# Configuración

## NetApp Solutions

NetApp
April 23, 2024

This PDF was generated from https://docs.netapp.com/es-es/netapp-solutions/containers/rh-os-n_use_case_multitenancy_configuration_prerequisites.html on April 23, 2024. Always check docs.netapp.com for the latest.

# Tabla de contenidos

Configuración . . . 1
Configuración . . . 1
Configuration: Tareas del administrador del clúster . . . 2
Configuration: Tareas del administrador del almacenamiento . . . 6
Validación . . . 9
Escala: Agregar más proyectos . . . 13

# Configuración

Para cualquier solución multitenant, ningún usuario puede tener acceso a más recursos del clúster de los que necesita. Por lo tanto, todo el conjunto de recursos que se van a configurar como parte de la configuración de multi-tenancy se divide entre cluster-admin, Storage-admin y los desarrolladores que trabajan en cada proyecto.

En la siguiente tabla se describen las distintas tareas que deben realizar los distintos usuarios:

| Función | Tareas |
|---|---|
| **Cluster-admin** | Crear proyectos para distintas aplicaciones o cargas de trabajo |
| | Cree ClusterRoles y RoleBindings para Storage-admin |
| | Cree funciones y RoleBindings para los desarrolladores que asignan acceso a proyectos específicos |
| | [Opcional] Configure proyectos para programar pods en nodos específicos |
| **Storage-admin** | Creación de SVM en ONTAP de NetApp |
| | Cree los back-ends de Trident |
| | Cree clases de almacenamiento |
| | Cree el recurso Quotas de almacenamiento |
| **Desarrolladores** | Validar el acceso para crear o revisar CVP o pods en el proyecto asignado |
| | Validar el acceso para crear o revisar CVP o pods en otro proyecto |
| | Valide el acceso para ver o editar proyectos, ResourceQuotas y StorageClasses |

# Configuración

## Requisitos previos

- Clúster de ONTAP de NetApp
- Clúster de Red Hat OpenShift
- Trident se instaló en el clúster
- Estación de trabajo de administración con herramientas trimentctl y oc instaladas y agregadas a $PATH
- Acceso de administrador a ONTAP
- Acceso de administrador de clúster a clúster OpenShift
- El clúster se integra con el proveedor de identidades
- El proveedor de identidades está configurado para distinguir eficientemente entre usuarios de distintos equipos

# Configuration: Tareas del administrador del clúster

El administrador de clúster de Red Hat OpenShift realiza las siguientes tareas:

1. Inicie sesión en el clúster de Red Hat OpenShift como cluster-admin.
2. Crear dos proyectos correspondientes a diferentes proyectos.

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

3. Cree el rol de desarrollador para el proyecto-1.

```
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:
      - tridentsnapshots
EOF
```

La definición de rol proporcionada en esta sección es sólo un ejemplo. Las funciones de desarrollador deben definirse en función de los requisitos del usuario final.

1. Del mismo modo, cree roles de desarrollador para project-2.
2. Todos los recursos de almacenamiento de OpenShift y NetApp suelen gestionarse mediante un administrador de almacenamiento. El acceso a los administradores de almacenamiento se controla mediante el rol del operador trident que se crea al instalar Trident. Además, el administrador de almacenamiento también necesita acceder a ResourceQuotas para controlar el consumo del almacenamiento.
3. Cree un rol para administrar ResourceQuotas en todos los proyectos del clúster para adjuntarlo al administrador de almacenamiento.

```
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. Asegúrese de que el clúster esté integrado con el proveedor de identidades de la organización y de que los grupos de usuarios estén sincronizados con los grupos de clústeres. En el ejemplo siguiente se muestra que el proveedor de identidades se ha integrado con el clúster y se ha sincronizado con los grupos de usuarios.

```
$ 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. Configure ClusterRoleBindings para los administradores de almacenamiento.

```
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
```

Para los administradores de almacenamiento, deben enlazar dos roles: trident-operador y Resource-Quotas.

1. Cree RoleBindings para desarrolladores que vinculen la función de desarrollador-proyecto-1 al grupo correspondiente (ocp-project-1) en el proyecto-1.

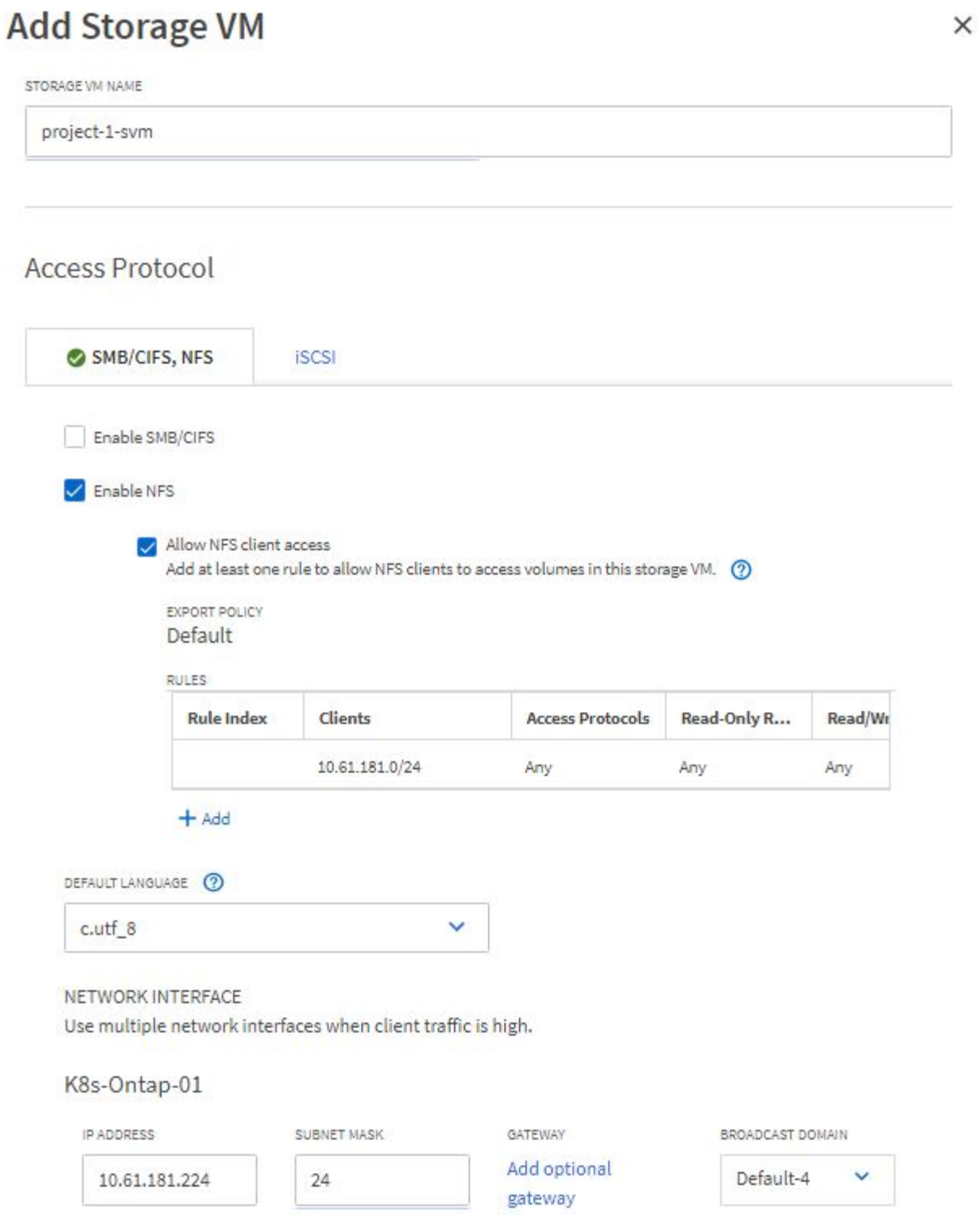
```
cat << EOF | oc create -f -
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: project-1-developer
  namespace: project-1
subjects:
  - kind: Group
    apiGroup: rbac.authorization.k8s.io
    name: ocp-project-1
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role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

2. De forma similar, cree RoleBindings para desarrolladores que vinculen las funciones de desarrollador al grupo de usuarios correspondiente en Project-2.

# Configuration: Tareas del administrador del almacenamiento

Un administrador de almacenamiento debe configurar los siguientes recursos:

1. Inicie sesión en el clúster de ONTAP de NetApp como administrador.
2. Vaya a almacenamiento > Storage VMs y haga clic en Add. Cree dos SVM, una para el proyecto-1 y otra para el proyecto-2, proporcionando los detalles necesarios. Además, cree una cuenta de vsadmin para gestionar la SVM y sus recursos.




1. Inicie sesión en el clúster de Red Hat OpenShift como administrador de almacenamiento.
2. Cree el back-end para el proyecto-1 y asígnelo a la SVM dedicada al proyecto. NetApp recomienda utilizar la cuenta vsadmin de la SVM para conectar el back-end a SVM en lugar de utilizar el administrador del clúster de ONTAP.

```
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
```

En este ejemplo, estamos usando el controlador ontap-nas. Utilice el controlador adecuado al crear el backend según el caso de uso.

Asumimos que Trident se instala en el proyecto trident.

1. De forma similar, cree el back-end de Trident para el proyecto-2 y asígnelo al proyecto 2 dedicado.
2. A continuación, cree las clases de almacenamiento. Cree la clase de almacenamiento para el proyecto-1 y configúrela para que utilice los pools de almacenamiento desde back-end dedicado al proyecto-1 mediante la configuración del parámetro storagePools.

```
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. Del mismo modo, cree una clase de almacenamiento para el proyecto 2 y configúrela para que utilice los pools de almacenamiento desde back-end dedicado al proyecto 2.
4. Cree un ResourceQuota para restringir los recursos del proyecto-1 solicitando el almacenamiento de storagegrid dedicado a otros proyectos.

```
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. Del mismo modo, cree un ResourceQuota para restringir los recursos del proyecto 2 solicitando almacenamiento de storagegrid dedicado a otros proyectos.

# Validación

Para validar la arquitectura multi-tenant configurada en los pasos anteriores, realice los siguientes pasos:

## Validar el acceso para crear RVP o pods en el proyecto asignado

1. Inicie sesión como ocp-project-1-usuario, desarrollador en proyecto-1.
2. Compruebe el acceso para crear un proyecto nuevo.

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

3. Cree un PVC en el proyecto-1 utilizando el storagegrid que está asignado al proyecto-1.

```
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. Compruebe el VP asociado a la RVP.

```
oc get pv
```

5. Validar que el VP y su volumen se crean en una SVM dedicada al proyecto-1 en ONTAP de NetApp.

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

6. Cree un pod en el proyecto-1 y monte el PVC creado en el paso anterior.

```
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. Compruebe si el pod está en ejecución y si montó el volumen.

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

## Validar el acceso para crear RVP o pods en otro proyecto o utilizar recursos dedicados a otro proyecto

1. Inicie sesión como ocp-project-1-usuario, desarrollador en proyecto-1.
2. Cree un PVC en el proyecto-1 utilizando el storagegrid que está asignado al proyecto-2.

```
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. Cree un PVC en el proyecto-2.

```
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. Asegúrese de que las EVs `test-pvc-project-1-sc-2` y.. `test-pvc-project-2-sc-1` no se han creado.

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

5. Cree un pod en el proyecto-2.

```
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
```

## Valide el acceso para ver y editar proyectos, ResourceQuotas y StorageClasses

1. Inicie sesión como ocp-project-1-usuario, desarrollador en proyecto-1.
2. Compruebe el acceso para crear nuevos proyectos.

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

3. Validar el acceso para ver los proyectos.

```
oc get ns
```

4. Compruebe si el usuario puede ver o editar ResourceQuotas en project-1.

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

5. Valide que el usuario tiene acceso para ver storagegrid.

```
oc get sc
```

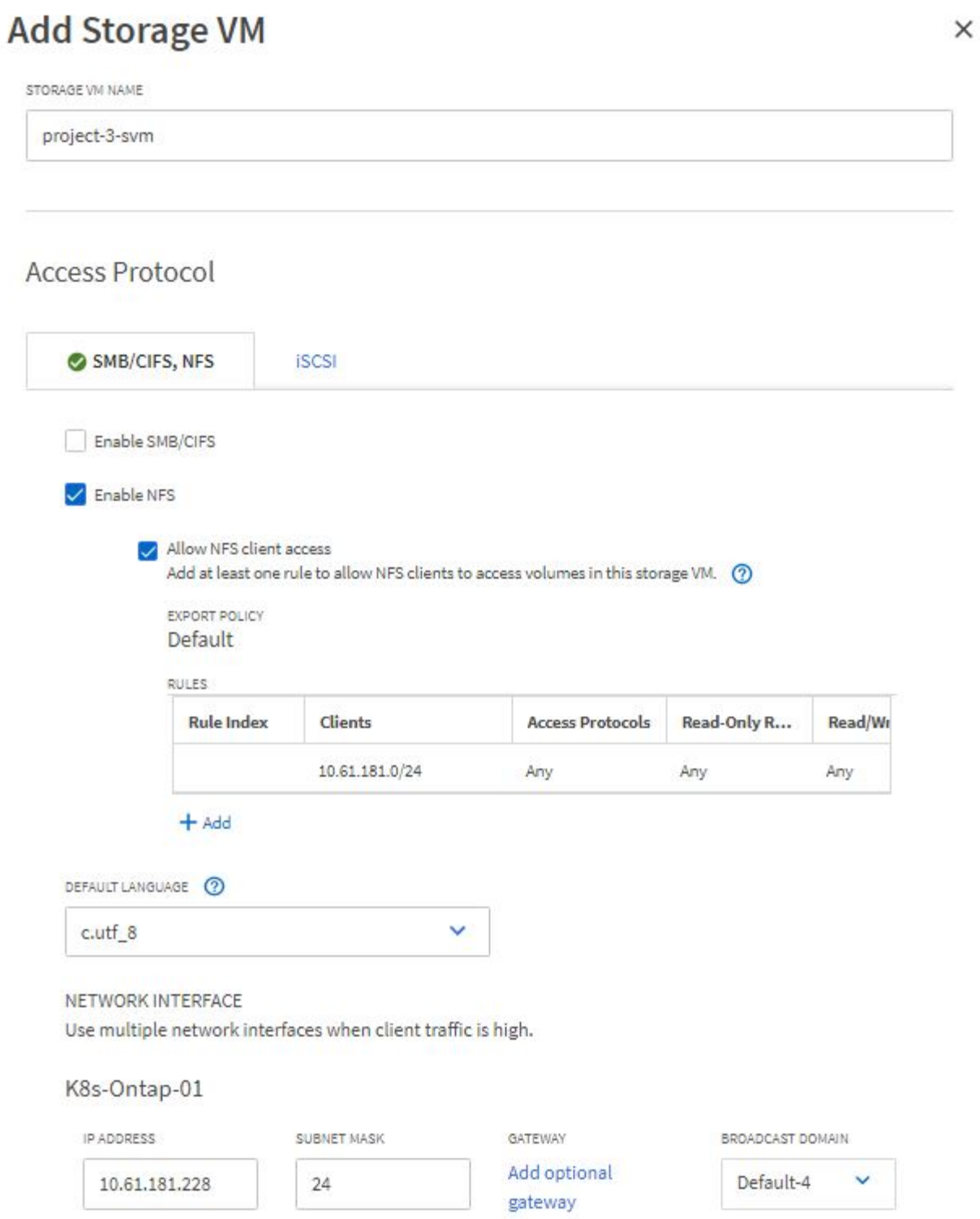
6. Compruebe el acceso para describir storagegrid.
7. Valide el acceso del usuario para editar storagegrid.

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

# Escala: Agregar más proyectos

En una configuración multitenant, agregar nuevos proyectos con recursos de almacenamiento requiere una configuración adicional para asegurarse de que no se infringe la multi-tenancy. Para agregar más proyectos en un clúster multitenant, realice los siguientes pasos:

1. Inicie sesión en el clúster de ONTAP de NetApp como administrador de almacenamiento.
2. Vaya a. `Storage` → `Storage VMs` y haga clic en `Add`. Cree una nueva SVM dedicada al proyecto-3. Además, cree una cuenta de vsadmin para gestionar la SVM y sus recursos.




1. Inicie sesión en el clúster de Red Hat OpenShift como administrador de clúster.
2. Cree un proyecto nuevo.

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

3. Asegúrese de que el grupo de usuarios para project-3 se crea en IDP y se sincroniza con el clúster

OpenShift.

```
oc get groups
```

4. Cree el rol de desarrollador para el proyecto-3.

```
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:
      - tridentsnapshots
EOF
```

> La definición de rol proporcionada en esta sección es sólo un ejemplo. La función de desarrollador debe definirse en función de los requisitos del usuario final.

1. Crear RoleBinding para desarrolladores en el proyecto-3 enlazar el rol de desarrollador-proyecto-3 al grupo correspondiente (ocp-proyecto-3) en el proyecto-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. Inicie sesión en el clúster Red Hat OpenShift como administrador de almacenamiento
3. Cree un back-end de Trident y asígnelo al SVM dedicado al proyecto-3. NetApp recomienda utilizar la cuenta vsadmin de la SVM para conectar el back-end a la SVM en lugar de utilizar el administrador del clúster de ONTAP.

```
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
```

> En este ejemplo, estamos usando el controlador ontap-nas. Utilice el controlador apropiado para crear el backend basado en el caso de uso.

> Asumimos que Trident se instala en el proyecto trident.

1. Cree la clase de almacenamiento para el proyecto-3 y configúrela para que utilice los pools de almacenamiento desde back-end dedicado al proyecto-3.

```
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. Cree un ResourceQuota para restringir los recursos del proyecto-3 solicitando almacenamiento de storagegrid dedicado a otros proyectos.

```
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. Aplicar un parche a ResourceQuotas en otros proyectos para restringir el acceso de los recursos de dichos proyectos al almacenamiento desde storageeclass dedicado al proyecto 3.

```
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}}}'
```

**Información de copyright**

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

**Información de la marca comercial**

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.