Protezione automatica dei dati Oracle

NetApp Solutions

NetApp
April 26, 2024

Sommario

Panoramica della soluzione 1
Protezione automatica dei dati per database Oracle 1
Per iniziare 2
Procedura di implementazione passo-passo 7

Panoramica della soluzione

Protezione automatica dei dati per database Oracle

Le organizzazioni stanno automatizzando i propri ambienti per ottenere efficienze, accelerare le implementazioni e ridurre l'impegno manuale. I tool di gestione della configurazione come Ansible vengono utilizzati per ottimizzare le operazioni dei database aziendali. In questa soluzione, dimostreremo come utilizzare Ansible per automatizzare la protezione dei dati di Oracle con NetApp ONTAP. Consentendo agli amministratori dello storage, agli amministratori di sistema e ai DBA di configurare in modo rapido e coerente la replica dei dati in un data center offsite o nel cloud pubblico, otterrete i seguenti vantaggi:

- Elimina le complessità di progettazione e gli errori umani e implementa un'implementazione coerente e ripetibile e Best practice
- Riduzione dei tempi di configurazione della replica Intercluster, dell'istanza CVO e del ripristino dei database Oracle
- Aumenta la produttività di amministratori di database, sistemi e amministratori dello storage
- Fornisce un workflow di recovery del database per semplificare il test di uno scenario di DR.

NetApp offre ai clienti i moduli e i ruoli Ansible validati per accelerare l'implementazione, la configurazione e la gestione del ciclo di vita del tuo ambiente di database Oracle. Questa soluzione fornisce istruzioni e codice del playbook Ansible per aiutarti a:

On Prem to on premise Replication

- Creare Lifs di intercluster su origine e destinazione
- Stabilire il peering di cluster e vserver
- Creare e inizializzare SnapMirror dei volumi Oracle
- Creare una pianificazione di replica tramite AWX/Tower per file binari, database e registri Oracle
- Ripristinare Oracle DB sulla destinazione e portare il database online

On Prem to CVO in AWS

- Creare AWS Connector
- Creare un'istanza CVO in AWS
- Aggiungere il cluster on-premise a Cloud Manager
- Creazione di lifs tra cluster sull'origine
- Stabilire il peering di cluster e vserver
- Creare e inizializzare SnapMirror dei volumi Oracle
- Creare una pianificazione di replica tramite AWX/Tower per file binari, database e registri Oracle
- Ripristinare Oracle DB sulla destinazione e portare il database online

Una volta pronti, fare clic su "qui per iniziare con la soluzione".

Per iniziare

Questa soluzione è stata progettata per essere eseguita in un ambiente AWX/Tower.

AWX/Tower

Per gli ambienti AWX/tower, viene fornita una guida alla creazione di un inventario della gestione del cluster ONTAP e del server Oracle (IP e nomi host), alla creazione di credenziali, alla configurazione di un progetto che estrae il codice Ansible da NetApp Automation Github e al modello di lavoro che avvia l'automazione.

1. La soluzione è stata progettata per essere eseguita in uno scenario di cloud privato (da on-premise a on-premise) e in un cloud ibrido (da on-premise a cloud pubblico Cloud Volumes ONTAP [CVO])
2. Compilare le variabili specifiche del proprio ambiente, quindi copiarle e incollarle nei campi Extra Vars del modello di lavoro.
3. Una volta aggiunti i var aggiuntivi al modello di lavoro, è possibile avviare l'automazione.
4. L'automazione viene eseguita in tre fasi (Setup, Replication Schedule for Oracle binaries, Database, Logs e Replication Schedule solo per i registri) e una quarta fase per il ripristino del database in un sito DR.
5. Per istruzioni dettagliate su come ottenere le chiavi e i token necessari per la visita CVO Data Protection "Raccogliere i prerequisiti per le implementazioni CVO e Connector"

Requisiti

** oN- |**

Ambiente	Requisiti
Ambiente Ansible	AWX/Tower
	Ansible v.2.10 e versioni successive
	Python 3
	Librerie Python - netapp-lib - xmltodict - jmespath
ONTAP	ONTAP versione 9.8 +
	Due aggregati di dati
	VLAN NFS e ifgrp create
Server Oracle	RHEL 7/8
	Oracle Linux 7/8
	Interfacce di rete per NFS, gestione pubblica e opzionale
	Ambiente Oracle esistente on-source e sistema operativo Linux equivalente a destinazione (sito DR o cloud pubblico)

** **

Ambiente	Requisiti
Ambiente Ansible	AWX/Tower
	Ansible v.2.10 e versioni successive
	Python 3
	Librerie Python - netapp-lib - xmltodict - jmespath
ONTAP	ONTAP versione 9.8 +
	Due aggregati di dati
	VLAN NFS e ifgrp create
Server Oracle	
	RHEL 7/8
	Oracle Linux 7/8
	Interfacce di rete per NFS, gestione pubblica e opzionale
	Ambiente Oracle esistente on-source e sistema operativo Linux equivalente a destinazione (sito DR o cloud pubblico)
	Impostare lo spazio di swap appropriato sull’istanza Oracle EC2, per impostazione predefinita alcune istanze EC2 sono implementate con 0 swap
Cloud Manager/AWS	Chiave segreta/accesso AWS
	NetApp Cloud Manager
	Token di aggiornamento di NetApp Cloud Manager

Dettagli sull’automazione

** oN- |**

Questa implementazione automatica è progettata con un singolo playbook Ansible che consiste di tre ruoli separati. I ruoli sono per le configurazioni ONTAP, Linux e Oracle. La seguente tabella descrive le attività automatizzate.

Playbook	Attività
ontap_setup	Verifica preliminare dell'ambiente ONTAP
	Creazione di LIF Intercluster sul cluster di origine (OPZIONALE)
	Creazione di LIF Intercluster sul cluster di destinazione (OPZIONALE)
	Creazione del peering di cluster e SVM
	Creazione di SnapMirror di destinazione e inizializzazione dei volumi Oracle designati
ora_replication_cg	Abilitare la modalità di backup per ogni database in /etc/oratab
	Snapshot dei volumi Oracle Binary e Database
	SnapMirror aggiornato
	Disattivare la modalità di backup per ogni database in /etc/oratab
ora_replication_log	Cambiare il log corrente per ogni database in /etc/oratab
	Snapshot del volume Oracle Log
	SnapMirror aggiornato
ora_recovery	Interrompere SnapMirror
	Abilitare NFS e creare un percorso di giunzione per i volumi Oracle sulla destinazione
	Configurare l'host Oracle DR
	Montare e verificare i volumi Oracle
	Ripristinare e avviare il database Oracle

** **

Questa implementazione automatica è progettata con un singolo playbook Ansible che consiste di tre ruoli separati. I ruoli sono per le configurazioni ONTAP, Linux e Oracle. La seguente tabella descrive le attività automatizzate.

Playbook	Attività
cvo_setup	Verifica preliminare dell'ambiente
	AWS Configure/AWS Access Key ID/Secret Key/Default Region
	Creazione del ruolo AWS
	Creazione dell'istanza di NetApp Cloud Manager Connector in AWS
	Creazione dell'istanza CVO (Cloud Volumes ONTAP) in AWS
	Aggiungere il cluster ONTAP di origine on-premise a NetApp Cloud Manager
	Creazione di SnapMirror di destinazione e inizializzazione dei volumi Oracle designati
ora_replication_cg	Abilitare la modalità di backup per ogni database in /etc/oratab
	Snapshot dei volumi Oracle Binary e Database
	SnapMirror aggiornato
	Disattivare la modalità di backup per ogni database in /etc/oratab
ora_replication_log	Cambiare il log corrente per ogni database in /etc/oratab
	Snapshot del volume Oracle Log
	SnapMirror aggiornato
ora_recovery	Interrompere SnapMirror
	Abilitare NFS e creare un percorso di giunzione per i volumi Oracle sul CVO di destinazione
	Configurare l'host Oracle DR
	Montare e verificare i volumi Oracle
	Ripristinare e avviare il database Oracle

Parametri predefiniti

Per semplificare l'automazione, abbiamo preimpostato molti parametri Oracle richiesti con valori predefiniti. In genere non è necessario modificare i parametri predefiniti per la maggior parte delle implementazioni. Un utente più avanzato può apportare modifiche ai parametri predefiniti con cautela. I parametri predefiniti si trovano in ogni cartella di ruoli nella directory dei valori predefiniti.

Licenza

Leggere le informazioni sulla licenza come indicato nel repository Github. Accedendo, scaricando, installando o utilizzando il contenuto di questo repository, l'utente accetta i termini della licenza stabilita "qui".

Si noti che esistono alcune limitazioni relative alla produzione e/o alla condivisione di qualsiasi opera derivata con il contenuto di questo repository. Leggere attentamente i termini del "Licenza" prima di utilizzare il contenuto. Se non si accettano tutti i termini, non accedere, scaricare o utilizzare il contenuto di questo repository.

Una volta pronti, fare clic su "Qui per le procedure AWX/Tower dettagliate".

Procedura di implementazione passo-passo

Protezione dei dati Oracle AWX/Tower

Crea l'inventario, il gruppo, gli host e le credenziali per il tuo ambiente

Questa sezione descrive la configurazione di inventario, gruppi, host e credenziali di accesso in AWX/Ansible Tower che preparano l'ambiente per l'utilizzo delle soluzioni automatizzate di NetApp.

1. Configurare l'inventario.
   a. Accedere a Resources → Inventories → Add e fare clic su Add Inventory (Aggiungi inventario).
   b. Fornire il nome e i dettagli dell'organizzazione, quindi fare clic su Save (Salva).
   c. Nella pagina Inventories (inventari), fare clic sull'inventario creato.
   d. Accedere al sottomenu Groups (gruppi) e fare clic su Add (Aggiungi).
   e. Fornire il nome oracle per il primo gruppo e fare clic su Save (Salva).
   f. Ripetere la procedura per un secondo gruppo denominato dr_oracle.
   g. Selezionare il gruppo oracle creato, accedere al sottomenu hosts e fare clic su Add New host (Aggiungi nuovo host).
   h. Fornire l'indirizzo IP dell'IP di gestione dell'host Oracle di origine e fare clic su Save (Salva).
   i. Questo processo deve essere ripetuto per il gruppo dr_oracle e deve essere aggiunto l'IP/nome host di gestione dell'host DR/destinazione Oracle.

> Di seguito sono riportate le istruzioni per la creazione dei tipi di credenziale e delle credenziali on-premise con ONTAP o CVO su AWS.

On-Prem

1. Configurare le credenziali.
2. Creare tipi di credenziale. Per le soluzioni che utilizzano ONTAP, è necessario configurare il tipo di credenziale in modo che corrisponda alle voci di nome utente e password.
   a. Accedere a Administration → Credential Types (Amministrazione tipi di credenziali) e fare clic su Add (Aggiungi).
   b. Fornire il nome e la descrizione.
   c. Incollare il seguente contenuto in Input Configuration (Configurazione input):

```
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. Incollare il seguente contenuto in Injector Configuration (Configurazione iniettore), quindi fare clic su Save (Salva):

```
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. Crea credenziale per ONTAP
   a. Accedere a Resources → Credentials (risorse credenziali) e fare clic su Add (Aggiungi).
   b. Immettere il nome e i dettagli dell'organizzazione per le credenziali ONTAP
   c. Selezionare il tipo di credenziale creato nel passaggio precedente.
   d. In Dettagli tipo, immettere il nome utente e la password per i cluster di origine e di destinazione.
   e. Fare clic su Salva
4. Crea credenziale per Oracle

a. Accedere a Resources → Credentials (risorse credenziali) e fare clic su Add (Aggiungi).
b. Immettere il nome e i dettagli dell'organizzazione per Oracle
c. Selezionare il tipo di credenziale Machine.
d. In Dettagli tipo, immettere il nome utente e la password per gli host Oracle.
e. Selezionare il metodo corretto di escalation dei privilegi e immettere il nome utente e la password.
f. Fare clic su Salva
g. Ripetere la procedura se necessario per una credenziale diversa per l'host dr_oracle.

CVO

1. Configurare le credenziali.
2. Creare tipi di credenziale. Per le soluzioni che coinvolgono ONTAP, devi configurare il tipo di credenziale in modo che corrisponda alle voci di nome utente e password, aggiungeremo anche le voci per Cloud Central e AWS.
   a. Accedere a Administration → Credential Types (Amministrazione tipi di credenziali) e fare clic su Add (Aggiungi).
   b. Fornire il nome e la descrizione.
   c. Incollare il seguente contenuto in Input Configuration (Configurazione input):

```
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. Incollare il seguente contenuto in Injector Configuration (Configurazione iniettore) e fare clic su

Save (Salva):

```
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. Crea credenziale per ONTAP/CVO/AWS
   a. Accedere a Resources → Credentials (risorse credenziali) e fare clic su Add (Aggiungi).
   b. Immettere il nome e i dettagli dell'organizzazione per le credenziali ONTAP
   c. Selezionare il tipo di credenziale creato nel passaggio precedente.
   d. In Dettagli tipo, immettere il nome utente e la password per i cluster di origine e CVO, Cloud Central/Manager, AWS Access/Secret Key e Cloud Central Refresh Token.
   e. Fare clic su Salva
4. Crea credenziale per Oracle (origine)
   a. Accedere a Resources → Credentials (risorse credenziali) e fare clic su Add (Aggiungi).
   b. Immettere il nome e i dettagli dell'organizzazione per l'host Oracle
   c. Selezionare il tipo di credenziale Machine.
   d. In Dettagli tipo, immettere il nome utente e la password per gli host Oracle.
   e. Selezionare il metodo corretto di escalation dei privilegi e immettere il nome utente e la password.
   f. Fare clic su Salva
5. Crea credenziale per destinazione Oracle
   a. Accedere a Resources → Credentials (risorse credenziali) e fare clic su Add (Aggiungi).
   b. Inserire il nome e i dettagli dell'organizzazione dell'host Oracle DR
   c. Selezionare il tipo di credenziale Machine.
   d. In Dettagli tipo, immettere il nome utente (ec2-user o se è stato modificato dall'impostazione predefinita) e la chiave privata SSH
   e. Selezionare il metodo corretto di escalation dei privilegi (sudo) e immettere il nome utente e la password, se necessario.
   f. Fare clic su Salva

Creare un progetto

1. Accedere a risorse → progetti e fare clic su Aggiungi.
   a. Inserire il nome e i dettagli dell'organizzazione.
   b. Selezionare Git nel campo Source Control Credential Type (tipo credenziale controllo origine).
   c. invio <https://github.com/NetApp-Automation/na_oracle19c_data_protection.git> Come URL del controllo di origine.
   d. Fare clic su Salva.
   e. Potrebbe essere necessario sincronizzare il progetto occasionalmente quando il codice sorgente cambia.

Configurare le variabili globali

Le variabili definite in questa sezione si applicano a tutti gli host Oracle, ai database e al cluster ONTAP.

1. Inserire i parametri specifici dell'ambiente nel seguente formato vars o variabili globali incorporate.

> Gli elementi in blu devono essere modificati in base all'ambiente in uso.

On-Prem

```yaml
# 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"
```

```yaml
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"
```

Playbook per l'automazione

È necessario eseguire quattro playbook separati.

1. Playbook per la configurazione del tuo ambiente, on-premise o CVO.
2. Playbook per la replica di file binari e database Oracle in base a una pianificazione
3. Playbook per la replica dei registri Oracle in base a una pianificazione
4. Playbook per il ripristino del database su un host di destinazione

Setup ONTAP/CVO

Configurazione ONTAP e CVO

Configurare e avviare il modello di lavoro.

1. Creare il modello di lavoro.
   a. Accedere a risorse → modelli → Aggiungi e fare clic su Aggiungi modello di processo.
   b. Immettere il nome ONTAP/CVO Setup
   c. Selezionare il tipo di lavoro; Esegui consente di configurare il sistema in base a una guida.
   d. Seleziona l'inventario, il progetto, il playbook e le credenziali corrispondenti per il playbook.
   e. Selezionare il playbook ontap_setup.yml per un ambiente on-Prem oppure selezionare cvo_setup.yml per la replica su un'istanza CVO.
   f. Incollare le variabili globali copiate dal passaggio 4 nel campo Template Variables (variabili modello) nella scheda YAML.
   g. Fare clic su Salva.
2. Avviare il modello di lavoro.
   a. Accedere a risorse → modelli.
   b. Fare clic sul modello desiderato, quindi fare clic su Launch (Avvia).

   Utilizzeremo questo modello e lo copieremo per gli altri playbook.

Replica per volumi binari e database

Pianificazione del manuale di replica binario e database

Configurare e avviare il modello di lavoro.

1. Copiare il modello di lavoro creato in precedenza.
   a. Accedere a risorse → modelli.
   b. Individuare il modello di installazione di ONTAP/CVO e fare clic con il pulsante destro del mouse su Copy Template (Copia modello)
   c. Fare clic su Edit Template (Modifica modello) nel modello copiato e modificare il nome in Binary and Database Replication Playbook (Playbook di replica binario e database).
   d. Mantenere lo stesso inventario, progetto e credenziali per il modello.
   e. Selezionare ora_Replication_cg.yml come manuale da eseguire.
   f. Le variabili rimarranno le stesse, ma l'IP del cluster CVO dovrà essere impostato nella variabile dst_cluster_ip.
   g. Fare clic su Salva.
2. Pianificare il modello di lavoro.
   a. Accedere a risorse → modelli.
   b. Fare clic sul modello Playbook di replica binario e database, quindi fare clic su Pianificazioni nella parte superiore del set di opzioni.
   c. Fare clic su Add (Aggiungi), add Name Schedule (Aggiungi pianificazione nome) per la replica binaria e del database, scegliere la data/ora di inizio all'inizio dell'ora, scegliere il fuso orario

locale e la frequenza di esecuzione. La frequenza di esecuzione sarà spesso la replica di SnapMirror verrà aggiornata.

> Verrà creata una pianificazione separata per la replica del volume Log, in modo che possa essere replicata con cadenza più frequente.

Replica per i volumi di log

Pianificazione del Playbook di replica del registro

Configurare e avviare il modello di lavoro.

1. Copiare il modello di lavoro creato in precedenza.
   a. Accedere a risorse → modelli.
   b. Individuare il modello di installazione di ONTAP/CVO e fare clic con il pulsante destro del mouse su Copy Template (Copia modello)
   c. Fare clic su Edit Template (Modifica modello) sul modello copiato e modificare il nome in Log Replication Playbook (Playbook replica registro).
   d. Mantenere lo stesso inventario, progetto e credenziali per il modello.
   e. Selezionare ora_Replication_logs.yml come manuale da eseguire.
   f. Le variabili rimarranno le stesse, ma l'IP del cluster CVO dovrà essere impostato nella variabile dst_cluster_ip.
   g. Fare clic su Salva.
2. Pianificare il modello di lavoro.
   a. Accedere a risorse → modelli.
   b. Fare clic sul modello Log Replication Playbook, quindi fare clic su Schedules (Pianificazioni) nella parte superiore del set di opzioni.
   c. Fare clic su Add (Aggiungi), Add Name Schedule (Aggiungi pianificazione nome) per Log Replication (replica registro), scegliere Start date/time (Data/ora di inizio) all'inizio dell'ora, scegliere il fuso orario locale e la frequenza di esecuzione. La frequenza di esecuzione sarà spesso la replica di SnapMirror verrà aggiornata.

   > Si consiglia di impostare la pianificazione del registro per l'aggiornamento ogni ora, in modo da garantire il ripristino dell'ultimo aggiornamento orario.

Ripristinare e ripristinare il database

Pianificazione del Playbook di replica del registro

Configurare e avviare il modello di lavoro.

1. Copiare il modello di lavoro creato in precedenza.
   a. Accedere a risorse → modelli.
   b. Individuare il modello di installazione di ONTAP/CVO e fare clic con il pulsante destro del mouse su Copy Template (Copia modello)
   c. Fare clic su Edit Template (Modifica modello) sul modello copiato e modificare il nome in Restore and Recovery Playbook (Guida per il ripristino e il ripristino).

d. Mantenere lo stesso inventario, progetto e credenziali per il modello.

e. Selezionare ora_recovery.yml come manuale da eseguire.

f. Le variabili rimarranno le stesse, ma l'IP del cluster CVO dovrà essere impostato nella variabile dst_cluster_ip.

g. Fare clic su Salva.

> Questo manuale non verrà eseguito fino a quando non si sarà pronti a ripristinare il database nel sito remoto.

Ripristino del database Oracle

1. Produzione on-premise i volumi di dati dei database Oracle sono protetti tramite la replica di NetApp SnapMirror su un cluster ONTAP ridondante nel data center secondario o su Cloud Volume ONTAP nel cloud pubblico. In un ambiente di disaster recovery completamente configurato, le istanze di calcolo del recovery nel data center secondario o nel cloud pubblico sono in standby e pronte per il ripristino del database di produzione in caso di disastro. Le istanze di calcolo in standby vengono mantenute in sincronia con le istanze on-premise eseguendo aggiornamenti di paraellel sulla patch del kernel del sistema operativo o aggiornando in un passo di blocco.
2. In questa soluzione dimostrata, il volume binario Oracle viene replicato sulla destinazione e montato sull'istanza di destinazione per richiamare lo stack software Oracle. Questo approccio per il ripristino di Oracle ha un vantaggio rispetto a una nuova installazione di Oracle all'ultimo momento in cui si è verificato un disastro. Garantisce che l'installazione di Oracle sia completamente sincronizzata con l'installazione del software di produzione on-premise, con i livelli di patch e così via Tuttavia, questo potrebbe avere o meno ulteriori implicazioni di licenza software per il volume binario Oracle replicato nel sito di recovery, a seconda di come è strutturato il licensing software con Oracle. Si consiglia all'utente di verificare con il proprio personale addetto alle licenze software per valutare il potenziale requisito di licenza Oracle prima di decidere di utilizzare lo stesso approccio.
3. L'host Oracle di standby nella destinazione viene configurato con le configurazioni dei prerequisiti Oracle.
4. Gli SnapMirror sono rotti e i volumi sono resi scrivibili e montati sull'host Oracle di standby.
5. Il modulo di ripristino Oracle esegue le seguenti attività per il ripristino e l'avvio di Oracle nel sito di ripristino dopo che tutti i volumi DB sono stati montati nell'istanza di calcolo in standby.
   a. Sincronizza il file di controllo: Abbiamo implementato file di controllo Oracle duplicati su diversi volumi di database per proteggere file di controllo critici del database. Uno si trova sul volume di dati e l'altro sul volume di log. Poiché i volumi di dati e log vengono replicati con frequenza diversa, al momento del ripristino non saranno sincronizzati.
   b. Relink Oracle binary: Poiché il binario Oracle viene trasferito in un nuovo host, è necessario un relink.
   c. Ripristino del database Oracle: Il meccanismo di recovery recupera l'ultimo numero di modifica del sistema nell'ultimo log archiviato disponibile nel volume di log Oracle dal file di controllo e ripristina il database Oracle per recuperare tutte le transazioni aziendali che sono state replicate nel sito di DR al momento dell'errore. Il database viene quindi avviato in una nuova incarnazione per portare avanti le connessioni utente e le transazioni di business nel sito di recovery.

> Prima di eseguire il playbook di ripristino, assicurarsi di disporre di quanto segue: Assicurarsi che venga copiato su /etc/oratab e /etc/orainst.loc dall'host Oracle di origine all'host di destinazione