



# 使用**NetApp ONTAP** 功能在**Red Hat OpenShift**上設定多租戶共享 NetApp Solutions

NetApp  
April 12, 2024

# 目錄

使用NetApp ONTAP 功能在Red Hat OpenShift上設定多租戶共享 .....	1
使用NetApp在Red Hat OpenShift上設定多租戶共享 .....	1
架構 .....	1
組態 .....	3

# 使用NetApp ONTAP 功能在Red Hat OpenShift上設定多租戶共享

## 使用NetApp在Red Hat OpenShift上設定多租戶共享

許多在容器上執行多個應用程式或工作負載的組織、傾向於針對每個應用程式或工作負載部署一個Red Hat OpenShift叢集。這可讓他們針對應用程式或工作負載實作嚴格的隔離、最佳化效能並減少安全性弱點。不過、為每個應用程式部署個別的Red Hat OpenShift叢集、會產生自己的問題集。它會增加營運成本、必須自行監控及管理每個叢集、因為不同應用程式的專屬資源而增加成本、並阻礙有效的擴充性。

若要克服這些問題、您可以考慮在單一Red Hat OpenShift叢集中執行所有應用程式或工作負載。但是在這樣的架構中、資源隔離和應用程式安全性弱點是其中一項重大挑戰。某個工作負載中的任何安全弱點都可能自然延伸到另一個工作負載、進而增加影響區域。此外、任何應用程式突然無法控制的資源使用率、都可能影響另一個應用程式的效能、因為預設不會有資源配置原則。

因此、企業組織希望能在這兩個領域中找到最佳的解決方案、例如允許他們在單一叢集中執行所有工作負載、同時為每個工作負載提供專屬叢集的優點。

其中一個有效的解決方案是在Red Hat OpenShift上設定多租戶共享。多租戶共享是一種架構、可讓多個租戶在同一個叢集上共存、並適當隔離資源、安全性等。在這種情況下、租戶可視為叢集資源的子集、而這些資源已設定為供特定使用者群組專用。在Red Hat OpenShift叢集上設定多租戶共享可提供下列優點：

- 允許共用叢集資源、進而降低資本支出和營運成本
- 降低營運與管理成本
- 保護工作負載免於安全漏洞的交叉污染
- 保護工作負載、避免資源爭用造成非預期的效能降級

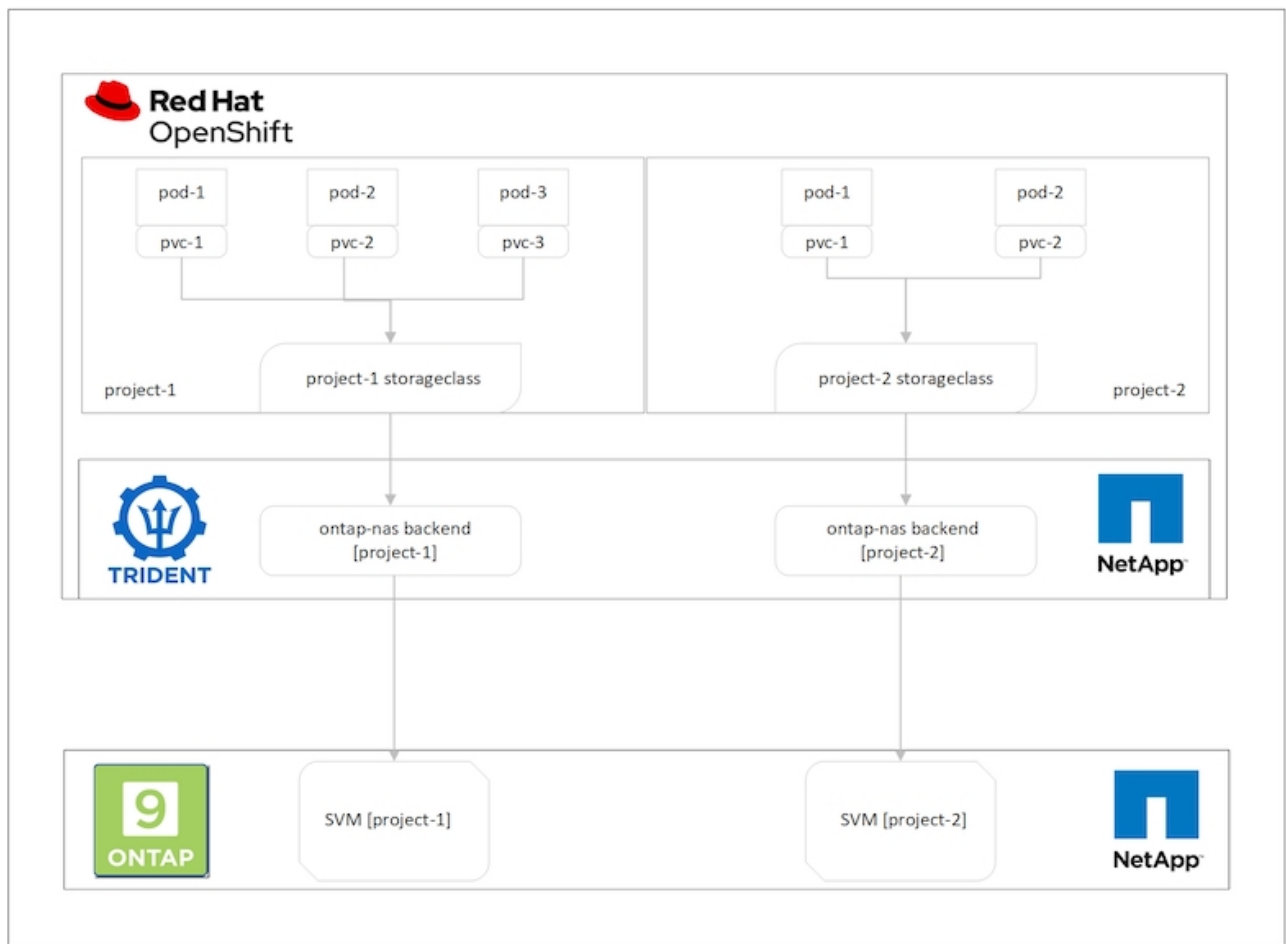
對於完全實現的多租戶OpenShift叢集、必須針對屬於不同資源桶的叢集資源設定配額和限制：運算、儲存、網路、安全性等。雖然我們涵蓋本解決方案中所有資源桶的某些層面、我們將重點放在隔離和保護同一個Red Hat OpenShift叢集上多個工作負載所提供或使用的資料的最佳實務做法上、方法是在由Astra Trident以NetApp ONTAP S動地 配置的儲存資源上設定多租戶。

## 架構

雖然Red Hat OpenShift和Astra Trident以NetApp ONTAP 支援、但在預設情況下並未隔離不同的工作負載、但它們提供多種功能、可用來設定多租戶。為了更深入瞭ONTAP 解如何在採用NetApp®技術的Astra Trident的Red Hat OpenShift叢集上設計多租戶解決方案、請讓我們參考一組需求範例、並概述相關的組態。

假設某組織在Red Hat OpenShift叢集上執行兩項工作負載、這是兩個不同團隊正在進行的兩個專案的一部分。這些工作負載的資料位於PVCS上、由Astra Trident在NetApp ONTAP 的NAS後端動態配置。組織必須針對這兩項工作負載設計多租戶解決方案、並隔離用於這些專案的資源、以確保安全性和效能得以維持、主要著重於為這些應用程式提供服務的資料。

下圖說明Red Hat OpenShift叢集上的多租戶解決方案、其中Astra Trident以NetApp ONTAP 效益為後盾。



## 技術需求

1. NetApp ONTAP 解決方案儲存叢集
2. Red Hat OpenShift叢集
3. Astra Trident

## Red Hat OpenShift–叢集資源

從Red Hat OpenShift叢集觀點來看、最重要的資源是專案。OpenShift專案可視為叢集資源、將整個OpenShift叢集分成多個虛擬叢集。因此、專案層級的隔離功能可提供設定多租戶的基礎。

接下來是在叢集中設定RBAC。最佳實務做法是讓所有開發人員在身分識別供應商（IDP）的單一使用者群組中、處理單一專案或工作負載。Red Hat OpenShift允許IDP整合和使用者群組同步、因此可將IDP中的使用者和群組匯入叢集。這有助於叢集管理員將專案專屬的叢集資源存取權、隔離給該專案的使用者群組、進而限制未獲授權存取任何叢集資源。若要深入瞭解IDP與Red Hat OpenShift的整合、請參閱文件 ["請按這裡"](#)。

## NetApp ONTAP

將共享儲存設備隔離為Red Hat OpenShift叢集的持續儲存提供者非常重要、因為如此可確保在儲存設備上為每個專案建立的磁碟區、在主機看來就像是在不同的儲存設備上建立的磁碟區一樣。為達成此目標、請在NetApp ONTAP 支援上建立數量不限的SVM（儲存虛擬機器）、如同專案或工作負載一樣多、並將每個SVM專用於工作負載。

## Astra Trident

在NetApp ONTAP 支援上建立不同專案的不同SVM之後、您必須將每個SVM對應到不同的Trident後端。Trident 上的後端組態會將持續儲存設備分配給OpenShift叢集資源、而且需要將SVM的詳細資料對應至該資源。這至少應該是後端的傳輸協定驅動程式。您也可以選擇定義如何在儲存設備上配置磁碟區、以及設定磁碟區大小或集合體使用量等限制。如需有關Trident後端定義的詳細資料、請參閱 ["請按這裡"](#)。

## Red Hat OpenShift–儲存資源

設定Trident後端之後、下一步是設定StorageClass。設定多個後端儲存類別、讓每個儲存類別都能存取、只在一個後端上增加磁碟區。我們可以在定義儲存類別時、使用storagePools參數、將StorageClass對應至特定的Trident後端。您可以找到定義儲存類別的詳細資料 ["請按這裡"](#)。因此、StorageClass與Trident後端之間有一對一對應關係、可指向一個SVM。如此可確保透過指派給該專案的StorageClass進行的所有儲存設備宣告、均由專屬該專案的SVM提供服務。

由於儲存類別並非命名資源、我們如何確保另一個命名空間或專案中的Pod對某個專案的儲存類別提出的要求遭到拒絕？答案是使用資源配額。資源配額是控制每個專案資源總使用量的物件。它可以限制專案中物件可耗用的資源數量和總容量。使用資源配額幾乎可以限制專案的所有資源、而且有效率地使用資源、有助於組織降低因資源過度配置或過度使用而造成的成本與中斷。請參閱文件 ["請按這裡"](#) 以取得更多資訊。

在此使用案例中、我們需要限制特定專案中的Pod、使其無法從非專屬專案的儲存類別中申請儲存設備。為達成此目標、我們必須將「<storage-class-name>.storageclass.storage.k8s.io/永久性 磁碟區」設為0、以限制其他儲存類別的持續磁碟區宣告。此外、叢集管理員必須確保專案中的開發人員不應擁有修改資源配額的存取權。

## 組態

對於任何多租戶解決方案、任何使用者都無法存取超過所需的叢集資源。因此、要設定為多租戶組態一部分的一整組資源、會分為叢集管理、儲存管理員和開發人員、分別負責每個專案。

下表概述不同使用者要執行的不同工作：

角色	工作
叢集管理	為不同的應用程式或工作負載建立專案
	為儲存管理員建立Cluster角色 和角色繫結
	建立角色與角色繫結、讓開發人員指派特定專案的存取權
	[選用]設定專案以排程特定節點上的Pod
儲存設備管理	在NetApp ONTAP 上建立SVM
	建立Trident後端
	建立StorageClass
	建立儲存資源配額

角色	工作
開發人員	驗證存取權限、以便在指派的專案中建立或修補PVCS或Pod
	驗證存取權限、以在另一個專案中建立或修補PVCS或Pod
	驗證存取權限、以檢視或編輯專案、資源配額和儲存類別

## 組態

### 先決條件

- NetApp ONTAP 產品叢集
- Red Hat OpenShift叢集
- 叢集上安裝的Trident
- 安裝了tridentctl和occ工具並新增至\$path的管理工作站
- 管理員存取ONTAP 功能
- 叢集管理存取OpenShift叢集
- 叢集已與Identity Provider整合
- 身分識別供應商的設定可有效區分不同團隊中的使用者

## 組態：叢集管理工作

Red Hat OpenShift叢集管理會執行下列工作：

1. 以叢集管理的身分登入Red Hat OpenShift叢集。
2. 建立兩個對應於不同專案的專案。

```
oc create namespace project-1
oc create namespace project-2
```

3. 建立專案1的開發人員角色。

```
cat << EOF | oc create -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: project-1
  name: developer-project-1
rules:
  - verbs:
    - '*'
```

```

    apiGroups:
      - apps
      - batch
      - autoscaling
      - extensions
      - networking.k8s.io
      - policy
      - apps.openshift.io
      - build.openshift.io
      - image.openshift.io
      - ingress.operator.openshift.io
      - route.openshift.io
      - snapshot.storage.k8s.io
      - template.openshift.io
    resources:
      - '*'
- verbs:
  - '*'
  apiGroups:
    - ''
  resources:
    - bindings
    - configmaps
    - endpoints
    - events
    - persistentvolumeclaims
    - pods
    - pods/log
    - pods/attach
    - podtemplates
    - replicationcontrollers
    - services
    - limitranges
    - namespaces
    - componentstatuses
    - nodes
- verbs:
  - '*'
  apiGroups:
    - trident.netapp.io
  resources:
    - trident snapshots
EOF

```



本節提供的角色定義只是一個範例。開發人員角色必須根據終端使用者需求加以定義。

1. 同樣地、請為專案2建立開發人員角色。
2. 所有OpenShift和NetApp儲存資源通常由儲存管理員管理。儲存管理員的存取權由安裝Trident時所建立的Trident操作員角色控制。此外、儲存管理員也需要存取資源配額、才能控制儲存設備的使用方式。
3. 在叢集中的所有專案中建立管理資源配額的角色、以將其附加至儲存設備管理員。

```
cat << EOF | oc create -f -
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: resource-quotas-role
rules:
  - verbs:
    - '*'
    apiGroups:
    - ''
    resources:
    - resourcequotas
  - verbs:
    - '*'
    apiGroups:
    - quota.openshift.io
    resources:
    - '*'
EOF
```

4. 請確定叢集已與組織的身分識別提供者整合、而且使用者群組已與叢集群組同步。下列範例顯示身分識別提供者已與叢集整合、並與使用者群組同步。

```
$ oc get groups
NAME                                USERS
ocp-netapp-storage-admins          ocp-netapp-storage-admin
ocp-project-1                      ocp-project-1-user
ocp-project-2                      ocp-project-2-user
```

1. 為儲存管理員設定Cluster勞力 綁定。



```

cat << EOF | oc create -f -
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: netapp-storage-admin-trident-operator
subjects:
  - kind: Group
    apiGroup: rbac.authorization.k8s.io
    name: ocp-netapp-storage-admins
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: trident-operator
---
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: netapp-storage-admin-resource-quotas-cr
subjects:
  - kind: Group
    apiGroup: rbac.authorization.k8s.io
    name: ocp-netapp-storage-admins
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: resource-quotas-role
EOF

```



對於儲存管理員、必須綁定兩個角色：Trident運算子和資源配額。

1. 為開發人員建立角色連結、將開發人員專案1角色繫結至專案1中對應的群組（OCP專案-1）。

```
cat << EOF | oc create -f -
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: project-1-developer
  namespace: project-1
subjects:
- kind: Group
  apiGroup: rbac.authorization.k8s.io
  name: ocp-project-1
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: developer-project-1
EOF
```

2. 同樣地、請為開發人員建立角色連結至專案2中對應的使用者群組的角色連結。

## 組態：儲存設備管理工作

儲存管理員必須設定下列資源：

1. 以admin身分登入NetApp ONTAP 解決方案叢集。
2. 瀏覽至Storage（儲存設備）> Storage VM（儲存設備VM）、然後按一下Add提供所需的詳細資料、建立兩個SVM、一個用於專案1、另一個用於專案2。也可建立vsadmin帳戶來管理SVM及其資源。

# Add Storage VM



STORAGE VM NAME

project-1-svm

## Access Protocol



SMB/CIFS, NFS

iSCSI



Enable SMB/CIFS



Enable NFS



Allow NFS client access

Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

RULES

Rule Index	Clients	Access Protocols	Read-Only R...	Read/Wr
	10.61.181.0/24	Any	Any	Any

+ Add

DEFAULT LANGUAGE [?](#)

c.utf\_8



NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

K8s-Ontap-01

IP ADDRESS

10.61.181.224

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN

Default-4



1. 以儲存管理員身分登入Red Hat OpenShift叢集。
2. 建立專案1的後端、並將其對應至專案專用的SVM。NetApp建議使用SVM的vsadmin帳戶、將後端連線至SVM、而非ONTAP 使用該叢集管理員。

```
cat << EOF | tridentctl -n trident create backend -f
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "nfs_project_1",
  "managementLIF": "172.21.224.210",
  "dataLIF": "10.61.181.224",
  "svm": "project-1-svm",
  "username": "vsadmin",
  "password": "NetApp123"
}
EOF
```



本例使用的是ONTAP-NAS驅動程式。根據使用案例建立後端時、請使用適當的驅動程式。



我們假設Trident安裝在Trident專案中。

1. 同樣地、請為專案2建立Trident後端、並將其對應至專案2專用的SVM。
2. 接下來、建立儲存類別。建立專案1的儲存類別、並設定storagePools參數、以使用從專屬後端到專案1的儲存資源池。

```
cat << EOF | oc create -f -
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: project-1-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: ontap-nas
  storagePools: "nfs_project_1:.*"
EOF
```

3. 同樣地、請為專案2建立儲存類別、並將其設定為使用從專屬後端到專案2的儲存資源池。
4. 建立資源配額、以限制專案1中的資源、要求儲存資源來自其他專案專用的儲存設備。

```
cat << EOF | oc create -f -
kind: ResourceQuota
apiVersion: v1
metadata:
  name: project-1-sc-rq
  namespace: project-1
spec:
  hard:
    project-2-sc.storageclass.storage.k8s.io/persistentvolumeclaims: 0
EOF
```

5. 同樣地、也可以建立資源配額、以限制專案2中的資源、要求儲存資源來自其他專案專用的儲存設備。

## 驗證

若要驗證先前步驟中設定的多租戶架構、請完成下列步驟：

驗證存取權、以在指派的專案中建立**PVCS**或**Pod**

1. 以專案1的開發人員OCP專案1使用者身分登入。
2. 檢查存取權限以建立新專案。

```
oc create ns sub-project-1
```

3. 在專案1中使用指派給專案1的storageclass建立一個PVC.

```
cat << EOF | oc create -f -
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: test-pvc-project-1
  namespace: project-1
  annotations:
    trident.netapp.io/reclaimPolicy: Retain
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: project-1-sc
EOF
```

4. 檢查與室早相關的PV。

```
oc get pv
```

5. 驗證PV及其Volume是否是在專門用於NetApp ONTAP 上專案1的SVM中建立。

```
volume show -vserver project-1-svm
```

6. 在專案1中建立一個Pod、然後掛載上一步建立的永久虛擬儲存設備。

```
cat << EOF | oc create -f -
kind: Pod
apiVersion: v1
metadata:
  name: test-pvc-pod
  namespace: project-1
spec:
  volumes:
    - name: test-pvc-project-1
      persistentVolumeClaim:
        claimName: test-pvc-project-1
  containers:
    - name: test-container
      image: nginx
      ports:
        - containerPort: 80
          name: "http-server"
      volumeMounts:
        - mountPath: "/usr/share/nginx/html"
          name: test-pvc-project-1
EOF
```

7. 檢查Pod是否正在執行、以及是否已掛載磁碟區。

```
oc describe pods test-pvc-pod -n project-1
```

驗證存取權限、以在另一個專案中建立PVCS或Pod、或使用其他專案專用的資源

1. 以專案1的開發人員OCP專案1使用者身分登入。
2. 使用指派給專案2的儲存裝置在專案1中建立一個PVC.

```
cat << EOF | oc create -f -
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: test-pvc-project-1-sc-2
  namespace: project-1
  annotations:
    trident.netapp.io/reclaimPolicy: Retain
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: project-2-sc
EOF
```

### 3. 在專案2中建立一個PVC.

```
cat << EOF | oc create -f -
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: test-pvc-project-2-sc-1
  namespace: project-2
  annotations:
    trident.netapp.io/reclaimPolicy: Retain
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: project-1-sc
EOF
```

### 4. 確保未建立PVCS「test-PVC-project - 1-sc-2」和「test-PVC-project - 2-sc-1」。

```
oc get pvc -n project-1
oc get pvc -n project-2
```

### 5. 在專案2中建立Pod。

```
cat << EOF | oc create -f -
kind: Pod
apiVersion: v1
metadata:
  name: test-pvc-pod
  namespace: project-1
spec:
  containers:
  - name: test-container
    image: nginx
    ports:
    - containerPort: 80
      name: "http-server"
EOF
```

驗證存取權限、以檢視及編輯專案、資源配額和儲存類別

1. 以專案1的開發人員OCP專案1使用者身分登入。
2. 檢查存取權限以建立新專案。

```
oc create ns sub-project-1
```

3. 驗證存取權限以檢視專案。

```
oc get ns
```

4. 檢查使用者是否可以在專案1中檢視或編輯資源配額。

```
oc get resourcequotas -n project-1
oc edit resourcequotas project-1-sc-rq -n project-1
```

5. 驗證使用者是否有權檢視儲存空間。

```
oc get sc
```

6. 檢查存取以描述儲存空間。
7. 驗證使用者的存取權、以編輯儲存空間。

```
oc edit sc project-1-sc
```



## 擴充：新增更多專案

在多租戶組態中、新增含有儲存資源的專案需要額外的組態、以確保不違反多租戶共享。若要在多租戶叢集中新增更多專案、請完成下列步驟：

1. 以儲存管理員身分登入NetApp ONTAP 解決方案叢集。
2. 瀏覽至「儲存虛擬機器」、然後按一下「Add（新增）」。建立專案3專用的新SVM。也可建立vsadmin帳戶來管理SVM及其資源。

# Add Storage VM



STORAGE VM NAME

project-3-svm

## Access Protocol

☒ SMB/CIFS, NFS

iSCSI

☐ Enable SMB/CIFS

☒ Enable NFS

☒ Allow NFS client access

Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

RULES

Rule Index	Clients	Access Protocols	Read-Only R...	Read/Wr
	10.61.181.0/24	Any	Any	Any

[+ Add](#)

DEFAULT LANGUAGE [?](#)

c.utf\_8

NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

K8s-Ontap-01

IP ADDRESS

10.61.181.228

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN

Default-4

1. 以叢集管理身分登入Red Hat OpenShift叢集。
2. 建立新專案。

```
oc create ns project-3
```

3. 確認專案3的使用者群組是在IDP上建立、並與OpenShift叢集同步。

```
oc get groups
```

4. 建立專案3的開發人員角色。

```
cat << EOF | oc create -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: project-3
  name: developer-project-3
rules:
  - verbs:
      - '*'
    apiGroups:
      - apps
      - batch
      - autoscaling
      - extensions
      - networking.k8s.io
      - policy
      - apps.openshift.io
      - build.openshift.io
      - image.openshift.io
      - ingress.operator.openshift.io
      - route.openshift.io
      - snapshot.storage.k8s.io
      - template.openshift.io
    resources:
      - '*'
  - verbs:
      - '*'
    apiGroups:
      - ''
    resources:
      - bindings
      - configmaps
      - endpoints
      - events
      - persistentvolumeclaims
      - pods
      - pods/log
      - pods/attach
      - podtemplates
```

```

- replicationcontrollers
- services
- limitranges
- namespaces
- componentstatuses
- nodes
- verbs:
  - '*'
apiGroups:
- trident.netapp.io
resources:
- trident snapshots
EOF

```



本節提供的角色定義只是一個範例。開發人員角色必須根據終端使用者需求加以定義。

1. 在Project 3中為開發人員建立角色繫結、將開發人員專案3角色繫結至專案3中對應的群組（OCP專案3）。


```


cat << EOF | oc create -f -
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: project-3-developer
  namespace: project-3
subjects:
- kind: Group
  apiGroup: rbac.authorization.k8s.io
  name: ocp-project-3
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: developer-project-3
EOF

```

2. 以儲存管理員身分登入Red Hat OpenShift叢集
3. 建立Trident後端、並將其對應至專案3專用的SVM。NetApp建議使用SVM的vsadmin帳戶、將後端連線至SVM、而非ONTAP 使用叢集管理員。

```
cat << EOF | tridentctl -n trident create backend -f
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "nfs_project_3",
  "managementLIF": "172.21.224.210",
  "dataLIF": "10.61.181.228",
  "svm": "project-3-svm",
  "username": "vsadmin",
  "password": "NetApp!23"
}
EOF
```

 本例使用的是ONTAP-NAS驅動程式。根據使用案例、使用適當的驅動程式來建立後端。

 我們假設Trident安裝在Trident專案中。

1. 建立專案3的儲存類別、並將其設定為使用從專案3專用後端的儲存資源池。

```
cat << EOF | oc create -f -
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: project-3-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: ontap-nas
  storagePools: "nfs_project_3:.*"
EOF
```

2. 建立資源配額、以限制專案3中的資源、要求儲存資源來自其他專案專用的儲存設備。

```
cat << EOF | oc create -f -
kind: ResourceQuota
apiVersion: v1
metadata:
  name: project-3-sc-rq
  namespace: project-3
spec:
  hard:
    project-1-sc.storageclass.storage.k8s.io/persistentvolumeclaims: 0
    project-2-sc.storageclass.storage.k8s.io/persistentvolumeclaims: 0
EOF
```

3. 修補其他專案中的資源配額、限制這些專案中的資源無法從專案3專用的儲存設備存取儲存設備。

```
oc patch resourcequotas project-1-sc-rq -n project-1 --patch
'{"spec":{"hard":{"project-3-sc.storageclass.storage.k8s.io/persistentvolumeclaims": 0}}}'
oc patch resourcequotas project-2-sc-rq -n project-2 --patch
'{"spec":{"hard":{"project-3-sc.storageclass.storage.k8s.io/persistentvolumeclaims": 0}}}'
```

## 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。