使用 VMware vSphere 的 RBAC

ONTAP tools for VMware vSphere 10

NetApp
November 17, 2025

目錄

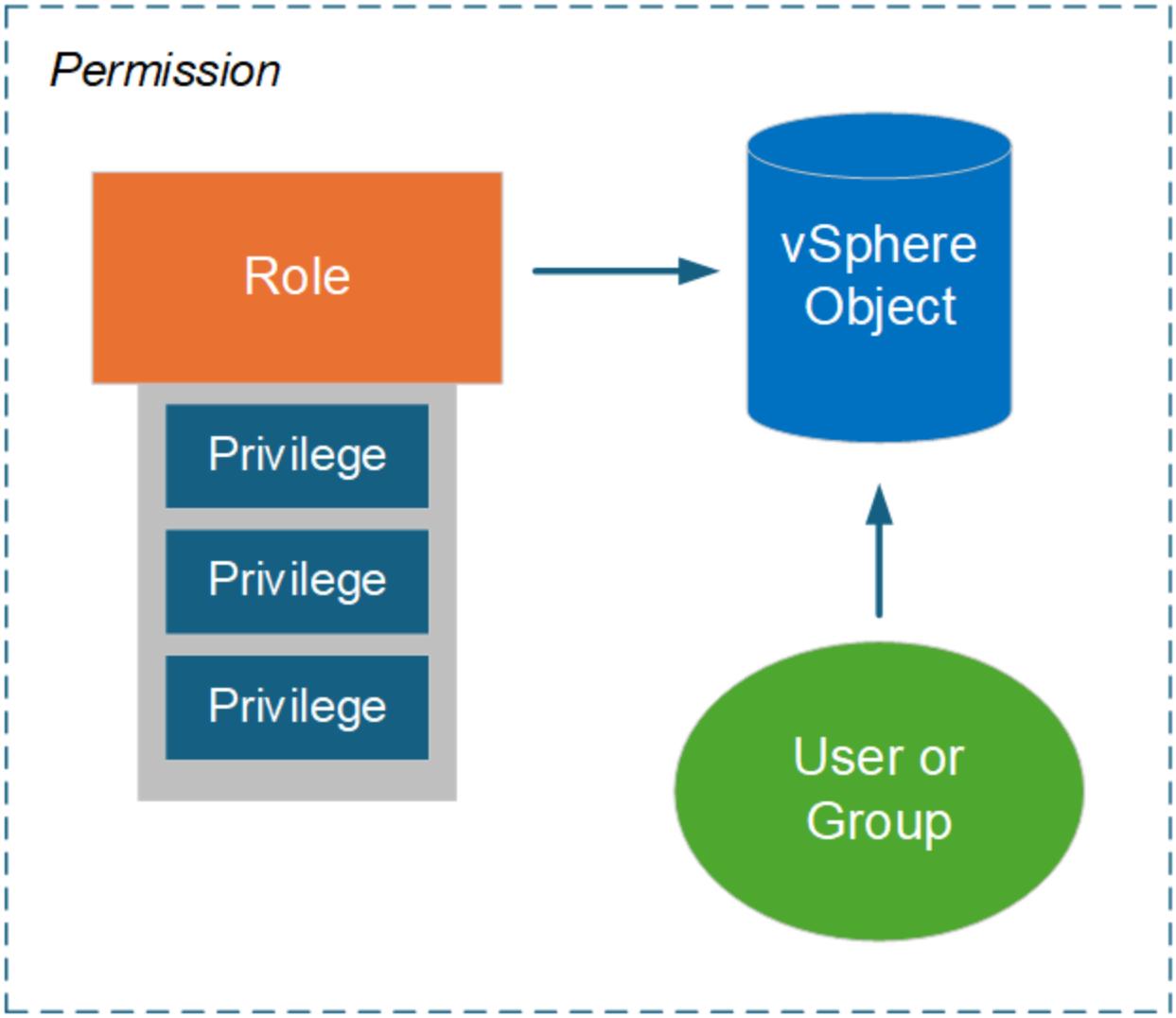
使用 VMware vSphere 的 RBAC

vCenter Server RBAC 環境搭配適用於 VMware vSphere 10 的 ONTAP 工具

VMware vCenter Server 提供 RBAC 功能，可讓您控制對 vSphere 物件的存取。這是 vCenter 集中式驗證和授權安全服務的重要部分。

vCenter Server 權限的圖例

權限是在 vCenter Server 環境中強制執行存取控制的基礎。它會套用至具有權限定義所包含之使用者或群組的 vSphere 物件。下圖提供 vCenter 權限的高階圖例。



vCenter Server 權限的元件

vCenter Server 權限是一組包含多個元件的套件，這些元件會在建立權限時綁定在一起。

vSphere物件

權限會與 vSphere 物件相關聯，例如 vCenter Server ， ESXi 主機，虛擬機器，資料存放區，資料中心和資料夾。vCenter Server 會根據物件的指派權限，決定每個使用者或群組可以對物件執行哪些動作或工作。針對適用於 VMware vSphere 的 ONTAP 工具所特有的工作，所有權限都會在 vCenter Server 的根或根資料夾層級指派和驗證。如需詳細資訊、請參閱 "將 RBAC 搭配 vCenter 伺服器使用" 。

Privileges 和角色

ONTAP 工具適用於 VMware vSphere 10 的 vSphere Privileges 有兩種類型。為了簡化在此環境中使用 RBAC 的作業， ONTAP 工具提供包含所需原生和自訂 Privileges 的角色。Privileges 包括：

- 原生vCenter Server權限

  這些是 vCenter Server 提供的 Privileges 。

- ONTAP 工具專屬權限

  這些是專為 VMware vSphere ONTAP 工具所設計的自訂 Privileges 。

使用者與群組

您可以使用 Active Directory 或本機 vCenter Server 執行個體來定義使用者和群組。結合角色，您可以針對 vSphere 物件階層中的物件建立權限。權限會根據相關角色中的 Privileges 來授予存取權。請注意，角色不會直接指派給隔離的使用者。而是使用者和群組透過角色 Privileges 取得物件的存取權，這是較大的 vCenter Server 權限的一部分。

使用 vCenter Server RBAC 搭配適用於 VMware vSphere 10 的 ONTAP 工具

在正式作業環境中使用 VMware vSphere 10 RBAC 實作的 ONTAP 工具有幾個層面，您應該先考慮這些層面。

vCenter 角色和管理員帳戶

如果您想要限制 vSphere 物件和相關管理工作的存取，只需定義和使用自訂 vCenter Server 角色。如果不需要限制存取，您可以改用系統管理員帳戶。每個系統管理員帳戶都是以物件階層最上層的系統管理員角色來定義。這可讓您完整存取 vSphere 物件，包括 ONTAP 工具為 VMware vSphere 10 新增的物件。

vSphere 物件階層架構

vSphere 物件詳細目錄是以階層架構來組織。例如，您可以依照下列方式向下移動階層：

`vCenter Server--> --> --> --> Datacenter --> Cluster --> --> ESXi host Virtual Machine`

所有權限都會在 vSphere 物件階層中驗證，但 VAAI 外掛程式作業除外，這些作業會針對目標 ESXi 主機進行驗

證。

適用於 **VMware vSphere 10** 的 **ONTAP** 工具隨附的角色

為了簡化使用 vCenter Server RBAC 的過程，適用於 VMware vSphere 的 ONTAP 工具可針對各種管理工作提供預先定義的角色。

> 您可以視需要建立新的自訂角色。在這種情況下，您應該複製其中一個現有的 ONTAP 工具角色，並視需要進行編輯。變更組態後，受影響的 vSphere 用戶端使用者必須登出並重新登入，才能啟動變更。

若要檢視適用於 VMware vSphere 角色的 ONTAP 工具，請選取 vSphere Client 頂端的 * 功能表 * ，然後按一下 * 管理 * ，然後按一下左側的 * 角色 * 。有三種預先定義的角色，如下所述。

適用於 **VMware vSphere** 管理員的 **NetApp ONTAP** 工具

提供執行核心 ONTAP 工具以執行 VMware vSphere 管理員工作所需的所有原生 vCenter Server Privileges 和 ONTAP 工具專屬 Privileges 。

適用於 **VMware vSphere** 的 **NetApp ONTAP** 工具唯讀

提供 ONTAP 工具的唯讀存取權。這些使用者無法針對存取控制的 VMware vSphere 動作執行任何 ONTAP 工具。

VMware vSphere 佈建的 **NetApp ONTAP** 工具

提供部分原生 vCenter Server 權限和 ONTAP 工具專屬權限、這些權限是配置儲存設備所需的。您可以執行下列工作：

- 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

這兩種 RBAC 環境可一起運作。在 vSphere 用戶端介面中執行工作時，會先檢查定義至 vCenter Server 的 ONTAP 工具角色。如果 vSphere 允許此作業，則會檢查 ONTAP 角色 Privileges 。第二個步驟是根據建立及設定儲存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 Privileges 和權限時，需要考量一些事項。

必要權限

若要存取適用於 VMware vSphere 10 使用者介面的 ONTAP 工具，您必須擁有 ONTAP 工具專屬的 _ 檢視 _ 權限。如果您在沒有此權限的情況下登入 vSphere ，並按一下 NetApp 圖示，適用於 VMware vSphere 的 ONTAP 工具會顯示錯誤訊息，並阻止您存取使用者介面。

vSphere 物件階層中的指派層級會決定您可以存取的使用者介面部分。將檢視權限指派給根物件可讓您按一下 NetApp 圖示來存取適用於 VMware vSphere 的 ONTAP 工具。

您可以將檢視權限指派給另一個較低的 vSphere 物件層級。不過，這會限制您可以存取和使用的 VMware vSphere ONTAP 工具功能表。

指派權限

如果您想要限制 vSphere 物件和工作的存取，則需要使用 vCenter Server 權限。在 vSphere 物件階層中指派權限的位置，決定使用者可以執行的 VMware vSphere 10 工作的 ONTAP 工具。

除非您需要定義更嚴格的存取，否則在根物件或根資料夾層級指派權限通常是個不錯的做法。

適用於 VMware vSphere 10 的 ONTAP 工具所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 VMware vSphere 根物件的 ONTAP 工具，因為沒有您可以指派的 vSphere 物件。例如，任何包含適用於 VMware vSphere 「新增 / 修改 / 移除儲存系統」權限的 ONTAP 工具權限，都應在根物件層級指派。

在物件階層中定義較高層級的權限時，您可以設定權限，讓子物件向下傳遞並繼承權限。如果需要，您可以指派額外權限給子物件，這些子物件會覆寫從父物件繼承的權限。

您可以隨時修改權限。如果您在權限內變更任何 Privileges ，則與權限相關的使用者必須登出 vSphere ，然後重新登入才能啟用變更。

版權資訊

商標資訊