Configuration

NetApp Solutions

NetApp
April 20, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/netapp-solutions/containers/rh-os-n_use_case_multitenancy_configuration_prerequisites.html on April 20, 2024. Always check docs.netapp.com for the latest.

Sommaire

Configuration 1
Configuration 1
Configuration : tâches d’administration du cluster 2
Configuration : tâches d’administration du stockage 6
Validation 9
Évolutivité : ajout de projets 14

Configuration

N’importe quelle solution mutualisée permet à aucun utilisateur d’accéder à davantage de ressources du cluster que nécessaire. Ainsi, l’ensemble des ressources à configurer dans le cadre de la configuration de colocation est divisé entre l’administrateur cluster, l’administrateur stockage et les développeurs travaillant sur chaque projet.

Le tableau suivant présente les différentes tâches à effectuer par différents utilisateurs :

Rôle	Tâches
Cluster-admin	Créez des projets pour différentes applications ou charges de travail
	Créez ClusterRoles et roles pour Storage-admin
	Créez des rôles et des roleliaisons pour les développeurs qui assignaient un accès à des projets spécifiques
	[Facultatif] configurez les projets pour planifier des pods sur des nœuds spécifiques
Storage-admin	Créez des SVM sur NetApp ONTAP
	Création des systèmes back-end Trident
	Créez des classes de stockage
	Créer des devis de ressources de stockage
Développeurs	Valider l’accès pour créer ou corriger des demandes de volume persistant ou des pods dans le projet affecté
	Valider l’accès pour créer ou corriger des demandes de volume persistant ou des pods dans un autre projet
	Validez l’accès pour afficher ou modifier des projets, des ResourceQuotas et des classes de stockage

Configuration

Prérequis

- Cluster NetApp ONTAP
- Cluster Red Hat OpenShift
- Trident est installé sur le cluster
- Station de travail Admin avec les outils tridentctl et oc installés et ajoutés à $PATH
- Accès administrateur à ONTAP
- L’accès cluster-admin au cluster OpenShift
- Le cluster est intégré avec Identity Provider

- Le fournisseur d'identités est configuré pour distinguer efficacement les utilisateurs de différentes équipes

Configuration : tâches d'administration du cluster

Les tâches suivantes sont réalisées par Red Hat OpenShift Cluster-admin :

1. Connectez-vous au cluster Red Hat OpenShift en tant qu'administrateur cluster.
2. Créer deux projets correspondant à différents projets.

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

3. Créer le rôle de développeur du projet-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 définition de rôle fournie dans cette section n’est qu’un exemple. Les rôles de développeur doivent être définis en fonction des exigences de l’utilisateur final.

1. De la même façon, créez des rôles de développement pour Project-2.
2. Toutes les ressources de stockage OpenShift et NetApp sont généralement gérées par un administrateur du stockage. L’accès pour les administrateurs du stockage est contrôlé par le rôle de l’opérateur trident créé lors de l’installation de Trident. En outre, l’administrateur du stockage nécessite également l’accès à ResourceQuotas pour contrôler la consommation du stockage.
3. Créez un rôle pour gérer ResourceQuotas dans tous les projets du cluster afin de le relier à l’administrateur de stockage.

```
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. Assurez-vous que le cluster est intégré au fournisseur d'identité de l'entreprise et que les groupes d'utilisateurs sont synchronisés avec les groupes de clusters. L'exemple suivant montre que le fournisseur d'identités a été intégré au cluster et synchronisé avec les groupes d'utilisateurs.

```
$ 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. Configurer les liaisons ClusterRoleBindages pour les administrateurs de stockage.

```
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
```

Pour les administrateurs du stockage, deux rôles doivent être liés : trident-Operator et Resource-quotas.

1. Créer des liaisons de type rôle pour les développeurs liant le rôle développeur-projet-1 au groupe correspondant (ocp-project-1) dans Project-1.

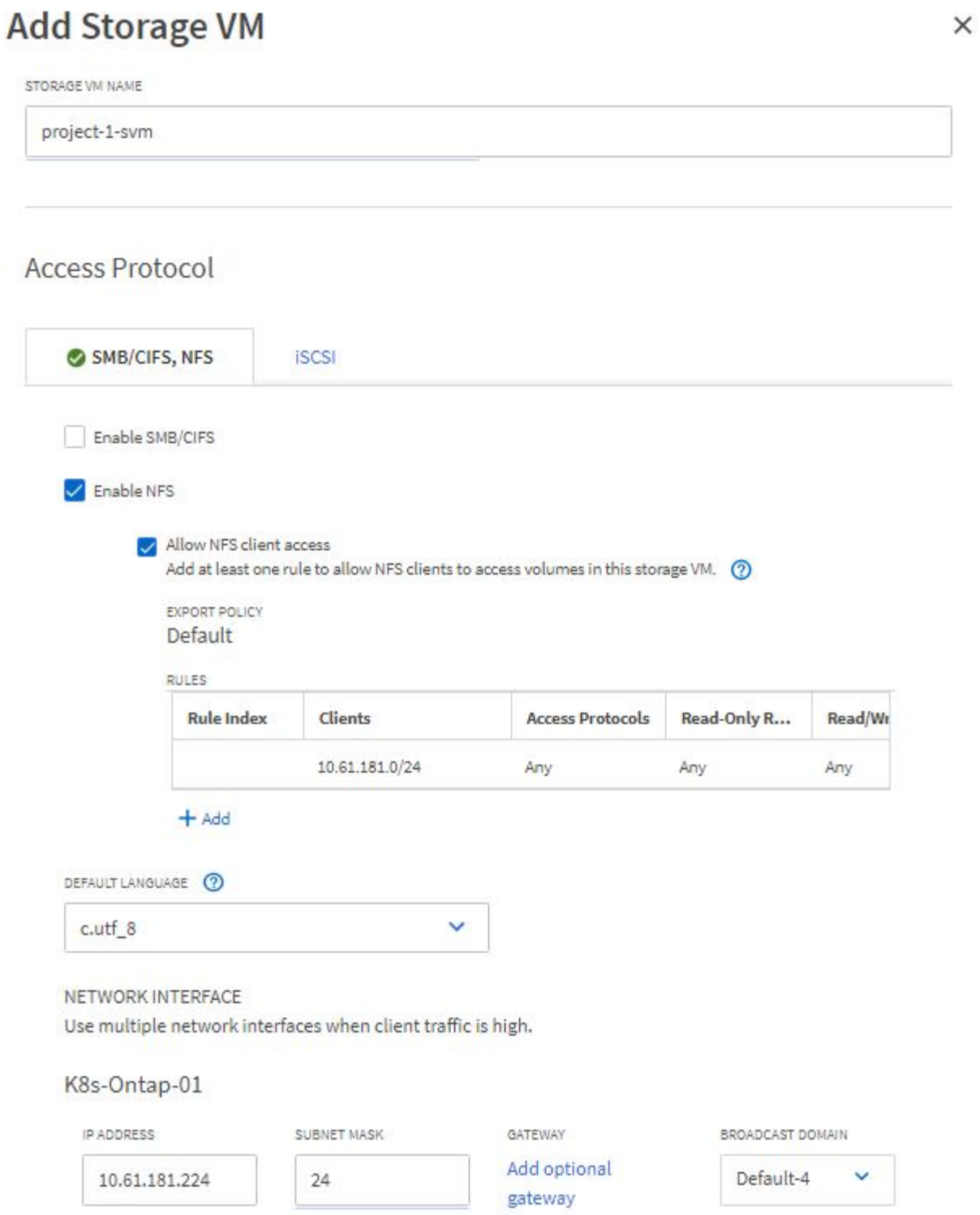
```
cat << EOF | oc create -f -
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: project-1-developer
  namespace: project-1
subjects:
  - kind: Group
    apiGroup: rbac.authorization.k8s.io
    name: ocp-project-1
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role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

2. De même, créez des liaisons de type rôle pour les développeurs qui lient les rôles de développeur au groupe d'utilisateurs correspondant dans Project-2.

Configuration : tâches d'administration du stockage

Les ressources suivantes doivent être configurées par un administrateur de stockage :

1. Connectez-vous au cluster NetApp ONTAP en tant qu'administrateur.
2. Accédez à Storage > Storage VM et cliquez sur Add. Créer deux SVM, un pour le projet-1 et l'autre pour le projet-2, en fournissant les détails requis. Créer également un compte vsadmin pour gérer le SVM et ses ressources



1. Connectez-vous au cluster Red Hat OpenShift en tant qu'administrateur du stockage.
2. Créer le backend pour projet-1 et le mapper au SVM dédié au projet NetApp recommande d'utiliser le compte vsadmin du SVM afin de connecter le backend au SVM au lieu d'utiliser l'administrateur du cluster 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
```

Nous utilisons le pilote ontap-nas dans cet exemple. Utilisez le pilote approprié lors de la création du back-end en fonction du cas d'utilisation.

Nous partons du principe que Trident est installé dans le projet trident.

1. Créer de la même manière le back-end Trident pour le projet-2 et le mapper sur le SVM dédié au projet-2.
2. Créez ensuite les classes de stockage. Créez la classe de stockage pour Project-1 et configurez-la pour utiliser les pools de stockage du back-end dédié au projet-1 en définissant le paramètre 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. De même, créez une classe de stockage pour Project-2 et configurez-la pour utiliser les pools de stockage du système back-end dédié au projet-2.
4. Créer un Resourcequota pour limiter les ressources dans le projet-1 demandant le stockage de storageclasses dédiés à d'autres projets.

```
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. De même, créez un Resourcequota pour limiter les ressources du projet 2 demandant du stockage de storageclasses dédiés à d'autres projets.

Validation

Pour valider l'architecture mutualisée configurée lors des étapes précédentes, procédez comme suit :

Valider l'accès pour créer des demandes de volume persistant ou des pods dans le projet attribué

1. Connectez-vous en tant qu'utilisateur ocp-project-1, développeur dans Project-1.
2. Vérifiez l'accès pour créer un nouveau projet.

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

3. Créez un PVC dans Project-1 en utilisant le storageclass affecté au projet-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. Vérifiez le volume persistant associé à la demande de volume persistant.

```
oc get pv
```

5. Vérifiez que le volume persistant et son volume sont créés dans un SVM dédié à Project-1 sur NetApp ONTAP.

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

6. Créez un pod dans Project-1 et montez le PVC créé à l'étape précédente.

```
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. Vérifiez si le pod est en cours d'exécution et si il a monté le volume.

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

Valider l'accès pour créer des demandes de volume persistant ou des pods dans un autre projet ou utiliser des ressources dédiées à un autre projet

1. Connectez-vous en tant qu'utilisateur ocp-project-1, développeur dans Project-1.
2. Créez un PVC dans Project-1 en utilisant le storageclass affecté au projet-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. Création d'une demande de volume persistant dans Project-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. Assurez-vous que les ESV `test-pvc-project-1-sc-2` et `test-pvc-project-2-sc-1` n'ont pas été créés.

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

5. Créez un pod dans Project-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
```

Validez l’accès pour afficher et modifier les projets, ResourceQuotas et Storageclasses

1. Connectez-vous en tant qu’utilisateur ocp-project-1, développeur dans Project-1.
2. Vérifiez l’accès pour créer de nouveaux projets.

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

3. Valider l’accès pour afficher les projets.

```
oc get ns
```

4. Vérifiez si l’utilisateur peut afficher ou modifier ResourceQuotas dans Project-1.

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

5. Vérifiez que l’utilisateur a accès à l’affichage des données de stockage.

```
oc get sc
```

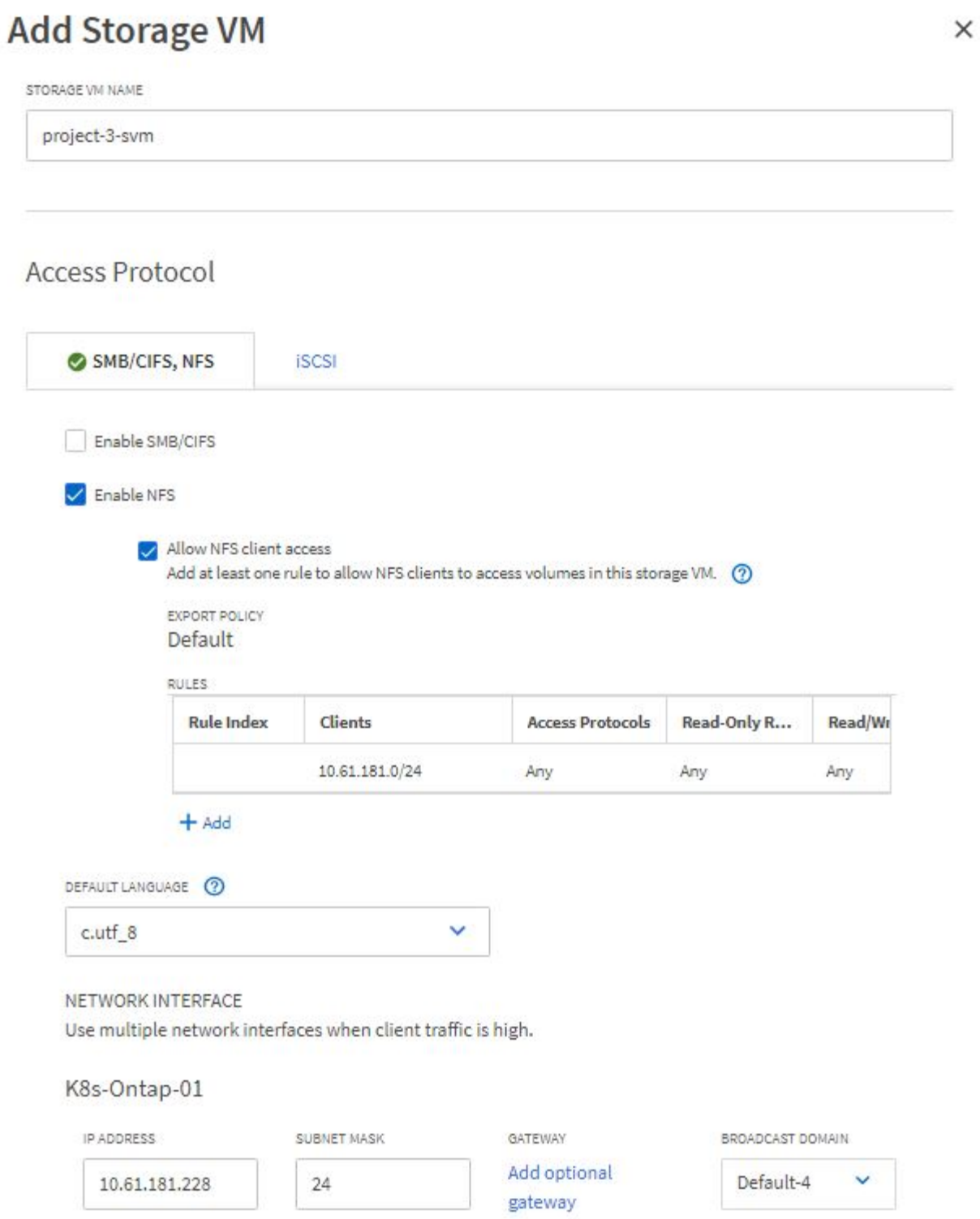
6. Vérifiez l’accès pour décrire les storageclasses.
7. Validez l’accès de l’utilisateur pour modifier les storageclasses.

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

Évolutivité : ajout de projets

Dans une configuration mutualisée, l'ajout de nouveaux projets avec des ressources de stockage nécessite une configuration supplémentaire pour garantir que la colocation n'est pas respectée. Pour ajouter d'autres projets dans un cluster mutualisé, effectuez les opérations suivantes :

1. Connectez-vous au cluster NetApp ONTAP en tant qu'administrateur du stockage.
2. Accédez à `Storage → Storage VMs` et cliquez sur `Add`. Créez un nouveau SVM dédié au projet-3. Créer également un compte vsadmin pour gérer le SVM et ses ressources



1. Connectez-vous au cluster Red Hat OpenShift en tant qu'administrateur de cluster.
2. Créer un nouveau projet.

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

3. Assurez-vous que le groupe d'utilisateurs du projet Project-3 est créé sur IDP et synchronisé avec le

cluster OpenShift.

```
oc get groups
```

4. Créer le rôle de développeur du projet-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 définition de rôle fournie dans cette section n'est qu'un exemple. Le rôle de développeur doit être défini en fonction des exigences de l'utilisateur final.

1. Créer RoleBinding pour les développeurs dans projet-3 liant le rôle développeur-projet-3 au groupe correspondant (ocp-project-3) dans projet-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. Connectez-vous au cluster Red Hat OpenShift en tant qu'administrateur du stockage
3. Créer un système back-end Trident et le mapper sur le SVM dédié au projet-3. NetApp recommande d'utiliser le compte vsadmin du SVM afin de connecter le backend au SVM au lieu d'utiliser l'administrateur du cluster 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
```

Nous utilisons le pilote ontap-nas dans cet exemple. Utilisez le pilote approprié pour créer le back-end en fonction du cas d'utilisation.

Nous partons du principe que Trident est installé dans le projet trident.

1. Créez la classe de stockage pour Project-3 et configurez-la pour qu'elle utilise les pools de stockage du système back-end dédié au projet-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. Créer un Resourcequota pour limiter les ressources dans le projet-3 demandant du stockage de storageclasses dédié à d'autres projets.

```
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. Patch des ResourceQuotas dans d'autres projets pour limiter les ressources de ces projets à l'accès au stockage depuis le storageclass dédié au projet-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}}}'
```

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.