



Protezione automatizzata dei dati Oracle

NetApp database solutions

NetApp
August 18, 2025

Sommario

- Protezione automatizzata dei dati Oracle 1
 - Panoramica della soluzione 1
 - Protezione automatizzata dei dati per i database Oracle 1
 - Iniziare 2
 - AWX/Torre 2
 - Requisiti 2
 - Dettagli di automazione 4
 - Parametri predefiniti 6
 - Licenza 6
 - Procedura di distribuzione passo dopo passo 7
 - AWX/Tower Oracle Protezione dei dati 7

Protezione automatizzata dei dati Oracle

Panoramica della soluzione

Questa pagina descrive il metodo automatizzato per distribuire Oracle19c sullo storage NetApp ONTAP .

Protezione automatizzata dei dati per i database Oracle

Le organizzazioni stanno automatizzando i propri ambienti per aumentare l'efficienza, accelerare le distribuzioni e ridurre lo sforzo manuale. Strumenti di gestione della configurazione come Ansible vengono utilizzati per semplificare le operazioni dei database aziendali. In questa soluzione, dimostriamo come utilizzare Ansible per automatizzare la protezione dei dati di Oracle con NetApp ONTAP. Consentendo agli amministratori di storage, agli amministratori di sistema e agli amministratori di database di configurare in modo rapido e coerente la replica dei dati su un data center esterno o su un cloud pubblico, si ottengono i seguenti vantaggi:

- Eliminare le complessità di progettazione e gli errori umani e implementare una distribuzione coerente e ripetibile e le migliori pratiche
- Ridurre i tempi di configurazione della replicazione Intercluster, dell'istanziamento CVO e del ripristino dei database Oracle
- Aumenta la produttività degli amministratori di database, dei sistemi e degli amministratori di storage
- Fornisce un flusso di lavoro di ripristino del database per semplificare il test di uno scenario DR.

NetApp fornisce ai clienti moduli e ruoli Ansible convalidati per accelerare la distribuzione, la configurazione e la gestione del ciclo di vita del tuo ambiente di database Oracle. Questa soluzione fornisce istruzioni e codice playbook Ansible per aiutarti a:

Replica da locale a locale

- Crea intercluster lifs su origine e destinazione
- Stabilire il cluster e il peering del server virtuale
- Crea e inizializza SnapMirror dei volumi Oracle
- Creare una pianificazione di replicazione tramite AWX/Tower per binari, database e log Oracle
- Ripristinare Oracle DB sulla destinazione e portare il database online

Da On Prem a CVO in AWS

- Crea connettore AWS
- Crea un'istanza CVO in AWS
- Aggiungi cluster On-Prem a Cloud Manager
- Crea intercluster lifs sulla sorgente
- Stabilire il cluster e il peering del server virtuale
- Crea e inizializza SnapMirror dei volumi Oracle
- Creare una pianificazione di replicazione tramite AWX/Tower per binari, database e log Oracle
- Ripristinare Oracle DB sulla destinazione e portare il database online

Quando sei pronto, clicca ["qui per iniziare con la soluzione"](#) .

Iniziare

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

AWX/Torre

Per gli ambienti AWX/Tower, verrai guidato nella creazione di un inventario della gestione del cluster ONTAP e del server Oracle (IP e nomi host), nella creazione delle credenziali, nella configurazione di un progetto che estrae il codice Ansible da NetApp Automation Github e nel modello di lavoro che avvia l'automazione.

1. La soluzione è stata progettata per essere eseguita in uno scenario cloud privato (da locale a locale) e cloud ibrido (da locale a cloud pubblico Cloud Volumes ONTAP [CVO])
2. Compila le variabili specifiche del tuo ambiente, quindi copiale e incollale nei campi Extra Vars nel tuo modello di lavoro.
3. Dopo aver aggiunto le variabili extra al modello di lavoro, è possibile avviare l'automazione.
4. L'automazione è impostata per essere eseguita in tre fasi (installazione, pianificazione della replica per i file binari Oracle, database, registri e pianificazione della replica 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 ["Raccogli i prerequisiti per le distribuzioni CVO e Connector"](#)

Requisiti

<strong class="big">In sede

Ambiente	Requisiti
Ambiente Ansible	AWX/Torre
	Ansible v.2.10 e versioni successive
	Python 3
	Librerie Python - netapp-lib - xmldict - jmespath
* ONTAP*	ONTAP versione 9.8 +
	Due aggregati di dati
	NFS vlan e ifgrp creati
Server Oracle	RHEL 7/8
	Oracle Linux 7/8
	Interfacce di rete per NFS, pubbliche e di gestione facoltativa
	Ambiente Oracle esistente sulla sorgente e sistema operativo Linux equivalente sulla destinazione (sito DR o cloud pubblico)

<strong class="big">CVO

Ambiente	Requisiti
Ambiente Ansible	AWX/Torre
	Ansible v.2.10 e versioni successive
	Python 3
	Librerie Python - netapp-lib - xmldict - jmespath
* ONTAP*	ONTAP versione 9.8 +
	Due aggregati di dati
	NFS vlan e ifgrp creati
Server Oracle	RHEL 7/8
	Oracle Linux 7/8
	Interfacce di rete per NFS, pubbliche e di gestione facoltativa
	Ambiente Oracle esistente sulla sorgente e sistema operativo Linux equivalente sulla destinazione (sito DR o cloud pubblico)
	Imposta lo spazio di swap appropriato sull'istanza Oracle EC2, per impostazione predefinita alcune istanze EC2 vengono distribuite con 0 swap
Gestore cloud/AWS	Chiave di accesso/segreto AWS
	Account NetApp Cloud Manager
	Token di aggiornamento di NetApp Cloud Manager
	Aggiungi lif intercluster di origine al gruppo di sicurezza AWS

In sede

Questa distribuzione automatizzata è progettata con un singolo playbook Ansible composto da tre ruoli separati. I ruoli sono per le configurazioni ONTAP, Linux e Oracle. La tabella seguente descrive quali attività vengono automatizzate.

Manuale di gioco	Compiti
ontap_setup	Pre-controllo dell'ambiente ONTAP
	Creazione di LIF intercluster sul cluster sorgente (FACOLTATIVO)
	Creazione di LIF intercluster sul cluster di destinazione (FACOLTATIVO)
	Creazione di cluster e peering SVM
	Creazione dello SnapMirror di destinazione e inizializzazione dei volumi Oracle designati
ora_replication_cg	Abilita 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	Cambia il registro corrente per ogni database in /etc/oratab
	Istantanea acquisita del volume Oracle Log
	Snapmirror aggiornato
ora_recupero	Interrompi SnapMirror
	Abilita NFS e crea un percorso di giunzione per i volumi Oracle sulla destinazione
	Configurare DR Oracle Host
	Montare e verificare i volumi Oracle
	Ripristina e avvia il database Oracle

CVO

Questa distribuzione automatizzata è progettata con un singolo playbook Ansible composto da tre ruoli separati. I ruoli sono per le configurazioni ONTAP, Linux e Oracle. La tabella seguente descrive quali attività vengono automatizzate.

Manuale di gioco	Compiti
cvo_setup	Pre-controllo dell'ambiente
	Configurazione AWS/ID chiave di accesso AWS/Chiave segreta/Regione predefinita
	Creazione del ruolo AWS
	Creazione dell'istanza di NetApp Cloud Manager Connector in AWS
	Creazione dell'istanza Cloud Volumes ONTAP (CVO) in AWS
	Aggiungi il cluster ONTAP di origine locale a NetApp Cloud Manager
	Creazione dello SnapMirror di destinazione e inizializzazione dei volumi Oracle designati
ora_replication_cg	Abilita 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	Cambia il registro corrente per ogni database in /etc/oratab
	Istantanea acquisita del volume Oracle Log
	Snapmirror aggiornato
ora_recupero	Interrompi SnapMirror
	Abilita NFS e crea un percorso di giunzione per i volumi Oracle sul CVO di destinazione
	Configurare DR Oracle Host
	Montare e verificare i volumi Oracle
	Ripristina e avvia 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 distribuzioni. Un utente più esperto può apportare modifiche ai parametri predefiniti con cautela. I parametri predefiniti si trovano in ogni cartella dei ruoli nella directory defaults.

Licenza

Dovresti leggere le informazioni sulla licenza come indicato nel repository Github. Accedendo, scaricando, installando o utilizzando il contenuto di questo repository, accetti i termini della licenza stabiliti ["Qui"](#).

Si noti che esistono alcune restrizioni relative alla produzione e/o alla condivisione di lavori derivati dai contenuti di questo repository. Si prega di assicurarsi di leggere i termini del ["Licenza"](#) prima di utilizzare il contenuto. Se non accetti tutti i termini, non accedere, scaricare o utilizzare i contenuti di questo repository.

Quando sei pronto, clicca ["qui per le procedure dettagliate AWX/Tower"](#).

Procedura di distribuzione passo dopo passo

Questa pagina descrive la protezione automatizzata dei dati di Oracle19c sullo storage NetApp ONTAP .

AWX/Tower Oracle Protezione dei dati

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 NetApp .

1. Configurare l'inventario.
 - a. Vai su Risorse → Inventari → Aggiungi e fai clic su Aggiungi inventario.
 - b. Inserisci il nome e i dettagli dell'organizzazione, quindi fai clic su Salva.
 - c. Nella pagina Inventari, fare clic sull'inventario creato.
 - d. Vai al sottomenu Gruppi e fai clic su Aggiungi.
 - e. Inserisci il nome Oracle per il tuo primo gruppo e fai clic su Salva.
 - f. Ripetere il procedimento per un secondo gruppo denominato dr_oracle.
 - g. Selezionare il gruppo Oracle creato, andare al sottomenu Host e fare clic su Aggiungi nuovo host.
 - h. Fornire l'indirizzo IP dell'IP di gestione dell'host Oracle di origine e fare clic su Salva.
 - i. Questo processo deve essere ripetuto per il gruppo dr_oracle e aggiungere l'IP/nome host di gestione dell'host Oracle DR/Destination.



Di seguito sono riportate le istruzioni per creare i tipi di credenziali e le credenziali per On-Prem con ONTAP o CVO su AWS.

In sede

1. Configurare le credenziali.
2. Crea tipi di credenziali. Per le soluzioni che coinvolgono ONTAP, è necessario configurare il tipo di credenziale in modo che corrisponda alle voci di nome utente e password.
 - a. Vai su Amministrazione → Tipi di credenziali e fai clic su Aggiungi.
 - b. Fornire il nome e la descrizione.
 - c. Incolla il seguente contenuto nella Configurazione di 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. Incolla il seguente contenuto nella configurazione dell'iniettore e poi fai clic su 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 credenziali per ONTAP
 - a. Vai su Risorse → Credenziali e fai clic su Aggiungi.
 - b. Inserisci 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 credenziali per Oracle
 - a. Vai su Risorse → Credenziali e fai clic su Aggiungi.
 - b. Inserisci il nome e i dettagli dell'organizzazione per Oracle

- c. Selezionare il tipo di credenziale Macchina.
- d. In Dettagli tipo, immettere il nome utente e la password per gli host Oracle.
- e. Selezionare il metodo di escalation dei privilegi corretto e immettere nome utente e password.
- f. Fare clic su Salva
- g. Se necessario, ripetere il processo per una credenziale diversa per l'host dr_oracle.

CVO

1. Configurare le credenziali.
2. Creare tipi di credenziali. Per le soluzioni che coinvolgono ONTAP, è necessario configurare il tipo di credenziale in modo che corrisponda alle voci di nome utente e password; aggiungeremo anche voci per Cloud Central e AWS.
 - a. Vai su Amministrazione → Tipi di credenziali e fai clic su Aggiungi.
 - b. Fornire il nome e la descrizione.
 - c. Incolla il seguente contenuto nella Configurazione di 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. Incolla il seguente contenuto nella configurazione dell'iniettore e fai clic su 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 credenziali per ONTAP/CVO/AWS

- a. Vai su Risorse → Credenziali e fai clic su Aggiungi.
- b. Inserisci 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, inserisci il nome utente e la password per i cluster di origine e CVO, Cloud Central/Manager, la chiave di accesso/segreta AWS e il token di aggiornamento Cloud Central.
- e. Fare clic su Salva

4. Crea credenziali per Oracle (fonte)

- a. Vai su Risorse → Credenziali e fai clic su Aggiungi.
- b. Inserisci il nome e i dettagli dell'organizzazione per l'host Oracle
- c. Selezionare il tipo di credenziale Macchina.
- d. In Dettagli tipo, immettere il nome utente e la password per gli host Oracle.
- e. Selezionare il metodo di escalation dei privilegi corretto e immettere nome utente e password.
- f. Fare clic su Salva

5. Crea credenziali per la destinazione Oracle

- a. Vai su Risorse → Credenziali e fai clic su Aggiungi.
- b. Immettere il nome e i dettagli dell'organizzazione per l'host Oracle DR
- c. Selezionare il tipo di credenziale Macchina.
- d. In Dettagli tipo, inserisci il nome utente (ec2-user o se lo hai modificato rispetto al valore predefinito inseriscilo) e la chiave privata SSH
- e. Selezionare il metodo di escalation dei privilegi corretto (sudo) e immettere il nome utente e la password, se necessario.
- f. Fare clic su Salva

Crea un progetto

1. Vai su Risorse → Progetti e fai clic su Aggiungi.

- a. Inserisci il nome e i dettagli dell'organizzazione.
- b. Selezionare Git nel campo Tipo di credenziale di controllo del codice sorgente.
- c. entrare `https://github.com/NetApp-Automation/na_oracle19c_data_protection.git` come URL del controllo sorgente.
- d. Fare clic su Salva.
- e. Potrebbe essere necessario sincronizzare occasionalmente il progetto 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. Inserisci i parametri specifici del tuo ambiente nelle seguenti variabili globali incorporate o nel modulo vars.



Gli elementi in blu devono essere modificati per adattarli all'ambiente.

In sede

```
# 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 security group that allows access to on-prem
resources.
security_group: "sg-123123123"

# Your 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"
```

Manuali di automazione

Ci sono quattro playbook distinti che devono essere eseguiti.

1. Manuale per la configurazione del tuo ambiente, On-Prem o CVO.
2. Playbook per la replica di Oracle Binary e Database secondo una pianificazione
3. Playbook per la replica dei log Oracle secondo una pianificazione
4. Playbook per il ripristino del database su un host di destinazione

Configurazione ONTAP/CVO

[.sottolineato]* Configurazione ONTAP e CVO*

Configura e avvia il modello di lavoro.

1. Crea il modello di lavoro.
 - a. Vai su Risorse → Modelli → Aggiungi e fai clic su Aggiungi modello di lavoro.
 - b. Inserisci il nome ONTAP/CVO Setup
 - c. Selezionare il tipo di lavoro; Esegui configura il sistema in base a un playbook.
 - d. Selezionare 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 in un'istanza CVO.
 - f. Incolla le variabili globali copiate dal passaggio 4 nel campo Variabili modello nella scheda YAML.
 - g. Fare clic su Salva.
2. Avvia il modello di lavoro.
 - a. Vai a Risorse → Modelli.
 - b. Fare clic sul modello desiderato e quindi su Avvia.



Utilizzeremo questo modello e lo copieremo per gli altri manuali.

Replica per volumi binari e di database

Pianificazione del playbook di replica binaria e del database

Configura e avvia il modello di lavoro.

1. Copiare il modello di lavoro creato in precedenza.
 - a. Vai a Risorse → Modelli.
 - b. Trova il modello di configurazione ONTAP/CVO e all'estrema destra fai clic su Copia modello
 - c. Fare clic su Modifica modello sul modello copiato e modificare il nome in Playbook di replica binaria e database.
 - d. Mantenere lo stesso inventario, progetto e credenziali per il modello.
 - e. Selezionare `ora_replication_cg.yml` come playbook 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. Pianifica il modello di lavoro.
 - a. Vai a Risorse → Modelli.
 - b. Fare clic sul modello Playbook di replica binaria e database, quindi fare clic su Pianificazioni nel set di opzioni in alto.
 - c. Fare clic su Aggiungi, aggiungere Nome pianificazione 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 frequente e la replica SnapMirror verrà aggiornata.



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

Replica per volumi di registro

Pianificazione del playbook di replicazione del log

Configura e avvia il modello di lavoro

1. Copiare il modello di lavoro creato in precedenza.
 - a. Vai a Risorse → Modelli.
 - b. Trova il modello di configurazione ONTAP/CVO e all'estrema destra fai clic su Copia modello
 - c. Fare clic su Modifica modello sul modello copiato e modificare il nome in Log Replication Playbook.
 - d. Mantenere lo stesso inventario, progetto e credenziali per il modello.
 - e. Selezionare ora_replication_logs.yml come playbook 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. Pianifica il modello di lavoro.
 - a. Vai a Risorse → Modelli.
 - b. Fare clic sul modello Log Replication Playbook, quindi su Pianificazioni nel set di opzioni in alto.
 - c. Fare clic su Aggiungi, aggiungere Nome pianificazione per la replica del registro, scegliere Data/ora di inizio all'inizio dell'ora, scegliere il fuso orario locale e Frequenza di esecuzione. La frequenza di esecuzione sarà frequente e la replica SnapMirror verrà aggiornata.



Si consiglia di impostare la pianificazione del registro in modo che venga aggiornato ogni ora per garantire il ripristino all'ultimo aggiornamento orario.

Ripristina e recupera il database

Pianificazione del playbook di replicazione del log

Configura e avvia il modello di lavoro.

1. Copiare il modello di lavoro creato in precedenza.
 - a. Vai a Risorse → Modelli.
 - b. Trova il modello di configurazione ONTAP/CVO e all'estrema destra fai clic su Copia modello
 - c. Fare clic su Modifica modello sul modello copiato e modificare il nome in Playbook di ripristino e ripristino.
 - d. Mantenere lo stesso inventario, progetto e credenziali per il modello.
 - e. Selezionare ora_recovery.yml come playbook 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 playbook non verrà eseguito finché non sarai pronto a ripristinare il database nel sito remoto.

Recupero del database Oracle

1. I volumi di dati dei database Oracle di produzione on-premise sono protetti tramite la replica 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 elaborazione di ripristino nel data center secondario o nel cloud pubblico sono in standby e pronte a ripristinare il database di produzione in caso di disastro. Le istanze di elaborazione in standby vengono mantenute sincronizzate con le istanze on-prem eseguendo aggiornamenti paralleli sulla patch del kernel del sistema operativo o aggiornandoli in modo graduale.
2. In questa soluzione dimostrata, il volume binario Oracle viene replicato sulla destinazione e montato sull'istanza di destinazione per avviare lo stack software Oracle. Questo approccio per ripristinare Oracle è più vantaggioso rispetto a una nuova installazione di Oracle all'ultimo minuto quando si verifica un disastro. Garantisce che l'installazione di Oracle sia completamente sincronizzata con l'installazione del software di produzione locale corrente, con i livelli di patch, ecc. Tuttavia, ciò potrebbe avere o meno implicazioni aggiuntive sulla licenza software per il volume binario Oracle replicato nel sito di ripristino, a seconda di come è strutturata la licenza software con Oracle. Si consiglia all'utente di verificare con il personale addetto alle licenze software la potenziale necessità di licenza Oracle prima di decidere di utilizzare lo stesso approccio.
3. L'host Oracle di standby nella destinazione è configurato con le configurazioni prerequisite di Oracle.
4. Gli SnapMirror vengono danneggiati e i volumi vengono resi scrivibili e montati sull'host Oracle in standby.
5. Il modulo di ripristino di Oracle esegue le seguenti attività per ripristinare e avviare Oracle nel sito di ripristino dopo che tutti i volumi DB sono stati montati nell'istanza di elaborazione in standby.
 - a. Sincronizzazione del file di controllo: abbiamo distribuito file di controllo Oracle duplicati su volumi di database diversi per proteggere i file di controllo critici del database. Uno riguarda il volume dei dati e l'altro il volume dei registri. Poiché i volumi di dati e di registro vengono replicati con frequenze diverse, al momento del ripristino non saranno sincronizzati.
 - b. Ricollegamento del binario Oracle: poiché il binario Oracle è stato spostato su un nuovo host, è necessario ricollegarlo.
 - c. Recupera database Oracle: il meccanismo di recupero recupera l'ultimo numero di modifica del sistema nell'ultimo registro archiviato disponibile nel volume di registro Oracle dal file di controllo e recupera il database Oracle per recuperare tutte le transazioni aziendali che potevano essere replicate sul sito DR al momento dell'errore. Il database viene quindi avviato in una nuova incarnazione per gestire le connessioni degli utenti e le transazioni aziendali nel sito di ripristino.



Prima di eseguire il playbook di recupero, assicurati di avere quanto segue: assicurati di copiare `/etc/oratab` e `/etc/orainst.loc` dall'host Oracle di origine all'host di destinazione

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.