VMware vSphere 的 RBAC

ONTAP tools for VMware vSphere 10

NetApp
November 04, 2025

目錄

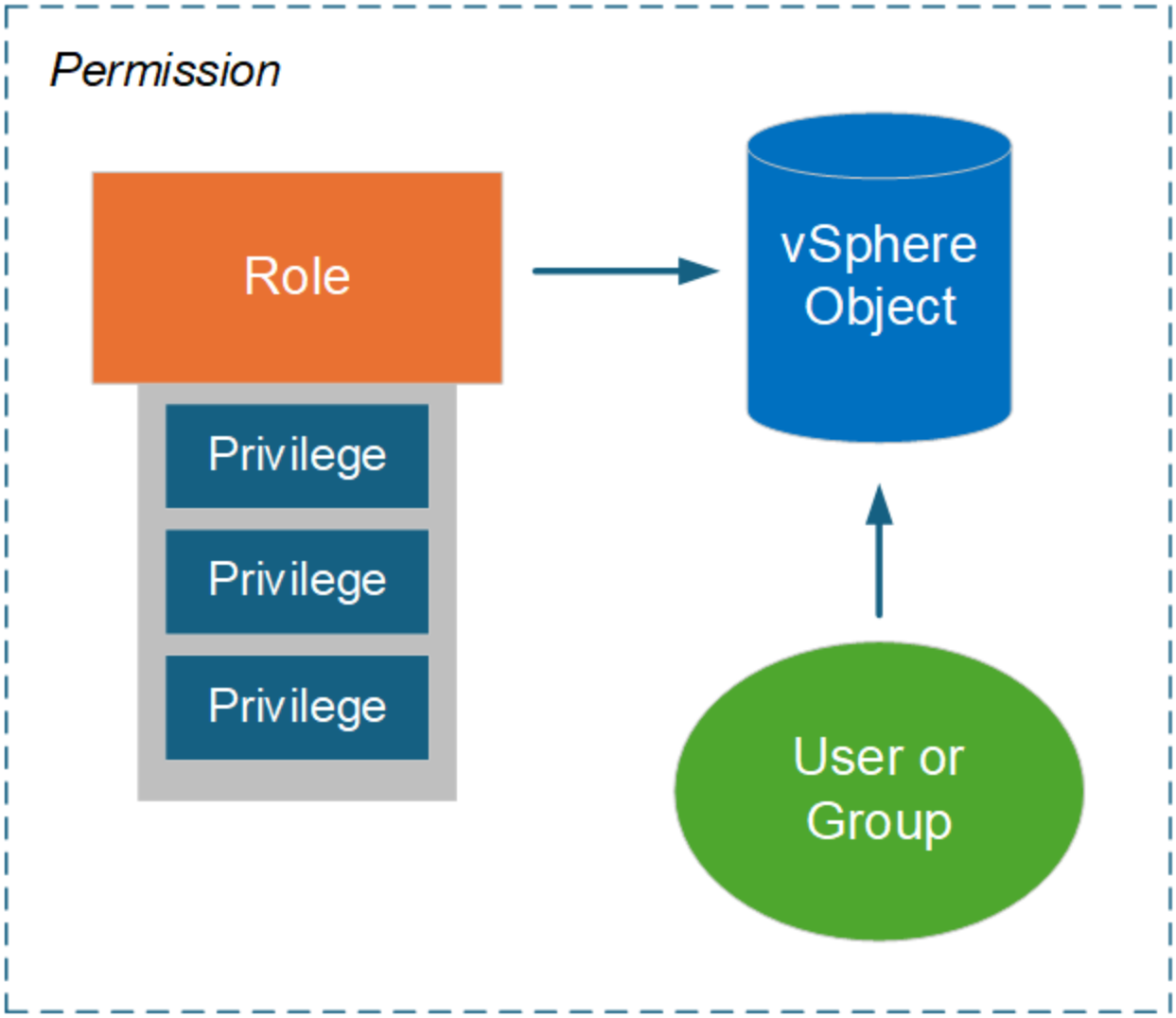
VMware vSphere 的 RBAC

ONTAP tools for VMware vSphere的 vCenter Server RBAC 環境

VMware vCenter Server 提供了 RBAC 功能，讓您能夠控制對 vSphere 物件的存取。它是vCenter集中身份驗證和授權安全服務的重要組成部分。

vCenter Server 權限的圖示

權限是 vCenter Server 環境中強制執行存取控制的基礎。它適用於具有權限定義中包含的使用者或群組的 vSphere 物件。下圖提供了 vCenter 權限的進階說明。



vCenter Server 權限的組成部分

vCenter Server 權限是建立權限時綁定在一起的幾個元件的套件。

vSphere 對象

權限與 vSphere 物件相關聯，例如 vCenter Server、ESXi 主機、虛擬機器、資料儲存區、資料中心和資料夾。根據物件指派的權限，vCenter Server 決定每個使用者或群組可以對該物件執行哪些操作或任務。對於特定於ONTAP tools for VMware vSphere的任務，所有權限均在 vCenter Server 的根或根資料夾層級指派和驗證。看"將 RBAC 與 vCenter 伺服器結合使用"了解更多。

Privileges和角色

適用於ONTAP tools for VMware vSphere使用兩種類型的 vSphere 權限。為了簡化在此環境中使用 RBAC 的工作， ONTAP工具提供了包含所需的本機和自訂權限的角色。特權包括：

- 本機 vCenter Server 權限

  這些是 vCenter Server 提供的權限。

- ONTAP工具特定的權限

  這些是適用於ONTAP tools for VMware vSphere獨有的自訂權限。

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，您可以建立對 vSphere 物件層次結構中物件的權限。此權限根據關聯角色中的特權授予存取權限。請注意，角色並非直接指派給單獨使用者。相反，使用者和群組透過角色特權獲得對物件的存取權限，這是更大的 vCenter Server 權限的一部分。

將 vCenter Server RBAC 與ONTAP tools for VMware vSphere結合使用

在生產環境中使用適用於ONTAP tools for VMware vSphere之前，您應該考慮它的幾個面向。

vCenter 角色和管理員帳戶

如果您想要限制對 vSphere 物件和相關管理任務的訪問，則只需定義和使用自訂 vCenter Server 角色。如果不需要限制訪問，您可以改用管理員帳戶。每個管理員帳戶都定義為位於物件層次結構頂層的管理員角色。這提供了對 vSphere 物件的完全存取權限，包括由ONTAP tools for VMware vSphere 10 新增的物件。

vSphere 物件層次結構

vSphere 物件清單依層次結構組織。例如，您可以如下向下移動層次結構：

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

除 VAAI 插件操作外，所有權限均在 vSphere 物件層次結構中驗證，VAAI 插件操作則針對目標 ESXi 主機進行

驗證。

ONTAP tools for VMware vSphere中所包含的角色

為了簡化使用 vCenter Server RBAC 的工作，ONTAP tools for VMware vSphere提供了針對各種管理任務自訂的預先定義角色。

> 如果需要，您可以建立新的自訂角色。在這種情況下，您應該複製現有的ONTAP工具角色之一並根據需要進行編輯。進行設定變更後，受影響的 vSphere 用戶端使用者需要登出並重新登入才能啟動變更。

若要查看ONTAP tools for VMware vSphere，請選擇 vSphere Client 頂部的“選單”，然後按一下左側的“管理”和“角色”。有三個預先定義的角色，如下所述。

適用於 **VMware vSphere** 管理員的**NetApp ONTAP tools for VMware vSphere**

提供執行ONTAP tools for VMware vSphere管理員任務所需的所有本機 vCenter Server 權限和ONTAP工具特定權限。

ONTAP tools for VMware vSphere唯讀的**NetApp ONTAP** 工具

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

適用於 **VMware vSphere Provision** 的**NetApp ONTAP tools for VMware vSphere**

提供配置儲存所需的一些本機 vCenter Server 權限和ONTAP工具特定的權限。您可以執行以下任務：

- 建立新的資料存儲
- 管理資料儲存區

vSphere 物件和ONTAP儲存後端

兩個 RBAC 環境協同工作。在 vSphere 用戶端介面中執行任務時，首先檢查定義到 vCenter Server 的ONTAP工具角色。如果 vSphere 允許該操作，則檢查ONTAP角色權限。第二步是根據建立和配置儲存後端時分配給使用者的ONTAP角色執行的。

使用 vCenter Server RBAC

使用 vCenter Server 特權和權限時需要考慮一些事項。

所需權限

若要存取適用ONTAP tools for VMware vSphere，您需要擁有特定於ONTAP工具的 *View* 權限。如果您在沒有此權限的情況下登入 vSphere 並點擊NetApp圖標，則ONTAP tools for VMware vSphere將顯示錯誤訊息並阻止您存取使用者介面。

vSphere 物件層次結構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物件後，您可以透過點選NetApp圖示來存取適用ONTAP tools for VMware vSphere。

您可以將檢視權限指派給另一個較低的 vSphere 物件等級。但是，這將限制您可以存取和使用的ONTAP tools for VMware vSphere。

分配權限

如果您想要限制對 vSphere 物件和任務的訪問，則需要使用 vCenter Server 權限。您在 vSphere 物件層次結構中指派權限的位置決定了使用者可以執行的ONTAP tools for VMware vSphere。

除非您需要定義更嚴格的存取權限，否則在根物件或根資料夾層級分配權限通常是一種很好的做法。

ONTAP tools for VMware vSphere提供的權限適用於自訂非 vSphere 對象，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，因為沒有可以將其指派給的 vSphere 物件。例如，任何包含適用ONTAP tools for VMware vSphere「新增/修改/刪除儲存系統」權限的權限都應在根物件層級指派。

當在物件層次結構的較高層級定義權限時，您可以配置該權限，以便它被傳遞並由子物件繼承。如果需要，您可以為子物件指派額外的權限，以覆寫從父物件繼承的權限。

您可以隨時修改權限。如果您變更權限中的任何特權，則與該權限關聯的使用者需要登出 vSphere 並重新登入以啟用變更。

版權資訊

商標資訊