基於角色的存取控制（RBAC）

ONTAP tools for VMware vSphere 10

NetApp
September 29, 2025

目錄

基於角色的存取控制（RBAC）

瞭解適用於 VMware vSphere 10 RBAC 的 ONTAP 工具

角色型存取控制（ RBAC ）是控制組織內資源存取的安全架構。RBAC 可定義具有特定權限層級的角色來執行動作，而非將授權指派給個別使用者，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。

RBAC 標準模式包含數種實作技術或複雜度增加的階段。結果是，根據軟體廠商及其客戶的需求，實際的 RBAC 部署可能會有所不同，而且範圍從相對簡單到非常複雜。

RBAC元件

在高層級上，每個 RBAC 實作通常都包含數個元件。在定義授權程序時，這些元件會以不同的方式結合在一起。

權限

特權是指可以允許或拒絕的操作或能力。它可能是簡單的操作，例如讀取檔案的能力，也可能是特定於特定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特權，也可能允許管理員建立自訂特權。

角色

role 是包含一或多個 Privileges 的容器。角色通常是根據特定工作或工作功能來定義。將角色指派給使用者時，會將角色中包含的所有 Privileges 授予使用者。與 Privileges 一樣，實作也包括預先定義的角色，通常允許建立自訂角色。

物件

object 代表在 RBAC 環境中識別的真實或抽象資源。透過 Privileges 定義的動作會在相關的物件上執行或與相關的物件一起執行。視實作而定， Privileges 可授予物件類型或特定物件執行個體。

使用者與群組

Users 會在驗證後指派或與套用的角色相關聯。某些 RBAC 實作只允許將一個角色指派給使用者，而其他角色則允許每個使用者擁有多個角色，可能一次只有一個角色處於作用中狀態。將角色指派給 *Groups* 可進一步簡化安全性管理。

權限

permission 是將使用者或群組與角色繫結至物件的定義。權限可用於階層式物件模型，階層中的子系可選擇性地繼承這些物件模型。

兩種 RBAC 環境

在使用適用於 VMware vSphere 10 的 ONTAP 工具時，您需要考量兩種不同的 RBAC 環境。

VMware vCenter Server

VMware vCenter Server 中的 RBAC 實作可用於限制存取透過 vSphere Client 使用者介面公開的物件。在安裝適用於 VMware vSphere 10 的 ONTAP 工具時， RBAC 環境會延伸至包含代表 ONTAP 工具功能的其他物件。這些物件的存取是透過遠端外掛程式提供。如需詳細資訊，請參閱"vCenter Server RBAC 環境"。

叢集ONTAP

適用於 VMware vSphere 10 的 ONTAP 工具會透過 ONTAP REST API 連線至 ONTAP 叢集，以執行與儲存相關的作業。存取儲存資源是透過與驗證期間提供的 ONTAP 使用者相關聯的 ONTAP 角色來控制。如需詳細資訊、請參閱 "ONTAP RBAC 環境" 。

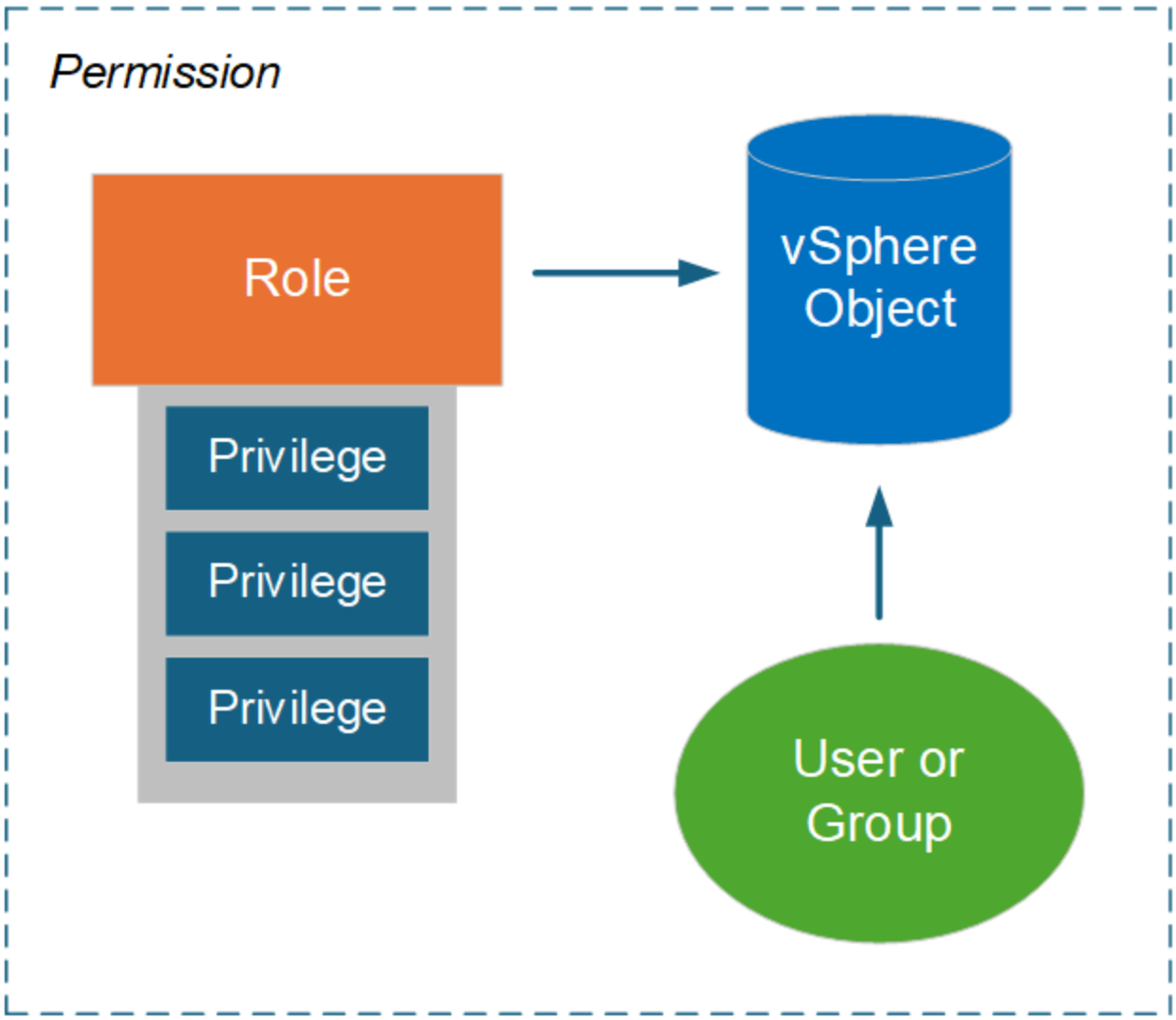
使用 VMware vSphere 的 RBAC

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

VMware vCenter Server 提供 RBAC 功能，可讓您控制對 vSphere 物件的存取。這是 vCenter 集中式驗證和授權安全服務的重要部分。

vCenter Server 權限的圖例

權限是在 vCenter Server 環境中強制執行存取控制的基礎。它會套用至具有權限定義所包含之使用者或群組的 vSphere 物件。下圖提供 vCenter 權限的高階圖例。



vCenter Server 權限的元件

vCenter Server 權限是一組包含多個元件的套件，這些元件會在建立權限時綁定在一起。

vSphere物件

權限會與 vSphere 物件相關聯，例如 vCenter Server ， ESXi 主機，虛擬機器，資料存放區，資料中心和資料夾。vCenter Server 會根據物件的指派權限，決定每個使用者或群組可以對物件執行哪些動作或工作。針對適用於 VMware vSphere 的 ONTAP 工具所特有的工作，所有權限都會在 vCenter Server 的根或根資料夾層級指派和驗證。如需詳細資訊、請參閱 "將 RBAC 搭配 vCenter 伺服器使用" 。

Privileges 和角色

ONTAP 工具適用於 VMware vSphere 10 的 vSphere Privileges 有兩種類型。為了簡化在此環境中使用 RBAC 的作業， ONTAP 工具提供包含所需原生和自訂 Privileges 的角色。Privileges 包括：

- 原生vCenter Server權限

  這些是 vCenter Server 提供的 Privileges 。

- ONTAP 工具專屬權限

  這些是專為 VMware vSphere ONTAP 工具所設計的自訂 Privileges 。

使用者與群組

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，您可以建立對 vSphere 物件層次結構中物件的權限。此權限根據關聯角色中的特權授予存取權限。請注意，角色並非直接指派給單獨使用者。相反，使用者和群組透過角色特權獲得對物件的存取權限，這是更大的 vCenter Server 權限的一部分。

使用 vCenter Server RBAC 搭配適用於 VMware vSphere 10 的 ONTAP 工具

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

vCenter 角色和管理員帳戶

如果您想要限制 vSphere 物件和相關管理工作的存取，只需定義和使用自訂 vCenter Server 角色。如果不需要限制存取，您可以改用系統管理員帳戶。每個系統管理員帳戶都是以物件階層最上層的系統管理員角色來定義。這可讓您完整存取 vSphere 物件，包括 ONTAP 工具為 VMware vSphere 10 新增的物件。

vSphere 物件階層架構

vSphere 物件詳細目錄是以階層架構來組織。例如，您可以依照下列方式向下移動階層：

```
vCenter Server--> --> --> --> Datacenter --> Cluster --> --> ESXi host Virtual Machine
```

所有權限都會在 vSphere 物件階層中驗證，但 VAAI 外掛程式作業除外，這些作業會針對目標 ESXi 主機進行驗證。

適用於 **VMware vSphere 10** 的 **ONTAP** 工具隨附的角色

為了簡化使用 vCenter Server RBAC 的過程，適用於 VMware vSphere 的 ONTAP 工具可針對各種管理工作提供預先定義的角色。

> 您可以視需要建立新的自訂角色。在這種情況下，您應該複製其中一個現有的 ONTAP 工具角色，並視需要進行編輯。變更組態後，受影響的 vSphere 用戶端使用者必須登出並重新登入，才能啟動變更。

若要檢視適用於 VMware vSphere 角色的 ONTAP 工具，請選取 vSphere Client 頂端的 * 功能表 * ，然後按一下 * 管理 * ，然後按一下左側的 * 角色 * 。有三種預先定義的角色，如下所述。

適用於 **VMware vSphere** 管理員的 **NetApp ONTAP** 工具

提供執行核心 ONTAP 工具以執行 VMware vSphere 管理員工作所需的所有原生 vCenter Server Privileges 和 ONTAP 工具專屬 Privileges 。

適用於 **VMware vSphere** 的 **NetApp ONTAP** 工具唯讀

提供 ONTAP 工具的唯讀存取權。這些使用者無法針對存取控制的 VMware vSphere 動作執行任何 ONTAP 工具。

VMware vSphere 佈建的 **NetApp ONTAP** 工具

提供部分原生 vCenter Server 權限和 ONTAP 工具專屬權限、這些權限是配置儲存設備所需的。您可以執行下列工作：

- 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

這兩種 RBAC 環境可一起運作。在 vSphere 用戶端介面中執行工作時，會先檢查定義至 vCenter Server 的 ONTAP 工具角色。如果 vSphere 允許此作業，則會檢查 ONTAP 角色 Privileges 。第二個步驟是根據建立及設定儲存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 Privileges 和權限時，需要考量一些事項。

必要權限

若要存取適用於 VMware vSphere 10 使用者介面的 ONTAP 工具，您必須擁有 ONTAP 工具專屬的 _ 檢視 _ 權限。如果您在沒有此權限的情況下登入 vSphere ，並按一下 NetApp 圖示，適用於 VMware vSphere 的 ONTAP 工具會顯示錯誤訊息，並阻止您存取使用者介面。

vSphere 物件階層中的指派層級會決定您可以存取的使用者介面部分。將檢視權限指派給根物件可讓您按一下 NetApp 圖示來存取適用於 VMware vSphere 的 ONTAP 工具。

您可以將檢視權限指派給另一個較低的 vSphere 物件層級。不過，這會限制您可以存取和使用的 VMware vSphere ONTAP 工具功能表。

指派權限

如果您想要限制 vSphere 物件和工作的存取，則需要使用 vCenter Server 權限。在 vSphere 物件階層中指派權限的位置，決定使用者可以執行的 VMware vSphere 10 工作的 ONTAP 工具。

除非您需要定義更嚴格的存取，否則在根物件或根資料夾層級指派權限通常是個不錯的做法。

適用於 VMware vSphere 10 的 ONTAP 工具所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 VMware vSphere 根物件的 ONTAP 工具，因為沒有您可以指派的 vSphere 物件。例如，任何包含適用於 VMware vSphere 「新增 / 修改 / 移除儲存系統」權限的 ONTAP 工具權限，都應在根物件層級指派。

在物件階層中定義較高層級的權限時，您可以設定權限，讓子物件向下傳遞並繼承權限。如果需要，您可以指派額外權限給子物件，這些子物件會覆寫從父物件繼承的權限。

您可以隨時修改權限。如果您在權限內變更任何 Privileges ，則與權限相關的使用者必須登出 vSphere ，然後重新登入才能啟用變更。

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

商標資訊