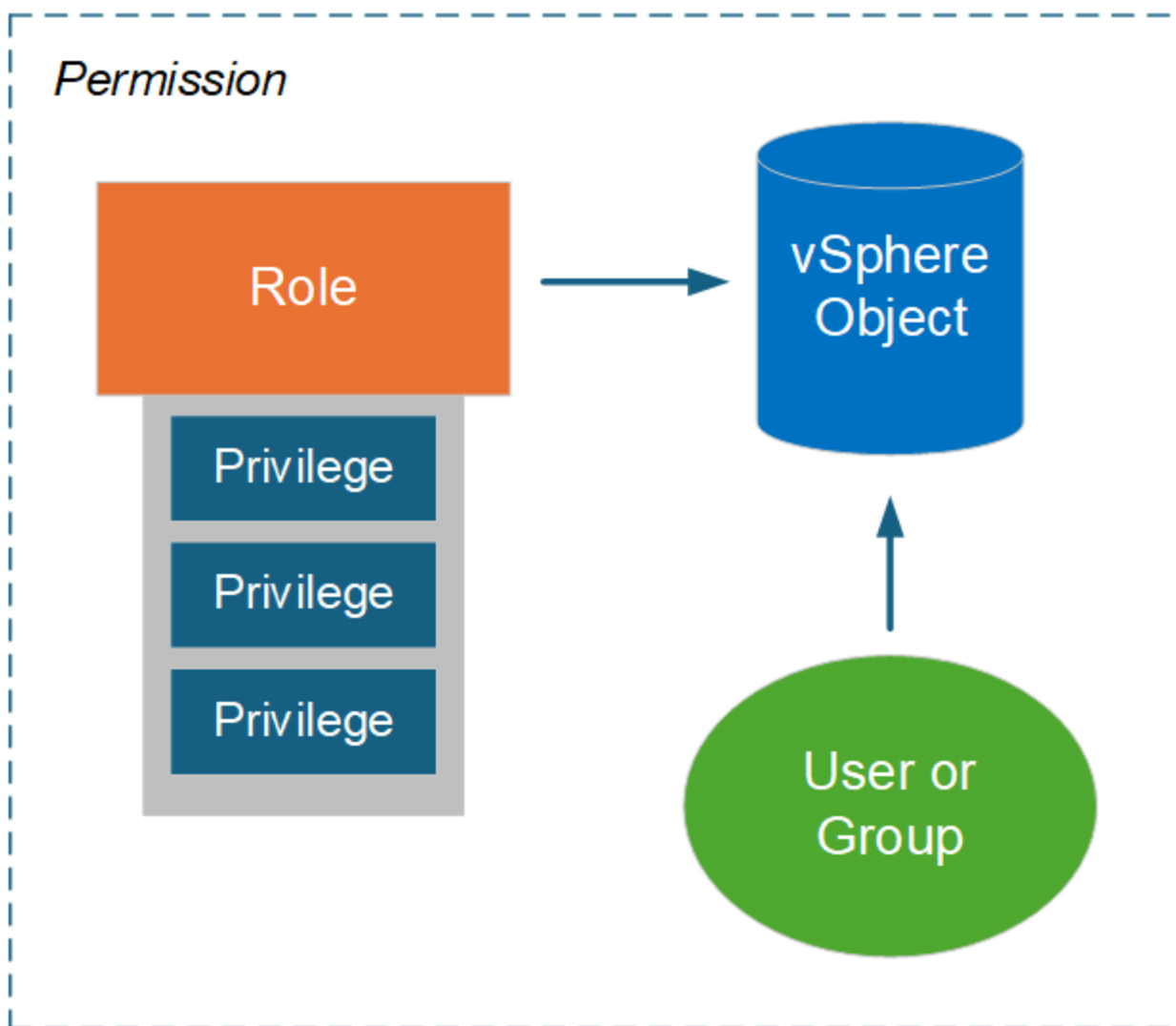
VMware vSphere 的角色型存取控制（RBAC）

vCenter Server RBAC 如何與 ONTAP tools 協同工作

VMware vCenter Server 提供基於角色的存取控制（RBAC）功能，可讓您控制對 vSphere 物件的存取。它是 vCenter 集中式驗證和授權安全性服務的重要組成部分。

vCenter Server 權限示意圖

權限是在 vCenter Server 環境中實施存取控制的基礎。它應用於 vSphere 物件，權限定義中包含使用者或群組。下圖提供了 vCenter 權限的高階說明。



vCenter Server 權限的組成部分

vCenter Server 權限是由多個元件組成的套件，這些元件在建立權限時綁定在一起。

vSphere 物件

權限與 vSphere 物件相關聯，例如 vCenter 伺服器、ESXi 主機、虛擬機器、資料存放區、資料中心和資料夾。vCenter 伺服器根據物件已指派的權限，決定每個使用者或群組可以對該物件執行哪些操作或工作。對於 ONTAP tools for VMware vSphere 的特定工作，所有權限均在 vCenter 伺服器的根目錄或根目錄資料夾層級指派和驗證。如需詳細資訊，請參閱 ["使用 RBAC 搭配 vCenter 伺服器"](#)。

Privileges 和角色

搭配 ONTAP tools for VMware vSphere 10 使用的 vSphere 權限有兩種類型。為了簡化在此環境中搭配使用 RBAC 的作業，ONTAP tools 提供了包含所需原生與自訂權限的角色。這些權限包括：

- 原生 vCenter Server Privileges

這些是 vCenter Server 提供的權限。

- ONTAP tools 專屬 Privileges

這些是 ONTAP tools for VMware vSphere 特有的自訂 Privileges。

使用者和群組

您可以使用 Active Directory 或本機 vCenter Server 執行個體定義使用者和群組。結合角色，您可以在 vSphere 物件階層中的物件上建立權限。此權限根據關聯角色中的 Privileges 授予存取。請注意，角色並非直接單獨指派給使用者。而是使用者和群組作為較大範圍 vCenter Server 權限的一部分，透過角色 Privileges 取得物件的存取權。

vCenter Server 對 ONTAP 工具的 RBAC 注意事項

在正式作業環境中使用 ONTAP tools for VMware vSphere 10 RBAC 實作搭配 vCenter Server 之前，您應該考慮以下幾個方面。

vCenter 角色和系統管理員帳戶

只有在您想要限制對 vSphere 物件及相關管理工作的存取時，才需要定義和使用自訂的 vCenter Server 角色。如果不需要限制存取，您可以使用系統管理員帳戶。每個系統管理員帳戶都在物件階層架構的最高層級定義了 Administrator 角色。這可提供對 vSphere 物件的完整存取權限，包括由 ONTAP tools for VMware vSphere 10 新增的物件。

vSphere 物件階層

The vSphere 物件清單依層級結構組織。例如，您可以如下向下瀏覽層級結構：

vCenter Server → Datacenter → Cluster → ESXi host → Virtual Machine

除了 VAAI 外掛操作之外，所有權限都在 vSphere 物件層級中進行驗證，VAAI 外掛操作則針對目標 ESXi 主機進行驗證。

ONTAP tools for VMware vSphere 10 隨附的角色

為了簡化 vCenter Server RBAC 的使用，ONTAP tools for VMware vSphere 提供了針對各種管理任務量身定制的預先定義角色。



如有需要，您可以建立新的自訂角色。為此，請複製現有的 ONTAP tools 角色之一，並根據需要進行編輯。進行組態變更後，受影響的 vSphere 用戶端使用者需要登出並重新登入以啟動變更。

若要檢視 ONTAP tools for VMware vSphere 角色、請在 vSphere Client 頂端選取 **Menu**、然後按一下 **Administration**、再按一下左側的 **Roles**。指派給負責部署或上線 vCenter Server 之 vCenter 使用者的角色、必須包含下列權限。請確保將這些權限設定為部署或上線程序的先決條件。

- 警示
 - 確認警示
- 內容程式庫
 - 新增程式庫項目
 - 簽入範本
 - 查看模板
 - 下載檔案
 - 匯入儲存設備
 - 讀取儲存設備
 - 同步程式庫項目
 - 同步已訂閱的程式庫
 - 檢視組態設定
- 資料存放區
 - 分配空間
 - 瀏覽資料存放區
 - 低階檔案作業
 - 移除檔案
 - 更新虛擬機器檔案
 - 更新虛擬機器中繼資料
- ESX Agent Manager
 - 檢視
- 資料夾
 - 建立資料夾
- 主機
 - 組態
 - 進階設定

- 更改設定
 - 網路組態
 - 系統資源
 - 虛擬機器自動啟動組態
- 本機作業
 - 建立虛擬機器
 - 刪除虛擬機器
 - 重新配置虛擬機器
- 網路
 - 指派網路
 - 設定
- OvfManager
 - OvfConsumer 存取
- 主機設定檔
 - 檢視
- 資源
 - 將虛擬機器指派給資源池
- 排程工作
 - 建立工作
 - 修改工作
 - 執行工作
- 任務
 - 建立工作
 - 更新工作
- vApp
 - 新增虛擬機器
 - 分配資源池
 - 分配 vApp
 - 建立
 - 匯入
 - 移動
 - 關閉電源
 - 開機
 - 從 URL 拉取

- 查看 OVF 環境
- 虛擬機器
 - 變更組態
 - 新增現有磁碟
 - 新增磁碟
 - 新增或移除設備
 - 進階組態
 - 變更 CPU 計數
 - 變更記憶體
 - 更改設定
 - 更改資源
 - 擴充虛擬磁碟
 - 修改裝置設定
 - 移除磁碟
 - 重設訪客資訊
 - 升級虛擬機器相容性
 - 編輯庫存
 - 從現有項目建立
 - 建立新的
 - 移動
 - 註冊使用
 - 移除
 - 取消註冊
 - 互動
 - 虛擬機器備份作業
 - 設定 CD 媒體
 - 設定軟碟媒體
 - 連接裝置
 - 主控台互動
 - 透過 VIX API 進行客體作業系統管理
 - 關閉電源
 - 開機
 - 重置
 - 暫停

- 資源配置
 - 允許磁碟存取
 - 複製範本
 - 自訂客體
 - 部署範本
 - 修改自訂規格
 - 閱讀自訂規格
- Snapshot 快照技術管理
 - 建立快照
 - 移除快照
 - 重新命名快照
 - 還原至快照

以下說明三種預先定義的角色。

NetApp ONTAP tools for VMware vSphere 系統管理員

提供執行核心 ONTAP tools for VMware vSphere 系統管理員工作所需的所有原生 vCenter Server 權限和 ONTAP tools 特定權限。

NetApp ONTAP tools for VMware vSphere 唯讀

提供對 ONTAP tools 的唯讀存取。這些使用者無法執行任何受存取控制的 ONTAP tools for VMware vSphere 動作。

NetApp ONTAP tools for VMware vSphere 資源配置

提供部分原生 vCenter Server 權限和 ONTAP tools 特定權限，這些權限是資源配置儲存設備所必需的。您可以執行以下工作：

- 建立新的資料存放區
- 管理資料存放區

vSphere 物件和 ONTAP 儲存設備後端

這兩個基於角色的存取控制（RBAC）環境協同運作。在 vSphere 用戶端介面執行工作時，會先檢查 vCenter Server 上定義的 ONTAP tools 角色。如果 vSphere 允許該操作，則進一步檢查 ONTAP 角色權限。第二步驟是根據建立和設定儲存設備後端時指派給使用者的 ONTAP 角色來執行。

使用 vCenter Server RBAC

使用 vCenter Server 權限時，有幾點需要注意。

所需權限

若要存取 ONTAP tools for VMware vSphere 10 使用者介面，您需要擁有 ONTAP tools 專屬的「檢視」權限。如果您在未具備此權限的情況下登入 vSphere，並按一下 NetApp 圖示，ONTAP tools for VMware vSphere 將顯示錯誤訊息，並阻止您存取使用者介面。

在 vSphere 物件階層中的指派層級，決定了您可以存取使用者介面的哪些部分。將「檢視」權限指派給根目錄物件，可讓您透過按一下 NetApp 圖示來存取 ONTAP tools for VMware vSphere。

您也可以將「檢視」權限指派給較低 vSphere 物件層級。但是，這將限制您可以存取和使用的 ONTAP tools for VMware vSphere 功能表。

指派權限

如果您想要限制對 vSphere 物件和工作的存取，則需要使用 vCenter Server 權限。您在 vSphere 物件階層中分配權限的位置，決定了使用者可以執行的 ONTAP tools for VMware vSphere 10 工作。



除非您需要定義更嚴格的存取，否則通常最好在根目錄物件或根目錄資料夾層級指派權限。

ONTAP tools for VMware vSphere 10 提供的權限適用於自訂非 vSphere 物件，例如儲存系統。如果可能，您應該將這些權限指派給 ONTAP tools for VMware vSphere 根目錄物件，因為沒有可以指派這些權限的 vSphere 物件。例如，任何包含 ONTAP tools for VMware vSphere 「新增/修改/移除儲存系統」權限的權限，都應指派至根目錄物件層級。

在物件層次結構的較高層級定義權限時，您可以設定該權限，使其向下傳遞並由子物件繼承。如有需要，您可以為子物件指派額外的權限，以置換從父物件繼承的權限。

您可以隨時修改權限。如果您變更了權限中的任何特權，則與該權限關聯的使用者需要登出 vSphere 並重新登入才能使變更生效。

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

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

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

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

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

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

商標資訊

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