



# 以角色為基礎的存取控制 (RBAC) SnapCenter

SnapCenter Software 5.0

NetApp  
July 18, 2024

# 目錄

以角色為基礎的存取控制 (RBAC) SnapCenter .....	1
RBAC類型 .....	1
RBAC權限和角色 .....	2
預先定義SnapCenter 的功能和權限 .....	4

# 以角色為基礎的存取控制（RBAC） SnapCenter

## RBAC類型

以角色為基礎的存取控制（RBAC）和權限功能可讓管理員將對各種資源的控制權委派給不同的使用者或使用者群組。SnapCenter ONTAP SnapCenter SnapCenter這項集中管理的存取功能可讓應用程式管理員在委派的環境中安全地工作。

您可以隨時建立及修改角色、並新增資源存取權限給使用者、但SnapCenter 第一次設定時、您至少應該將Active Directory使用者或群組新增至角色、然後將資源存取權限新增至這些使用者或群組。



您無法使用SnapCenter 無法建立使用者或群組帳戶。您應該在作業系統或資料庫的Active Directory中建立使用者或群組帳戶。

使用下列類型的角色型存取控制：SnapCenter

- RBAC SnapCenter
- 列舉RBAC外掛程式（適用於部分外掛程式） SnapCenter
- 應用程式層級RBAC
- 權限ONTAP

## RBAC SnapCenter

### 角色與權限

隨附預先定義且已指派權限的角色。SnapCenter您可以將使用者或使用者群組指派給這些角色。您也可以建立新角色、並管理權限和使用者。

### 指派權限給使用者或群組

您可以指派權限給使用者或群組、以存取SnapCenter 諸如主機、儲存連線和資源群組等物件。您無法變更SnapCenterAdmin角色的權限。

您可以將RBAC權限指派給同一個樹系中的使用者和群組、以及屬於不同樹系的使用者。您無法將RBAC權限指派給跨樹系屬於巢狀群組的使用者。



如果您建立自訂角色、則必須包含SnapCenter 所有的「管理員」角色權限。如果您只複製部分權限、例如「主機新增」或「主機移除」、就無法執行這些作業。

### 驗證

使用者必須在登入期間、透過圖形使用者介面（GUI）或使用PowerShell Cmdlet來提供驗證。如果使用者是多個角色的成員、則在輸入登入認證之後、系統會提示使用者指定想要使用的角色。使用者也必須提供驗證、才能執行API。

## 應用程式層級RBAC

使用認證資料來驗證獲授權的使用者是否也擁有應用程式層級的權限。SnapCenter SnapCenter

例如、如果您要在 SQL Server 環境中執行 Snapshot 和資料保護作業、則必須使用適當的 Windows 或 SQL 認證來設定認證。此伺服器SnapCenter 會使用任一種方法驗證認證集。如果您要在 ONTAP 儲存設備上的 Windows 檔案系統環境中執行 Snapshot 和資料保護作業、SnapCenter 管理員角色必須在 Windows 主機上擁有管理員權限。

同樣地、如果您要在Oracle資料庫上執行資料保護作業、而且資料庫主機中的作業系統（OS）驗證已停用、則必須使用Oracle資料庫或Oracle ASM認證來設定認證資料。根據作業情況、此伺服器會使用下列其中一種方法來驗證認證集。SnapCenter

## VMware vSphere RBAC的插件SnapCenter

如果您使用SnapCenter VMware vCenter外掛程式來提供VM一致的資料保護、vCenter Server會提供額外的RBAC層級。VMware支援vCenter Server RBAC和VMware RBAC外掛程式。SnapCenter Data ONTAP

如需相關資訊、請參閱 ["VMware vSphere RBAC的插件SnapCenter"](#)

## 權限ONTAP

您應該建立具有存取儲存系統所需權限的vsadmin帳戶。

如需建立帳戶及指派權限的資訊、請參閱 ["以ONTAP 最低權限建立一個不含任何權限的叢集角色"](#)

## RBAC權限和角色

利用角色型存取控制（RBAC）、您可以建立角色並指派權限給這些角色、然後將使用者或使用者群組指派給這些角色。SnapCenter如此一來SnapCenter、管理員就能建立集中管理的環境、而應用程式管理員則能管理資料保護工作。隨附一些預先定義的角色和權限。SnapCenter

## 職務SnapCenter

隨附下列預先定義的角色。SnapCenter您可以將使用者和群組指派給這些角色、或是建立新角色。

當您指派角色給使用者時、除非您指派SnapCenter「管理員」角色、否則「工作」頁面中只會顯示與該使用者相關的工作。

- 應用程式備份與複製管理
- 備份與複製檢視器
- 基礎架構管理員
- SnapCenterAdmin

## VMware vSphere角色適用的外掛程式SnapCenter

為了管理VM、VMDK和資料存放區的VM一致資料保護、SnapCenter vCenter中的VMware vSphere支

援VMware vSphere的VMware外掛程式會建立下列角色：

- 選擇控制閥管理員
- 選擇控制閥視圖
- 選擇控制閥備用
- 選擇控制閥恢復
- 選擇控制閥客體檔案還原

如需詳細資訊、請參閱 "[VMware vSphere使用者適用的RBAC外掛程式類型SnapCenter](#)"

最佳實務做法：NetApp建議您為ONTAP VMware vSphere作業建立一個適用於SnapCenter VMware vSphere的解決方案、並指派所有必要的權限給它。

## 權限SnapCenter

支援下列權限：SnapCenter

- 資源群組
- 原則
- 備份
- 主機
- 儲存連線
- 複製
- 資源配置（僅適用於Microsoft SQL資料庫）
- 儀表板
- 報告
- 還原
  - 完整Volume還原（僅適用於自訂外掛程式）
- 資源

非系統管理員需要外掛程式權限、才能執行資源探索作業。

- 外掛程式安裝或解除安裝



啟用外掛程式安裝權限時、您也必須修改主機權限、才能啟用讀取和更新。

- 移轉
- 掛載（僅適用於Oracle資料庫）
- 卸載（僅適用於Oracle資料庫）
- 工作監控

「工作監控」權限可讓不同角色的成員查看指派給他們的所有物件上的作業。

# 預先定義SnapCenter 的功能和權限

隨附預先定義的角色、每個角色都已啟用一組權限。SnapCenter設定及管理角色型存取控制（RBAC）時、您可以使用這些預先定義的角色、或是建立新的角色。

包含下列預先定義的角色：SnapCenter

- 系統管理員角色SnapCenter
- 應用程式備份與複製管理員角色
- 備份與複製檢視器角色
- 基礎架構管理員角色

將使用者新增至角色時、您必須指派StorageConnection權限以啟用儲存虛擬機器（SVM）通訊、或指派SVM給使用者、以啟用使用SVM的權限。儲存連線權限可讓使用者建立SVM連線。

例如、具有SnapCenter「管理員」角色的使用者可以建立SVM連線、並將其指派給具有「應用程式備份與複製管理」角色的使用者、此角色預設無權建立或編輯SVM連線。如果沒有SVM連線、使用者將無法完成任何備份、複製或還原作業。

## 系統管理員角色SnapCenter

「支援管理員」角色已啟用所有權限。SnapCenter您無法修改此角色的權限。您可以將使用者和群組新增至角色、或將其移除。

## 應用程式備份與複製管理員角色

應用程式備份與複製管理角色擁有執行應用程式備份與複製相關工作之管理動作所需的權限。此角色沒有主機管理、資源配置、儲存連線管理或遠端安裝的權限。

權限	已啟用	建立	讀取	更新	刪除
資源群組	不適用	是的	是的	是的	是的
原則	不適用	是的	是的	是的	是的
備份	不適用	是的	是的	是的	是的
主機	不適用	是的	是的	是的	是的
儲存連線	不適用	否	是的	否	否
複製	不適用	是的	是的	是的	是的
資源配置	不適用	否	是的	否	否
儀表板	是的	不適用	不適用	不適用	不適用

權限	已啟用	建立	讀取	更新	刪除
報告	是的	不適用	不適用	不適用	不適用
還原	是的	不適用	不適用	不適用	不適用
資源	是的	是的	是的	是的	是的
外掛程式安裝/解除安裝	否	不適用		不適用	不適用
移轉	否	不適用	不適用	不適用	不適用
掛載	是的	是的	不適用	不適用	不適用
卸載	是的	是的	不適用	不適用	不適用
完整Volume還原	否	否	不適用	不適用	不適用
工作監控	是的	不適用	不適用	不適用	不適用

## 備份與複製檢視器角色

「備份與複製檢視器」角色具有所有權限的唯讀檢視。此角色也具備探索、報告及儀表板存取權限。

權限	已啟用	建立	讀取	更新	刪除
資源群組	不適用	否	是的	否	否
原則	不適用	否	是的	否	否
備份	不適用	否	是的	否	否
主機	不適用	否	是的	否	否
儲存連線	不適用	否	是的	否	否
複製	不適用	否	是的	否	否
資源配置	不適用	否	是的	否	否
儀表板	是的	不適用	不適用	不適用	不適用
報告	是的	不適用	不適用	不適用	不適用

權限	已啟用	建立	讀取	更新	刪除
還原	否	否	不適用	不適用	不適用
資源	否	否	是的	是的	否
外掛程式安裝/解除安裝	否	不適用	不適用	不適用	不適用
移轉	否	不適用	不適用	不適用	不適用
掛載	是的	不適用	不適用	不適用	不適用
卸載	是的	不適用	不適用	不適用	不適用
完整Volume還原	否	不適用	不適用	不適用	不適用
工作監控	是的	不適用	不適用	不適用	不適用

## 基礎架構管理員角色

基礎架構管理員角色已啟用主機管理、儲存管理、資源配置、資源群組、遠端安裝報告、並存取儀表板。

權限	已啟用	建立	讀取	更新	刪除
資源群組	不適用	是的	是的	是的	是的
原則	不適用	否	是的	是的	是的
備份	不適用	是的	是的	是的	是的
主機	不適用	是的	是的	是的	是的
儲存連線	不適用	是的	是的	是的	是的
複製	不適用	否	是的	否	否
資源配置	不適用	是的	是的	是的	是的
儀表板	是的	不適用	不適用	不適用	不適用
報告	是的	不適用	不適用	不適用	不適用
還原	是的	不適用	不適用	不適用	不適用



權限	已啟用	建立	讀取	更新	刪除
資源	是的	是的	是的	是的	是的
外掛程式安裝/解除安裝	是的	不適用	不適用	不適用	不適用
移轉	否	不適用	不適用	不適用	不適用
掛載	否	不適用	不適用	不適用	不適用
卸載	否	不適用	不適用	不適用	不適用
完整Volume還原	否	否	不適用	不適用	不適用
工作監控	是的	不適用	不適用	不適用	不適用

## 版權資訊

Copyright © 2024 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。