基於角色的存取控制

ONTAP tools for VMware vSphere 10

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/ontap-tools-vmware-vsphere-104/concepts/rbac-learn-about.html on November 04, 2025. Always check docs.netapp.com for the latest.

目錄

基於角色的存取控制 1
了解適用於ONTAP tools for VMware vSphere 1
RBAC 組件 1
兩個 RBAC 環境 1
VMware vSphere 的 RBAC 2
ONTAP tools for VMware vSphere的 vCenter Server RBAC 環境 2
將 vCenter Server RBAC 與ONTAP tools for VMware vSphere結合使用 3
使用ONTAP的 RBAC 5
適用於ONTAP tools for VMware vSphere的ONTAP RBAC 環境 5
將ONTAP RBAC 與ONTAP tools for VMware vSphere結合使用 6

基於角色的存取控制

了解適用於ONTAP tools for VMware vSphere

基於角色的存取控制 (RBAC) 是用於控制組織內資源存取的安全框架。 RBAC 透過定義具有特定權限等級的角色來執行操作，而不是將授權指派給單一用戶，從而簡化了管理。將定義的角色指派給用戶，這有助於降低錯誤風險並簡化整個組織的存取控制管理。

RBAC標準模型由幾種複雜度不斷增加的實現技術或階段組成。結果是，根據軟體供應商及其客戶的需求，實際的 RBAC 部署可能會有所不同，範圍從相對簡單到非常複雜。

RBAC 組件

從高層次來看，每個 RBAC 實作通常包含幾個元件。作為定義授權流程的一部分，這些元件以不同的方式綁定在一起。

Privileges

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

_角色_是包含一個或多個權限的容器。角色通常根據特定任務或工作職能來定義。當將角色指派給使用者時，該使用者被授予該角色包含的所有權限。與特權一樣，實作包括預先定義的角色，並且通常允許創建自訂角色。

物件

_物件_代表在 RBAC 環境中識別的真實或抽象資源。透過權限定義的操作在相關物件上或透過相關物件執行。根據實作情況，可以將特權授予物件類型或特定物件實例。

使用者和群組

_使用者_被指派或與身分驗證後所應用的角色相關聯。有些 RBAC 實作只允許為一個使用者指派一個角色，而其他實作則允許每個使用者擁有多個角色，並且可能一次只啟動一個角色。將角色指派給_組_可以進一步簡化安全管理。

權限

permission 是將使用者或群組與角色綁定到物件的定義。權限對於分層物件模型很有用，其中權限可以選擇由層次結構中的子項繼承。

兩個 RBAC 環境

使用適用於ONTAP tools for VMware vSphere時，需要考慮兩種不同的 RBAC 環境。

VMware vCenter 伺服器

VMware vCenter Server 中的 RBAC 實作用於限制透過 vSphere Client 使用者介面公開的物件的存取。作為為ONTAP tools for VMware vSphere的一部分，RBAC 環境已擴展，以包含其他代表ONTAP工具功能的物件。透過遠端插件可以存取這些物件。請參閱"vCenter Server RBAC 環境"了解更多。

ONTAP叢集

ONTAP tools for VMware vSphere透過ONTAP REST API 連接到ONTAP叢集以執行與儲存相關的操作。對儲存資源的存取是透過與身份驗證期間提供的ONTAP用戶關聯的ONTAP角色來控制的。看"ONTAP RBAC 環境"了解更多。

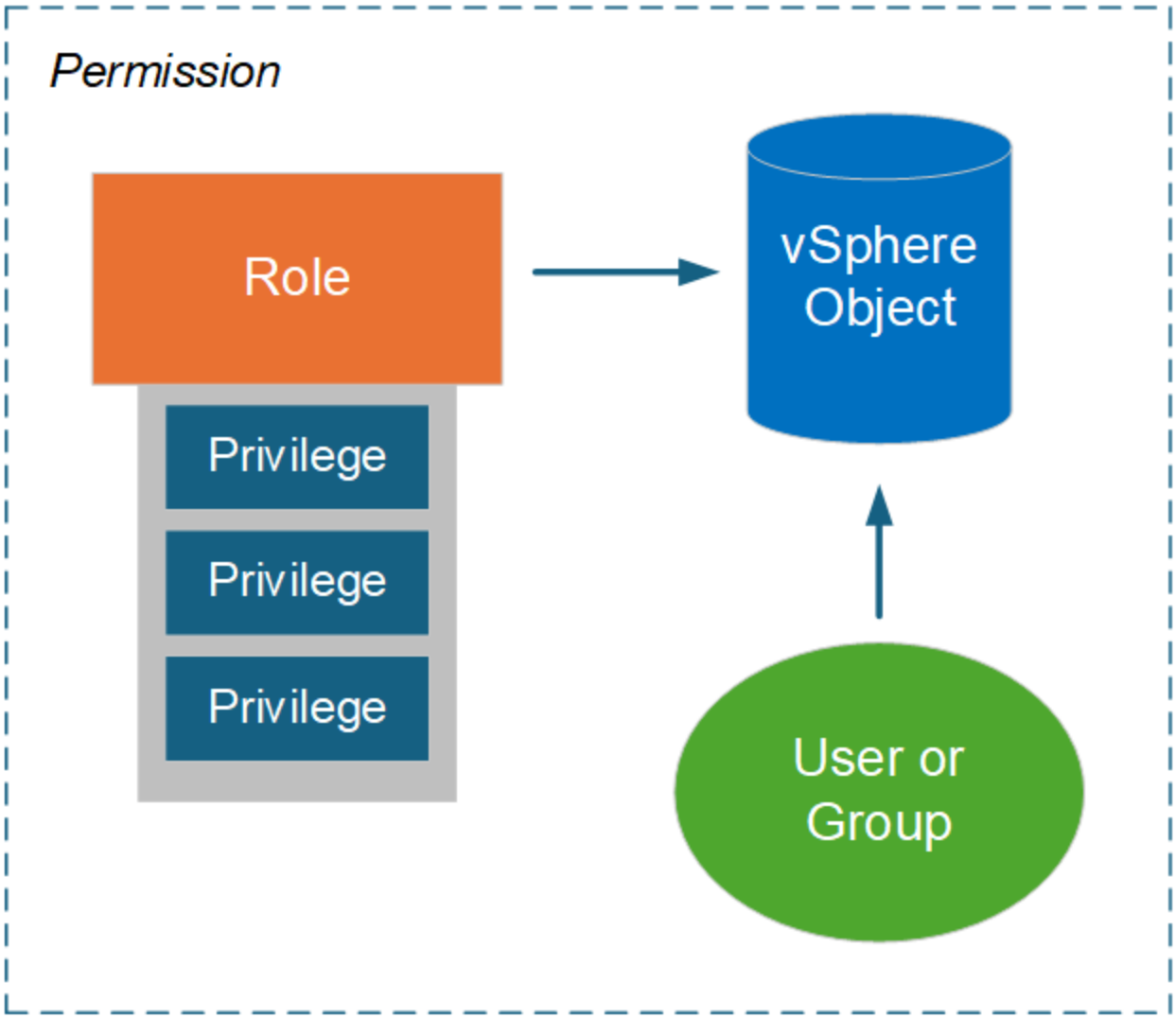
VMware vSphere 的 RBAC

ONTAP tools for VMware vSphere的 vCenter Server RBAC 環境

VMware vCenter Server 提供了 RBAC 功能，讓您能夠控制對 vSphere 物件的存取。它是vCenter集中身份驗證和授權安全服務的重要組成部分。

vCenter Server 權限的圖示

權限是 vCenter Server 環境中強制執行存取控制的基礎。它適用於具有權限定義中包含的使用者或群組的 vSphere 物件。下圖提供了 vCenter 權限的進階說明。



vCenter Server 權限的組成部分

vCenter Server 權限是建立權限時綁定在一起的幾個元件的套件。

vSphere 對象

權限與 vSphere 物件相關聯，例如 vCenter Server、ESXi 主機、虛擬機器、資料儲存區、資料中心和資料夾。根據物件指派的權限，vCenter Server 決定每個使用者或群組可以對該物件執行哪些操作或任務。對於特定於ONTAP tools for VMware vSphere的任務，所有權限均在 vCenter Server 的根或根資料夾層級指派和驗證。看"將 RBAC 與 vCenter 伺服器結合使用"了解更多。

Privileges和角色

適用於ONTAP tools for VMware vSphere使用兩種類型的 vSphere 權限。為了簡化在此環境中使用 RBAC 的工作， ONTAP工具提供了包含所需的本機和自訂權限的角色。特權包括：

- 本機 vCenter Server 權限

  這些是 vCenter Server 提供的權限。

- ONTAP工具特定的權限

  這些是適用於ONTAP tools for VMware vSphere獨有的自訂權限。

使用者和群組

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。

將 vCenter Server RBAC 與ONTAP tools for VMware vSphere結合使用

在生產環境中使用適用於ONTAP tools for VMware vSphere之前，您應該考慮它的幾個面向。

vCenter 角色和管理員帳戶

如果您想要限制對 vSphere 物件和相關管理任務的訪問，則只需定義和使用自訂 vCenter Server 角色。如果不需要限制訪問，您可以改用管理員帳戶。每個管理員帳戶都定義為位於物件層次結構頂層的管理員角色。這提供了對 vSphere 物件的完全存取權限，包括由ONTAP tools for VMware vSphere 10 新增的物件。

vSphere 物件層次結構

vSphere 物件清單依層次結構組織。例如，您可以如下向下移動層次結構：

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

除 VAAI 插件操作外，所有權限均在 vSphere 物件層次結構中驗證，VAAI 插件操作則針對目標 ESXi 主機進行驗證。

ONTAP tools for VMware vSphere中所包含的角色

為了簡化使用 vCenter Server RBAC 的工作，ONTAP tools for VMware vSphere提供了針對各種管理任務自訂的預先定義角色。

> 如果需要，您可以建立新的自訂角色。在這種情況下，您應該複製現有的ONTAP工具角色之一並根據需要進行編輯。進行設定變更後，受影響的 vSphere 用戶端使用者需要登出並重新登入才能啟動變更。

若要查看ONTAP tools for VMware vSphere，請選擇 vSphere Client 頂部的“選單”，然後按一下左側的“管理”和“角色”。有三個預先定義的角色，如下所述。

適用於 VMware vSphere 管理員的NetApp ONTAP tools for VMware vSphere

提供執行ONTAP tools for VMware vSphere管理員任務所需的所有本機 vCenter Server 權限和ONTAP工具特定權限。

ONTAP tools for VMware vSphere唯讀的NetApp ONTAP 工具

提供對ONTAP工具的唯讀存取權限。這些使用者無法執行任何受存取控制的ONTAP tools for VMware vSphere操作。

適用於 VMware vSphere Provision 的NetApp ONTAP tools for VMware vSphere

提供配置儲存所需的一些本機 vCenter Server 權限和ONTAP工具特定的權限。您可以執行以下任務：

- 建立新的資料存儲
- 管理資料儲存區

vSphere 物件和ONTAP儲存後端

兩個 RBAC 環境協同工作。在 vSphere 用戶端介面中執行任務時，首先檢查定義到 vCenter Server 的ONTAP工具角色。如果 vSphere 允許該操作，則檢查ONTAP角色權限。第二步是根據建立和配置儲存後端時分配給使用者的ONTAP角色執行的。

使用 vCenter Server RBAC

使用 vCenter Server 特權和權限時需要考慮一些事項。

所需權限

若要存取適用ONTAP tools for VMware vSphere，您需要擁有特定於ONTAP工具的 *View* 權限。如果您在沒有此權限的情況下登入 vSphere 並點擊NetApp圖標，則ONTAP tools for VMware vSphere將顯示錯誤訊息並阻止您存取使用者介面。

vSphere 物件層次結構中的指派層級決定了您可以存取使用者介面的哪些部分。將檢視權限指派給根物件後，您可以透過點選NetApp圖示來存取適用ONTAP tools for VMware vSphere。

您可以將檢視權限指派給另一個較低的 vSphere 物件等級。但是，這將限制您可以存取和使用的ONTAP tools for VMware vSphere。

分配權限

如果您想要限制對 vSphere 物件和任務的訪問，則需要使用 vCenter Server 權限。您在 vSphere 物件層次結構

中指派權限的位置決定了使用者可以執行的ONTAP tools for VMware vSphere。

> 除非您需要定義更嚴格的存取權限，否則在根物件或根資料夾層級分配權限通常是一種很好的做法。

ONTAP tools for VMware vSphere提供的權限適用於自訂非 vSphere 對象，例如儲存系統。如果可能，您應該將這些權限指派給ONTAP tools for VMware vSphere，因為沒有可以將其指派給的 vSphere 物件。例如，任何包含適用ONTAP tools for VMware vSphere「新增/修改/刪除儲存系統」權限的權限都應在根物件層級指派。

當在物件層次結構的較高層級定義權限時，您可以配置該權限，以便它被傳遞並由子物件繼承。如果需要，您可以為子物件指派額外的權限，以覆寫從父物件繼承的權限。

您可以隨時修改權限。如果您變更權限中的任何特權，則與該權限關聯的使用者需要登出 vSphere 並重新登入以啟用變更。

使用ONTAP的 RBAC

適用於ONTAP tools for VMware vSphere的ONTAP RBAC 環境

ONTAP提供了強大且可擴展的 RBAC 環境。您可以使用 RBAC 功能來控制透過 REST API 和 CLI 公開的儲存和系統操作的存取。在使用ONTAP tools for VMware vSphere 10 部署之前，熟悉環境會很有幫助。

管理選項概述

根據您的環境和目標，使用ONTAP RBAC 時有多種可用選項。以下是主要行政決定的概述。另請參閱 "ONTAP 自動化：RBAC 安全概述"了解更多。

> 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（例如用於 vCenter Server 的權限）。

角色和權限的類型

定義ONTAP使用者時需要ONTAP角色。 ONTAP角色有兩種類型：

- 休息

  REST 角色是在ONTAP 9.6 中引入的，通常適用於透過 REST API 存取ONTAP 的使用者。這些角色中所包含的權限是根據對ONTAP REST API 端點的存取及其相關操作來定義的。

- 傳統的

  這些是ONTAP 9.6 之前包含的舊角色。它們仍然是 RBAC 的基礎面向。權限是根據對ONTAP CLI 命令的存取來定義的。

雖然 REST 角色是最近才引入的，但傳統角色也具有一些優勢。例如，可以選擇包含附加查詢參數，以便權限更精確地定義它們所套用的物件。

範圍

ONTAP角色可以透過兩種不同的範圍之一來定義。它們可以應用於特定資料 SVM（SVM 層級）或整個ONTAP叢集（叢集層級）。

角色定義

ONTAP在叢集和 SVM 層級提供了一組預定義角色。您也可以定義自訂角色。

使用**ONTAP REST** 角色

使用ONTAP tools for VMware vSphere隨附的ONTAP REST 角色時需要考慮幾個事項。

角色映射

無論使用傳統角色還是 REST 角色，所有ONTAP存取決策都是基於底層 CLI 命令做出的。但由於 REST 角色中的權限是根據 REST API 端點定義的，因此ONTAP需要為每個 REST 角色建立一個_映射_傳統角色。因此，每個 REST 角色都映射到一個底層傳統角色。這使得ONTAP能夠以一致的方式做出存取控制決策，而不管角色類型如何。您不能修改並行映射的角色。

使用 **CLI** 權限定義 **REST** 角色

由於ONTAP始終使用 CLI 命令來確定基本層級的存取權限，因此可以使用 CLI 命令權限而不是 REST 端點來表達 REST 角色。這種方法的一個好處是可以比傳統角色提供更多的粒度。

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，使用系統管理器介面以及透過ONTAP工具管理器提供的 JSON 檔案會更方便。看"將ONTAP RBAC 與ONTAP tools for VMware vSphere結合使用"了解更多。

將**ONTAP RBAC** 與**ONTAP tools for VMware vSphere**結合使用

在生產環境中使用ONTAPONTAP tools for VMware vSphere 10 RBAC 實作之前，您應該考慮幾個面向。

配置流程概述

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。

下面詳細描述了主要的設定步驟。參考"配置ONTAP用戶角色和權限"了解更多詳情。

1.準備

您需要擁有ONTAP工具管理器和ONTAP叢集的管理憑證。

2.下載 **JSON** 定義文件

登入ONTAP工具管理器使用者介面後，您可以下載包含 RBAC 定義的 JSON 檔案。

3.建立具有角色的**ONTAP**用戶

登入系統管理員後，您可以建立使用者和角色：

1. 選擇左側的“**Cluster**”，然後選擇“**Settings**”。
2. 向下捲動到*使用者和角色*並點擊 –→。
3. 選擇*使用者*下的*新增*，然後選擇*虛擬化產品*。

4. 在本機工作站上選擇 JSON 檔案並上傳。

4.配置角色

作為定義角色的一部分，您需要做出幾個管理決策。看[使用系統管理員配置角色]了解更多詳情。

使用系統管理員配置角色

在您開始使用系統管理員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。

核心使用者和角色配置

RBAC 定義被打包為多種產品功能，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相關密碼。

Privileges

根據對ONTAP儲存所需的存取級別，角色權限分為四組。角色所基於的權限包括：

- 發現

  此角色使您能夠新增儲存系統。

- 建立儲存

  此角色使您能夠建立儲存空間。它還包括與發現角色相關的所有特權。

- 修改儲存

  此角色使您能夠修改儲存空間。它還包括與發現和創建儲存角色相關的所有權限。

- 銷毀存儲

  此角色使您能夠銷毀儲存空間。它還包括與發現、建立儲存和修改儲存角色相關的所有權限。

產生具有角色的用戶

為您的環境選擇配置選項後，按一下“新增”， ONTAP將建立使用者和角色。產生的角色的名稱是以下值的組合：

- JSON 檔案中定義的常數前綴值（例如“OTV_10”）
- 您選擇的產品功能
- 權限集列表。

例子

```
OTV_10_VSC_Discovery_Create
```

新用戶將被加入到「用戶和角色」頁面的清單中。請注意，HTTP 和 ONTAPI 使用者登入方法均受支援。

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。