



Recommandation de bonnes pratiques

NetApp Solutions

NetApp
September 26, 2024

Sommaire

- Recommandation de bonnes pratiques 1
 - Recommandations sur les meilleures pratiques pour les VM dans Red Hat OpenShift Virtualization 1

Recommandation de bonnes pratiques

Recommandations sur les meilleures pratiques pour les VM dans Red Hat OpenShift Virtualization

Auteur: Banu Sundhar, NetApp

Cette section décrit les différents facteurs à prendre en compte lors du déploiement de nouvelles machines virtuelles ou de l'importation de machines virtuelles existantes à partir d'une instance VMware vSphere dans OpenShift Virtualization sur OpenShift Container Platform.

Performances des VM

Lors de la création d'une nouvelle machine virtuelle dans OpenShift Virtualization, vous devez tenir compte du modèle d'accès et des exigences de performances (IOPS et débit) de la charge de travail qui s'exécutera sur la machine virtuelle. Cela aura une incidence sur le nombre de machines virtuelles à exécuter sur OpenShift Virtualization dans une plateforme de conteneurs OpenShift et sur le type de stockage à utiliser pour les disques de machines virtuelles.

Le type de stockage que vous souhaitez choisir pour vos disques de machine virtuelle dépend des facteurs suivants :

- Le protocole d'accès dont vous avez besoin pour assurer l'accès aux données de vos workloads
- Les modes d'accès dont vous avez besoin (RWO vs RWX)
- Les caractéristiques de performance dont vous avez besoin pour vos workloads

Pour plus d'informations, reportez-vous à la section Configuration du stockage ci-dessous.

Haute disponibilité des workloads de machines virtuelles

OpenShift Virtualization prend en charge les migrations dynamiques d'une machine virtuelle. La migration dynamique permet à une instance de machine virtuelle (VMI) en cours d'exécution de se déplacer vers un autre nœud sans interrompre la charge de travail. La migration peut s'avérer utile pour assurer une transition en douceur lors des mises à niveau des clusters ou lorsqu'un nœud doit être vidangé à des fins de maintenance ou de modification de la configuration. La migration dynamique nécessite l'utilisation d'une solution de stockage partagé qui fournit le mode d'accès ReadWriteMany (RWX). Les disques VM doivent être sauvegardés par l'option de stockage qui fournit le mode d'accès RWX. OpenShift Virtualization vérifiera qu'un VMI est **migrable en direct** et si tel est le cas, la **eviction Strategy** sera définie sur **LiveMigrate**. Voir "[À propos de la migration en direct dans la documentation Red Hat](#)" pour plus de détails.

Il est important d'utiliser un pilote qui prend en charge le mode d'accès **RWX**. Reportez-vous à la section Configuration du stockage ci-dessous pour plus de détails sur les pilotes ONTAP qui prennent en charge le mode d'accès RWX.

Configuration du stockage

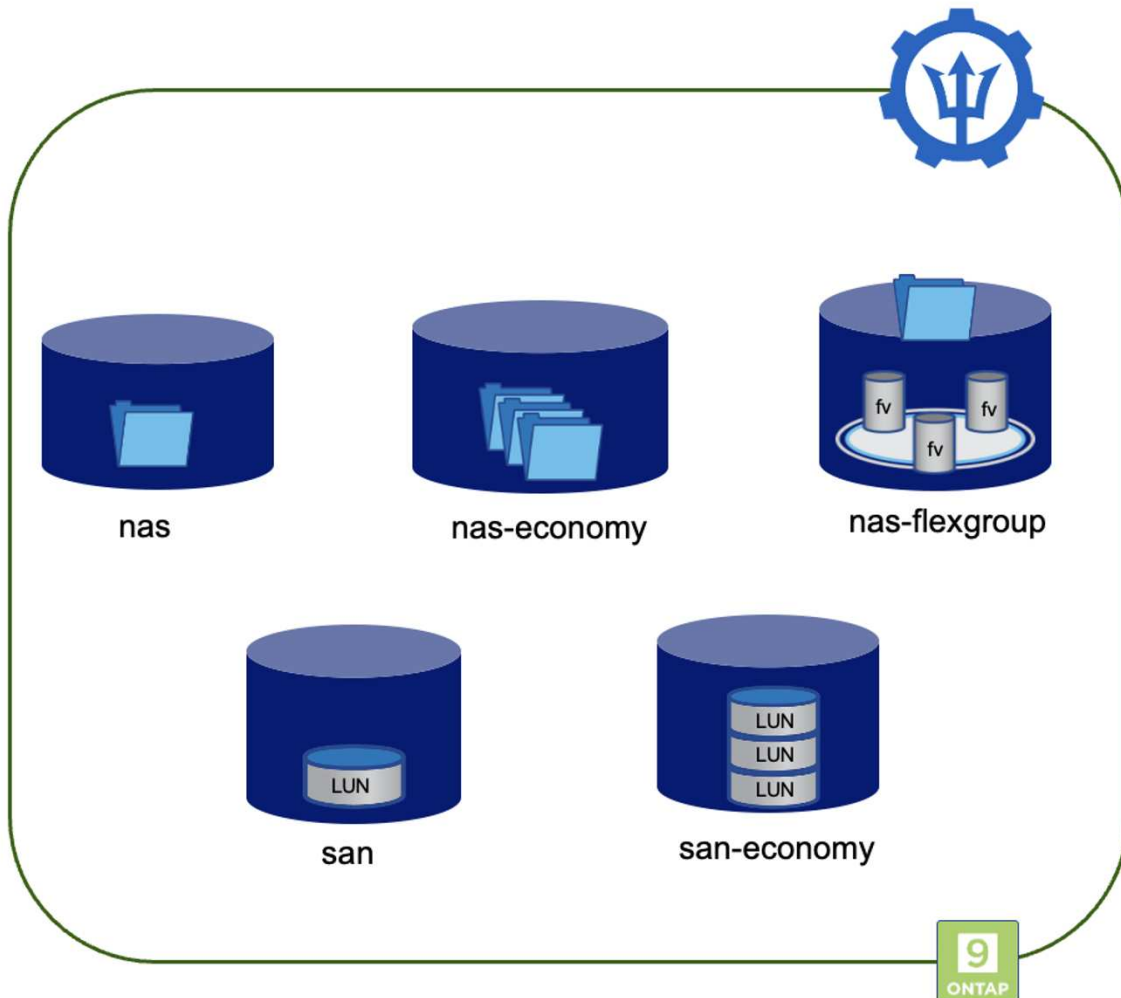
Le mécanisme de provisionnement Trident CSI fournit plusieurs facteurs (nas, économie nas, nas-FlexGroup, san et économie san) pour le provisionnement du stockage reposant sur les options de stockage NetApp.

Protocoles utilisés : * les pilotes nas utilisent des protocoles NAS (NFS et SMB) * les pilotes san utilisent le protocole iSCSI ou NVMe/TCP

Les éléments suivants vous aideront à décider de la configuration du stockage en fonction des exigences des charges de travail et de l'utilisation du stockage.

- **Pilote nas** crée un volume persistant (PV) sur un volume FlexVolume.
- **Pilote nas-economy** crée un PV sur un qtree sur un FlexVolume partagé. (Un FlexVolume pour 200 PVS, configurable entre 50 et 300)
- **Pilote nas-FlexGroup** crée sur un PV sur un FlexGroup
- Un pilote san crée un volume persistant sur une LUN sur un FlexVolume dédié
- **Pilote san-economy** crée un PV sur LUN sur FlexVolume partagé (un FlexVolume pour 100 PVS, configurable entre 50 et 200)

Le schéma suivant illustre cette situation.



De plus, les modes d'accès pris en charge par les pilotes diffèrent.

Prise en charge des pilotes nas ONTAP

- Accès au système de fichiers et modes d'accès RWO, ROX, RWX, RWOP.

Les pilotes san ONTAP prennent en charge les modes bloc brut ainsi que les modes de système de fichiers

- En mode bloc brut, il peut prendre en charge les modes d'accès RWO, ROX, RWX, RWOP.
- En mode système de fichiers, seuls les modes d'accès RWO et RWOP sont autorisés.

La migration dynamique des VM de virtualisation OpenShift nécessite que les disques disposent de modes d'accès RWX. Il est donc important de choisir des pilotes nas ou san en mode de volume de bloc brut pour créer des demandes de volume persistant et des volumes persistants soutenus par ONTAP.

Meilleures pratiques en matière de configuration du stockage

Machines virtuelles de stockage dédiées (SVM)

Les machines virtuelles de stockage (SVM) assurent l'isolation et la séparation administrative entre les locataires sur un système ONTAP. Le fait de dédier un SVM aux conteneurs OpenShift et aux VM de virtualisation OpenShift permet de déléguer Privileges et d'appliquer les bonnes pratiques afin de limiter l'utilisation des ressources.

Limiter le nombre maximal de volumes sur le SVM

Pour empêcher Trident de consommer tous les volumes disponibles sur le système de stockage, vous devez définir une limite sur la SVM. Vous pouvez le faire à partir de la ligne de commande :

```
vserver modify -vserver <svm_name> -max-volumes <num_of_volumes>
```

La valeur max-volumes correspond à l'ensemble des volumes provisionnés sur tous les nœuds du cluster ONTAP et non sur un nœud ONTAP individuel. Par conséquent, vous pouvez rencontrer des situations où un nœud de cluster ONTAP peut avoir plus ou moins de volumes provisionnés Trident qu'un autre nœud. Pour éviter cela, veiller à ce qu'un nombre égal d'agrégats de chaque nœud du cluster soit affecté au SVM utilisé par Trident.

Limiter la taille maximale des volumes créés par Trident

Il est possible de définir une taille maximale de volume par SVM dans ONTAP :

1. Créer le SVM avec la commande vserver create et définir la limite Storage :

```
vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume  
root_volume_name -rootvolume-security-style {unix|ntfs|mixed} -storage  
-limit value
```

1. Pour modifier la limite de stockage sur un SVM existant :

```
vserver modify -vserver vserver_name -storage-limit value -storage-limit
-threshold-alert percentage
```



Les limites de stockage ne peuvent pas être configurées pour des SVM contenant des volumes de protection des données, des volumes dans une relation SnapMirror ou dans une configuration MetroCluster.

Vous devez aussi exploiter les fonctionnalités Kubernetes pour contrôler la taille du volume au niveau de la baie de stockage.

1. Pour configurer la taille maximale des volumes pouvant être créés par Trident, utilisez le paramètre **limitVolumeSize** de votre définition backend.json.
2. Pour configurer la taille maximale des volumes FlexVol utilisés comme pools pour les pilotes ONTAP-san-Economy et ONTAP-nas-Economy, utilisez le paramètre **limitVolumePoolSize** dans votre définition backend.json.

Utiliser la politique de QoS de SVM

Appliquer des règles de qualité de service (QoS) au SVM afin de limiter le nombre d'IOPS consommables par les volumes Trident provisionnés. Cela permet d'éviter que les charges de travail utilisant le stockage provisionné Trident n'affectent les charges de travail en dehors du SVM Trident.

Les groupes de règles de QoS ONTAP proposent des options de QoS pour les volumes et permettent aux utilisateurs de définir le plafond de débit pour une ou plusieurs charges de travail. Pour plus d'informations sur les groupes de règles de QoS, reportez-vous à la section "[Commandes QoS de ONTAP 9.15](#)"

Limiter l'accès aux ressources de stockage aux membres du cluster Kubernetes

Utiliser des namespaces la limitation de l'accès aux volumes NFS et aux LUN iSCSI créés par Trident est un composant essentiel de la stratégie de sécurité pour votre déploiement Kubernetes. En effet, les hôtes qui ne font pas partie du cluster Kubernetes n'accèdent pas aux volumes et peuvent modifier les données de façon inattendue.

En outre, un processus dans un conteneur peut accéder au stockage monté sur l'hôte, mais qui n'est pas destiné au conteneur. L'utilisation d'espaces de noms pour fournir des limites logiques aux ressources peut éviter ce problème. Cependant,

Il est important de comprendre que les espaces de noms sont la limite logique des ressources dans Kubernetes. Il est donc essentiel de s'assurer que les espaces de noms sont utilisés pour assurer la séparation lorsque cela est approprié. Cependant, les conteneurs privilégiés s'exécutent avec beaucoup plus d'autorisations au niveau de l'hôte que la normale. Désactivez donc cette fonctionnalité en utilisant "[stratégies de sécurité des pods](#)".

Utiliser une stratégie d'exportation dédiée pour les déploiements OpenShift qui ont des nœuds d'infrastructure dédiés ou d'autres nœuds qui ne sont pas en mesure de planifier des applications utilisateur, des règles d'exportation distinctes doivent être utilisées pour limiter davantage l'accès aux ressources de stockage. Cela inclut la création d'une export policy pour les services qui sont déployés sur ces nœuds d'infrastructure (par exemple les services OpenShift Metrics et Logging Services), ainsi que pour les applications standard déployées sur des nœuds non liés à l'infrastructure.

Trident peut créer et gérer automatiquement des règles d'export. Trident limite ainsi l'accès aux volumes qu'il

provisionne aux nœuds du cluster Kubernetes et simplifie l'ajout et la suppression des nœuds.

Toutefois, si vous choisissez de créer une export-policy manuellement, remplissez-la avec une ou plusieurs règles d'export qui traitent chaque demande d'accès au nœud.

Désactiver showmount pour l'application SVM Un pod déployé dans le cluster Kubernetes peut exécuter la commande `showmount -e` sur la LIF de données et recevoir une liste des montages disponibles, y compris ceux auxquels il n'a pas accès. Pour éviter cela, désactivez la fonction `showmount` à l'aide de l'interface de ligne de commande suivante :

```
vserver nfs modify -vserver <svm_name> -showmount disabled
```



Pour plus d'informations sur les meilleures pratiques de configuration du stockage et d'utilisation de Trident, consultez "[Documentation Trident](#)".

OpenShift Virtualization - Guide de réglage et d'évolutivité

Red Hat a documenté "[Recommandations et limites de l'évolutivité d'OpenShift Cluster](#)".

En outre, ils ont également documenté "[Guide d'optimisation de la virtualisation OpenShift](#)" et "[Limites prises en charge pour OpenShift Virtualization 4.x](#)".



Un abonnement Red Hat actif est requis pour accéder au contenu ci-dessus.

Le guide de réglage contient des informations sur de nombreux paramètres de réglage, notamment :

- Réglage des paramètres pour créer de nombreuses machines virtuelles à la fois ou par lots volumineux
- Migration en direct des machines virtuelles
- "[Configuration d'un réseau dédié pour la migration en direct](#)"
- Personnalisation d'un modèle de machine virtuelle en incluant un type de charge de travail

Les limites prises en charge documentent les valeurs maximales d'objet testées lors de l'exécution de VM sur OpenShift

Maximums de machine virtuelle incluant

- Nombre max. De CPU virtuels par machine virtuelle
- Mémoire minimale et maximale par machine virtuelle
- Taille maximale d'un seul disque par machine virtuelle
- Nombre maximal de disques enfichables à chaud par machine virtuelle

Maximum d'hôtes incluant * migrations simultanées en direct (par nœud et par cluster)

Cluster maximums incluant * nombre maximum de VM définies

Migration des machines virtuelles à partir de l'environnement VMware

Migration Toolkit pour OpenShift Virtualization est un opérateur fourni par Red Hat, disponible auprès d'OperatorHub de la plateforme de conteneurs OpenShift. Cet outil permet de migrer des machines virtuelles

depuis vSphere, Red Hat Virtualization, OpenStack et OpenShift Virtualization.

Pour plus d'informations sur la migration des machines virtuelles à partir de vSphere, reportez-vous à la section ["Workflows ; Red Hat OpenShift Virtualization avec NetApp ONTAP"](#)

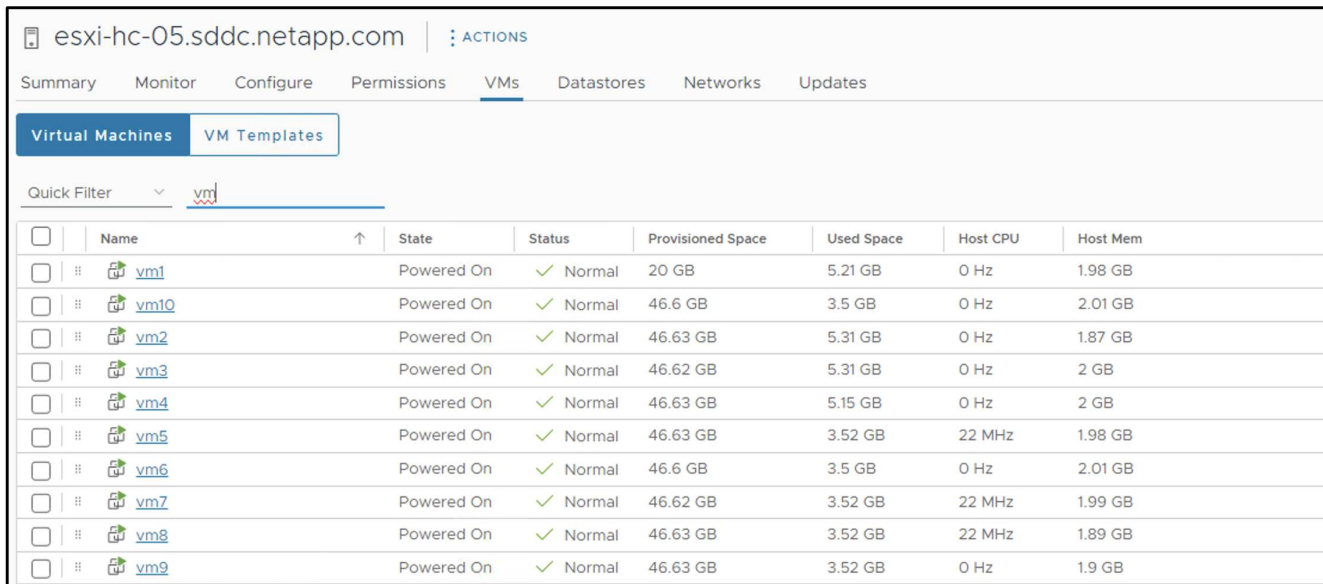
Vous pouvez configurer des limites pour divers paramètres à partir de l'interface de ligne de commande ou de la console Web de migration. Certains échantillons sont donnés ci-dessous

1. Nombre maximal de migrations simultanées de machines virtuelles définit le nombre maximal de machines virtuelles pouvant être migrées simultanément. La valeur par défaut est 20 machines virtuelles.
2. Intervalle de précopie (minutes) contrôle l'intervalle auquel un nouvel instantané est demandé avant le lancement d'une migration à chaud. La valeur par défaut est 60 minutes.
3. L'intervalle d'interrogation des snapshots (en secondes) détermine la fréquence à laquelle le système vérifie l'état de création ou de suppression des snapshots pendant la migration à chaud oVirt. La valeur par défaut est 10 secondes.

Si vous migrez plus de 10 machines virtuelles à partir d'un hôte ESXi dans le même plan de migration, vous devez augmenter la mémoire du service NFC de l'hôte. Sinon, la migration échouera car la mémoire de service NFC est limitée à 10 connexions parallèles. Pour plus de détails, consultez la documentation Red Hat : ["Augmentation de la mémoire de service NFC d'un hôte ESXi"](#)

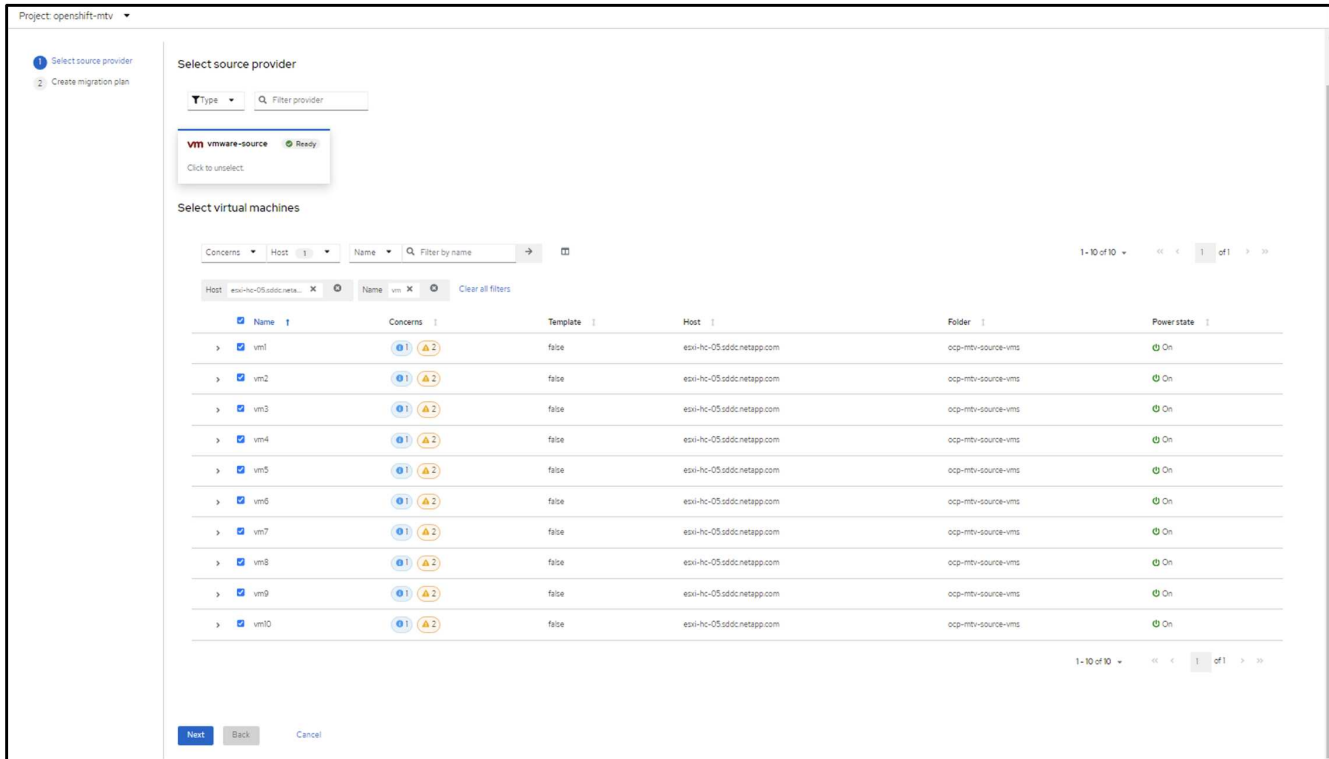
Voici une migration parallèle réussie de 10 machines virtuelles du même hôte dans vSphere vers OpenShift Virtualization à l'aide de migration Toolkit pour la virtualisation.

VM sur le même hôte ESXi

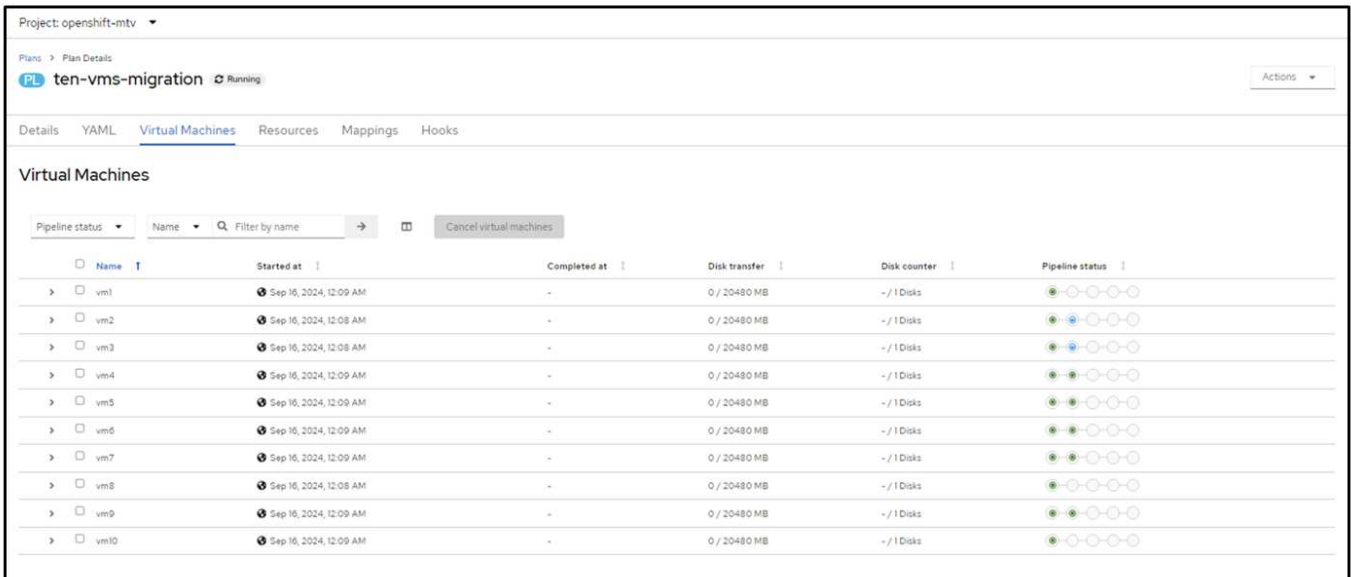


<input type="checkbox"/>	Name	↑	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
<input type="checkbox"/>	vm1		Powered On	✓ Normal	20 GB	5.21 GB	0 Hz	1.98 GB
<input type="checkbox"/>	vm1Q		Powered On	✓ Normal	46.6 GB	3.5 GB	0 Hz	2.01 GB
<input type="checkbox"/>	vm2		Powered On	✓ Normal	46.63 GB	5.31 GB	0 Hz	1.87 GB
<input type="checkbox"/>	vm3		Powered On	✓ Normal	46.62 GB	5.31 GB	0 Hz	2 GB
<input type="checkbox"/>	vm4		Powered On	✓ Normal	46.63 GB	5.15 GB	0 Hz	2 GB
<input type="checkbox"/>	vm5		Powered On	✓ Normal	46.63 GB	3.52 GB	22 MHz	1.98 GB
<input type="checkbox"/>	vm6		Powered On	✓ Normal	46.6 GB	3.5 GB	0 Hz	2.01 GB
<input type="checkbox"/>	vm7		Powered On	✓ Normal	46.62 GB	3.52 GB	22 MHz	1.99 GB
<input type="checkbox"/>	vm8		Powered On	✓ Normal	46.63 GB	3.52 GB	22 MHz	1.89 GB
<input type="checkbox"/>	vm9		Powered On	✓ Normal	46.63 GB	3.52 GB	0 Hz	1.9 GB

Un plan est d'abord créé pour la migration de 10 machines virtuelles à partir de VMware



L'exécution du plan de migration a commencé



Les 10 VM ont migré avec succès

Project: openshift-mtv

Plans > Plan Details

ten-vms-from-same-host Succeeded Actions

Details **YAML** Virtual Machines Resources Mappings Hooks

Virtual Machines

Pipeline status Name Filter by name Remove virtual machines

Name	Started at	Completed at	Disk transfer	Disk counter	Pipeline status
vm1	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:41 AM	20480 / 20480 MB	- / 1 Disks	● ● ● ● ● ● ● ● ● ●
vm2	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:41 AM	20480 / 20480 MB	- / 1 Disks	● ● ● ● ● ● ● ● ● ●
vm3	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:38 AM	20480 / 20480 MB	- / 1 Disks	● ● ● ● ● ● ● ● ● ●
vm4	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:42 AM	20480 / 20480 MB	- / 1 Disks	● ● ● ● ● ● ● ● ● ●
vm5	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:42 AM	20480 / 20480 MB	- / 1 Disks	● ● ● ● ● ● ● ● ● ●
vm6	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:37 AM	20480 / 20480 MB	- / 1 Disks	● ● ● ● ● ● ● ● ● ●
vm7	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:38 AM	20480 / 20480 MB	- / 1 Disks	● ● ● ● ● ● ● ● ● ●
vm8	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:37 AM	20480 / 20480 MB	- / 1 Disks	● ● ● ● ● ● ● ● ● ●
vm9	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:38 AM	20480 / 20480 MB	- / 1 Disks	● ● ● ● ● ● ● ● ● ●
vm10	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:37 AM	20480 / 20480 MB	- / 1 Disks	● ● ● ● ● ● ● ● ● ●

Les 10 machines virtuelles sont en cours d'exécution dans OpenShift Virtualization

Project: ten-vms-from-same-host

VirtualMachines

Filter Name Search by name... 1-10 of 10 1 of 1

Name	Status	Conditions	Node	IP address
vm1	Running		ocp7-worker3	-
vm2	Running		ocp7-worker1	-
vm3	Running		ocp7-worker2	-
vm4	Running		ocp7-worker1	-
vm5	Running		ocp7-worker2	-
vm6	Running		ocp7-worker2	-
vm7	Running		ocp7-worker1	-
vm8	Running		ocp7-worker3	-
vm9	Running		ocp7-worker2	-
vm10	Running		ocp7-worker1	-

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 DÉLICTEUELLE (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.