



Déployez Google Cloud NetApp Volumes avec Oracle HA

NetApp database solutions

NetApp
June 25, 2026

Sommaire

Déployez Google Cloud NetApp Volumes avec Oracle HA	1
Provisionner des instances Google Compute Engine pour Google Cloud NetApp Volumes	1
Étape 1 : Créer les machines virtuelles	1
Étape 2 : Configurer le pare-feu VPC pour TCP 1521	2
Étape 3 : Configurer le nom d'hôte, le DNS et <code>/etc/hosts</code>	2
Étape 4 : Préparez le système d'exploitation uniquement sur les hôtes de la base de données	3
Étape 5 : Capturez le nom de l'initiateur iSCSI IQN	4
Et ensuite ?	5
Provisionnez le stockage iSCSI Google Cloud NetApp Volumes pour Oracle Database 26ai	5
Étape 1 : Créez des pools iSCSI GCNV	5
Étape 2 : Créez des groupes d'hôtes	6
Étape 3 : Créez des volumes iSCSI GCNV	6
Étape 4 : Configurer iSCSI et le multipath	7
Étape 5 : Partitionner les périphériques ASM	9
Étape 6 : Formatez et montez <code>/u01</code>	10
Et ensuite ?	11
Installez Oracle Grid Infrastructure et Oracle Database 26ai sur Google Cloud NetApp Volumes	11
Étape 1 : Installez l'infrastructure Grid sur chaque hôte de base de données	11
Étape 2 : Installez Oracle Database sur chaque hôte de base de données	14
Et ensuite ?	16
Créez la base de données principale Oracle sur Google Cloud NetApp Volumes	16
Et ensuite ?	18
Créez la base de données de secours Oracle avec l'amorçage de la couche de stockage Google Cloud NetApp Volumes	18
Étape 1 : Configurer les paramètres de l'écouteur et de Data Guard	19
Étape 2 : Préparez le fichier <code>pfile</code> de secours et <code>NOMOUNT</code>	20
Étape 3 : Initialiser le stockage de secours avec GCNV	21
Étape 4 : Enregistrez le serveur de secours auprès d'Oracle Restart	25
Et ensuite ?	27
Finalisez la base de données de secours pour Data Guard sur Google Cloud NetApp Volumes	27
Étape 1 : Créez des fichiers journaux de restauration en attente	28
Étape 2 : Activez le flashback et lancez la récupération	28
Étape 3 : Activer la réexpédition des journaux de reprise	29
Étape 4 : Vérifiez l'état de Data Guard	30
Et ensuite ?	31
Configurer Data Guard Broker et le basculement rapide automatique pour Oracle Database 26ai sur Google Cloud NetApp Volumes	31
Étape 1 : Activer Data Guard Broker	32
Étape 2 : Confirmez le flashback pour FSFO	33
Étape 3 : Configurer et activer FSFO	33
Étape 4 : Installer Instant Client sur Observer	34
Étape 5 : Exécutez Observer en tant que service <code>systemd</code>	35

Étape 6 : Tester FSFO	38
Et ensuite ?	39

Déployez Google Cloud NetApp Volumes avec Oracle HA

Provisionner des instances Google Compute Engine pour Google Cloud NetApp Volumes

Provisionnez des machines virtuelles Google Compute Engine pour héberger Oracle Database 26ai sur le stockage iSCSI Google Cloud NetApp Volumes. Cette procédure couvre la création des hôtes de base de données primaire et de secours et de la VM Fast-Start Failover Observer, la configuration des règles de pare-feu VPC pour Oracle Net, la configuration de la résolution des noms d'hôte, la préparation du système d'exploitation et la capture des noms d'initiateur iSCSI pour le provisionnement du stockage GCNV.

Étape 1 : Créer les machines virtuelles

Créez trois machines virtuelles Google Compute Engine dans différentes zones d'une même région pour isoler les pannes zonales. Utilisez la console Cloud, `gcloud`, Terraform ou votre flux de travail de provisionnement standard.

1. Créez les trois machines virtuelles avec les spécifications indiquées dans le tableau ci-dessous.

Privilégiez une région à faibles émissions de carbone pour le coût total de possession et la durabilité, lorsque cela répond aux besoins en matière de latence et de conformité (par exemple `us-west1` vs `us-central1`):

VM	Zone	Type de machine	disque de démarrage	Réseau	But
oracdb1	us-west1-a	n4-highmem-8(exemple) ou c4-standard-*	OL 10, Hyperdisk équilibré de 50 Go (OS only)	oracle-vpc / oracle-subnet, gVNIC	Base de données principale
oracdb2	us-west1-b	Identique au primaire	OL 10, Hyperdisk équilibré de 50 Go (OS only)	Même	Base de données de secours
oradg-obs	us-west1-c	e2-medium	OL 10, 20 Go Hyperdisk Balanced	Même	Observateur FSFO (Client instantané uniquement)

Utilisez le niveau réseau Premium lorsque la latence ou le débit sortant (>~200 Gio/mois) sont importants ; utilisez le niveau Standard pour un coût total de possession plus faible en développement/test.

2. Activez les fonctionnalités de la machine virtuelle protégée et vérifiez la configuration du disque de démarrage :

Activez **Secure Boot**, **vTPM** et **Integrity Monitoring** sur les trois machines virtuelles.

Le disque de démarrage contient uniquement le système d'exploitation. /u01 Les répertoires Grid/DB, l'environnement de transit et toutes les données ASM utilisent des volumes iSCSI GCNV (voir [Provisionner des volumes iSCSI GCNV](#))

N'attachez **pas** de disque de données GCE séparé pour /u01.

Étape 2 : Configurer le pare-feu VPC pour TCP 1521

Créez des règles de pare-feu VPC pour autoriser TCP/1521 entre les trois machines virtuelles pour le transport redo Oracle Net et la connectivité Observer. L'absence de ces règles interrompt la réplication Data Guard.

1. Créez une règle d'entrée de pare-feu VPC pour autoriser TCP/1521 entre les trois adresses IP internes des machines virtuelles. Utilisez des règles de pare-feu VPC ou des politiques de pare-feu avec la même allowlist :

Console Cloud : Réseau VPC → Pare-feu → Créer une règle `allow-oracle-net-dbhosts` sur `oracle-vpc` — Entrée, Autoriser, sources = trois /32 IP, TCP 1521. Dupliquer la sortie si nécessaire.

2. Validez la connectivité depuis chaque machine virtuelle pour vérifier que les règles du pare-feu sont en place :

```
sudo dnf install -y nmap-ncat

for tgt in <oracdb1-ip> <oracdb2-ip> <oradg-obs-ip>; do
  nc -zv -w 5 "$tgt" 22
  nc -zv -w 5 "$tgt" 1521
done
```

Port	Attendu	Signification
22	Connecté	Le chemin SSH fonctionne
1521	Connexion refusée	Pare-feu ouvert ; l'écouteur de grille démarre pendant Étape 1 : Installez Oracle Grid Infrastructure (Oracle Restart) sur chaque hôte de base de données
Soit	Délai d'attente	Corriger le pare-feu ou le routage

Exécutez la commande depuis les trois machines virtuelles vers chaque adresse IP homologue.

Étape 3 : Configurer le nom d'hôte, le DNS et `/etc/hosts`

Configurez la résolution de nom d'hôte et DNS sur les trois machines virtuelles afin que la résolution de noms directe et inverse fonctionne pour Oracle Net, le Data Guard Broker et l'Observer.

1. Définissez le nom d'hôte et ajoutez `/etc/hosts` des entrées sur les trois hôtes. Remplacez les adresses IP internes GCE (visibles dans la liste **Compute Engine** → **Instances de VM**, colonne *Adresse IP interne*) :

```
# Run on each VM, substituting the local short name (oracdb1, oracdb2,
oradg-obs)
sudo hostnamectl set-hostname <this-host>.example.internal

# Run on every VM (same content)
sudo tee -a /etc/hosts >/dev/null <<EOF

# Oracle DG peers + FSFO Observer
<oracdb1-ip>    oracdb1.example.internal    oracdb1
<oracdb2-ip>    oracdb2.example.internal    oracdb2
<oradg-obs-ip>  oradg-obs.example.internal    oradg-obs
EOF
```

2. Validez la résolution de noms à partir de chaque hôte :

```
ping -c 1 oracdb1 && ping -c 1 oracdb2 && ping -c 1 oradg-obs
```

Étape 4 : Préparez le système d'exploitation uniquement sur les hôtes de la base de données

Préparez le système d'exploitation sur `oracdb1` et `oracdb2` pour Oracle Database 26ai en installant le package de préinstallation, en créant les utilisateurs et les groupes, en installant les packages iSCSI et multipath, et en configurant l'initiateur iSCSI. La configuration de l'observateur est abordée dans [Étape 4 : Installez Oracle Instant Client sur l'hôte Observer](#).



Prérequis : HTTPS sortant vers `yum.oracle.com` (Cloud NAT ou miroir interne sur des sous-réseaux privés).

1. Installez le package de préinstallation Oracle Database, créez l'`grid`utilisateur et les groupes ASM, puis ajoutez l'`oracle`utilisateur aux groupes ASM :

```
# Oracle 26ai preinstall (package name varies by repo)
sudo dnf install -y oracle-ai-database-preinstall-26ai \
|| sudo dnf install -y oracle-database-preinstall-26ai \
|| sudo dnf install -y oracle-database-preinstall-23ai

# grid user + asm groups
sudo groupadd -g 54327 asmadmin; sudo groupadd -g 54328 asmdba; sudo
groupadd -g 54329 asmoper
sudo useradd -u 54322 -g oinstall -G dba,oper,asmadmin,asmdba,asmoper
grid
sudo passwd -l grid; sudo passwd -l oracle
sudo usermod -a -G asmdba,asmadmin oracle
```

2. Installez les packages iSCSI, multipath et JDK, puis vérifiez le THP et la synchronisation de l'heure :

```
sudo dnf install -y iscsi-initiator-utils device-mapper-multipath
sg3_utils \
    java-21-openjdk-headless libxcrypt-compat

# THP and time
cat /sys/kernel/mm/transparent_hugepage/enabled # expect [never]
timedatectl
chronyc tracking
```

3. Configurez les paramètres SELinux, du pare-feu et de l'initiateur iSCSI, puis redémarrez :



Configuration de sécurité (OL 10) : Les commandes ci-dessous configurent SELinux en mode permissif et le désactivent firewalld. Il s'agit d'une configuration minimale pour un environnement de laboratoire. Pour une configuration SELinux et pare-feu renforcée, consultez le référentiel de sécurité de votre organisation.

```
sudo setenforce 0
sudo sed -i 's/^SELINUX=.*SELINUX=permissive/' /etc/selinux/config
sudo systemctl disable --now firewalld

sudo cp -n /etc/iscsi/iscsid.conf /etc/iscsi/iscsid.conf.orig
sudo sed -i '/^[#[:space:]]*node\.session\.timeo\.replacement_timeout/d'
/etc/iscsi/iscsid.conf
echo "node.session.timeo.replacement_timeout = 120" | sudo tee -a
/etc/iscsi/iscsid.conf
sudo systemctl enable --now iscsid

sudo reboot
```

Étape 5 : Capturez le nom de l'initiateur iSCSI IQN

Après le redémarrage, récupérez le nom de l'initiateur iSCSI (IQN) de chaque hôte de base de données. Vous utiliserez ces IQN pour créer les groupes d'hôtes GCNV dans [Étape 2 : Créer les groupes hôtes](#).

1. Capturez l'IQN à partir de `oracdb1` et enregistrez-le :

```
sudo cat /etc/iscsi/initiatorname.iscsi
# InitiatorName=iqn.1994-05.com.redhat:abc123def456
```

2. Répétez l'opération sur `oracdb2` et notez son IQN. Utilisez un groupe d'hôtes par hôte afin que le redémarrage ou la régénération de l'IQN d'un hôte n'affecte pas la visibilité du volume iSCSI GCNV d'un autre hôte.



VM clonées : Si les deux hôtes partagent le même IQN, régénérez sur `oracdb2` (arrêtez `iscsi`, effacez `/var/lib/iscsi/nodes/*`, nouveau `InitiatorName` dans `/etc/iscsi/initiatorname.iscsi`, redémarrez `iscsid`).

Et ensuite ?

Pour fournir un stockage partagé pour les binaires Oracle et les groupes de disques ASM, accédez à [Provisionner des pools iSCSI, des groupes d'hôtes et des volumes Google Cloud NetApp Volumes](#).

Provisionnez le stockage iSCSI Google Cloud NetApp Volumes pour Oracle Database 26ai

Provisionnez le stockage bloc iSCSI Google Cloud NetApp Volumes pour la haute disponibilité d'Oracle Database 26ai sur Google Compute Engine. Cette procédure couvre la création de pools de stockage GCNV Flex Unified, la définition des groupes d'hôtes, la création de volumes iSCSI pour chaque hôte de base de données, la configuration d'iSCSI et de multipath sous Linux, le partitionnement des périphériques ASM, et le montage du `/u01` système de fichiers.

Étape 1 : Créez des pools iSCSI GCNV

Créez deux pools de stockage Flex Unified, un dans chaque zone de base de données, afin de fournir des volumes iSCSI aux hôtes principal et de secours. Chaque hôte de base de données utilise les volumes du pool de sa zone locale.

1. Créez deux pools de stockage à l'aide de la Cloud Console. Utilisez les spécifications du tableau ci-dessous et répétez le processus de création pour chaque zone :

Nom du pool	Zone	Utilisé par
<code>oracle-pool-a</code>	<code>us-west1-a</code>	<code>oracdb1</code> (primaire)
<code>oracle-pool-b</code>	<code>us-west1-b</code>	<code>oracdb2</code> (attendre)

NetApp Volumes → **Pools de stockage** → **Créer** pour chaque pool :

- **Niveau de service** : Flex (et non Premium)
 - **Type** : Unifié
 - **Zone** : correspond à la zone de la machine virtuelle de la base de données (`us-west1-a/ us-west1-b`)
 - **Avis important** : connecté à `oracle-vpc`
 - **Capacité** : dimensionnée en fonction de la charge de travail ; utiliser un débit/IOPS provisionné personnalisé lorsque le redo, la sauvegarde ou la restauration dépasse la marge par défaut (jusqu'à 5120 Mio/s ou 160K IOPS par pool, dans les limites du produit)
2. Attendez que les deux pools atteignent le statut `READY` avant de continuer. Adaptez la taille des pools à l'encombrement de votre base de données (les tailles dans [Étape 3 : Créer les volumes iSCSI GCNV](#) sont des exemples) :



Mode par défaut (ce guide) : Les pools Flex Unified utilisent le mode par défaut (`--mode=default`). Créez des pools et des volumes iSCSI avec Cloud Console ou `gcloud netapp`. La réplication de volumes, les snapshots et les clones utilisent les API Google Cloud ([Étape 3 : Initialisation de la veille GCNV](#)).

Étape 2 : Créez des groupes d'hôtes

Créez un groupe d'hôtes par hôte de base de données afin que chaque machine virtuelle ne voie que ses propres volumes. Les hôtes principal et de secours ne doivent pas partager les volumes iSCSI GCNV afin de maintenir un stockage indépendant.

1. Créez le groupe d'hôtes pour `oracdb1` à l'aide de la Cloud Console :

NetApp Volumes → **Groupes d'hôtes** → **Créer**

- **Nom:** `oracdb1-hg`
- **Région:** `us-west1`
- **Type :** Initiateur iSCSI
- **Type de système d'exploitation :** Linux
- **Hôtes :** collez l'IQN à partir de `oracdb1` (la valeur de `/etc/iscsi/initiatorname.iscsi`)
- **Description :** « Hôte principal Oracle `oracdb1` »
- **Créer**

2. Répétez l'opération pour `oracdb2` avec le nom `oracdb2-hg` et l'IQN de `oracdb2`. L'hôte Observer ne nécessite aucune ressource GCNV.

Étape 3 : Créez des volumes iSCSI GCNV

Créez cinq volumes iSCSI GCNV pour chaque hôte de base de données : un pour `/u01` et quatre pour les périphériques de support ASM. Les volumes de chaque hôte doivent être créés dans le pool de stockage de la zone locale correspondante, avec le groupe d'hôtes associé.

1. Créez les cinq volumes pour `oracdb1` dans `oracle-pool-a` avec le groupe d'hôtes `oracdb1-hg`. Utilisez les spécifications du tableau ci-dessous :

Volume iSCSI GCNV	Taille	Utiliser	Alias multipath
<code>ora_<host>_u01</code>	100 Gio	<code>`/u01`</code> Volume iSCSI GCNV — Répertoires Grid/Oracle, zone de transit	<code>/dev/mapper/ora_<host>_u01</code>
<code>ora_<host>_data_01</code>	50 Gio	ASM +DATA	<code>/dev/mapper/ora_<host>_data_01</code>
<code>ora_<host>_data_02</code>	50 Gio	ASM +DATA (rayé)	<code>/dev/mapper/ora_<host>_data_02</code>
<code>ora_<host>_arch_01</code>	100 Gio	ASM +RECO	<code>/dev/mapper/ora_<host>_arch_01</code>

Volume iSCSI GCNV	Taille	Utiliser	Alias multipath
ora_<host>_fra_01	100 Gio	ASM +FRA	/dev/mapper/ora_<host>_fra_01

Noms de volumes : lettres, chiffres, traits de soulignement uniquement (pas de traits d'union).



Configuration minimale (validation uniquement) : Deux LUN par hôte (*_data, *_reco avec arch_01p1→+RECO et arch_01p2→+FRA est acceptable pour le laboratoire ; la production utilise cinq volumes par [Étape 3 : Créer les volumes iSCSI GCNV](#).

2. Créez les cinq volumes pour oracdb2 dans oracle-pool-b avec le groupe d'hôtes oracdb2-hg en utilisant les mêmes spécifications. Pour chaque pool, utilisez **NetApp Volumes** → **Volumes** → **Create** — iSCSI, pool et groupe d'hôtes appropriés, Linux. Notez les informations suivantes :
 - Adresses IP des portails iSCSI → <ISCSI_PORTAL_1>, <ISCSI_PORTAL_2> (portails du pool principal sur oracdb1; portails du pool de secours sur oracdb2 — ils peuvent différer)
 - Numéro de série du volume depuis la console cloud — à utiliser avec le WWID découvert par l'hôte dans [Étape 4 : Configurer iSCSI Linux et le multipath pour les volumes iSCSI GCNV](#)

Étape 4 : Configurer iSCSI et le multipath

Configurez iSCSI et device-mapper-multipath sur chaque hôte de base de données pour accéder aux volumes GCNV via les deux adresses IP du portail de stockage. Exécutez ces étapes sur oracdb1 en utilisant les adresses IP du portail du pool principal, puis répétez-les sur oracdb2 en utilisant celles du portail du pool de secours. Si la sortie de l'hôte est restreinte, autorisez TCP/3260 de chaque machine virtuelle de base de données vers ses adresses IP de portail iSCSI GCNV (en plus de TCP/1521 entre machines virtuelles [Étape 2 : Pare-feu VPC — autoriser la liste blanche TCP/1521 sur les trois zones](#)).

1. Découvrez les cibles, connectez-vous et persistez le démarrage du nœud :

```
sudo iscsiadm --mode discovery --op update --type sendtargets --portal
<ISCSI_PORTAL_1>
sudo iscsiadm --mode discovery --op update --type sendtargets --portal
<ISCSI_PORTAL_2>
sudo iscsiadm --mode node --op update --name node.startup --value
automatic
sudo iscsiadm --mode node -l all
sudo systemctl enable --now iscsid iscsi multipathd
sudo iscsiadm --mode session          # expect 10 sessions (5 GCNV iSCSI
volumes × 2 portals)
sudo lsblk -o NAME,SIZE,WWN,VENDOR,MODEL
```

Après le redémarrage, vérifiez à nouveau avant de démarrer Oracle :

```
sudo iscsiadm --mode session
sudo multipath -ll
```

2. Configurer device-mapper-multipath avec des valeurs par défaut et des règles de liste noire :

```
sudo tee /etc/multipath.conf >/dev/null <<'EOF'  
defaults {  
    find_multipaths    yes  
    user_friendly_names yes  
}  
blacklist {  
    devnode "^(ram|raw|loop|fd|md|dm-|sr|scd|st) [0-9]*"  
    devnode "^hd[a-z]"  
    devnode "^cciss.*"  
}  
EOF  
  
sudo systemctl enable --now multipathd  
sudo multipath -ll
```

3. Ajoutez les alias WWID détectés par l'hôte /etc/multipath.conf (ne devinez pas — multipath.conf ne développe **pas** les variables du shell). Découvrez les WWID :

```
sudo multipath -ll  
for dev in /dev/sd*; do  
    [ -b "$dev" ] || continue  
    printf '%s: ' "$dev"  
    sudo /usr/lib/udev/scsi_id --whitelisted --device="$dev" 2>/dev/null  
    || true  
    echo  
done
```

Ajoutez des alias concrets pour cet hôte à /etc/multipath.conf, puis `sudo systemctl restart multipathd`.

Sur `oracdb1`, ajoutez :

```

multipaths {
    multipath { wwid <host-discovered-wwid-for-u01>      alias
ora_oracdb1_u01      }
    multipath { wwid <host-discovered-wwid-for-data-01>  alias
ora_oracdb1_data_01 }
    multipath { wwid <host-discovered-wwid-for-data-02>  alias
ora_oracdb1_data_02 }
    multipath { wwid <host-discovered-wwid-for-arch-01>  alias
ora_oracdb1_arch_01 }
    multipath { wwid <host-discovered-wwid-for-fra-01>  alias
ora_oracdb1_fra_01  }
}

```

Sur oracdb2, utilisez le même modèle avec ora_oracdb2_* des alias, puis :

```

sudo systemctl restart multipathd
ls -l /dev/mapper/ora_$(hostname -s)_*

```

Étape 5 : Partitionner les périphériques ASM

Partitionnez les quatre périphériques de stockage ASM (à l'exclusion u01) avec une partition GPT chacun pour la consommation par ASM, puis configurez les règles udev pour l'appartenance au groupe grid. Exécutez ces étapes sur chaque hôte de base de données.

1. Partitionnez les quatre périphériques de stockage ASM avec GPT et vérifiez les partitions :

```

HOST=$(hostname -s)      # oracdb1 on the primary, oracdb2 on the
standby
for dev in /dev/mapper/ora_${HOST}_data_01 \
           /dev/mapper/ora_${HOST}_data_02 \
           /dev/mapper/ora_${HOST}_arch_01 \
           /dev/mapper/ora_${HOST}_fra_01; do
    sudo parted -s "$dev" mklabel gpt
    sudo parted -s "$dev" mkpart primary 0% 100%
done
sudo partprobe
sudo systemctl reload multipathd
ls /dev/mapper/ora_${HOST}_*p1      # expect 4 partitions

```

2. Configurez les règles udev pour attribuer la propriété grid et déclencher les modifications :

```

HOST=$(hostname -s)
sudo tee /etc/udev/rules.d/99-oracle-asm.rules >/dev/null <<'EOF'
KERNEL=="dm-*", ENV{DM_UUID}=="part?-mpath-*",
ENV{DM_NAME}=="ora_oracdb*_*p?", \
    OWNER="grid", GROUP="asmadmin", MODE="0660"
EOF

sudo udevadm control --reload-rules
for part in /dev/mapper/ora_${HOST}_*p1; do
    dm=$(readlink -f "$part" | xargs basename)
    sudo udevadm trigger --action=change --name-match="/dev/${dm}"
done
sudo udevadm settle
ls -lL /dev/mapper/ora_${HOST}_*p1      # grid:asmadmin 0660

```

Étape 6 : Formatez et montez /u01

Formatez le ora_<host>_u01`volume GCNV avec XFS et montez-le de manière permanente en utilisant l'UUID dans `/etc/fstab. Le /u01 système de fichiers contient Grid home, Oracle home et les fichiers de staging.

1. Formatez le périphérique multipath avec XFS et capturez son UUID :

```

HOST=$(hostname -s)
U01_DEV=/dev/mapper/ora_${HOST}_u01
ls -l "$U01_DEV"

sudo mkfs.xfs -f "$U01_DEV"
U01_UUID=$(sudo blkid -s UUID -o value "$U01_DEV")

```

2. Ajoutez l'entrée de montage basée sur l'UUID à /etc/fstab et montez le système de fichiers :

```

sudo mkdir -p /u01
echo "UUID=${U01_UUID} /u01 xfs defaults,_netdev,nofail,x-
systemd.requires=iscsi.service,x-systemd.requires=multipathd.service,x-
systemd.after=iscsi.service,x-systemd.after=multipathd.service 0 0" |
sudo tee -a /etc/fstab
sudo mount -a

```

3. Créez la structure de répertoires avec la propriété appropriée pour les logiciels Grid et Oracle :

```
sudo mkdir -p /u01/app/oraInventory /u01/app/26ai/grid /u01/app/grid \  
/u01/app/oracle/product/26ai/db_1 /u01/stage  
sudo chown -R grid:oinstall /u01/app/oraInventory /u01/app/26ai  
/u01/app/grid  
sudo chown -R oracle:oinstall /u01/app/oracle /u01/stage  
sudo chmod -R 775 /u01/app /u01/stage
```

Redémarrez une fois et confirmez /u01 les montages avant [installation du logiciel Oracle](#).

Et ensuite ?

Pour installer les binaires Oracle Grid Infrastructure et Database sur les hôtes préparés, allez à [Installez le logiciel Oracle Grid Infrastructure et Oracle Database](#) sur les deux hôtes.

Installez Oracle Grid Infrastructure et Oracle Database 26ai sur Google Cloud NetApp Volumes

Installez Oracle Grid Infrastructure avec Oracle Restart et ASM sur le stockage iSCSI NetApp Volumes de Google Cloud pour chaque hôte de base de données, puis installez le logiciel Oracle Database 26ai. Cette procédure comprend la mise en place des GoldImages Oracle, l'exécution d'installations silencieuses à l'aide de fichiers de réponses, la création de groupes de disques ASM sur les volumes GCNV, ainsi que la préparation des hôtes principal et de secours avec un logiciel Oracle identique avant la création de la base de données.

Étape 1 : Installez l'infrastructure Grid sur chaque hôte de base de données

Installez l'infrastructure Oracle Grid GoldImage sur chaque hôte de base de données pour activer Oracle Restart et ASM. Les deux hôtes nécessitent chacun leur propre répertoire Grid, instance ASM et groupes de disques ; Data Guard réplique les données via Oracle Net, et non via un stockage partagé. Effectuez toutes les étapes sur `oracdb1` avant de les répéter sur `oracdb2`.

1. Placez les binaires Oracle GoldImages, Release Update et OPatch dans /u01/stage :

```
sudo chown oracle:oinstall /u01/stage && sudo chmod 775 /u01/stage  
# Upload GoldImages, RU, OPatch to /u01/stage.
```

2. Décompressez le Grid GoldImage à l'emplacement du Grid home cible. La version 26ai GoldImage s'installe en la décompressant directement dans le répertoire cible :

```

sudo -u grid bash -c '
cd /u01/app/26ai/grid
unzip -q /u01/stage/LINUX.X64_<RELEASE>_grid_home.zip
'
sudo chown -R grid:oinstall /u01/app/26ai/grid

```

Si la grille GoldImage est plus ancienne que l'unité de mise à jour cible, appliquez le correctif au répertoire d'installation de la grille lors de la configuration en utilisant le flux `gridSetup.sh -applyRU`, ou utilisez une GoldImage avec l'unité de mise à jour intégrée. Veillez à ce que les répertoires d'installation de la grille et de la base de données conservent le même niveau de correctif prévu.

3. Créez le `gridSetup`` fichier de réponses ``/tmp/grid.rsp` sur chaque hôte. Remplacez le nom d'hôte et utilisez des mots de passe robustes :

```

HOST=$(hostname -s)

sudo -u grid bash -c "cat > /tmp/grid.rsp <<RSP
oracle.install.responseFileVersion=/oracle/install/rspfmt_crsinstall_res
ponse_schema_v23.0.0
INVENTORY_LOCATION=/u01/app/oraInventory
installOption=HA_CONFIG
ORACLE_BASE=/u01/app/grid
clusterUsage=GENERAL_PURPOSE
OSDBA=asmdba
OSOPER=asmoper
OSASM=asmadmin
storageOption=FLEX_ASM_STORAGE
sysasmPassword=WelcomeOracle1!
asmsnmpPassword=WelcomeOracle1!
diskGroupName=DATA
redundancy=EXTERNAL
auSize=4
diskString=/dev/mapper/ora_${HOST}_*p*
diskList=/dev/mapper/ora_${HOST}_data_01p1,/dev/mapper/ora_${HOST}_data_
02p1
managementOption=NONE
RSP"
sudo -u grid chmod 600 /tmp/grid.rsp

```

4. Exécutez `gridSetup.sh` en mode silencieux pour copier les fichiers binaires et préparer la configuration. Attendez-vous à `Successfully Setup Software with warning(s)` . et au code de sortie 6 (avertissements) ou 0 :

```
sudo -u grid bash -c '  
export ORACLE_HOME=/u01/app/26ai/grid  
export ORACLE_BASE=/u01/app/grid  
cd /u01/app/26ai/grid  
./gridSetup.sh -silent -responseFile /tmp/grid.rsp -ignorePrereqFailure  
'
```

5. Exécutez `orainstRoot.sh` et `root.sh` en tant que `root`. Le script `root.sh` crée les wrappers `crsctl`, `srvctl` et `asmcmd` et lance OHAS :

```
sudo /u01/app/oraInventory/orainstRoot.sh  
sudo /u01/app/26ai/grid/root.sh
```

6. Exécutez `gridSetup.sh -executeConfigTools` pour lancer les assistants de configuration (NETCA, ASMCA, CVU) sur [le fichier de réponse](#). Cela crée l'instance ASM et le groupe de disques +DATA. Attendez-vous à Successfully Configured Software. après NETCA / ASMCA / CVU :

```
sudo -u grid bash -c '  
export ORACLE_HOME=/u01/app/26ai/grid  
export ORACLE_BASE=/u01/app/grid  
cd /u01/app/26ai/grid  
./gridSetup.sh -silent -executeConfigTools -responseFile /tmp/grid.rsp  
'
```

7. Créez les groupes de disques +RECO et +FRA à l'aide de `asmca`. L'installation en une seule étape crée uniquement +DATA :

```

HOST=$(hostname -s)

sudo -u grid bash -c "
export ORACLE_HOME=/u01/app/26ai/grid
export ORACLE_SID=+ASM

\${ORACLE_HOME}/bin/asmca -silent -createDiskGroup \
  -diskGroupName RECO \
  -disk /dev/mapper/ora_${HOST}_arch_01p1 \
  -redundancy EXTERNAL -au_size 4

\${ORACLE_HOME}/bin/asmca -silent -createDiskGroup \
  -diskGroupName FRA \
  -disk /dev/mapper/ora_${HOST}_fra_01p1 \
  -redundancy EXTERNAL -au_size 4
"

```

- Vérifiez l'état des groupes de disques ASM et de la ressource Oracle Restart :

```

sudo -u grid ORACLE_HOME=/u01/app/26ai/grid ORACLE_SID=+ASM \
  /u01/app/26ai/grid/bin/sqlplus -s / as sysasm <<'SQL'
SELECT name, total_mb, free_mb, state FROM v$asm_diskgroup ORDER BY
name;
SQL

sudo /u01/app/26ai/grid/bin/crsctl stat res -t
# Expected ONLINE: ora.DATA.dg, ora.RECO.dg, ora.FRA.dg,
ora.LISTENER.lsnr, ora.asm, ora.cssd, ora.evmd.

```

- Répétez les étapes ci-dessus sur `oracdb2`. Le `HOST=$(hostname -s)` modèle dans [étapes 3 et 4](#) et [étape 7](#) sélectionne automatiquement les périphériques iSCSI GCNV de cet hôte.

Utilisez les mêmes noms de groupes de disques ASM : Data Guard réplique via Oracle Net, et non via le stockage.

Étape 2 : Installez Oracle Database sur chaque hôte de base de données

Installez le répertoire du logiciel Oracle Database 26ai sur chaque hôte de base de données en utilisant une installation silencieuse, logicielle uniquement, avec la dernière Release Update appliquée. Effectuez toutes les étapes sur `oracdb1` avant de les répéter sur `oracdb2`.

- Décompressez le répertoire d'installation de la base de données, la dernière version d'OPatch et le correctif RU dans leurs répertoires respectifs. Consultez la documentation Oracle pour l'arborescence des répertoires RU et le `-applyRU` chemin d'accès :

```

sudo su - oracle
cd /u01/app/oracle/product/26ai/db_1
unzip -q /u01/stage/LINUX.X64_<RELEASE>_db_home.zip
rm -rf OPatch
unzip -q /u01/stage/p6880880_<base>_Linux-x86-64.zip
# latest OPatch
unzip -q /u01/stage/p<RU_PATCH>_<base>_Linux-x86-64.zip -d /u01/stage
# latest 26ai RU

```

- Écrivez le fichier de réponses d'installation et exécutez l'installation silencieuse du logiciel uniquement avec le RU appliqué. Sur OL 8/9, omettez `-applyOneOffs` de la ligne `runInstaller` :

```

sudo -u oracle tee /u01/stage/dbinstall.rsp >/dev/null <<'EOF'
oracle.install.option=INSTALL_DB_SWONLY
UNIX_GROUP_NAME=oinstall
INVENTORY_LOCATION=/u01/app/oraInventory
ORACLE_HOME=/u01/app/oracle/product/26ai/db_1
ORACLE_BASE=/u01/app/oracle
oracle.install.db.InstallEdition=EE
oracle.install.db.OSDBA_GROUP=dba
oracle.install.db.OSOPER_GROUP=oper
oracle.install.db.OSBACKUPDBA_GROUP=backupdba
oracle.install.db.OSDGDBA_GROUP=dgdba
oracle.install.db.OSKMDBA_GROUP=kmdba
oracle.install.db.OSRACDBA_GROUP=racdba
oracle.install.db.rootconfig.executeRootScript=false
EOF

sudo -u oracle bash -c '
export CV_ASSUME_DISTID=OEL10      # OEL9 / OEL8.10 if cluify requires it
cd /u01/app/oracle/product/26ai/db_1
./runInstaller -applyRU /u01/stage/<RU_PATCH> \
  -applyOneOffs /u01/stage/39292021 \
  -silent -ignorePrereqFailure -responseFile /u01/stage/dbinstall.rsp
'

```

- Exécutez le script racine post-installation :

```

sudo /u01/app/oracle/product/26ai/db_1/root.sh

```

- Définissez l'environnement Oracle sur chaque hôte de base de données. Utilisez `ORACLE_SID=orcl` sur `oracdb1` et `ORACLE_SID=orcls` sur `oracdb2` :

```
sudo -u oracle tee -a /home/oracle/.bash_profile >/dev/null <<'EOF'  
export ORACLE_HOME=/u01/app/oracle/product/26ai/db_1  
export ORACLE_SID=orcl # use 'orcls' on oracdb2  
export GRID_HOME=/u01/app/26ai/grid  
export PATH=$ORACLE_HOME/bin:$GRID_HOME/bin:$PATH  
export TNS_ADMIN=$ORACLE_HOME/network/admin  
EOF
```

La base de données de secours est créée dans [Créer la base de données de secours](#).

Et ensuite ?

Pour créer l'instance principale de production pour votre déploiement HA, allez à [Créer la base de données Oracle principale](#) sur `oracdb1`.

Créez la base de données principale Oracle sur Google Cloud NetApp Volumes

Créez la base de données Oracle principale sur le stockage iSCSI Google Cloud NetApp Volumes à l'aide de l'Assistant de configuration de base de données Oracle en mode silencieux. Cette procédure couvre l'exécution de `dbca` pour créer la base de données conteneur et la base de données enfichable sur des groupes de disques ASM pris en charge par GCNV, la configuration des destinations des journaux d'archive, et l'ajout d'un service applicatif basé sur les rôles pour un basculement transparent après l'activation de Data Guard.

Étapes

Créez la base de données conteneur Oracle et la base de données pluggable sur `oracdb1` en utilisant `dbca` en mode silencieux, configurez les destinations des journaux d'archivage, vérifiez l'enregistrement Oracle Restart et ajoutez un service applicatif basé sur les rôles pour un basculement transparent du client.

1. Exécutez `dbca` en mode silencieux pour créer la CDB et la PDB sur les groupes de disques ASM :

```

sudo -u oracle bash -c '
export ORACLE_HOME=/u01/app/oracle/product/26ai/db_1
export PATH=$ORACLE_HOME/bin:$PATH

dbca -silent -createDatabase \
  -templateName General_Purpose.dbc \
  -gdbname orcl -sid orcl \
  -characterSet AL32UTF8 -nationalCharacterSet AL16UTF16 \
  -sysPassword "ChangeMe!1" -systemPassword "ChangeMe!1" \
  -emConfiguration NONE \
  -datafileDestination +DATA -storageType ASM \
  -recoveryAreaDestination +FRA -recoveryAreaSize 25000 \
  -enableArchive true -archiveLogMode AUTO \
  -memoryMgmtType AUTO_SGA -totalMemory 4096 \
  -databaseType MULTIPURPOSE \
  -createAsContainerDatabase true -numberOfPDBs 1 \
  -pdbName orclpdb -pdbAdminPassword "ChangeMe!1" \
  -ignorePreReqs
'
```

2. Pointez les journaux d'archivage vers +RECO et ouvrez puis enregistrez l'état de la base de données enfichable. La base de données de secours utilise des paramètres de journaux d'archivage correspondants dans [Étape 2 : Standby init.ora, pfile et NOMOUNT](#) :

```

sudo -u oracle bash -c '
export ORACLE_HOME=/u01/app/oracle/product/26ai/db_1
export ORACLE_SID=orcl
$ORACLE_HOME/bin/sqlplus -s / as sysdba <<SQL
ALTER SYSTEM SET log_archive_dest_1='\"'LOCATION=+RECO
VALID_FOR=(ALL_LOGFILES,ALL_ROLES) DB_UNIQUE_NAME=orcl'\"' SCOPE=BOTH;
ALTER PLUGGABLE DATABASE ALL OPEN;
ALTER PLUGGABLE DATABASE ALL SAVE STATE;
EXIT
SQL
'
```

3. Vérifiez que la base de données s'exécute sous Oracle Restart :

```

sudo /u01/app/26ai/grid/bin/srvctl status database -d orcl
# Expected: Database is running

sudo -u oracle sqlplus -s / as sysdba <<<"SELECT name, open_mode,
log_mode FROM v\${database};"
# Expected: ORCL, READ WRITE, ARCHIVELOG

```

4. Créez un service applicatif afin que les applications se connectent via orclapp et que le basculement soit transparent lorsque Data Guard est activé :

```

sudo -u oracle bash -c '
export GRID_HOME=/u01/app/26ai/grid
export ORACLE_HOME=/u01/app/oracle/product/26ai/db_1
export PATH=$ORACLE_HOME/bin:$GRID_HOME/bin:$PATH

srvctl add service \
  -db orcl \
  -service orclapp \
  -pdb orclpdb \
  -role PRIMARY \
  -policy AUTOMATIC

srvctl start service -db orcl -service orclapp
srvctl status service -db orcl -service orclapp
'
```

Après l'activation de Data Guard Broker, orclapp s'exécute uniquement sur le PRIMARY. Multiplexez les fichiers de contrôle sur les groupes de disques ASM et dimensionnez la mémoire en fonction de la charge de travail.

Et ensuite ?

Pour établir une protection de secours et une préparation au basculement, allez à [Créer la base de données Oracle de secours](#) sur oracdb2.

Créez la base de données de secours Oracle avec l'amorçage de la couche de stockage Google Cloud NetApp Volumes

Créez la base de données de secours physique Oracle en utilisant la réplication au niveau de la couche de stockage Google Cloud NetApp Volumes, les snapshots ou les clones pour accélérer l'initialisation de la base de données de secours par rapport aux méthodes RMAN traditionnelles. Cette procédure couvre la configuration du listener, la création du pfile de secours, l'initialisation des volumes de secours avec la réplication

GCNV, la finalisation de l'instance Oracle et l'enregistrement de la base de données de secours auprès d'Oracle Restart. Tous les niveaux HA effectuent ces étapes. Pour le niveau **Prod HA (Data Guard + FSFO)**, continuez avec [Finalisation de Data Guard](#) avant de configurer [Data Guard Broker](#), [basculement rapide automatique](#) et [Observer](#).

Étape 1 : Configurer les paramètres de l'écouteur et de Data Guard

Configurez l'écouteur sur les deux hôtes de base de données pour prendre en charge les connexions Data Guard, y compris le `_DGMGRL` service requis pour le broker. Configurez le fichier de mots de passe et les paramètres de journalisation d'archive sur la base de données principale.

1. Configurez l'écouteur principal et vérifiez l'environnement sur `oracdb1`:

```
sudo su - oracle
. ~/.bash_profile          # ORACLE_SID=orcl, ORACLE_HOME set
```

2. Configurez l'écouteur de secours sur `oracdb2` pour inclure les `orcls` et `orcls_DGMGRL` services :

```
GRID_HOME=/u01/app/26ai/grid
sudo -u grid tee "$GRID_HOME/network/admin/listener.ora" >/dev/null <<
'EOF'
LISTENER =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP) (HOST = oracdb2.example.internal) (PORT =
1521)))

SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC = (GLOBAL_DBNAME = orcls)          (ORACLE_HOME =
/u01/app/oracle/product/26ai/db_1) (SID_NAME = orcls))
    (SID_DESC = (GLOBAL_DBNAME = orcls_DGMGRL) (ORACLE_HOME =
/u01/app/oracle/product/26ai/db_1) (SID_NAME = orcls)))
EOF
```

3. Redémarrez le service d'écoute via Oracle Restart sur les deux hôtes et vérifiez que le `_DGMGRL` service est enregistré :

```
sudo -u grid bash -c '
export GRID_HOME=/u01/app/26ai/grid
export ORACLE_HOME=$GRID_HOME
$GRID_HOME/bin/srvctl stop listener
$GRID_HOME/bin/srvctl start listener
$GRID_HOME/bin/lsnrctl status
'
```

```
lsnrctl status doit lister <SID> et <SID>_DGMGRL.
```

Étape 2 : Préparez le fichier pfile de secours et NOMOUNT

Préparez l'instance de base de données de secours en copiant le fichier de mots de passe depuis la base principale, en créant un fichier pfile init.ora minimal avec les paramètres Data Guard, puis en démarrant l'instance en mode NOMOUNT.

1. Copiez le fichier de mot de passe principal sur l'hôte de secours à l'aide d'IAP et `gcloud compute scp` :

```
PRIMARY_ZONE=us-west1-a      # zone of oracdb1
STANDBY_ZONE=us-west1-b      # zone of oracdb2

gcloud compute scp \
  oracdb1:/u01/app/oracle/product/26ai/db_1/dbs/orapworcl ./orapworcl \
  --zone=$PRIMARY_ZONE --tunnel-through-iap

gcloud compute scp \
  ./orapworcl oracdb2:/u01/app/oracle/product/26ai/db_1/dbs/orapworcls \
  --zone=$STANDBY_ZONE --tunnel-through-iap
```

2. Interrogez la valeur du paramètre `compatible` à partir de la base de données principale :

```
# On oracdb1
sudo -u oracle sqlplus -s / as sysdba \
  <<<"SELECT value FROM v\${parameter} WHERE name='compatible';"
```

3. Créez le fichier pfile de secours sur `oracdb2`, définissez le propriétaire du fichier de mots de passe et démarrez l'instance en mode NOMOUNT. Remplacez la valeur `compatible` de l'étape précédente par `<COPY_FROM_PRIMARY>` :

```
sudo -u oracle mkdir -p /u01/app/oracle/admin/orcls/adump
sudo chown oracle:oinstall
/u01/app/oracle/product/26ai/db_1/dbs/orapworcls
sudo chmod 0600 /u01/app/oracle/product/26ai/db_1/dbs/orapworcls

sudo -u oracle tee /u01/app/oracle/product/26ai/db_1/dbs/initorcls.ora
>/dev/null <<'EOF'
*.db_name='orcl'
*.db_unique_name='orcls'
*.audit_file_dest='/u01/app/oracle/admin/orcls/adump'
*.diagnostic_dest='/u01/app/oracle'
*.compatible='<COPY_FROM_PRIMARY>'
*.sga_target=3072m
```

```

*.pga_aggregate_target=1024m
*.processes=320
*.remote_login_passwordfile='EXCLUSIVE'
*.standby_file_management='AUTO'
*.fal_server='orcl'
*.log_archive_config='DG_CONFIG=(orcl,orcls)'
*.log_archive_dest_1='LOCATION=+RECO VALID_FOR=(ALL_LOGFILES,ALL_ROLES)
DB_UNIQUE_NAME=orcls'
*.log_archive_dest_2='SERVICE=orcl AFFIRM SYNC
VALID_FOR=(ONLINE_LOGFILES,PRIMARY_ROLE) DB_UNIQUE_NAME=orcl'
*.log_archive_dest_state_2='DEFER'
*.log_archive_format='%t_%s_%r.arc'
*.dg_broker_start=TRUE
*.undo_tablespace='UNDOTBS1'
*.open_cursors=300
*.db_create_file_dest='+DATA'
*.db_create_online_log_dest_1='+DATA'
*.db_recovery_file_dest='+FRA'
*.db_recovery_file_dest_size=25000m

```

EOF

```

echo "orcls:/u01/app/oracle/product/26ai/db_1:N" | sudo tee -a
/etc/oratab

```

```

sudo -u oracle bash -c '
export ORACLE_HOME=/u01/app/oracle/product/26ai/db_1
export ORACLE_SID=orcls
sqlplus / as sysdba <<SQL
STARTUP NOMOUNT
PFILE=/u01/app/oracle/product/26ai/db_1/dbs/initorcls.ora;
EXIT
SQL
'

```

L'instance de secours est maintenant en mode NOMOUNT sans fichiers de données jusqu'à [Étape 3 : Initialiser le stockage de secours avec GCNV](#).

Étape 3 : Initialiser le stockage de secours avec GCNV

Initialisez les volumes de secours dans oracle-pool-b, attachez-les à oracdb2, montez les groupes de disques ASM et finalisez l'instance de secours à l'état MOUNT.

Utilisez la réplication GCNV pour l'amorçage en production et l'amorçage par instantané pour les flux de travail de laboratoire ponctuels.

Choisissez le chemin de seeding

Choisissez la méthode d'ensemencement de secours en fonction de votre environnement et de vos exigences de récupération.

- **Recommandé pour la production** : Utilisez le chemin de réplication dans [Chemin de réplication : créer et synchroniser les répliquions](#) et [Chemin de réplication : basculer et attacher les volumes de secours](#).
- **Alternative pour les laboratoires** : Utilisez [Chemin alternatif : initialisation à partir d'un instantané](#).

Tous les chemins se rejoignent à [Monter les groupes de disques ASM de secours](#) et [Finalisez l'instance de secours](#).

Vérifiez les prérequis

Confirmez les prérequis suivants avant d'initialiser les volumes de secours.

- `gcloud netapp` avec prise en charge de la réplication de volumes.
- Deux pools en mode **par défaut** à des emplacements différents (`oracle-pool-a`, `oracle-pool-b`).
- Volumes sources sur le pool principal attachés `oracdb1-hg`; volumes de destination créés par réplication.
- Exécutez la réplication depuis Cloud Shell ou un poste de travail — pas depuis des machines virtuelles de base de données.
- Sur `oracdb2`, configuration complète de l'hôte iSCSI et ASM à partir de [Étape 4](#), [Étape 5](#) et [Étape 6](#).

```
export PROJECT=<your-gcp-project>
export LOC_A=us-west1-a
export LOC_B=us-west1-b
export DEST_POOL="projects/${PROJECT}/locations/${LOC_B
}/storagePools/oracle-pool-b"
```

- Créez un pool de secours si nécessaire :

```
gcloud netapp storage-pools create oracle-pool-b \
  --project="${PROJECT}" --location="${LOC_B}" \
  --service-level=flex --type=unified --mode=default \
  --capacity=1024 --network=name=<your-vpc>
```

Créer et synchroniser des répliquions

Créez des relations de réplication entre les volumes principaux et les volumes de secours, puis attendez la fin de la synchronisation initiale.

```

gcloud netapp volumes replications create repl-oracdb2-data \
  --project="${PROJECT}" --location="${LOC_A}" --volume=oracdb1_data \
  --replication-schedule=EVERY_10_MINUTES \
  --destination-volume-parameters="storage_pool=${DEST_POOL
},volume_id=oracdb2_data,share_name=oracdb2_data"

gcloud netapp volumes replications create repl-oracdb2-reco \
  --project="${PROJECT}" --location="${LOC_A}" --volume=oracdb1_reco \
  --replication-schedule=EVERY_10_MINUTES \
  --destination-volume-parameters="storage_pool=${DEST_POOL
},volume_id=oracdb2_reco,share_name=oracdb2_reco"

```

+

Attendez que `mirrorState` soit `MIRRORED` et que la synchronisation initiale soit terminée pour chaque réplication.

Basculez et attachez les volumes de veille

Mettez au repos le serveur principal, arrêtez la réplication après la synchronisation finale et attachez les volumes de destination au groupe d'hôtes de secours.

Sur le système principal, mettez en veille les écritures et capturez les métadonnées de restauration :

```

ALTER DATABASE BEGIN BACKUP;
SELECT CURRENT_SCN FROM V$DATABASE;
ALTER DATABASE CREATE STANDBY CONTROLFILE AS '/tmp/orcls_stby.ctl';

```

Autorisez un dernier cycle de réplication, puis arrêtez les réplications :

```

gcloud netapp volumes replications stop repl-oracdb2-data \
  --project="${PROJECT}" --location="${LOC_A}" --volume=oracdb1_data
--force

gcloud netapp volumes replications stop repl-oracdb2-reco \
  --project="${PROJECT}" --location="${LOC_A}" --volume=oracdb1_reco
--force

```

Attachez les volumes de destination à `oracdb2-hg` (les LUN répliqués peuvent conserver les noms sources) :

```

HG=$(gcloud netapp host-groups describe oracdb2-hg --project="${PROJECT}"
\
  --location=us-west1 --format='value(name) ')

gcloud netapp volumes update oracdb2_data --project="${PROJECT}"
--location="${LOC_B}" \
  --block-devices="name=oracdb1_data_lun,host-groups=${HG},os-type=LINUX"

```

Copiez le fichier de contrôle de secours vers oracdb2, puis mettez fin au mode de sauvegarde sur le serveur principal :

```
ALTER DATABASE END BACKUP;
```

Initialiser à partir d'un instantané

Utilisez ce chemin pour un ensemencement ponctuel en laboratoire lorsque la réplication continue n'est pas nécessaire.

Pour un environnement de test ponctuel, créez un instantané source et créez des volumes de secours à partir de cet instantané dans `oracle-pool-b` (Cloud Console ou API). Attachez les volumes créés à `oracdb2-hg`, puis continuez avec [Monter les groupes de disques ASM de secours](#).

Monter les groupes de disques ASM de secours

Sur l'hôte de secours, découvrez les chemins de stockage connectés et montez les groupes de disques ASM avant la restauration de la base de données.

Sur `oracdb2`, connectez-vous aux portails iSCSI du pool de secours et analysez à nouveau les périphériques multipath. Si les en-têtes de disque ASM correspondent à la dénomination principale dans un flux de travail de laboratoire, utilisez des alias de style principal (par exemple `ora_oracdb1_data_01`, `ora_oracdb1_arch_01`), définissez `asm_diskstring='/dev/mapper/ora_oracdb1_*p*'` et vérifiez que le propriétaire de la partition est `grid:asmadmin, puis montez les groupes de disques :`

```

ALTER DISKGROUP DATA MOUNT FORCE;
ALTER DISKGROUP RECO MOUNT FORCE;
ALTER DISKGROUP FRA MOUNT FORCE;

```

Finalisez l'instance de secours

Restaurez le fichier de contrôle de secours, récupérez jusqu'au SCN capturé, convertissez en secours physique et démarrez la récupération gérée.

```
STARTUP NOMOUNT;
RESTORE STANDBY CONTROLFILE FROM '/tmp/orcls_stby.ctl';
ALTER DATABASE MOUNT;
RECOVER DATABASE UNTIL SCN <quiesce_scn>;
ALTER DATABASE CONVERT TO PHYSICAL STANDBY;
SHUTDOWN IMMEDIATE;
STARTUP MOUNT;
ALTER DATABASE RECOVER MANAGED STANDBY DATABASE DISCONNECT FROM SESSION;
```

À ce stade, le système de secours devrait être `PHYSICAL STANDBY` et `'MOUNTED'` avec la récupération gérée démarrée.

Prochaines étapes spécifiques à chaque niveau :

- **Haute disponibilité de production (sans Data Guard)** : Passez directement à [Étape 4 : Enregistrez le serveur de secours auprès d'Oracle Restart](#).
- **Haute disponibilité de production (Data Guard + FSFO)** : Continuez vers [Étape 4 : Enregistrez le serveur de secours auprès d'Oracle Restart](#), puis procédez à [Étapes de finalisation de Data Guard](#).

Étape 4 : Enregistrez le serveur de secours auprès d'Oracle Restart

Enregistrez la base de données de secours auprès d'Oracle Restart afin que les redémarrages permettent la récupération automatique des groupes de disques ASM, le montage de la base de données de secours et le redémarrage de la récupération gérée. Ajoutez également le service applicatif aux deux ressources de base de données.

1. Capturez l'emplacement du spfile depuis la base de données de secours et enregistrez-le auprès d'Oracle Restart sur `oracdb2`. Remplacez `<STANDBY_SPFILE_PATH>` à partir de la requête (souvent sous `+DATA`) :

```

sudo -u oracle bash -c '
export ORACLE_SID=orcls
sqlplus -s / as sysdba <<< "SHOW PARAMETER spfile;"
'

sudo -u oracle bash -c '
export GRID_HOME=/u01/app/26ai/grid
export ORACLE_HOME=/u01/app/oracle/product/26ai/db_1
export PATH=$ORACLE_HOME/bin:$GRID_HOME/bin:$PATH

srvctl add database \
  -db orcls \
  -dbname orcl \
  -oraclehome /u01/app/oracle/product/26ai/db_1 \
  -spfile <STANDBY_SPFILE_PATH> \
  -pwfile /u01/app/oracle/product/26ai/db_1/dbs/orapworcls \
  -role PHYSICAL_STANDBY \
  -startoption MOUNT \
  -stopoption IMMEDIATE \
  -diskgroup DATA,RECO,FRA

srvctl config database -db orcls
srvctl status database -db orcls
'

```

2. Vérifiez et mettez à jour la ressource de base de données principale sur `oracdb1` afin d'inclure toutes les dépendances du groupe de disques ASM :

```

sudo -u oracle bash -c '
export GRID_HOME=/u01/app/26ai/grid
export ORACLE_HOME=/u01/app/oracle/product/26ai/db_1
export PATH=$ORACLE_HOME/bin:$GRID_HOME/bin:$PATH
srvctl config database -db orcl
srvctl modify database -db orcl -diskgroup DATA,RECO,FRA
srvctl config database -db orcl
'

```

3. Ajoutez le service applicatif à la ressource de base de données de secours (`orcls` sur `oracdb2`). Utilisez le rôle `PRIMARY` des deux côtés afin que `orclapp` soit disponible après le basculement :

```

sudo -u oracle bash -c '
export GRID_HOME=/u01/app/26ai/grid
export ORACLE_HOME=/u01/app/oracle/product/26ai/db_1
export PATH=$ORACLE_HOME/bin:$GRID_HOME/bin:$PATH

srvctl add service \
  -db orcls \
  -service orclapp \
  -pdb orclpdb \
  -role PRIMARY \
  -policy AUTOMATIC

srvctl config service -db orcls -service orclapp
'
```

4. Vérifiez la ressource de base de données de secours sur oracdb2 :

```

sudo -u oracle bash -c '
export GRID_HOME=/u01/app/26ai/grid
export ORACLE_HOME=/u01/app/oracle/product/26ai/db_1
export PATH=$ORACLE_HOME/bin:$GRID_HOME/bin:$PATH
srvctl status database -db orcls
'
```

Et ensuite ?

Spécifique au niveau :

- **Haute disponibilité de production (sans Data Guard) :** Pour maintenir une cible de récupération basée sur la réplication du stockage, l'initialisation de la base de secours est terminée et la base de secours est enregistrée auprès d'Oracle Restart en tant qu'instance de sauvegarde.
- **Haute disponibilité de production (Data Guard + FSFO) :** Pour activer le basculement géré par le broker et le basculement rapide, poursuivez avec [Finalisez la base de données de secours pour Data Guard](#).

Finalisez la base de données de secours pour Data Guard sur Google Cloud NetApp Volumes

Finalisez la base de données de secours pour Oracle Data Guard sur Google Cloud NetApp Volumes en créant des fichiers journaux de restauration de secours, en activant la fonctionnalité flashback database, en activant l'expédition des journaux de restauration et en vérifiant l'état de Data Guard.

Spécifique au niveau : Cette procédure est requise uniquement pour le niveau **Prod HA (Data Guard +**

FSFO).

Étape 1 : Créez des fichiers journaux de restauration en attente

Créez des fichiers journaux de restauration de secours sur les deux hôtes de base de données pour assurer la prise en charge du basculement rapide Fast-Start Failover. La taille doit être supérieure ou égale à celle du plus grand journal de restauration principal en ligne, et le nombre doit être égal au nombre de groupes en ligne par thread + 1. Après le semis GCNV, supprimez puis recréez les journaux de restauration de secours sur le serveur de secours afin de corriger les chemins répliqués.

1. Créer des fichiers journaux de restauration de secours sur la base de données principale (orcl :

```
ALTER SYSTEM SET db_create_file_dest='+DATA' SCOPE=BOTH;
ALTER DATABASE ADD STANDBY LOGFILE THREAD 1 ('+DATA') SIZE 1024M;
-- repeat (online log groups + 1) times
```

2. Supprimez et recréez les fichiers journaux de restauration de secours sur la base de données de secours (orcl2 après l'initialisation de GCNV. Les chemins répliqués sous +DATA/ORCL/... causent ORA-19527 / ORA-16086 jusqu'à reconstruction :

```
ALTER DATABASE RECOVER MANAGED STANDBY DATABASE CANCEL;
ALTER SYSTEM SET standby_file_management=MANUAL SCOPE=BOTH;
-- DROP STANDBY LOGFILE GROUP for each group# in v$standby_log;
ALTER SYSTEM SET db_create_file_dest='+DATA' SCOPE=BOTH;
ALTER SYSTEM SET standby_file_management=AUTO SCOPE=BOTH;
ALTER DATABASE ADD STANDBY LOGFILE THREAD 1 ('+DATA') SIZE 1024M;
-- repeat (online groups + 1) times; one member per group
ALTER DATABASE RECOVER MANAGED STANDBY DATABASE USING CURRENT LOGFILE
DISCONNECT FROM SESSION;
```

Étape 2 : Activez le flashback et lancez la récupération

Activez la fonctionnalité flashback database sur le serveur de secours pour permettre la restauration automatique après un basculement, puis lancez la récupération gérée avec application en temps réel. La fonctionnalité flashback doit être activée avant de démarrer la récupération gérée, car elle ne peut pas être activée lorsque le MRP est en cours d'exécution.

1. Arrêtez la base de données de secours, redémarrez en mode MOUNT et activez la fonctionnalité flashback database sur oracdb2 :

```
# On oracdb2
sudo -u oracle bash -c '
. ~/.bash_profile
export ORACLE_SID=orcl
sqlplus / as sysdba <<SQL
SHUTDOWN IMMEDIATE;
STARTUP MOUNT;
ALTER SYSTEM SET db_flashback_retention_target=1440 SCOPE=BOTH;
ALTER DATABASE FLASHBACK ON;
EXIT
SQL'
```

2. Démarrez la récupération gérée avec application en temps réel :

```
sudo -u oracle bash -c '
. ~/.bash_profile
export ORACLE_SID=orcl
sqlplus / as sysdba <<SQL
ALTER DATABASE RECOVER MANAGED STANDBY DATABASE USING CURRENT LOGFILE
DISCONNECT FROM SESSION;
EXIT
SQL'
```

`USING CURRENT LOGFILE` permet l'application en temps réel (le redo est appliqué dès son arrivée dans les SRL).

Étape 3 : Activer la réexpédition des journaux de reprise

Activez le transport des journaux de restauration du serveur principal vers le serveur de secours en activant LOG_ARCHIVE_DEST_STATE_2, qui a été délibérément défini sur DEFER dans [Étape 2](#) de la procédure d'initialisation du serveur de secours afin de supprimer ORA-12154 les erreurs lors de la création du serveur de secours.

1. Passez LOG_ARCHIVE_DEST_STATE_2 à `ENABLE` et forcez un changement de journal pour initier l'expédition des redo logs :

```
sudo -u oracle bash -c '
. ~/.bash_profile
sqlplus / as sysdba <<SQL
ALTER SYSTEM SET LOG_ARCHIVE_DEST_STATE_2=ENABLE SCOPE=BOTH;
ALTER SYSTEM SWITCH LOGFILE;
ALTER SYSTEM ARCHIVE LOG CURRENT;
EXIT
SQL'
```

2. Vérifiez que la réexpédition de redo fonctionne correctement :

```
sudo -u oracle bash -c '  
. ~/.bash_profile  
sqlplus / as sysdba <<SQL  
SELECT dest_id, status, error FROM v\${archive_dest_status} WHERE dest_id  
IN (1,2);  
EXIT  
SQL'  
# Expected: dest_id=2, STATUS=VALID, ERROR null.
```

Si `dest_2` affiche `ORA-12154`, relancez le primaire. Après [Étape 1 : Activer le courtier sur les deux bases de données](#), gérez le transport via DGMGRL.

Étape 4 : Vérifiez l'état de Data Guard

Vérifiez que la base de données principale est en mode LECTURE/ÉCRITURE et que la base de données de secours est montée avec une récupération gérée appliquant les journaux de reprise.

1. Vérifiez le rôle de la base de données principale et le mode d'ouverture sur `oracdb1` :

```
sudo -u oracle sqlplus -s / as sysdba \  
<<<"SELECT database_role || ' | ' || open_mode FROM v\${database};"  
# Expected: PRIMARY | READ WRITE
```

2. Vérifiez le rôle de la base de données de secours, le mode d'ouverture et l'état de la récupération gérée sur `oracdb2` :

```

gcloud compute ssh oracdb2 --tunnel-through-iap --zone=us-west1-b

sudo -u oracle bash <<'BASH'
. ~/.bash_profile
export ORACLE_SID=orcls

sqlplus -s / as sysdba <<'SQL'
SELECT database_role || ' | ' || open_mode
FROM v$database;

SELECT process, status, sequence#
FROM v$managed_standby
WHERE process IN ('MRP0','RFS');

EXIT
SQL
BASH

```

Attendu en veille : PHYSICAL STANDBY | MOUNTED; MRP0 avec APPLYING_LOG.

3. Si le standby signale MOUNTED mais que l'application n'est pas en cours d'exécution, redémarrez la récupération gérée sur oracdb2 :

```

sudo -u oracle bash -c '
. ~/.bash_profile
export ORACLE_SID=orcls
sqlplus / as sysdba <<SQL
ALTER DATABASE RECOVER MANAGED STANDBY DATABASE CANCEL;
ALTER DATABASE RECOVER MANAGED STANDBY DATABASE USING CURRENT LOGFILE
DISCONNECT FROM SESSION;
EXIT
SQL'

```

Et ensuite ?

Pour activer la gestion automatisée des rôles et la protection contre les basculements, continuez avec [Configurer Oracle Data Guard Broker, Fast-Start Failover et l'observateur](#).

Configurer Data Guard Broker et le basculement rapide automatique pour Oracle Database 26ai sur Google Cloud NetApp Volumes

Configurez Oracle Data Guard Broker et Fast-Start Failover avec un observateur dédié

pour activer les transitions de rôle automatiques pour Oracle Database 26ai sur Google Cloud NetApp Volumes.

Spécifique au niveau : Cette procédure s'applique uniquement au niveau **Prod HA (Data Guard + FSFO)**.

Cette procédure décrit l'activation du broker sur les deux bases de données, la création de la configuration Data Guard, l'activation de FSFO avec le mode de protection MaxAvailability, l'installation d'Oracle Instant Client sur l'hôte Observer, le démarrage de l'Observer en tant que service systemd avec des identifiants basés sur un portefeuille, ainsi que les tests de basculement et de reprise après incident. Après `ENABLE CONFIGURATION`, gérez le transport et les rôles via **DGMGRL** (et non via ``LOG_ARCHIVE_DEST_*` SQL ad hoc).

Étape 1 : Activer Data Guard Broker

Activez Data Guard Broker sur les deux hôtes de base de données et créez la configuration du broker qui relie les bases de données principale et de secours sous une gestion unifiée.

1. Définissez `dg_broker_start=TRUE` sur les hôtes de base de données principale et de secours :

```
sudo -u oracle bash -c '  
  . ~/.bash_profile  
  sqlplus / as sysdba <<SQL  
  ALTER SYSTEM SET dg_broker_start=TRUE SCOPE=BOTH;  
  EXIT  
  SQL'
```

2. Sur le serveur principal, connectez-vous à DGMGRL avec l'authentification du système d'exploitation et créez la configuration du broker :



Sur l'hôte Observer uniquement, utilisez `dgmgrl /@orcl` après que le portefeuille de connexion automatique existe. Ne mettez pas de mots de passe sur la ligne de commandes `dgmgrl`.

```
sudo -u oracle bash -c '  
  export ORACLE_HOME=/u01/app/oracle/product/26ai/db_1  
  export ORACLE_SID=orcl  
  export PATH=$ORACLE_HOME/bin:$PATH  
  dgmgrl /  
  '
```

```
DGMGRL> CREATE CONFIGURATION 'orcl_dg' AS
        PRIMARY DATABASE IS 'orcl' CONNECT IDENTIFIER IS orcl;
DGMGRL> ADD DATABASE 'orcls' AS CONNECT IDENTIFIER IS orcls;
DGMGRL> ENABLE CONFIGURATION;
DGMGRL> SHOW CONFIGURATION;
-- Expect: Configuration Status: SUCCESS, both members SUCCESS.
```

3. Validez la configuration — corrigez toute WARNING ou valeur non nulle ERROR avant [Étape 3 : Configurer les propriétés FSFO et activer](#) :

```
DGMGRL> VALIDATE DATABASE 'orcls';
DGMGRL> SHOW CONFIGURATION VERBOSE;
```

Étape 2 : Confirmez le flashback pour FSFO

Confirmez que la fonctionnalité flashback database est activée sur les deux hôtes. Flashback est requis pour la réintégration automatique FSFO, ce qui permet à l'ancien serveur principal de rejoindre automatiquement la configuration en tant que serveur de secours après un basculement.

1. Confirmez `flashback_on` est `YES` présent sur les deux hôtes de base de données :

```
sudo -u oracle bash -c '
. ~/.bash_profile
sqlplus -s / as sysdba <<<"SELECT flashback_on FROM v\${database};"
'
# Expected on both hosts: YES
```

2. Sur le système principal uniquement, si la rétention du flashback n'est pas déjà définie :

```
sudo -u oracle bash -c '
. ~/.bash_profile
export ORACLE_SID=orcl
sqlplus / as sysdba <<SQL
ALTER SYSTEM SET db_flashback_retention_target=1440 SCOPE=BOTH;
EXIT
SQL'
```

Étape 3 : Configurer et activer FSFO

Définissez le transport redo SYNC, configurez le mode de protection MaxAvailability, définissez les cibles FSFO sur chaque base de données et activez le basculement Fast-Start Failover.

1. Configurez le mode de transport des journaux de restauration SYNC sur les deux bases de données et

augmentez le niveau de protection à MaxAvailability :

```
DGMGRL> EDIT DATABASE 'orcl' SET PROPERTY LogXptMode='SYNC';
DGMGRL> EDIT DATABASE 'orcls' SET PROPERTY LogXptMode='SYNC';
DGMGRL> EDIT CONFIGURATION SET PROTECTION MODE AS MaxAvailability;
```

2. Configurez les cibles FSFO de sorte que chaque base de données désigne l'autre comme sa cible de basculement, puis configurez le seuil et le comportement de rétablissement automatique :

```
-- Each side names the other
DGMGRL> EDIT DATABASE 'orcl' SET PROPERTY FastStartFailoverTarget =
'orcls';
DGMGRL> EDIT DATABASE 'orcls' SET PROPERTY FastStartFailoverTarget =
'orcl';

-- 30 s is the default; lower for faster RTO but more sensitive to
network blips
DGMGRL> EDIT CONFIGURATION SET PROPERTY FastStartFailoverThreshold = 30;
DGMGRL> EDIT CONFIGURATION SET PROPERTY FastStartFailoverAutoReinstate =
TRUE;
```

3. Activez le basculement Fast-Start et confirmez la configuration :

```
DGMGRL> ENABLE FAST_START FAILOVER;
DGMGRL> SHOW FAST_START FAILOVER;
-- Expected: Threshold 30 seconds, Target orcls, Observer not yet
registered.
```

Étape 4 : Installer Instant Client sur Observer

Installez Oracle Instant Client sur la machine virtuelle Observer dédiée (oradg-obs), créez un utilisateur OS dédié oracle, et configurez l'environnement Oracle Net afin que l'Observer puisse se connecter aux deux membres de la base de données sur TCP/1521.

1. Installez les packages Oracle Instant Client sur l'hôte Observer (oradg-obs :

```
# Use -el8 / -el9 if the Observer is on an older OL/RHEL release
sudo dnf install -y oracle-instantclient-release-el10
sudo dnf install -y oracle-instantclient-basic \
                    oracle-instantclient-sqlplus \
                    oracle-instantclient-tools
```

2. Créez un utilisateur oracle OS dédié qui sera propriétaire du portefeuille et de l'unité systemd :

```
sudo useradd -u 54321 -m oracle
sudo passwd -l oracle
```

3. Configurez l'environnement Oracle Net et créez `tnsnames.ora` des entrées pour les deux hôtes de base de données :

```
sudo mkdir -p /etc/oracle/network/admin
sudo chown -R oracle:oracle /etc/oracle

sudo -u oracle tee /home/oracle/.bash_profile >/dev/null <<'EOF'
export ORACLE_HOME=/usr/lib/oracle/26/client64
export LD_LIBRARY_PATH=$ORACLE_HOME/lib
export PATH=$ORACLE_HOME/bin:$PATH
export TNS_ADMIN=/etc/oracle/network/admin
EOF

# tnsnames.ora - must reach both DB hosts on TCP/1521
sudo tee /etc/oracle/network/admin/tnsnames.ora >/dev/null <<'EOF'
orcl =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP) (HOST = oracdb1) (PORT = 1521))
      (CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME =
orcl)))
orcls =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP) (HOST = oracdb2) (PORT = 1521))
      (CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME =
orcls)))
EOF
sudo chown oracle:oracle /etc/oracle/network/admin/tnsnames.ora
```

Étape 5 : Exécutez Observer en tant que service systemd

Créez un portefeuille de connexion automatique avec les identifiants des deux membres de la base de données, puis configurez et démarrez l'Observer en tant que service systemd afin qu'il survive aux redémarrages et se reconnecte automatiquement à la configuration.

Stockez les identifiants d'un compte d'administrateur Data Guard dédié (par exemple, `SYSDG`) dans le portefeuille plutôt que `sys`. Les identifiants ne doivent jamais apparaître sur une `dgmgrl` ligne de commandes, où ils sont visibles par `ps` et `journalctl`; connectez-vous toujours en utilisant `/@<tns_alias>` sur l'Observateur.

1. Créez le portefeuille chiffré et renseignez les identifiants pour les deux membres de la base de données :

```

sudo -iu oracle bash <<'BASH'
mkdir -p $TNS_ADMIN/wallet
mkstore -wrl $TNS_ADMIN/wallet -create          # prompts for a wallet
password - store in your secrets manager
mkstore -wrl $TNS_ADMIN/wallet -createCredential orcl sys ChangeMe!1
mkstore -wrl $TNS_ADMIN/wallet -createCredential orcls sys ChangeMe!1
BASH

sudo tee /etc/oracle/network/admin/sqlnet.ora >/dev/null <<'EOF'
WALLET_LOCATION = (SOURCE = (METHOD = FILE) (METHOD_DATA = (DIRECTORY =
/etc/oracle/network/admin/wallet)))
SQLNET.WALLET_OVERRIDE = TRUE
EOF
sudo chown oracle:oracle /etc/oracle/network/admin/sqlnet.ora
sudo chmod -R 0700 /etc/oracle/network/admin/wallet

sudo -iu oracle ls -l /etc/oracle/network/admin/wallet
# Expected: cwallet.sso and ewallet.p12

sudo -iu oracle bash <<'BASH'
sqlplus -L "/@orcl as sysdba" <<'SQL'
SELECT database_role FROM v$database;
EXIT
SQL
BASH

sudo -iu oracle bash <<'BASH'
sqlplus -L "/@orcls as sysdba" <<'SQL'
SELECT database_role FROM v$database;
EXIT
SQL
BASH

sudo -iu oracle dgmgrl /@orcl 'SHOW CONFIGURATION;'
sudo -iu oracle dgmgrl /@orcls 'SHOW CONFIGURATION;'

```

2. Générez le portefeuille de connexion automatique `cwallet.sso` afin que le service `systemd Observer` puisse démarrer sans invite de mot de passe. Si `cwallet.sso` est manquant après l'exécution de `mkstore`, utilisez `orapki` du package d'outils Instant Client ou d'un répertoire de base de données pour le créer, puis réajoutez les informations d'identification enregistrées :

```

sudo -iu oracle orapki wallet create \
  -wallet /etc/oracle/network/admin/wallet \
  -auto_login
sudo -iu oracle ls -l /etc/oracle/network/admin/wallet
# Expected: cwallet.sso and ewallet.p12

```

3. Créez l'unité systemd, activez le service et vérifiez que l'Observer est connecté :

```

sudo tee /etc/systemd/system/dgmgml-observer.service >/dev/null <<'EOF'
[Unit]
Description=Oracle Data Guard Fast-Start Failover Observer
After=network-online.target
Wants=network-online.target

[Service]
Type=simple
User=oracle
Group=oracle
Environment=ORACLE_HOME=/usr/lib/oracle/26/client64
Environment=LD_LIBRARY_PATH=/usr/lib/oracle/26/client64/lib
Environment=TNS_ADMIN=/etc/oracle/network/admin
Environment=PATH=/usr/lib/oracle/26/client64/bin:/usr/bin:/bin
ExecStart=/usr/lib/oracle/26/client64/bin/dgmgml -silent /@orcl "START
OBSERVER FILE IS '/var/lib/oracle/dgmgml-observer.dat'"
Restart=always
RestartSec=5

[Install]
WantedBy=multi-user.target
EOF

```

```

sudo install -d -o oracle -g oracle -m 0755 /var/lib/oracle
sudo install -o oracle -g oracle -m 0640 /dev/null /var/log/dgmgml-
observer.log

sudo tee /etc/logrotate.d/dgmgml-observer >/dev/null <<'EOF'
/var/log/dgmgml-observer.log {
    weekly
    rotate 8
    compress delaycompress missingok notifempty
    create 0640 oracle oracle
    copytruncate
}
EOF

sudo systemctl daemon-reload && sudo systemctl enable --now dgmgml-
observer.service
sudo systemctl status dgmgml-observer.service

```

L'observateur doit lire CONNECTED à partir du serveur principal (un DISCONNECTED observateur suspend silencieusement FSFO) :

```

DGMGRL> SHOW FAST_START FAILOVER;
DGMGRL> SHOW CONFIGURATION;          -- Configuration Status: SUCCESS,
FSFO: ENABLED

```

Étape 6 : Tester FSFO

Validez la configuration Data Guard avec VALIDATE DATABASE, puis effectuez un basculement planifié et, dans une fenêtre de test, un basculement imprévu avec réinitialisation de VM pour confirmer que FSFO fonctionne de bout en bout.

1. Testez un basculement planifié et rétablissez la topologie d'origine :

```

DGMGRL> VALIDATE DATABASE 'orcls';
DGMGRL> SWITCHOVER TO 'orcls';
DGMGRL> SHOW CONFIGURATION;
DGMGRL> SWITCHOVER TO 'orcl';          -- restore topology

```

2. Testez un basculement non planifié à l'aide d'une réinitialisation de machine virtuelle dans une fenêtre de test contrôlée :

Effectuez une réinitialisation de la machine virtuelle (test de type plantage) ; un arrêt normal peut ne pas déclencher FSFO. Tail /var/log/dgmgml-observer.log sur oradg-obs pour surveiller la progression du basculement ; rétablissez la topologie une fois terminé.

Et ensuite ?

La configuration d'Oracle Data Guard Broker, de Fast-Start Failover et d'Observer est désormais en place pour ce déploiement.

Informations sur le copyright

Copyright © 2026 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.