UNIX的安全功能SnapDrive

Snapdrive for Unix

NetApp
October 04, 2023

目錄

UNIX的安全功能SnapDrive

在使用SnapDrive 適用於UNIX的功能之前、您必須先瞭解其安全功能、並瞭解如何存取這些功能。

什麼是安全功能

適用於UNIX的支援功能可讓您更安全地使用。SnapDrive這些功能可讓您更有效地控制哪些使用者可以在儲存系統上執行作業、以及從哪個主機執行作業。

安全功能可讓您執行下列工作：

- 設定存取控制權限
- 指定儲存系統的登入資訊
- 指定SnapDrive UNIX版的支援使用HTTPS

存取控制功能可讓您指定執行SnapDrive 支援UNIX的主機可在儲存系統上執行哪些作業。您可以分別為每個主機設定這些權限。此外、為了讓SnapDrive UNIX的功能能夠存取儲存系統、您必須提供該儲存系統的登入名稱和密碼。

HTTPS功能可讓您透過管理ONTAP 支援介面、指定所有與儲存系統互動的SSL加密、包括傳送密碼。此行為是SnapDrive UNIX版的預設功能、而AIX版的更新版本則是預設功能；不過、您可以將「use－https－to－filer」組態變數的值變更為「Off（關）」、以停用SSL加密。

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。

  檔案名稱為「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「shedgeneric.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。

     若要授予名稱為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顯通知、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.
```

儲存系統的登入資訊

使用者名稱或密碼可讓SnapDrive UNIX使用者存取每個儲存系統。它也提供安全性、因為除了以root身分登入、執行SnapDrive UNIX的人員必須在系統提示時提供正確的使用者名稱或密碼。如果登入遭到入侵、您可以刪除登入並設定新的使用者登入。

您在設定每個儲存系統時、都已建立使用者登入。若要讓UNIX與儲存系統搭配使用、您必須提供此登入資訊。SnapDrive根據您在設定儲存系統時所指定的內容、每個儲存系統都可以使用相同的登入或獨特的登入。

適用於UNIX的支援將這些登入和密碼以加密形式儲存在每個主機上。SnapDrive您可以SnapDrive 設定「*SnapDrive*、*conf*」組態變數「*use-https*到*filer=on*」、指定當與儲存系統通訊時、UNIX版的Sfor UNIX會加密此資訊。

指定登入資訊

您必須指定儲存系統的使用者登入資訊。視您設定儲存系統時所指定的內容而定、每個儲

存系統可使用相同的使用者名稱或密碼、或是唯一的使用者名稱或密碼。如果所有儲存系統都使用相同的使用者名稱或密碼資訊、您必須執行下列步驟一次。如果儲存系統使用獨特的使用者名稱或密碼、您必須針對每個儲存系統重複下列步驟。

請確定您以root使用者身分登入。

步驟

1. 輸入下列命令：

   「* SnapDrive 組態集_user_name filename_[*filename…*]*」

   「*user_name*」是您第一次設定儲存系統時所指定的使用者名稱。

   「*filename*」是儲存系統的名稱。

   「*[filename…]*」定義如果所有儲存系統名稱都有相同的使用者登入或密碼、您可以在單一命令列上輸入多個儲存系統名稱。您必須輸入至少一個儲存系統的名稱。

2. 出現提示時、輸入密碼（如果有）。

   > 如果未設定密碼、請在提示輸入密碼時按Enter（null值）。

   此範例為名為「root」的儲存系統設定使用者名稱、稱為「快顯通知」：

   ```
   # snapdrive config set `root` toaster
   Password for root:
   Retype Password:
   ```

   本範例針對三個儲存系統設定一個名為「root」的使用者：

   ```
   # snapdrive config set root toaster oven broiler
   Password for root:
   Retype Password:
   ```

3. 如果您有另一個儲存系統的使用者名稱或密碼不同、請重複這些步驟。

驗證與**SnapDrive UNIX**版的功能相關聯的儲存系統使用者名稱

您可以執行「組態清單」命令、驗證SnapDrive UNIX的使用者名稱哪些與儲存系統相關聯SnapDrive 。

您必須以root使用者的身分登入。

步驟

1. 輸入下列命令：

‘* SnapDrive 組態清單*’

此命令會顯示SnapDrive 所有系統的使用者名稱或儲存系統配對、這些系統的使用者均在適用於UNIX的範圍內指定。它不會顯示儲存系統的密碼。

此範例顯示與名為rapunzel與中型儲存系統相關的使用者：

```
# snapdrive config list
user name           storage system name
-----------------------------
rumplestiltskins    rapunzel
longuser            mediumstoragesystem
```

刪除儲存系統的使用者登入資訊

您可以執行「SnapDrive show config delete」命令、刪除一或多個儲存系統的使用者登入資訊。

請確定您以root使用者身分登入。

步驟

1. 輸入下列命令：

   「* SnapDrive 」此為組態刪除_applie_name [applie_name]_*

   「*applete_name*」是您要刪除使用者登入資訊的儲存系統名稱。

   適用於UNIX的解決方法會移除您指定儲存系統的使用者名稱或密碼登入資訊。SnapDrive

   若要讓SnapDrive UNIX版的支援功能存取儲存系統、您必須指定新的使用者登入資訊。

設定HTTP

您可以設定SnapDrive UNIX版的支援功能、將HTTP用於您的主機平台。

請確定您以root使用者身分登入。

步驟

1. 備份「snapdrive.conf」檔案。
2. 在文字編輯器中開啟「snapdrive.conf」檔案。
3. 將'*US-https-to -filer*'變數的值變更為「Off」。

   修改「snapdrive.conf」檔案的最佳做法是執行下列步驟：

   a. 註釋掉您要修改的行。

b. 複製註解輸出行。

c. 移除井號（#）、取消註釋複製的文字。

d. 修改值。

4. 變更後儲存檔案。

   UNIX版的還原功能會在每次啟動時自動檢查此檔案。SnapDrive您必須重新啟動SnapDrive UNIX版的功能、變更才會生效。