



RBAC 與 ONTAP

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

This PDF was generated from <https://docs.netapp.com/zh-tw/ontap-tools-vmware-vsphere-105/concepts/rbac-ontap-environment.html> on July 24, 2026. Always check docs.netapp.com for the latest.

目錄

RBAC 與 ONTAP	1
ONTAP RBAC 如何與 ONTAP tools 協同工作	1
管理選項總覽	1
使用 ONTAP REST 角色	1
ONTAP tools 的 ONTAP RBAC 注意事項	2
組態流程概述	2
使用 System Manager 設定角色	2

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。

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。