RBAC 與 ONTAP

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

目錄

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

商標資訊