



RBAC

ONTAP Automation

NetApp
July 11, 2024

目錄

RBAC	1
準備使用 RBAC	1
建立角色	1
建立具有角色的使用者	5

RBAC

準備使用 RBAC

視您的環境而定、您可以使用多種不同的 ONTAP RBAC 功能。本節將以工作流程形式呈現幾種常見案例。在每個案例中、重點都是特定的安全性和管理目標。

在建立任何角色並將角色指派給 ONTAP 使用者帳戶之前、您應該先檢閱下列主要安全需求和選項、以做好準備。此外、請務必檢閱上的一般工作流程概念 "[準備好使用工作流程](#)"。

您使用的**ONTAP** 是哪個版本？

此版本可決定哪些REST端點和RBAC功能可供使用。ONTAP

識別受保護的資源和範圍

您需要識別要保護的資源或命令、以及範圍（叢集或SVM）。

使用者應該擁有哪些存取權限？

在識別資源和範圍之後、您需要判斷要授與的存取層級。

使用者將如何存取**ONTAP** 此產品？

使用者可ONTAP 透過REST API或CLI或兩者存取功能。

其中一個內建角色是否足夠、或是需要自訂角色？

使用現有的內建角色比較方便、但您可以視需要建立新的自訂角色。

需要哪種角色？

根據安全需求和ONTAP 不必要存取、您需要選擇是要建立休息或傳統角色。

建立角色

限制對**SVM Volume**作業的存取

您可以定義角色、以限制 SVM 內的儲存磁碟區管理。

關於此工作流程

首先會建立傳統角色、以開始允許存取所有主要的 Volume 管理功能（複製除外）。角色的定義具有下列特性：

- 能夠執行所有CRUD Volume作業、包括Get、Create、Modify和Delete
- 無法建立Volume複製

接著您可以視需要選擇性地更新角色。在此工作流程中、角色會在第二個步驟中變更、以允許使用者建立 Volume 複製。

步驟 1：建立角色

您可以發出 API 呼叫來建立 RBAC 角色。

HTTP 方法和端點

此 REST API 呼叫使用下列方法和端點。

HTTP方法	路徑
貼文	/API/SECSecurity /角色

Curl範例

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/roles" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSONN輸入範例

```
{  
  "name": "role1",  
  "owner": {  
    "name": "cluster-1",  
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"  
  },  
  "privileges": [  
    { "path": "volume create", "access": "all" },  
    { "path": "volume delete", "access": "all" }  
  ]  
}
```

步驟 2：更新角色

您可以發出 API 呼叫來更新現有角色。

HTTP 方法和端點

此 REST API 呼叫使用下列方法和端點。

HTTP方法	路徑
貼文	/API/SECSecurity /角色

捲曲範例的其他輸入參數

除了所有 REST API 呼叫通用的參數之外、本步驟的捲髮範例中也會使用下列參數。

參數	類型	必要	說明
\$SVM_ID	路徑	是的	這是包含角色定義的 SVM 的 UUID。

參數	類型	必要	說明
\$Role_name	路徑	是的	這是要更新的 SVM 中的角色名稱。

Curl範例

```
curl --request POST \
--location
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/priveleges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSONN輸入範例

```
{
  "path": "volume clone",
  "access": "all"
}
```

啟用資料保護的管理

您可以為使用者提供有限的資料保護功能。

關於此工作流程

建立的傳統角色具有下列特性：

- 能夠建立和刪除快照、以及更新SnapMirror關係
- 無法建立或修改較高層級的物件、例如磁碟區或SVM

HTTP 方法和端點

此 REST API 呼叫使用下列方法和端點。

HTTP方法	路徑
貼文	/API/SECSecurity /角色

Curl範例

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSONN輸入範例

```
{
  "name": "role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
    {"path": "volume snapshot create", "access": "all"},
    {"path": "volume snapshot delete", "access": "all"},
    {"path": "volume show", "access": "readonly"},
    {"path": "vserver show", "access": "readonly"},
    {"path": "snapmirror show", "access": "readonly"},
    {"path": "snapmirror update", "access": "all"}
  ]
}
```

允許產生 ONTAP 報告

您可以建立REST角色、讓使用者能夠產生ONTAP 各種報告。

關於此工作流程

建立的角色具有下列特性：

- 能夠擷取與容量和效能相關的所有儲存物件資訊（例如Volume、qtree、LUN、Aggregate、節點、和SnapMirror關係）
- 無法建立或修改較高層級的物件（例如磁碟區或SVM）

HTTP 方法和端點

此 REST API 呼叫使用下列方法和端點。

HTTP方法	路徑
貼文	/API/SECSecurity /角色

Curl範例

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/roles" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSONN輸入範例

```
{
  "name": "rest_role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
    {"path": "/api/storage/volumes", "access": "readonly"},
    {"path": "/api/storage/qtrees", "access": "readonly"},
    {"path": "/api/storage/luns", "access": "readonly"},
    {"path": "/api/storage/aggregates", "access": "readonly"},
    {"path": "/api/cluster/nodes", "access": "readonly"},
    {"path": "/api/snapmirror/relationships", "access": "readonly"},
    {"path": "/api/svm/svms", "access": "readonly"}
  ]
}
```

建立具有角色的使用者

您可以使用此工作流程來建立具有相關 REST 角色的使用者。

關於此工作流程

此工作流程包括建立自訂 REST 角色並將其與新使用者帳戶建立關聯所需的一般步驟。使用者和角色都有SVM 範圍、並與特定資料SVM相關聯。某些步驟可能是選擇性的、或是需要根據您的環境而變更。

步驟 1：列出叢集中的資料 SVM

執行下列REST API呼叫、列出叢集中的SVM。輸出中會提供每個 SVM 的 UUID 和名稱。

HTTP 方法和端點

此 REST API 呼叫使用下列方法和端點。

HTTP方法	路徑
取得	/API/SVM/svms

Curl範例

```
curl --request GET \
--location "https://$FQDN_IP/api/svm/svms?order_by=name" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

完成後

從您要建立新使用者和角色的清單中選取所需的SVM。

步驟 2：列出定義給 **SVM** 的使用者

執行下列REST API呼叫、列出您所選SVM中定義的使用者。您可以透過擁有者參數來識別SVM。

HTTP 方法和端點

此 REST API 呼叫使用下列方法和端點。

HTTP方法	路徑
取得	/API/SECSecurity /帳戶

Curl範例

```
curl --request GET \  
--location "https://$FQDN_IP/api/security/accounts?owner.name=dmp" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

完成後

根據已在SVM中定義的使用者、為新使用者選擇唯一名稱。

步驟 3：列出定義給 **SVM** 的其餘角色

執行下列REST API呼叫、列出您所選SVM中定義的角色。您可以透過擁有者參數來識別SVM。

HTTP 方法和端點

此 REST API 呼叫使用下列方法和端點。

HTTP方法	路徑
取得	/API/SECSecurity /角色

Curl範例

```
curl --request GET \  
--location "https://$FQDN_IP/api/security/roles?owner.name=dmp" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

完成後

根據已在SVM中定義的角色、為新角色選擇唯一名稱。

步驟 4：建立自訂 REST 角色

執行下列REST API呼叫、以在SVM中建立自訂REST角色。角色一開始只有一個權限會建立*無*的預設存取權、因此會拒絕所有存取權。

HTTP 方法和端點

此 REST API 呼叫使用下列方法和端點。

HTTP方法	路徑
貼文	/API/SECSecurity /角色

Curl範例

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/roles" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSONN輸入範例

```
{  
  "name": "dprole1",  
  "owner": {  
    "name": "dmp",  
    "uuid": "752d96be-f17c-11ec-9d19-005056bbad91"  
  },  
  "privileges": [  
    {"path": "/api", "access": "none"},  
  ]  
}
```

完成後

(可選) 再次執行步驟3以顯示新角色。您也可以可以在ONTAP CLI中顯示角色。

步驟 5：新增更多權限以更新角色

執行下列REST API呼叫、視需要新增權限以修改角色。

HTTP 方法和端點

此 REST API 呼叫使用下列方法和端點。

HTTP方法	路徑
貼文	/API/SECURIE/角色/ {Oner.uuid} / {name} /權限

捲曲範例的其他輸入參數

除了所有 REST API 呼叫通用的參數之外、本步驟的捲髮範例中也會使用下列參數。

參數	類型	必要	說明
\$SVM_ID	路徑	是的	包含角色定義的 SVM UUID。
\$Role_name	路徑	是的	要更新的 SVM 中角色的名稱。

Curl範例

```
curl --request POST \  
--location \  
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/privileges" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSONN輸入範例

```
{  
  "path": "/api/storage/volumes",  
  "access": "readonly"  
}
```

完成後

(可選) 再次執行步驟3以顯示新角色。您也可以在此ONTAP CLI中顯示角色。

步驟 6：建立使用者

執行下列REST API呼叫以建立使用者帳戶。上述建立的角色 * dprole1* 與新使用者相關聯。



您可以建立沒有角色的使用者。在這種情況下、會為使用者指派預設角色（兩者皆可） admin 或 vsadmin）取決於使用者是使用叢集或 SVM 範圍來定義。您需要修改使用者以指派不同的角色。

HTTP 方法和端點

此 REST API 呼叫使用下列方法和端點。

HTTP方法	路徑
貼文	/API/SECSecurity /帳戶

Curl範例

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/accounts" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSONN輸入範例

```
{  
  "owner": {"uuid": "daf84055-248f-11ed-a23d-005056ac4fe6"},  
  "name": "david",  
  "applications": [  
    {"application": "ssh",  
      "authentication_methods": ["password"],  
      "second_authentication_method": "none"}  
  ],  
  "role": "dprole1",  
  "password": "netapp123"  
}
```

完成後

您可以使用新使用者的認證登入SVM管理介面。

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。