



Consigli sulle Best practice

NetApp Solutions

NetApp
September 26, 2024

Sommario

- Consigli sulle Best practice 1
- Consigli sulle Best practice per le macchine virtuali in Red Hat OpenShift Virtualization 1

Consigli sulle Best practice

Consigli sulle Best practice per le macchine virtuali in Red Hat OpenShift Virtualization

Autore: Banu Sundhar, NetApp

Questa sezione descrive i diversi fattori da prendere in considerazione quando si implementano nuove macchine virtuali o quando si importano macchine virtuali esistenti da VMware vSphere nella virtualizzazione OpenShift su OpenShift Container Platform.

Performance delle macchine virtuali

Quando si crea una nuova macchina virtuale nella virtualizzazione OpenShift, è necessario considerare il modello di accesso insieme ai requisiti di performance (IOPS e throughput) del carico di lavoro che verrà eseguito sulla macchina virtuale. Ciò influirà sul numero di VM da eseguire su OpenShift Virtualization in una piattaforma OpenShift Container e sul tipo di storage da utilizzare per i dischi VM.

Il tipo di storage che si desidera scegliere per i dischi VM è influenzato dai seguenti fattori:

- L'accesso al protocollo di cui hai bisogno per l'accesso ai dati dei tuoi carichi di lavoro
- Le modalità di accesso necessarie (RWO vs RWX)
- Le caratteristiche di performance necessarie per i carichi di lavoro

Per ulteriori informazioni, consultare la sezione Storage Configuration (Configurazione storage) riportata di seguito.

Elevata disponibilità dei carichi di lavoro VM

OpenShift Virtualization supporta le migrazioni Live di una VM. La migrazione in tempo reale consente a un'istanza VMI (Virtual Machine Instance) in esecuzione di spostarsi su un altro nodo senza interrompere il carico di lavoro. La migrazione può essere utile per una transizione agevole durante gli upgrade del cluster o in qualsiasi momento in cui un nodo deve essere drenato in caso di manutenzione o modifiche alla configurazione. La migrazione in tempo reale richiede l'utilizzo di una soluzione di archiviazione condivisa che fornisca la modalità di accesso a ReadWriteMany (RWX). Il backup dei dischi della VM deve essere eseguito mediante un'opzione di archiviazione che fornisce la modalità di accesso RWX. OpenShift Virtualization verificherà che un VMI sia **live migratable** e in tal caso la **evictionStrategy** sarà impostata su **LiveMigrate**. Per ulteriori informazioni, vedere ["Sezione sulla migrazione live nella documentazione di Red Hat"](#).

È importante utilizzare un driver che supporti la modalità di accesso **RWX**. Per ulteriori informazioni sui driver ONTAP che supportano la modalità di accesso RWX, vedere la sezione Configurazione archiviazione riportata di seguito.

Configurazione dello storage

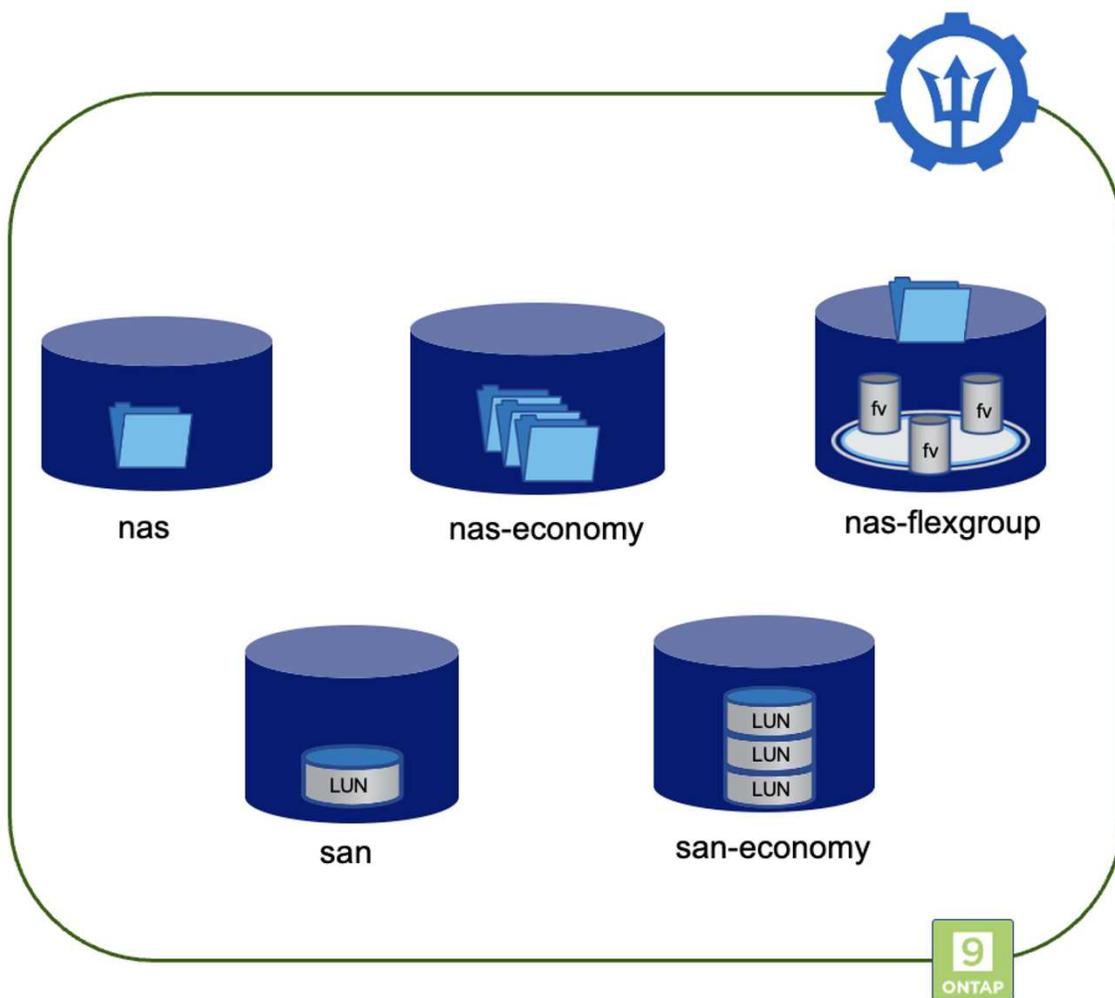
Il provisioner Trident CSI offre diversi driver (nas, nas-Economy, nas-FlexGroup, san e economia san) per il provisioning dello storage supportato dalle opzioni storage NetApp.

Protocolli utilizzati: * i driver nas utilizzano protocolli NAS (NFS e SMB) * i driver san utilizzano il protocollo iSCSI o NVMe/TCP

Di seguito è possibile scegliere la configurazione dello storage desiderata in base ai requisiti del carico di lavoro e all'utilizzo dello storage.

- Il driver **nas** crea un volume persistente (PV) su un FlexVolume.
- Il driver **nas-Economy** crea un PV su un qtree su un FlexVolume condiviso. (Un FlexVolume per ogni 200 PVS, configurabile tra 50 e 300 TB)
- Il driver **nas-FlexGroup** crea su un PV su un FlexGroup
- Il driver **san** crea un PV su LUN su un FlexVolume dedicato
- Il driver **san-Economy** crea un PV su LUN su FlexVolume condiviso (un FlexVolume per ogni 100 PVS, configurabile tra 50 e 200)

Lo schema seguente lo illustra.



Inoltre, le modalità di accesso supportate dai driver sono diverse.

Supporto driver nas ONTAP

- Accesso al filesystem e modalità di accesso RWO, ROX, RWX, RWOP.

I driver ONTAP san supportano sia il blocco raw che le modalità del filesystem

- Nella modalità di blocco RAW, può supportare modalità di accesso RWO, ROX, RWX, RWOP.
- Nella modalità filesystem, sono consentite solo le modalità di accesso RWO, RWOP.

La migrazione live delle VM di virtualizzazione OpenShift richiede che i dischi dispongano delle modalità di accesso RWX. Pertanto, è importante scegliere driver nas o driver san in modalità volume a blocchi raw per creare PVC e PVC supportati da ONTAP.

Best practice per la configurazione dello storage

Storage Virtual Machine (SVM) dedicate

Le macchine virtuali di storage (SVM) forniscono isolamento e separazione amministrativa tra tenant su un sistema ONTAP. L'impiego di una SVM ai container OpenShift e alle macchine virtuali di virtualizzazione OpenShift consente la delega di Privileges e l'applicazione delle Best practice per la limitazione del consumo delle risorse.

Limitare il conteggio massimo dei volumi sulla SVM

Per evitare che Trident utilizzi tutti i volumi disponibili sul sistema storage, è necessario impostare un limite per SVM. È possibile eseguire questa operazione dalla riga di comando:

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

Il valore di max-volumi è il volume totale fornito in tutti i nodi del cluster ONTAP, non su un singolo nodo ONTAP. Di conseguenza, potrebbero verificarsi alcune condizioni in cui un nodo del cluster ONTAP potrebbe avere volumi con provisioning Trident molto più o meno elevati rispetto a un altro nodo. Per evitare questo problema, assicurati che alla SVM utilizzata da Trident sia assegnato lo stesso numero di aggregati per ciascun nodo del cluster.

Limitare le dimensioni massime dei volumi creati da Trident

Puoi impostare un limite per le dimensioni massime del volume su base per SVM in ONTAP:

1. Creare l'SVM con il comando vserver create e impostare il limite di storage:

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

1. Per modificare il limite di storage su una SVM esistente:

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



I limiti di storage non possono essere configurati per qualsiasi SVM che contiene volumi di protezione dei dati, volumi in una relazione SnapMirror o in una configurazione MetroCluster.

Oltre a controllare le dimensioni del volume nell'array di storage, è necessario sfruttare le funzionalità di Kubernetes.

1. Per configurare la dimensione massima per i volumi che possono essere creati da Trident, utilizzare il parametro **limitVolumeSize** nella definizione backend.json.
2. Per configurare le dimensioni massime dei FlexVol utilizzati come pool per i driver ONTAP-san-economy e ONTAP-nas-economy, utilizzare il parametro **limitVolumePoolSize** nella definizione backend.json.

Usa policy QOS SVM

Applicare la policy di qualità del servizio alla SVM per limitare il numero di IOPS consumabili dai volumi oggetto del provisioning di Trident. In questo modo è possibile prevenire l'impatto dei workload che utilizzano lo storage con provisioning Trident sui workload esterni alla SVM di Trident.

I gruppi di policy QoS ONTAP offrono opzioni di qualità del servizio per i volumi e consentono agli utenti di definire il limite massimo di throughput per uno o più carichi di lavoro. Per ulteriori informazioni sui gruppi di criteri QoS, fare riferimento a. "[Comandi QoS di ONTAP 9.15](#)"

Limitare l'accesso alle risorse di storage ai membri del cluster Kubernetes

Usa Namespaces limitare l'accesso ai volumi NFS e alle LUN iSCSI create da Trident è un componente critico della postura di sicurezza per l'implementazione di Kubernetes. In questo modo si impedisce agli host che non fanno parte del cluster Kubernetes di accedere ai volumi e di modificare i dati in modo imprevisto.

Inoltre, un processo in un contenitore può accedere all'archivio montato sull'host, ma che non è destinato al contenitore. L'utilizzo di Namespaces per fornire un limite logico per le risorse può evitare questo problema. Tuttavia,

È importante comprendere che gli spazi dei nomi sono il limite logico delle risorse in Kubernetes. Pertanto, è fondamentale garantire che gli spazi dei nomi vengano utilizzati per fornire la separazione quando appropriato. Tuttavia, i container con privilegi vengono eseguiti con un numero sostanzialmente maggiore di autorizzazioni a livello di host rispetto al normale. Pertanto, disattivare questa funzionalità utilizzando "[policy di sicurezza pod](#)".

Utilizzare una policy di esportazione dedicata per le distribuzioni OpenShift che hanno nodi di infrastruttura dedicati o altri nodi che non sono in grado di pianificare applicazioni utente, è necessario utilizzare policy di esportazione separate per limitare ulteriormente l'accesso alle risorse di archiviazione. Ciò include la creazione di una policy di esportazione per i servizi implementati nei nodi dell'infrastruttura (ad esempio, i servizi OpenShift Metrics e Logging) e le applicazioni standard implementate nei nodi non dell'infrastruttura.

Trident può creare e gestire automaticamente le policy di esportazione. In questo modo, Trident limita l'accesso ai volumi che fornisce ai nodi nel cluster Kubernetes e semplifica l'aggiunta/eliminazione dei nodi.

Tuttavia, se si sceglie di creare manualmente un criterio di esportazione, compilarlo con una o più regole di esportazione che elaborano ogni richiesta di accesso al nodo.

Disattiva showmount per l'applicazione SVM Un pod implementato nel cluster Kubernetes può emettere il comando showmount -e sulla LIF dati e ricevere un elenco dei mount disponibili, compresi quelli a cui non ha accesso. Per evitare questo, disabilitare la funzione showmount utilizzando il seguente CLI:

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



Per ulteriori informazioni sulle Best practice per la configurazione dello storage e l'utilizzo di Trident, consultare la sezione "[Documentazione di Trident](#)"

OpenShift Virtualization - Guida all'ottimizzazione e alla scalabilità

Red Hat ha documentato "[Raccomandazioni e limitazioni sulla scalabilità del cluster OpenShift](#)".

Inoltre, hanno anche documentato "[Guida all'ottimizzazione della virtualizzazione OpenShift](#)" e "[Limiti supportati per OpenShift Virtualization 4.x](#)".



Per accedere ai contenuti di cui sopra è necessario un abbonamento Red Hat attivo.

La guida alla sintonizzazione contiene informazioni su molti parametri di sintonizzazione, tra cui:

- Regolazione dei parametri per creare più macchine virtuali contemporaneamente o in grandi lotti
- Migrazione live delle macchine virtuali
- "[Configurazione di una rete dedicata per la migrazione live](#)"
- Personalizzazione di un modello di macchina virtuale includendo un tipo di carico di lavoro

I limiti supportati documentano i massimi degli oggetti testati quando si eseguono le VM su OpenShift

Valori massimi delle macchine virtuali inclusi

- Numero massimo di CPU virtuali per macchina virtuale
- Memoria massima e minima per VM
- Dimensioni massime dei singoli dischi per VM
- Numero massimo di dischi hot-plug per VM

Massimi di host che includono * migrazioni simultanee in tempo reale (per nodo e per cluster)

Massimi cluster, compreso * numero massimo di VM definite

Migrazione delle VM dall'ambiente VMware

Migration Toolkit for OpenShift Virtualization è un operatore fornito da Red Hat disponibile dall'OperatorHub della OpenShift Container Platform. Questo tool può essere utilizzato per la migrazione di macchine virtuali da vSphere, Red Hat Virtualization, OpenStack e OpenShift Virtualization.

I dettagli sulla migrazione delle VM da vSphere sono disponibili in [Flussi di lavoro > virtualizzazione Red Hat OpenShift con NetApp ONTAP](#)

È possibile configurare i limiti per i vari parametri dalla CLI o dalla console Web di migrazione. Di seguito sono riportati alcuni campioni

1. Max migrazioni di macchine virtuali simultanee Imposta il numero massimo di macchine virtuali che è possibile migrare simultaneamente. Il valore predefinito è 20 macchine virtuali.

2. Intervallo di precedenza (minuti) Controlla l'intervallo in cui viene richiesta una nuova istantanea prima di iniziare una migrazione a caldo. Il valore predefinito è 60 minuti.
3. L'intervallo di polling degli snapshot (secondi) determina la frequenza con cui il sistema controlla lo stato di creazione o rimozione degli snapshot durante la migrazione a caldo di oVirt. Il valore predefinito è 10 secondi.

Se si migrano più di 10 VM da un host ESXi nello stesso piano di migrazione, è necessario aumentare la memoria del servizio NFC dell'host. In caso contrario, la migrazione non riuscirà perché la memoria di servizio NFC è limitata a 10 connessioni parallele. Per ulteriori dettagli, consultate la documentazione di Red Hat: ["Aumento della memoria di servizio NFC di un host ESXi"](#)

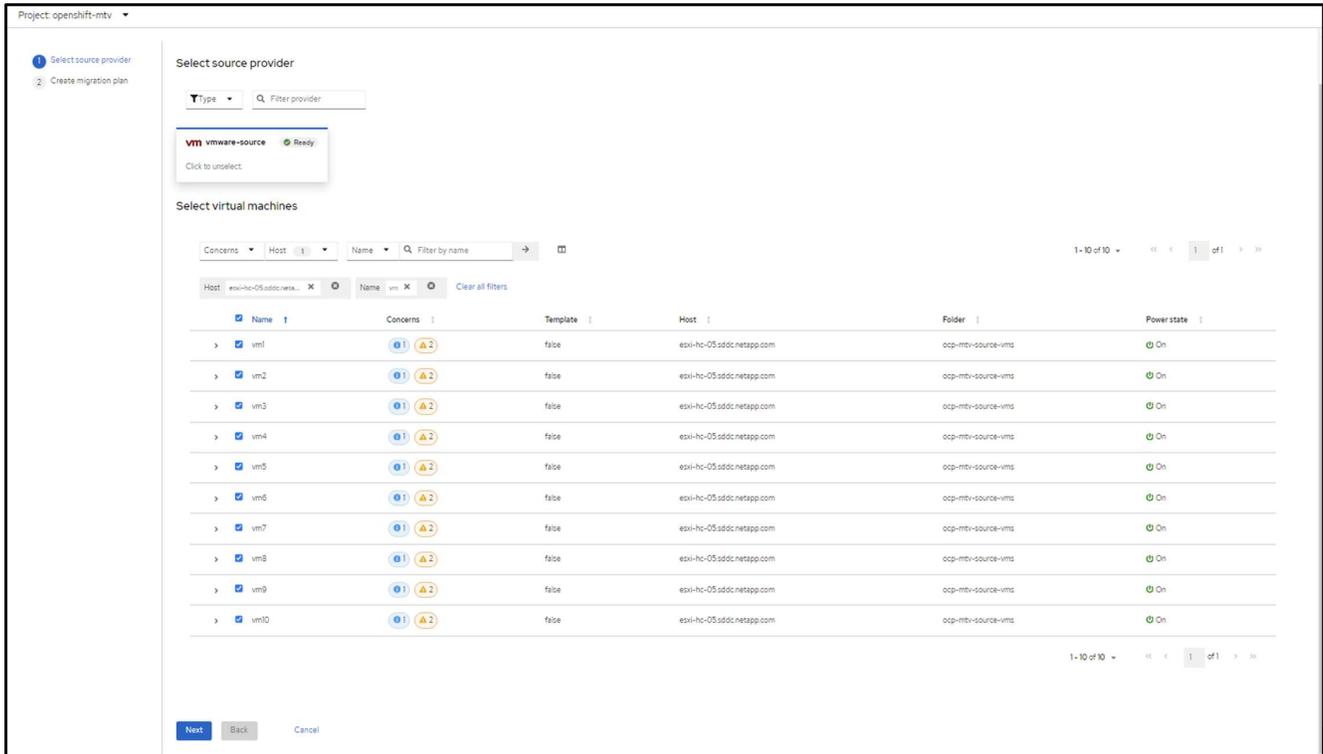
Ecco una migrazione parallela di successo di 10 VM dallo stesso host in vSphere alla virtualizzazione OpenShift utilizzando Migration Toolkit for Virtualization.

VM sullo stesso host ESXi

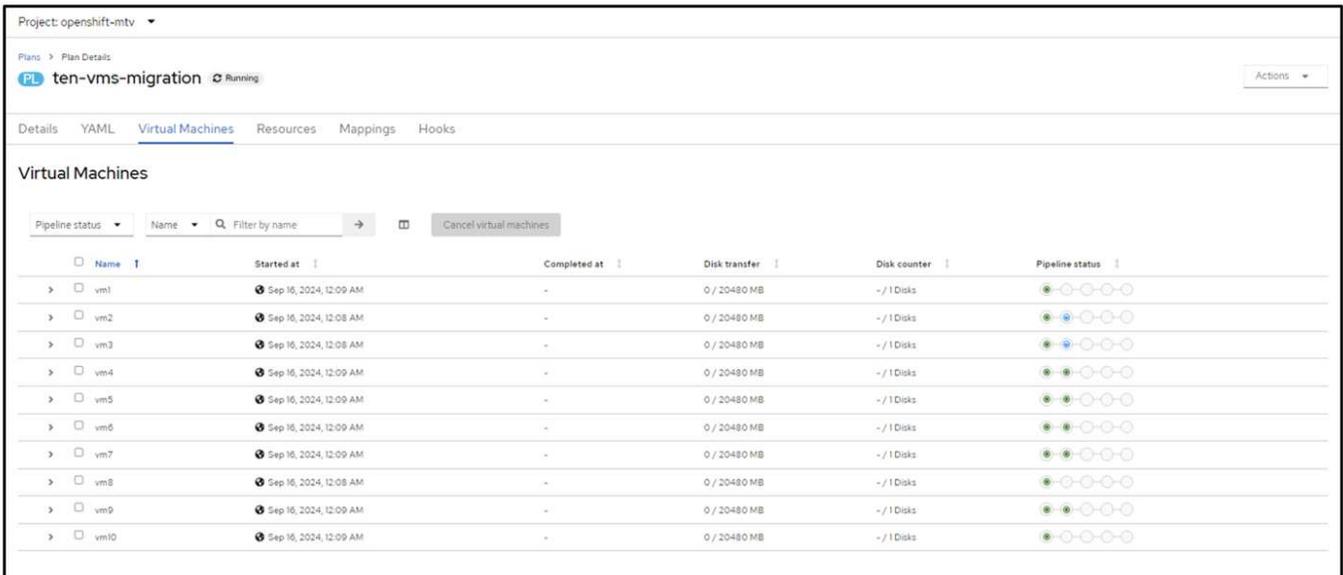
The screenshot shows the vSphere interface for host 'esxi-hc-05.sddc.netapp.com'. The 'VMs' tab is selected, displaying a list of 10 virtual machines. All VMs are in a 'Powered On' state with a 'Normal' status. The VMs are named vm1 through vm9, and vm10. The table below summarizes the data shown in the screenshot.

Name	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
vm1	Powered On	Normal	20 GB	5.21 GB	0 Hz	1.98 GB
vm10	Powered On	Normal	46.6 GB	3.5 GB	0 Hz	2.01 GB
vm2	Powered On	Normal	46.63 GB	5.31 GB	0 Hz	1.87 GB
vm3	Powered On	Normal	46.62 GB	5.31 GB	0 Hz	2 GB
vm4	Powered On	Normal	46.63 GB	5.15 GB	0 Hz	2 GB
vm5	Powered On	Normal	46.63 GB	3.52 GB	22 MHz	1.98 GB
vm6	Powered On	Normal	46.6 GB	3.5 GB	0 Hz	2.01 GB
vm7	Powered On	Normal	46.62 GB	3.52 GB	22 MHz	1.99 GB
vm8	Powered On	Normal	46.63 GB	3.52 GB	22 MHz	1.89 GB
vm9	Powered On	Normal	46.63 GB	3.52 GB	0 Hz	1.9 GB

Per la prima volta viene creato Un piano per la migrazione di 10 VM da VMware



Il piano di migrazione è iniziato ad essere eseguito



Tutte le 10 VM sono state migrate con successo

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	●

Tutte le macchine virtuali 10 sono in esecuzione in 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	-

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.