



UNIX版的存取控制SnapDrive

Snapdrive for Unix

NetApp
October 04, 2023

This PDF was generated from https://docs.netapp.com/zh-tw/snapdrive-unix/aix/concept_what_access_control_settings_are.html on October 04, 2023. Always check docs.netapp.com for the latest.

目錄

UNIX版的存取控制SnapDrive	1
什麼是存取控制設定	1
可用的存取控制層級	2
設定存取控制權限	2
檢視存取控制權限	3

UNIX版的存取控制SnapDrive

適用於UNIX的支援功能可讓您控制每個主機對主機所連接之每個儲存系統的存取層級。SnapDrive

UNIX版的存取層級SnapDrive 指出當主機鎖定特定儲存系統時、允許執行哪些作業。除了show和list作業之外、存取控制權限可能會影響所有Snapshot和儲存作業。

什麼是存取控制設定

為了判斷使用者存取權、SnapDrive UNIX版的程式碼會檢查儲存系統根磁碟區中兩個權限檔案的其中一個。您必須檢查這些檔案中設定的規則、才能評估存取控制。

- 「DHost-name.prbac」檔案位於目錄「/vol/vol0/sdprbac」SnapDrive（以角色為基礎的存取控制權限）中。

檔案名稱「shDhost-name.prbac」、其中「*host-name*」是權限套用的主機名稱。您可以為附加至儲存系統的每個主機設定權限檔案。您可以使用「SnapDrive 效能分析存取」命令來顯示特定儲存系統上主機可用權限的相關資訊。

如果不存在「shdHost-name.prbac」、請使用「shdsgeneric.prbac」檔案來檢查存取權限。

- 「dsgeneric.prbac」檔案也位於目錄「/vol/vol0/sdprbac」中。

檔案名稱「shdgeneric.prbac」是儲存系統上無法存取「shidhost-name.prbac」檔案的多個主機的預設存取設定。

如果您在「/vol/vol0/sdprbac」路徑中同時有「shdHost-name.prbac」和「shdgeneric.prbac」檔案、請使用「shdHost-name.prbac」來檢查存取權限、因為這會覆寫為「shdgeneric.prbac」檔案提供的值。

如果您沒有「shDhost-name.prbac」和「shdgeneric.prbac」檔案、請檢查在「snapdrive.conf」檔案中定義的組態變數「_all-access-if-RBAC未指定」。

從特定主機設定存取控制至特定vFiler單元、是一項手動操作。來自特定主機的存取權是由位於受影響vFiler單元根Volume中的檔案所控制。檔案包含「/vol/<vFilerroot vole>/sdprbac/sdhost-name.prbac」、其中「*host-name*」是受影響主機的名稱、由「gethostname (3)」傳回。您應確保此檔案可從可存取的主機讀取、但不可寫入。



若要判斷主機名稱、請執行「主機名稱」命令。

如果檔案是空的、無法讀取的或格式無效、SnapDrive 則UNIX版的for不會授予主機任何作業的存取權。

如果檔案遺失、SnapDrive UNIX版的Sfesfing會在「snapdrive.conf」檔案中檢查組態變數「_all-access-if-RBAC未指定」。如果變數設為「On」（開啟）（預設值）、則可讓主機完整存取該儲存系統上的所有這些作業。如果變數設為「Off」（關閉）、SnapDrive 則UNIX版的還原功能會拒絕主機執行該儲存系統存取控制所管理的任何作業權限。

可用的存取控制層級

適用於UNIX的支援為使用者提供各種存取控制層級。SnapDrive這些存取層級與Snapshot複本和儲存系統作業有關。

您可以設定下列存取層級：

- 無：主機無法存取儲存系統。
- Snapcreate：主機可以建立Snapshot複本。
- SnapUse（快照使用）-主機可以刪除並重新命名Snapshot複本。
- Snapall：主機可以建立、還原、刪除及重新命名Snapshot複本。
- Storage create DELETE（儲存設備建立刪除）：主機可以建立、調整大小及刪除儲存設備。
- 儲存設備用途：主機可連接和中斷儲存設備連線、也可在儲存設備上執行實體複本分割預估和實體複本分割。
- 儲存設備：主機可建立、刪除、連線及中斷儲存設備連線、也可在儲存設備上執行實體複本分割預估和實體複本分割。
- All access-主機可存取上述SnapDrive 所有的UNIX作業。

每個層級都是不同的。如果您只指定特定作業的權限、SnapDrive 則適用於UNIX的功能僅能執行這些作業。例如、如果您指定使用儲存設備、主機可以使用SnapDrive UNIX版的支援功能來連線和中斷儲存設備連線、但它無法執行其他任何受存取控制權限管理的作業。

設定存取控制權限

您可以SnapDrive 在儲存系統的根Volume中建立特殊目錄和檔案、以設定UNIX版的存取控制權限。

請確定您以root使用者身分登入。

步驟

1. 在目標儲存系統的根磁碟區中建立目錄「shdprbac」。

讓根磁碟區存取的方法之一、是使用NFS掛載磁碟區。

2. 在「shdprbac」目錄中建立權限檔案。請確認下列陳述正確無誤：
 - 檔案必須命名為「shDhost-name.prbac」、其中host-name是您指定存取權限的主機名稱。
 - 檔案必須是唯讀的、才能確保SnapDrive UNIX版的功能能夠讀取、但無法修改。

若要授予名為dev-sun1的主機存取權限、您可以在儲存系統上建立下列檔案：
：「/vol/vol1/sdprbac/sddev-sun1.prbac」

3. 在該主機的檔案中設定權限。

您必須針對檔案使用下列格式：

- 您只能指定一層權限。若要讓主機完整存取所有作業、請輸入字串all存取。
- 權限字串必須是檔案中的第一件事。如果權限字串不在第一行中、則檔案格式無效。
- 權限字串不區分大小寫。
- 權限字串前面不得有空格。
- 不允許任何意見。

這些有效的權限字串允許下列存取層級：

- 無：主機無法存取儲存系統。
- Snapcreate：主機可以建立Snapshot複本。
- SnapUse（快照使用）-主機可以刪除並重新命名Snapshot複本。
- Snapall：主機可以建立、還原、刪除及重新命名Snapshot複本。
- Storage create DELETE（儲存設備建立刪除）：主機可以建立、調整大小及刪除儲存設備。
- 儲存設備用途：主機可連接和中斷儲存設備連線、也可在儲存設備上執行實體複本分割預估和實體複本分割。
- 儲存設備：主機可建立、刪除、連線及中斷儲存設備連線、也可在儲存設備上執行實體複本分割預估和實體複本分割。
- All access-主機可存取上述SnapDrive 所有的UNIX作業。每個權限字串都是獨立的。如果您指定SnapUse、主機可以刪除或重新命名Snapshot複本、但無法建立Snapshot複本、或還原或執行任何儲存資源配置作業。

無論您設定的權限為何、主機都能執行show和list作業。

4. 輸入下列命令來驗證存取權限：

「* SnapDrive 」此功能可存取show *filer_name**

檢視存取控制權限

您可以執行「SnapDrive View config access show」命令來檢視存取控制權限。

步驟

1. 執行「SnapDrive 效能分析存取show」命令。

此命令的格式如下：SnapDrive 「不完整組態存取 {show | list} filename」

無論您輸入命令的「顯示」或「清單」版本、都可以使用相同的參數。

此命令列會檢查儲存系統快照通知、以判斷主機擁有哪些權限。根據輸出結果、此儲存系統上主機的權限會全部快照。

```
# snapdrive config access show toaster
This host has the following access permission to filer, toaster:
SNAP ALL
Commands allowed:
snap create
snap restore
snap delete
snap rename
#
```

在此範例中、權限檔案不在儲存系統上、SnapDrive 所以針對UNIX而言、將檢查「snapdrive.conf」檔案中的變數「_all-access-if-RBAC未指定」、以判斷主機擁有哪些權限。此變數設為「開啟」、相當於建立權限檔案、並將存取層級設為「所有存取」。

```
# snapdrive config access list toaster
This host has the following access permission to filer, toaster:
ALL ACCESS
Commands allowed:
snap create
snap restore
snap delete
snap rename
storage create
storage resize
snap connect
storage connect
storage delete
snap disconnect
storage disconnect
clone split estimate
clone split start
#
```

此範例顯示如果儲存系統快顯通知中沒有權限檔案、您會收到的訊息類型、而在「snapdrive.conf」檔案中的變數「_all-access-if-RBAC未指定」會設為「Off」。

```
# snapdrive config access list toaster
Unable to read the access permission file on filer, toaster. Verify that
the
file is present.
Granting no permissions to filer, toaster.
```

版權資訊

Copyright © 2023 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。