



# **Présentation de mise en route**

## **NetApp Solutions**

NetApp  
April 25, 2024

This PDF was generated from [https://docs.netapp.com/fr-fr/netapp-solutions/databases/hybrid\\_dbops\\_snapcenter\\_getting\\_started\\_onprem.html](https://docs.netapp.com/fr-fr/netapp-solutions/databases/hybrid_dbops_snapcenter_getting_started_onprem.html) on April 25, 2024. Always check docs.netapp.com for the latest.

# Sommaire

- Présentation de mise en route ..... 1
  - Sur site ..... 1
  - Cloud public AWS ..... 1
  - Pour commencer sur site ..... 1
  - Mise en route du cloud public AWS ..... 54

# Présentation de mise en route

Cette section présente un récapitulatif des tâches à accomplir pour répondre aux exigences préalables requises, comme indiqué dans la section précédente. La section suivante énumère les tâches générales, à la fois pour les opérations sur site et dans le cloud public. Les processus et procédures détaillés sont accessibles en cliquant sur les liens correspondants.

## Sur site

- Configurer l'utilisateur admin de la base de données dans SnapCenter
- Conditions préalables à l'installation du plug-in SnapCenter
- Installation du plug-in hôte SnapCenter
- Découverte de ressources DE BASE DE DONNÉES
- Configuration de la réplication du volume de peering de clusters et de BDD
- Ajouter le SVM de stockage de base de données CVO à SnapCenter
- Configurez la stratégie de sauvegarde de la base de données dans SnapCenter
- Mise en œuvre d'une stratégie de sauvegarde pour protéger la base de données
- Validation de la sauvegarde

## Cloud public AWS

- Contrôle avant vol
- Étapes de déploiement de Cloud Manager et de Cloud Volumes ONTAP dans AWS
- Déployez l'instance de calcul EC2 pour les workloads de base de données

Cliquez sur les liens suivants pour plus d'informations :

["Sur site"](#), ["Cloud public - AWS"](#)

## Pour commencer sur site

L'outil NetApp SnapCenter utilise le contrôle d'accès basé sur des rôles (RBAC) pour gérer l'accès aux ressources utilisateur et les autorisations, et l'installation d'SnapCenter crée des rôles préremplis. Vous pouvez également créer des rôles personnalisés en fonction de vos besoins ou de vos applications.

### Sur site

#### 1. Configurer l'utilisateur administrateur de la base de données dans SnapCenter

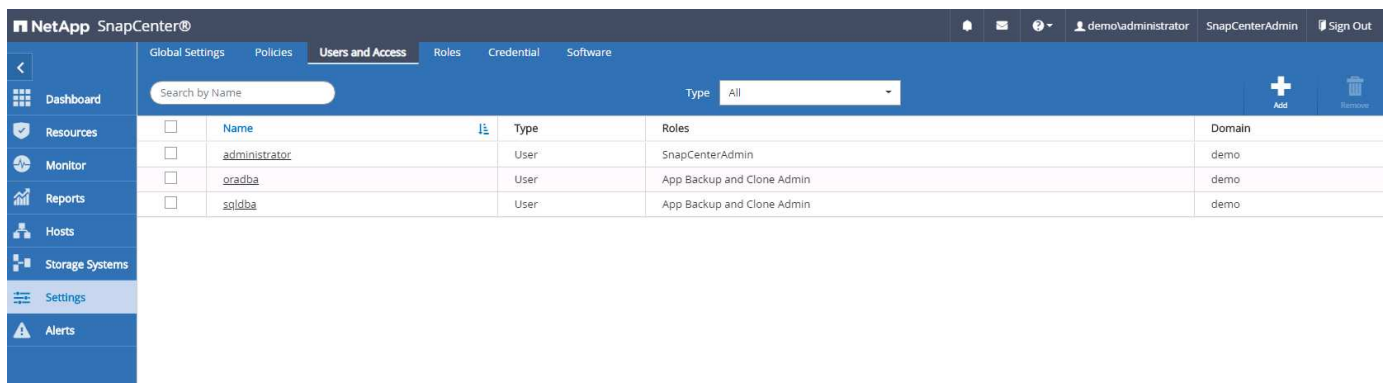
Il est judicieux de disposer d'un ID utilisateur d'administration dédié pour chaque plateforme de base de données prise en charge par SnapCenter pour la sauvegarde, la restauration de bases de données et/ou la reprise après incident. Vous pouvez également utiliser un ID unique pour gérer toutes les bases de données. Dans nos tests de cas et notre démonstration, nous avons créé un utilisateur administratif dédié

respectivement à Oracle et à SQL Server.

Certaines ressources SnapCenter ne peuvent être provisionnées que avec le rôle SnapCenter. Les ressources peuvent ensuite être attribuées à d'autres ID d'utilisateur pour l'accès.

Dans un environnement SnapCenter sur site préinstallé et configuré, les tâches suivantes peuvent déjà avoir été effectuées. Si ce n'est pas le cas, procédez comme suit pour créer un utilisateur administrateur de base de données :

1. Ajoutez l'utilisateur admin à Windows Active Directory.
2. Connectez-vous à SnapCenter à l'aide d'un ID attribué avec le rôle SnapCenterAdmin.
3. Accédez à l'onglet accès sous Paramètres et utilisateurs, puis cliquez sur Ajouter pour ajouter un nouvel utilisateur. Le nouvel ID utilisateur est lié à l'utilisateur admin créé dans Windows Active Directory à l'étape 1. . Attribuez le rôle approprié à l'utilisateur selon les besoins. Affectez des ressources à l'utilisateur administrateur, le cas échéant.



## 2. Conditions préalables à l'installation du plug-in SnapCenter

SnapCenter effectue des sauvegardes, des restaurations, des clones et d'autres fonctions à l'aide d'un agent de plug-in exécuté sur les hôtes de base de données. Il se connecte à l'hôte et à la base de données via les informations d'identification configurées sous l'onglet Paramètres et informations d'identification pour l'installation du plug-in et d'autres fonctions de gestion. Il existe des conditions de privilège spécifiques en fonction du type d'hôte cible, tel que Linux ou Windows, ainsi que du type de base de données.

Les informations d'identification des hôtes DB doivent être configurées avant l'installation du plug-in SnapCenter. En général, vous souhaitez utiliser un compte d'utilisateur administrateur sur l'hôte DB comme informations d'identification de connexion hôte pour l'installation du plug-in. Vous pouvez également attribuer le même ID utilisateur pour l'accès à la base de données à l'aide de l'authentification basée sur le système d'exploitation. En revanche, vous pouvez également utiliser l'authentification de base de données avec différents ID d'utilisateur de base de données pour l'accès à la gestion de base de données. Si vous décidez d'utiliser l'authentification basée sur le système d'exploitation, l'ID utilisateur admin du système d'exploitation doit disposer d'un accès DB. Pour l'installation de SQL Server sous domaine Windows, un compte d'administrateur de domaine peut être utilisé pour gérer tous les serveurs SQL du domaine.

Hôte Windows pour SQL Server :

1. Si vous utilisez des informations d'identification Windows pour l'authentification, vous devez configurer vos informations d'identification avant d'installer des plug-ins.
2. Si vous utilisez une instance SQL Server pour l'authentification, vous devez ajouter les informations d'identification après avoir installé des plug-ins.
3. Si vous avez activé l'authentification SQL lors de la configuration des informations d'identification,

l'instance ou la base de données découverte s'affiche avec une icône de verrouillage rouge. Si l'icône de verrouillage apparaît, vous devez spécifier les informations d'identification de l'instance ou de la base de données pour pouvoir ajouter l'instance ou la base de données à un groupe de ressources.

4. Vous devez affecter ces informations d'identification à un utilisateur RBAC sans accès sysadmin lorsque les conditions suivantes sont remplies :
  - Les informations d'identification sont affectées à une instance SQL.
  - L'instance ou l'hôte SQL est affecté à un utilisateur RBAC.
  - L'utilisateur administrateur de BD RBAC doit disposer à la fois du groupe de ressources et des privilèges de sauvegarde.

Hôte UNIX pour Oracle :

1. Vous devez avoir activé la connexion SSH par mot de passe pour l'utilisateur root ou non-root en modifiant sshd.conf et en redémarrant le service sshd. L'authentification SSH basée sur le mot de passe sur une instance AWS est désactivée par défaut.
2. Configurez les privilèges sudo pour que l'utilisateur non-root installe et démarre le processus de plug-in. Après avoir installé le plug-in, les processus s'exécutent en tant qu'utilisateur root efficace.
3. Créez des informations d'identification avec le mode d'authentification Linux pour l'utilisateur d'installation.
4. Vous devez installer Java 1.8.x (64 bits) sur votre hôte Linux.
5. L'installation du plug-in de base de données Oracle installe également le plug-in SnapCenter pour Unix.

### 3. Installation du plug-in hôte SnapCenter

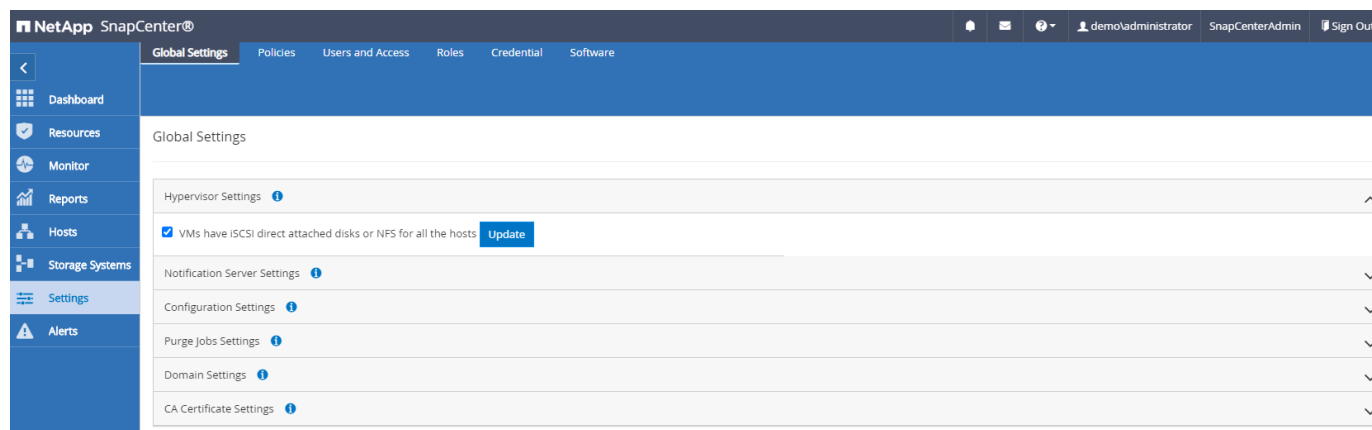


Avant de tenter d'installer des plug-ins SnapCenter sur des instances de serveur BDD cloud, assurez-vous que toutes les étapes de configuration sont terminées, comme indiqué dans la section cloud appropriée pour le déploiement de l'instance de calcul.

Les étapes suivantes illustrent la manière dont un hôte de base de données est ajouté à SnapCenter pendant qu'un plug-in SnapCenter est installé sur l'hôte. La procédure s'applique à l'ajout d'hôtes sur site et d'hôtes cloud. La démonstration suivante ajoute un hôte Windows ou Linux résidant dans AWS.

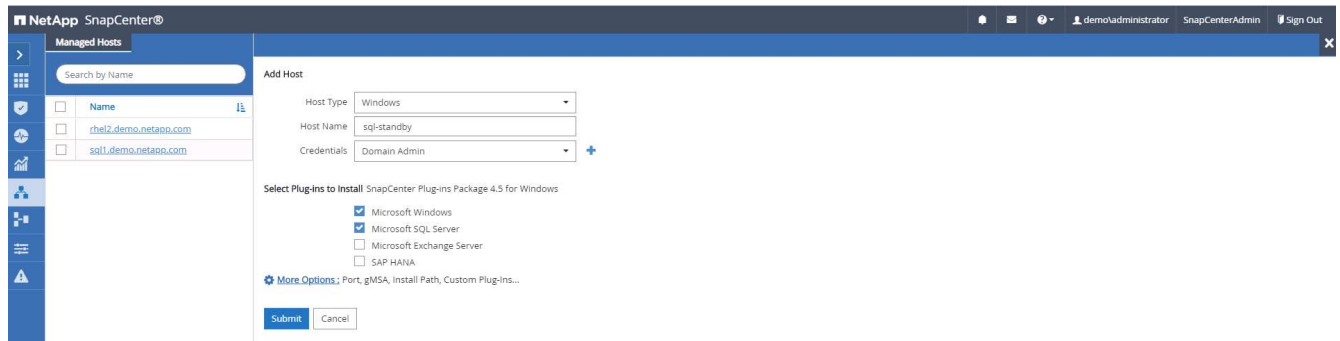
#### Configurez les paramètres globaux de SnapCenter VMware

Accédez à Paramètres > Paramètres globaux. Sous Paramètres de l'hyperviseur, sélectionnez « les machines virtuelles ont des disques iSCSI à connexion directe ou NFS pour tous les hôtes », puis cliquez sur mettre à jour.

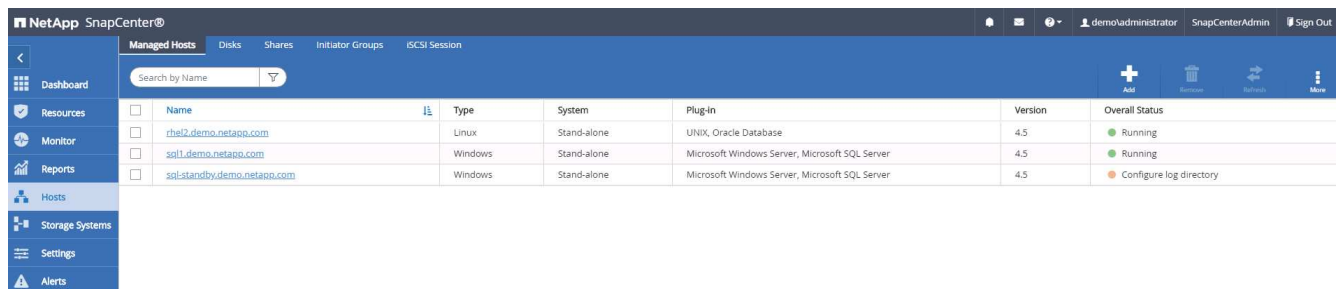


## Ajoutez l'hôte Windows et l'installation du plug-in sur l'hôte

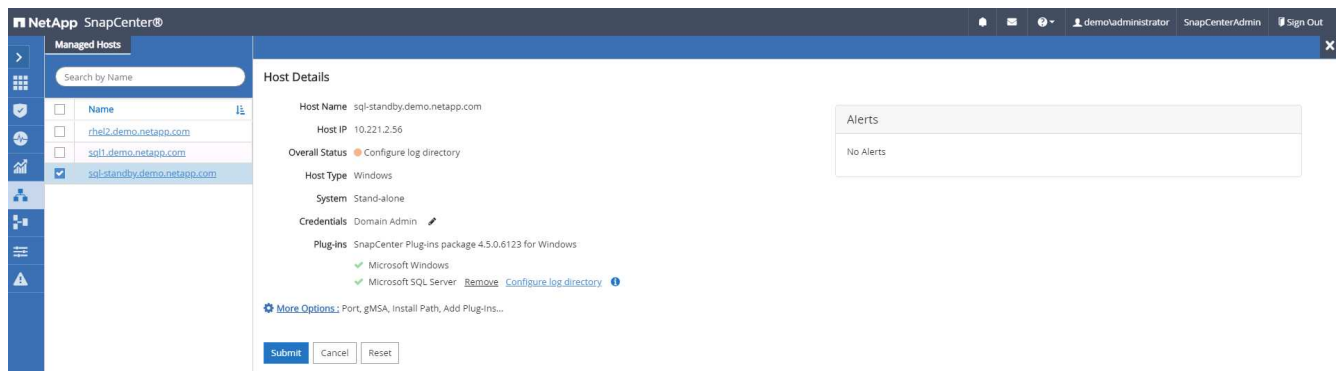
1. Connectez-vous à SnapCenter avec un ID utilisateur doté des privilèges SnapCenterAdmin.
2. Cliquez sur l'onglet hôtes dans le menu de gauche, puis cliquez sur Ajouter pour ouvrir le flux de travail Ajouter hôte.
3. Choisissez Windows pour le type d'hôte ; le nom d'hôte peut être un nom d'hôte ou une adresse IP. Le nom d'hôte doit être résolu à l'adresse IP d'hôte correcte de l'hôte SnapCenter. Choisissez les informations d'identification de l'hôte créées à l'étape 2. Choisissez Microsoft Windows et Microsoft SQL Server comme modules d'extension à installer.



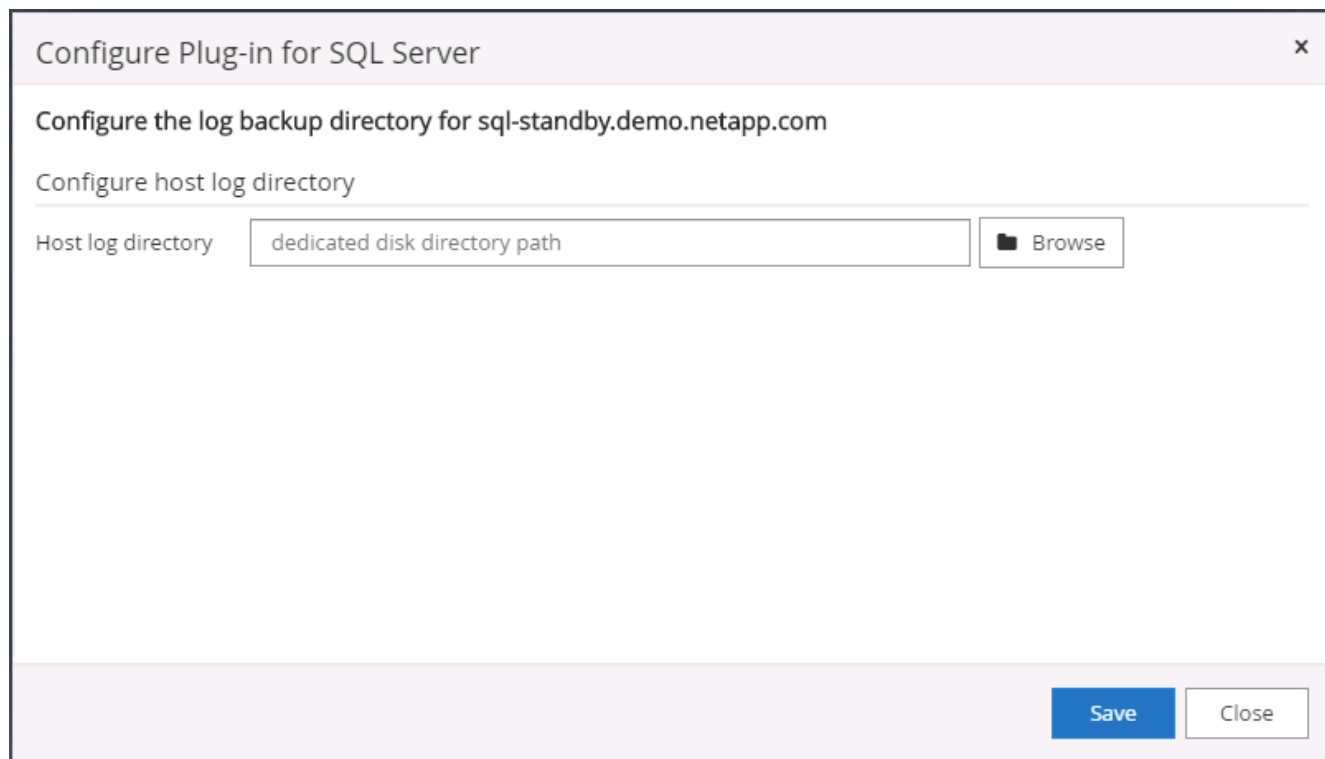
4. Une fois le plug-in installé sur un hôte Windows, son état global s'affiche sous la forme "configurer le répertoire du journal".



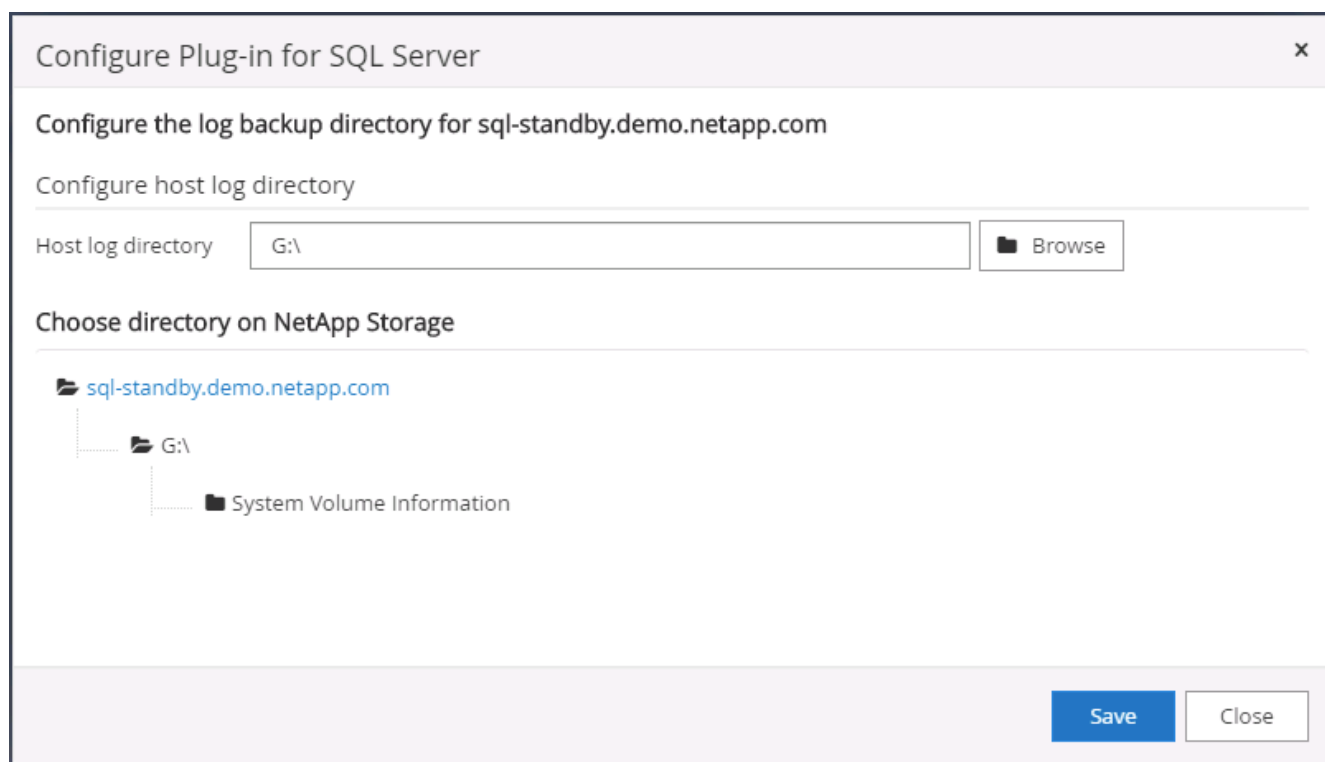
5. Cliquez sur le nom d'hôte pour ouvrir la configuration du répertoire du journal de SQL Server.



6. Cliquez sur « configurer le répertoire du journal » pour ouvrir « configurer le plug-in pour SQL Server ».

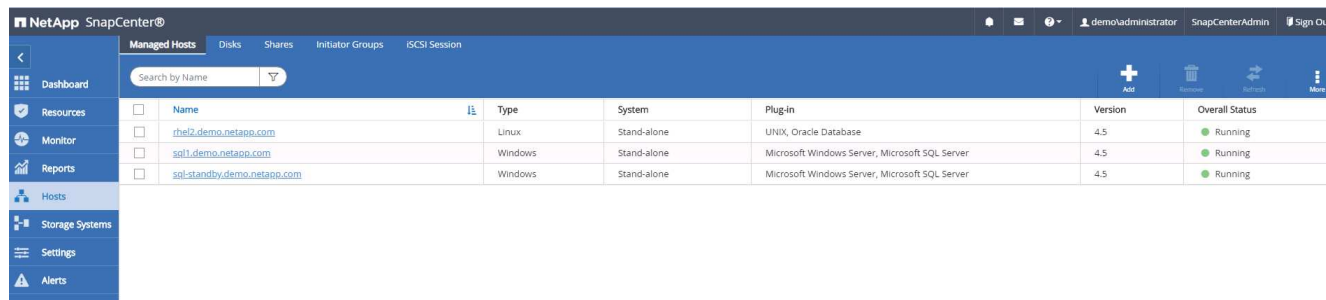


7. Cliquez sur Parcourir pour découvrir le stockage NetApp afin de définir un répertoire de journaux ; SnapCenter utilise ce répertoire de journaux pour restaurer les fichiers journaux de transactions du serveur SQL. Cliquez ensuite sur Enregistrer.



Pour que le stockage NetApp provisionné sur un hôte de base de données soit découvert, le stockage (sur site ou CVO) doit être ajouté à SnapCenter, comme illustré à l'étape 6 pour CVO.

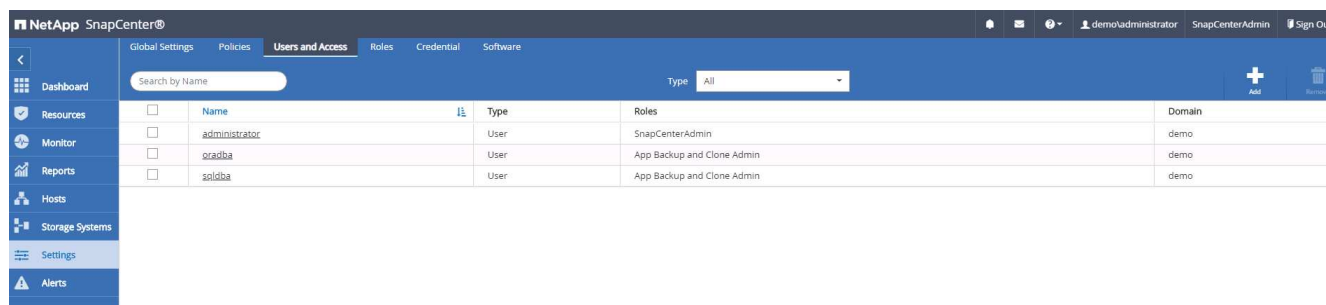
8. Une fois le répertoire du journal configuré, l'état global du plug-in hôte Windows est défini sur en cours d'exécution.



The screenshot shows the NetApp SnapCenter interface with the 'Managed Hosts' tab selected. The table lists three hosts: 'rhel2.demo.netapp.com' (Linux, Stand-alone), 'sql1.demo.netapp.com' (Windows, Stand-alone), and 'sql-standby.demo.netapp.com' (Windows, Stand-alone). All hosts have a 'Running' status.

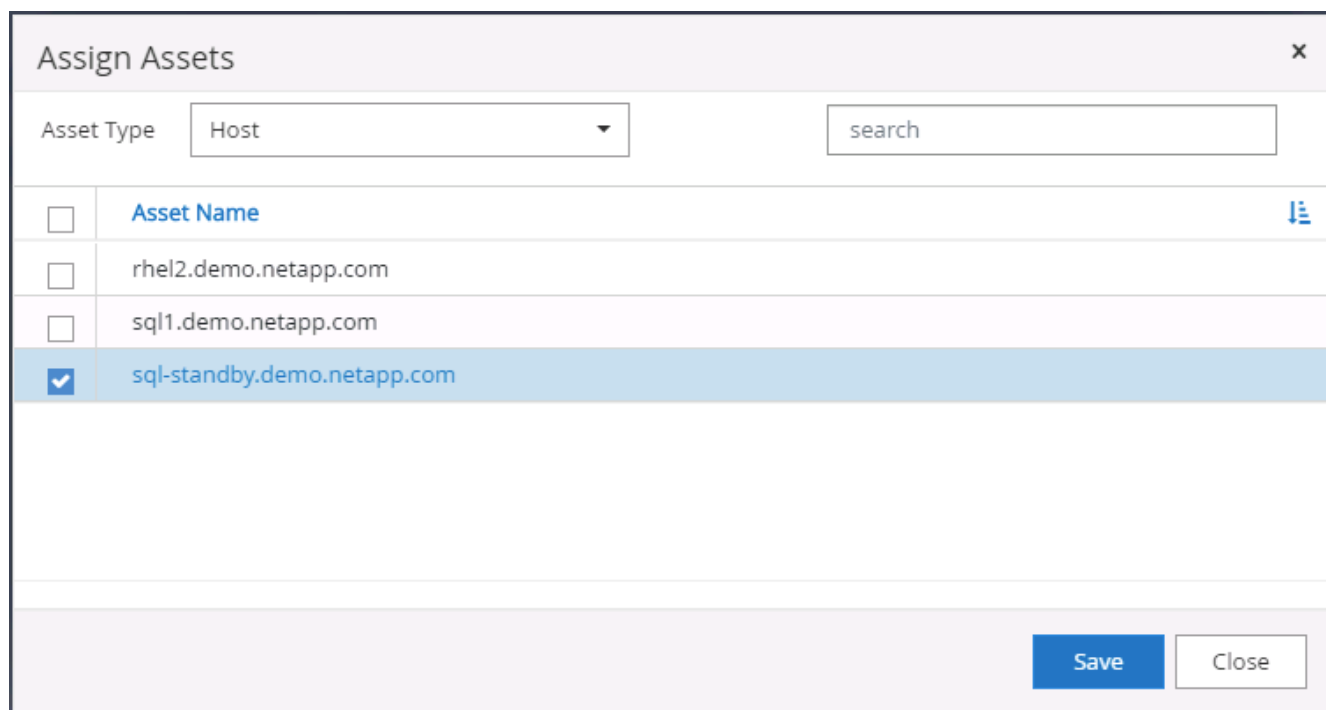
Name	Type	System	Plug-in	Version	Overall Status
rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running
sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running
sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running

9. Pour attribuer l'hôte à l'ID utilisateur de gestion de base de données, accédez à l'onglet accès sous Paramètres et utilisateurs, cliquez sur l'ID utilisateur de gestion de base de données (dans notre cas, l'ID utilisateur de gestion de base de données à affecter à l'hôte), puis cliquez sur Enregistrer pour terminer l'affectation de ressources hôte.



The screenshot shows the NetApp SnapCenter interface with the 'Users and Access' tab selected. The table lists three users: 'administrator', 'oraoba', and 'sqloba'. The 'administrator' user is assigned the 'SnapCenterAdmin' role, while 'oraoba' and 'sqloba' are assigned the 'App Backup and Clone Admin' role.

Name	Type	Roles	Domain
administrator	User	SnapCenterAdmin	demo
oraoba	User	App Backup and Clone Admin	demo
sqloba	User	App Backup and Clone Admin	demo



The 'Assign Assets' dialog box shows a list of assets. The 'Asset Type' is set to 'Host'. The list includes 'rhel2.demo.netapp.com', 'sql1.demo.netapp.com', and 'sql-standby.demo.netapp.com'. The 'sql-standby.demo.netapp.com' asset is selected with a checkmark.

Asset Name
rhel2.demo.netapp.com
sql1.demo.netapp.com
sql-standby.demo.netapp.com

Buttons: Save, Close

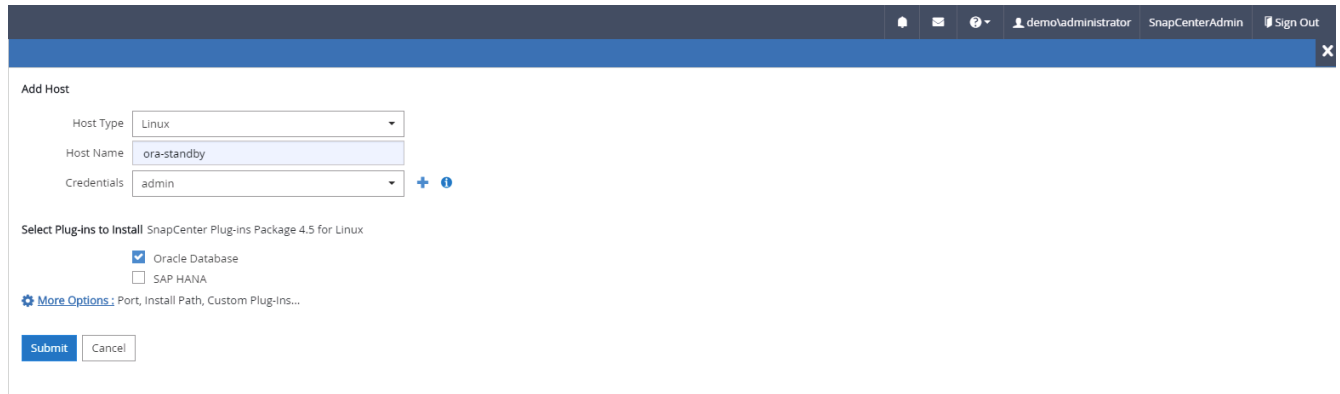
#### Ajoutez l'hôte Unix et l'installation du plug-in sur l'hôte

1. Connectez-vous à SnapCenter avec un ID utilisateur doté des privilèges SnapCenterAdmin.
2. Cliquez sur l'onglet hôtes dans le menu de gauche, puis cliquez sur Ajouter pour ouvrir le flux de travail



Ajouter hôte.

3. Choisissez Linux comme Type d'hôte. Le nom d'hôte peut être soit le nom d'hôte, soit une adresse IP. Cependant, le nom d'hôte doit être résolu pour corriger l'adresse IP de l'hôte SnapCenter. Choisissez les informations d'identification de l'hôte créées à l'étape 2. Les informations d'identification de l'hôte nécessitent des privilèges sudo. Vérifiez Oracle Database en tant que plug-in à installer, qui installe à la fois les plug-ins hôtes Oracle et Linux.



Add Host

Host Type: Linux

Host Name: ora-standby

Credentials: admin

Select Plug-ins to Install: SnapCenter Plug-ins Package 4.5 for Linux

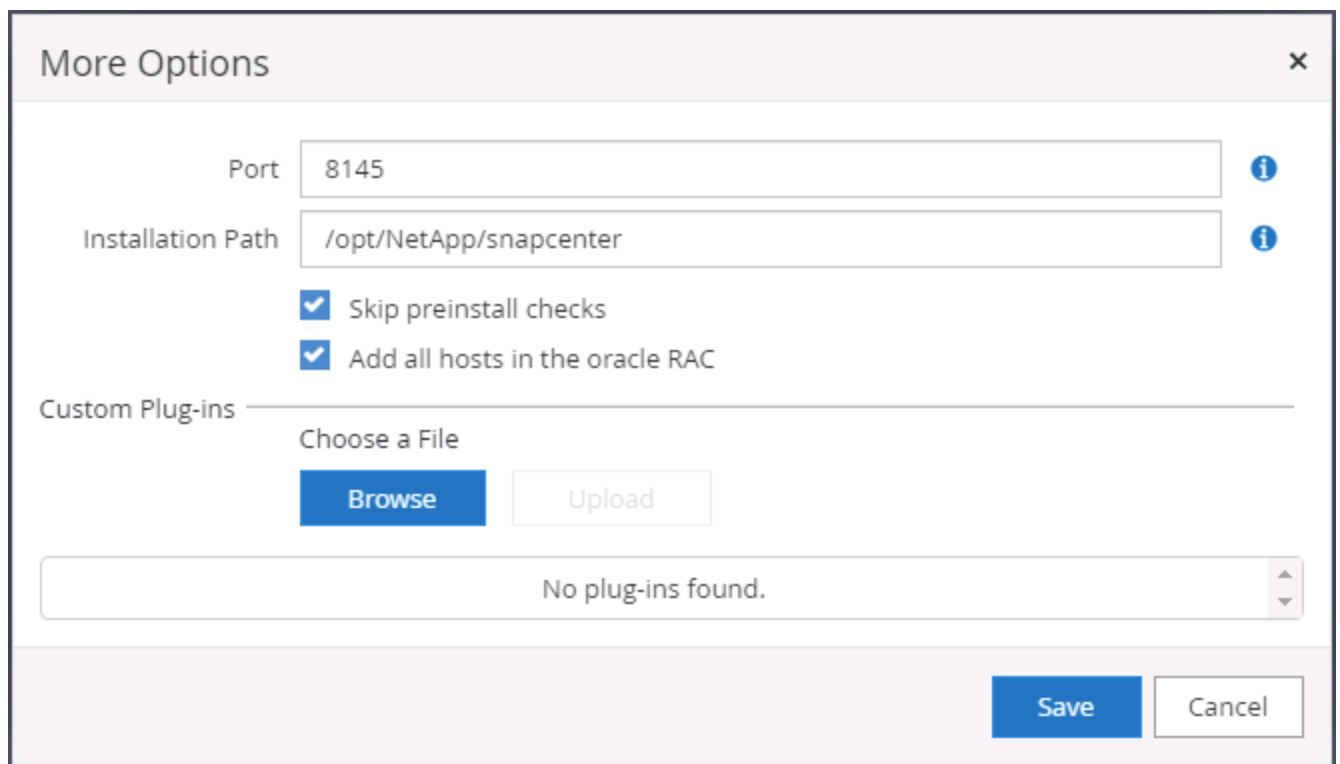
☒ Oracle Database

☐ SAP HANA

[More Options](#): Port, Install Path, Custom Plug-ins...

Submit Cancel

4. Cliquez sur plus d'options et sélectionnez « Ignorer les vérifications de préinstallation ». Vous êtes invité à confirmer l'omission de la vérification de préinstallation. Cliquez sur Oui, puis sur Enregistrer.



More Options

Port: 8145

Installation Path: /opt/NetApp/snapcenter

☒ Skip preinstall checks

☒ Add all hosts in the oracle RAC

Custom Plug-ins

Choose a File

Browse Upload

No plug-ins found.

Save Cancel

5. Cliquez sur soumettre pour démarrer l'installation du plug-in. Vous êtes invité à confirmer l'empreinte digitale comme indiqué ci-dessous.

Confirm Fingerprint

Authenticity of the host cannot be determined

Host name	Fingerprint	Valid
ora-standby.demo.netapp.com	ssh-rsa 3072 5C:02:EF:6B:63:54:59:10:84:DF:4D:6B:AB:FB:61:67	

Confirm and Submit

Close

6. SnapCenter effectue la validation et l'enregistrement des hôtes, puis le plug-in est installé sur l'hôte Linux. L'état passe de installation du plug-in à exécution.

NetApp SnapCenter®							
<div> <div>Managed Hosts</div> <div>Disks</div> <div>Shares</div> <div>Initiator Groups</div> <div>ISCSI Session</div> </div>							
<div> <div>Search by Name</div> <div>+</div> <div>+</div> <div>+</div> <div>+</div> </div>							
	Name	Type	System	Plug-in	Version	Overall Status	
<input type="checkbox"/>	ora-standby.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running	
<input type="checkbox"/>	rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running	
<input type="checkbox"/>	sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running	
<input type="checkbox"/>	sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running	

7. Affectez l'hôte nouvellement ajouté à l'ID utilisateur de gestion de base de données approprié (dans notre cas, oradba).

NetApp SnapCenter®

Users and Access

Users/Groups Details

Search by Name

Name
administrator
oradba
sqlidba

User Name

Domain

Roles

oradba

demo

App Backup and Clone Admin

Assign Assets

Asset Name	Type	Asset Type
10.0.0.1	DataOntapCluster	Storage Connection
192.168.0.101	DataOntapCluster	Storage Connection
admin		Credentials
Linux Admin		Credentials
Oracle Archive Log Backup		Policy
Oracle Full Online Backup		Policy
rhel2.demo.netapp.com		Host

Submit

Cancel

Assign Assets

Asset Type
Host
search

<input type="checkbox"/>	Asset Name
<input checked="" type="checkbox"/>	ora-standby.demo.netapp.com
<input type="checkbox"/>	rhel2.demo.netapp.com
<input type="checkbox"/>	sql1.demo.netapp.com
<input type="checkbox"/>	sql-standby.demo.netapp.com

Save
Close

## 4. Découverte de ressources de base de données

Une fois l'installation du plug-in réussie, les ressources de la base de données sur l'hôte peuvent être immédiatement découvertes. Cliquez sur l'onglet Ressources dans le menu de gauche. Selon le type de plateforme de base de données, un certain nombre de vues sont disponibles, comme la base de données, le groupe de ressources, etc. Vous devrez peut-être cliquer sur l'onglet Actualiser les ressources si les ressources de l'hôte ne sont pas découvertes et affichées.

NetApp SnapCenter®

Oracle Database

View Database Search databases

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com				Not protected

Lorsque la base de données est initialement découverte, l'état global est indiqué comme « non protégé ». La capture d'écran précédente montre qu'une base de données Oracle n'est pas encore protégée par une règle de sauvegarde.

Lorsqu'une configuration ou une stratégie de sauvegarde est configurée et qu'une sauvegarde a été exécutée, l'état général de la base de données affiche l'état de sauvegarde « sauvegarde réussie » et l'horodatage de la dernière sauvegarde. La capture d'écran suivante montre l'état de sauvegarde d'une base de données utilisateur SQL Server.

Name	Instance	Host	Last Backup	Overall Status	Type
master	sql1	sql1.demo.netapp.com		Not available for backup	System database
model	sql1	sql1.demo.netapp.com		Not available for backup	System database
msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tempdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tpcc	sql1	sql1.demo.netapp.com	09/14/2021 2:35:07 PM	Backup succeeded	User database

Si les informations d'identification d'accès à la base de données ne sont pas correctement configurées, un bouton de verrouillage rouge indique que la base de données n'est pas accessible. Par exemple, si les informations d'identification Windows ne disposent pas d'un accès sysadmin à une instance de base de données, les informations d'identification de la base de données doivent être reconfigurées pour déverrouiller le verrou rouge.

Name	Host	Resource Groups	Policies	State	Type
sql-standby	sql-standby.demo.netapp.com			Running	Standalone ()
sql1	sql1.demo.netapp.com			Running	Standalone (15.0.2000)

Name	Host	Resource Groups	Policies	State	Type
sql-standby	sql-standby.demo.netapp.com			Running	Standalone (15.0.2000)
sql1	sql1.demo.netapp.com			Running	Standalone (15.0.2000)

Une fois que les informations d'identification appropriées sont configurées soit au niveau de Windows, soit au niveau de la base de données, le verrou rouge disparaît et les informations de type de serveur SQL sont rassemblées et vérifiées.

Name	Host	Resource Groups	Policies	State	Type
sql1	sql1.demo.netapp.com			Running	Standalone (15.0.2000)
sql-standby	sql-standby.demo.netapp.com			Running	Standalone (15.0.2000)

## 5. Configuration de la réplication des volumes de peering de cluster de stockage et de BDD

Pour protéger vos données de base de données sur site à l'aide d'un cloud public comme destination cible, les volumes de base de données du cluster ONTAP sur site sont répliqués dans Cloud volumes CVO à l'aide de la technologie NetApp SnapMirror. Les volumes cibles répliqués peuvent ensuite être clonés pour LE

DÉVELOPPEMENT/opérations ou la reprise après incident. Les étapes de haut niveau suivantes vous permettent de configurer le peering de clusters et la réplication des volumes de la base de données.

1. Configurer les LIF intercluster pour le peering de cluster sur le cluster sur site et sur l'instance du cluster CVO. Cette étape peut être réalisée avec ONTAP System Manager. Un déploiement CVO par défaut est configuré automatiquement pour les LIF inter-cluster.

Cluster sur site :

Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Protocols	Type
onPrem-01_IC	Up		Default	192.168.0.113	onPrem-01	e0b		Intercluster
onPrem-01_mgmt1	Up		Default	192.168.0.111	onPrem-01	e0c		Cluster/Node Mgmt
cluster_mgmt	Up		Default	192.168.0.101	onPrem-01	e0a		Cluster/Node Mgmt

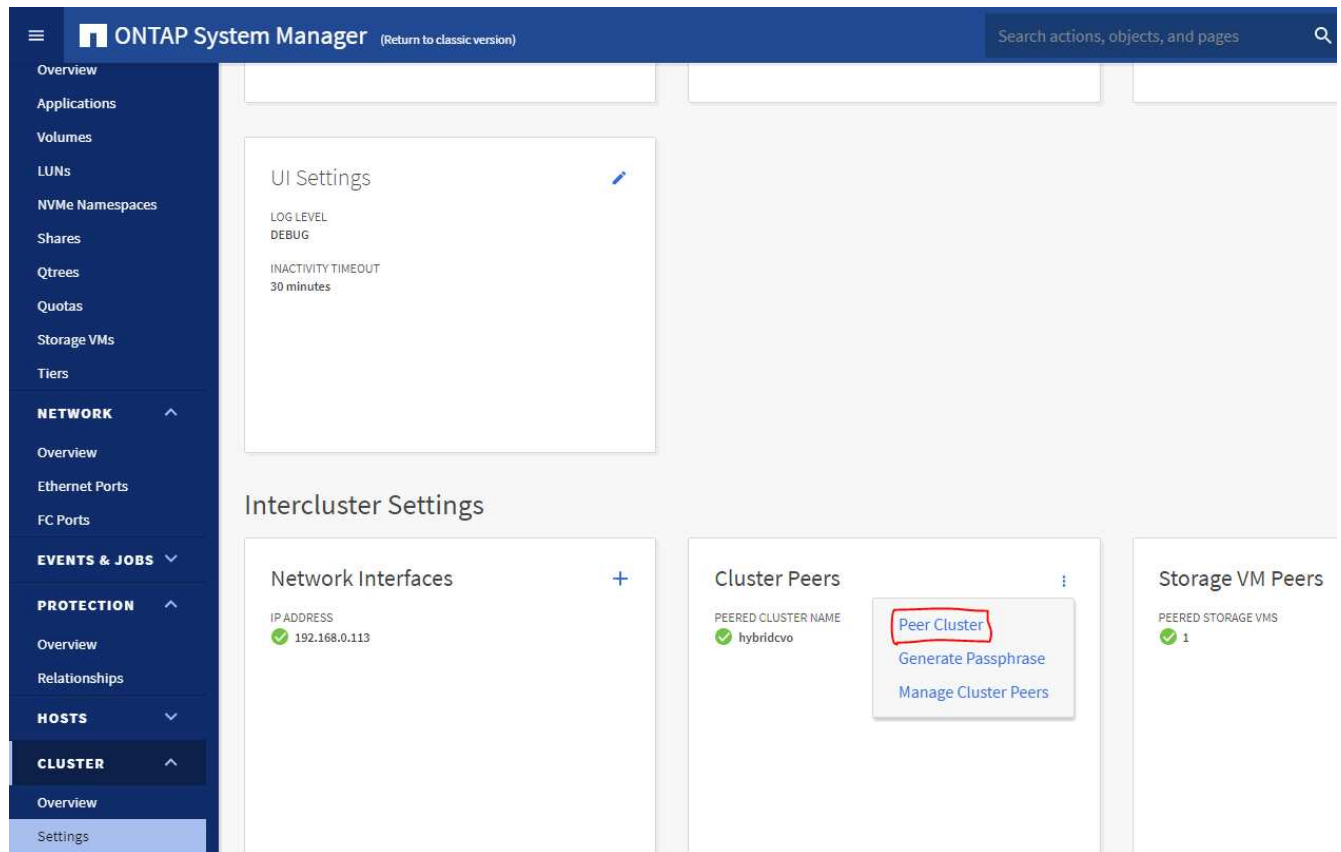
Cluster CVO cible :

Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Protocols	Type	Throughput (I)
hybridcvo-02_mgmt1	Up		Default	10.221.2.104	hybridcvo-02	e0a		Cluster/Node Mgmt	0
Inter_1	Up		Default	10.221.1.180	hybridcvo-01	e0a		Intercluster,Cluster/Node Mgmt	0.02
Inter_2	Up		Default	10.221.2.250	hybridcvo-02	e0a		Intercluster,Cluster/Node Mgmt	0.03
iscsi_1	Up	svm_hybridcvo	Default	10.221.1.5	hybridcvo-01	e0a	ISCSI	Data	0
iscsi_2	Up	svm_hybridcvo	Default	10.221.2.168	hybridcvo-02	e0a	ISCSI	Data	0

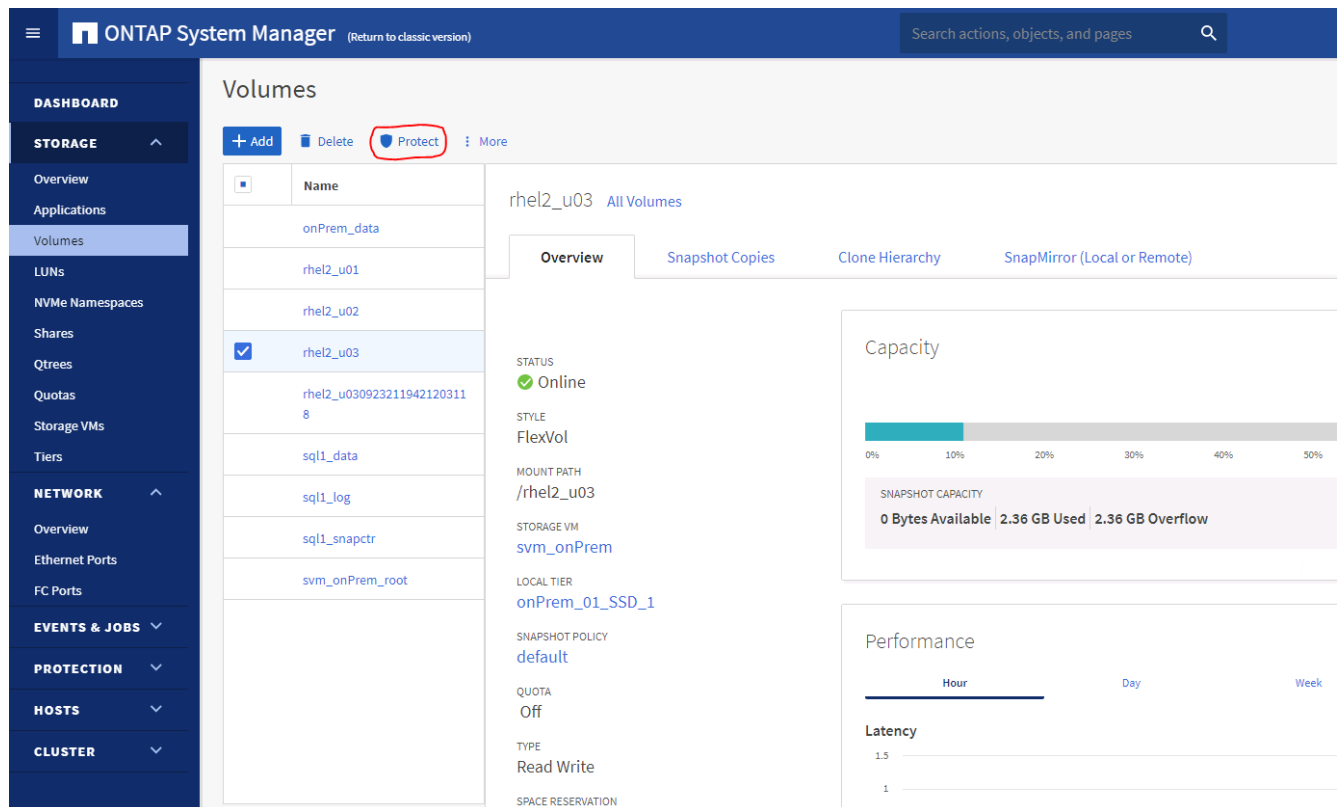
2. Lorsque les LIF intercluster sont configurées, le peering de clusters et la réplication des volumes peuvent être configurés en utilisant le glisser-déposer dans NetApp Cloud Manager. Voir "[Mise en route - Cloud public AWS](#)" pour plus d'informations.

Vous pouvez également effectuer la réplication de volume de peering de clusters et de bases de données à l'aide de ONTAP System Manager, comme suit :

3. Connectez-vous à ONTAP System Manager. Naviguez jusqu'à Cluster > Paramètres et cliquez sur Peer Cluster pour configurer le cluster peering avec l'instance CVO dans le cloud.



- Accédez à l'onglet volumes. Sélectionnez le volume de la base de données à répliquer et cliquez sur protéger.



- Définissez la règle de protection sur asynchrone. Sélectionner le cluster de destination et le SVM de

stockage.

ONTAP System Manager

(Return to classic version)

Search actions, objects, and pages

DASHBOARD

STORAGE

Overview

Applications

Volumes

LUNs

NVMe Namespaces

Shares

Qtrees

Quotas

Storage VMs

Tiers

NETWORK

Overview

Ethernet Ports

FC Ports

EVENTS & JOBS

PROTECTION

HOSTS

CLUSTER

Protect Volumes

PROTECTION POLICY

Asynchronous

Source

CLUSTER

onPrem

STORAGE VM

svm\_onPrem

SELECTED VOLUMES

rhel2\_u03

Destination

CLUSTER

hybridcvo

STORAGE VM

svm\_hybridcvo

Destination Settings

2 matching labels

VOLUME NAME

PREFIX

vol\_

<SourceVolumeName>

SUFFIX

\_dest

Override default storage service name

Configuration Details

Initialize relationship

Enable FabricPool

Save

Cancel

6. Vérifier que le volume est synchronisé entre la source et la cible et que la relation de réplication fonctionne correctement.

Volumes

+ Add

Delete

Protect

More

rhel2\_u03

All Volumes

Edit

More

onPrem\_data

rhel2\_u01

rhel2\_u02

rhel2\_u03

rhel2\_u0309232119421203118

Overview

Snapshot Copies

Clone Hierarchy

SnapMirror (Local or Remote)

Source	Destination	Protection Policy	Relationship Health	Relationship Status	Lag
svm_onPremorhel2_u03	svm_hybridcvoorhel2_u03_dr	MirrorAllSnapshots	Healthy	Mirrored	12 seconds

6. Ajouter le SVM de stockage de base de données CVO à SnapCenter

1. Connectez-vous à SnapCenter avec un ID utilisateur doté des privilèges SnapCenterAdmin.

2. Cliquez sur l'onglet Storage System dans le menu, puis sur New pour ajouter un SVM de stockage CVO qui héberge les volumes de base de données cible répliqués dans SnapCenter. Saisissez l'IP de gestion de cluster dans le champ Storage System, puis saisissez le nom d'utilisateur et le mot de passe appropriés.

3. Cliquez sur plus d'options pour ouvrir d'autres options de configuration de stockage. Dans le champ plateforme, sélectionnez Cloud Volumes ONTAP, cochez secondaire, puis cliquez sur Enregistrer.

4. Attribuez les systèmes de stockage aux ID d'utilisateur de gestion de la base de données SnapCenter, comme indiqué dans la [3. Installation du plug-in hôte SnapCenter](#).

Name	IP	Cluster Name	User Name	Platform	Controller License
svm_hybridv0	10.0.0.1			CVO	⊗
svm_onPrem	192.168.0.101			CVO	✓

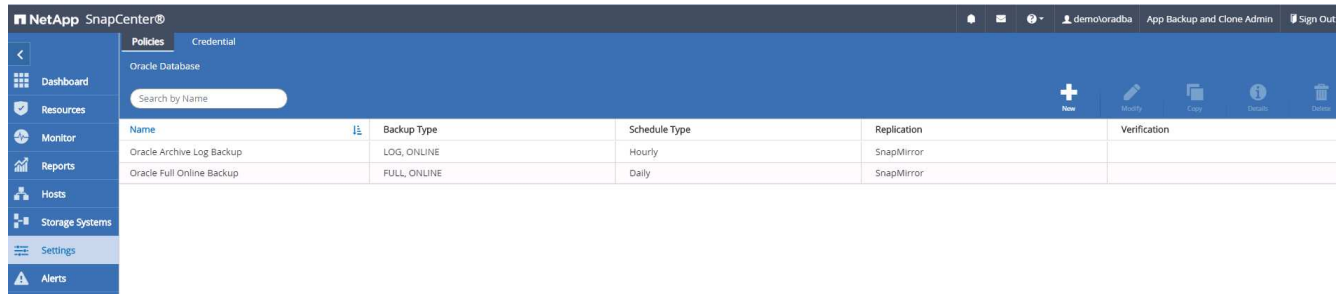
## 7. Configurer la politique de sauvegarde de la base de données dans SnapCenter

Les procédures suivantes montrent comment créer une stratégie de sauvegarde complète de base de données ou de fichiers journaux. La stratégie peut ensuite être mise en œuvre pour protéger les ressources des bases de données. L'objectif de point de récupération (RPO) ou l'objectif de délai de restauration (RTO) détermine la fréquence des sauvegardes de bases de données et/ou de journaux.



## Créez une stratégie de sauvegarde complète de la base de données pour Oracle

1. Connectez-vous à SnapCenter en tant qu'ID utilisateur de gestion de base de données, cliquez sur Paramètres, puis sur stratégies.



2. Cliquez sur Nouveau pour lancer un nouveau workflow de création de stratégie de sauvegarde ou choisir une stratégie existante pour la modification.

### Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

Details

Previous

Next

3. Sélectionnez le type de sauvegarde et la fréquence de planification.

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select Oracle database backup options

Choose backup type

☒ Online backup

☒ Datafiles, control files, and archive logs

☐ Datafiles and control files

☐ Archive logs

☐ Offline backup

☒ Mount

☐ Shutdown

☐ Save state of PDBs

Choose schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ On demand

☐ Hourly

☒ Daily

Previous

Next

4. Définissez le paramètre de conservation de sauvegarde. Cet objectif définit le nombre de copies de sauvegarde complètes à conserver dans une base de données.

16

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

Daily retention settings

Data backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

14

days

Archive Log backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

14

days

Previous

Next

5. Sélectionnez les options de réplication secondaires pour envoyer les sauvegardes de snapshots primaires locaux à répliquer vers un emplacement secondaire dans le cloud.

17

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Daily

Error retry count

3

Previous

Next

6. Spécifiez tout script facultatif à exécuter avant et après l'exécution d'une sauvegarde.

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before and after performing a backup job

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Prescript arguments

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Postscript arguments

Script timeout

60

secs

Previous

Next

7. Exécutez la vérification des sauvegardes si nécessaire.

19

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select the options to run backup verification

Run Verifications for following backup schedules

Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

☐ Daily

Verification script commands

Script timeout

60

secs

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Prescript arguments

Choose optional arguments...

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Postscript arguments

Choose optional arguments...

Previous

Next

## 8. Récapitulatif.

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

Policy name	Oracle Full Online Backup
Details	Backup all data and log files
Backup type	Online backup
Schedule type	Daily
RMAN catalog backup	Disabled
Archive log pruning	None
On demand data backup retention	None
On demand archive log backup retention	None
Hourly data backup retention	None
Hourly archive log backup retention	None
Daily data backup retention	Delete Snapshot copies older than : 14 days
Daily archive log backup retention	Delete Snapshot copies older than : 14 days
Weekly data backup retention	None
Weekly archive log backup retention	None
Monthly data backup retention	None
Monthly archive log backup retention	None
Replication	SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3

Previous

Finish

## Créez une stratégie de sauvegarde du journal de base de données pour Oracle

1. Connectez-vous à SnapCenter à l'aide d'un ID utilisateur de gestion de base de données, cliquez sur Paramètres, puis sur stratégies.
2. Cliquez sur Nouveau pour lancer un nouveau workflow de création de stratégie de sauvegarde ou choisissez une stratégie existante à modifier.

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

Details

Oracle Archive Log Backup

Backup Oracle archive logs

Previous

Next

3. Sélectionnez le type de sauvegarde et la fréquence de planification.

22



New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select Oracle database backup options

Choose backup type

☒ Online backup

☐ Datafiles, control files, and archive logs

☐ Datafiles and control files

☒ Archive logs

☐ Offline backup

☒ Mount

☐ Shutdown

☐ Save state of PDBs

Choose schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ On demand

☒ Hourly

☐ Daily

Previous

Next

4. Définissez la période de conservation du journal.

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

Hourly retention settings

Data backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

14 days

Archive Log backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

7 days

Previous

Next

5. Répliquez la réplication dans un emplacement secondaire dans le cloud public.

24

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Hourly

Error retry count

3

Previous

Next

6. Spécifiez tous les scripts facultatifs à exécuter avant et après la sauvegarde du journal.

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before and after performing a backup job

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Prescript arguments

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Postscript arguments

Script timeout

60

secs

Previous

Next

7. Spécifiez tous les scripts de vérification de sauvegarde.

26

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select the options to run backup verification

Run Verifications for following backup schedules

Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

Verification script commands

Script timeout

60

secs

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Prescript arguments

Choose optional arguments...

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Postscript arguments

Choose optional arguments...

Previous

Next

8. Récapitulatif.

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

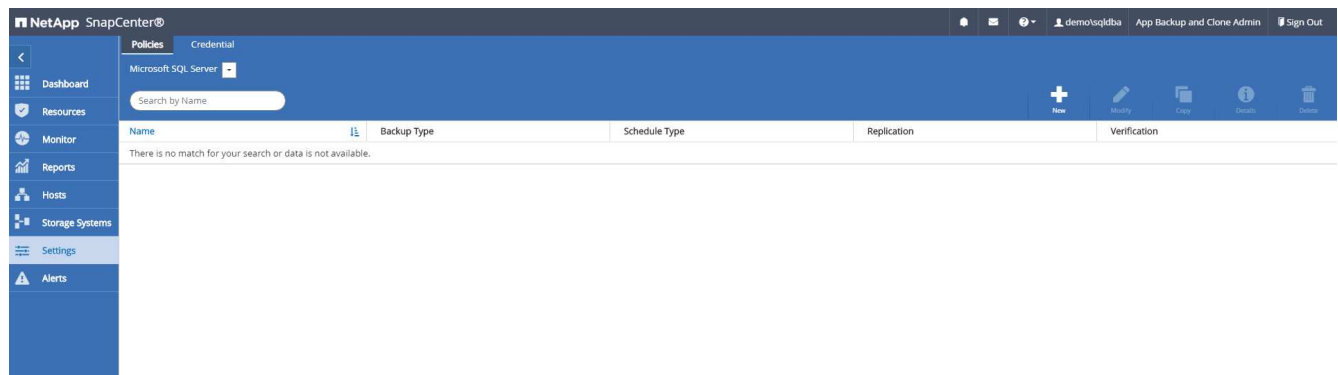
Policy name	Oracle Archive Log Backup
Details	Backup Oracle archive logs
Backup type	Online backup
Schedule type	Hourly
RMAN catalog backup	Disabled
Archive log pruning	None
On demand data backup retention	None
On demand archive log backup retention	None
Hourly data backup retention	None
Hourly archive log backup retention	Delete Snapshot copies older than : 7 days
Daily data backup retention	None
Daily archive log backup retention	None
Weekly data backup retention	None
Weekly archive log backup retention	None
Monthly data backup retention	None
Monthly archive log backup retention	None
Replication	SnapMirror enabled , Secondary policy label: Hourly , Error retry count: 3

Previous

Finish

## Créez une stratégie de sauvegarde complète de la base de données pour SQL

1. Connectez-vous à SnapCenter à l'aide d'un ID utilisateur de gestion de base de données, cliquez sur Paramètres, puis sur stratégies.



2. Cliquez sur Nouveau pour lancer un nouveau workflow de création de stratégie de sauvegarde ou choisissez une stratégie existante à modifier.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

SQL Server Full Backup

Details

Backup all data and log files

Previous

Next

3. Définissez l'option de sauvegarde et la fréquence de planification. Pour SQL Server configuré avec un groupe de disponibilité, il est possible de définir une réplique de sauvegarde préférée.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select SQL server backup options

Choose backup type

☒ Full backup and log backup

☐ Full backup

☐ Log backup

☐ Copy only backup

Maximum databases backed up per Snapshot copy:

Availability Group Settings

Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ On demand

☐ Hourly

☒ Daily

☐ Weekly

☐ Monthly

Previous

Next

4. Définissez la période de conservation des sauvegardes.



New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

Retention settings for up-to-the-minute restore operation ⓘ

☒ Keep log backups applicable to last

7

full backups

☐ Keep log backups applicable to last

14

days

Full backup retention settings ⓘ

Daily

☒ Total Snapshot copies to keep

7

☐ Keep Snapshot copies for

14

days

Previous

Next

5. Intégrez la réplication de copie de sauvegarde à un emplacement secondaire dans le cloud.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Daily

Error retry count

3

Previous

Next

6. Spécifiez tous les scripts facultatifs à exécuter avant ou après une procédure de sauvegarde.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments

Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments

Script timeout

Choose optional arguments...

Choose optional arguments...

60secs

Previous

Next

7. Spécifiez les options d'exécution de la vérification de sauvegarde.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select the options to run backup verification

Run verifications for the following backup schedules

Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

☐ Daily

Database consistency checks options

☒ Limit the integrity structure to physical structure of the database (PHYSICAL\_ONLY)
☒ Suppress all information message (NO\_INFOMSGS)
☐ Display all reported error messages per object (ALL\_ERRORMSGs)
☐ Do not check non-clustered indexes (NOINDEX)
☐ Limit the checks and obtain the locks instead of using an internal database Snapshot copy (TABLOCK)

Log backup

☐ Verify log backup.

Verification script settings

Script timeout

60

secs

Previous

Next

8. Récapitulatif.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Summary

Policy name	SQL Server Full Backup
Details	Backup all data and log files
Backup type	Full backup and log backup
Availability group settings	Backup only on preferred backup replica
Schedule Type	Daily
UTM retention	Total backup copies to retain : 7
Daily Full backup retention	Total backup copies to retain : 7
Replication	SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3
Backup prescript settings	undefined Prescript arguments:
Backup postscript settings	undefined Postscript arguments:
Verification for backup schedule type	none
Verification prescript settings	undefined Prescript arguments:
Verification postscript settings	undefined Postscript arguments:

Previous

Finish

### Créez une stratégie de sauvegarde du journal de base de données pour SQL.

1. Connectez-vous à SnapCenter à l'aide d'un ID utilisateur de gestion de base de données, cliquez sur Paramètres > règles, puis sur Nouveau pour lancer un nouveau workflow de création de règles.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

Details

SQL Server Log Backup

Backup SQL server log

Previous

Next

2. Définissez l'option de sauvegarde du journal et la fréquence de planification. Pour SQL Server configuré avec un groupe de disponibilité, une réplique de sauvegarde préférée peut être définie.

36

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select SQL server backup options

Choose backup type

☐ Full backup and log backup

☐ Full backup

☒ Log backup

☐ Copy only backup

Maximum databases backed up per Snapshot copy:

Availability Group Settings

Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ On demand

☒ Hourly

☐ Daily

☐ Weekly

☐ Monthly

Previous

Next

3. La stratégie de sauvegarde des données de SQL Server définit la rétention de la sauvegarde des journaux ; acceptez les valeurs par défaut ici.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Log backup retention settings

Up-to-the-minute (UTM) retention settings retains log backups created as part of full backup and full and log backup operations. UTM retention settings also decides for how many full backups the log backups are to be retained. For example, if UTM retention settings is configured to retain log backups of the last 5 full backups, then the log backups of the last 5 full backups are retained and the rest are deleted.

Previous

Next

4. Réplication de sauvegardes de journaux sur un stockage secondaire dans le cloud.



New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Hourly

Error retry count

3

Previous

Next

5. Spécifiez tous les scripts facultatifs à exécuter avant ou après une procédure de sauvegarde.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments

Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments

Script timeout

Choose optional arguments...

Choose optional arguments...

60secs

Previous

Next

6. Récapitulatif.

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

Policy name	SQL Server Log Backup
Details	Backup SQL server log
Backup type	Log transaction backup
Availability group settings	Backup only on preferred backup replica
Schedule Type	Hourly
Replication	SnapMirror enabled , Secondary policy label: Hourly , Error retry count: 3
Backup prescript settings	undefined Prescript arguments:
Backup postscript settings	undefined Postscript arguments:
Verification for backup schedule type	none
Verification prescript settings	undefined Prescript arguments:
Verification postscript settings	undefined Postscript arguments:

Previous

Finish

## 8. Mettre en œuvre une politique de sauvegarde pour protéger la base de données

SnapCenter utilise un groupe de ressources pour sauvegarder une base de données dans un groupe logique de ressources de bases de données, par exemple plusieurs bases de données hébergées sur un serveur, une base de données partageant les mêmes volumes de stockage, plusieurs bases de données prenant en charge une application professionnelle, etc. La protection d'une base de données unique crée un groupe de ressources lui-même. Les procédures suivantes montrent comment mettre en œuvre une stratégie de sauvegarde créée à la section 7 pour protéger les bases de données Oracle et SQL Server.

### Créez un groupe de ressources pour la sauvegarde complète d'Oracle

1. Connectez-vous à SnapCenter à l'aide d'un ID utilisateur de gestion de base de données et accédez à l'onglet Ressources. Dans la liste déroulante Affichage, choisissez base de données ou Groupe de ressources pour lancer le flux de travail de création de groupe de ressources.

NetApp SnapCenter®

demolordba

App Backup and Clone Admin

Sign Out

<

Dashboard

Resources

Monitor

Reports

Hosts

Storage Systems

Settings

Alerts

Oracle Database

View Database

Search databases

Refresh Resources

New Resource Group

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
cdb2	Single Instance (Multitenant)	rhe12.demo.netapp.com				Not protected

2. Indiquez un nom et des balises pour le groupe de ressources. Vous pouvez définir un format de nommage

pour la copie Snapshot et contourner la destination redondante du journal d'archivage si elle est configurée.

NetApp SnapCenter®

Oracle Database

Search databases

17 Name

cdb2

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide a name and tags for the resource group

Name rhe12\_cdb2

Tags orafullbkup

☒ Use custom name format for Snapshot copy

\$CustomText

rhe12\_cdb2

Backup settings

Exclude archive log destinations from backup

3. Ajoutez des ressources de base de données au groupe de ressources.

NetApp SnapCenter®

Oracle Database

Search databases

17 Name

cdb2

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Add resources to Resource Group

Host All

Available Resources

search available resources

Selected Resources

cdb2 (rhe12.demo.netapp.com)

4. Sélectionnez une stratégie de sauvegarde complète créée dans la section 7 dans la liste déroulante.

NetApp SnapCenter®

Oracle Database

Search databases

17 Name

cdb2

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select one or more policies and configure schedules

Oracle Full Online Backup

Configure schedules for selected policies

Policy	Applied Schedules	Configure Schedules
Oracle Full Online Backup	None	+

Total 1

5. Cliquez sur le signe (+) pour configurer le programme de sauvegarde souhaité.



## 8. Récapitulatif.

### Créez un groupe de ressources pour la sauvegarde du journal d'Oracle

1. Connectez-vous à SnapCenter à l'aide d'un ID utilisateur de gestion de base de données et accédez à l'onglet Ressources. Dans la liste déroulante Affichage, choisissez base de données ou Groupe de ressources pour lancer le flux de travail de création de groupe de ressources.

Name	Resources	Tags	Policies	Last Backup	Overall Status
rhei2_cdb2	1	orafullbkup	Oracle Full Online Backup		

2. Indiquez un nom et des balises pour le groupe de ressources. Vous pouvez définir un format de nommage pour la copie Snapshot et contourner la destination redondante du journal d'archivage si elle est configurée.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2\_cdb2

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide a name and tags for the resource group

Name

Tags

☒ Use custom name format for Snapshot copy

Backup settings

Exclude archive log destinations from backup

3. Ajoutez des ressources de base de données au groupe de ressources.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2\_cdb2

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Add resources to Resource Group

Host

Available Resources

search available resources

Selected Resources

cdb2 (rhel2.demo.netapp.com)

Total 1

Previous Next

4. Sélectionnez une stratégie de sauvegarde de journal créée dans la section 7 dans la liste déroulante.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2\_cdb2

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select one or more policies and configure schedules

Oracle Archive Log Backup

Oracle Full Online Backup

Oracle Archive Log Backup

Policy

Applied Schedules

Configure Schedules

Oracle Archive Log Backup

None

Total 1

Previous Next

5. Cliquez sur le signe (+) pour configurer le programme de sauvegarde souhaité.

Add schedules for policy Oracle Archive Log Backup

Hourly

Start date

09/10/2021 3:00 PM

☒ Expires on

12/31/2021 3:00 PM

Repeat every

1

hours

0

mins

i

The schedules are triggered in the SnapCenter Server time zone.

Cancel

OK

6. Si la vérification de sauvegarde est configurée, elle s'affiche ici.

NetApp SnapCenter®

demolora@ba App Backup and Clone Admin Sign Out

Oracle Database

Search resource groups

Name

rhel2\_cdb2

Total 1

New Resource Group

1

2

3

4

5

6

Name

Resources

Policies

Verification

Notification

Summary

Configure verification schedules

Policy

Schedule Type

Applied Schedules

Configure Schedules

There is no match for your search or data is not available.

Total 0

Previous

Next

7. Configurez un serveur SMTP pour la notification par e-mail si vous le souhaitez.



NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2\_cdb2

Total 1

New Resource Group

If you want to send notifications for scheduled or on demand jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide email settings ⓘ

Select the service accounts or people to notify regarding protection issues.

Email preference: Never

From: From email

To: Email to

Subject: Notification

☐ Attach job report

Previous Next

## 8. Récapitulatif.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2\_cdb2

Total 1

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Resource group name: rhel2\_cdb2\_log

Tags: oralogbkup

Policy: Oracle Archive Log Backup: Hourly

Plug-in: SnapCenter Plug-in for Oracle Database

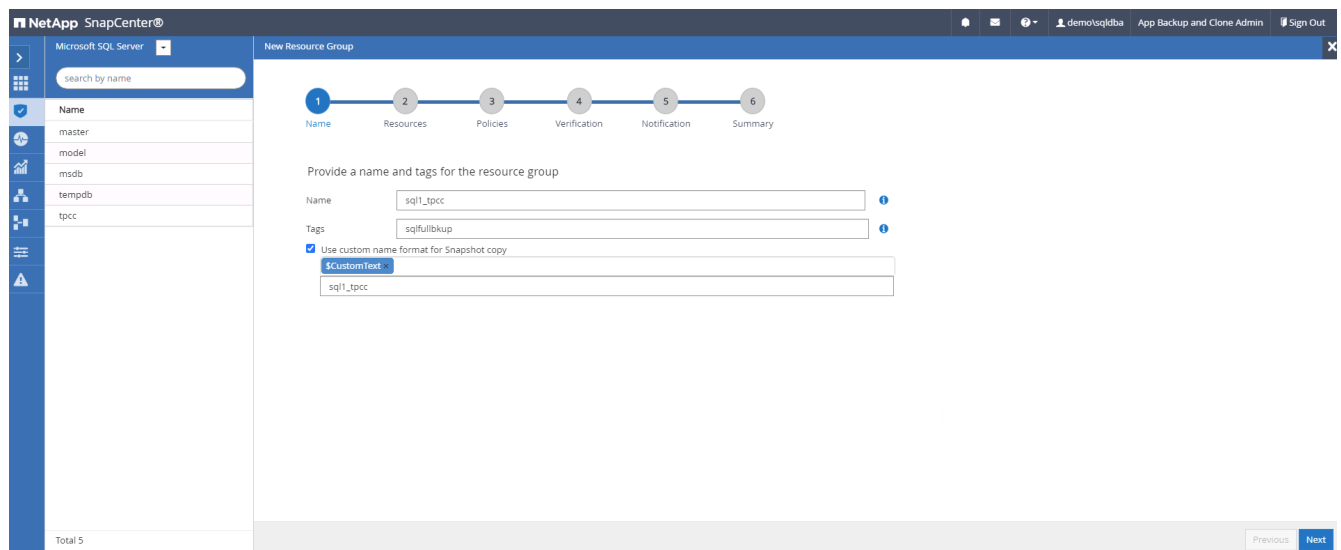
Verification enabled for policy: None

Send email: No

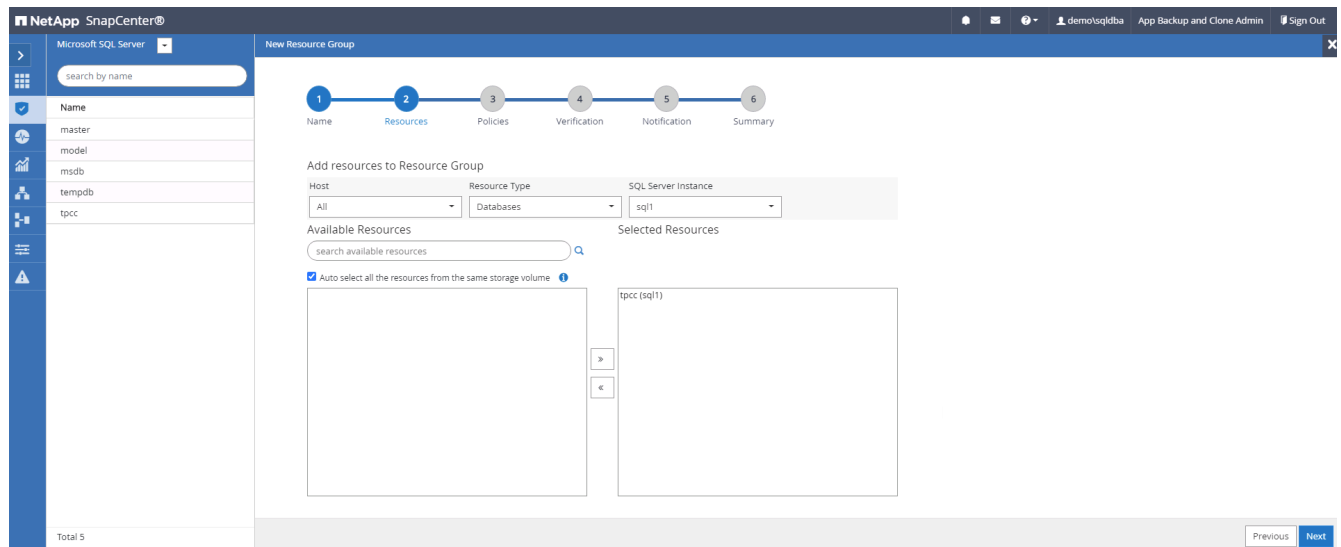
Previous Finish

## Créez un groupe de ressources pour la sauvegarde complète de SQL Server

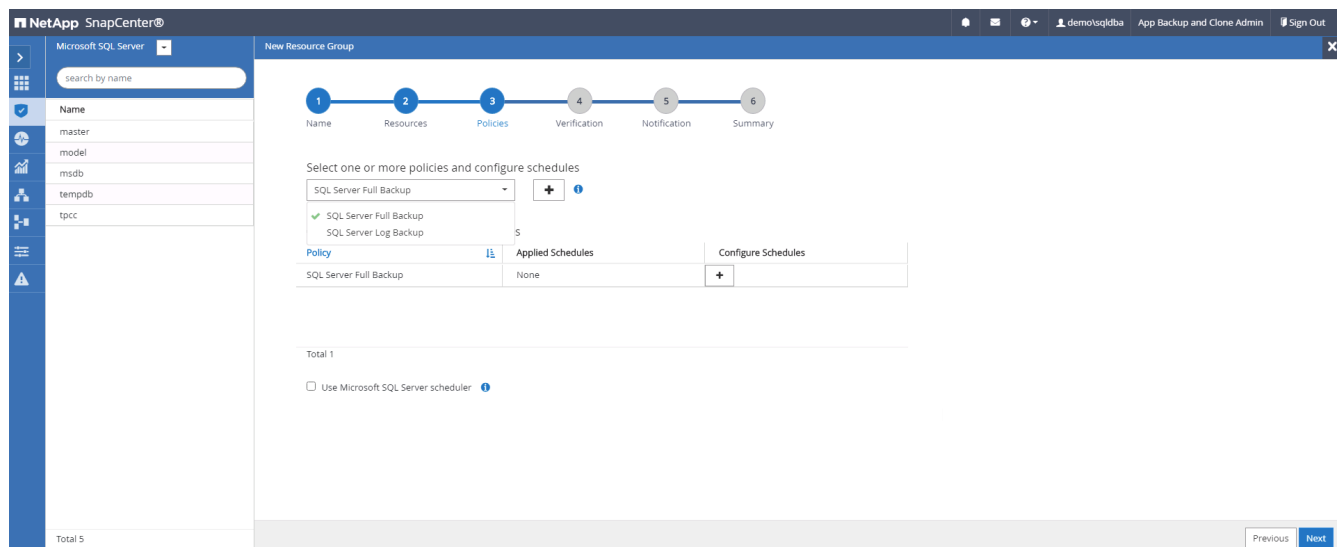
1. Connectez-vous à SnapCenter à l'aide d'un ID utilisateur de gestion de base de données et accédez à l'onglet Ressources. Dans la liste déroulante Affichage, choisissez une base de données ou un groupe de ressources pour lancer le flux de travail de création de groupe de ressources. Indiquez un nom et des balises pour le groupe de ressources. Vous pouvez définir un format d'attribution de nom à la copie Snapshot.



2. Sélectionnez les ressources de base de données à sauvegarder.



3. Sélectionnez une stratégie de sauvegarde SQL complète créée dans la section 7.



4. Ajoutez la durée exacte des sauvegardes ainsi que la fréquence.

Add schedules for policy SQL Server Full Backup

Daily

Start date 09/10/2021 6:20 PM

☒ Expires on 12/31/2021 6:20 PM

Repeat every 1 days

*i* The schedules are triggered in the SnapCenter Server time zone.

Cancel OK

5. Choisissez le serveur de vérification pour la sauvegarde sur secondaire si la vérification de sauvegarde doit être effectuée. Cliquez sur Charger le localisateur pour renseigner l'emplacement de stockage secondaire.

NetApp SnapCenter®

Microsoft SQL Server

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select the verification servers

Verification server Select one or more servers

Load secondary locators to verify backups on secondary Load locators

Secondary storage location: SnapVault or SnapMirror

Source Volume Destination Volume

svm\_onPremsql1\_data svm\_hybridvolsql1\_data\_dr

svm\_onPremsql1\_log svm\_hybridvolsql1\_log\_dr

Configure verification schedules

Policy Schedule Type Applied Schedules Configure Schedules

There is no match for your search or data is not available.

Total 5

Previous Next

6. Configurez le serveur SMTP pour la notification par e-mail si vous le souhaitez.

NetApp SnapCenter®

Microsoft SQL Server

search by name

master  
model  
msdb  
tempdb  
tpcc

Total 5

New Resource Group

If you want to send notifications for scheduled or on demand jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide email settings ⓘ  
Select the service accounts or people to notify regarding protection issues.

Email preference: Never

From: From email

To: Email to

Subject: Notification

☐ Attach job report

Previous Next

## 7. Récapitulatif.

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

There is no match for your search or data is not available.

Resources are not found. Click Refresh Resources to discover databases in the database view or create new resource group on the discovered databases from the resource view.

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Resource group name: sql1\_tpcc

Tags: sqlfullbkup

Policy: SQL Server Full Backup: Daily

Plug-in: SnapCenter Plug-in for Microsoft SQL Server

Verification Server: None

Verification enabled for policy: None

Send email: No

Previous Finish

### Créez un groupe de ressources pour la sauvegarde des journaux de SQL Server

1. Connectez-vous à SnapCenter à l'aide d'un ID utilisateur de gestion de base de données et accédez à l'onglet Ressources. Dans la liste déroulante Affichage, choisissez une base de données ou un groupe de ressources pour lancer le flux de travail de création de groupe de ressources. Indiquez le nom et les balises du groupe de ressources. Vous pouvez définir un format d'attribution de nom à la copie Snapshot.

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

sql1\_tpcc

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide a name and tags for the resource group

Name

sql1\_tpcc\_log

Tags

sqllogbkup

☒ Use custom name format for Snapshot copy

\$CustomText

sql1\_tpcc\_log

Total 1

Previous Next

2. Sélectionnez les ressources de base de données à sauvegarder.

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

sql1\_tpcc

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Add resources to Resource Group

Host

All

Resource Type

Databases

SQL Server Instance

sql1

Available Resources

search available resources

☒ Auto select all the resources from the same storage volume

tpcc (sql1)

Total 1

Previous Next

3. Sélectionnez une stratégie de sauvegarde du journal SQL créée à la section 7.

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

sql1\_tpcc

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select one or more policies and configure schedules

SQL Server Log Backup

SQL Server Full Backup

SQL Server Log Backup

Policy

SQL Server Log Backup

Applied Schedules

None

Configure Schedules

+

Total 1

☐ Use Microsoft SQL Server scheduler

Total 1

Previous Next

4. Ajoutez la synchronisation exacte pour la sauvegarde ainsi que la fréquence.

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

sql1\_tpcc

Total 1

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select one or more policies and configure schedules

SQL Server Log Backup

Configure schedules for selected policies

Policy	Applied Schedules	Configure Schedules
SQL Server Log Backup	Hourly: Repeat every 1 hours	

Total 1

☐ Use Microsoft SQL Server scheduler

Previous Next

5. Choisissez le serveur de vérification pour la sauvegarde sur secondaire si la vérification de sauvegarde doit être effectuée. Cliquez sur le localisateur de charge pour renseigner l'emplacement de stockage secondaire.

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

sql1\_tpcc

Total 1

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select the verification servers

Verification server: Select one or more servers

Load secondary locators to verify backups on secondary

Load locators

Secondary storage location: SnapVault or SnapMirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcv:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcv:sql1_log_dr

Configure verification schedules

Policy	Schedule Type	Applied Schedules	Configure Schedules
SQL Server Log Backup	Hourly: Repeat every 1 hours		

There is no match for your search or data is not available.

Previous Next

6. Configurez le serveur SMTP pour la notification par e-mail si vous le souhaitez.

NetApp SnapCenter®

Microsoft SQL Server

search by name

sql1\_tpcc

Total 1

New Resource Group

If you want to send notifications for scheduled or on demand jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide email settings

Select the service accounts or people to notify regarding protection issues.

Email preference: Never

From: From email

To: Email to

Subject: Notification

☐ Attach job report

Previous Next

## 7. Récapitulatif.

NetApp SnapCenter®

Microsoft SQL Server

search by name

sql1\_tpcc

Total 1

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Resource group name: sql1\_tpcc\_log

Tags: sqllogbkup

Policy: SQL Server Log Backup: Hourly

Plug-in: SnapCenter Plug-in for Microsoft SQL Server

Verification Server: None

Verification enabled for policy: None

Send email: No

Previous Finish

## 9. Valider la sauvegarde

Une fois que des groupes de ressources de sauvegarde de base de données sont créés pour protéger les ressources de base de données, les tâches de sauvegarde s'exécutent en fonction du planning prédéfini. Vérifiez l'état d'exécution du travail sous l'onglet moniteur.

NetApp SnapCenter®

Jobs Schedules Events Logs

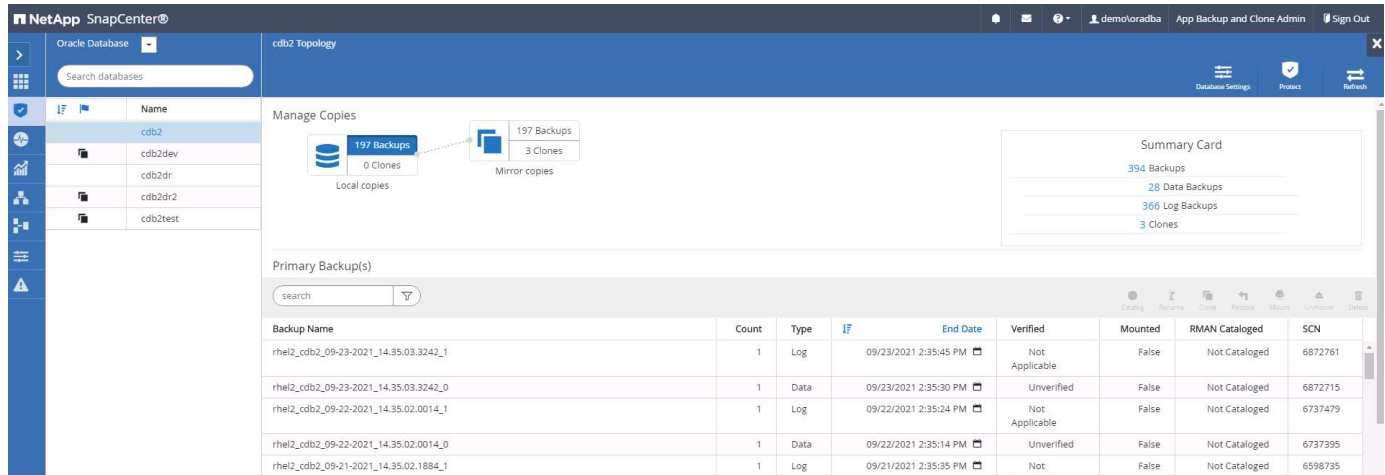
search by name

Jobs - Filter

ID	Status	Name	Start date	End date	Owner
532	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 8:35:01 PM	09/14/2021 8:37:10 PM	demo/sqldba
528	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 7:35:01 PM	09/14/2021 7:37:09 PM	demo/sqldba
524	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 6:35:01 PM	09/14/2021 6:37:08 PM	demo/sqldba
521	✓	Backup of Resource Group 'sql1_tpcc' with policy 'SQL Server Full Backup'	09/14/2021 6:25:01 PM	09/14/2021 6:27:14 PM	demo/sqldba
517	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 5:35:01 PM	09/14/2021 5:37:09 PM	demo/sqldba
513	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 4:35:01 PM	09/14/2021 4:37:08 PM	demo/sqldba
509	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 3:35:01 PM	09/14/2021 3:37:10 PM	demo/sqldba
503	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 2:35:01 PM	09/14/2021 2:37:09 PM	demo/sqldba

Accédez à l'onglet Ressources, cliquez sur le nom de la base de données pour afficher les détails de la

sauvegarde de la base de données, et basculez entre les copies locales et les copies miroir pour vérifier que les sauvegardes Snapshot sont répliquées dans un emplacement secondaire du cloud public.



The screenshot shows the NetApp SnapCenter interface. On the left, there's a sidebar with navigation icons. The main area is titled 'Manage Copies' and shows a diagram with 'Local copies' (197 Backups, 0 Clones) and 'Mirror copies' (197 Backups, 3 Clones). A 'Summary Card' on the right displays: 394 Backups, 28 Data Backups, 366 Log Backups, and 3 Clones. Below this, a table lists 'Primary Backup(s)' with columns: Backup Name, Count, Type, End Date, Verified, Mounted, RMAN Cataloged, and SCN. The table contains five rows of backup data.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_09-23-2021_14.35.03.3242_1	1	Log	09/23/2021 2:35:45 PM	Not Applicable	False	Not Cataloged	6872761
rhel2_cdb2_09-23-2021_14.35.03.3242_0	1	Data	09/23/2021 2:35:30 PM	Unverified	False	Not Cataloged	6872715
rhel2_cdb2_09-22-2021_14.35.02.0014_1	1	Log	09/22/2021 2:35:24 PM	Not Applicable	False	Not Cataloged	6737479
rhel2_cdb2_09-22-2021_14.35.02.0014_0	1	Data	09/22/2021 2:35:14 PM	Unverified	False	Not Cataloged	6737395
rhel2_cdb2_09-21-2021_14.35.02.1884_1	1	Log	09/21/2021 2:35:35 PM	Not Applicable	False	Not Cataloged	6598735

À ce stade, les copies de sauvegarde de base de données dans le cloud sont prêtes à cloner pour exécuter des processus de développement/test ou pour la reprise après incident en cas de panne principale.

## Mise en route du cloud public AWS

Cette section décrit le processus de déploiement de Cloud Manager et de Cloud Volumes ONTAP dans AWS.

### Cloud public AWS



Pour simplifier l'suivi, nous avons créé ce document en nous basant sur le déploiement dans AWS. Cependant, ce processus est très similaire pour Azure et GCP.

#### 1. Contrôle avant vol

Avant le déploiement, s'assurer que l'infrastructure permet le déploiement à l'étape suivante. Ceci inclut les éléments suivants :

- Compte AWS
- VPC dans votre région
- Sous-réseau avec accès à l'Internet public
- Autorisations permettant d'ajouter des rôles IAM à votre compte AWS
- Une clé secrète et une clé d'accès pour votre utilisateur AWS

#### 2. Étapes de déploiement de Cloud Manager et de Cloud Volumes ONTAP dans AWS

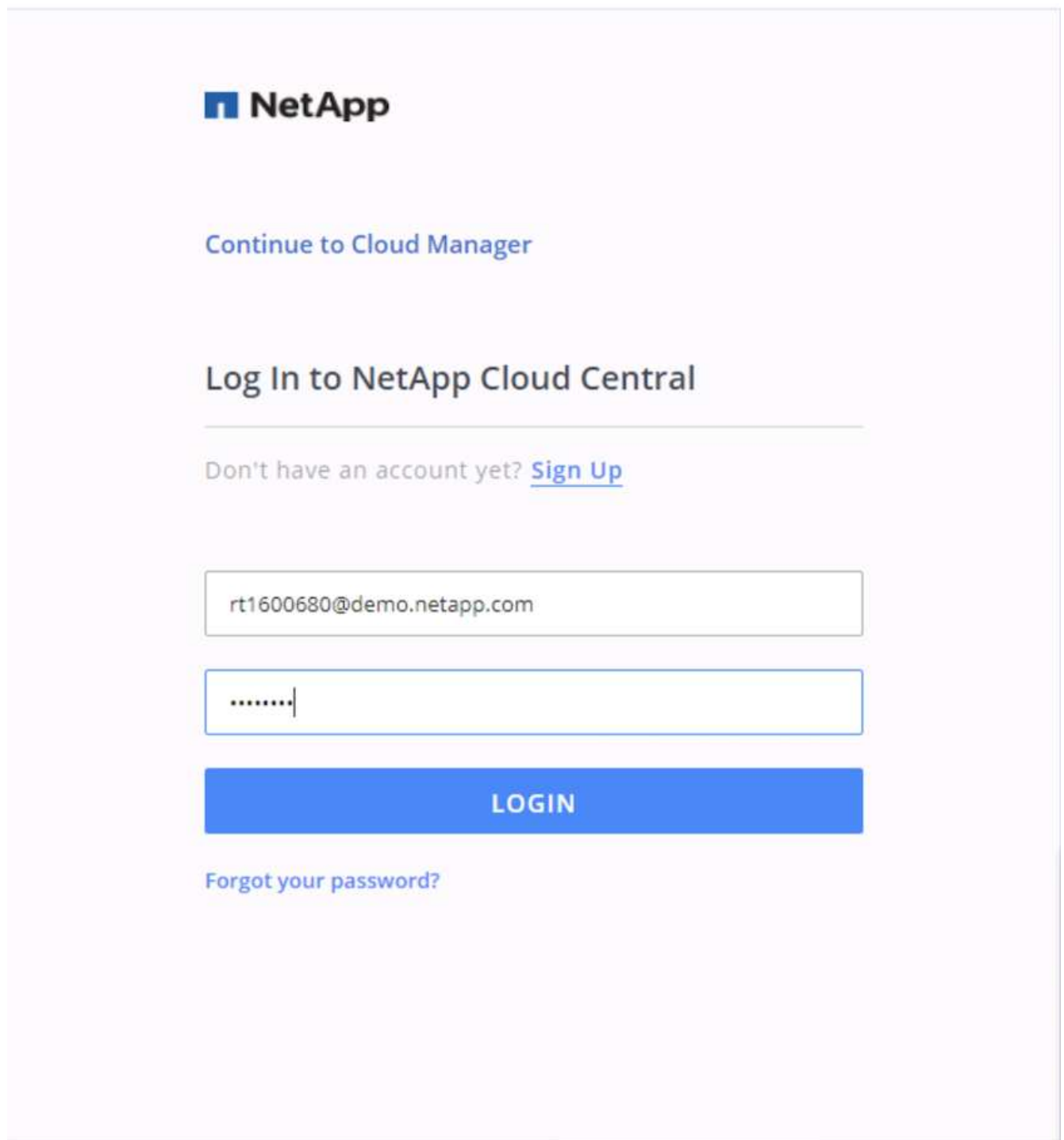


De nombreuses méthodes de déploiement de Cloud Manager et de Cloud Volumes ONTAP sont disponibles. Cette méthode est la plus simple, mais requiert la plupart des autorisations. Si cette méthode n'est pas adaptée à votre environnement AWS, consultez le "[Documentation cloud NetApp](#)".



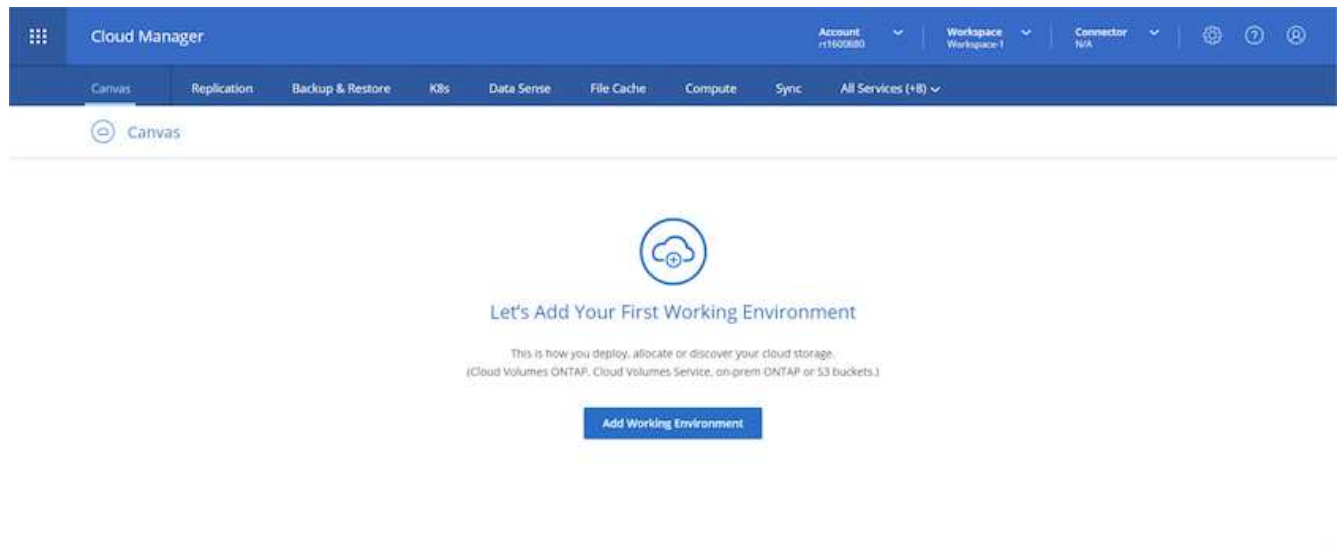
## Déployez Cloud Manager Connector

1. Accédez à "[NetApp Cloud Central](#)" et connectez-vous ou inscrivez-vous.

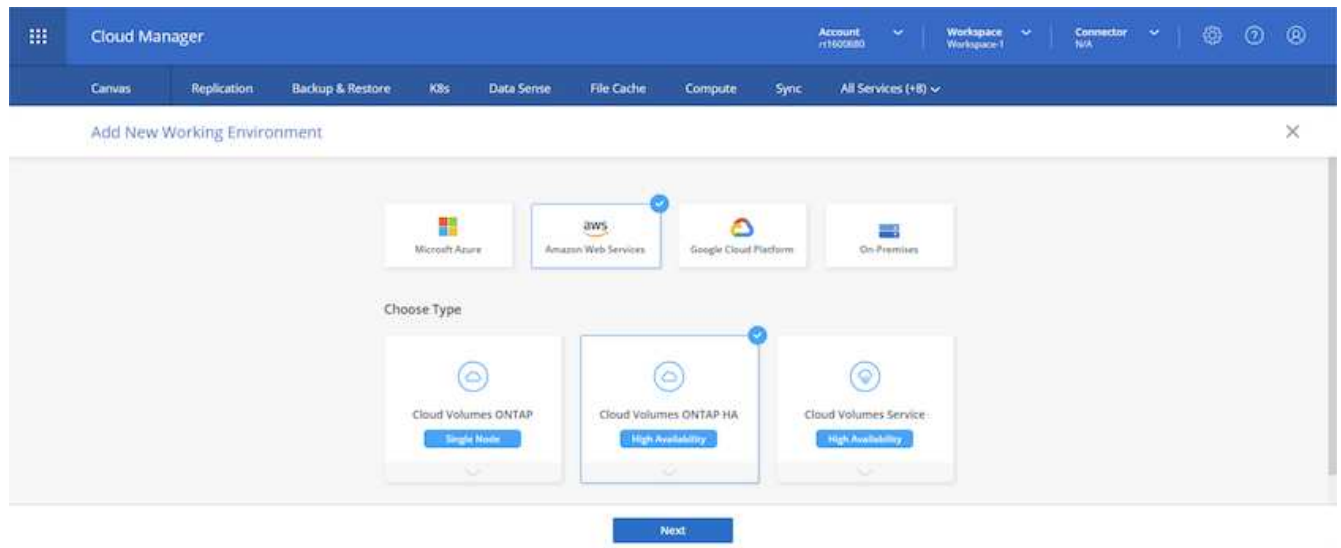


The image shows the NetApp Cloud Central login page. At the top is the NetApp logo. Below it is a link to "Continue to Cloud Manager". The main heading is "Log In to NetApp Cloud Central". Below the heading is a link for users who don't have an account: "Don't have an account yet? [Sign Up](#)". There are two input fields: the first contains the email address "rt1600680@demo.netapp.com", and the second contains a masked password ".....". Below these fields is a blue "LOGIN" button. At the bottom of the login section is a link: "Forgot your password?".

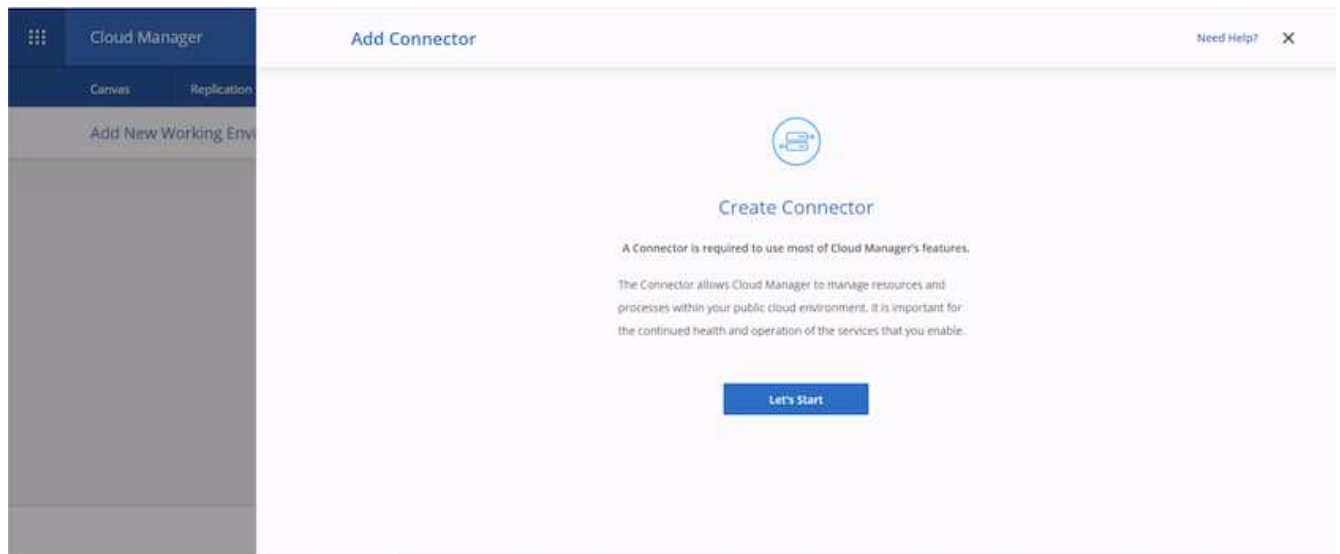
2. Une fois connecté, vous devez être redirigé vers la toile.



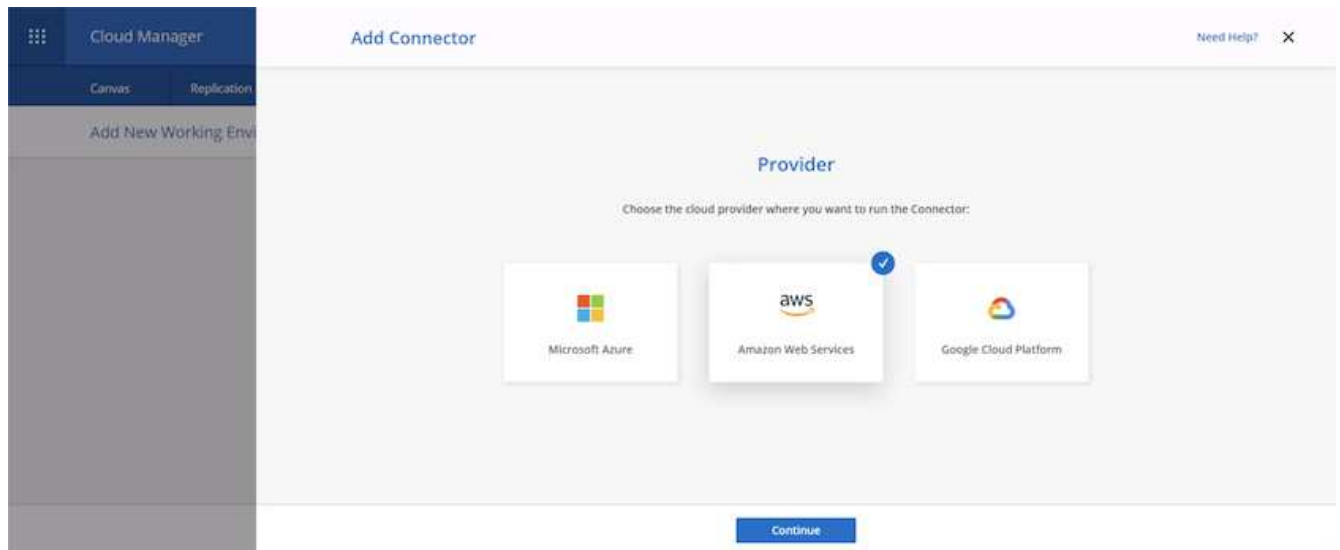
3. Cliquez sur Add Working Environment (Ajouter un environnement de travail) et choisissez Cloud Volumes ONTAP in AWS. Vous pouvez également choisir de déployer un système à un seul nœud ou une paire haute disponibilité. J'ai choisi de déployer une paire haute disponibilité.



4. Si aucun connecteur n'a été créé, une fenêtre contextuelle s'affiche vous demandant de créer un connecteur.



5. Cliquez sur Oui, puis choisissez AWS.



6. Saisissez votre clé secrète et votre clé d'accès. Assurez-vous que votre utilisateur dispose des autorisations appropriées indiquées sur le "Page règles NetApp".

Cloud Manager

Add Connector

Need Help? X

Get Ready AWS Credentials Details Network Security Group Review

### AWS Credentials

AWS Access Key

AWS Access Key is required

AWS Secret Key

Region

us-east-1 | US East (N. Virginia)

Want to launch an instance without AWS Credentials?

Previous Next

7. Attribuez un nom au connecteur et utilisez un rôle prédéfini comme décrit sur le ["Page règles NetApp"](#). Vous pouvez également demander à Cloud Manager de créer le rôle dont vous avez besoin.

Cloud Manager

Add Connector

Need Help? X

Get Ready AWS Credentials Details Network Security Group Review

### Details

Connector Instance Name

awscloudmanager

Connector Role

Create Role Select an existing Role

Role Name

Cloud-Manager-Operator-IBht24j

Add Tags to Connector Instance

Previous Next

8. Fournissez les informations de mise en réseau nécessaires au déploiement du connecteur. Vérifiez que l'accès Internet sortant est activé par :
- En donnant au connecteur une adresse IP publique
  - Donner au connecteur un proxy pour fonctionner
  - Donner au connecteur une route vers l'Internet public par le biais d'une passerelle Internet

**Cloud Manager**

Canvas Replication

Add New Working Env

**Add Connector**

Need Help? X

Get Ready AWS Credentials Details **4 Network** 5 Security Group 6 Review

**Connectivity**

VPC: vpc-083fcbd79f75dfb6e - 10.221.0.0/16

Subnet: 10.221.4.0/24 | publicSN\_us-east-1a\_r11600...

Key Pair: r11600680

Public IP: Enable

**Proxy Configuration (Optional)**

HTTP Proxy: Example: https://172.16.254.1:8080

Define Credentials for this Proxy

Upload a root certificate

Previous Next

9. Établir une communication avec le connecteur via SSH, HTTP et HTTPS en fournissant un groupe de sécurité ou en créant un nouveau groupe de sécurité. J'ai activé l'accès au connecteur à partir de mon adresse IP uniquement.

**Cloud Manager**

Canvas Replication

Add New Working Env

**Add Connector**

Need Help? X

Get Ready AWS Credentials Details Network **5 Security Group** 6 Review

The security group must allow inbound HTTP, HTTPS and SSH access.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

HTTP (Port 80)	HTTPS (Port 443)	SSH (Port 22)
Source Type: My IP	Source Type: My IP	Source Type: My IP
Source (CIDR): 216.240.31.145/32	Source (CIDR): 216.240.31.145/32	Source (CIDR): 216.240.31.145/32

Previous Next

10. Vérifiez les informations de la page de résumé et cliquez sur Ajouter pour déployer le connecteur.

Cloud Manager

Canvas Replication

Add New Working Env

Add Connector

Need Help? X

Get Ready AWS Credentials Details Network Security Group Review

Code for Terraform Automation

Connector Name: awscloudmanager

Region: us-east-1

VPC: vpc-083fcbd79f75dfb6e - 10.221.0.0/16

Subnet: 10.221.4.0/24 | publicSN\_us-east-1a\_rt1600680

Key Pair: rt1600680

Public IP: Enable

Proxy: None

Security Group: HTTP: 216.240.31.145/32, HTTPS: 216.240.31.145/32, SSH: 216.240.31.145/32

Previous Add

11. Le connecteur se déploie à présent à l'aide d'une pile de formation de nuages. Vous pouvez contrôler sa progression depuis Cloud Manager ou via AWS.

Cloud Manager

Canvas Replication

Add New Working Env

Deploying a Connector

Show Details

- Keep this wizard open until the deployment process is complete. It usually takes about 7 minutes.
- No other Cloud Manager features are available during deployment.
- When the process is complete, you can continue the operation that you started.

12. Une fois le déploiement terminé, une page de réussite s'affiche.

Cloud Manager

Canvas Replication

Add New Working Env

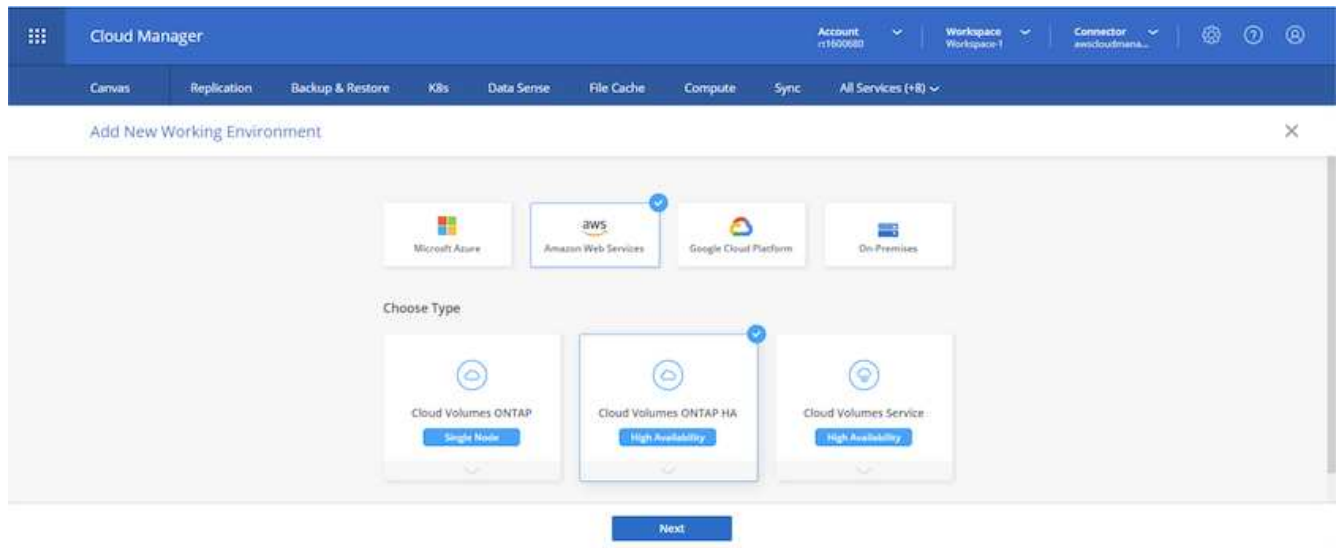
Connector Successfully Created

The Connector was created successfully.

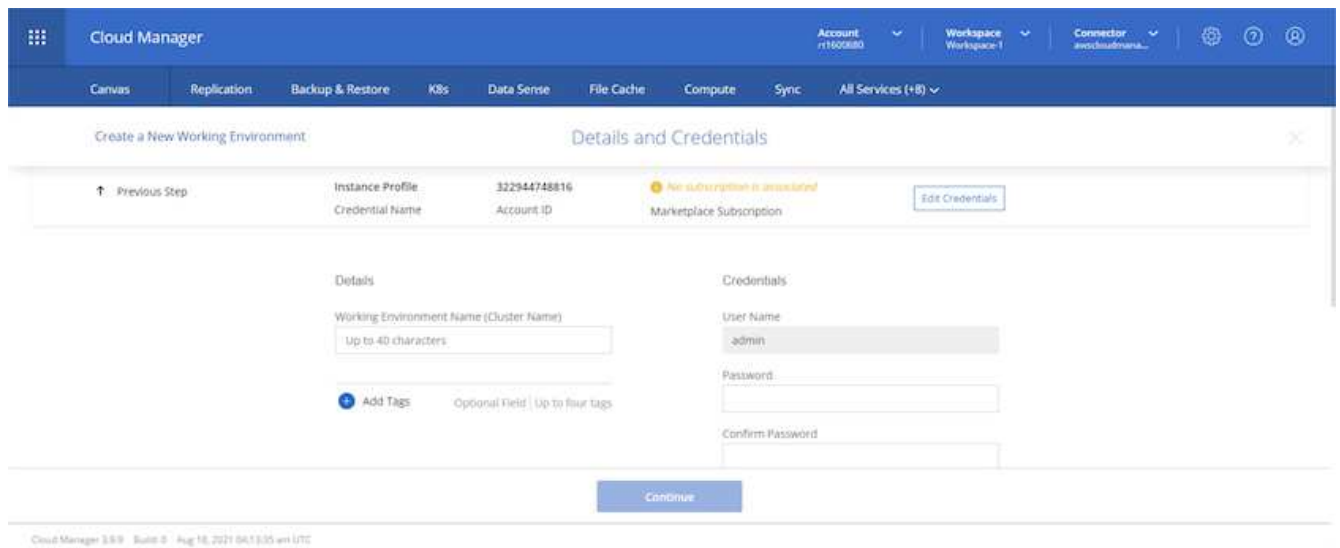
Continue

## Déployez Cloud Volumes ONTAP

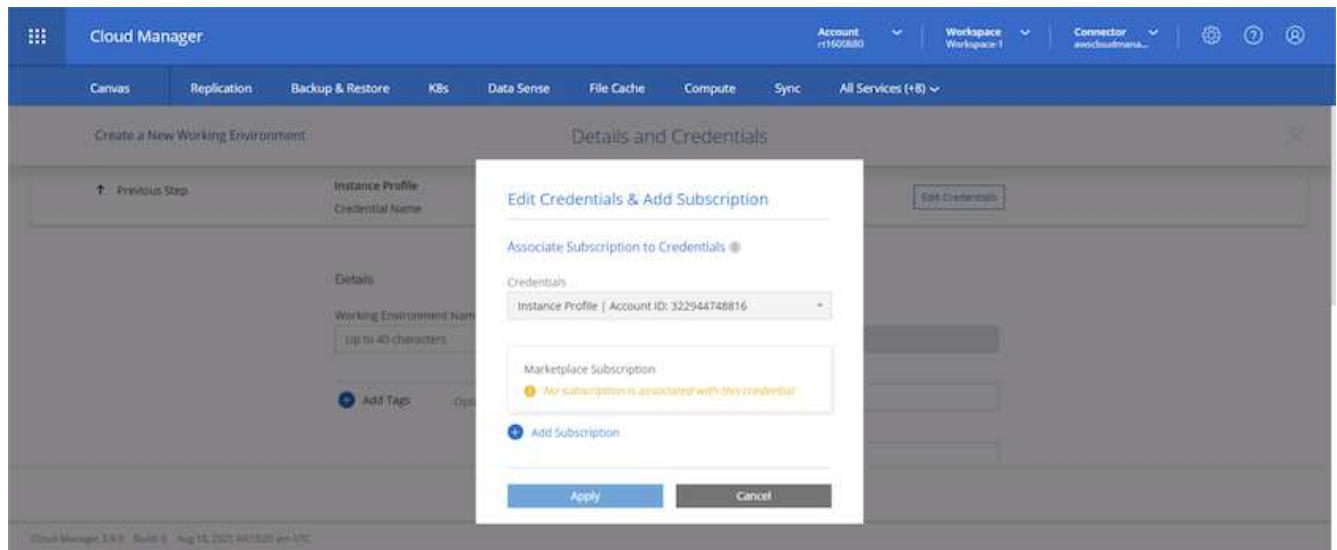
1. Sélectionnez AWS et le type de déploiement selon vos besoins.



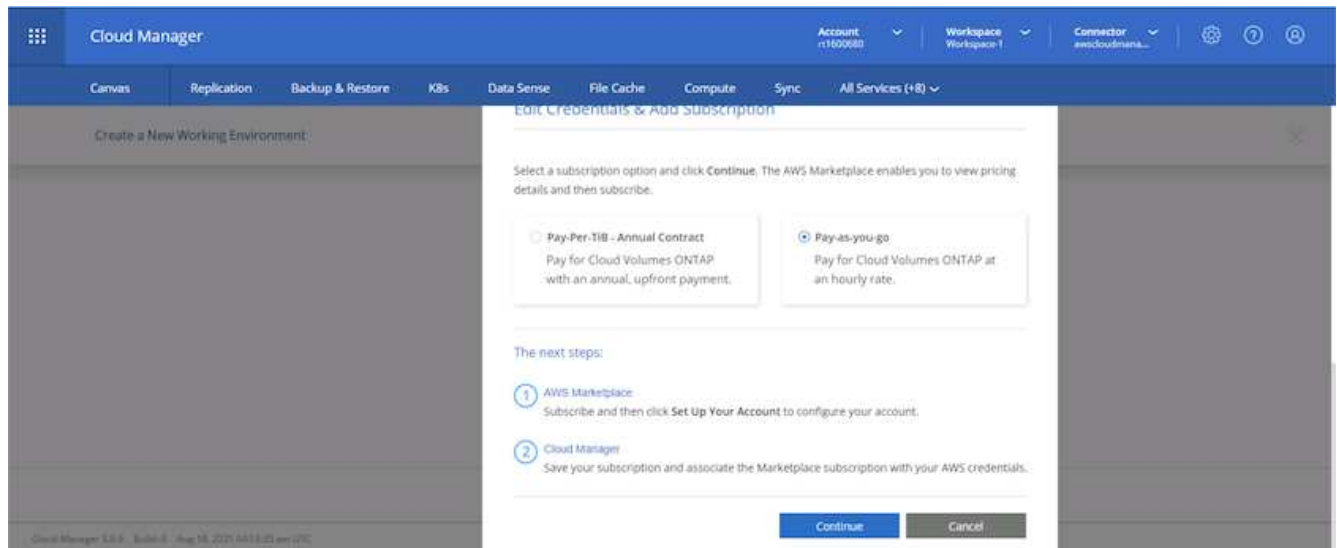
2. Si aucun abonnement n'a été attribué et que vous souhaitez acheter avec PAYGO, choisissez Modifier les informations d'identification.



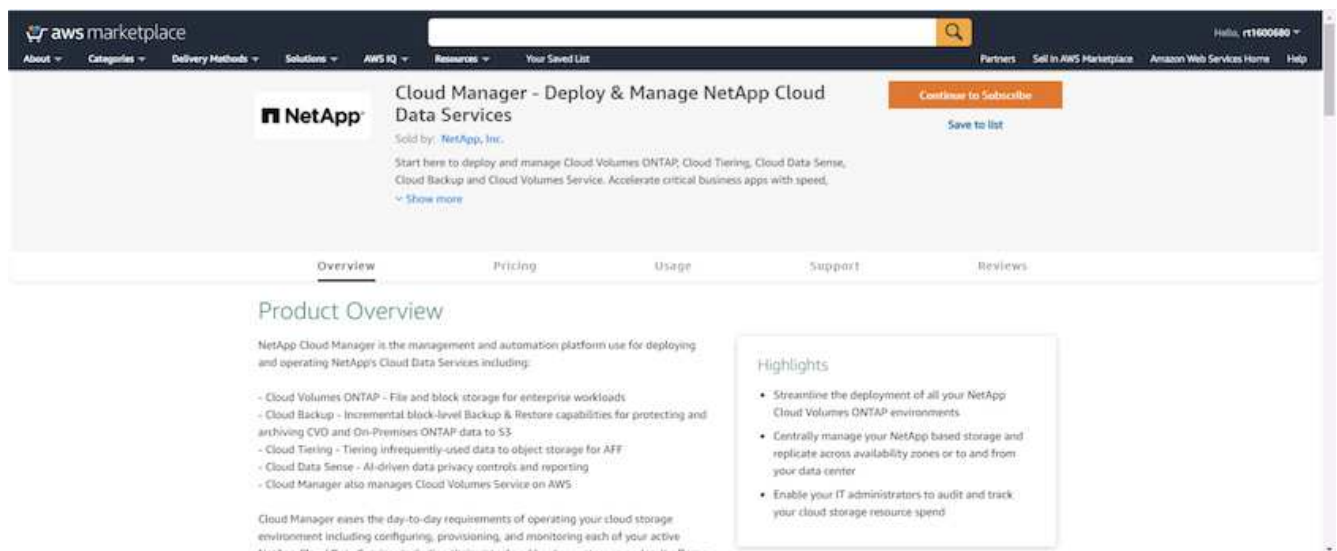
3. Choisissez Ajouter un abonnement.



4. Choisissez le type de contrat auquel vous souhaitez vous abonner. J'ai choisi le paiement à l'utilisation.

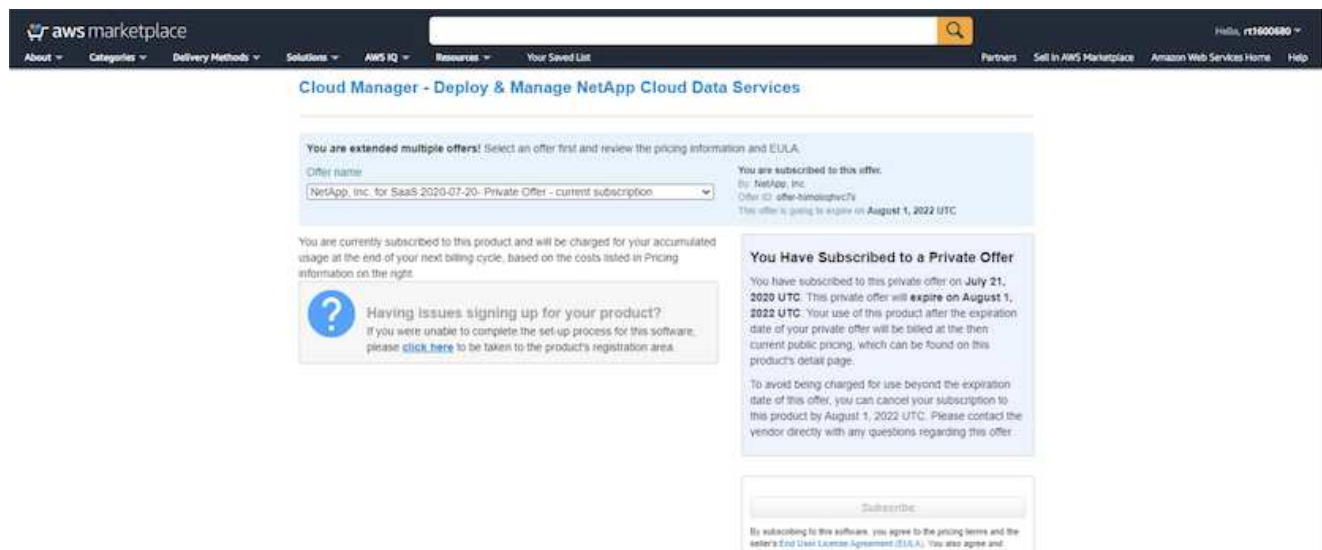


5. Vous êtes redirigé vers AWS ; sélectionnez Continuer pour vous inscrire.

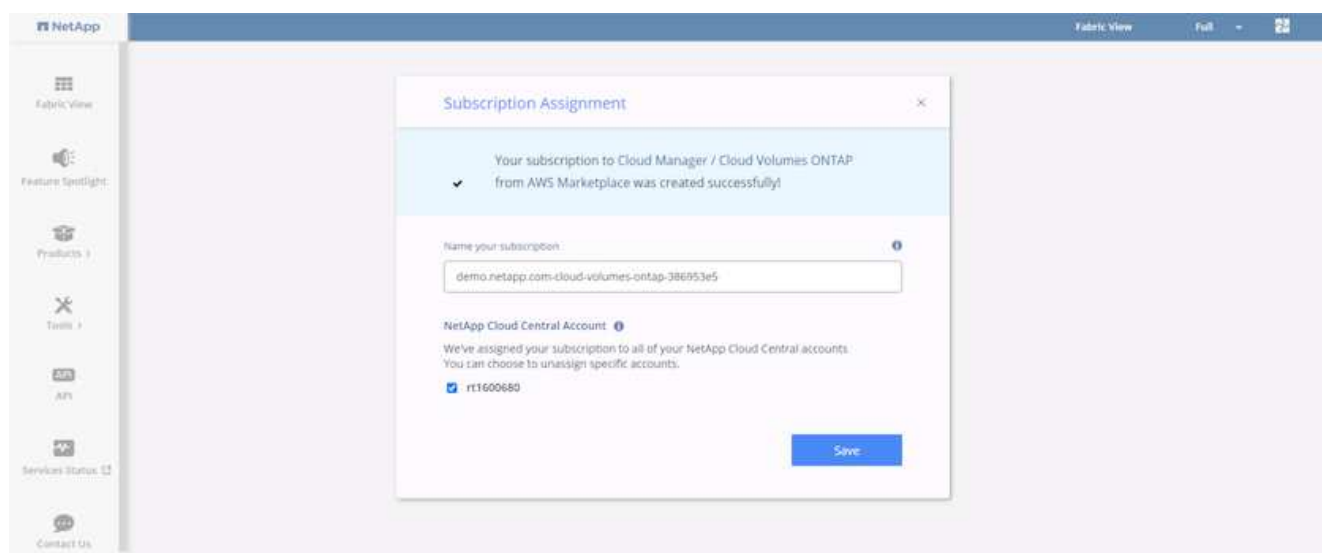




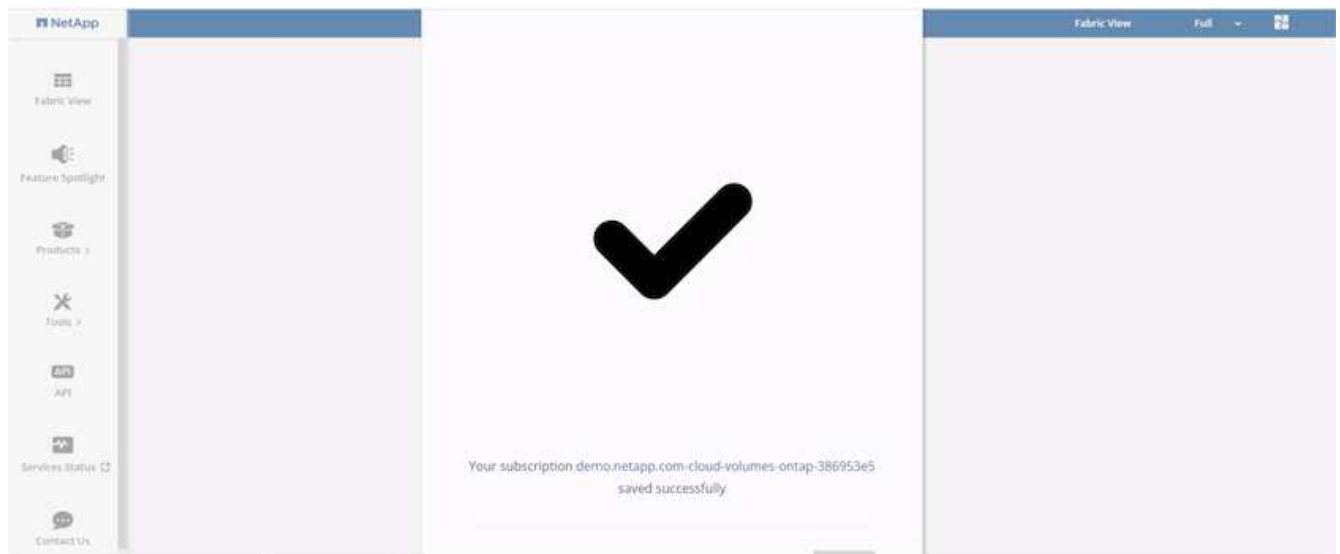
6. Vous allez être redirigé vers NetApp Cloud Central. Si vous êtes déjà abonné et que vous n'êtes pas redirigé, cliquez ici.



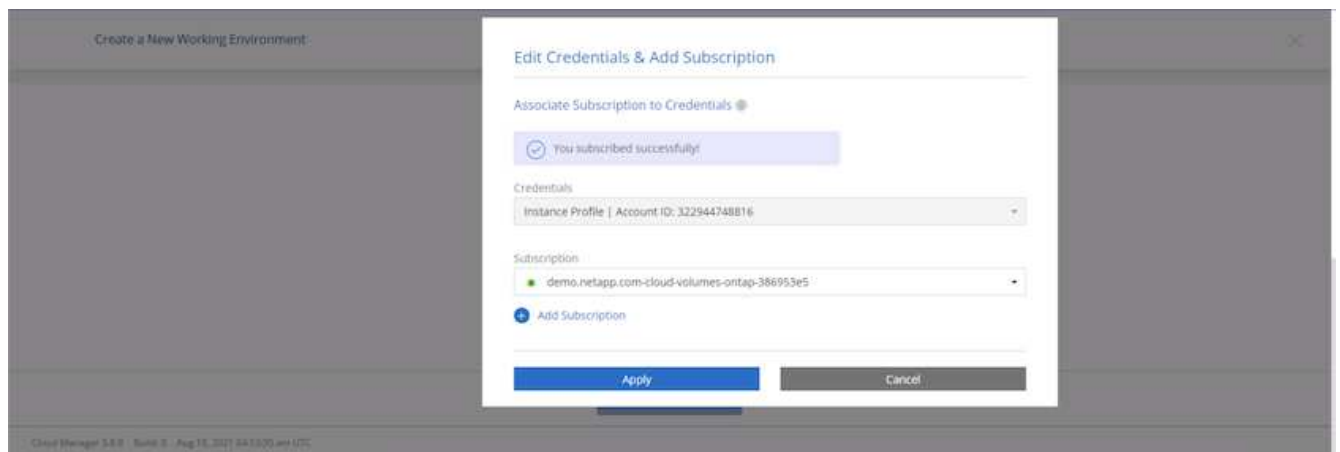
7. Vous êtes redirigé vers Cloud Central, où vous devez nommer votre abonnement et l'attribuer à votre compte Cloud Central.



8. Une fois réussi, une page de coche s'affiche. Revenez à l'onglet Cloud Manager.



9. L'abonnement s'affiche désormais dans Cloud Central. Cliquez sur appliquer pour continuer.



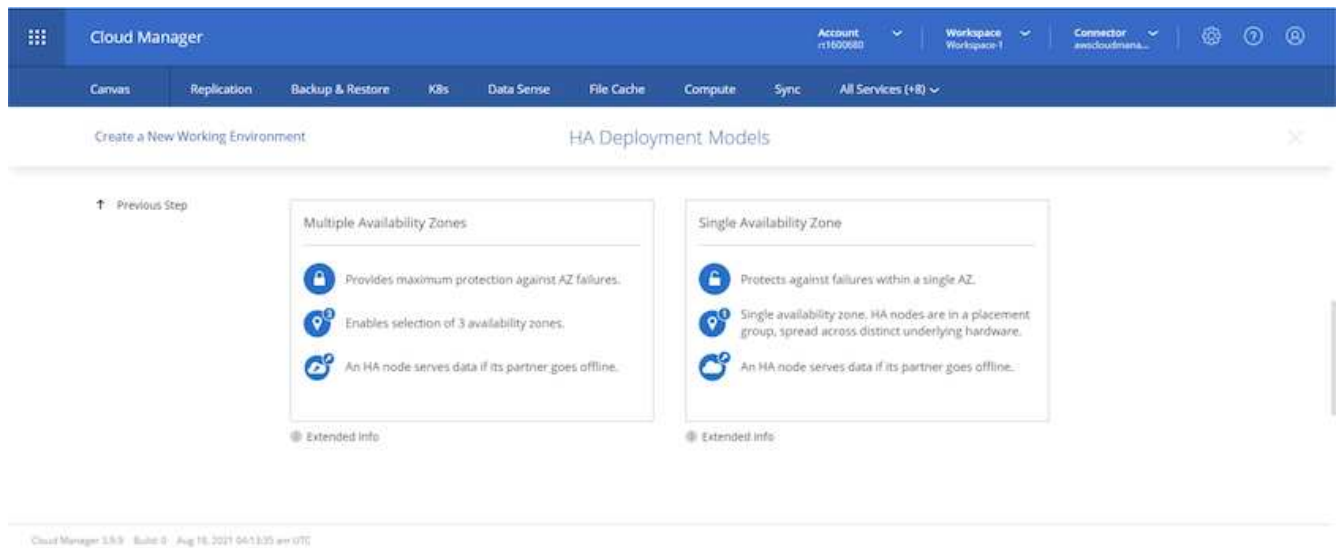
10. Saisissez les détails de l'environnement de travail, notamment :
- a. Nom du cluster
  - b. Mot de passe du cluster
  - c. Balises AWS (en option)

The screenshot shows the 'Details and Credentials' step in the 'Create a New Working Environment' wizard. The top navigation bar includes 'Cloud Manager', 'Account: r1600880', 'Workspace: Workspace 1', and 'Connector: awscloudmana...'. The main navigation menu lists 'Canvas', 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'File Cache', 'Compute', 'Sync', and 'All Services (+8)'. The wizard progress shows 'Previous Step' and 'Details and Credentials'. The 'Details' section contains a 'Working Environment Name (Cluster Name)' field with the value 'hybridawsco' and an 'Add Tags' button. The 'Credentials' section contains 'User Name' (admin), 'Password' (masked), and 'Confirm Password' (masked) fields. An 'Edit Credentials' button is also present. A 'Continue' button is at the bottom.

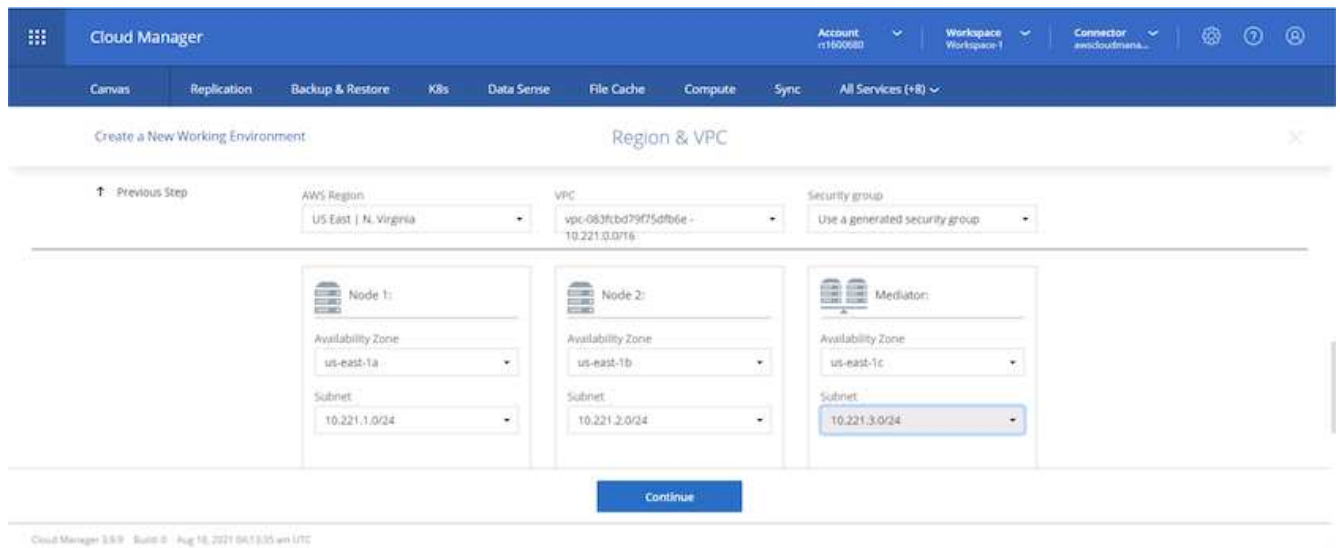
11. Choisissez les services supplémentaires que vous souhaitez déployer. Pour en savoir plus sur ces services, rendez-vous sur la "Page d'accueil de NetApp Cloud".

The screenshot shows the 'Services' step in the 'Create a New Working Environment' wizard. The top navigation bar and main navigation menu are the same as in the previous screenshot. The wizard progress shows 'Previous Step' and 'Services'. The 'Services' section lists three services with toggle switches and dropdown menus: 'Data Sense & Compliance', 'Backup to Cloud', and 'Monitoring'. All three services are currently enabled. A 'Continue' button is at the bottom.

12. Choisissez si vous souhaitez le déployer dans plusieurs zones de disponibilité (trois sous-réseaux, chacun dans une zone AZ différente) ou dans une seule zone de disponibilité. J'ai choisi plusieurs AZS.



13. Choisissez la région, le VPC et le groupe de sécurité dans lequel le cluster doit être déployé. Dans cette section, vous affectez également les zones de disponibilité par nœud (et médiateur) ainsi que les sous-réseaux qu'ils occupent.



14. Choisissez les méthodes de connexion pour les nœuds et le médiateur.

Cloud Manager

Account: rt1600680 | Workspace: Workspace 1 | Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8)

Create a New Working Environment | Connectivity & SSH Authentication

Previous Step

**Nodes**

SSH Authentication Method: Password

**Mediator**

Security Group: Use a generated security group

Key Pair Name: rt1600680

Internet Connection Method: Public IP address

Continue

Cloud Manager 5.8.9 | Build 2 | Aug 18, 2021 06:13:05 am UTC



Le médiateur requiert la communication avec les API AWS. Une adresse IP publique n'est pas requise tant que les API sont accessibles après le déploiement de l'instance EC2 médiateur.

1. Les adresses IP flottantes sont utilisées pour permettre l'accès aux différentes adresses IP utilisées par Cloud Volumes ONTAP, y compris la gestion du cluster et le traitement des adresses IP. Ces adresses doivent être déjà routables sur votre réseau et ajoutées aux tables d'acheminement dans votre environnement AWS. Ils sont nécessaires pour activer des adresses IP cohérentes pour une paire haute disponibilité lors du basculement. Vous trouverez plus d'informations sur les adresses IP flottantes dans le ["Documentation cloud NetApp"](#).

Cloud Manager

Account: rt1618549 | Workspace: Workspace 1 | Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8)

Create a New Working Environment | Floating IPs

Previous Step

Floating IP addresses are required for cluster and SVM access and for NFS and CIFS data access. These floating IPs can migrate between HA nodes if failures occur. To access the data from outside the VPC, you can set up an AWS transit gateway.

You must specify IP addresses that are outside of the CIDR blocks for all VPCs in the selected AWS region.

Floating IP address for cluster management: 10.222.0.200

Floating IP address 1 for NFS and CIFS data: 10.222.0.201

Floating IP address 2 for NFS and CIFS data: 10.222.0.202

Floating IP address for SVM management (Optional): Enter Floating IP Address

Continue

2. Sélectionnez les tables de routage auxquelles les adresses IP flottantes sont ajoutées. Ces tables de routage sont utilisées par les clients pour communiquer avec Cloud Volumes ONTAP.

Cloud Manager

Account: r1600680 Workspace: Workspace 1 Connector: #wicloudmana...

Canvas Replication Backup & Restore KMs Data Sense File Cache Compute Sync All Services (+8)

Create a New Working Environment Route Tables

Previous Step

Select the route tables that should include routes to the floating IP addresses. This enables client access to the Cloud Volumes ONTAP HA pair. If you leave a route table unselected, clients that are associated with the route table cannot access the HA pair.

Additional information ⓘ

<input checked="" type="checkbox"/>	Name	Main	ID	Associate with Subnet	Tags
<input checked="" type="checkbox"/>	private_rt_r1600680	No	rtb-08b4cb88f5c826a5	3 Subnets	1 Tags
<input checked="" type="checkbox"/>	public_rt_r1600680	Yes	rtb-0e46720d0da10c593	1 Subnets	1 Tags

2 Route Tables | The main route table is the default for the VPC

Continue

Cloud Manager 3.8.9 Build 0 Aug 18, 2021 06:13:35 am UTC

- Elles peuvent choisir d'activer le chiffrement géré par AWS ou le KMS AWS pour chiffrer la racine ONTAP, le démarrage et les disques de données.


Cloud Manager

Account: r1600680 Workspace: Workspace 1 Connector: #wicloudmana...

Canvas Replication Backup & Restore KMs Data Sense File Cache Compute Sync All Services (+8)

Create a New Working Environment Data Encryption

Previous Step

 AWS Managed Encryption

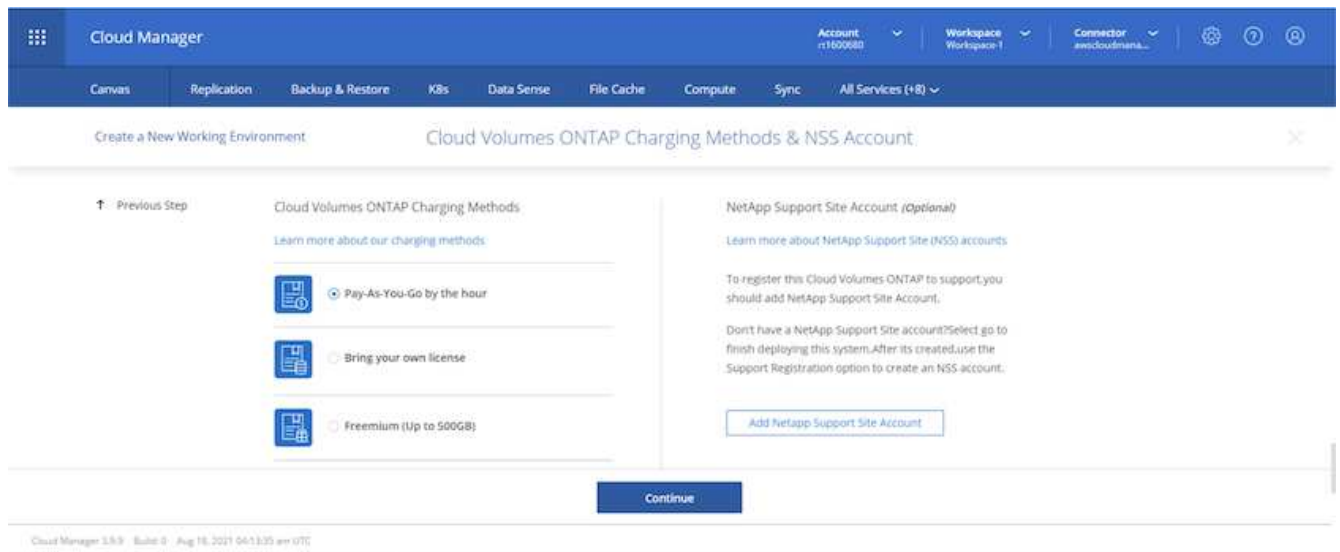
AWS is responsible for data encryption and decryption operations. Key management is handled by AWS key management services.

Default Master Key: aws/ebs

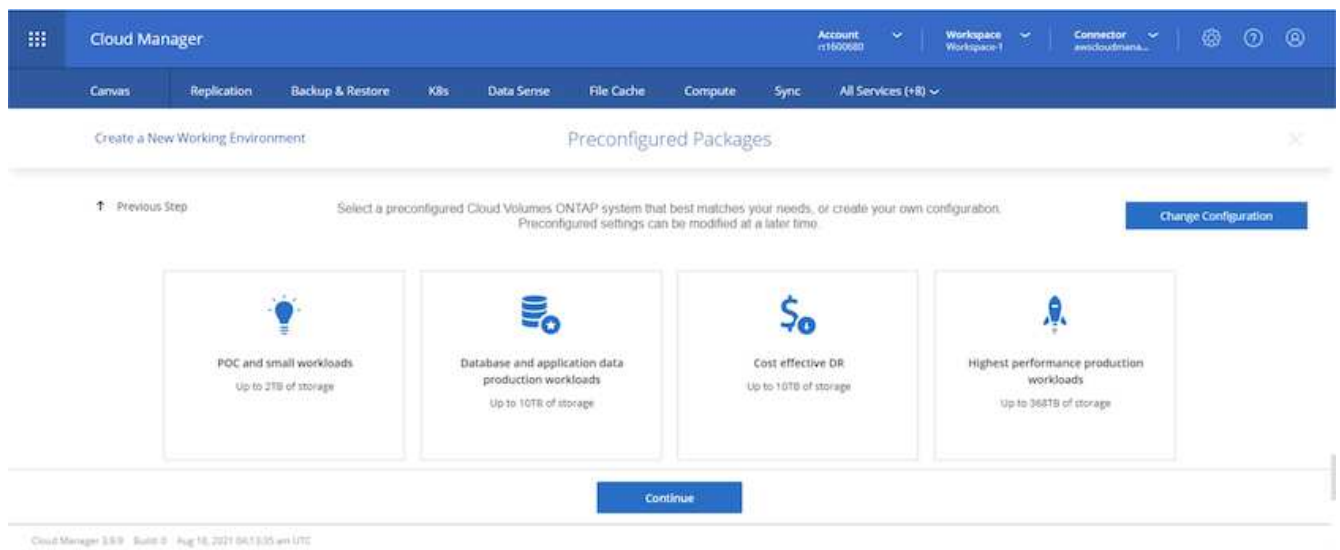
Continue

Cloud Manager 3.8.9 Build 0 Aug 18, 2021 06:13:35 am UTC

- Choisissez votre modèle de licence. Si vous ne savez pas quel choix choisir, contactez votre représentant NetApp.



5. Sélectionnez la configuration la mieux adaptée à votre utilisation. Cela est lié aux considérations de dimensionnement décrites dans la page des prérequis.



6. Créer un volume (facultatif) Cette opération n'est pas requise, car les étapes suivantes utilisent SnapMirror, qui crée les volumes pour nous.

Cloud Manager

Account: r1600880 | Workspace: Workspace 1 | Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8)

Create a New Working Environment | Create Volume

Previous Step

**Details & Protection**

Volume Name:  Size (GiB):  Volume size:

Snapshot Policy:

**Protocol**

NFS | CIFS | iSCSI

Access Control:

Custom export policy:

Advanced options:

Continue | Skip

Cloud Manager 3.9.9 | Build 9 | Aug 18, 2021 04:13:35 am UTC

7. Vérifiez les sélections effectuées et cochez les cases pour vérifier que Cloud Manager déploie des ressources dans votre environnement AWS. Une fois terminé, cliquez sur Go.

Cloud Manager

Account: r1600880 | Workspace: Workspace 1 | Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8)

Create a New Working Environment | Review & Approve

Previous Step: hybridawscvo | us-east-1 | HA | Show API request

☒ I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp. [More information >](#)

☒ I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements. [More information >](#)

Overview | Networking | Storage

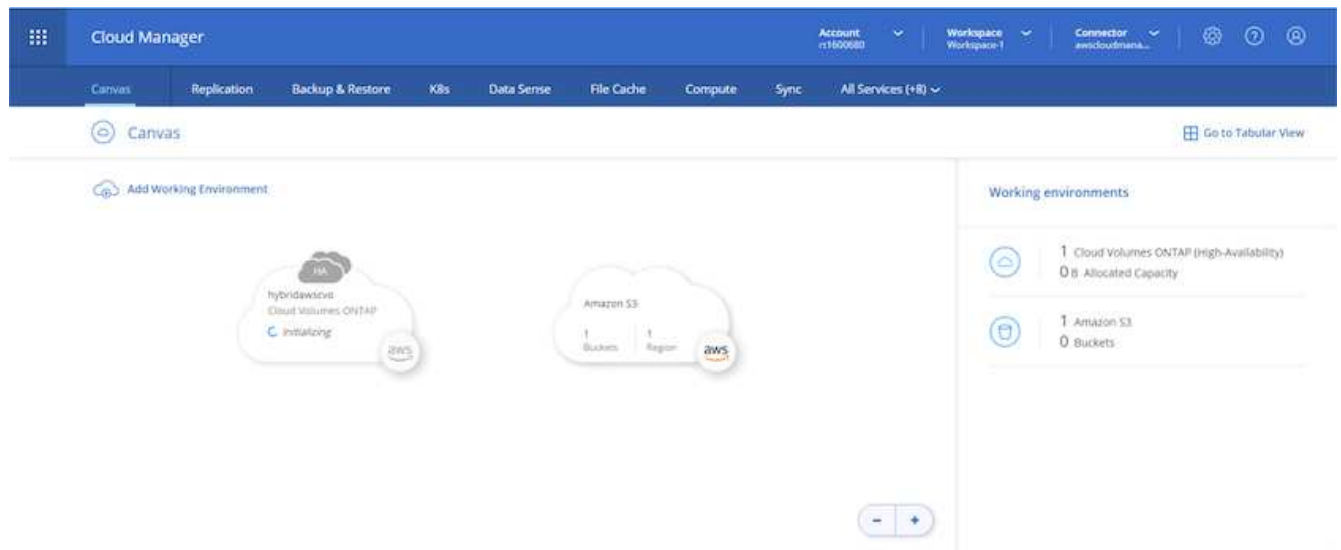
Storage System:	Cloud Volumes ONTAP HA	HA Deployment Model:	Multiple Availability Zones
License Type:	Cloud Volumes ONTAP Standard	Encryption:	AWS Managed
Capacity Limit:	10TB	Customer Master Key:	aws/ebc

Go

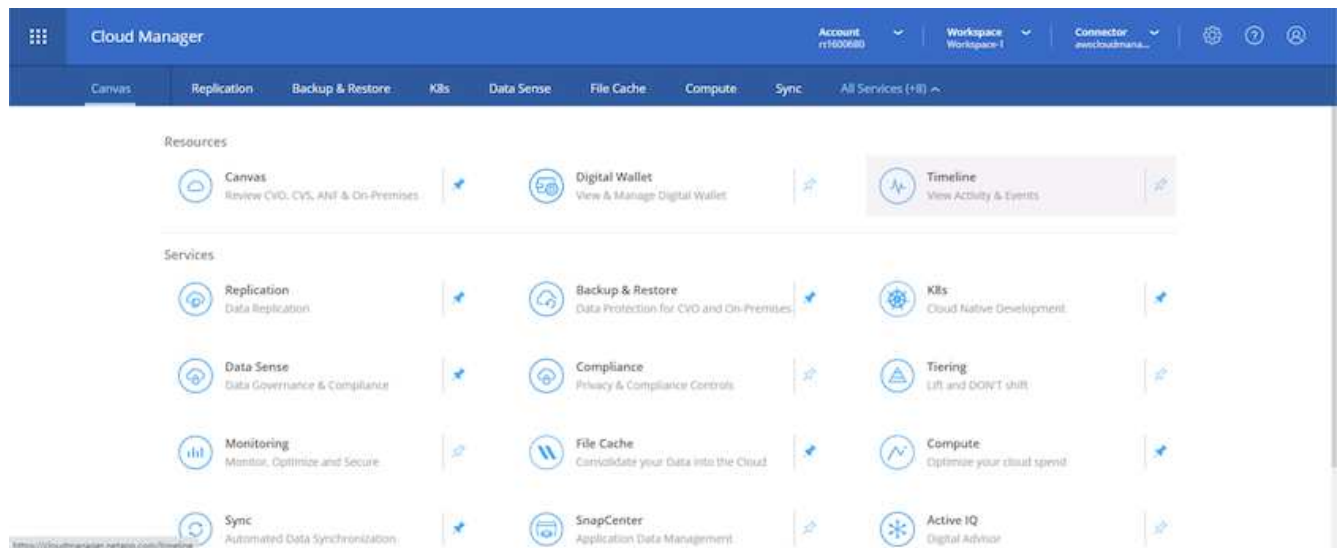
Cloud Manager 3.9.9 | Build 9 | Aug 18, 2021 04:13:35 am UTC

8. Le processus de déploiement commence maintenant par Cloud Volumes ONTAP. Cloud Manager utilise les API AWS et les piles de formation cloud pour déployer Cloud Volumes ONTAP. Il configure ensuite le système selon vos spécifications, vous offrant ainsi un système prêt à l'emploi qu'il est possible d'utiliser instantanément. La durée de ce processus varie en fonction des sélections effectuées.





9. Vous pouvez contrôler la progression en accédant à la chronologie.



10. La chronologie représente un audit de toutes les actions effectuées dans Cloud Manager. Vous pouvez afficher tous les appels d'API effectués par Cloud Manager lors de la configuration sur AWS et sur le cluster ONTAP. Elle peut également être utilisée efficacement pour résoudre tous les problèmes auxquels vous êtes confronté.

Cloud Manager

Account: r1600680 | Workspace: Workspace-1 | Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8)

Timeline

Filters: Time (1) | Service | Action | Agent (1) | Resource | User | Status | Reset

Time	Action	Service	Agent	Resource	User	Status
Aug 18 2021, 9:42:32 pm	Check Connectivity	Cloud Manager	awscloudman...	hybridawsco	Full Name	Success
Aug 18 2021, 9:42:00 pm	Create Aws Ha Working Environment	Cloud Manager	awscloudma...	hybridawsco	Full Name	Pending
Aug 18 2021, 10:09:39 pm	Describe Operation Status					Success
Aug 18 2021, 10:09:39 pm	Describe Operation Status					Success

11. Une fois le déploiement terminé, le cluster CVO s'affiche dans Canvas, pour lequel la capacité actuelle est de 1 GB. Le cluster ONTAP à l'état actuel est entièrement configuré pour offrir une véritable expérience prête à l'emploi.

Cloud Manager

Account: r1600680 | Workspace: Workspace-1 | Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8)

Canvas

Add Working Environment

Working environments

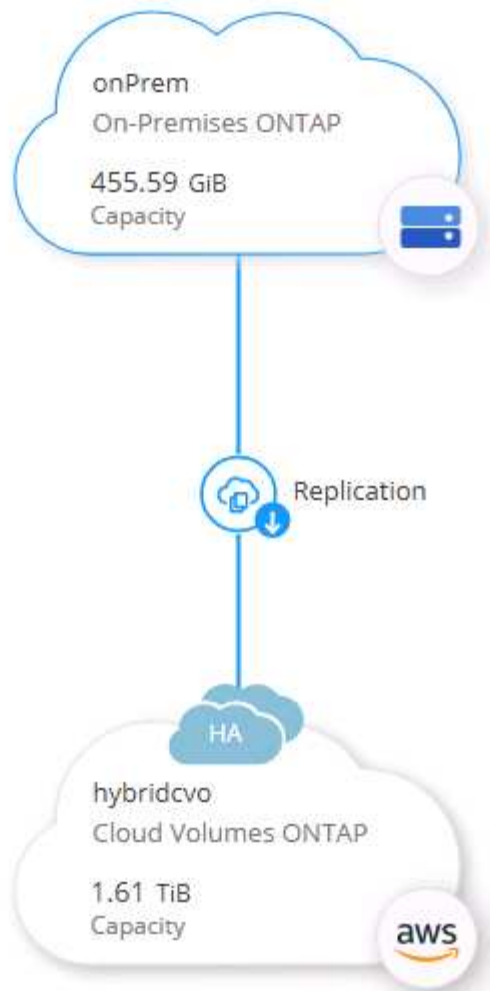
- 1 Cloud Volumes ONTAP (High-Availability) | 1 GB Allocated Capacity
- 1 Amazon S3 | 0 Buckets

### Configurez SnapMirror sur site vers le cloud

Dès lors que vous disposez d'un système ONTAP source et d'un système ONTAP de destination déployés, vous pouvez répliquer des volumes contenant des données de base de données dans le cloud.

Pour obtenir un guide sur les versions ONTAP compatibles avec SnapMirror, reportez-vous à la ["Matrice de compatibilité SnapMirror"](#).

1. Cliquez sur le système ONTAP source (sur site) et faites-le glisser vers la destination, sélectionnez réplication > Activer ou sélectionnez réplication > Menu > répliquer.



Sélectionnez Activer.

#### SERVICES

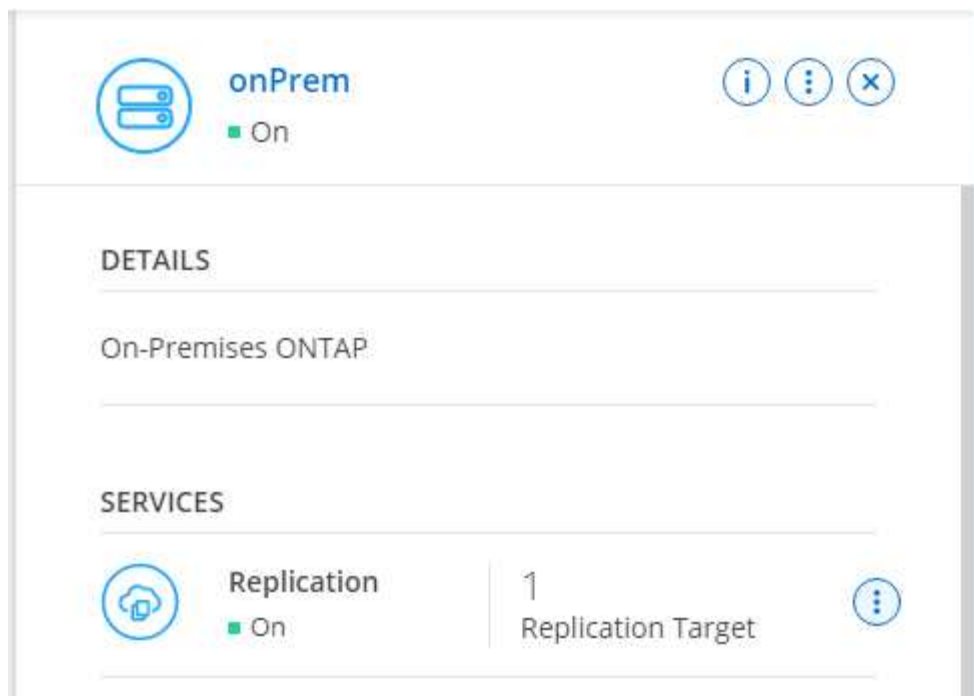


Replication  
■ Off

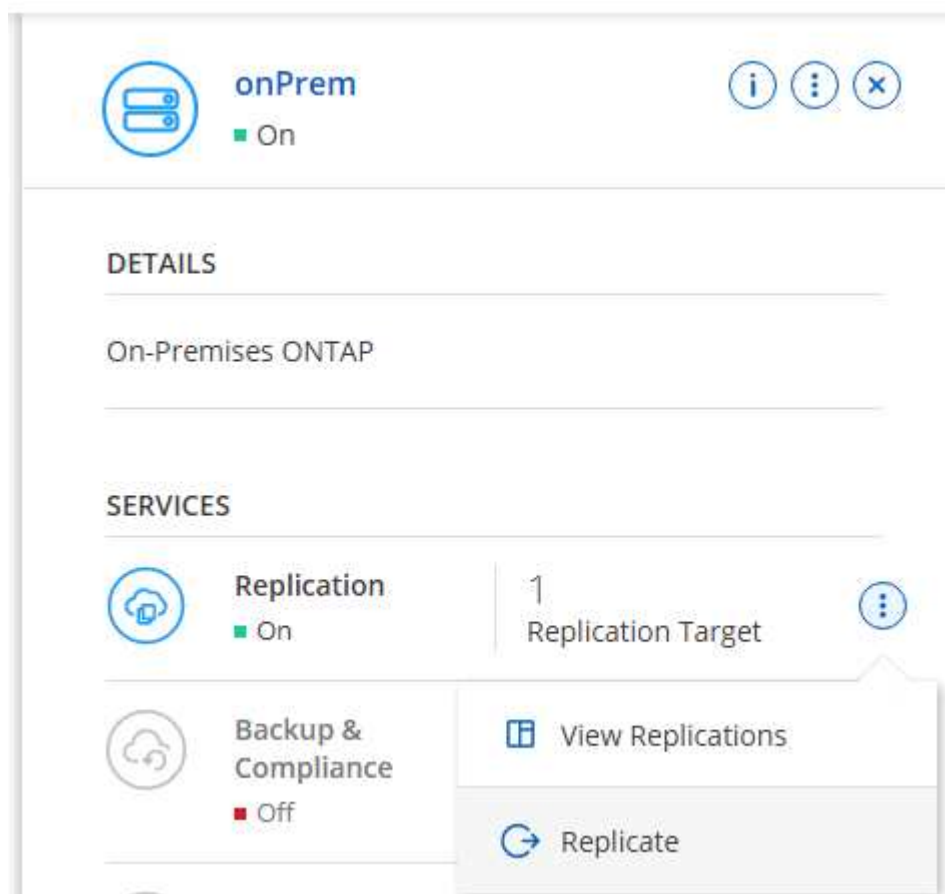
Enable



Ou Options.



Répliquer.



2. Si vous n'avez pas effectué de glisser-déposer, choisissez le cluster de destination vers lequel effectuer la réplique.

## Replicate Data

From: onPrem

To: select the Working Environment to which you want to replicate data

Replication Target

hybridcvo (Cloud Volumes ONTAP) ✓

Start Replication Wizard Cancel

3. Choisissez le volume que vous souhaitez répliquer. Nous avons répliqué les données et tous les volumes des journaux.

Replication Setup Source Volume Selection

Volume Name	Storage VM Name	Tiering Policy	Volume Type	Capacity	Disk Used	Status
rhel2_u03	svm_onPrem	None	RW	100 GB	7.29 GB	ONLINE
rhel2_u0309232119421203118	svm_onPrem	None	RW	100 GB	35.83 MB	ONLINE
sql1_data	svm_onPrem	None	RW	53.37 GB	45.09 GB	ONLINE
sql1_log	svm_onPrem	None	RW	21.35 GB	18.16 GB	ONLINE
sql1_snapctr	svm_onPrem	None	RW	24.87 GB	21.23 GB	ONLINE

Cloud Manager 3.9.10 Build: 2 Sep 12, 2021 06:47:41 am UTC


4. Choisissez le type de disque de destination et la règle de hiérarchisation. Pour la reprise après incident, nous recommandons l'utilisation d'un disque SSD comme type de disque et pour maintenir le Tiering des données. Le Tiering des données procède au Tiering des données en miroir dans un stockage objet à faible coût et vous permet d'économiser de l'argent sur des disques locaux. Lorsque vous rompez la relation ou que vous clonez le volume, les données utilisent le stockage local rapide.


Replication Setup Destination Disk Type and Tiering ×


---


[↑ Previous Step](#)

Destination Disk Type

  
General Purpose SSD

  
General Purpose SSD - Dynamic Performance

  
Throughput Optimized HDD

 S3 Tiering What are storage tiers?

☒ Enabled ☐ Disabled

Note: If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.

Continue

---

Cloud Manager 3.9.10 Build: 2 Sep 12, 2021 06:47:41 am UTC

5. Sélectionnez le nom du volume de destination : nous avons choisi `[source_volume_name]_dr`.

---

## Destination Volume Name

---

Destination Volume Name

`sql1_data_dr`

Destination Aggregate

Automatically select the best aggregate ▼

6. Sélectionnez la vitesse de transfert maximale pour la réplication. Cela vous permet d'économiser de la bande passante si vous disposez d'une connexion à faible bande passante au cloud, par exemple un VPN.

## Max Transfer Rate

You should limit the transfer rate. An unlimited rate might negatively impact the performance of other applications and it might impact your Internet performance.


- ☒ Limited to:  MB/s
- ☐ Unlimited (recommended for DR only machines)

7. Définissez la règle de réplication. Nous avons choisi un miroir, qui prend le jeu de données le plus récent et le réplique dans le volume de destination. Vous pouvez également choisir une politique différente en fonction de vos besoins.

## Replication Policy


Default Policies

Additional Policies

 Mirror

Typically used for disaster recovery

More info

 Mirror and Backup (1 month retention)

Configures disaster recovery and long-term retention of backups on the same destination volume

More info

8. Choisissez la planification du déclenchement de la réplication. NetApp recommande de définir une planification « journalière » pour le volume de données et une planification « horaire » pour les volumes de journaux, même si cela peut être modifié en fonction des besoins.

Replication Setup

Schedule

Previous Step

Select a replication schedule

One-time copy

No schedule

10min

Every hour  
Minutes: 0th, 10th, 20th, 3...

12-hourly

Every day  
Hours: 12 AM and 12 PM  
Minutes: 15th minute

5min

Every hour  
Minutes: 0th, 5th, 10th, 15t...

6-hourly

Every day  
Hours: 12 AM, 6 AM, 12 PM...  
Minutes: 15th minute

8hour

Every day  
Hours: 2 AM, 10 AM and 6 ...  
Minutes: 15th minute

daily

Every day  
Hours: 12 AM  
Minutes: 10th minute

hourly

Every hour  
Minutes: 5th minute

monthly

Every month  
Days: 2nd  
Hours: 12 AM  
Minutes: 20th minute

pg-15-minutely

Every hour

pg-6-hourly

Every day

pg-daily

Every day

pg-daily-set2

Every day

9. Vérifier les informations saisies, cliquer sur Go pour déclencher l'homologue du cluster et l'homologue SVM (si c'est votre première réplication entre les deux clusters), puis mettre en œuvre et initialiser la relation SnapMirror.

Replication Setup

Review & Approve

Previous Step

Review your selection and start the replication process

Source

onPrem

sql1\_data

Destination

hybridcvo

sql1\_data\_copy

☒ I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements.
 [More Information >](#)

Source Volume Allocated Size:	53.37 GB	Destination Thin Provisioning:	Yes
Source Volume Used Size:	45.09 GB	Destination Aggregate:	aggr1 (Automatically s...
Source Thin Provisioning:	Yes	Destination Storage VM:	svm_hybridcvo
Destination Volume Allocated Size:	53.37 GB	Max Transfer Rate:	100 MB/s
Destination Volume Disk Type:	General Purpose SSD (...)	SnapMirror Policy:	Mirror
Capacity Tiering:	S3	Replication Schedule:	daily

Go

10. Poursuivez ce processus pour les volumes de données et de journaux.
11. Pour vérifier toutes vos relations, accédez à l'onglet réplication dans Cloud Manager. Vous pouvez ici gérer vos relations et connaître leur statut.

Replication

7 Volume Relationships

153.32 GiB Replicated Capacity

0 Currently Transferring

7 Healthy

0 Failed

7 Volume Relationships

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	rhel2_u01 onPrem	rhel2_u01_dr hybridcvo	43 minutes 43 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:50 AI 19.73 MiB
✓	rhel2_u02 onPrem	rhel2_u02_dr hybridcvo	1 hour 37 minutes 59 seconds	idle	snapmirrored	Sep 30, 2021, 2:37:08 PM 239.78 MiB
✓	rhel2_u03 onPrem	rhel2_u03_dr hybridcvo	16 hours 1 minute 9 seconds	idle	snapmirrored	Sep 30, 2021, 4:07:14 PM 225.37 KiB
✓	sql1_data onPrem	sql1_data_dr hybridcvo	1 hour 6 minutes 50 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:28 AI 24.56 KiB

12. Une fois tous les volumes répliqués, vous êtes dans un état stable et prêt à passer aux flux de travail de reprise après incident et de développement/test.



### 3. Déployez l'instance de calcul EC2 pour les workloads de bases de données

AWS a préconfiguré des instances de calcul EC2 pour diverses charges de travail. Le choix du type d'instance détermine le nombre de cœurs de processeur, la capacité de mémoire, le type de stockage et la capacité, ainsi que la performance du réseau. Pour ces cas d'usage, à l'exception de la partition OS, le stockage principal permettant l'exécution de la charge de travail de la base de données est alloué à partir de CVO ou du moteur de stockage FSX ONTAP. Par conséquent, les principaux facteurs à prendre en compte sont le choix des cœurs de processeur, de la mémoire et du niveau de performance du réseau. Les types d'instances AWS EC2 classiques sont disponibles ici : ["Type d'instance EC2"](#).

#### Dimensionnement de l'instance de calcul

1. Sélectionnez le type d'instance approprié en fonction de la charge de travail requise. Les facteurs à prendre en compte incluent le nombre de transactions commerciales à prendre en charge, le nombre d'utilisateurs simultanés, le dimensionnement des jeux de données, etc.
2. Le déploiement d'instances EC2 peut être lancé via le tableau de bord EC2. Les procédures de déploiement précises dépassent le cadre de cette solution. Voir ["Amazon EC2"](#) pour plus d'informations.

#### Configuration de l'instance Linux pour le workload Oracle

Cette section contient des étapes de configuration supplémentaires après le déploiement d'une instance EC2 Linux.

1. Ajoutez une instance de secours Oracle au serveur DNS pour la résolution de nom dans le domaine de gestion SnapCenter.
2. Ajoutez un ID utilisateur de gestion Linux en tant que identifiants SnapCenter OS avec des autorisations sudo sans mot de passe. Activez l'ID avec l'authentification par mot de passe SSH sur l'instance EC2. (Par défaut, l'authentification par mot de passe SSH et le sudo sans mot de passe sont désactivés sur les instances EC2.)
3. Configurez l'installation Oracle pour qu'elle corresponde à l'installation Oracle sur site, par exemple les correctifs du système d'exploitation, les versions et correctifs d'Oracle, etc.
4. Les rôles d'automatisation de la base de données NetApp Ansible peuvent être utilisés pour configurer les instances EC2 pour le développement/test des bases de données et la reprise après incident. Le code d'automatisation peut être téléchargé sur le site GitHub public de NetApp : ["Déploiement automatisé Oracle 19c"](#). L'objectif est d'installer et de configurer une pile logicielle de base de données sur une instance EC2 afin qu'elle corresponde aux configurations du système d'exploitation et de la base de données sur site.

#### Configuration de l'instance Windows pour la charge de travail SQL Server

Cette section répertorie d'autres étapes de configuration après le déploiement initial d'une instance de Windows EC2.

1. Récupérez le mot de passe administrateur Windows pour vous connecter à une instance via RDP.
2. Désactivez le pare-feu Windows, rejoignez l'hôte dans le domaine SnapCenter de Windows et ajoutez l'instance au serveur DNS pour la résolution du nom.
3. Provisionnez un volume log SnapCenter pour stocker les fichiers log de SQL Server.
4. Configurez iSCSI sur l'hôte Windows pour monter le volume et formater le lecteur de disque.
5. Là encore, une grande partie des tâches précédentes peuvent être automatisées avec la solution d'automatisation NetApp pour SQL Server. Consultez le site GitHub public d'automatisation NetApp pour connaître les nouveaux rôles et solutions publiés : ["Automatisation NetApp"](#).

## 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 DÉLICTELLE (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.