角色型存取控制（RBAC）

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

目錄

角色型存取控制（RBAC）

了解 ONTAP tools RBAC

基於角色的存取控制 （RBAC） 是一種用於控制組織內資源存取的安全性架構。RBAC 透過定義具有特定權限層級的角色來執行動作，而非為個別使用者指派授權，藉此簡化管理。已定義的角色會指派給使用者，有助於降低錯誤風險，並簡化整個組織的存取控制管理。

基於角色的存取控制（RBAC）標準模型包含多種實作技術或階段，其複雜度逐漸遞增。因此，實際的 RBAC 部署會根據軟體供應商及其客戶的需求而有所不同，複雜程度從相對簡單到非常複雜不等。

RBAC 元件

從總體上看，每個 RBAC 實作通常包含幾個元件。這些元件以不同的方式結合在一起，共同定義授權流程。

Privileges

權限 是指可以允許或拒絕的操作或能力。它可以是簡單的權限，例如讀取檔案，也可以是特定於某個軟體系統的更抽象的操作。Privileges 也可以用於限制對 REST API 端點和 CLI 命令的存取。每個 RBAC 實作都包含預先定義的權限，並且可能允許管理員建立自訂權限。

角色

角色是一個包含一個或多個 Privileges 的 Container。角色通常根據特定的任務或工作職能來定義。當角色指派給使用者時，該使用者將獲得該角色中包含的所有 Privileges。與 Privileges 一樣，實作通常包含預先定義的角色，並且通常也允許建立自訂角色。

物件

在基於角色的存取控制 (RBAC) 環境中，_物件_代表一個真實或抽象化的資源。透過 Privileges 定義的動作會在關聯的物件上或與關聯的物件一起執行。根據實作方式，Privileges 可以授予物件類型或特定的物件執行個體。

使用者和群組

Users 在驗證後會被指派或關聯一個角色。一些 RBAC 實作只允許一個使用者擁有一個角色，而有些則允許一個使用者擁有多個角色，但可能一次只能啟動一個角色。將角色指派給 *groups* 可以進一步簡化安全性管理。

權限

權限是一種定義，它將使用者或使用者群組以及角色綁定到物件。權限在層級物件模型中非常有用，因為層級結構中的子物件可以選擇繼承權限。

兩種 RBAC 環境

在使用 ONTAP tools for VMware vSphere 10 時，需要考慮兩種不同的 RBAC 環境。ONTAP tools for VMware vSphere 10 需要在 vCenter 和 ONTAP 中擁有特定的 Privileges 才能執行操作。雖然 ONTAP tools 可以自動執行儲存管理工作，但它不會在 vCenter 或 ONTAP 中建立使用者帳戶。服務帳戶必須由 vSphere 系統管理員視需要建立。本文件旨在指導系統管理員如何指派必要的角色和權限，以有效管理 ONTAP tools。

VMware vCenter Server

VMware vCenter Server 中的 RBAC 實作用於限制對透過 vSphere Client 使用者介面所公開物件的存取。在為 VMware vSphere 10 安裝 ONTAP tools 時，RBAC 環境會擴展以包含代表 ONTAP tools 功能的其他物件。這些

物件的存取權限透過遠端外掛提供。如需詳細資訊，請參閱 "vCenter Server RBAC 環境"。

ONTAP 叢集

ONTAP tools for VMware vSphere 10 透過 ONTAP REST API 連線至 ONTAP 叢集，以執行儲存設備相關作業。對儲存資源的存取由與驗證期間所提供的 ONTAP 使用者相關聯的 ONTAP 角色控制。如需詳細資訊，請參閱 "ONTAP RBAC 環境"。

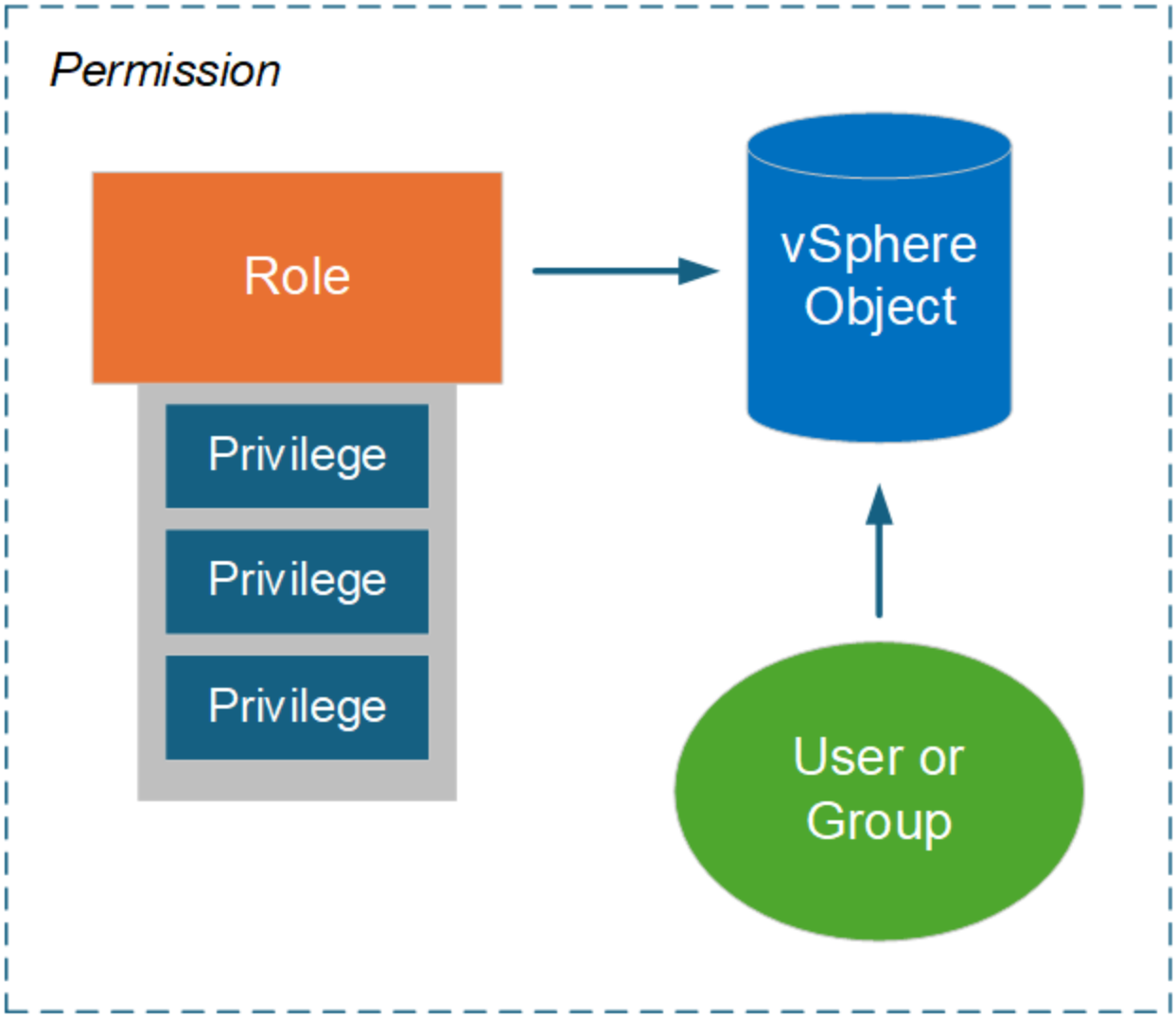
VMware vSphere 的角色型存取控制 （RBAC）

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。

RBAC 與 ONTAP

ONTAP RBAC 如何與 ONTAP tools 協同工作

ONTAP 提供強大且可擴充的 RBAC 環境。您可以使用 RBAC 功能來控制透過 REST API 和 CLI 公開的儲存設備和系統操作的存取。在搭配 ONTAP tools for VMware vSphere 10 部署使用之前，建議先熟悉此環境。

管理選項總覽

根據您的環境和目標，使用 ONTAP RBAC 時有多種選項可供選擇。以下提供主要管理決策的總覽。另請參閱 "ONTAP 自動化：RBAC 安全性總覽"以取得更多資訊。

> ONTAP RBAC 專為儲存環境量身定制，比 vCenter Server 提供的 RBAC 實作更簡單。使用 ONTAP，您可以直接為使用者指派角色。與 vCenter Server 所使用的明確權限組態不同，ONTAP RBAC 無需進行此類組態。

角色和 **Privileges** 類型

定義 ONTAP 使用者時需要指定 ONTAP 角色。ONTAP 角色有兩種類型：

- REST

  REST 角色是在 ONTAP 9.6 中引入的，通常應用於透過 REST API 存取 ONTAP 的使用者。這些角色所包含的 Privileges 是根據對 ONTAP REST API 端點及其相關動作的存取來定義的。

- 傳統的

  這些是 ONTAP 9.6 之前的舊版角色。它們仍然是 RBAC 的基礎層面。權限是根據對 ONTAP CLI 命令的存取權限來定義的。

雖然 REST 角色是最近才推出的，但傳統角色也有一些優勢。例如，可以新增額外的查詢參數，使 Privileges 能夠更精確地定義其適用的物件。

範圍

ONTAP 角色可以使用兩種不同範圍之一來定義。它們可以套用至特定的資料 SVM （SVM 層級）或整個 ONTAP 叢集（叢集層級）。

角色定義

ONTAP 在叢集和 SVM 層級都提供了一組預先定義的角色。您也可以定義自訂角色。

使用 **ONTAP REST** 角色

使用 ONTAP tools for VMware vSphere 10 中包含的 ONTAP REST 角色時，需要考慮以下幾個面向。

角色映射

無論使用傳統角色還是 REST 角色，所有 ONTAP 存取決策都基於底層 CLI 命令。但由於 REST 角色中的 Privileges 是根據 REST API 端點定義的，因此 ONTAP 需要為每個 REST 角色建立一個映射的傳統角色。因此，每個 REST 角色都映射到一個底層的傳統角色。這使得 ONTAP 能夠以一致的方式做出存取控制決策，而無需考慮角色類型。您無法修改這些並行映射的角色。

使用 **CLI Privileges** 定義 **REST** 角色

由於 ONTAP 始終使用 CLI 命令來確定基礎層級的存取，因此可以使用 CLI 命令權限而不是 REST 端點來表示 REST 角色。這種方法的一個優點是傳統角色所提供的額外精細度。

定義 **ONTAP** 角色時的管理介面

您可以使用 ONTAP CLI 和 REST API 建立使用者和角色。但是，使用 System Manager 介面以及透過 ONTAP tools Manager 提供的 JSON 檔案會更方便。如需詳細資訊、請參閱 "將 ONTAP RBAC 與 ONTAP tools for VMware vSphere 10 搭配使用"。

ONTAP tools 的 ONTAP RBAC 注意事項

在正式作業環境中使用 ONTAP tools for VMware vSphere 10 與 ONTAP 的 RBAC 實作之前，您應該考慮幾個方面。

組態流程概述

ONTAP tools for VMware vSphere 支援建立具有自訂角色的 ONTAP 使用者。這些定義封裝在一個 JSON 檔案中，您可以將其上傳到 ONTAP 叢集。您可以建立使用者並根據您的環境和安全性需求自訂角色。

主要組態步驟的高階說明如下。如需更多詳細資訊，請參閱 "設定 ONTAP 使用者角色和 Privileges"。

1.準備

您需要擁有 ONTAP tools Manager 和 ONTAP 叢集的系統管理員憑證。

2.下載 **JSON** 定義檔案

登入 ONTAP tools Manager 使用者介面後，您可以下載包含 RBAC 定義的 JSON 檔案。

3.建立具有角色的 **ONTAP** 使用者

登入 System Manager 後，您可以建立使用者和角色：

1. 在左側選擇 **Cluster** ，然後選擇 **Settings** 。
2. 向下捲動至 **Users and roles**，然後按一下 -→。
3. 在 **Users** 下選擇 **Add**，然後選擇 **Virtualization products**。
4. 選擇本機工作站上的 JSON 檔案並上傳。

4.設定角色

作為角色定義的一部分，您需要做出幾個行政決策。如需詳細資訊，請參閱 使用 System Manager 設定角色。

使用 **System Manager** 設定角色

使用 System Manager 建立新使用者和角色並上傳 JSON 檔案後，您可以根據您的環境和需求自訂角色。

核心使用者和角色組態

RBAC 定義打包在多個產品功能中，包括 VSC、VASA Provider 和 SRA 的組合。您應該選擇需要 RBAC 支援的環境。例如，如果您希望角色支援遠端外掛功能，請選擇 VSC。您還需要選擇使用者名稱和關聯的密碼。

Privileges

根據 ONTAP 儲存所需的存取層級，角色 Privileges 分為四組。角色所依據的 Privileges 包括：

- 探索

  此角色可讓您新增儲存設備系統。

- 建立儲存設備

  此角色允許您建立儲存設備。它還包含與探索角色關聯的所有權限。

- 修改儲存設備

  此角色允許您修改儲存設備。它還包含與探索和建立儲存設備角色相關的所有權限。

- 毀損儲存設備

  此角色允許您毀損儲存設備。它還包含與探索、建立儲存設備和修改儲存設備角色相關的所有權限。

產生具有角色的使用者

選擇好環境的組態選項後，按一下 **Add**，ONTAP 將建立使用者和角色。產生的角色名稱是以下值的串連：

- JSON 檔案中定義的常數前綴值（例如 "OTV_10"）
- 您選擇的產品功能
- Privileges 集清單。

範例

```
OTV_10_VSC_Discovery_Create
```

新使用者將新增至「使用者與角色」頁面上的清單。請注意，HTTP 和 ONTAPI 使用者登入方法均受支援。