Protección automatizada de datos de Oracle

NetApp database solutions

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/es-es/netapp-solutions-databases/automation/db-protection-overview.html on August 18, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Protección automatizada de datos de Oracle . . . 1
- Descripción general de la solución . . . 1
  - Protección de datos automatizada para bases de datos Oracle . . . 1
- Empezando . . . 2
  - AWX/Torre . . . 2
  - Requisitos . . . 2
  - Detalles de la automatización . . . 4
  - Parámetros predeterminados . . . 6
  - Licencia . . . 6
- Procedimiento de implementación paso a paso . . . 7
  - AWX/Torre Protección de datos Oracle . . . 7

Protección automatizada de datos de Oracle

Descripción general de la solución

Esta página describe el método automatizado para implementar Oracle19c en el almacenamiento NetApp ONTAP .

Protección de datos automatizada para bases de datos Oracle

Las organizaciones están automatizando sus entornos para ganar eficiencia, acelerar las implementaciones y reducir el esfuerzo manual. Se están utilizando herramientas de gestión de configuración como Ansible para optimizar las operaciones de bases de datos empresariales. En esta solución, demostramos cómo puede utilizar Ansible para automatizar la protección de datos de Oracle con NetApp ONTAP. Al permitir que los administradores de almacenamiento, administradores de sistemas y DBA configuren de manera consistente y rápida la replicación de datos en un centro de datos externo o en la nube pública, obtiene los siguientes beneficios:

- Elimine las complejidades de diseño y los errores humanos, e implemente una implementación consistente y repetible y las mejores prácticas.
- Disminuya el tiempo de configuración de la replicación entre clústeres, la creación de instancias de CVO y la recuperación de bases de datos de Oracle
- Aumente la productividad de los administradores de bases de datos, sistemas y almacenamiento
- Proporciona un flujo de trabajo de recuperación de base de datos para facilitar la prueba de un escenario de recuperación ante desastres.

NetApp proporciona a los clientes módulos y roles de Ansible validados para acelerar la implementación, la configuración y la gestión del ciclo de vida de su entorno de base de datos Oracle. Esta solución proporciona instrucciones y código de libro de estrategias de Ansible para ayudarle a:

Replicación local a local

- Crear LIF entre clústeres en origen y destino
- Establecer peering entre clústeres y vservidores
- Crear e inicializar SnapMirror de volúmenes de Oracle
- Cree un programa de replicación a través de AWX/Tower para binarios, bases de datos y registros de Oracle
- Restaurar Oracle DB en el destino y poner la base de datos en línea

De local a CVO en AWS

- Crear un conector de AWS
- Crear una instancia de CVO en AWS
- Agregar un clúster local a Cloud Manager
- Crear LIF entre clústeres en la fuente
- Establecer peering entre clústeres y vservidores
- Crear e inicializar SnapMirror de volúmenes de Oracle

- Cree un programa de replicación a través de AWX/Tower para binarios, bases de datos y registros de Oracle
- Restaurar Oracle DB en el destino y poner la base de datos en línea

Cuando esté listo, haga clic en"Aquí para comenzar con la solución." .

Empezando

Esta solución ha sido diseñada para ejecutarse en un entorno AWX/Tower.

AWX/Torre

Para los entornos AWX/Tower, se le guiará a través de la creación de un inventario de su administración de clústeres ONTAP y del servidor Oracle (IP y nombres de host), la creación de credenciales, la configuración de un proyecto que extrae el código Ansible de NetApp Automation Github y la plantilla de trabajo que inicia la automatización.

1. La solución ha sido diseñada para ejecutarse en un escenario de nube privada (local a local) y en una nube híbrida (local a nube pública Cloud Volumes ONTAP [CVO]).
2. Complete las variables específicas de su entorno y cópielas y péguelas en los campos Variables adicionales en su plantilla de trabajo.
3. Una vez que se hayan agregado las variables adicionales a su plantilla de trabajo, puede iniciar la automatización.
4. La automatización se ejecutará en tres fases (configuración, programación de replicación para binarios de Oracle, base de datos, registros y programación de replicación solo para registros) y una cuarta fase para recuperar la base de datos en un sitio de recuperación ante desastres.
5. Para obtener instrucciones detalladas para obtener las claves y tokens necesarios para la Protección de Datos CVO, visite"Recopilar requisitos previos para las implementaciones de CVO y conectores"

Requisitos

En las instalaciones

Ambiente	Requisitos
Entorno Ansible	AWX/Torre
	Ansible v.2.10 y superior
	Python 3
	Bibliotecas de Python: netapp-lib, xmltodict y jmespath
* ONTAP*	Versión 9.8+ de ONTAP
	Dos agregados de datos
	VLAN NFS y grupo IF creados
Servidores Oracle	RHEL 7/8
	Oracle Linux 7/8
	Interfaces de red para NFS, públicas y de gestión opcional
	Entorno Oracle existente en el origen y el sistema operativo Linux equivalente en el destino (sitio de recuperación ante desastres o nube pública)

CVO

Ambiente	Requisitos
Entorno Ansible	AWX/Torre
	Ansible v.2.10 y superior
	Python 3
	Bibliotecas de Python: netapp-lib, xmltodict y jmespath
* ONTAP*	Versión 9.8+ de ONTAP
	Dos agregados de datos
	VLAN NFS y grupo IF creados
Servidores Oracle	RHEL 7/8
	Oracle Linux 7/8
	Interfaces de red para NFS, públicas y de gestión opcional
	Entorno Oracle existente en el origen y el sistema operativo Linux equivalente en el destino (sitio de recuperación ante desastres o nube pública)
	Establezca un espacio de intercambio adecuado en la instancia de Oracle EC2; de manera predeterminada, algunas instancias de EC2 se implementan con 0 espacio de intercambio.
Administrador de la nube/AWS	Clave de acceso/secreta de AWS
	Cuenta de NetApp Cloud Manager
	Token de actualización de NetApp Cloud Manager
	Agregar LIF entre clústeres de origen al grupo de seguridad de AWS

Detalles de la automatización

En las instalaciones

Esta implementación automatizada está diseñada con un único manual de Ansible que consta de tres roles separados. Los roles son para configuraciones de ONTAP, Linux y Oracle. En la siguiente tabla se describen qué tareas se están automatizando.

Manual de estrategias	Tareas
configuración al pulsar	Comprobación previa del entorno ONTAP
	Creación de LIF entre clústeres en el clúster de origen (OPCIONAL)
	Creación de LIF entre clústeres en el clúster de destino (OPCIONAL)
	Creación de clúster y peering SVM
	Creación de SnapMirror de destino e inicialización de volúmenes Oracle designados
ora_replication_cg	Habilitar el modo de copia de seguridad para cada base de datos en /etc/oratab
	Instantánea tomada de volúmenes binarios y de base de datos de Oracle
	Snapmirror actualizado
	Desactivar el modo de copia de seguridad para cada base de datos en /etc/oratab
ora_registro_de_replicación	Cambiar el registro actual de cada base de datos en /etc/oratab
	Instantánea tomada del volumen de registro de Oracle
	Snapmirror actualizado
ora_recovery	Romper SnapMirror
	Habilite NFS y cree una ruta de unión para los volúmenes de Oracle en el destino
	Configurar el host de Oracle de recuperación ante desastres
	Montar y verificar volúmenes de Oracle
	Recuperar e iniciar la base de datos Oracle

CVO

Esta implementación automatizada está diseñada con un único manual de Ansible que consta de tres roles separados. Los roles son para configuraciones de ONTAP, Linux y Oracle. En la siguiente tabla se describen qué tareas se están automatizando.

Manual de estrategias	Tareas
cvo_setup	Comprobación previa del entorno
	AWS Configure/ID de clave de acceso de AWS/Clave secreta/Región predeterminada
	Creación de un rol de AWS
	Creación de una instancia de NetApp Cloud Manager Connector en AWS
	Creación de una instancia de Cloud Volumes ONTAP (CVO) en AWS
	Agregar clúster ONTAP de origen local a NetApp Cloud Manager
	Creación de SnapMirror de destino e inicialización de volúmenes Oracle designados
ora_replication_cg	Habilitar el modo de copia de seguridad para cada base de datos en /etc/oratab
	Instantánea tomada de volúmenes binarios y de base de datos de Oracle
	Snapmirror actualizado
	Desactivar el modo de copia de seguridad para cada base de datos en /etc/oratab
ora_registro_de_replicación	Cambiar el registro actual de cada base de datos en /etc/oratab
	Instantánea tomada del volumen de registro de Oracle
	Snapmirror actualizado
ora_recovery	Romper SnapMirror
	Habilite NFS y cree una ruta de unión para los volúmenes de Oracle en el CVO de destino
	Configurar el host de Oracle de recuperación ante desastres
	Montar y verificar volúmenes de Oracle
	Recuperar e iniciar la base de datos Oracle

Parámetros predeterminados

Para simplificar la automatización, hemos preestablecido muchos parámetros de Oracle requeridos con valores predeterminados. Por lo general, no es necesario cambiar los parámetros predeterminados para la mayoría de las implementaciones. Un usuario más avanzado puede realizar cambios en los parámetros predeterminados con precaución. Los parámetros predeterminados se encuentran en cada carpeta de función, en el directorio de valores predeterminados.

Licencia

Debes leer la información de la licencia tal como se indica en el repositorio de Github. Al acceder, descargar, instalar o utilizar el contenido de este repositorio, usted acepta los términos de la licencia establecida"aquí" .

Tenga en cuenta que existen ciertas restricciones en torno a la producción y/o intercambio de cualquier trabajo derivado del contenido de este repositorio. Asegúrese de leer los términos del"Licencia" antes de utilizar el contenido. Si no está de acuerdo con todos los términos, no acceda, descargue ni utilice el contenido de este repositorio.

Cuando esté listo, haga clic en"Aquí para conocer los procedimientos detallados de AWX/Tower" .

Procedimiento de implementación paso a paso

Esta página describe la protección de datos automatizada de Oracle19c en el almacenamiento NetApp ONTAP .

AWX/Torre Protección de datos Oracle

Cree el inventario, el grupo, los hosts y las credenciales para su entorno

Esta sección describe la configuración del inventario, los grupos, los hosts y las credenciales de acceso en AWX/Ansible Tower que preparan el entorno para consumir soluciones automatizadas de NetApp .

1. Configurar el inventario.
    a. Vaya a Recursos → Inventarios → Agregar y haga clic en Agregar inventario.
    b. Proporcione el nombre y los detalles de la organización y haga clic en Guardar.
    c. En la página Inventarios, haga clic en el inventario creado.
    d. Vaya al submenú Grupos y haga clic en Agregar.
    e. Proporcione el nombre oráculo para su primer grupo y haga clic en Guardar.
    f. Repita el proceso para un segundo grupo llamado dr_oracle.
    g. Seleccione el grupo de Oracle creado, vaya al submenú Hosts y haga clic en Agregar nuevo host.
    h. Proporcione la dirección IP de la IP de administración del host Oracle de origen y haga clic en Guardar.
    i. Este proceso se debe repetir para el grupo dr_oracle y agregar la IP/nombre de host de administración del host Oracle de DR/Destino.

A continuación, se muestran instrucciones para crear los tipos de credenciales y credenciales para On-Prem con ONTAP o CVO en AWS.

En las instalaciones

1. Configurar las credenciales.
2. Crear tipos de credenciales. Para las soluciones que involucran ONTAP, debe configurar el tipo de credencial para que coincida con las entradas de nombre de usuario y contraseña.
   a. Vaya a Administración → Tipos de credenciales y haga clic en Agregar.
   b. Proporcione el nombre y la descripción.
   c. Pegue el siguiente contenido en Configuración de entrada:

```
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. Pegue el siguiente contenido en Configuración del inyector y luego haga clic en Guardar:

```
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. Crear credenciales para ONTAP
   a. Vaya a Recursos → Credenciales y haga clic en Agregar.
   b. Ingrese el nombre y los detalles de la organización para las credenciales de ONTAP
   c. Seleccione el tipo de credencial que se creó en el paso anterior.
   d. En Detalles de tipo, ingrese el nombre de usuario y la contraseña para los clústeres de origen y destino.
   e. Haga clic en Guardar
4. Crear credenciales para Oracle
   a. Vaya a Recursos → Credenciales y haga clic en Agregar.

b. Introduzca el nombre y los detalles de la organización de Oracle

c. Seleccione el tipo de credencial de la máquina.

d. En Detalles de tipo, ingrese el nombre de usuario y la contraseña para los hosts de Oracle.

e. Seleccione el método de escalada de privilegios correcto e ingrese el nombre de usuario y la contraseña.

f. Haga clic en Guardar

g. Repita el proceso si es necesario para una credencial diferente para el host dr_oracle.

CVO

1. Configurar las credenciales.
2. Crear tipos de credenciales. Para las soluciones que involucran ONTAP, debe configurar el tipo de credencial para que coincida con las entradas de nombre de usuario y contraseña; también agregaremos entradas para Cloud Central y AWS.
   a. Vaya a Administración → Tipos de credenciales y haga clic en Agregar.
   b. Proporcione el nombre y la descripción.
   c. Pegue el siguiente contenido en Configuración de entrada:

```
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. Pegue el siguiente contenido en Configuración del inyector y haga clic en Guardar:

```
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. Crear credenciales para ONTAP/CVO/AWS
   a. Vaya a Recursos → Credenciales y haga clic en Agregar.
   b. Ingrese el nombre y los detalles de la organización para las credenciales de ONTAP
   c. Seleccione el tipo de credencial que se creó en el paso anterior.
   d. En Detalles de tipo, ingrese el nombre de usuario y la contraseña para sus clústeres de origen y CVO, Cloud Central/Manager, clave secreta/de acceso de AWS y token de actualización de Cloud Central.
   e. Haga clic en Guardar
4. Crear credenciales para Oracle (Fuente)
   a. Vaya a Recursos → Credenciales y haga clic en Agregar.
   b. Ingrese el nombre y los detalles de la organización para el host de Oracle
   c. Seleccione el tipo de credencial de la máquina.
   d. En Detalles de tipo, ingrese el nombre de usuario y la contraseña para los hosts de Oracle.
   e. Seleccione el método de escalada de privilegios correcto e ingrese el nombre de usuario y la contraseña.
   f. Haga clic en Guardar
5. Crear credenciales para Oracle Destination
   a. Vaya a Recursos → Credenciales y haga clic en Agregar.
   b. Ingrese el nombre y los detalles de la organización para el host de Oracle de recuperación ante desastres
   c. Seleccione el tipo de credencial de la máquina.
   d. En Detalles de tipo, ingrese el nombre de usuario (ec2-user o si lo ha cambiado del predeterminado, introdúzcalo) y la clave privada SSH.
   e. Seleccione el método de escalada de privilegios correcto (sudo) e ingrese el nombre de usuario y la contraseña si es necesario.
   f. Haga clic en Guardar

Crear un proyecto

1. Vaya a Recursos → Proyectos y haga clic en Agregar.
   a. Introduzca el nombre y los detalles de la organización.
   b. Seleccione Git en el campo Tipo de credencial de control de fuente.
   c. ingresar `https://github.com/NetApp-Automation/na_oracle19c_data_protection.git` como la URL de control de origen.
   d. Haga clic en Guardar.
   e. Es posible que el proyecto necesite sincronizarse ocasionalmente cuando cambie el código fuente.

Configurar variables globales

Las variables definidas en esta sección se aplican a todos los hosts, bases de datos y el clúster ONTAP de Oracle.

1. Ingrese los parámetros específicos de su entorno en el siguiente formato de variables o variables globales integradas.

Los elementos en azul deben cambiarse para que coincidan con su entorno.

En las instalaciones

```
# 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"
```

Manuales de automatización

Hay cuatro manuales de estrategias diferentes que deben ejecutarse.

1. Manual para configurar su entorno, local o CVO.
2. Manual para replicar binarios y bases de datos de Oracle según un cronograma
3. Manual para replicar registros de Oracle según un cronograma
4. Manual para recuperar su base de datos en un host de destino

Configuración de ONTAP/CVO

Configuración de ONTAP y CVO

Configurar y ejecutar la plantilla de trabajo.

1. Crear la plantilla de trabajo.
   a. Vaya a Recursos → Plantillas → Agregar y haga clic en Agregar plantilla de trabajo.
   b. Introduzca el nombre ONTAP/CVO Setup
   c. Seleccione el tipo de trabajo; Ejecutar configura el sistema según un libro de estrategias.
   d. Seleccione el inventario, el proyecto, el libro de jugadas y las credenciales correspondientes para el libro de jugadas.
   e. Seleccione el libro de estrategias ontap_setup.yml para un entorno local o seleccione cvo_setup.yml para replicar a una instancia CVO.
   f. Pegue las variables globales copiadas del paso 4 en el campo Variables de plantilla debajo de la pestaña YAML.
   g. Haga clic en Guardar.
2. Iniciar la plantilla de trabajo.
   a. Vaya a Recursos → Plantillas.
   b. Haga clic en la plantilla deseada y luego haga clic en Iniciar.

Usaremos esta plantilla y la copiaremos para los otros manuales.

Replicación para volúmenes binarios y de bases de datos

Programación del manual de replicación binaria y de base de datos

Configurar y ejecutar la plantilla de trabajo.

1. Copiar la plantilla de trabajo creada anteriormente.
   a. Vaya a Recursos → Plantillas.
   b. Busque la plantilla de configuración de ONTAP/CVO y, en el extremo derecho, haga clic en Copiar plantilla
   c. Haga clic en Editar plantilla en la plantilla copiada y cambie el nombre a Manual de replicación binaria y de base de datos.
   d. Mantenga el mismo inventario, proyecto y credenciales para la plantilla.
   e. Seleccione ora_replication_cg.yml como el libro de estrategias que se ejecutará.
   f. Las variables seguirán siendo las mismas, pero será necesario configurar la IP del clúster CVO en la variable dst_cluster_ip.
   g. Haga clic en Guardar.
2. Programe la plantilla de trabajo.
   a. Vaya a Recursos → Plantillas.
   b. Haga clic en la plantilla Manual de replicación binaria y de base de datos y, a continuación, haga clic en Programaciones en el conjunto superior de opciones.

c. Haga clic en Agregar, agregue Programación de nombres para replicación binaria y de base de datos, elija la fecha/hora de inicio al comienzo de la hora, elija su zona horaria local y la frecuencia de ejecución. La frecuencia de ejecución será la misma con la que se actualizará la replicación de SnapMirror .

> Se creará una programación separada para la replicación del volumen de registro, de modo que pueda replicarse con una cadencia más frecuente.

Replicación para volúmenes de registro

Programación del manual de replicación de registros

Configurar y ejecutar la plantilla de trabajo

1. Copiar la plantilla de trabajo creada anteriormente.
   a. Vaya a Recursos → Plantillas.
   b. Busque la plantilla de configuración de ONTAP/CVO y, en el extremo derecho, haga clic en Copiar plantilla
   c. Haga clic en Editar plantilla en la plantilla copiada y cambie el nombre a Manual de replicación de registros.
   d. Mantenga el mismo inventario, proyecto y credenciales para la plantilla.
   e. Seleccione ora_replication_logs.yml como el libro de estrategias que se ejecutará.
   f. Las variables seguirán siendo las mismas, pero será necesario configurar la IP del clúster CVO en la variable dst_cluster_ip.
   g. Haga clic en Guardar.
2. Programe la plantilla de trabajo.
   a. Vaya a Recursos → Plantillas.
   b. Haga clic en la plantilla Manual de replicación de registros y luego haga clic en Programaciones en el conjunto superior de opciones.
   c. Haga clic en Agregar, agregue Nombre Programa para Replicación de Registro, elija la Fecha/hora de Inicio al comienzo de la hora, elija su Zona horaria local y la Frecuencia de ejecución. La frecuencia de ejecución será la misma con la que se actualizará la replicación de SnapMirror .

> Se recomienda configurar la programación del registro para que se actualice cada hora para garantizar la recuperación a la última actualización por hora.

Restaurar y recuperar la base de datos

Programación del manual de replicación de registros

Configurar y ejecutar la plantilla de trabajo.

1. Copiar la plantilla de trabajo creada anteriormente.
   a. Vaya a Recursos → Plantillas.
   b. Busque la plantilla de configuración de ONTAP/CVO y, en el extremo derecho, haga clic en Copiar plantilla

c. Haga clic en Editar plantilla en la plantilla copiada y cambie el nombre a Manual de restauración y recuperación.

d. Mantenga el mismo inventario, proyecto y credenciales para la plantilla.

e. Seleccione ora_recovery.yml como el libro de estrategias que se ejecutará.

f. Las variables seguirán siendo las mismas, pero será necesario configurar la IP del clúster CVO en la variable dst_cluster_ip.

g. Haga clic en Guardar.

Este manual no se ejecutará hasta que esté listo para restaurar su base de datos en el sitio remoto.

Recuperación de la base de datos Oracle

1. Los volúmenes de datos de bases de datos Oracle de producción local están protegidos a través de la replicación de NetApp SnapMirror en un clúster ONTAP redundante en un centro de datos secundario o en Cloud Volume ONTAP en la nube pública. En un entorno de recuperación ante desastres completamente configurado, las instancias de cómputo de recuperación en el centro de datos secundario o en la nube pública están en espera y listas para recuperar la base de datos de producción en caso de un desastre. Las instancias de cómputo en espera se mantienen sincronizadas con las instancias locales ejecutando actualizaciones paralelas en el parche o actualización del kernel del sistema operativo al unísono.
2. En esta solución demostrada, el volumen binario de Oracle se replica en el destino y se monta en la instancia de destino para activar la pila de software de Oracle. Este enfoque para recuperar Oracle tiene ventajas sobre una nueva instalación de Oracle en el último minuto cuando ocurre un desastre. Garantiza que la instalación de Oracle esté completamente sincronizada con la instalación del software de producción local actual y los niveles de parches, etc. Sin embargo, esto puede tener o no implicaciones adicionales en la licencia de software para el volumen binario de Oracle replicado en el sitio de recuperación dependiendo de cómo esté estructurada la licencia de software con Oracle. Se recomienda al usuario consultar con su personal de licencias de software para evaluar los posibles requisitos de licencia de Oracle antes de decidir utilizar el mismo enfoque.
3. El host Oracle en espera en el destino está configurado con las configuraciones de requisitos previos de Oracle.
4. Los SnapMirrors están dañados y los volúmenes se pueden escribir y montar en el host Oracle en espera.
5. El módulo de recuperación de Oracle realiza las siguientes tareas para recuperar e iniciar Oracle en el sitio de recuperación después de que todos los volúmenes de base de datos se hayan montado en la instancia de cómputo en espera.
    a. Sincronizar el archivo de control: implementamos archivos de control de Oracle duplicados en diferentes volúmenes de base de datos para proteger el archivo de control de base de datos crítico. Uno está en el volumen de datos y otro en el volumen de registro. Dado que los volúmenes de datos y registros se replican con diferentes frecuencias, no estarán sincronizados en el momento de la recuperación.
    b. Volver a vincular el binario de Oracle: dado que el binario de Oracle se reubica en un nuevo host, necesita volver a vincularse.
    c. Recuperar la base de datos de Oracle: el mecanismo de recuperación recupera el último número de cambio del sistema en el último registro archivado disponible en el volumen de registro de Oracle desde el archivo de control y recupera la base de datos de Oracle para recuperar todas las transacciones comerciales que se pudieron replicar en el sitio de recuperación ante desastres en el momento de la falla. Luego, la base de datos se inicia en una nueva encarnación para continuar las conexiones de los usuarios y las transacciones comerciales en el sitio de recuperación.

Antes de ejecutar el libro de estrategias de recuperación, asegúrese de tener lo siguiente: Asegúrese de copiar /etc/oratab y /etc/oraInst.loc desde el host de Oracle de origen al host de destino

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.