



Oracle データ保護の自動化

NetApp Solutions

NetApp
April 10, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/netapp-solutions/databases/db_protection_getting_started.html on April 10, 2024. Always check docs.netapp.com for the latest.

目次

解決策の概要	1
Oracle データベースのデータ保護を自動化	1
はじめに	2
ステップバイステップの導入手順	7

解決策の概要

Oracle データベースのデータ保護を自動化

組織は環境を自動化して、効率を高め、導入を高速化し、手動作業を削減しています。Ansible などの構成管理ツールを使用して、エンタープライズデータベースの運用を合理化しています。この解決策では、Ansible を使用して NetApp ONTAP による Oracle のデータ保護を自動化する方法を紹介します。ストレージ管理者、システム管理者、DBA は、オフサイトのデータセンターやパブリッククラウドへのデータレプリケーションを一貫して迅速にセットアップできるため、次のようなメリットがあります。

- 設計の複雑さと人為的ミスを排除し、繰り返し実行可能な一貫した導入とベストプラクティスを実装する
- クラスタ間レプリケーション、CVO のインスタンス化、Oracle データベースのリカバリの構成にかかる時間を短縮できます
- データベース管理者、システム管理者、ストレージ管理者の生産性を向上
- データベースリカバリワークフローを使用して、DR シナリオを簡単にテストできます。

ネットアップは、検証済みの Ansible モジュールとロールをお客様に提供し、Oracle データベース環境の導入、構成、ライフサイクル管理を迅速化します。この解決策では、以下の作業に役立つ Ansible の Playbook コードを提供しています。

オンプレミスからオンプレミスへのレプリケーション

- ソースとデスティネーションにクラスタ間 LIF を作成
- クラスタと SVM のピア関係を確立
- Oracle ボリュームの SnapMirror を作成して初期化
- AWX/Tower を使用して、Oracle バイナリ、データベース、ログ用のレプリケーションスケジュールを作成します
- デスティネーションで Oracle DB のリストアを行い、データベースをオンラインにします

オンプレミスから **AWS** の **CVO** へ

- AWS コネクタを作成します
- AWS で CVO インスタンスを作成
- オンプレミスのクラスタを Cloud Manager に追加
- ソースにクラスタ間 LIF を作成
- クラスタと SVM のピア関係を確立
- Oracle ボリュームの SnapMirror を作成して初期化
- AWX/Tower を使用して、Oracle バイナリ、データベース、ログ用のレプリケーションスケジュールを作成します
- デスティネーションで Oracle DB のリストアを行い、データベースをオンラインにします

準備ができれば、をクリックします ["解決策の使用を開始するには、こちらをクリックしてください"](#)。

はじめに

この解決策は、AWX/Tower 環境で動作するように設計されています。

AWX / タワー

AWX / タワー環境の場合は、ONTAP クラスタ管理と Oracle サーバ（IP およびホスト名）のインベントリの作成、クレデンシャルの作成、NetApp Automation Github から Ansible コードを取得するプロジェクトの設定、および自動化を開始するジョブテンプレートの設定を案内されます。

1. 解決策は、プライベートクラウドのシナリオ（オンプレミスからオンプレミス）およびハイブリッドクラウド（オンプレミスからパブリッククラウドへの Cloud Volumes ONTAP [CVO]）で実行するように設計されています。
2. 環境に固有の変数を入力し、ジョブテンプレートのその他の VAR フィールドにコピーして貼り付けます。
3. ジョブテンプレートに変数を追加したら、自動化を起動できます。
4. 自動化は、Oracle バイナリのセットアップ、データベース、ログ、ログのレプリケーションスケジュール、ログのみのレプリケーションスケジュールの 3 つのフェーズと、DR サイトでのデータベースリカバリのための 4 つのフェーズで実行されます。
5. CVO Data Protection に必要なキーとトークンの取得方法の詳細については、を参照してください "[CVO の導入と Connector の導入の前提条件を収集](#)"

要件

<strong class="big"> オンプレミス |

環境	要件
* Ansible 環境 *	AWX / タワー
	Ansible v.2.10 以上
	Python 3.
	Python ライブラリ - NetApp-lib-xmltodict-jmespath
* ONTAP *	ONTAP バージョン 9.8+
	データアグリゲート × 2
	NFS VLAN および ifgrp が作成されました
* Oracle サーバ *	RHEL 7/8
	Oracle Linux 7/8
	NFS、パブリック、オプションの管理用のネットワークインターフェイス
	ソース上の既存の Oracle 環境と、デスティネーション（DR サイトまたはパブリッククラウド）上の同等の Linux オペレーティングシステム

 「ビッグ」 >CVO

環境	要件
* Ansible 環境 *	AWX / タワー
	Ansible v.2.10 以上
	Python 3.
	Python ライブラリ - NetApp-lib-xmltodict-jmespath
* ONTAP *	ONTAP バージョン 9.8+
	データアグリゲート × 2
	NFS VLAN および ifgrp が作成されました
* Oracle サーバ *	RHEL 7/8
	Oracle Linux 7/8
	NFS、パブリック、オプションの管理用のネットワークインターフェイス
	ソース上の既存の Oracle 環境と、デスティネーション（DR サイトまたはパブリッククラウド）上の同等の Linux オペレーティングシステム
	Oracle EC2 インスタンスに適切なスワップスペースを設定します。デフォルトでは、一部の EC2 インスタンスは 0 スワップで導入されます
* Cloud Manager / AWS *	AWS のアクセス / シークレットキー
	NetApp Cloud Manager アカウント
	NetApp Cloud Manager Refresh Token

自動化の詳細

<strong class="big"> オンプレミス |

この自動導入は、3つのロールで構成される Ansible プレイブックを使用して設計されています。ロールは ONTAP、Linux、Oracle の各構成に対応しています。次の表に、自動化されるタスクを示します。

Playbook	タスク
* ONTAP_setup*	ONTAP 環境の事前チェック
	ソースクラスタでのクラスタ間 LIF の作成（オプション）
	デスティネーションクラスタでのクラスタ間 LIF の作成（オプション）
	クラスタ / SVM ピアリングの作成
	SnapMirror デスティネーションの作成と、指定された Oracle ボリュームの初期化
* ora_replication_cg *	/etc/oratab 内の各データベースのバックアップモードを有効にします
	Oracle バイナリボリュームとデータベースボリュームの Snapshot
	SnapMirror を更新しました
	/etc/oratab 内の各データベースのバックアップモードをオフにします
* ora_replication_log *	/etc/oratab 内の各データベースの現在のログを切り替えます
	Oracle ログボリュームの Snapshot
	SnapMirror を更新しました
* ora_recovery*	SnapMirror を解除します
	デスティネーションで NFS を有効にし、Oracle ボリュームのジャンクションパスを作成します
	DR Oracle ホストを設定
	Oracle ボリュームをマウントして確認
	Oracle データベースをリカバリして起動します

 「ビッグ」 >CVO

この自動導入は、3つのロールで構成される Ansible プレイブックを使用して設計されています。ロールは ONTAP、Linux、Oracle の各構成に対応しています。次の表に、自動化されるタスクを示します。

Playbook	タスク
* CVF_setup*	環境の事前チェック
	AWS Configure / AWS Access Key ID / Secret Key / Default Region
	AWS ロールの作成
	AWS での NetApp Cloud Manager Connector インスタンスの作成
	AWS での Cloud Volumes ONTAP （CVO）インスタンスの作成
	オンプレミスのソース ONTAP クラスタを NetApp Cloud Manager に追加
	SnapMirror デスティネーションの作成と、指定された Oracle ボリュームの初期化
* ora_replication_cg *	/etc/oratab 内の各データベースのバックアップモードを有効にします
	Oracle バイナリボリュームとデータベースボリュームの Snapshot
	SnapMirror を更新しました
	/etc/oratab 内の各データベースのバックアップモードをオフにします
* ora_replication_log *	/etc/oratab 内の各データベースの現在のログを切り替えます
	Oracle ログボリュームの Snapshot
	SnapMirror を更新しました
* ora_recovery*	SnapMirror を解除します
	デスティネーション CVO で NFS を有効にし、Oracle ボリュームのジャンクションパスを作成してください
	DR Oracle ホストを設定
	Oracle ボリュームをマウントして確認
	Oracle データベースをリカバリして起動します

デフォルトパラメータ

自動化を簡易化するために、必要な Oracle パラメータがデフォルト値で多数設定されています。通常、ほとんどの環境でデフォルトパラメータを変更する必要はありません。上級ユーザーは 'デフォルト・パラメータ' を変更する際に注意してくださいデフォルトのパラメータは、各ロールフォルダの defaults ディレクトリにあります。

使用許諾

Github リポジトリに記載されているライセンス情報をお読みください。このリポジトリ内のコンテンツにアクセス、ダウンロード、インストール、または使用することにより、ライセンスの条項に同意したものとみなされます ["こちらをご覧ください"](#)。

このリポジトリ内のコンテンツの作成および / または派生著作物の共有に関しては、一定の制限事項があります。の条件を必ずお読みください ["使用許諾"](#) コンテンツを使用する前に。すべての条件に同意しない場合は、このリポジトリのコンテンツにアクセスしたり、コンテンツをダウンロードしたり、使用したりしないでください。

準備ができれば、をクリックします ["AWX/Tower の詳細な手順については、こちらを参照してください"](#)。

ステップバイステップの導入手順

AWX/Tower Oracle データ保護

環境のインベントリ、グループ、ホスト、クレデンシャルを作成します

このセクションでは、ネットアップの自動化ソリューションを使用する環境を準備するための AWX/Ansible タワーでのインベントリ、グループ、ホスト、アクセスクレデンシャルのセットアップについて説明します。

1. インベントリを設定します。
 - a. リソース→インベントリ→追加と進み、インベントリの追加をクリックします。
 - b. 名前と組織の詳細を入力し、[保存] をクリックします。
 - c. インベントリページで、作成されたインベントリをクリックします。
 - d. [グループ] サブメニューに移動し、[追加] をクリックします。
 - e. 最初のグループの Oracle という名前を入力し、[保存] をクリックします。
 - f. DR_Oracle という名前の 2 つ目のグループに対してこの手順を繰り返します。
 - g. 作成した Oracle グループを選択し、Hosts サブメニューに移動して、Add New Host をクリックします。
 - h. ソース Oracle ホストの管理 IP の IP アドレスを入力し、[保存] をクリックします。
 - i. DR_Oracle グループに対してこの手順を繰り返し、DR/Destination Oracle ホストの管理 IP / ホスト名を追加する必要があります。



以下は、オンプレミスと ONTAP、または AWS 上の CVO のクレデンシャルタイプとクレデンシャルを作成する手順です。

オンプレミス

1. クレデンシャルを設定します。
2. クレデンシャルタイプの作成ONTAP を使用するソリューションでは、ユーザ名とパスワードのエントリを照合するようにクレデンシャルタイプを設定する必要があります。
 - a. [管理] → [資格情報の種類] に移動し、[追加] をクリックします。
 - b. 名前と概要を指定します。
 - c. 入力構成に次の内容を貼り付けます。

```
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. 次の内容をインジェクタ設定に貼り付け、[保存] をクリックします。

```
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. ONTAP のクレデンシャルを作成します
 - a. [リソース] → [資格情報] に移動し、[追加] をクリックします。
 - b. ONTAP クレデンシャルの名前と組織の詳細を入力します
 - c. 前の手順で作成したクレデンシャルタイプを選択します。
 - d. タイプの詳細で、ソースクラスタとデスティネーションクラスタのユーザ名とパスワードを入力します。
 - e. [保存] をクリックします .
4. Oracle のクレデンシャルを作成します

- a. [リソース] → [資格情報] に移動し、[追加] をクリックします。
- b. Oracle の名前と組織の詳細を入力します。
- c. マシクレデンシャルタイプを選択します。
- d. Type Details （タイプの詳細）に、Oracle ホストのユーザー名とパスワードを入力します。
- e. 適切な特権昇格方式を選択し、ユーザ名とパスワードを入力します。
- f. [保存] をクリックします。
- g. 必要に応じて、DR_Oracle ホストの別のクレデンシャルに対して同じ手順を繰り返します。

CVO を確認して

1. クレデンシャルを設定します。
2. クレデンシャルタイプを作成する。ONTAP が関連するソリューションでは、ユーザ名とパスワードのエントリに一致するクレデンシャルタイプを設定する必要があります。また、Cloud Central と AWS のエントリも追加します。
 - a. [管理] → [資格情報の種類] に移動し、[追加] をクリックします。
 - b. 名前と概要を指定します。
 - c. 入力構成に次の内容を貼り付けます。

```
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. 次の内容をインジェクタ構成に貼り付け、[保存 (Save)] をクリックする。

```
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. ONTAP / CVO / AWS のクレデンシャルを作成

- a. [リソース] → [資格情報] に移動し、[追加] をクリックします。
- b. ONTAP クレデンシャルの名前と組織の詳細を入力します
- c. 前の手順で作成したクレデンシャルタイプを選択します。
- d. Type Details に、ソースクラスタと CVO クラスタ、Cloud Central / Manager 、AWS Access / Secret Key 、Cloud Central Refresh Token のユーザ名とパスワードを入力します。
- e. [保存] をクリックします。

4. Oracle のクレデンシャルの作成（ソース）

- a. [リソース] → [資格情報] に移動し、[追加] をクリックします。
- b. Oracle ホストの名前と組織の詳細を入力します
- c. マシンのクレデンシャルタイプを選択します。
- d. Type Details （タイプの詳細）に、Oracle ホストのユーザー名とパスワードを入力します。
- e. 適切な特権昇格方式を選択し、ユーザ名とパスワードを入力します。
- f. [保存] をクリックします。

5. Oracle 保存先のクレデンシャルを作成します

- a. [リソース] → [資格情報] に移動し、[追加] をクリックします。
- b. DR Oracle ホストの名前と組織の詳細を入力します
- c. マシンのクレデンシャルタイプを選択します。
- d. Type Details に、ユーザ名（ec2-user またはデフォルトの入力から変更した場合は、そのユーザ名）と SSH 秘密鍵を入力します
- e. 適切な特権昇格方式（sudo）を選択し、必要に応じてユーザ名とパスワードを入力します。
- f. [保存] をクリックします。

プロジェクトを作成します

1. [リソース] → [プロジェクト] に移動し、[追加] をクリックします。
 - a. 名前と組織の詳細を入力します
 - b. Source Control Credential Type フィールドで Git を選択します。
 - c. 入力するコマンド <https://github.com/NetApp-Automation/na_oracle19c_data_protection.git> をソース管理 URL として指定します。
 - d. [保存] をクリックします。
 - e. ソースコードが変更されたときに、プロジェクトの同期が必要になることがあります。

グローバル変数を設定します

このセクションで定義する変数は、すべての Oracle ホスト、データベース、および ONTAP クラスタに適用されます。

1. 次の組み込みグローバル変数または変数フォームに環境固有のパラメータを入力します。



青の項目は、環境に合わせて変更する必要があります。

オンプレミス

```
# 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を確認して

```

#####
### 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"
```

自動化ハンドブック

実行する必要があるプレイブックは4つあります。

1. 環境のセットアップに関するプレイブック：オンプレミス、CVO
2. Oracle バイナリとデータベースをスケジュールどおりにレプリケートする Playbook
3. Oracle ログをスケジュールどおりにレプリケートするためのプレイブック
4. デスティネーションホストでのデータベースのリカバリに関するプレイブック

ONTAP/CVO セットアップ

ONTAP と CVO のセットアップ

ジョブテンプレートを設定して起動します。

1. ジョブテンプレートを作成します。
 - a. [リソース]→[テンプレート]→[追加]に移動し、[ジョブテンプレートの追加]をクリックします。
 - b. 「ONTAP/CVO Setup」という名前を入力します
 - c. ジョブタイプを選択します。Run は、プレイブックに基づいてシステムを設定します。
 - d. 対応するインベントリ、プロジェクト、プレイブック、およびクレデンシャルを選択します。
 - e. オンプレミス環境用の ONTAP_setup.yml プレイブックを選択するか、CVO-setup.yml を選択して CVO インスタンスにレプリケーションします。
 - f. 手順 4 からコピーしたグローバル変数を YAML タブの Template Variables フィールドに貼り付けます。
 - g. [保存]をクリックします。
2. ジョブテンプレートを起動します。
 - a. [リソース]→[テンプレート]に移動します。
 - b. 目的のテンプレートをクリックし、[起動]をクリックします。



このテンプレートを使用して、他のプレイブック用にコピーします。

バイナリおよびデータベースボリュームのレプリケーション

バイナリおよびデータベースのレプリケーションマニュアルのスケジュール

ジョブテンプレートを設定して起動します。

1. 以前に作成したジョブテンプレートをコピーします。
 - a. [リソース]→[テンプレート]に移動します。
 - b. 「ONTAP/CVO Setup Template」を探して、右端で「Copy Template」をクリックします
 - c. コピーしたテンプレートで[テンプレートの編集]をクリックし、名前を[バイナリおよびデータベースのレプリケーションのマニュアル]に変更します。
 - d. テンプレートの同じインベントリ、プロジェクト、資格情報を保持します。
 - e. 実行するプレイブックとして ora_replication_cg.yml を選択します。
 - f. 変数は変更されませんが、CVO クラスターの IP は変数 dst_cluster_ip に設定する必要があります。
 - g. [保存]をクリックします。
2. ジョブテンプレートをスケジュールします。
 - a. [リソース]→[テンプレート]に移動します。

- b. バイナリおよびデータベースのレプリケーション用プレイブックテンプレートをクリックし、一番上のオプションセットにあるスケジュールをクリックします。
- c. [追加] をクリックし、[バイナリおよびデータベースレプリケーションの名前スケジュールの追加] をクリックし、時間の開始時に [開始日時] を選択し、[ローカルタイムゾーン] を選択して、[実行頻度] をクリックします。実行頻度は、多くの場合、SnapMirror レプリケーションが更新されます。



ログボリュームのレプリケーション用に別のスケジュールが作成されるため、より頻繁にレプリケートできます。

ログボリュームのレプリケーション

ログ・レプリケーション・プレイブックのスケジュール

ジョブテンプレートを設定して起動します。

1. 以前に作成したジョブテンプレートをコピーします。
 - a. [リソース] → [テンプレート] に移動します。
 - b. 「ONTAP/CVO Setup Template」を探して、右端で「Copy Template」をクリックします
 - c. コピーしたテンプレートで [テンプレートの編集] をクリックし、名前を [ログレプリケーションのプレイブック] に変更します。
 - d. テンプレートの同じインベントリ、プロジェクト、資格情報を保持します。
 - e. 実行するプレイブックとして ora_replication_loges.yml を選択します。
 - f. 変数は変更されませんが、CVO クラスターの IP は変数 dst_cluster_ip に設定する必要があります。
 - g. [保存] をクリックします。
2. ジョブテンプレートをスケジュールします。
 - a. [リソース] → [テンプレート] に移動します。
 - b. Log Replication Playbook テンプレートをクリックし、一番上のオプションセットにある Schedules (スケジュール) をクリックします。
 - c. [追加] をクリックし、[ログ複製の名前スケジュールの追加] をクリックし、時間の開始時に開始日時を選択し、[ローカルタイムゾーン] と [実行頻度] を選択します。実行頻度は、多くの場合、SnapMirror レプリケーションが更新されます。



1 時間ごとの最新の更新に確実にリカバリできるように、ログスケジュールを 1 時間ごとに更新するように設定することを推奨します。

データベースのリストアとリカバリ

ログ・レプリケーション・プレイブックのスケジュール

ジョブテンプレートを設定して起動します。

1. 以前に作成したジョブテンプレートをコピーします。
 - a. [リソース] → [テンプレート] に移動します。

- b. 「ONTAP/CVO Setup Template」を探して、右端で「Copy Template」をクリックします
- c. コピーしたテンプレートで [テンプレートの編集] をクリックし、名前を [リストアとリカバリプレイブック] に変更します。
- d. テンプレートの同じインベントリ、プロジェクト、資格情報を保持します。
- e. 実行するプレイブックとして ora_recovery.yml を選択します。
- f. 変数は変更されませんが、CVO クラスターの IP は変数 dst_cluster_ip に設定する必要があります。
- g. [保存] をクリックします。



このプレイブックは、リモートサイトでデータベースをリストアする準備ができるまでは実行されません。

Oracle データベースをリカバリしています

1. オンプレミスの本番 Oracle データベースのデータボリュームは、NetApp SnapMirror レプリケーションを使用して、セカンダリデータセンターの冗長 ONTAP クラスターまたはパブリッククラウドの Cloud Volume ONTAP に保護されます。完全に構成されたディザスタリカバリ環境では、セカンダリデータセンターまたはパブリッククラウドのリカバリコンピューティングインスタンスがスタンバイ状態になり、災害発生時に本番データベースをリカバリできます。スタンバイコンピューティングインスタンスは、OS カーネルパッチで parallel アップデートを実行するか、ロックステップでアップグレードすることで、オンプレミスインスタンスと同期したままになります。
2. この解決策で実証されている Oracle バイナリ・ボリュームは、ターゲット・インスタンスに複製され、ターゲット・インスタンスにマウントされて、Oracle ソフトウェア・スタックが起動されます。この Oracle リカバリアプローチには、災害発生時に Oracle を新規にインストールした場合よりも優れています。Oracle のインストールは、現在のオンプレミスの本番ソフトウェアのインストールレベルやパッチレベルと完全に同期されていることが保証されます。ただし、Oracle でのソフトウェアライセンスの構成によっては、リカバリサイトで複製された Oracle バイナリボリュームにソフトウェアライセンスが影響する場合とそうでない場合があります。ユーザは、Oracle のライセンス要件を評価するために、ソフトウェアライセンス担当者に確認してから、同じ方法を使用することを推奨します。
3. デスティネーションのスタンバイ Oracle ホストには、Oracle の前提条件となる構成が設定されています。
4. SnapMirror が切断され、ボリュームが書き込み可能になり、スタンバイ Oracle ホストにマウントされます。
5. すべての DB ボリュームがスタンバイコンピューティングインスタンスにマウントされたあと、Oracle リカバリモジュールは以下のタスクを実行して、リカバリサイトで Oracle をリカバリおよび起動します。
 - a. 制御ファイルを同期します。重要なデータベース制御ファイルを保護するために、異なるデータベースボリュームに Oracle 制御ファイルを重複して配置しました。1 つはデータボリューム上にあり、もう 1 つはログボリューム上にあります。データボリュームとログボリュームは異なる頻度でレプリケートされるため、リカバリ時に同期されません。
 - b. Oracle バイナリの再リンク：Oracle バイナリは新しいホストに再配置されるため、再リンクが必要です。
 - c. Oracle データベースのリカバリ：リカバリ・メカニズムは、Oracle ログ・ボリューム内の最後に使用可能なアーカイブ・ログのシステム変更番号を制御ファイルから取得し、Oracle データベースをリカバリして、障害発生時に DR サイトにレプリケートされたすべてのビジネス・トランザクションをリカバリします。次に、データベースが新しいインカンセーションで起動され、リカバリサイトでユー

ザ接続とビジネストランザクションが実行されます。



Recovering Playbook を実行する前に、次の情報を確認してください。 /etc/oratab および /etc/orainst.loc を介して、ソース Oracle ホストからデスティネーションホストにコピーしてください

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。