# 使用 ONTAP 的 RBAC

ONTAP tools for VMware vSphere 10

NetApp
September 29, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/ontap-tools-vmware-vsphere-10/concepts/rbac-ontap-environment.html on September 29, 2025. Always check docs.netapp.com for the latest.

# 目錄

使用 ONTAP 的 RBAC . . . 1
ONTAP RBAC 環境搭配適用於 VMware vSphere 10 的 ONTAP 工具 . . . 1
管理選項總覽 . . . 1
使用 ONTAP REST 角色 . . . 1
使用 ONTAP RBAC 搭配適用於 VMware vSphere 10 的 ONTAP 工具 . . . 2
組態程序總覽 . . . 2
使用 System Manager 設定角色 . . . 2

# 使用 ONTAP 的 RBAC

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

ONTAP 提供健全且可擴充的 RBAC 環境。您可以使用 RBAC 功能來控制透過 REST API 和 CLI 公開的儲存和系統作業存取。在使用 ONTAP 工具進行 VMware vSphere 10 部署之前，熟悉環境是很有幫助的。

### 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。下文概述主要的行政決策。如需詳細資訊，請參閱 "ONTAP 自動化： RBAC 安全性總覽"。

> ONTAP RBAC 針對儲存環境進行了客製化，並且比 vCenter Server 提供的 RBAC 實作更簡單。使用ONTAP，您可以直接向使用者指派角色。 ONTAP RBAC 不需要配置明確的權限（例如與 vCenter Server 一起使用的權限）。

角色類型和 **Privileges**

定義 ONTAP 使用者時，需要 ONTAP 角色。ONTAP 角色有兩種類型：

- 休息

  其餘角色是ONTAP 以32個9.6加入、一般適用於透過ONTAP REST API存取的使用者。這些角色中包含的 Privileges 是以存取 ONTAP REST API 端點和相關動作的方式來定義。

- 傳統

  以上是ONTAP 支援支援支援支援支援支援支援的舊角色。它們仍是 RBAC 的基礎層面。Privileges 是以存取 ONTAP CLI 命令的方式來定義。

雖然其餘角色最近才推出，但傳統角色卻有一些優點。例如，您可以選擇性地加入其他查詢參數，讓 Privileges 更精確地定義要套用的物件。

範圍

ONTAP 角色可以使用兩個不同範圍的其中一個來定義。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 層級提供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 工具 for VMware vSphere 10 隨附的 ONTAP REST 角色時，有幾個考量事項。

角色對應

無論是使用傳統或 REST 角色，所有 ONTAP 存取決策都是根據基礎 CLI 命令來決定。但由於靜態 Privileges

是以其餘 API 端點來定義，因此 ONTAP 需要為每個其餘角色建立一個 _ 對應 _ 傳統角色。因此，每個 REST 角色都會對應至底層的傳統角色。如此一來，無論角色類型為何， ONTAP 都能以一致的方式做出存取控制決策。您無法修改平行對應的角色。

#### 使用 **CLI Privileges** 定義 **REST** 角色

由於 ONTAP 一律使用 CLI 命令來判斷基礎層級的存取權限，因此可以使用 CLI 命令 Privileges 來表示 REST 角色，而非使用 REST 端點。這種方法的優點之一，就是傳統角色所能提供的額外精細度。

#### 定義 **ONTAP** 角色時的管理介面

您可以使用 ONTAP CLI 和 REST API 來建立使用者和角色。不過，使用系統管理員介面和 ONTAP 工具管理員提供的 JSON 檔案更為方便。如需詳細資訊、請參閱 "使用 ONTAP RBAC 搭配適用於 VMware vSphere 10 的 ONTAP 工具" 。

# 使用 **ONTAP RBAC** 搭配適用於 **VMware vSphere 10** 的 **ONTAP** 工具

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

## 組態程序總覽

ONTAP tools for VMware vSphere支援建立具有自訂角色的ONTAP使用者。這些定義打包在一個 JSON 檔案中，您可以將其上傳到ONTAP叢集。您可以根據您的環境和安全需求建立使用者並自訂角色。

主要組態步驟如下所述。如"設定 ONTAP 使用者角色和權限"需詳細資訊、請參閱。

#### **1.**準備

您必須同時擁有 ONTAP 工具管理員和 ONTAP 叢集的管理認證。

#### **2.**下載 **JSON** 定義檔案

登入 ONTAP Tools Manager 使用者介面之後，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 之後，您可以建立使用者和角色：

1. 選擇左側的 * 叢集 * ，然後選擇 * 設定 * 。
2. 向下捲動至 * 使用者與角色 * ，然後按一下 -→。
3. 在 * 使用者 * 下選取 * 新增 * ，然後選取 * 虛擬化產品 * 。
4. 選取本機工作站上的 JSON 檔案並上傳。

#### **4.**設定角色

在定義角色時，您必須做出數項管理決策。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

開始使用 System Manager 建立新的使用者和角色，並上傳 JSON 檔案之後，即可根據您的環境和需求自訂角色。

核心使用者和角色組態

RBAC 定義會封裝為多種產品功能，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，如果您想要角色支援遠端外掛程式功能，請選取 VSC 。您也需要選擇使用者名稱和相關密碼。

權限

角色 Privileges 會根據 ONTAP 儲存設備所需的存取層級，以四組形式排列。角色所依據的 Privileges 包括：

- 探索

  此角色可讓您新增儲存系統。

- 建立儲存設備

  此角色可讓您建立儲存設備。它也包含與探索角色相關的所有 Privileges 。

- 修改儲存設備

  此角色可讓您修改儲存設備。它也包含與探索相關的所有 Privileges ，並建立儲存角色。

- 銷毀儲存設備

  此角色可讓您銷毀儲存設備。它也包含與探索，建立儲存和修改儲存角色相關的所有 Privileges 。

產生具有角色的使用者

選取環境的組態選項之後，請按一下 * 新增 * ， ONTAP 便會建立使用者和角色。產生的角色名稱是下列值的串連：

- 在 JSON 檔案中定義的固定首碼值（例如「 OTV_10 」）
- 您選擇的產品功能
- 權限集清單。

範例

```
OTV_10_VSC_Discovery_Create
```

新使用者將新增至「使用者和角色」頁面上的清單。請注意， HTTP 和 ONTAPI 使用者登入方法都受到支援。

版權資訊

Copyright © 2025 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 保留隨時變更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。