



在SnapDrive UNIX版的不適用功能組態中設定角色型存取控制

Snapdrive for Unix

NetApp
October 04, 2023

目錄

在SnapDrive UNIX版的不適用功能組態中設定角色型存取控制	1
在Operations Manager主控台設定SD-admin	1
將SD-HostName新增至儲存系統	2
在SnapDrive UNIX版的使用者認證上設定使用者認證	3
使用Operations Manager主控台執行存取檢查的使用者名稱格式	4
角色型存取控制的組態變數	4

在SnapDrive UNIX版的不適用功能組態中設定角色型存取控制

您必須完成各種工作、才能設定角色型存取控制（RBAC） SnapDrive 以供UNIX使用。您可以使用Operations Manager主控台或命令列介面來執行工作。

在Operations Manager主控台設定SD-admin

Operations Manager主控台管理員可建立SD-admin使用者。

Operations Manager主控台管理員會建立名為SD-admin的使用者、並能在全域群組（全域「Dfm.Core.AccessCheck」）上執行核心存取檢查。Operations Manager主控台管理員設定SD-admin使用者之後、您必須手動將認證資訊傳送SnapDrive 給UNIX管理員的地方。如需使用Operations Manager主控台設定使用者和角色的詳細資訊、請參閱_Operations Manager主控台管理指南_和線上說明。



您可以使用任何名稱來取代SD-admin、不過最好使用SD-admin。

若要在Operations Manager主控台中建立角色、請選取*設定*>*角色*。在SD-admin組態頁面中、Operations Manager主控台管理員必須將全域群組上的「Dfm.Database.Write」功能指派給SD-admin-role、SnapDrive 以便UNIX版的Sfor UNIX能在Operations Manager主控台中重新整理儲存實體。

使用命令列介面設定SD-admin

儲存系統管理員可使用命令列介面來設定SD-admin使用者。

步驟

1. 新增名為SD-admin的使用者。

```
# useradd sd-admin
```

```
# passwd sd-admin
Changing password for sd-admin.
New password:
Re-enter new password:
Password changed
```

2. 新增名為SD-admin的系統管理員。

```
# dfm user add sd-admin
Added administrator sd-admin.
```

3. 建立名為SD-admin-role的角色。

```
# dfm role create sd-admin-role
Created role sd-admin-role.
```

4. 新增功能至步驟3所建立的角色。

```
# dfm role add sd-admin-role DFM.Core.AccessCheck Global
Added 1 capability to role sd-admin-role.
```

5. Operations Manager管理員也可以將全域群組的「Dfm.Database.Write」功能授予「<sd-admin>」、讓SnapDrive UNIX的支援功能在Operations Manager中重新整理儲存系統實體。

```
# dfm role add sd-admin-role DFM.Database.Write Global
Added 1 capability to role sd-admin-role.
```

6. 將SD-admin-role角色新增至SD-admin使用者。

```
# dfm user role set sd-admin sd-admin-role
Set 1 role for administrator sd-admin.
```

將SD-HostName新增至儲存系統

Operations Manager主控台管理員可使用Operations Manager主控台、在儲存系統上建立SD-hostname使用者。完成這些步驟之後、Operations Manager主控台管理員必須手動將認證資料傳送SnapDrive 給UNIX管理員。您可以使用任何名稱來取代SD-hostname;不過最好使用SD-hostname。

步驟

1. 取得儲存系統的root密碼並儲存密碼。

若要新增儲存系統的密碼、請選取*管理*>*儲存系統*。

2. 為每個UNIX系統建立SD-HostName使用者。
3. 將「API-」和「login-」功能指派給SD角色等角色。
4. 將此角色（SD-role）納入新的使用者群組、例如SD-usergroup。
5. 將此使用者群組（SD-usergroup）與儲存系統上的SD主機名稱使用者建立關聯。

使用CLI將SD-主機名稱新增至儲存系統

儲存系統管理員可以使用useradmin命令來建立及設定SD-hostname使用者。

步驟

1. 新增儲存設備。

```
# dfm host add storage_array1
Added host storage_array1.lab.eng.btc.xyz.in
```

2. 設定主機的密碼。

```
# dfm host password save -u root -p xxxxxxxx storage_array1
Changed login for host storage_array1.lab.eng.btc.xyz.in to root.
Changed Password for host storage_array1.lab.eng.btc.xyz.in to
xxxxxxx
.in
```

3. 在主機上建立角色。

```
# dfm host role create -h storage_array1 -c "api-*,login-*" sd-unixhost-
role
Created role sd-unixhost-role on storage_array1
```

4. 建立使用者群組。

```
# dfm host usergroup create -h storage_array1 -r sd-unixhost-role sd-
unixhost-ug
Created usergroup sd-unixhost-ug(44) on storage_array1
```

5. 建立本機使用者。

```
# dfm host user create -h storage_array1 -p xxxxxxxx -g sd-unixhost-ug
sd-unixhost
Created local user sd-unixhost on storage_array1
```

在SnapDrive UNIX版的使用者認證上設定使用者認證

UNIX版的系統管理員會從Operations Manager主控台管理員收到使用者認證資料。SnapDrive這些使用者認證資料必須在SnapDrive UNIX的版次上設定、才能正常執行儲存作業。

步驟

1. 在儲存系統上設定SD-admin。

```
[root]#snapdrive config set -dfm sd-admin ops_mngr_server
Password for sd-admin:
Retype password:
```

2. 在儲存系統上設定SD-HostName。

```
[root]#snapdrive config set sd-unix_host storage_array1
Password for sd-unix_host:
Retype password:
```

3. 使用「SnapDrive flexconfig list」命令確認步驟1和步驟2。

user name	appliance name	appliance type
sd-admin	ops_mngr_server	DFM
sd-unix_host	storage_array1	StorageSystem

4. 將SnapDrive Operations Manager主控台角色型存取控制（RBAC）設定為使用、方法是在「snapdrive.conf」檔案中設定組態變數「RBAC方法= DFM」。



使用者認證資料會加密並儲存在現有的「.sdupw」檔案中。較早檔案的預設位置為「/opt/NetApp/SnapDrive/.sdupw」。

使用Operations Manager主控台執行存取檢查的使用者名稱格式

UNIX版使用使用者名稱格式來執行Operations Manager主控台的存取檢查。SnapDrive這些格式取決於您是網路資訊系統（NIS）或本機使用者。

UNIX版使用下列格式來檢查使用者是否有權執行特定工作：SnapDrive

- 如果您是NIS使用者、執行「SnapDrive 樣」命令、SnapDrive 則UNIX版的用例格式為「<nisdomain>\<使用者名稱>」（例如、「netapp.com\marc」）。
- 如果您是UNIX主機（例如Inx197/141）的本機使用者、SnapDrive 則適用於UNIX的支援中心會使用「<主機名稱>\<使用者名稱>」格式（例如、「Inx197/141\john」）。
- 如果您是UNIX主機的系統管理員（root）、SnapDrive 那麼適用於UNIX的支援將管理員視為本機使用者、並使用「Inx197/141\root」格式。

角色型存取控制的組態變數

您必須在「snapdrive.conf」檔案中、設定與角色型存取控制相關的各種組態變數。

變動	說明
h_contact-http-dfm-port = 8088_'	指定用於與Operations Manager主控台伺服器通訊的HTTP連接埠。預設值為8088。
「contact-SSL-DFM-port = 8488_」	指定用於與Operations Manager主控台伺服器通訊的SSL連接埠。預設值為8488。
「_RBAC方法= DFM」	<p>指定存取控制方法。可能的值包括「原生」和「dFM」。</p> <p>如果該值為「原生」、則儲存在「/vol/vol0/sdprbac/sdhost-name.prbac」中的存取控制檔案將用於存取檢查。</p> <p>如果該值設為「dFM」、則營運經理主控台是必備條件。在這種情況SnapDrive下、UNIX版的支援中心會將存取檢查傳送至Operations Manager主控台。</p>
「_RBAC快取=開啟」	<p>適用於UNIX的可維護存取檢查查詢的快取及對應結果。SnapDrive僅當所有已設定的Operations Manager主控台伺服器都停機時、UNIX版的適用對象才會使用此快取。SnapDrive</p> <p>您可以將此值設為「On（開啟）」以啟用快取、或設為「Off（關閉）」以停用快取。預設值為「Off」（關）、您可以將SnapDrive UNIX的支援功能設定為使用Operations Manager主控台、並將「RBAC方法」組態變數設定為「dFM」。</p>
「_RBAC快取快取逾時」	<p>指定RBAC快取逾時期間、僅適用於啟用「_RBAC快取」的情況。預設值為「24小時」。</p> <p>僅當所有已設定的Operations Manager主控台伺服器都停機時、UNIX版的適用對象才會使用此快取。SnapDrive</p>
「use-https-to - dfm=on」	此變數可讓您將SnapDrive UNIX的支援設定為在與Operations Manager主控台通訊時使用SSL加密（HTTPS）。預設值為「開啟」。

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。