角色型存取控制

ONTAP tools for VMware vSphere 10

NetApp
September 30, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/ontap-tools-vmware-vsphere-102/concepts/vcenter-server-role-based-access-control-features.html on September 30, 2025. Always check docs.netapp.com for the latest.

目錄

角色型存取控制 1
VMware vSphere ONTAP 工具中角色型存取控制概觀 1
有關指派和修改 vCenter Server 角色的重點 1
適用於 VMware vSphere 的 ONTAP 工具隨附的標準角色 1
ONTAP 儲存設備後端和 vSphere 物件的權限 2
vCenter Server權限的元件 2
權限 3
vSphere物件 3
使用者與群組 4
指派和修改 vCenter Server 的權限 4
指派權限 4
權限與非vSphere物件 4
修改權限 4
VMware vSphere 工作所需的 ONTAP 工具權限 5
VMware vSphere ONTAP 工具的建議 ONTAP 角色 5

角色型存取控制

VMware vSphere ONTAP 工具中角色型存取控制概觀

vCenter Server 提供角色型存取控制（RBAC）功能、可讓您控制對 vSphere 物件的存取。 vCenter Server 使用角色和 Privileges 的使用者和群組權限、在其資源清冊中提供多個不同層級的集中式驗證和授權服務。 vCenter Server 具備五個主要元件、可用於管理 RBAC ：

元件	說明
權限	權限可啟用或拒絕在 vSphere 中執行動作的存取。
角色	角色包含一或多個系統權限、其中每個權限都會定義系統中特定物件或物件類型的管理權限。透過指派使用者角色、使用者將繼承該角色中定義之權限的功能。
使用者與群組	使用者和群組可在權限中使用、從 Active Directory （AD）指派角色。 vCenter Server 有自己的本機使用者和群組、您可以使用這些使用者和群組。
權限	權限可讓您將 Privileges 指派給使用者或群組、以執行特定動作並變更 vCenter Server 內部的物件。 vCenter Server 權限僅會影響登入 vCenter Server 的使用者、而不會影響直接登入 ESXi 主機的使用者。
物件	執行動作的實體。VMware vCenter 物件包括資料中心、資料夾、資源池、叢集、主機、 和 VM

若要成功完成工作、您應該擁有適當的 vCenter Server RBAC 角色。在工作期間、 ONTAP Tools for VMware vSphere 會先檢查使用者的 vCenter Server 角色、然後再檢查使用者的 ONTAP 權限。

> vCenter Server 角色適用於適用於 VMware vSphere vCenter 使用者的 ONTAP 工具、而非系統管理員。依預設、系統管理員擁有產品的完整存取權、不需要指派角色給他們。

使用者和群組可以成為 vCenter Server 角色的一部分、藉此存取角色。

有關指派和修改 vCenter Server 角色的重點

如果您想限制 vSphere 物件和工作的存取、只需要設定 vCenter Server 角色。否則、您可以以系統管理員的身分登入。此登入可讓您自動存取所有vSphere物件。

指派角色的位置決定使用者可執行的 VMware vSphere 工作之 ONTAP 工具。您可以隨時修改一個角色。如果您變更角色內的權限、則與該角色相關聯的使用者應登出、然後重新登入以啟用更新的角色。

適用於 VMware vSphere 的 ONTAP 工具隨附的標準角色

為了簡化使用 vCenter Server 權限和 RBAC 的過程、適用於 VMware vSphere 的 ONTAP 工具提供適用於 VMware vSphere 角色的標準 ONTAP 工具、可讓您針對 VMware vSphere 工作執行重要的 ONTAP 工具。還有一個唯讀角色、可讓您檢視資訊、但不執行任何工作。

您可以按一下 vSphere Client 首頁上的 * 角色 * 、檢視適用於 VMware vSphere 標準角色的 ONTAP 工具。ONTAP 工具 for VMware vSphere 提供的角色可讓您執行下列工作：

角色	說明
適用於 VMware vSphere 管理員的 NetApp ONTAP 工具	提供執行部分 ONTAP 工具以執行 VMware vSphere 工作所需的所有原生 vCenter Server 權限和 ONTAP 工具專屬權限。
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

ONTAP tools Manager 管理員角色未在 vCenter Server 中登錄。此職務專屬於 ONTAP 工具經理。

如果貴公司要求您實作的角色比 VMware vSphere 角色的標準 ONTAP 工具更具限制性、您可以使用適用於 VMware vSphere 角色的 ONTAP 工具來建立新角色。

在這種情況下、您將會複製 VMware vSphere 角色所需的 ONTAP 工具、然後編輯複製的角色、使其僅擁有使用者所需的權限。

ONTAP 儲存設備後端和 vSphere 物件的權限

如果 vCenter Server 權限足夠、則適用於 VMware vSphere 的 ONTAP 工具會檢查與儲存設備後端認證（使用者名稱和密碼）相關聯的 ONTAP RBAC 權限（您的 ONTAP 角色）。 判斷您是否有足夠權限在該儲存後端執行 ONTAP 工具 for VMware vSphere 工作所需的儲存作業。如果您擁有正確的 ONTAP Privileges 、您可以存取儲存設備後端、並執行 ONTAP 工具來執行 VMware vSphere 工作。ONTAP 角色可決定可在儲存後端執行的 VMware vSphere 工作的 ONTAP 工具。

vCenter Server權限的元件

vCenter Server可辨識權限、而非權限。每個vCenter Server權限均由三個元件組成。

vCenter Server具有下列元件：

- 一或多個權限（角色）

  權限定義使用者可以執行的工作。

- vSphere物件

  物件是工作的目標。

- 使用者或群組

使用者或群組會定義可以執行工作的人員。

> 在此圖中、灰色方塊表示vCenter Server中存在的元件、而白色方塊則表示vCenter Server執行所在作業系統中存在的元件。

權限

VMware vSphere的VMware vSphere的VMware VMware工具有兩種權限：ONTAP

- 原生vCenter Server權限

  這些權限隨附於vCenter Server。

- ONTAP 工具專屬權限

  這些權限是針對 VMware vSphere 工作的特定 ONTAP 工具所定義。這些工具是專為 VMware vSphere 所設計的 ONTAP 工具。

適用於 VMware vSphere 工作的 ONTAP 工具需要 ONTAP 工具專屬權限和 vCenter Server 原生權限。這些權限構成使用者的「角色」。權限可以有多個權限。這些權限適用於登入vCenter Server的使用者。

> 為了簡化 vCenter Server RBAC 的使用、適用於 VMware vSphere 的 ONTAP 工具提供數種標準角色、其中包含執行 ONTAP 工具以執行 VMware vSphere 工作所需的所有 ONTAP 工具專屬和原生權限。

如果您變更權限內的權限、則與該權限相關的使用者應登出、然後登入以啟用更新的權限。

vSphere物件

權限與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。您可以將權限指派給任何vSphere物件。vCenter Server會根據指派給vSphere物件的權限、決定誰可以在該物件上執行哪些工作。針對 VMware vSphere 特定工作的 ONTAP 工具、權限只會在根資料夾層級（vCenter Server）指派和驗證、而不會在任何其他實體上指派和驗證。除了 VAAI 外掛程式作業、此作業會針對相關的 ESXi 主機驗證權限。

使用者與群組

您可以使用Active Directory（或本機vCenter Server機器）來設定使用者和使用者群組。接著您可以使用 vCenter Server 權限、將存取權授予這些使用者或群組、讓他們能夠針對 VMware vSphere 工作執行特定的 ONTAP 工具。

> 這些 vCenter Server 權限適用於適用於 VMware vSphere vCenter 使用者的 ONTAP 工具、而非適用於 VMware vSphere 管理員的 ONTAP 工具。根據預設、適用於 VMware vSphere 管理員的 ONTAP 工具具有產品的完整存取權、不需要指派權限給他們。

使用者和群組並未指派角色給他們。他們可透過vCenter Server權限的一部分來存取角色。

指派和修改 vCenter Server 的權限

使用vCenter Server權限時、請謹記幾個重點。VMware vSphere工作的VMware選用功能是否成功、取決於您指派權限的位置、或使用者在修改權限後採取的行動。ONTAP

指派權限

如果您只想限制對vSphere物件和工作的存取、則只需要設定vCenter Server權限。否則、您可以以系統管理員的身分登入。此登入可讓您自動存取所有vSphere物件。

指派權限的位置決定使用者可執行的 VMware vSphere 工作之 ONTAP 工具。

有時候、為了確保工作完成、您應該指派較高層級的權限、例如根物件。當工作需要不適用於特定vSphere物件的權限（例如追蹤工作）、或是需要的權限套用至非vSphere物件（例如儲存系統）時、就會發生這種情況。

在這些情況下、您可以設定權限、讓子實體繼承權限。您也可以將其他權限指派給子實體。指派給子實體的權限一律會覆寫繼承自父實體的權限。這表示您可以授予子實體權限、以限制指派給根物件且由子實體繼承的權限範圍。

> 除非貴公司的安全性原則需要更嚴格的權限、否則指派權限給根物件（也稱為根資料夾）是很好的做法。

權限與非vSphere物件

您建立的權限會套用至非 vSphere 物件。例如、儲存系統不是vSphere物件。如果權限套用至儲存系統、您應該將包含該權限的權限指派給 VMware vSphere 根物件的 ONTAP 工具、因為沒有 vSphere 物件可供您指派。

例如、任何包含 VMware vSphere 權限的 ONTAP 工具等權限「新增 / 修改 / 略過儲存系統」的權限、都應該指派給根物件層級。

修改權限

您可以隨時修改一個權限。

如果您變更權限內的權限、則與該權限相關的使用者應登出、然後重新登入以啟用更新的權限。

VMware vSphere 工作所需的 ONTAP 工具權限

針對 VMware vSphere 工作的不同 ONTAP 工具需要不同的權限組合、這些權限是專為 VMware vSphere 的 ONTAP 工具和原生 vCenter Server 權限而設計。

若要存取適用於 VMware vSphere GUI 的 ONTAP 工具、您應該在正確的 vSphere 物件層級指派產品層級的 ONTAP 工具專屬檢視權限。如果您沒有此權限登入、則當您按一下 NetApp 圖示時、適用於 VMware vSphere 的 ONTAP 工具會顯示錯誤訊息、並阻止您存取 ONTAP 工具。

在 * 檢視 * 權限中、您可以存取適用於 VMware vSphere 的 ONTAP 工具。此權限無法讓您在 VMware vSphere 的 ONTAP 工具中執行工作。若要針對 VMware vSphere 工作執行任何 ONTAP 工具、您應該擁有適用於這些工作的正確 ONTAP 工具專屬和原生 vCenter Server 權限。

指派層級決定您可以看到的UI部分。將檢視權限指派給根物件（資料夾）可讓您按一下 NetApp 圖示、輸入適用於 VMware vSphere 的 ONTAP 工具。

您可以將「檢視」權限指派給其他 vSphere 物件層級、但這麼做會限制您可以查看和使用的 VMware vSphere ONTAP 工具功能表。

根物件是指派任何包含檢視權限的權限的建議位置。

VMware vSphere ONTAP 工具的建議 ONTAP 角色

您可以設定數ONTAP 個建議的VMware vCenter角色、以搭配ONTAP VMware vSphere 的VMware VMware vCenter及角色型存取控制（RBAC）等各種功能。這些角色包含執行 ONTAP 工具執行 VMware vSphere 工作所需的 ONTAP 權限。

若要建立新的使用者角色、您應該以執行 ONTAP 的儲存系統管理員身分登入。您可以使用 ONTAP 系統管理員 9.8P1 或更新版本來建立 ONTAP 角色。

每個 ONTAP 角色都有相關的使用者名稱和密碼配對、構成角色的認證。如果您未使用這些認證登入、則無法存取與該角色相關的儲存作業。

為了安全起見、 VMware vSphere 特定 ONTAP 角色的 ONTAP 工具會以階層順序排列。這表示第一個角色的限制性最大、而且只有與 VMware vSphere 儲存作業最基本的 ONTAP 工具集相關的權限。下一個角色包括其本身的權限、以及與前一個角色相關的所有權限。對於支援的儲存作業、每個額外角色的限制都較少。

以下是在 VMware vSphere 中使用 ONTAP 工具時、建議使用的一些 ONTAP RBAC 角色。建立這些角色之後、您可以將其指派給必須執行儲存相關工作的使用者、例如資源配置虛擬機器。

角色	* 權限 *
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。此角色也包含與探索角色相關聯的所有權限。
修改儲存設備	此角色可讓您修改儲存設備。此角色也包含與探索角色和建立儲存角色相關聯的所有權限。
摧毀儲存設備	此角色可讓您銷毀儲存設備。此角色也包含與探索角色、建立儲存角色及修改儲存角色相關的所有權限。

如果您使用適用於 VMware vSphere 的 ONTAP 工具、也應該設定原則型管理（ PBM ）角色。此角色可讓您使用儲存原則來管理儲存設備。這項職務要求您也必須設定「探索」角色。

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。