使用 **ONTAP** 的 **RBAC**

ONTAP tools for VMware vSphere 10

NetApp
November 17, 2025

目錄

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 是專為儲存環境量身打造，比 vCenter Server 隨附的 RBAC 實作更簡單。使用 ONTAP ，您可以直接指派角色給使用者。ONTAP RBAC 不需要設定明確的權限，例如與 vCenter Server 搭配使用的權限。

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

適用於 VMware vSphere 10 的 ONTAP 工具支援建立具有自訂角色的 ONTAP 使用者。這些定義會封裝在 JSON 檔案中，您可以將其上傳至 ONTAP 叢集。您可以建立使用者，並根據您的環境和安全需求量身打造角色。

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

商標資訊