身分和存取管理

NetApp Console setup and administration

NetApp
February 11, 2026

目錄

身分和存取管理

了解NetApp Console身分和存取管理

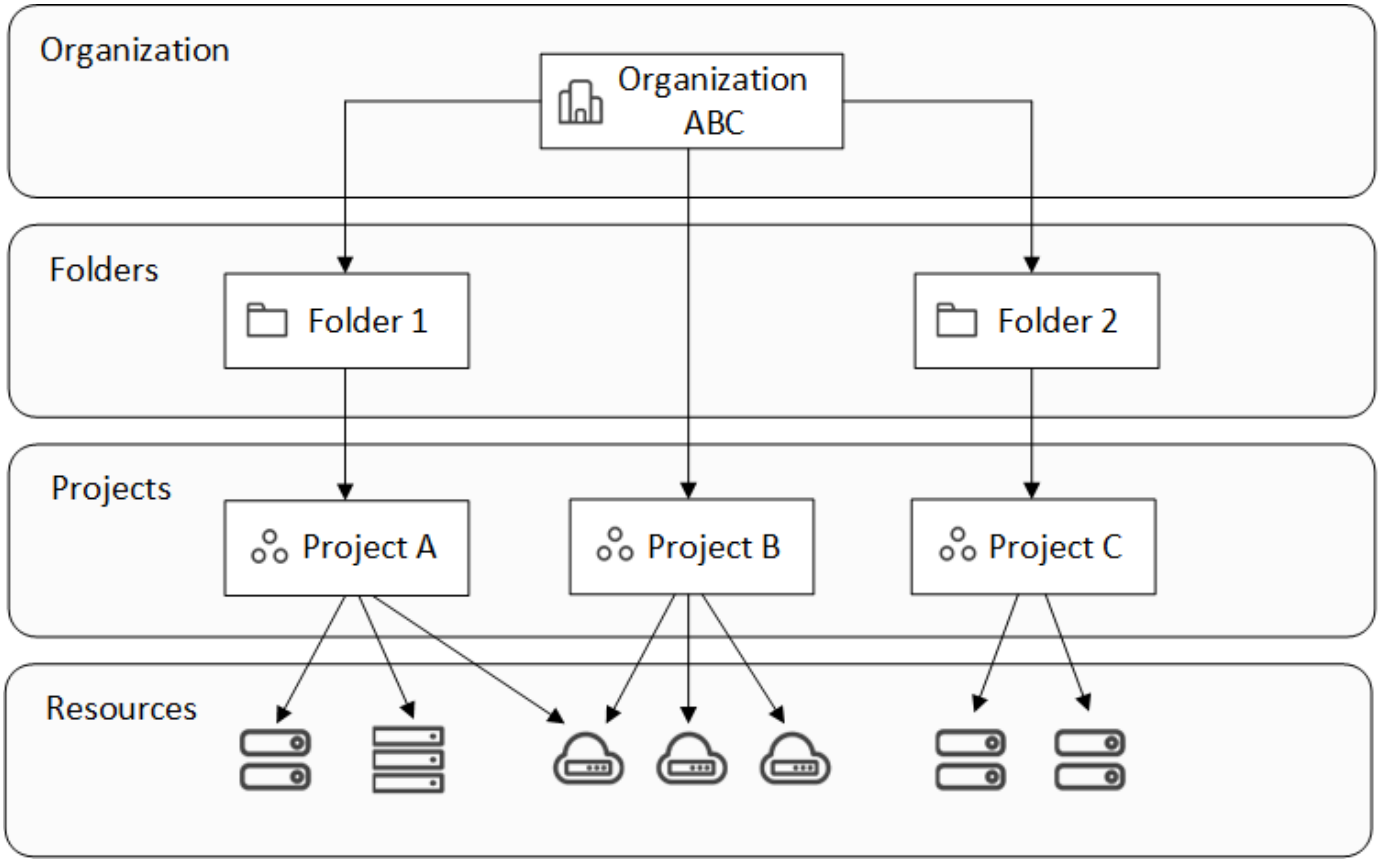
使用NetApp控制台的身分和存取管理 (IAM) 來組織您的NetApp資源，並根據您的業務結構（按位置、部門或專案）控制存取權限。

資源按層級排列：組織位於頂層，其次是資料夾（可以包含其他資料夾或項目），然後是項目，項目包含儲存系統、工作負載和代理。

在組織、資料夾或專案層級指派存取角色，以便使用者擁有對資源的正確存取權限。

您必須擁有_超級管理員_、_組織管理員_或_資料夾或專案管理員_角色才能在NetApp Console中管理 IAM。

下圖從基本層面說明了這個層次結構。



]

身分和存取管理元件

在NetApp Console中，您可以使用三個主要元件來組織儲存資源：組織元件、資源元件和使用者存取元件。

組織內的專案和資料夾

在您的 IAM 架構中，您使用三個組織元件：組織、專案和資料夾。您可以透過為使用者指派以下任何層級的角色來授予他們存取權限。

組織

_組織_是控制台 IAM 系統的頂層，通常代表您的公司。您的組織由資料夾、專案、成員、角色和資源組成。代理與組織內的特定項目相關聯。

專案

項目用於提供對儲存資源的存取。必須先將資源分配給項目，其他人才能存取這些資源。您可以將多個資源指派給一個項目，也可以建立多個項目。然後，您可以為使用者指派專案權限，使他們能夠存取專案中的資源。

例如，您可以根據需要，將本機ONTAP系統與單一專案或組織中的所有專案關聯起來。

"了解如何為您的組織新增項目。"

資料夾

將相關項目分組到_資料夾_中，以便按位置、站點或業務部門進行組織。您無法直接將資源與資料夾關聯，但將使用者指派到資料夾層級的角色，即可使其存取該資料夾中的所有項目。

"了解如何為您的組織新增資料夾。"

資源

資源 是指 NetApp Console 可識別並可指派給專案的實體。資源 包括儲存系統、Keystone 訂閱、部分 NetApp Backup and Recovery 工作負載以及 NetApp Console 代理。

+ 必須先將資源與項目關聯，其他人才能存取該資源。

+

例如，您可以將Cloud Volumes ONTAP系統與一個專案或組織中的所有專案關聯起來。資源的分配方式取決於貴組織的需求。

+

"了解如何將資源關聯到專案。"

儲存系統和**Keystone**訂閱

儲存系統是您在 NetApp Console 中管理的主要資源。NetApp Console 支援管理內部部署和雲端儲存系統。您必須將儲存系統新增至專案，以便指派給該專案的人員可以存取它。

儲存系統

儲存系統會自動關聯到新增它們的專案，但您也可以在 **Resources** 頁面中將它們關聯到其他專案或資料夾。您無法將 FSx for NetApp ONTAP 儲存系統關聯到專案或資料夾，但可以在 **Systems** 頁面或 Workloads 中查看它們。

Keystone訂閱

Keystone訂閱也是您可以與專案關聯的資源，以便授予使用者在NetApp Console中存取訂閱的權限。

備份與還原工作負載（**Oracle** 和 **Microsoft SQL Server**）

某些 Backup and Recovery 工作負載也被視為資源。您可以為使用者指派存取 Backup and Recovery 的權限。

控制台代理

組織管理員建立控制台代理來管理儲存系統並啟用NetApp資料服務。代理最初與創建它們的項目關聯，但管理員可以從“代理”頁面將它們添加到其他項目或資料夾。

將代理程式與專案關聯起來，可以管理該專案中的資源；而將代理程式與資料夾關聯起來，可以讓資料夾或專案管理員決定哪些專案應該使用該代理程式。代理人必須與特定項目關聯才能提供管理能力。

"了解如何將代理商與項目關聯起來。"

成員及角色

成員

您的組織的成員是使用者帳戶或服務帳戶。應用程式通常使用服務帳戶來完成指定的任務，而無需人工幹預。

成員註冊NetApp Console後，您需要將他們新增至您的組織。添加完成後，您可以為他們指派角色，以便授予他們存取資源的權限。您可以手動從控制台新增服務帳戶，也可以透過NetApp ConsoleIAM API 自動建立和管理服務帳戶。

"了解如何為您的組織新增成員。"

訪問角色

控制台提供您可以指派給組織成員的存取角色。

將成員與角色關聯時，您可以為整個組織、特定資料夾或特定專案授予該角色。您選擇的角色賦予成員對層次結構中選取部分的資源的權限。

NetApp Console提供細粒度的角色控制，遵循「最小權限」原則，這表示存取角色旨在僅向使用者授予其所需的權限。

這意味著隨著使用者職責的增加，他們可能會被分配多個角色。

"了解訪問角色" 。

IAM 策略範例

小型組織策略

對於使用者少於 50 人且採用集中式儲存管理的組織，可以考慮使用超級管理員和超級查看者角色的簡化方法。

範例：**ABC**公司（**5**人團隊）

- 組織架構： 單一組織，下設 3 個項目（生產、開發、備份）
- 角色：
  - 2 位高階成員：擁有*超級管理員*角色，可取得完整的管理權限
  - 3 位團隊成員：*超級檢視者*角色，擁有監控權限但無修改權限

- 代理策略：所有項目都關聯一個代理，以實現資源共享存取。
- 優勢：簡化管理，降低角色複雜性，適合需要廣泛存取權限的團隊

多區域企業策略

對於擁有區域營運和專業團隊的大型組織，應採用層級式方法，並以資料夾表示地理或業務單元邊界。

例如：**XYZ**公司（跨國公司）

- 結構： 組織結構 > 區域資料夾（北美、歐洲、亞太） > 每個區域的專案資料夾
- 平台角色：
  - 1 組織管理：全球監督與政策管理
  - 3 資料夾或專案管理員：區域控制（每個區域一個）
  - 1 聯盟管理員：企業身分提供者集成
- 按區域劃分的儲存角色：
  - 9 儲存管理員：發現並管理指定區域中的儲存系統
  - 2 儲存檢視器：監控跨區域的儲存資源
  - 1 系統健康專家：無需修改系統即可管理儲存健康狀況
- 數據服務角色：
  - 備份與復原管理員：按項目依備份職責而定
  - 勒索軟體復原管理員：負責跨專案的安全團隊監控
- 代理策略：與相應地理項目相關的區域代理
- 優勢： 透過角色分離、區域自主權和遵守當地法規來增強安全性

部門專業化策略

對於擁有需要特定資料服務存取權限的專業團隊的組織，應根據職能職責進行有針對性的角色分配。

例如：**TechCorp**（一家中型科技公司）

- 結構： 組織 > 部門資料夾（IT、安全、開發） > 專案特定資源
- 專業職缺：
  - 安全團隊：*勒索軟體復原管理員*和*分類檢視器*角色
  - 備份團隊：備份與還原超級管理員，負責全面的備份作業
  - 開發團隊：測試環境管理儲存管理員
  - 合規團隊：營運支援分析師，負責監控與支援個案管理
- 代理策略： 根據資源所有權將代理與部門項目關聯起來
- 優勢： 可自訂的存取控制、更高的營運效率以及明確的專案任務責任劃分

NetApp Console中 IAM 的後續步驟

- "開始使用NetApp Console中的 IAM"
- "監控或稽核 IAM 活動"
- "了解NetApp Console IAM 的 API"

開始在NetApp Console中使用身分和存取權限

當您註冊NetApp Console時，系統會提示您建立一個新的組織。該組織包括一名成員（組織管理員）和一個預設項目。要設定身分和存取管理 (IAM) 來滿足您的業務需求，您需要自訂組織的層次結構、新增其他成員、新增或發現資源，並在整個層次結構中關聯這些資源。

您需要擁有*組織管理員*或*超級管理員*權限才能管理組織的身分和存取權限。擁有*資料夾或專案管理員*權限，您只能管理您有權存取的資料夾和專案。

請依照以下步驟建立一個新組織。該順序可能會根據您組織的需求而有所不同。

1 編輯預設項目或加入組織的層次結構

使用預設項目或建立與您的業務層次結構相符的其他項目和資料夾。

"了解如何使用資料夾和項目來組織資源" 。

2 將成員與您的組織關聯

當使用者註冊NetApp Console後，您必須明確地將他們新增至您的 Console 組織。您也可以選擇為您的組織新增服務帳戶。

"了解如何管理成員及其權限" 。

3 新增或發現資源

在控制台新增或發現資源（系統）。組織成員從專案內部管理系統。

了解如何建立或發現資源：

- "Amazon FSx for NetApp ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes ONTAP"
- "E系列系統"
- "本地ONTAP集群"
- "StorageGRID"

4 將資源與其他項目關聯

在控制台中新增或發現系統會自動將資源與目前選定的項目關聯。若要使該資源可供組織中的另一個專案使用，請將其與對應的專案關聯。如果使用控制台代理程式來管理資源，請將控制台代理程式與對應的項目關聯。

- "了解如何管理組織的資源層次結構" 。
- "了解如何將控制台代理與資料夾或項目關聯" 。

相關資訊

- "了解NetApp Console中的身分和存取管理"
- "了解身分和存取 API"

設定您的控制台組織

將資料夾和專案新增至NetApp Console組織

新增資料夾和項目，以符合您的業務結構。建立資料夾和專案後，您可以將資源與它們關聯起來，並管理成員對這些項目的存取權。

建立新組織時，控制台會自動為您建立專案。大多數組織都需要多個項目，以及資料夾來保持井然有序。"了解NetApp Console中的資源層次結構"。

使用資料夾和項目來組織資源

在NetApp Console中，組織包含資料夾和項目，可協助您組織資源。資料夾可以幫助您將相關項目分組，專案可以幫助您管理資源和成員存取權限。

資料夾

資料夾可以幫助您整理相關項目。您可以建立嵌套資料夾來表示組織結構的不同層級。例如，您可以為每個業務部門建立一個頂級資料夾，然後在該業務部門內為不同的團隊建立子資料夾。然後，您可以在資料夾內建立項目。

資料夾還可以透過角色繼承更有效地管理成員存取權。在資料夾層級為成員指派角色時，他們將繼承所有子項目和資料夾的權限。

資料夾是一種組織工具，對於沒有 IAM 權限的成員（例如組織管理員、資料夾或專案管理員或超級管理員角色）是不可見的。成員存取的是項目，而不是資料夾。

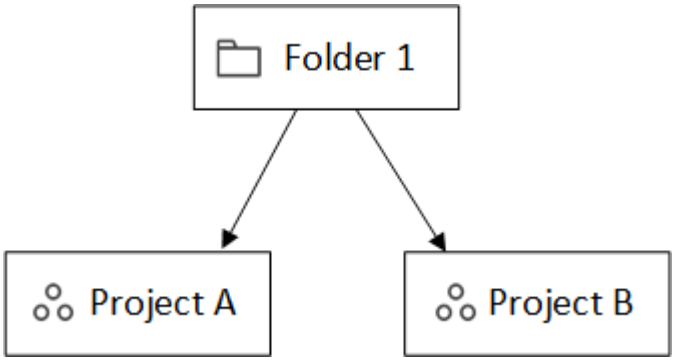
組織管理員可以透過建立資料夾來委派管理職責。建立資料夾後，組織管理員可以為特定資料夾指派資料夾管理員或專案管理員角色。這些成員無需訪問整個組織即可管理該資料夾內的所有項目。

資料夾可以包含其他資料夾或項目作為子資料夾，但不能直接關聯資源。資源必須與項目關聯。

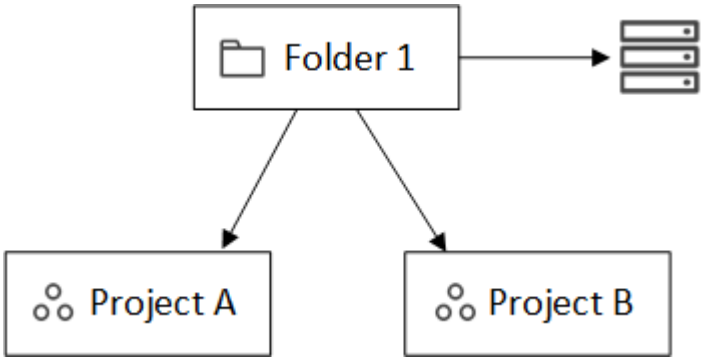
何時將資源與資料夾關聯

_組織管理員_可以將資源與資料夾關聯，以便_資料夾或專案管理員_可以將其連結到資料夾中的相應項目。

例如，假設您有一個包含兩個項目的資料夾：

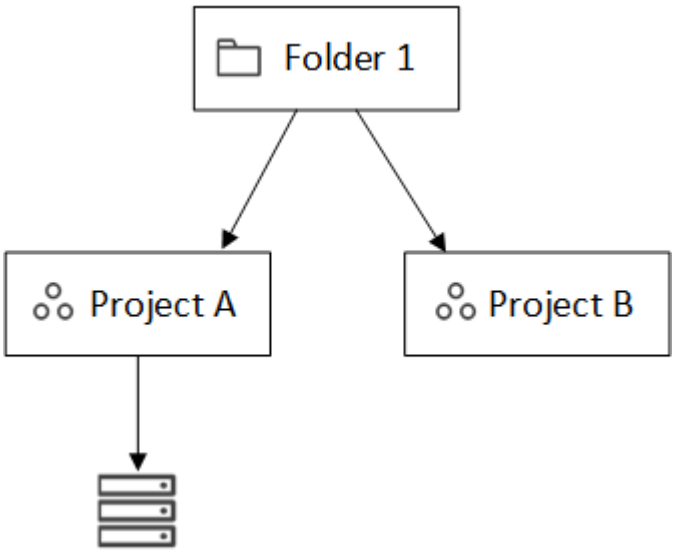


_組織管理員_可以將資源與資料夾關聯：



將資源與資料夾關聯並不會使所有項目都可以存取它；只有資料夾或專案管理員可以看到它。 _資料夾或專案管理員_決定哪些項目可以存取它，並將資源與適當的專案關聯。

在此範例中，管理員將資源與專案 A 關聯：



擁有專案 A 權限的成員現在可以存取該資源。

專案

將資源與專案關聯起來，以便成員進行管理。資源必須與專案關聯才能進行管理和使用者存取。

一個組織可以有一個或多個專案。項目可以直接位於組織下，也可以位於資料夾內。如果使用代理程式來發現專案中的資源，則也必須將該代理與該專案關聯起來。

使用者可在「系統」頁面上瀏覽已指派的項目，以管理與每個項目相關的資源。

新增資料夾或項目

新增專案以管理資源，新增資料夾以對相關項目進行分組。建立新組織時，控制台會包含一個項目。

您可以在組織的資源結構中建立最多七層的資料夾和項目。根據需要建立嵌套資料夾來整理資源。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*組織*。
3. 從*組織*頁面中，選擇*新增資料夾或項目*。
4. 選擇*資料夾*或*項目*。
5. 請輸入資料夾或項目詳細資料：
   - 名稱和位置：輸入資料夾或項目的名稱並選擇其位置。您可以將資料夾或項目放置在組織下，也可以放置在其他資料夾內。
   - 資源：選擇要與此資料夾或項目關聯的資源。如果您尚未向主機新增儲存系統，您可以稍後執行此步驟。

     只有當資料夾中的資源被指派給某個專案後，成員才能存取這些資源。使用資料夾暫時存放資源，直到建立必要的項目為止。這可以幫助組織管理員將資源分配委派給資料夾或專案管理員，然後由該管理員將資源指派給資料夾內的專案。

   - 存取權限：選擇*新增成員*以指派存取權限和角色。您可以隨時在專案或資料夾中新增或刪除成員。

     "了解訪問角色" 。
6. 選擇“新增”。

重新命名資料夾或項目

根據需要重新命名資料夾或項目。重新命名不會影響相關資源或成員存取權限。

步驟

1. 從「組織」頁面，導覽至表中的項目或資料夾，選擇 ••• 然後選擇*編輯資料夾*或*編輯項目*。
2. 在*編輯*頁面上，輸入新名稱並選擇*應用*。

刪除資料夾或項目

刪除不再需要的資料夾和項目，例如團隊重組或專案完成後。

刪除資料夾或項目之前，請確保其中不包含任何資源。了解如何移除資源。

步驟

1. 從「組織」頁面，導覽至表中的項目或資料夾，選擇 ••• 然後選擇*刪除*。
2. 確認您要刪除資料夾或項目。

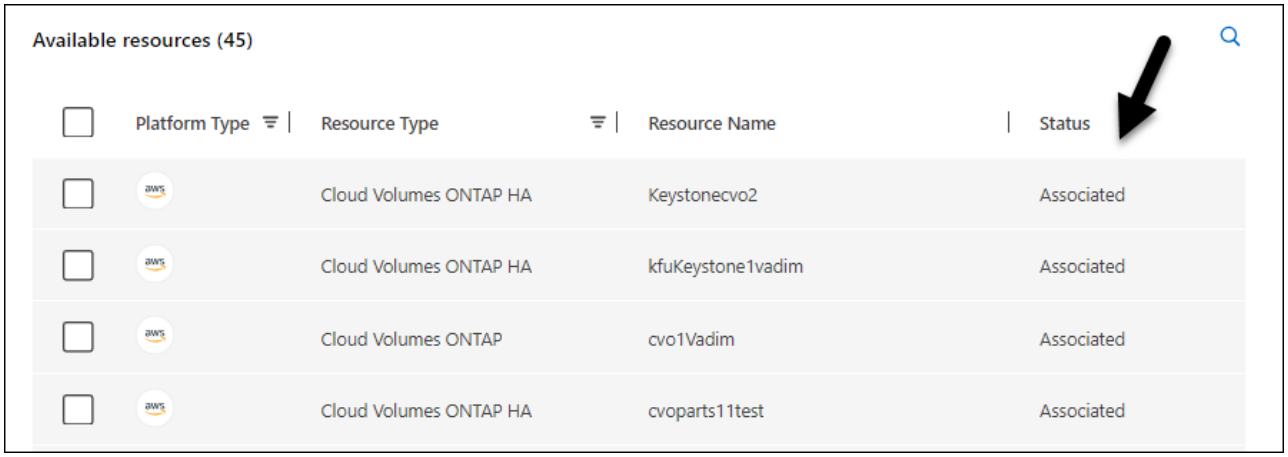
查看與資料夾或項目關聯的資源

查看哪些資源和成員與資料夾或項目相關聯。

步驟

1. 從「組織」頁面，導覽至表中的項目或資料夾，選擇 ••• 然後選擇*編輯資料夾*或*編輯項目*。

2. 在*編輯*頁面上，您可以透過展開*資源*或*存取*部分來查看有關所選資料夾或項目的詳細資訊。
   - 選擇"資源"來查看相關資源。在表中，「狀態」列標識與資料夾或項目相關的資源。



更改與資料夾或項目關聯的資源

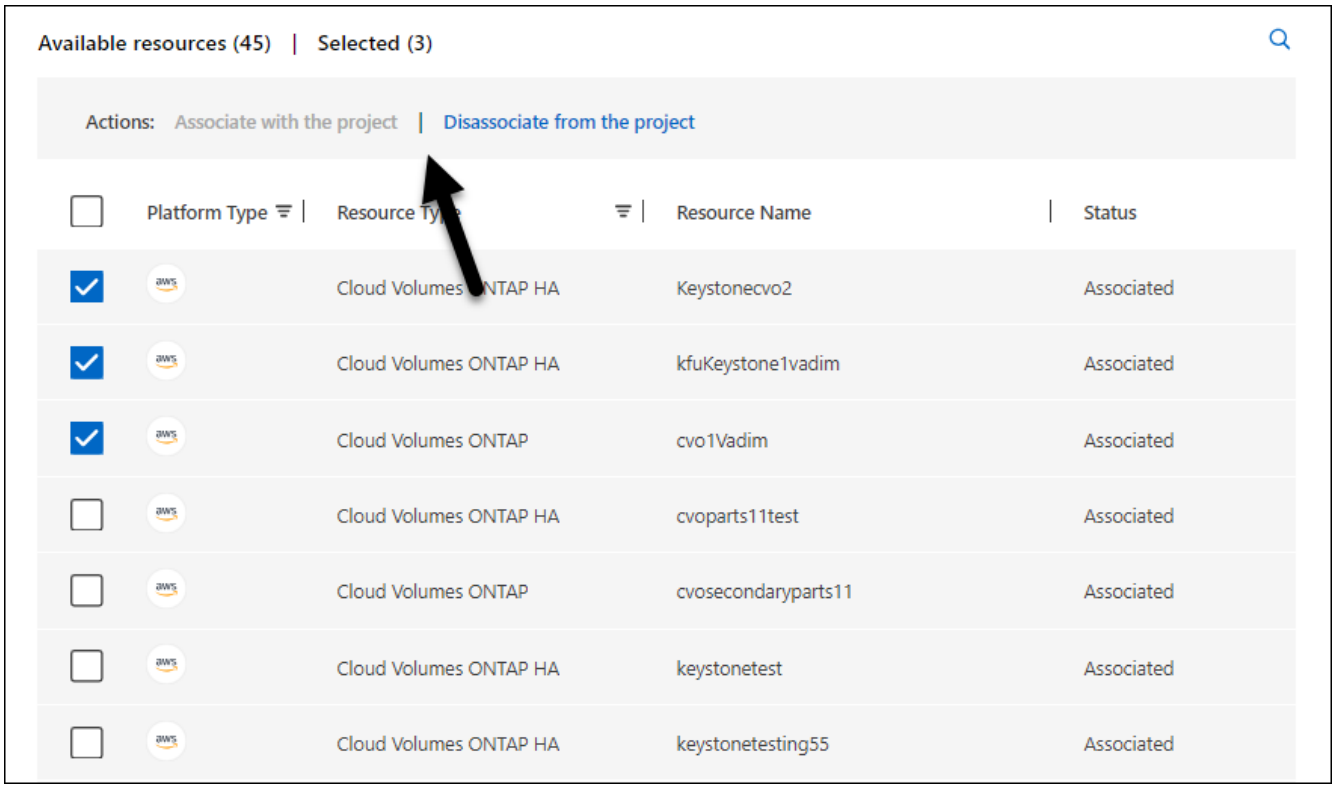
您可以根據組織的需求變更與資料夾或項目相關的資源變更。

步驟

1. 從「組織」頁面，導覽至表中的項目或資料夾，選擇 ••• 然後選擇*編輯資料夾*或*編輯項目*。
2. 在*編輯*頁面上，選擇*資源*。

   在表中，「狀態」列標識與資料夾或項目相關的資源。

3. 選擇您想要關聯或取消關聯的資源。
4. 根據您選擇的資源，選擇「與項目關聯」或「與項目取消關聯」。



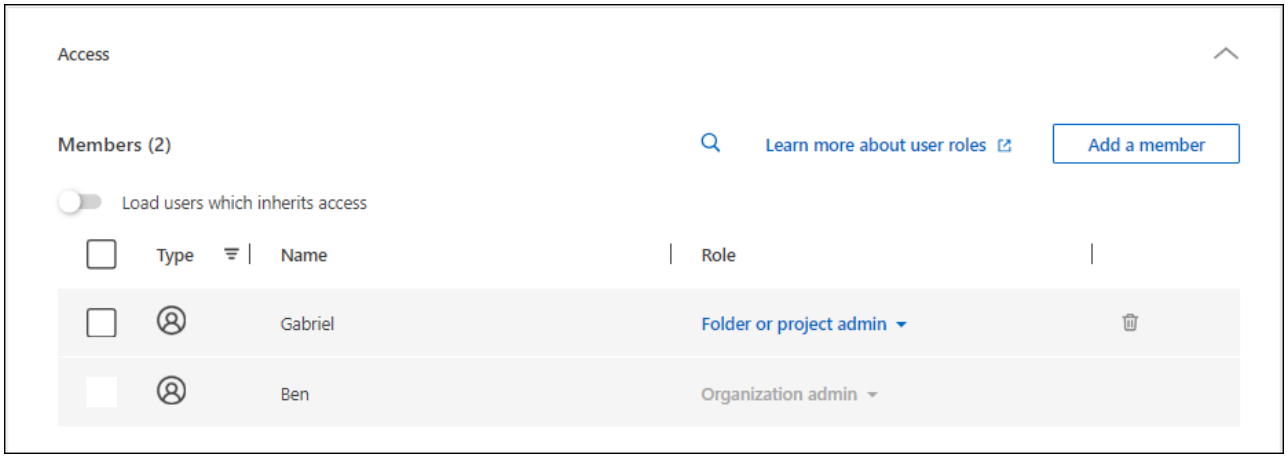
5. 選擇*應用*。

查看與資料夾或項目關聯的成員

您可以從「組織」頁面查看與資料夾或項目關聯的成員。

步驟

1. 從「組織」頁面，導覽至表中的項目或資料夾，選擇 ••• 然後選擇*編輯資料夾*或*編輯項目*。
2. 在*編輯*頁面上，選擇*存取*以查看有權存取所選資料夾或項目的成員清單。
   - 選擇*存取*來查看有權存取該資料夾或項目的成員。



修改成員對資料夾或項目的存取權限

修改成員存取權限以控制資源存取。請記住，在資料夾層級分配的角色將被所有子項目和資料夾繼承。

如果成員存取權限是從資料夾或組織層級繼承的，則無法在較低層級變更成員存取權限。變更較高層級成員的權限以變更存取權限。或者，您可以 "從「會員」頁面管理權限"。

步驟

1. 從「組織」頁面，導覽至表中的項目或資料夾，選擇 ••• 然後選擇*編輯資料夾*或*編輯項目*。
2. 在*編輯*頁面上，選擇*存取*以查看有權存取所選資料夾或項目的成員清單。
3. 修改會員存取權限：
   - 新增成員：選擇您想要新增至資料夾或專案的成員並為他們指派角色。
   - 變更成員的角色：對於具有組織管理員以外角色的任何成員，選擇其現有角色，然後選擇新角色。
   - 刪除成員存取權限：對於在您正在查看的資料夾或專案中定義了角色的成員，您可以刪除他們的存取權限。
4. 選擇*應用*。

相關資訊

- "了解NetApp Console中的身分和存取權限"
- "開始使用身分和存取權限"
- "了解身分和存取 API"

在NetApp Console中新增資源

透過將使用者新增至NetApp Console組織中的專案和資料夾來控制使用者對資源的存取權限。授予專案級使用者存取權限。

資源是指控制台所感知到的實體，例如儲存資源、控制台代理程式或備份和還原工作負載。

您可以在控制台的「資源」頁面中檢視和管理資源。

控制台資源類型

您可以將多種類型的資源關聯到NetApp Console組織中的專案：

儲存資源

儲存資源是組織中最常見的資源類型，包括本地儲存系統和雲端儲存系統。在控制台中新增儲存系統時，您可以將其新增至資料夾或專案。在此之前，控制台會將其標記為未發現，並且不會在「資源」頁面上顯示它。

控制台代理

如果您使用控制台代理程式來發現儲存系統，請將該代理程式新增至相同資料夾或專案。這允許使用者執行代理啟用的功能，例如資料服務或控制台原生儲存管理。您可以從控制台的「代理」頁面新增代理程式到資料夾或專案。"了解如何將控制台代理與資料夾或項目關聯"。

Keystone訂閱

如果您的組織擁有Keystone訂閱，您可以在「資源」頁面上查看它們。您可以將Keystone訂閱與資料夾或項目關聯起來，以便提供擁有這些資料夾或專案權限的成員存取權限。

查看組織中的資源

您可以查看與您的組織相關的已發現和未發現的資源。系統會尋找儲存資源，並將其標記為未發現，直到您將其新增至控制台為止。

> 控制台會將Amazon FSx for NetApp ONTAP資源從「資源」頁面中排除，因為使用者無法將其與角色關聯。您可以在「系統」頁面或「工作負載」中查看這些資源。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*資源*。
3. 選擇*進階搜尋和過濾*。
4. 利用現有選項尋找資源：
   - 按資源名稱搜尋：輸入文字字串並選擇*新增*。
   - 平台：選擇一個或多個平台，例如 Amazon Web Services。
   - 資源：選擇一個或多個資源，例如Cloud Volumes ONTAP。
   - 組織、資料夾或專案：選擇整個組織、特定資料夾或特定專案。
5. 選擇*搜尋*。

將資源與資料夾和項目關聯

將資源關聯到資料夾或項目，使其可供具有該資料夾或項目權限的成員使用。

步驟

1. 從「資源」頁面，導覽到表中的資源，選擇 ••• 然後選擇*關聯到資料夾或項目*。
2. 選擇一個資料夾或項目，然後選擇*接受*。
3. 若要關聯其他資料夾或項目，請選擇*新增資料夾或項目*，然後選擇該資料夾或項目。

   請注意，您只能從您擁有管理員權限的資料夾和項目中進行選擇。

4. 選擇*關聯資源*。
   - 如果您將資源與項目關聯，則擁有這些項目權限的成員現在可以從控制台存取該資源。
   - 如果您將資源與資料夾關聯，則_資料夾或專案管理員_現在可以存取該資源並將其與資料夾內的項目關聯。"了解如何將資源與資料夾關聯"。

完成後

如果您使用控制台代理程式發現資源，請將控制台代理程式與專案關聯以授予存取權限。否則，沒有「組織管理員」角色的成員將無法存取控制台代理程式及其相關資源。

"了解如何將控制台代理與資料夾或項目關聯"。

查看與資源關聯的資料夾和項目

您可以查看與特定資源關聯的資料夾和項目。

如果您需要了解哪些組織成員有權存取該資源，您可以"查看有權存取與資源關聯的資料夾和項目的成員"。

步驟

1. 從「資源」頁面，導覽到表中的資源，選擇 ••• 然後選擇*查看詳細資訊*。

以下範例顯示了與一個項目關聯的資源。

要查看哪些組織成員有權存取該資源，"查看有權存取關聯資料夾和項目的成員" 。

從資料夾或項目中刪除資源

若要從資料夾或項目中刪除資源，請刪除其關聯。這樣可以防止成員管理該資料夾或專案中的資源。

若要從整個組織中刪除已發現的資源，請前往「系統」頁面並刪除該系統。

步驟

1. 從「資源」頁面，導覽到表中的資源，選擇 ••• 然後選擇*查看詳細資訊*。
2. 若要從資料夾或項目移除資源，請選擇 在資料夾或項目旁邊。
3. 選擇“刪除”以移除關聯。

相關資訊

- "了解NetApp Console中的身分和存取權限"
- "開始在NetApp Console中使用身分和存取權限"
- "了解身分和存取 API"

將控制台代理程式與其他資料夾和項目關聯

將控制台代理與特定項目關聯，以啟用資源管理和資料服務存取。透過控制台代理程式發現的資源需要資源和代理程式都與同一個專案關聯，才能實現團隊存取。

超級管理員和組織管理員可以建立代理，並將任何代理與任何專案或資料夾關聯起來。資料夾或專案管理員只能將現有代理與他們擁有權限的資料夾和項目關聯起來。"詳細了解資料夾或專案管理員可以完成的操作"。

步驟

1. 選擇*管理>身分和存取*>*代理*。
2. 從表中，找到要關聯的控制台代理程式。

   使用表格上方的搜尋功能尋找特定的控制台代理程式或依資源層次結構篩選表格。

3. 若要查看連結到控制台代理的資料夾和項目，請選擇 ••• 然後選擇*查看詳細資訊*。

   此頁面顯示與控制台代理程式關聯的資料夾和項目的詳細資訊。

4. 選擇*關聯到資料夾或項目*。
5. 選擇一個資料夾或項目，然後選擇*接受*。
6. 若要將控制台代理程式與其他資料夾或項目關聯，請選擇*新增資料夾或項目*，然後選擇該資料夾或項目。
7. 選擇*關聯代理*。

完成後

將控制台代理程式的資源與「資源」頁面中的相同資料夾和項目關聯。

"了解如何將資源與資料夾和項目關聯" 。

相關資訊

- "了解NetApp Console代理"
- "了解NetApp Console身分和存取管理"
- "開始使用身分和存取權限"
- "了解身分和存取管理的 API"

將使用者新增至您的控制台組織

將使用者新增至**NetApp Console**組織

在控制台中，您可以根據存取角色授予使用者對專案或資料夾的存取權限。_存取角色_包含一組權限，使成員（使用者或服務帳戶）能夠在資源層次結構的指定層級執行特定操作。

所需存取權限

超級管理員、組織管理員或資料夾或專案管理員（對於他們管理的資料夾和專案）。"了解訪問角色"。

了解如何在**NetApp Console**中授予存取權限

NetApp Console使用基於角色的存取控制 (RBAC) 來管理權限。可以單獨為使用者指派角色，也可以透過聯合群組為使用者指派角色。每個角色都定義了對特定資源允許的操作。

請注意以下關於在NetApp Console中授予存取權限的事項：

- 所有使用者必須先註冊NetApp Console，然後才能取得資源存取權限。
- 即使使用者是已指派角色的聯合群組的成員，也必須在控制台中明確地為每個使用者指派角色，然後他們才能存取資源。

- 您可以直接從控制台新增服務帳戶並為其指派角色。

在您的組織中加入成員

NetApp Console支援三種類型的成員：使用者帳戶、服務帳戶和聯合群組。

即使使用者屬於聯合群組，也必須先註冊NetApp Console，然後才能新增他們並指派角色。直接在控制台中建立服務帳戶。

所有成員必須至少被明確分配一個角色才能存取資源。

新增成員時，選擇資源層級（組織、資料夾或專案），並指派一個或多個具有所需權限的角色。

新增用戶

使用者註冊NetApp Console，但組織管理員、資料夾管理員或專案管理員必須將他們新增至組織、資料夾或專案中，以便他們能夠存取資源。

開始之前：

使用者必須已經註冊了NetApp Console。如果他們還沒有註冊，請引導他們... "註冊NetApp Console。"

如果要新增屬於聯合群組的用戶，請確保該用戶已註冊NetApp Console，並在控制台中明確指派了角色。NetApp建議指派最低存取權限角色，例如組織檢視者。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*成員*。
3. 選擇*新增成員*。
4. 對於*會員類型*，保持選擇*使用者*。
5. 對於*使用者的電子郵件*，輸入與其建立的登入相關聯的使用者的電子郵件地址。
6. 使用「選擇組織、資料夾或項目」部分來選擇成員應具有權限的資源層次結構層級。

   請注意以下事項：

   - 您只能選擇您擁有權限的資料夾和項目。
   - 選擇組織或資料夾時，即授予該成員對其所有內容的存取權限。
   - 您只能在組織層級指派*組織管理員*角色。
7. 選擇一個類別，然後選擇一個*角色*，該角色為成員提供與您選擇的組織、資料夾或專案相關的資源的權限。

   "了解訪問角色" 。
8. 若要授予對更多資料夾、項目或角色的存取權限，請選擇“新增角色”，選擇資料夾、項目或角色類別，然後選擇角色。
9. 選擇“新增”。

   控制台會透過電子郵件向使用者發送操作說明。

服務帳戶可讓您自動執行任務並安全地連接到控制台 API。對於簡單的設置，可以選擇客戶端 ID 和金鑰；對於自動化或雲端原生環境，可以選擇 JWT（JSON Web Token）以獲得更強的安全性。選擇符合您安全要求的方法。

開始之前：

對於 JWT 身份驗證，請準備您的公鑰或憑證。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*成員*。
3. 選擇*新增成員*。
4. 對於*會員類型*，選擇*服務帳戶*。
5. 輸入服務帳戶的名稱。
6. 若要使用 JWT 驗證，請選擇“使用私鑰 JWT 驗證”，然後上傳您的 RSA 公鑰或憑證。如果使用客戶端 ID 和金鑰，則跳過此步驟。

   您的 X.509 證書。它必須是 PEM、CRT 或 CER 格式。

   a. 設定證書到期通知。您可以選擇七天或三十天。到期通知將透過電子郵件發送給具有超級管理員或組織管理員角色的用戶，並在控制台中顯示。
7. 使用「選擇組織、資料夾或項目」部分來選擇成員應具有權限的資源層次結構層級。

   請注意以下事項：

   - 您只能從您有權限的資料夾和項目中進行選擇。
   - 選擇一個組織或資料夾將授予成員對其所有內容的權限。
   - 您只能在組織層級指派*組織管理員*角色。
8. 選擇一個*類別*，然後選擇一個*角色*，授予成員對所選組織、資料夾或專案中的資源的權限。

   "了解訪問角色" 。
9. 若要授予對更多資料夾、項目或角色的存取權限，請選擇“新增角色”，選擇資料夾、項目或角色類別，然後選擇角色。
10. 如果您沒有選擇使用 JWT 驗證，請下載或複製用戶端 ID 和用戶端金鑰。

    控制台只會顯示一次客戶端金鑰。請妥善備份；如果遺失，您可以稍後重新建立。
11. 如果您選擇 JWT 驗證，請下載或複製用戶端 ID 和 JWT 受眾群體。控制台只會顯示此資訊一次，之後無法再檢索。
12. 選擇*關閉*。

在您的組織中新增聯合組

您可以將身分提供者 (IdP) 中的聯合群組新增至您的組織，並為其指派一個或多個角色。聯合群組的成員將繼承您在控制台中指派給該群組的角色。

在為聯合組分配角色之前，請確保以下事項：

- 在身分識別提供者 (IdP) 和控制台之間建立聯盟。 "了解如何建立聯邦。"
- 該群組必須已存在於您的身分提供者 (IdP) 中，並且已被指派對控制台的應用程式存取權。
- 屬於該群組的使用者必須已經註冊了NetApp Console，並且已明確指派了控制台中的角色。NetApp建議指派最低存取權限角色，例如組織檢視者。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*成員*。
3. 選擇*新增成員*。
4. 對於“成員類型”，請選擇“聯合群組”。
5. 選擇該團體所屬的聯邦。
6. 對於“群組名稱”，請輸入您身分提供者 (IdP) 中群組的確切名稱。
7. 使用「選擇組織、資料夾或項目」部分來選擇成員應具有權限的資源層次結構層級。

   請注意以下事項：

   - 您只能從您有權限的資料夾和項目中進行選擇。
   - 選擇一個組織或資料夾將授予成員對其所有內容的權限。
   - 您只能在組織層級指派*組織管理員*角色。
8. 選擇一個*類別*，然後選擇一個*角色*，授予成員對所選組織、資料夾或專案中的資源的權限。

   "了解訪問角色" 。
9. 若要授予對更多資料夾、項目或角色的存取權限，請選擇“新增角色”，選擇資料夾、項目或角色類別，然後選擇角色。

相關資訊

- "了解NetApp Console中的身分和存取管理"
- "開始使用身分和存取權限"
- "NetApp Console存取角色"
- "了解身分和存取 API"

管理使用者存取權限和安全

了解**NetApp Console**基於角色的存取控制 **(RBAC)**

使用基於角色的存取控制 (RBAC) 管理使用者對NetApp Console的訪問，在組織、資料夾或專案層級指派預先定義角色。每個角色都授予特定的權限，定義使用者在其指派的權限範圍內可以執行哪些操作。

NetApp在設計控制台角色時遵循最小權限原則，因此每個角色僅包含其任務所需的權限。這種方法透過限制每個成員所需的存取權限來增強安全性。

將資源整理成資料夾和專案後，為組織成員指派特定資料夾或專案的角色，使他們只能履行自己的職責。

例如，您可以為特定專案層級的成員指派勒索軟體復原管理員角色，允許他們對該專案內的資源執行勒索軟體復原操作，而無需授予他們對整個組織的更廣泛存取權限。同一使用者可以被授予組織內多個專案的角色。

您可以根據使用者的職責，為相同範圍或不同範圍的使用者指派多個角色。例如，規模較小的組織可能會讓同一用戶在組織層級管理勒索軟體復原和備份與復原任務，而規模較大的組織可能會在專案層級為每個角色分配不同的使用者。

控制台組織成員的類型

NetApp Console組織中有三種類型的成員：* 使用者帳號：登入NetApp Console以管理資源的個人使用者。使用者必須先註冊NetApp Console，然後才能被加入到組織中。* 服務帳戶：應用程式或服務透過 API 與NetApp Console互動時使用的非人類帳戶。您可以將服務帳戶直接新增至您的控制台組織。* 聯合群組：從您的身分提供者 (IdP) 同步的群組，可讓您集中管理多個使用者的存取權限。聯合群組中的每個使用者都必須先註冊NetApp Console，並被新增到您的組織中，並且擁有相應的存取角色，然後才能存取授予該群組的資源。

"了解如何為您的組織新增成員。"

NetApp Console中的預先定義角色

NetApp Console包含預先定義角色，您可以將其指派給組織成員。每個角色都包含權限，用於指定成員在其指派的範圍（組織、資料夾或專案）內可以執行哪些操作。

NetApp Console角色採用最小權限原則，確保成員僅擁有完成任務所需的權限，並按角色提供的存取權限類型對其進行分類：

- 平台角色：提供控制台管理權限
- 資料服務角色：提供管理特定資料服務的權限，例如勒索軟體復原和備份與復原。
- 應用程式角色：提供管理儲存以及審核控制台事件和警報的權限

您可以根據成員的職責為其指派多個角色。例如，您可以為特定項目為一名成員指派勒索軟體復原管理員角色和備份與復原管理員角色。

"了解NetApp Console中可用的預先定義角色"。

在**NetApp Console**中管理成員存取權限

管理您在控制台組織中的成員存取權限。分配角色以設定權限。成員離開時將其移除。

所需存取權限

超級管理員、組織管理員或資料夾或專案管理員（對於他們管理的資料夾和專案）。連結：reference-iam-predefined-roles.html[了解訪問角色]。

您可以按項目或資料夾指派存取角色。例如，可以為使用者指派兩個特定項目的角色，或在資料夾層級指派角色，從而授予使用者對資料夾中所有項目的勒索軟體復原管理員角色。

請先新增資料夾和項目，然後再分配使用者存取權限。 "了解如何新增資料夾和項目。"

了解如何在**NetApp Console**中授予存取權限

NetApp Console使用基於角色的存取控制 (RBAC) 模型來管理使用者權限。您可以單獨或透過聯合群組為成員指派預先定義的角色。您可以為服務帳戶以及聯合群組新增和指派角色。每個角色都定義了成員可以在相關資源上執行哪些動作。

請注意以下關於在NetApp Console中授予存取權限的事項：

- 所有使用者必須先註冊NetApp Console，然後才能取得資源存取權限。
- 即使使用者是已指派角色的聯合群組的成員，也必須在控制台中明確地為每個使用者指派角色，然後他們才能存取資源。
- 您可以直接從控制台新增服務帳戶並為其指派角色。

使用角色繼承

在NetApp Console中，當您在組織、資料夾或專案層級指派角色時，所選範圍內的所有資源都會自動繼承該角色。例如，資料夾級角色適用於所有包含的項目，而專案級角色適用於該項目內的所有資源。

查看組織成員

若要了解成員可用的資源和權限，您可以查看在組織資源層級結構的不同層級指派給該成員的角色。"了解如何使用角色來控制對控制台資源的存取。"

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*成員*。

   *成員*表格列出了您組織的成員。

3. 從「成員」頁面，導覽至表中的成員，選擇 ••• 然後選擇*查看詳細資訊*。

查看指派給成員的角色

您可以查看他們目前被指派的角色。

如果您具有_資料夾或專案管理員_角色，則該頁面將顯示組織中的所有成員。但是，您只能查看和管理您擁有權限的資料夾和專案的成員權限。"詳細了解資料夾或專案管理員可以完成的操作" 。

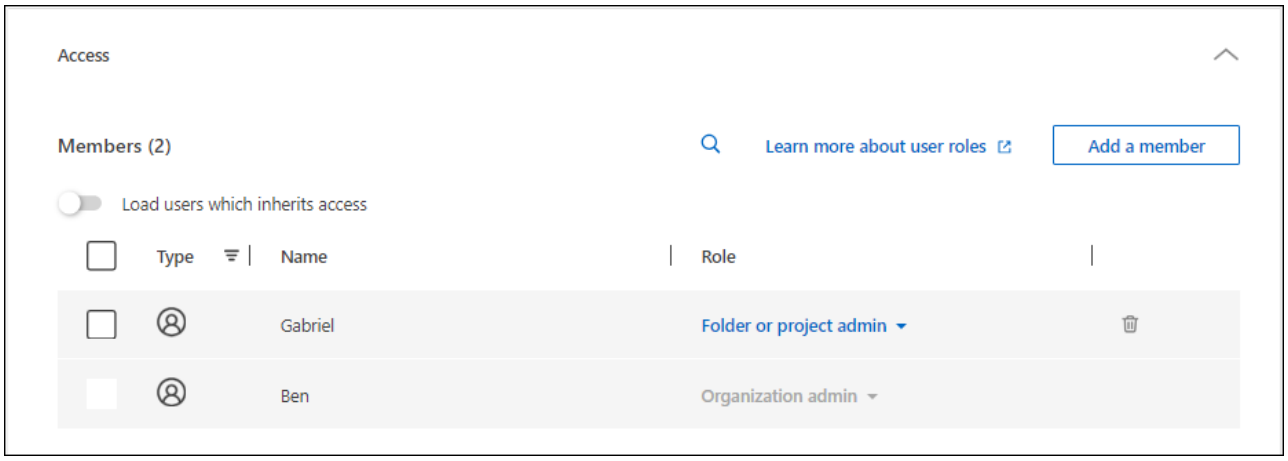
1. 在「成員」頁面中，導覽至表格中的某個成員，然後選擇 ••• 然後選擇“查看詳情”。
2. 在表格中，展開您想要查看成員指派角色的組織、資料夾或專案的對應行，然後在「角色」欄位中選擇「檢視」。

查看與資料夾或項目關聯的成員

您可以查看哪些成員有權存取特定資料夾或項目。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*組織*。
3. 從「組織」頁面，導覽至表中的項目或資料夾，選擇 ••• 然後選擇*編輯資料夾*或*編輯項目*。
   - 選擇*存取*來查看有權存取該資料夾或項目的成員。



分配或修改成員存取權限

使用者註冊NetApp Console後，您可以將他們新增至您的組織並指派角色，以便向他們提供資源存取權。 "了解如何為您的組織新增成員。"

您可以根據需要新增或刪除角色來調整成員的存取權限。

為成員新增存取角色

您通常在為組織新增成員時指派角色，但您可以隨時透過刪除或新增角色來更新它。

您可以為使用者指派組織、資料夾或專案的存取角色。

成員可以在同一個專案內或不同的專案中擔任多個角色。例如，規模較小的組織可能會將所有可用的存取角色分配給相同用戶，而規模較大的組織可能會讓用戶執行更專業的任務。或者，您也可以在組織層級為一名使用者指派勒索軟體復原管理員角色。在這個例子中，使用者可以對組織內的所有項目執行勒索軟體復原任務。

您的存取角色策略應與您組織NetApp資源的方式保持一致。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*成員*。
3. 選擇成員標籤之一：使用者、服務帳戶*或*聯合群組。
4. 選擇操作選單 ••• 在您想要指派角色的成員旁邊，選擇「新增角色」。
5. 若要新增角色，請完成對話方塊中的步驟：
   - 選擇組織、資料夾或專案：選擇成員應具有權限的資源層次結構層級。

     如果您選擇組織或資料夾，則該成員將擁有該組織或資料夾內所有內容的權限。

- 選擇類別：選擇角色類別。"了解訪問角色" 。
- 選擇*角色*：選擇一個角色，該角色為成員提供與您選擇的組織、資料夾或專案相關的資源的權限。
- 新增角色：如果您想提供組織內其他資料夾或項目的存取權限，請選擇*新增角色*，指定另一個資料夾或項目或角色類別，然後選擇一個角色類別和對應的角色。

6. 選擇*新增角色*。

更改成員的指定角色

更改成員角色以更新其存取權限。

必須為使用者指派至少一個角色。您無法刪除使用者的所有角色。如果您需要刪除所有角色，則必須從組織中刪除該使用者。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*成員*。
3. 選擇成員標籤之一：使用者、服務帳戶*或*聯合群組。
4. 從「成員」頁面，導覽至表中的成員，選擇 ••• 然後選擇*查看詳細資訊*。
5. 在表格中，展開要變更成員指派角色的組織、資料夾或專案的對應行，然後在「角色」欄位中選擇「檢視」以查看指派給該成員的角色。
6. 您可以變更成員的現有角色或刪除角色。
   a. 若要變更成員的角色，請選擇要變更的角色旁邊的「變更」 。您只能將角色變更為同一角色類別內的角色。例如，您可以從一個資料服務角色變更為另一個資料服務角色。確認更改。
   b. 若要取消指派成員的角色，請選擇 在角色旁邊，點擊即可從成員中移除對應的角色。您將被要求確認刪除操作。

從您的組織中移除成員

如果成員離開您的組織，則將其從組織中移除。

刪除成員時，系統會撤銷其控制台權限，但保留其控制台和NetApp支援網站帳號。

聯邦成員

- 當聯合使用者從您的身分提供者 (IdP) 中移除時，他們將自動失去對NetApp Console的存取權限。但您仍然應該將它們從您的控制台組織中刪除，以保持您的成員清單是最新的。
- 如果您從身分提供者 (IdP) 中的聯合群組中移除用戶，他們將失去與該群組關聯的控制台存取權限。但是，他們仍然保留在控制台中分配給他們的明確角色所關聯的任何存取權限。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*成員*。
3. 選擇成員標籤之一：使用者、服務帳戶*或*聯合群組。
4. 從「成員」頁面，導覽至表中的成員，選擇 ••• 然後選擇*刪除使用者*。

5. 確認您要從組織中刪除該成員。

使用者安全

透過管理成員安全設置，確保使用者對NetApp Console組織的存取權限。您可以重設使用者密碼、管理多因素身份驗證 (MFA) 以及重新建立服務帳戶憑證。

所需存取權限

超級管理員、組織管理員或資料夾或專案管理員（對於他們管理的資料夾和專案）。連結：reference-iam-predefined-roles.html[了解訪問角色]。

重設使用者密碼（僅限本地用戶）

組織管理員無法重設本機使用者的使用者密碼。但是，他們可以指導用戶重置自己的密碼。

指示使用者透過選擇「忘記密碼？」從控制台登入頁面重設密碼。

此選項不適用於聯合組織中的使用者。

管理用戶的多重身份驗證 **(MFA)**

如果使用者失去對其 MFA 設備的存取權限，您可以刪除或停用其 MFA 配置。

多因素身份驗證僅適用於本機用戶。聯合身份驗證使用者無法啟用多因素身份驗證 (MFA)。

使用者移除多因素身份驗證後，登入時必須重新設定多因素身份驗證。如果使用者暫時無法存取其 MFA 設備，他們可以使用已儲存的復原代碼登入。

如果他們沒有恢復代碼，請暫時停用 MFA 以允許登入。當您為使用者停用 MFA 時，它只會停用八個小時，然後自動重新啟用。在此期間，用戶無需 MFA 即可登入一次。八小時後，使用者必須使用 MFA 才能登入。

若要管理使用者的多重身分驗證，您必須擁有與受影響使用者位於相同網域的電子郵件地址。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*成員*。

   *成員*表格列出了您組織的成員。

3. 從「成員」頁面，導覽至表中的成員，選擇 ••• 然後選擇*管理多重身份驗證*。
4. 選擇是否刪除或停用使用者的 MFA 配置。

重新建立服務帳戶的憑證

如果您遺失或需要更新服務憑證，可以建立新的憑證。

建立新憑證會刪除舊憑證。您不能使用舊的憑證。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*成員*。
3. 在「成員」表中，導覽至服務帳戶，選擇 ... 然後選擇*重新建立秘密*。
4. 選擇*重新建立*。
5. 下載或複製客戶端 ID 和客戶端金鑰。

   控制台只會顯示一次客戶端金鑰。請務必複製或下載並妥善保存。

NetApp Console存取角色

了解NetApp Console存取角色

NetApp Console中的身分和存取管理 (IAM) 提供了預先定義的角色，您可以將這些角色指派給組織中不同資源層級的成員。在指派這些角色之前，您應該了解每個角色包含的權限。角色分為以下類別：平台、應用程式和資料服務。

平台角色

平台角色授予NetApp Console管理權限，包括角色指派和使用者管理。控制台具有多種平台角色。

平台角色	職責
"組織管理員"	允許使用者不受限制地存取組織內的所有項目和資料夾，為任何項目或資料夾添加成員，以及執行任何任務和使用任何沒有明確關聯角色的資料服務。具有此角色的使用者可以透過建立資料夾和專案、分配角色、新增使用者以及管理系統（如果他們擁有適當的憑證）來管理您的組織。這是唯一可以建立控制台代理的存取角色。
"資料夾或專案管理員"	允許使用者不受限制地存取已指派的項目和資料夾。可以將成員新增到他們管理的資料夾或專案中，以及執行任何任務並在他們被指派的資料夾或專案內的資源上使用任何資料服務或應用程式。資料夾或專案管理員無法建立控制台代理。
"聯盟管理員"	允許使用者使用控制台建立和管理聯合，從而實現單一登入 (SSO)。
"聯邦檢視器"	允許使用者使用控制台查看現有的聯合。無法建立或管理聯盟。
"合作夥伴管理員"	允許使用者創建和管理合作關係。
"合作夥伴檢視器"	允許用戶查看現有的合作關係。無法創建或管理合作關係。
"超管理員"	為使用者提供管理員角色的子集。此角色專為可能不需要在多個使用者之間分配控制台職責的小型組織而設計。
"超觀眾"	為使用者提供子集查看者角色。此角色專為可能不需要在多個使用者之間分配控制台職責的小型組織而設計。

應用程式角色

以下是應用程式類別中的角色清單。每個角色在其指定範圍內授予特定的權限。沒有所需應用程式或平台角色的

使用者無法存取相應的應用程式。

應用程式角色	職責
"Google Cloud NetApp Volumes管理員"	具有Google Cloud NetApp Volumes角色的使用者可以發現和管理Google Cloud NetApp Volumes。
"Google Cloud NetApp Volumes檢視器"	具有Google Cloud NetApp Volumes使用者角色的使用者可以查看Google Cloud NetApp Volumes。
"Keystone管理員"	具有Keystone管理員角色的使用者可以建立服務請求。允許使用者監控和查看他們正在存取的Keystone租戶內的使用情況、資源和管理詳細資訊。
"Keystone檢視器"	具有Keystone檢視者角色的使用者不能建立服務請求。允許使用者監控和查看他們正在存取的Keystone租戶內的消費、資產和管理資訊。
ONTAP調解器設定角色	具有ONTAP調解器設定角色的服務帳戶可以建立服務請求。服務帳戶中需要此角色來配置"ONTAP雲端調解器"。
"營運支援分析師"	提供對警報和監控工具的存取以及輸入和管理支援案例的能力。
"儲存管理員"	管理儲存健康和治理功能，發現儲存資源，以及修改和刪除現有系統。
"儲存檢視器"	查看儲存健康和治理功能，以及查看先前發現的儲存資源。無法發現、修改或刪除現有的儲存系統。
"系統健康專家"	管理儲存和健康和治理功能，儲存管理員的所有權限，但不能修改或刪除現有系統。

數據服務角色

以下是資料服務類別中的角色清單。每個角色在其指定範圍內授予特定的權限。沒有所需資料服務角色或平台角色的使用者將無法存取資料服務。

數據服務角色	職責
"備份和恢復超級管理員"	在NetApp Backup and Recovery中執行任何操作。
"備份和復原管理員"	執行本機快照備份、複製到二級儲存以及備份到物件儲存。
"備份和還原復原管理員"	恢復備份和復原中的工作負載。
"備份和還原克隆管理員"	在備份和復原中克隆應用程式和資料。
"備份和還原檢視器"	查看備份和復原資訊。
"災難復原管理員"	在NetApp Disaster Recovery服務中執行任何操作。
"災難復原故障轉移管理員"	執行故障轉移和遷移。
"災難復原應用程式管理員"	建立複製計劃、變更複製計劃並啟動測試故障轉移。
"災難復原檢視器"	僅查看資訊。
分類檢視器	允許使用者查看NetApp Data Classification掃描結果。具有此角色的使用者可以查看合規性資訊並產生他們有權存取的資源的報告。這些使用者無法啟用或停用磁碟區、儲存桶或資料庫模式的掃描。分類功能沒有管理員角色。
"勒索軟體抵禦能力管理員"	管理NetApp Ransomware Resilience的「保護」、「警報」、「復原」、「設定」和「報告」標籤上的操作。

數據服務角色	職責
"勒索軟體復原力檢視器"	在 Ransomware Resilience 中查看工作負載資料、查看警報資料、下載復原資料和下載報告。
"勒索軟體復原力用戶行為管理員"	在勒索軟體復原中設定、管理和查看可疑使用者行為偵測、警報和監控。
"勒索軟體恢復用戶行為檢視器"	查看勒索軟體復原中的可疑使用者行為警報和見解。
SnapCenter管理員	提供使用NetApp Backup and Recovery從本機ONTAP叢集備份應用程式快照的功能。具有此角色的成員可以完成以下操作：* 從“備份和恢復”>“應用程式”完成任何操作* 管理他們具有權限的項目和資料夾中的所有系統* 使用所有NetApp Console服務SnapCenter沒有查看者角色。

相關連結

- "了解NetApp Console身分和存取管理"
- "開始使用NetApp Console IAM"
- "管理NetApp Console成員及其權限"
- "了解NetApp Console IAM 的 API"

NetApp Console平台存取角色

為使用者指派平台角色，以授予管理NetApp Console、指派角色、新增使用者、建立控制台代理程式和管理聯合的權限。

大型跨國組織的組織角色範例

XYZ 公司按地區（北美、歐洲和亞太地區）組織資料儲存訪問，從而提供區域控制和集中監督。

XYZ 公司控制台中的*組織管理員*為每個區域建立一個初始組織和單獨的資料夾。每個區域的*資料夾或專案管理員*在該區域的資料夾中組織專案（及相關資源）。

具有「資料夾或專案管理員」角色的區域管理員透過新增資源和使用者來主動管理他們的資料夾。這些區域管理員還可以新增、刪除或重新命名他們管理的資料夾和項目。*組織管理員*繼承任何新資源的權限，保持整個組織的儲存使用情況的可見性。

在同一個組織內，一名使用者被指派了*共同管理員*角色來管理該組織與其企業 IdP 的聯合。該使用者可以新增或刪除聯合組織，但不能管理組織內的使用者或資源。*組織管理員*為使用者指派*共同檢視者*角色，以檢查聯合狀態並查看聯合組織。

下表列出了每個控制台平台角色可以執行的操作。

組織管理角色

任務	組織管理員	資料夾或專案管理員
創建代理	是的	不
從控制台建立、修改或刪除系統（新增或發現系統）	是的	是的
建立資料夾和項目，包括刪除	是的	不

任務	組織管理員	資料夾或專案管理員
重新命名現有資料夾和項目	是的	是的
分配角色並新增用戶	是的	是的
將資源與資料夾和項目關聯	是的	是的
將代理程式與資料夾和項目關聯	是的	不
從資料夾和項目中刪除代理	是的	不
管理代理程式（編輯證書、設定等）	是的	不
從管理 > 憑證管理憑證	是的	是的
建立、管理和檢視聯合	是的	不
透過控制台註冊支援並提交案例	是的	是的
使用與明確存取角色無關的資料服務	是的	是的
查看審核頁面和通知	是的	是的

聯盟角色

任務	聯盟管理員	聯邦檢視器
創建聯盟	是的	不
驗證域名	是的	不
將網域新增至聯合	是的	不
禁用和刪除聯盟	是的	不
測驗聯盟	是的	不
查看聯盟及其詳細信息	是的	是的

合作夥伴角色

任務	合作夥伴管理員	合作夥伴檢視器
可以建立合作關係	是的	不
為合作夥伴成員指派角色	是的	不
可以為合作關係加入成員	是的	不
可以查看組織合作關係詳細信息	是的	是的

超級管理員和查看者角色

*超級管理員*角色提供管理控制台功能、儲存和資料服務的完全存取權限。這個角色適合那些監督行政和治理的人。相較之下，「超級查看者」角色提供唯讀存取權限，非常適合需要查看資訊而不進行更改的審計員或利害關係人。

組織應謹慎使用*超級管理員*存取權限，以最大限度地降低安全風險並符合最小特權原則。大多數組織應該分配具有必要權限的細粒度角色，以降低風險並提高可審計性。

超級角色範例

ABC 公司擁有一個由五人組成的小團隊，利用NetApp Console進行資料服務和儲存管理。他們沒有分配多個角色，而是將「超級管理員」角色分配給兩名高階團隊成員，由他們負責所有管理任務，包括使用者管理和資源配置。其餘三名團隊成員被分配了*超級查看者*角色，允許他們監控儲存健康和數據服務狀態，但無法修改設定。

角色	繼承的角色
超管理員	• 組織管理員 • 資料夾或專案管理員 • 聯盟管理員 • 合作夥伴管理員 • 勒索軟體抵禦能力管理員 • 災難復原管理員 • 備份超級管理員 • 儲存管理員 • Keystone管理員 • Google Cloud NetApp Volumes管理員
超觀眾	• 組織檢視器 • 聯邦檢視器 • 合作夥伴檢視器 • 勒索軟體復原力檢視器 • 災難復原檢視器 • 備份檢視器 • 儲存檢視器 • Keystone檢視器 • Google Cloud NetApp Volumes檢視器

應用程式角色

NetApp Console中的Google Cloud NetApp Volumes角色

您可以為使用者指派以下角色，以便他們能夠存取NetApp Console中的Google Cloud NetApp Volumes。

Google Cloud NetApp Volumes使用下列角色：

- * Google Cloud NetApp Volumes管理員*：在控制台中發現並管理Google Cloud NetApp Volumes 。
- * Google Cloud NetApp Volumes檢視器*：在控制台中檢視Google Cloud NetApp Volumes 。

NetApp Console中的**Keystone**存取角色

Keystone角色提供對Keystone儀表板的存取權限，並允許使用者查看和管理他們的Keystone訂閱。 Keystone角色有兩種： Keystone管理員和Keystone檢視者。這兩個角色的主要區別在於他們在Keystone中可以採取的行動。 Keystone管理員角色是唯一允許建立服務要求或修改訂閱的角色。

NetApp Console中的**Keystone**角色範例

XYZ 公司有四名來自不同部門的儲存工程師查看Keystone訂閱資訊。雖然所有這些用戶都需要監控Keystone訂閱，但只有團隊負責人才被允許提出服務要求。團隊中的三名成員被賦予 * Keystone查看者* 角色，而團隊負責人被賦予 * Keystone管理員* 角色，以便對公司的服務請求進行控制。

下表列出了每個Keystone角色可以執行的操作。

特徵和動作	**Keystone**管理員	**Keystone**檢視器
查看以下選項卡：訂閱、資產、監控和管理	是的	是的
* Keystone訂閱頁面*：		
查看訂閱	是的	是的
修改或續訂	是的	不
* Keystone資產頁面*：		
查看資產	是的	是的
管理資產	是的	不
* Keystone警報頁面*：		
查看警報	是的	是的
管理警報	是的	不
為自己創建提醒	是的	是的
Licenses and subscriptions：		
可以查看授權和訂閱	是的	是的
* Keystone報告頁面*：		
下載報告	是的	是的
管理報告	是的	是的

特徵和動作	Keystone管理員	Keystone檢視器
為自己建立報告	是的	是的
服務請求：		
建立服務請求	是的	不
查看組織內任何使用者建立的服務請求	是的	是的

NetApp Console的營運支援分析師存取角色

您可以將營運支援分析師角色指派給用戶，以便他們能夠存取警報和監控功能。具有此角色的使用者還可以開啟支援案例。

營運支援分析師

任務	可以執行
從「設定」>「憑證」管理自己的使用者憑證	是的
查看發現的資源	是的
透過控制台註冊支援並提交案例	是的
查看審核頁面和通知	是的
查看、下載和設定警報	是的

NetApp Console的儲存存取角色

您可以為使用者指派以下角色，以便他們存取NetApp Console中的儲存管理功能。您可以為使用者指派管理角色來管理儲存或指派檢視者角色來監控。

NetApp Console合作夥伴 API 不會提供這些角色。

管理員可以為使用者指派以下儲存資源和功能的儲存角色：

儲存資源：

- 本地ONTAP集群
- StorageGRID
- E系列

控制台服務和功能：

- 數位顧問
- 軟體更新

- 生命週期規劃
- 永續性

NetApp Console中的儲存角色範例

XYZ 公司是一家跨國公司，擁有龐大的儲存工程師和儲存管理員團隊。它們允許該團隊管理其所在地區的儲存資產，同時限制對核心控制台任務（如使用者管理、代理建立和許可證管理）的存取。

在一個由 12 人組成的團隊中，有兩名使用者被賦予「儲存檢視者」角色，這使他們能夠監控與他們被分配到的控制台專案相關的儲存資源。其餘九人被賦予*儲存管理員*角色，包括管理軟體更新、透過控制台存取ONTAP系統管理員以及發現儲存資源（新增系統）的能力。團隊中的一名成員被賦予*系統健康專家*角色，以便他們可以管理其所在區域的儲存資源的健康狀況，但不能修改或刪除任何系統。此人還可以對其所分配項目的儲存資源執行軟體更新。

該組織還有兩個具有「組織管理員」角色的用戶，他們可以管理控制台的所有方面，包括用戶管理、代理創建和許可證管理，還有幾個具有「資料夾或專案管理員」角色的用戶，他們可以對分配到的資料夾和專案執行控制台管理任務。

下表顯示了每個儲存角色執行的操作。

特徵和動作	儲存管理員	系統健康專家	儲存檢視器
儲存管理：			
發現新資源（創建系統）	是的	是的	不
查看發現的系統	是的	是的	不
從控制台刪除系統	是的	不	不
修改系統	是的	不	不
建立代理	不	不	不
數位顧問			
查看所有頁面和功能	是的	是的	是的
Licenses and subscriptions			
查看所有頁面和功能	不	不	不
軟體更新			
查看登陸頁面和建議	是的	是的	是的
審查潛在的版本建議和主要優點	是的	是的	是的
查看叢集的更新詳細信息	是的	是的	是的

特徵和動作	儲存管理員	系統健康專家	儲存檢視器
執行更新前檢查並下載升級計劃	是的	是的	是的
安裝軟體更新	是的	是的	不
生命週期規劃			
審查容量規劃狀態	是的	是的	是的
選擇下一步行動（最佳實踐、層級）	是的	不	不
將冷數據分層到雲端儲存並釋放儲存空間	是的	是的	不
設定提醒	是的	是的	是的
永續性			
查看儀表板和建議	是的	是的	是的
下載報告數據	是的	是的	是的
編輯碳減排百分比	是的	是的	不
修復建議	是的	是的	不
延後建議	是的	是的	不
系統管理員存取			
可以輸入憑證	是的	是的	不
證書			
使用者憑證	是的	是的	不

數據服務角色

NetApp Console中的NetApp Backup and Recovery角色

您可以為使用者指派以下角色，以便他們存取控制台內的NetApp Backup and Recovery。備份和復原角色可讓您靈活地為使用者指派特定於他們需要在組織內完成的任務的角色。如何分配角色取決於您自己的業務和儲存管理實踐。

該服務使用特定於NetApp Backup and Recovery 的以下角色。

- 備份和還原超級管理員：在NetApp Backup and Recovery中執行任何操作。

- 備份和還原備份管理員：在NetApp Backup and Recovery中執行備份到本機快照、複製到二級儲存以及備份到物件儲存作業。
- 備份和還原復原管理員：使用NetApp Backup and Recovery復原工作負載。
- 備份和還原克隆管理：使用NetApp Backup and Recovery應用程式和資料。
- 備份和還原檢視器：查看NetApp Backup and Recovery中的信息，但不執行任何操作。

有關所有NetApp Console訪問角色的詳細信息，請參閱 "控制台設定和管理文檔"。

用於常見操作的角色

下表列出了每個NetApp Backup and Recovery角色可以針對所有工作負載執行的操作。

特徵和動作	備份和恢復超級管理員	備份和還原備份管理員	備份和還原復原管理員	備份和還原克隆管理員	備份和還原檢視器
新增、編輯或刪除主機	是的	不	不	不	不
安裝插件	是的	不	不	不	不
新增憑證（主機、實例、vCenter）	是的	不	不	不	不
查看儀表板和所有選項卡	是的	是的	是的	是的	是的
開始免費試用	是的	不	不	不	不
啟動工作負載發現	不	是的	是的	是的	不
查看許可證資訊	是的	是的	是的	是的	是的
啟動許可證	是的	不	不	不	不
查看主機	是的	是的	是的	是的	是的
時間表：					
啟動計劃	是的	是的	是的	是的	不
暫停時間表	是的	是的	是的	是的	不
政策與保護：					
查看保護計劃	是的	是的	是的	是的	是的
建立、修改或刪除保護計劃	是的	是的	不	不	不

特徵和動作	備份和恢復超級管理員	備份和還原備份管理員	備份和還原復原管理員	備份和還原克隆管理員	備份和還原檢視器
恢復工作負載	是的	不	是的	不	不
建立、拆分或刪除克隆	是的	不	不	是的	不
建立、修改或刪除策略	是的	是的	不	不	不
報告：					
查看報告	是的	是的	是的	是的	是的
建立報告	是的	是的	是的	是的	不
刪除報告	是的	不	不	不	不
從**SnapCenter**匯入並管理主機：					
查看導入的SnapCenter數據	是的	是的	是的	是的	是的
從SnapCenter匯入數據	是的	是的	不	不	不
管理（遷移）主機	是的	是的	不	不	不
配置設定：					
配置日誌目錄	是的	是的	是的	不	不
關聯或刪除實例憑證	是的	是的	是的	不	不
桶：					
查看儲存桶	是的	是的	是的	是的	是的
建立、編輯或刪除儲存桶	是的	是的	不	不	不

用於特定於工作負載的操作的角色

下表列出了每個NetApp Backup and Recovery角色可以針對特定工作負載執行的動作。

Kubernetes 工作負載

此表顯示了每個NetApp Backup and Recovery角色可以針對特定於 Kubernetes 工作負載的操作執行的操作。

特徵和動作	備份和恢復超級管理員	備份和還原備份管理員	備份和還原復原管理員	備份和還原檢視器
查看叢集、命名空間、儲存類別和 API 資源	是的	是的	是的	是的
新增的 Kubernetes 集群	是的	是的	不	不
更新叢集配置	是的	不	不	不
從管理中刪除集群	是的	不	不	不
查看應用程式	是的	是的	是的	是的
建立和定義新的應用程式	是的	是的	不	不
更新應用程式配置	是的	是的	不	不
從管理中刪除應用程式	是的	是的	不	不
查看受保護的資源和備份狀態	是的	是的	是的	是的
建立備份並使用策略保護應用程式	是的	是的	不	不
取消保護應用程式並刪除備份	是的	是的	不	不
查看恢復點和資源檢視器結果	是的	是的	是的	是的
從復原點還原應用程式	是的	不	是的	不
查看 Kubernetes 備份策略	是的	是的	是的	是的
建立 Kubernetes 備份策略	是的	是的	是的	不
更新備份策略	是的	是的	是的	不
刪除備份策略	是的	是的	是的	不
查看執行鉤子和鉤子來源	是的	是的	是的	是的
建立執行鉤子和鉤子來源	是的	是的	是的	不
更新執行鉤子和鉤子來源	是的	是的	是的	不

特徵和動作	備份和恢復超級管理員	備份和還原備份管理員	備份和還原復原管理員	備份和還原檢視器
刪除執行鉤子和鉤子來源	是的	是的	是的	不
查看執行鉤子模板	是的	是的	是的	是的
建立執行鉤子模板	是的	是的	是的	不
更新執行鉤子模板	是的	是的	是的	不
刪除執行鉤子模板	是的	是的	是的	不
查看工作負載摘要和分析儀表板	是的	是的	是的	是的
查看StorageGRID儲存桶和儲存目標	是的	是的	是的	是的

NetApp Console中的**NetApp Disaster Recovery**角色

您可以為使用者指派以下角色，以便他們存取控制台內的NetApp Disaster Recovery。災難復原角色可讓您靈活地為使用者指派特定於他們需要在組織內完成的任務的角色。如何分配角色取決於您自己的業務和儲存管理實踐。

災難復原使用以下角色：

- 災難復原管理員：執行任何動作。
- 災難復原故障轉移管理：執行故障轉移和遷移。
- 災難復原應用程式管理員：建立複製計劃。修改複製計劃。開始測試故障轉移。
- 災難復原檢視器：僅查看資訊。

下表列出了每個角色可以執行的操作。

特徵和動作	災難復原管理員	災難復原故障轉移管理員	災難復原應用程式管理員	災難復原檢視器
查看儀表板和所有選項卡	是的	是的	是的	是的
開始免費試用	是的	不	不	不
啟動工作負載發現	是的	不	不	不
查看許可證資訊	是的	是的	是的	是的
啟動許可證	是的	不	是的	不

特徵和動作	災難復原管理員	災難復原故障轉移管理員	災難復原應用程式管理員	災難復原檢視器
在「網站」標籤上：				
查看網站	是的	是的	是的	是的
新增、修改或刪除站點	是的	不	不	不
在複製計劃標籤上：				
查看複製計劃	是的	是的	是的	是的
查看複製計劃詳細信息	是的	是的	是的	是的
建立或修改複製計劃	是的	是的	是的	不
建立報告	是的	不	不	不
查看快照	是的	是的	是的	是的
執行故障轉移測試	是的	是的	是的	不
執行故障轉移	是的	是的	不	不
執行故障回復	是的	是的	不	不
執行遷移	是的	是的	不	不
在資源組標籤上：				
查看資源組	是的	是的	是的	是的
建立、修改或刪除資源組	是的	不	是的	不
在「作業監控」標籤上：				
查看職位	是的	不	是的	是的
取消作業	是的	是的	是的	不

NetApp Console的勒索軟體恢復存取角色

勒索軟體復原角色為使用者提供對NetApp Ransomware Resilience的存取權限。勒索軟體復原能力支援以下角色：

基線角色

- 勒索軟體復原管理員 - 配置勒索軟體復原設定；調查並回應加密警報
- 勒索軟體復原力檢視器 - 查看加密事件、報告和發現設置

使用者行為活動角色"可疑用戶活動偵測"警報提供對檔案活動事件等資料的可見性；這些警報包括檔案名稱和使用者執行的檔案操作（例如讀取、寫入、刪除、重新命名）。為了限制這些資料的可見性，只有具有這些角色的使用者才能管理或查看這些警報。

- 勒索軟體恢復用戶行為管理員 - 啟動可疑用戶活動檢測，調查並響應可疑用戶活動警報
- 勒索軟體恢復用戶行為檢視器 - 查看可疑用戶活動警報

使用者行為角色不是獨立角色；它們旨在添加到勒索軟體復原管理員或查看者角色中。有關詳細信息，請參閱 [使用者行為角色]。

有關每個角色的詳細描述，請參閱下表。

基線角色

下表描述了勒索軟體復原管理員和檢視者角色可執行的操作。

特徵和動作	勒索軟體抵禦能力管理員	勒索軟體復原力檢視器
查看儀表板和所有選項卡	是的	是的
在儀表板上更新推薦狀態	是的	不
開始免費試用	是的	不
啟動工作負載發現	是的	不
啟動工作負載的重新發現	是的	不
在「保護」標籤上：		
新增、修改或刪除加密策略的保護計劃	是的	不
保護工作負載	是的	不
透過資料分類識別敏感資料的暴露	是的	不
列出保護計劃和細節	是的	是的
列出保護組	是的	是的
查看保護組詳細信息	是的	是的
建立、編輯或刪除保護群組	是的	不

特徵和動作	勒索軟體抵禦能力管理員	勒索軟體復原力檢視器
下載數據	是的	是的
在「警報」標籤上：		
查看加密警報和警報詳細信息	是的	是的
編輯加密事件狀態	是的	不
標記加密警報以供恢復	是的	不
查看加密事件詳細信息	是的	是的
解除或解決加密事件	是的	不
取得加密事件中受影響文件的完整列表	是的	不
下載加密事件警報數據	是的	是的
封鎖使用者（使用工作負載安全代理程式配置）	是的	不
在「恢復」標籤上：		
下載加密事件中受影響的文件	是的	不
從加密事件中恢復工作負載	是的	不
從加密事件下載恢復數據	是的	是的
下載加密事件報告	是的	是的
在「設定」標籤上：		
新增或修改備份目標	是的	不
列出備份目的地	是的	是的
查看已連接的 SIEM 目標	是的	是的
新增或修改 SIEM 目標	是的	不
配置準備演練	是的	不
開始、重置或編輯準備情況演練	是的	不

特徵和動作	勒索軟體抵禦能力管理員	勒索軟體復原力檢視器
審查準備演習狀態	是的	是的
更新發現配置	是的	不
查看發現配置	是的	是的
在「報告」標籤上：		
下載報告	是的	是的

使用者行為角色

若要配置可疑使用者行為設定並回應警報，使用者必須具有勒索軟體復原使用者行為管理員角色。要僅查看可疑用戶行為警報，用戶應具有勒索軟體恢復用戶行為查看者角色。

應將使用者行為角色授予具有現有勒索軟體復原管理員或檢視者權限且需要存取"可疑用戶活動設定和警報"。例如，具有勒索軟體復原管理員角色的使用者應該獲得勒索軟體復原使用者行為管理員角色來配置使用者活動代理並封鎖或解除封鎖使用者。不應將勒索軟體復原使用者行為管理員角色授予勒索軟體復原檢視者。

若要啟動可疑使用者活動偵測，您必須具有控制台組織管理員角色。

下表描述了勒索軟體復原使用者行為管理員和檢視者角色可執行的操作。

特徵和動作	勒索軟體復原力用戶行為管理員	勒索軟體恢復用戶行為檢視器
在「設定」標籤上：		
建立、修改或刪除用戶活動代理	是的	不
建立或刪除使用者目錄連接器	是的	不
暫停或恢復資料收集器	是的	不
進行資料外洩準備演習	是的	不
在「保護」標籤上：		
新增、修改或刪除可疑使用者行為策略的保護計劃	是的	不
在「警報」標籤上：		
查看用戶活動警報和警報詳細信息	是的	是的
編輯使用者活動事件狀態	是的	不

特徵和動作	勒索軟體復原力用戶行為管理員	勒索軟體恢復用戶行為檢視器
標記用戶活動警報以供恢復	是的	不
查看用戶活動事件詳細信息	是的	是的
解除或解決使用者活動事件	是的	不
取得可疑使用者受影響文件的完整列表	是的	是的
下載用戶活動事件警報數據	是的	是的
封鎖或取消封鎖用戶	是的	不
在「恢復」標籤上：		
下載使用者活動事件受影響的文件	是的	不
從使用者活動事件恢復工作負載	是的	不
從用戶活動事件下載恢復數據	是的	是的
從用戶活動事件下載報告	是的	是的

身分和存取 API

組織和專案 ID

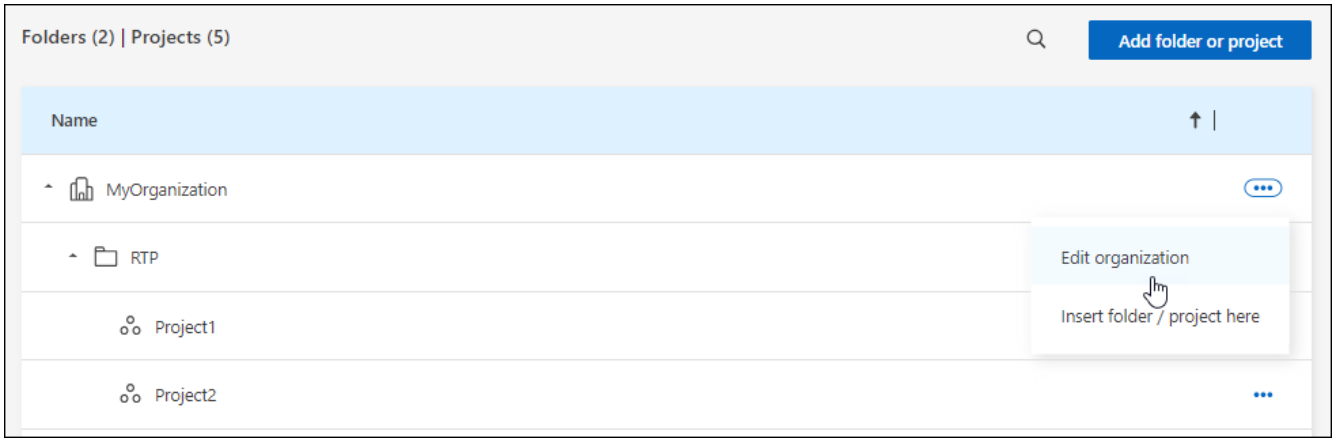
您的NetApp Console組織有一個名稱和一個 ID。您可以為您的組織選擇一個名稱以幫助識別它。您可能還需要檢索某些整合的組織 ID。

重新命名您的組織

您可以重新命名您的組織。如果您支持的不僅僅是組織，這將很有幫助。

步驟

1. 選擇*管理>身分和存取*。
2. 選擇*組織*。
3. 從「組織」頁面，導覽至表格的第一行，選擇 ... 然後選擇*編輯組織*。



4. 輸入新的組織名稱並選擇*套用*。

取得組織 ID

組織 ID 用於與控制台的某些整合。

您可以從組織頁面查看組織 ID，並根據需要將其複製到剪貼簿。

步驟

1. 選擇*管理>身分和存取*>*組織*。
2. 在*組織*頁面上，在摘要欄中尋找您的組織 ID 並將其複製到剪貼簿。您可以保存它以供以後使用，或直接將其複製到需要使用它的地方。

取得專案ID

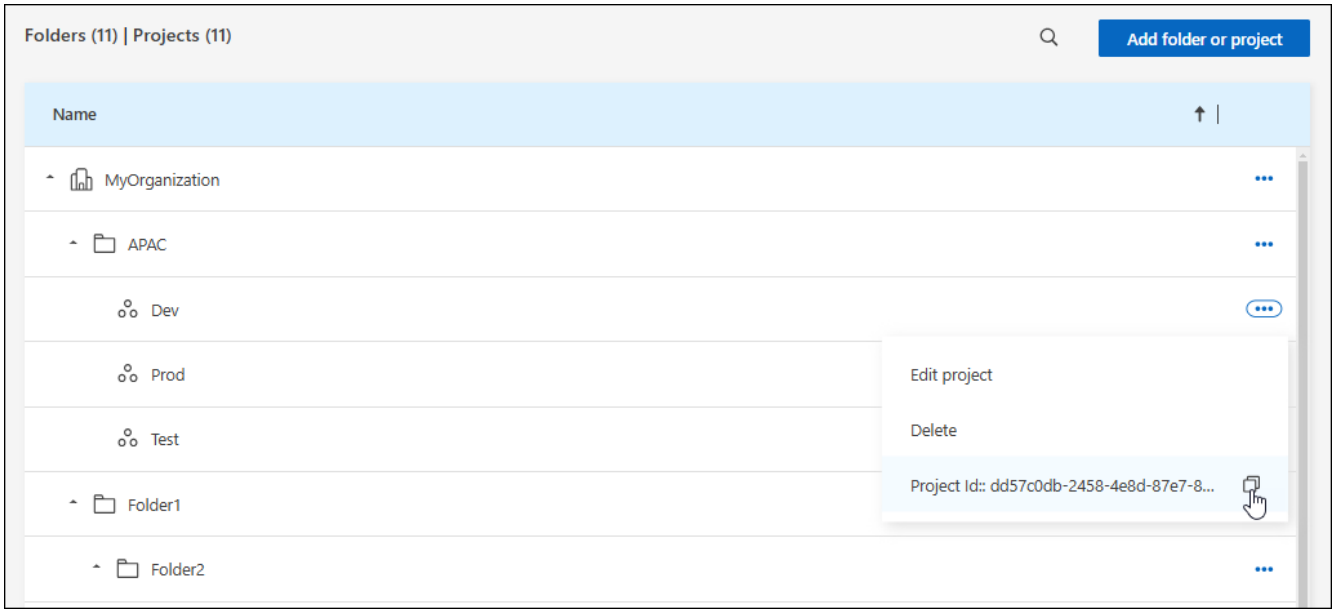
如果您使用 API，則需要取得項目的 ID。例如，在建立Cloud Volumes ONTAP系統時。

步驟

1. 從“組織”頁面，導航到表中的項目並選擇 •••

   顯示項目 ID。

2. 若要複製 ID，請選擇複製按鈕。



相關資訊

- "了解身分和存取管理"
- "開始使用身分和存取權限"
- "了解身分和存取 API"