Protection automatisée des données Oracle

NetApp database solutions

NetApp
August 18, 2025

Sommaire

Protection automatisée des données Oracle

Présentation de la solution

Cette page décrit la méthode automatisée de déploiement d'Oracle19c sur le stockage NetApp ONTAP .

Protection automatisée des données pour les bases de données Oracle

Les organisations automatisent leurs environnements pour gagner en efficacité, accélérer les déploiements et réduire les efforts manuels. Des outils de gestion de configuration comme Ansible sont utilisés pour rationaliser les opérations de base de données d'entreprise. Dans cette solution, nous démontrons comment vous pouvez utiliser Ansible pour automatiser la protection des données d'Oracle avec NetApp ONTAP. En permettant aux administrateurs de stockage, aux administrateurs système et aux administrateurs de bases de données de configurer de manière cohérente et rapide la réplication des données vers un centre de données hors site ou vers un cloud public, vous obtenez les avantages suivants :

- Éliminez les complexités de conception et les erreurs humaines, et mettez en œuvre un déploiement cohérent et reproductible ainsi que les meilleures pratiques
- Réduisez le temps de configuration de la réplication intercluster, de l'instanciation CVO et de la récupération des bases de données Oracle
- Augmenter la productivité des administrateurs de bases de données, de systèmes et de stockage
- Fournit un flux de travail de récupération de base de données pour faciliter le test d'un scénario DR.

NetApp fournit aux clients des modules et des rôles Ansible validés pour accélérer le déploiement, la configuration et la gestion du cycle de vie de votre environnement de base de données Oracle. Cette solution fournit des instructions et un code de playbook Ansible pour vous aider à :

Réplication sur site vers sur site

- Créer des LIF intercluster sur la source et la destination
- Établir un peering de cluster et de serveur virtuel
- Créer et initialiser SnapMirror des volumes Oracle
- Créez un calendrier de réplication via AWX/Tower pour les binaires, les bases de données et les journaux Oracle
- Restaurer la base de données Oracle sur la destination et mettre la base de données en ligne

Sur site vers CVO dans AWS

- Créer un connecteur AWS
- Créer une instance CVO dans AWS
- Ajouter un cluster sur site à Cloud Manager
- Créer des LIF intercluster sur la source
- Établir un peering de cluster et de serveur virtuel
- Créer et initialiser SnapMirror des volumes Oracle
- Créez un calendrier de réplication via AWX/Tower pour les binaires, les bases de données et les journaux

Oracle

- Restaurer la base de données Oracle sur la destination et mettre la base de données en ligne

Une fois que vous êtes prêt, cliquez sur"ici pour commencer avec la solution" .

Commencer

Cette solution a été conçue pour être exécutée dans un environnement AWX/Tower.

AWX/Tour

Pour les environnements AWX/Tower, vous êtes guidé dans la création d'un inventaire de votre gestion de cluster ONTAP et de votre serveur Oracle (adresses IP et noms d'hôte), la création d'informations d'identification, la configuration d'un projet qui extrait le code Ansible de NetApp Automation Github et le modèle de travail qui lance l'automatisation.

1. La solution a été conçue pour fonctionner dans un scénario de cloud privé (sur site vers sur site) et de cloud hybride (sur site vers cloud public Cloud Volumes ONTAP [CVO])
2. Remplissez les variables spécifiques à votre environnement, puis copiez-collez-les dans les champs Variables supplémentaires de votre modèle de travail.
3. Une fois les variables supplémentaires ajoutées à votre modèle de travail, vous pouvez lancer l'automatisation.
4. L'automatisation est configurée pour être exécutée en trois phases (configuration, planification de réplication pour les binaires Oracle, base de données, journaux et planification de réplication uniquement pour les journaux) et une quatrième phase pour récupérer la base de données sur un site DR.
5. Pour obtenir des instructions détaillées sur l'obtention des clés et des jetons nécessaires à la protection des données CVO, visitez"Rassembler les prérequis pour les déploiements CVO et Connector"

Exigences

Sur site

Environnement	Exigences
Environnement Ansible	AWX/Tour
	Ansible v.2.10 et supérieur
	Python 3
	Bibliothèques Python - netapp-lib - xmltodict - jmespath
* ONTAP*	ONTAP version 9.8 +
	Deux agrégats de données
	NFS vlan et ifgrp créés
Serveur(s) Oracle	RHEL 7/8
	Oracle Linux 7/8
	Interfaces réseau pour NFS, gestion publique et facultative
	Environnement Oracle existant sur la source et système d'exploitation Linux équivalent sur la destination (site DR ou cloud public)

CVO

Environnement	Exigences
Environnement Ansible	AWX/Tour
	Ansible v.2.10 et supérieur
	Python 3
	Bibliothèques Python - netapp-lib - xmltodict - jmespath
* ONTAP*	ONTAP version 9.8 +
	Deux agrégats de données
	NFS vlan et ifgrp créés
Serveur(s) Oracle	RHEL 7/8
	Oracle Linux 7/8
	Interfaces réseau pour NFS, gestion publique et facultative
	Environnement Oracle existant sur la source et système d'exploitation Linux équivalent sur la destination (site DR ou cloud public)
	Définissez un espace de swap approprié sur l'instance Oracle EC2. Par défaut, certaines instances EC2 sont déployées avec 0 swap.
Gestionnaire de cloud/AWS	Accès AWS/Clé secrète
	Compte NetApp Cloud Manager
	Jeton d'actualisation de NetApp Cloud Manager
	Ajouter des LIF intercluster source au groupe de sécurité AWS

Détails de l’automatisation

Sur site

Ce déploiement automatisé est conçu avec un seul playbook Ansible composé de trois rôles distincts. Les rôles sont destinés aux configurations ONTAP, Linux et Oracle. Le tableau suivant décrit les tâches qui sont automatisées.

Manuel de jeu	Tâches
ontap_setup	Pré-vérification de l'environnement ONTAP
	Création de LIF intercluster sur le cluster source (FACULTATIF)
	Création de LIF intercluster sur le cluster de destination (FACULTATIF)
	Création de cluster et peering SVM
	Création du SnapMirror de destination et initialisation des volumes Oracle désignés
ora_replication_cg	Activer le mode de sauvegarde pour chaque base de données dans /etc/oratab
	Capture instantanée des volumes binaires et de base de données Oracle
	Snapmirror mis à jour
	Désactiver le mode de sauvegarde pour chaque base de données dans /etc/oratab
ora_replication_log	Changer le journal actuel pour chaque base de données dans /etc/oratab
	Instantané pris du volume du journal Oracle
	Snapmirror mis à jour
ora_recovery	Briser SnapMirror
	Activer NFS et créer un chemin de jonction pour les volumes Oracle sur la destination
	Configurer l'hôte Oracle DR
	Monter et vérifier les volumes Oracle
	Récupérer et démarrer la base de données Oracle

CVO

Ce déploiement automatisé est conçu avec un seul playbook Ansible composé de trois rôles distincts. Les rôles sont destinés aux configurations ONTAP, Linux et Oracle. Le tableau suivant décrit les tâches qui sont automatisées.

Manuel de jeu	Tâches
cvo_setup	Pré-vérification de l'environnement
	Configuration AWS/ID de clé d'accès AWS/Clé secrète/Région par défaut
	Création d'un rôle AWS
	Création d'une instance NetApp Cloud Manager Connector dans AWS
	Création d'une instance Cloud Volumes ONTAP (CVO) dans AWS
	Ajouter un cluster ONTAP source sur site à NetApp Cloud Manager
	Création du SnapMirror de destination et initialisation des volumes Oracle désignés
ora_replication_cg	Activer le mode de sauvegarde pour chaque base de données dans /etc/oratab
	Capture instantanée des volumes binaires et de base de données Oracle
	Snapmirror mis à jour
	Désactiver le mode de sauvegarde pour chaque base de données dans /etc/oratab
ora_replication_log	Changer le journal actuel pour chaque base de données dans /etc/oratab
	Instantané pris du volume du journal Oracle
	Snapmirror mis à jour
ora_recovery	Briser SnapMirror
	Activer NFS et créer un chemin de jonction pour les volumes Oracle sur le CVO de destination
	Configurer l'hôte Oracle DR
	Monter et vérifier les volumes Oracle
	Récupérer et démarrer la base de données Oracle

Paramètres par défaut

Pour simplifier l'automatisation, nous avons prédéfini de nombreux paramètres Oracle requis avec des valeurs par défaut. Il n'est généralement pas nécessaire de modifier les paramètres par défaut pour la plupart des déploiements. Un utilisateur plus avancé peut apporter des modifications aux paramètres par défaut avec prudence. Les paramètres par défaut se trouvent dans chaque dossier de rôle sous le répertoire par défaut.

Licence

Vous devez lire les informations de licence telles qu'indiquées dans le référentiel Github. En accédant, en téléchargeant, en installant ou en utilisant le contenu de ce référentiel, vous acceptez les termes de la licence énoncée"ici" .

Veuillez noter qu'il existe certaines restrictions concernant la production et/ou le partage d'œuvres dérivées du contenu de ce référentiel. Veuillez vous assurer de lire les conditions de l'"Licence" avant d'utiliser le contenu. Si vous n'acceptez pas toutes les conditions, n'accédez pas, ne téléchargez pas et n'utilisez pas le contenu de ce référentiel.

Une fois que vous êtes prêt, cliquez sur"ici pour les procédures détaillées AWX/Tower" .

Procédure de déploiement étape par étape

Cette page décrit la protection automatisée des données d'Oracle19c sur le stockage NetApp ONTAP .

Protection des données Oracle AWX/Tower

Créez l'inventaire, le groupe, les hôtes et les informations d'identification pour votre environnement

Cette section décrit la configuration de l'inventaire, des groupes, des hôtes et des informations d'identification d'accès dans AWX/Ansible Tower qui préparent l'environnement pour la consommation de solutions automatisées NetApp .

1. Configurer l'inventaire.
    a. Accédez à Ressources → Inventaires → Ajouter, puis cliquez sur Ajouter un inventaire.
    b. Indiquez le nom et les détails de l'organisation, puis cliquez sur Enregistrer.
    c. Sur la page Inventaires, cliquez sur l'inventaire créé.
    d. Accédez au sous-menu Groupes et cliquez sur Ajouter.
    e. Indiquez le nom Oracle de votre premier groupe et cliquez sur Enregistrer.
    f. Répétez le processus pour un deuxième groupe appelé dr_oracle.
    g. Sélectionnez le groupe Oracle créé, accédez au sous-menu Hôtes et cliquez sur Ajouter un nouvel hôte.
    h. Fournissez l'adresse IP de l'adresse IP de gestion de l'hôte Oracle source, puis cliquez sur Enregistrer.
    i. Ce processus doit être répété pour le groupe dr_oracle et ajouter l'adresse IP/le nom d'hôte de gestion de l'hôte Oracle DR/Destination.

Vous trouverez ci-dessous des instructions pour créer les types d'informations d'identification et les informations d'identification pour On-Prem avec ONTAP ou CVO sur AWS.

Sur site

1. Configurer les informations d'identification.
2. Créer des types d'informations d'identification. Pour les solutions impliquant ONTAP, vous devez configurer le type d'informations d'identification pour qu'il corresponde aux entrées de nom d'utilisateur et de mot de passe.
   a. Accédez à Administration → Types d'informations d'identification, puis cliquez sur Ajouter.
   b. Fournissez le nom et la description.
   c. Collez le contenu suivant dans la configuration d'entrée :

```
fields:
  - id: dst_cluster_username
    type: string
    label: Destination Cluster Username
  - id: dst_cluster_password
    type: string
    label: Destination Cluster Password
    secret: true
  - id: src_cluster_username
    type: string
    label: Source Cluster Username
  - id: src_cluster_password
    type: string
    label: Source Cluster Password
    secret: true
```

   d. Collez le contenu suivant dans la configuration de l'injecteur, puis cliquez sur Enregistrer :

```
extra_vars:
  dst_cluster_username: '{{ dst_cluster_username }}'
  dst_cluster_password: '{{ dst_cluster_password }}'
  src_cluster_username: '{{ src_cluster_username }}'
  src_cluster_password: '{{ src_cluster_password }}'
```

3. Créer des informations d'identification pour ONTAP
   a. Accédez à Ressources → Informations d'identification, puis cliquez sur Ajouter.
   b. Saisissez le nom et les détails de l'organisation pour les informations d'identification ONTAP
   c. Sélectionnez le type d'informations d'identification créé à l'étape précédente.
   d. Sous Détails du type, saisissez le nom d'utilisateur et le mot de passe de vos clusters source et de destination.
   e. Cliquez sur Enregistrer
4. Créer des informations d'identification pour Oracle

a. Accédez à Ressources → Informations d'identification, puis cliquez sur Ajouter.
b. Saisissez le nom et les détails de l'organisation pour Oracle
c. Sélectionnez le type d'informations d'identification de la machine.
d. Sous Détails du type, entrez le nom d'utilisateur et le mot de passe des hôtes Oracle.
e. Sélectionnez la méthode d'escalade des privilèges appropriée et entrez le nom d'utilisateur et le mot de passe.
f. Cliquez sur Enregistrer
g. Répétez le processus si nécessaire pour des informations d'identification différentes pour l'hôte dr_oracle.

CVO

1. Configurer les informations d'identification.
2. Créer des types d'informations d'identification. Pour les solutions impliquant ONTAP, vous devez configurer le type d'informations d'identification pour qu'il corresponde aux entrées de nom d'utilisateur et de mot de passe. Nous ajouterons également des entrées pour Cloud Central et AWS.
   a. Accédez à Administration → Types d'informations d'identification, puis cliquez sur Ajouter.
   b. Fournissez le nom et la description.
   c. Collez le contenu suivant dans la configuration d'entrée :

```
fields:
  - id: dst_cluster_username
    type: string
    label: CVO Username
  - id: dst_cluster_password
    type: string
    label: CVO Password
    secret: true
  - id: cvo_svm_password
    type: string
    label: CVO SVM Password
    secret: true
  - id: src_cluster_username
    type: string
    label: Source Cluster Username
  - id: src_cluster_password
    type: string
    label: Source Cluster Password
    secret: true
  - id: regular_id
    type: string
    label: Cloud Central ID
    secret: true
  - id: email_id
    type: string
    label: Cloud Manager Email
    secret: true
  - id: cm_password
    type: string
    label: Cloud Manager Password
    secret: true
  - id: access_key
    type: string
    label: AWS Access Key
    secret: true
  - id: secret_key
    type: string
    label: AWS Secret Key
    secret: true
  - id: token
    type: string
    label: Cloud Central Refresh Token
    secret: true
```

d. Collez le contenu suivant dans la configuration de l'injecteur et cliquez sur Enregistrer :

```
extra_vars:
  dst_cluster_username: '{{ dst_cluster_username }}'
  dst_cluster_password: '{{ dst_cluster_password }}'
  cvo_svm_password: '{{ cvo_svm_password }}'
  src_cluster_username: '{{ src_cluster_username }}'
  src_cluster_password: '{{ src_cluster_password }}'
  regular_id: '{{ regular_id }}'
  email_id: '{{ email_id }}'
  cm_password: '{{ cm_password }}'
  access_key: '{{ access_key }}'
  secret_key: '{{ secret_key }}'
  token: '{{ token }}'
```

3. Créer des informations d'identification pour ONTAP/ CVO / AWS
   a. Accédez à Ressources → Informations d'identification, puis cliquez sur Ajouter.
   b. Saisissez le nom et les détails de l'organisation pour les informations d'identification ONTAP
   c. Sélectionnez le type d'informations d'identification créé à l'étape précédente.
   d. Sous Détails du type, saisissez le nom d'utilisateur et le mot de passe de vos clusters source et CVO, Cloud Central/Manager, AWS Access/Secret Key et Cloud Central Refresh Token.
   e. Cliquez sur Enregistrer
4. Créer des informations d'identification pour Oracle (source)
   a. Accédez à Ressources → Informations d'identification, puis cliquez sur Ajouter.
   b. Saisissez le nom et les détails de l'organisation pour l'hôte Oracle
   c. Sélectionnez le type d'informations d'identification de la machine.
   d. Sous Détails du type, entrez le nom d'utilisateur et le mot de passe des hôtes Oracle.
   e. Sélectionnez la méthode d'escalade des privilèges appropriée et entrez le nom d'utilisateur et le mot de passe.
   f. Cliquez sur Enregistrer
5. Créer des informations d'identification pour la destination Oracle
   a. Accédez à Ressources → Informations d'identification, puis cliquez sur Ajouter.
   b. Saisissez le nom et les détails de l'organisation de l'hôte Oracle DR
   c. Sélectionnez le type d'informations d'identification de la machine.
   d. Sous Détails du type, entrez le nom d'utilisateur (ec2-user ou si vous l'avez modifié par défaut, entrez-le) et la clé privée SSH.
   e. Sélectionnez la méthode d'escalade des privilèges appropriée (sudo) et entrez le nom d'utilisateur et le mot de passe si nécessaire.
   f. Cliquez sur Enregistrer

Créer un projet

1. Accédez à Ressources → Projets et cliquez sur Ajouter.
   a. Saisissez le nom et les détails de l'organisation.
   b. Sélectionnez Git dans le champ Type d'informations d'identification de contrôle de source.
   c. entrer `https://github.com/NetApp-Automation/na_oracle19c_data_protection.git` comme URL de contrôle de source.
   d. Cliquez sur Enregistrer.
   e. Le projet peut avoir besoin d'être synchronisé occasionnellement lorsque le code source change.

Configurer les variables globales

Les variables définies dans cette section s'appliquent à tous les hôtes Oracle, bases de données et au cluster ONTAP .

1. Saisissez vos paramètres spécifiques à l'environnement dans les variables globales intégrées suivantes ou sous la forme de variables.

Les éléments en bleu doivent être modifiés pour correspondre à votre environnement.

Sur site

```
# Oracle Data Protection global user configuration variables
# Ontap env specific config variables
hosts_group: "ontap"
ca_signed_certs: "false"

# Inter-cluster LIF details
src_nodes:
  - "AFF-01"
  - "AFF-02"

dst_nodes:
  - "DR-AFF-01"
  - "DR-AFF-02"

create_source_intercluster_lifs: "yes"

source_intercluster_network_port_details:
  using_dedicated_ports: "yes"
  using_ifgrp: "yes"
  using_vlans: "yes"
  failover_for_shared_individual_ports: "yes"
  ifgrp_name: "a0a"
  vlan_id: "10"
  ports:
    - "e0b"
    - "e0g"
  broadcast_domain: "NFS"
  ipspace: "Default"
  failover_group_name: "iclifs"

source_intercluster_lif_details:
  - name: "icl_1"
    address: "10.0.0.1"
    netmask: "255.255.255.0"
    home_port: "a0a-10"
    node: "AFF-01"
  - name: "icl_2"
    address: "10.0.0.2"
    netmask: "255.255.255.0"
    home_port: "a0a-10"
    node: "AFF-02"

create_destination_intercluster_lifs: "yes"
```

```
destination_intercluster_network_port_details:
  using_dedicated_ports: "yes"
  using_ifgrp: "yes"
  using_vlans: "yes"
  failover_for_shared_individual_ports: "yes"
  ifgrp_name: "a0a"
  vlan_id: "10"
  ports:
    - "e0b"
    - "e0g"
  broadcast_domain: "NFS"
  ipspace: "Default"
  failover_group_name: "iclifs"

destination_intercluster_lif_details:
  - name: "icl_1"
    address: "10.0.0.3"
    netmask: "255.255.255.0"
    home_port: "a0a-10"
    node: "DR-AFF-01"
  - name: "icl_2"
    address: "10.0.0.4"
    netmask: "255.255.255.0"
    home_port: "a0a-10"
    node: "DR-AFF-02"

# Variables for SnapMirror Peering
passphrase: "your-passphrase"

# Source & Destination List
dst_cluster_name: "dst-cluster-name"
dst_cluster_ip: "dst-cluster-ip"
dst_vserver: "dst-vserver"
dst_nfs_lif: "dst-nfs-lif"
src_cluster_name: "src-cluster-name"
src_cluster_ip: "src-cluster-ip"
src_vserver: "src-vserver"

# Variable for Oracle Volumes and SnapMirror Details
cg_snapshot_name_prefix: "oracle"
src_orabinary_vols:
  - "binary_vol"
src_db_vols:
  - "db_vol"
src_archivelog_vols:
  - "log_vol"
```

```
snapmirror_policy: "async_policy_oracle"

# Export Policy Details
export_policy_details:
  name: "nfs_export_policy"
  client_match: "0.0.0.0/0"
  ro_rule: "sys"
  rw_rule: "sys"

# Linux env specific config variables
mount_points:
  - "/u01"
  - "/u02"
  - "/u03"
hugepages_nr: "1234"
redhat_sub_username: "xxx"
redhat_sub_password: "xxx"

# DB env specific install and config variables
recovery_type: "scn"
control_files:
  - "/u02/oradata/CDB2/control01.ctl"
  - "/u03/orareco/CDB2/control02.ctl"
```

CVO

```
############################################
### Ontap env specific config variables ###
############################################

#Inventory group name
#Default inventory group name - "ontap"
#Change only if you are changing the group name either in
inventory/hosts file or in inventory groups in case of AWX/Tower
hosts_group: "ontap"

#CA_signed_certificates (ONLY CHANGE to "true" IF YOU ARE USING CA
SIGNED CERTIFICATES)
ca_signed_certs: "false"

#Names of the Nodes in the Source ONTAP Cluster
src_nodes:
  - "AFF-01"
  - "AFF-02"

#Names of the Nodes in the Destination CVO Cluster
```

```
dst_nodes:
  - "DR-AFF-01"
  - "DR-AFF-02"

#Define whether or not to create intercluster lifs on source cluster
(ONLY CHANGE to "No" IF YOU HAVE ALREADY CREATED THE INTERCLUSTER LIFS)
create_source_intercluster_lifs: "yes"

source_intercluster_network_port_details:
  using_dedicated_ports: "yes"
  using_ifgrp: "yes"
  using_vlans: "yes"
  failover_for_shared_individual_ports: "yes"
  ifgrp_name: "a0a"
  vlan_id: "10"
  ports:
    - "e0b"
    - "e0g"
  broadcast_domain: "NFS"
  ipspace: "Default"
  failover_group_name: "iclifs"

source_intercluster_lif_details:
  - name: "icl_1"
    address: "10.0.0.1"
    netmask: "255.255.255.0"
    home_port: "a0a-10"
    node: "AFF-01"
  - name: "icl_2"
    address: "10.0.0.2"
    netmask: "255.255.255.0"
    home_port: "a0a-10"
    node: "AFF-02"

##########################################
### CVO Deployment Variables ###
##########################################

####### Access Keys Variables ######

# Region where your CVO will be deployed.
region_deploy: "us-east-1"

########### CVO and Connector Vars ########

# AWS Managed Policy required to give permission for IAM role creation.
```

```
aws_policy: "arn:aws:iam::1234567:policy/OCCM"

# Specify your aws role name, a new role is created if one already does
not exist.
aws_role_name: "arn:aws:iam::1234567:policy/OCCM"

# Name your connector.
connector_name: "awx_connector"

# Name of the key pair generated in AWS.
key_pair: "key_pair"

# Name of the Subnet that has the range of IP addresses in your VPC.
subnet: "subnet-12345"

# ID of your AWS secuirty group that allows access to on-prem
resources.
security_group: "sg-123123123"

# You Cloud Manager Account ID.
account: "account-A23123A"

# Name of the your CVO instance
cvo_name: "test_cvo"

# ID of the VPC in AWS.
vpc: "vpc-123123123"

#############################################################################
############################
# Variables for - Add on-prem ONTAP to Connector in Cloud Manager
#############################################################################
############################

# For Federated users, Client ID from API Authentication Section of
Cloud Central to generate access token.
sso_id: "123123123123123123123"

# For regular access with username and password, please specify "pass"
as the connector_access. For SSO users, use "refresh_token" as the
variable.
connector_access: "pass"

#############################################################################
############################
# Variables for SnapMirror Peering
#############################################################################
```

```
##############################
passphrase: "your-passphrase"

#########################################################################
##############################
# Source & Destination List
#########################################################################
##############################
#Please Enter Destination Cluster Name
dst_cluster_name: "dst-cluster-name"

#Please Enter Destination Cluster (Once CVO is Created Add this
Variable to all templates)
dst_cluster_ip: "dst-cluster-ip"

#Please Enter Destination SVM to create mirror relationship
dst_vserver: "dst-vserver"

#Please Enter NFS Lif for dst vserver (Once CVO is Created Add this
Variable to all templates)
dst_nfs_lif: "dst-nfs-lif"

#Please Enter Source Cluster Name
src_cluster_name: "src-cluster-name"

#Please Enter Source Cluster
src_cluster_ip: "src-cluster-ip"

#Please Enter Source SVM
src_vserver: "src-vserver"

#########################################################################
##############################
# Variable for Oracle Volumes and SnapMirror Details
#########################################################################
##############################
#Please Enter Source Snapshot Prefix Name
cg_snapshot_name_prefix: "oracle"

#Please Enter Source Oracle Binary Volume(s)
src_orabinary_vols:
  - "binary_vol"
#Please Enter Source Database Volume(s)
src_db_vols:
  - "db_vol"
#Please Enter Source Archive Volume(s)
```

```
src_archivelog_vols:
  - "log_vol"
#Please Enter Destination Snapmirror Policy
snapmirror_policy: "async_policy_oracle"

###########################################################################
##############################
# Export Policy Details
###########################################################################
##############################
#Enter the destination export policy details (Once CVO is Created Add
this Variable to all templates)
export_policy_details:
  name: "nfs_export_policy"
  client_match: "0.0.0.0/0"
  ro_rule: "sys"
  rw_rule: "sys"

###########################################################################
##############################
### Linux env specific config variables ###
###########################################################################
##############################

#NFS Mount points for Oracle DB volumes
mount_points:
  - "/u01"
  - "/u02"
  - "/u03"

# Up to 75% of node memory size divided by 2mb. Consider how many
databases to be hosted on the node and how much ram to be allocated to
each DB.
# Leave it blank if hugepage is not configured on the host.
hugepages_nr: "1234"

# RedHat subscription username and password
redhat_sub_username: "xxx"
redhat_sub_password: "xxx"

#####################################################
### DB env specific install and config variables ###
#####################################################
#Recovery Type (leave as scn)
recovery_type: "scn"
```

```
#Oracle Control Files
control_files:
  - "/u02/oradata/CDB2/control01.ctl"
  - "/u03/orareco/CDB2/control02.ctl"
```

Manuels d'automatisation

Il y a quatre manuels de jeu distincts qui doivent être exécutés.

1. Manuel de configuration de votre environnement, sur site ou CVO.
2. Manuel de réplication des binaires et des bases de données Oracle selon un calendrier
3. Manuel de réplication des journaux Oracle selon un calendrier
4. Manuel de récupération de votre base de données sur un hôte de destination

Configuration ONTAP/ CVO

[.underline]* Configuration ONTAP et CVO*

Configurer et lancer le modèle de tâche.

1. Créez le modèle de travail.
   a. Accédez à Ressources → Modèles → Ajouter et cliquez sur Ajouter un modèle de travail.
   b. Entrez le nom ONTAP/CVO Setup
   c. Sélectionnez le type de travail ; Exécuter configure le système en fonction d'un playbook.
   d. Sélectionnez l'inventaire, le projet, le playbook et les informations d'identification correspondants pour le playbook.
   e. Sélectionnez le playbook ontap_setup.yml pour un environnement sur site ou sélectionnez cvo_setup.yml pour la réplication vers une instance CVO.
   f. Collez les variables globales copiées à l'étape 4 dans le champ Variables de modèle sous l'onglet YAML.
   g. Cliquez sur Enregistrer.
2. Lancez le modèle de travail.
   a. Accédez à Ressources → Modèles.
   b. Cliquez sur le modèle souhaité, puis sur Lancer.

   Nous utiliserons ce modèle et le copierons pour les autres playbooks.

Réplication pour les volumes binaires et de base de données

Planification du manuel de réplication binaire et de base de données

Configurer et lancer le modèle de tâche.

1. Copiez le modèle de travail précédemment créé.
   a. Accédez à Ressources → Modèles.
   b. Recherchez le modèle de configuration ONTAP/ CVO et, à l'extrême droite, cliquez sur Copier le modèle
   c. Cliquez sur Modifier le modèle sur le modèle copié et remplacez le nom par Playbook de réplication binaire et de base de données.
   d. Conservez le même inventaire, le même projet et les mêmes informations d'identification pour le modèle.
   e. Sélectionnez ora_replication_cg.yml comme playbook à exécuter.
   f. Les variables resteront les mêmes, mais l'adresse IP du cluster CVO devra être définie dans la variable dst_cluster_ip.
   g. Cliquez sur Enregistrer.
2. Planifiez le modèle de travail.
   a. Accédez à Ressources → Modèles.
   b. Cliquez sur le modèle Playbook de réplication binaire et de base de données, puis cliquez sur Planifications dans l'ensemble d'options supérieur.

c. Cliquez sur Ajouter, ajoutez le nom de la planification pour la réplication binaire et de base de données, choisissez la date/heure de début au début de l'heure, choisissez votre fuseau horaire local et la fréquence d'exécution. La fréquence d'exécution sera souvent celle à laquelle la réplication SnapMirror sera mise à jour.

> Un calendrier distinct sera créé pour la réplication du volume de journaux, afin qu'il puisse être répliqué à une cadence plus fréquente.

Réplication des volumes de journaux

Planification du manuel de réplication des journaux

Configurer et lancer le modèle de tâche

1. Copiez le modèle de travail précédemment créé.
   a. Accédez à Ressources → Modèles.
   b. Recherchez le modèle de configuration ONTAP/ CVO et, à l'extrême droite, cliquez sur Copier le modèle
   c. Cliquez sur Modifier le modèle sur le modèle copié et remplacez le nom par Playbook de réplication de journaux.
   d. Conservez le même inventaire, le même projet et les mêmes informations d'identification pour le modèle.
   e. Sélectionnez ora_replication_logs.yml comme playbook à exécuter.
   f. Les variables resteront les mêmes, mais l'adresse IP du cluster CVO devra être définie dans la variable dst_cluster_ip.
   g. Cliquez sur Enregistrer.
2. Planifiez le modèle de travail.
   a. Accédez à Ressources → Modèles.
   b. Cliquez sur le modèle Playbook de réplication des journaux, puis sur Planifications dans l'ensemble d'options supérieur.
   c. Cliquez sur Ajouter, ajoutez le nom de la planification pour la réplication du journal, choisissez la date/heure de début au début de l'heure, choisissez votre fuseau horaire local et la fréquence d'exécution. La fréquence d'exécution sera souvent celle à laquelle la réplication SnapMirror sera mise à jour.

> Il est recommandé de définir la planification du journal pour qu'il soit mis à jour toutes les heures afin de garantir la récupération jusqu'à la dernière mise à jour horaire.

Restaurer et récupérer la base de données

Planification du manuel de réplication des journaux

Configurer et lancer le modèle de tâche.

1. Copiez le modèle de travail précédemment créé.
   a. Accédez à Ressources → Modèles.
   b. Recherchez le modèle de configuration ONTAP/ CVO et, à l'extrême droite, cliquez sur Copier le modèle

c. Cliquez sur Modifier le modèle sur le modèle copié et remplacez le nom par Playbook de restauration et de récupération.

d. Conservez le même inventaire, le même projet et les mêmes informations d'identification pour le modèle.

e. Sélectionnez ora_recovery.yml comme playbook à exécuter.

f. Les variables resteront les mêmes, mais l'adresse IP du cluster CVO devra être définie dans la variable dst_cluster_ip.

g. Cliquez sur Enregistrer.

Ce playbook ne sera pas exécuté tant que vous ne serez pas prêt à restaurer votre base de données sur le site distant.

Récupération de la base de données Oracle

1. Les volumes de données des bases de données Oracle de production sur site sont protégés via la réplication NetApp SnapMirror vers un cluster ONTAP redondant dans un centre de données secondaire ou vers Cloud Volume ONTAP dans un cloud public. Dans un environnement de reprise après sinistre entièrement configuré, les instances de calcul de récupération dans un centre de données secondaire ou un cloud public sont en veille et prêtes à récupérer la base de données de production en cas de sinistre. Les instances de calcul de secours sont maintenues synchronisées avec les instances sur site en exécutant des mises à jour parallèles sur le correctif ou la mise à niveau du noyau du système d'exploitation en mode verrouillé.
2. Dans cette solution démontrée, le volume binaire Oracle est répliqué sur la cible et monté sur l'instance cible pour faire apparaître la pile logicielle Oracle. Cette approche pour récupérer Oracle présente un avantage par rapport à une nouvelle installation d'Oracle à la dernière minute lorsqu'un sinistre survient. Il garantit que l'installation d'Oracle est entièrement synchronisée avec l'installation actuelle du logiciel de production sur site et les niveaux de correctifs, etc. Cependant, cela peut ou non avoir des implications supplémentaires en matière de licence logicielle pour le volume binaire Oracle répliqué sur le site de récupération, en fonction de la manière dont la licence logicielle est structurée avec Oracle. Il est recommandé à l'utilisateur de vérifier auprès de son personnel chargé des licences logicielles afin d'évaluer les exigences potentielles en matière de licences Oracle avant de décider d'utiliser la même approche.
3. L'hôte Oracle de secours à la destination est configuré avec les configurations prérequises Oracle.
4. Les SnapMirrors sont cassés et les volumes sont rendus accessibles en écriture et montés sur l'hôte Oracle de secours.
5. Le module de récupération Oracle exécute les tâches suivantes pour récupérer et démarrer Oracle sur le site de récupération une fois que tous les volumes de base de données sont montés sur l'instance de calcul de secours.
    a. Synchroniser le fichier de contrôle : nous avons déployé des fichiers de contrôle Oracle en double sur différents volumes de base de données pour protéger le fichier de contrôle de base de données critique. L'un concerne le volume de données et l'autre le volume de journaux. Étant donné que les volumes de données et de journaux sont répliqués à des fréquences différentes, ils ne seront pas synchronisés au moment de la récupération.
    b. Relier le binaire Oracle : étant donné que le binaire Oracle est déplacé vers un nouvel hôte, il a besoin d'une nouvelle liaison.
    c. Récupérer la base de données Oracle : le mécanisme de récupération récupère le dernier numéro de modification du système dans le dernier journal archivé disponible dans le volume de journal Oracle à partir du fichier de contrôle et récupère la base de données Oracle pour récupérer toutes les

transactions commerciales qui ont pu être répliquées sur le site DR au moment de la panne. La base de données est ensuite démarrée dans une nouvelle incarnation pour effectuer les connexions utilisateur et les transactions commerciales sur le site de récupération.

Avant d'exécuter le playbook de récupération, assurez-vous de disposer des éléments suivants : Assurez-vous de copier les fichiers /etc/oratab et /etc/oraInst.loc de l'hôte Oracle source vers l'hôte de destination.