Automatisierter Oracle-Datenschutz

NetApp database solutions

NetApp
August 18, 2025

Inhalt

Automatisierter Oracle-Datenschutz

Lösungsübersicht

Auf dieser Seite wird die automatisierte Methode zum Bereitstellen von Oracle19c auf NetApp ONTAP -Speicher beschrieben.

Automatisierter Datenschutz für Oracle-Datenbanken

Organisationen automatisieren ihre Umgebungen, um die Effizienz zu steigern, Bereitstellungen zu beschleunigen und den manuellen Aufwand zu reduzieren. Konfigurationsmanagement-Tools wie Ansible werden verwendet, um den Datenbankbetrieb in Unternehmen zu optimieren. In dieser Lösung zeigen wir, wie Sie mit Ansible den Datenschutz von Oracle mit NetApp ONTAP automatisieren können. Indem Sie Speicheradministratoren, Systemadministratoren und DBAs die Möglichkeit geben, die Datenreplikation in einem externen Rechenzentrum oder in der öffentlichen Cloud konsistent und schnell einzurichten, erzielen Sie die folgenden Vorteile:

- Beseitigen Sie komplexe Designs und menschliche Fehler und implementieren Sie eine wiederholbare, konsistente Bereitstellung und bewährte Methoden.
- Verkürzen Sie die Zeit für die Konfiguration der Intercluster-Replikation, CVO-Instanziierung und Wiederherstellung von Oracle-Datenbanken
- Steigern Sie die Produktivität von Datenbankadministratoren, System- und Speicheradministratoren
- Bietet einen Datenbankwiederherstellungs-Workflow zum einfachen Testen eines DR-Szenarios.

NetApp stellt Kunden validierte Ansible-Module und -Rollen zur Verfügung, um die Bereitstellung, Konfiguration und Lebenszyklusverwaltung Ihrer Oracle-Datenbankumgebung zu beschleunigen. Diese Lösung bietet Anweisungen und Ansible-Playbook-Code, um Ihnen zu helfen:

On-Prem-zu-On-Prem-Replikation

- Erstellen Sie Intercluster-LIFS an Quelle und Ziel
- Cluster- und VServer-Peering einrichten
- Erstellen und initialisieren Sie SnapMirror von Oracle-Volumes
- Erstellen Sie einen Replikationszeitplan über AWX/Tower für Oracle-Binärdateien, Datenbanken und Protokolle
- Stellen Sie die Oracle-Datenbank auf dem Ziel wieder her und bringen Sie die Datenbank online

On Prem zum CVO in AWS

- AWS-Connector erstellen
- Erstellen Sie eine CVO-Instanz in AWS
- On-Prem-Cluster zu Cloud Manager hinzufügen
- Erstellen Sie Intercluster-LIFs auf der Quelle
- Cluster- und VServer-Peering einrichten
- Erstellen und initialisieren Sie SnapMirror von Oracle-Volumes
- Erstellen Sie einen Replikationszeitplan über AWX/Tower für Oracle-Binärdateien, Datenbanken und

Protokolle

- Stellen Sie die Oracle-Datenbank auf dem Ziel wieder her und bringen Sie die Datenbank online

Wenn Sie fertig sind, klicken Sie auf"Hier erfahren Sie, wie Sie mit der Lösung beginnen können" .

Erste Schritte

Diese Lösung wurde für die Ausführung in einer AWX/Tower-Umgebung entwickelt.

AWX/Turm

Für AWX/Tower-Umgebungen werden Sie durch die Erstellung eines Inventars Ihres ONTAP Clustermanagements und Oracle-Servers (IPs und Hostnamen), das Erstellen von Anmeldeinformationen, das Konfigurieren eines Projekts, das den Ansible-Code von NetApp Automation Github abruft, und der Jobvorlage geführt, die die Automatisierung startet.

1. Die Lösung wurde für den Betrieb in einem privaten Cloud-Szenario (On-Premise zu On-Premise) und einer Hybrid-Cloud (On-Premise zu Public Cloud Cloud Volumes ONTAP [CVO]) konzipiert.
2. Füllen Sie die für Ihre Umgebung spezifischen Variablen aus und kopieren Sie sie und fügen Sie sie in die Felder „Extra Vars“ in Ihrer Jobvorlage ein.
3. Nachdem die zusätzlichen Variablen zu Ihrer Jobvorlage hinzugefügt wurden, können Sie die Automatisierung starten.
4. Die Automatisierung ist so angelegt, dass sie in drei Phasen (Setup, Replikationszeitplan für Oracle-Binärdateien, Datenbank, Protokolle und Replikationszeitplan nur für Protokolle) und einer vierten Phase zur Wiederherstellung der Datenbank an einem DR-Standort ausgeführt wird.
5. Detaillierte Anweisungen zum Erhalt der für den CVO-Datenschutz erforderlichen Schlüssel und Token finden Sie unter"Voraussetzungen für CVO- und Connector-Bereitstellungen sammeln"

Anforderungen

Vor Ort

Umfeld	Anforderungen
Ansible-Umgebung	AWX/Turm
	Ansible v.2.10 und höher
	Python 3
	Python-Bibliotheken – netapp-lib – xmltodict – jmespath
* ONTAP*	ONTAP Version 9.8 +
	Zwei Datenaggregate
	NFS-VLAN und IFGRP erstellt
Oracle-Server	RHEL 7/8
	Oracle Linux 7/8
	Netzwerkschnittstellen für NFS, öffentliche und optionale Verwaltung
	Vorhandene Oracle-Umgebung auf der Quelle und das entsprechende Linux-Betriebssystem am Ziel (DR-Site oder öffentliche Cloud)

CVO

Umfeld	Anforderungen
Ansible-Umgebung	AWX/Turm
	Ansible v.2.10 und höher
	Python 3
	Python-Bibliotheken – netapp-lib – xmltodict – jmespath
* ONTAP*	ONTAP Version 9.8 +
	Zwei Datenaggregate
	NFS-VLAN und IFGRP erstellt
Oracle-Server	RHEL 7/8
	Oracle Linux 7/8
	Netzwerkschnittstellen für NFS, öffentliche und optionale Verwaltung
	Vorhandene Oracle-Umgebung auf der Quelle und das entsprechende Linux-Betriebssystem am Ziel (DR-Site oder öffentliche Cloud)
	Legen Sie den entsprechenden Swap-Speicherplatz auf der Oracle EC2-Instanz fest. Standardmäßig werden einige EC2-Instanzen mit 0 Swap bereitgestellt.
Cloud Manager/AWS	AWS-Zugriffs-/Geheimschlüssel
	NetApp Cloud Manager-Konto
	NetApp Cloud Manager-Aktualisierungstoken
	Fügen Sie der AWS-Sicherheitsgruppe Quell-Intercluster-LIFs hinzu

Automatisierungsdetails

Vor Ort

Diese automatisierte Bereitstellung wird mit einem einzigen Ansible-Playbook entwickelt, das aus drei separaten Rollen besteht. Die Rollen gelten für ONTAP, Linux- und Oracle-Konfigurationen. In der folgenden Tabelle wird beschrieben, welche Aufgaben automatisiert werden.

Spielbuch	Aufgaben
ontap_setup	Vorabprüfung der ONTAP -Umgebung
	Erstellung von Intercluster-LIFs auf dem Quellcluster (OPTIONAL)
	Erstellung von Intercluster-LIFs auf dem Zielcluster (OPTIONAL)
	Erstellen eines Clusters und SVM-Peering
	Erstellen des Ziel SnapMirror und Initialisieren der vorgesehenen Oracle-Volumes
ora_replication_cg	Aktivieren Sie den Sicherungsmodus für jede Datenbank in /etc/oratab
	Snapshot der Oracle-Binär- und Datenbankvolumes
	Snapmirror aktualisiert
	Deaktivieren Sie den Sicherungsmodus für jede Datenbank in /etc/oratab
ora_replication_log	Wechseln Sie das aktuelle Protokoll für jede Datenbank in /etc/oratab
	Snapshot des Oracle-Protokollvolumes
	Snapmirror aktualisiert
ora_recovery	SnapMirror unterbrechen
	Aktivieren Sie NFS und erstellen Sie einen Verbindungspfad für Oracle-Volumes auf dem Ziel
	Konfigurieren des DR-Oracle-Hosts
	Mounten und Überprüfen von Oracle-Volumes
	Wiederherstellen und Starten der Oracle-Datenbank

CVO

Diese automatisierte Bereitstellung wird mit einem einzigen Ansible-Playbook entwickelt, das aus drei separaten Rollen besteht. Die Rollen gelten für ONTAP, Linux- und Oracle-Konfigurationen. In der folgenden Tabelle wird beschrieben, welche Aufgaben automatisiert werden.

Spielbuch	Aufgaben
cvo_setup	Vorabprüfung der Umgebung
	AWS-Konfiguration/AWS-Zugriffsschlüssel-ID/Geheimschlüssel/Standardregion
	Erstellen einer AWS-Rolle
	Erstellen einer NetApp Cloud Manager Connector-Instanz in AWS
	Erstellen einer Cloud Volumes ONTAP (CVO)-Instanz in AWS
	On-Premise-Source ONTAP -Cluster zu NetApp Cloud Manager hinzufügen
	Erstellen des Ziel SnapMirror und Initialisieren der vorgesehenen Oracle-Volumes
ora_replication_cg	Aktivieren Sie den Sicherungsmodus für jede Datenbank in /etc/oratab
	Snapshot der Oracle-Binär- und Datenbankvolumes
	Snapmirror aktualisiert
	Deaktivieren Sie den Sicherungsmodus für jede Datenbank in /etc/oratab
ora_replication_log	Wechseln Sie das aktuelle Protokoll für jede Datenbank in /etc/oratab
	Snapshot des Oracle-Protokollvolumes
	Snapmirror aktualisiert
ora_recovery	SnapMirror unterbrechen
	Aktivieren Sie NFS und erstellen Sie einen Verbindungspfad für Oracle-Volumes auf dem Ziel-CVO
	Konfigurieren des DR-Oracle-Hosts
	Mounten und Überprüfen von Oracle-Volumes
	Wiederherstellen und Starten der Oracle-Datenbank

Standardparameter

Um die Automatisierung zu vereinfachen, haben wir viele erforderliche Oracle-Parameter mit Standardwerten voreingestellt. Für die meisten Bereitstellungen ist es im Allgemeinen nicht erforderlich, die Standardparameter zu ändern. Ein erfahrener Benutzer kann mit Vorsicht Änderungen an den Standardparametern vornehmen. Die Standardparameter befinden sich in jedem Rollenordner im Verzeichnis „Defaults“.

Lizenz

Sie sollten die Lizenzinformationen im Github-Repository lesen. Indem Sie auf die Inhalte dieses Repositorys zugreifen, sie herunterladen, installieren oder verwenden, stimmen Sie den Bedingungen der Lizenz zu."hier," .

Beachten Sie, dass hinsichtlich der Erstellung und/oder Weitergabe abgeleiteter Werke aus den Inhalten dieses Repositorys bestimmte Einschränkungen gelten. Bitte lesen Sie unbedingt die Bedingungen der"Lizenz" bevor Sie den Inhalt verwenden. Wenn Sie nicht allen Bedingungen zustimmen, dürfen Sie nicht auf die Inhalte

in diesem Repository zugreifen, sie nicht herunterladen oder verwenden.

Wenn Sie fertig sind, klicken Sie auf"Hier finden Sie detaillierte AWX/Tower-Verfahren" .

Schrittweises Bereitstellungsverfahren

Auf dieser Seite wird der automatisierte Datenschutz von Oracle19c auf NetApp ONTAP -Speicher beschrieben.

AWX/Tower Oracle-Datenschutz

Erstellen Sie das Inventar, die Gruppe, die Hosts und die Anmeldeinformationen für Ihre Umgebung

In diesem Abschnitt wird die Einrichtung von Inventar, Gruppen, Hosts und Zugangsdaten in AWX/Ansible Tower beschrieben, die die Umgebung für die Nutzung automatisierter NetApp -Lösungen vorbereiten.

1. Konfigurieren Sie das Inventar.
    a. Navigieren Sie zu Ressourcen → Bestände → Hinzufügen und klicken Sie auf Bestand hinzufügen.
    b. Geben Sie den Namen und die Organisationsdetails ein und klicken Sie auf „Speichern“.
    c. Klicken Sie auf der Seite „Inventare“ auf das erstellte Inventar.
    d. Navigieren Sie zum Untermenü „Gruppen“ und klicken Sie auf „Hinzufügen“.
    e. Geben Sie Ihrer ersten Gruppe den Namen „Oracle“ und klicken Sie auf „Speichern“.
    f. Wiederholen Sie den Vorgang für eine zweite Gruppe namens dr_oracle.
    g. Wählen Sie die erstellte Oracle-Gruppe aus, gehen Sie zum Untermenü „Hosts“ und klicken Sie auf „Neuen Host hinzufügen“.
    h. Geben Sie die IP-Adresse der Verwaltungs-IP des Oracle-Quellhosts ein und klicken Sie auf „Speichern“.
    i. Dieser Vorgang muss für die Gruppe dr_oracle wiederholt werden und die Verwaltungs-IP/der Verwaltungshostname des DR/Ziel-Oracle-Hosts hinzugefügt werden.

Nachfolgend finden Sie Anweisungen zum Erstellen der Anmeldeinformationstypen und Anmeldeinformationen für On-Prem mit ONTAP oder CVO auf AWS.

Vor Ort

1. Konfigurieren Sie die Anmeldeinformationen.
2. Erstellen Sie Anmeldeinformationstypen. Bei Lösungen mit ONTAP müssen Sie den Anmeldeinformationstyp so konfigurieren, dass er mit den Benutzernamen- und Kennworteingaben übereinstimmt.
   a. Navigieren Sie zu „Administration“ → „Anmeldeinformationstypen“ und klicken Sie auf „Hinzufügen“.
   b. Geben Sie den Namen und die Beschreibung ein.
   c. Fügen Sie den folgenden Inhalt in die Eingabekonfiguration ein:

```
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. Fügen Sie den folgenden Inhalt in die Injector-Konfiguration ein und klicken Sie dann auf Speichern:

```
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. Anmeldeinformationen für ONTAP erstellen
   a. Navigieren Sie zu Ressourcen → Anmeldeinformationen und klicken Sie auf Hinzufügen.
   b. Geben Sie den Namen und die Organisationsdetails für die ONTAP -Anmeldeinformationen ein
   c. Wählen Sie den Anmeldeinformationstyp aus, der im vorherigen Schritt erstellt wurde.
   d. Geben Sie unter „Typdetails“ den Benutzernamen und das Kennwort für Ihre Quell- und Zielcluster ein.
   e. Klicken Sie auf Speichern

4. Anmeldeinformationen für Oracle erstellen
    a. Navigieren Sie zu Ressourcen → Anmeldeinformationen und klicken Sie auf Hinzufügen.
    b. Geben Sie den Namen und die Organisationsdetails für Oracle ein
    c. Wählen Sie den Anmeldeinformationstyp des Computers aus.
    d. Geben Sie unter „Typdetails“ den Benutzernamen und das Kennwort für die Oracle-Hosts ein.
    e. Wählen Sie die richtige Methode zur Rechteerweiterung aus und geben Sie den Benutzernamen und das Kennwort ein.
    f. Klicken Sie auf Speichern
    g. Wiederholen Sie den Vorgang bei Bedarf für andere Anmeldeinformationen für den dr_oracle-Host.

CVO

1. Konfigurieren Sie die Anmeldeinformationen.
2. Erstellen Sie Anmeldeinformationstypen. Bei Lösungen mit ONTAP müssen Sie den Anmeldeinformationstyp so konfigurieren, dass er mit den Benutzernamen- und Kennworteinträgen übereinstimmt. Wir werden auch Einträge für Cloud Central und AWS hinzufügen.
    a. Navigieren Sie zu „Administration“ → „Anmeldeinformationstypen“ und klicken Sie auf „Hinzufügen“.
    b. Geben Sie den Namen und die Beschreibung ein.
    c. Fügen Sie den folgenden Inhalt in die Eingabekonfiguration ein:

```
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. Fügen Sie den folgenden Inhalt in die Injector-Konfiguration ein und klicken Sie auf Speichern:

```
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. Anmeldeinformationen für ONTAP/CVO/AWS erstellen
   a. Navigieren Sie zu Ressourcen → Anmeldeinformationen und klicken Sie auf Hinzufügen.
   b. Geben Sie den Namen und die Organisationsdetails für die ONTAP -Anmeldeinformationen ein
   c. Wählen Sie den Anmeldeinformationstyp aus, der im vorherigen Schritt erstellt wurde.
   d. Geben Sie unter „Typdetails“ den Benutzernamen und das Kennwort für Ihre Quell- und CVO-Cluster, Cloud Central/Manager, AWS-Zugriffs-/Geheimschlüssel und Cloud Central-Aktualisierungstoken ein.
   e. Klicken Sie auf Speichern
4. Anmeldeinformationen für Oracle erstellen (Quelle)
   a. Navigieren Sie zu Ressourcen → Anmeldeinformationen und klicken Sie auf Hinzufügen.
   b. Geben Sie den Namen und die Organisationsdetails für den Oracle-Host ein
   c. Wählen Sie den Anmeldeinformationstyp des Computers aus.
   d. Geben Sie unter „Typdetails“ den Benutzernamen und das Kennwort für die Oracle-Hosts ein.
   e. Wählen Sie die richtige Methode zur Rechteerweiterung aus und geben Sie den Benutzernamen und das Kennwort ein.
   f. Klicken Sie auf Speichern
5. Anmeldeinformationen für Oracle-Ziel erstellen
   a. Navigieren Sie zu Ressourcen → Anmeldeinformationen und klicken Sie auf Hinzufügen.
   b. Geben Sie den Namen und die Organisationsdetails für den DR Oracle-Host ein
   c. Wählen Sie den Anmeldeinformationstyp des Computers aus.
   d. Geben Sie unter „Typdetails“ den Benutzernamen (ec2-user oder, falls Sie ihn von der Standardeinstellung geändert haben, diesen ein) und den privaten SSH-Schlüssel ein.
   e. Wählen Sie die richtige Methode zur Rechteerweiterung (sudo) und geben Sie bei Bedarf den Benutzernamen und das Kennwort ein.
   f. Klicken Sie auf Speichern

Erstellen eines Projekts

1. Gehen Sie zu Ressourcen → Projekte und klicken Sie auf Hinzufügen.
   a. Geben Sie den Namen und die Organisationsdetails ein.
   b. Wählen Sie im Feld „Anmeldeinformationstyp der Quellcodeverwaltung“ die Option „Git“ aus.
   c. eingeben `https://github.com/NetApp-Automation/na_oracle19c_data_protection.git` als Quellcodeverwaltungs-URL.
   d. Klicken Sie auf Speichern.
   e. Das Projekt muss möglicherweise gelegentlich synchronisiert werden, wenn sich der Quellcode ändert.

Konfigurieren globaler Variablen

Die in diesem Abschnitt definierten Variablen gelten für alle Oracle-Hosts, Datenbanken und den ONTAP Cluster.

1. Geben Sie Ihre umgebungsspezifischen Parameter in das folgende eingebettete globale Variablen- oder Vars-Formular ein.

Die blauen Elemente müssen geändert werden, damit sie zu Ihrer Umgebung passen.

Vor Ort

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

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

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

create_source_intercluster_lifs: "yes"

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

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

create_destination_intercluster_lifs: "yes"
```

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

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

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

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

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

```
snapmirror_policy: "async_policy_oracle"

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

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

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

CVO

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# Name your connector.
connector_name: "awx_connector"

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Automatisierungs-Playbooks

Es müssen vier separate Playbooks ausgeführt werden.

1. Playbook zum Einrichten Ihrer Umgebung, On-Prem oder CVO.
2. Playbook zum planmäßigen Replizieren von Oracle-Binärdateien und -Datenbanken
3. Playbook zum planmäßigen Replizieren von Oracle-Protokollen
4. Playbook zum Wiederherstellen Ihrer Datenbank auf einem Zielhost

ONTAP/CVO-Setup

[.underline]* ONTAP und CVO-Setup*

Konfigurieren und starten Sie die Jobvorlage.

1. Erstellen Sie die Jobvorlage.
   a. Navigieren Sie zu Ressourcen → Vorlagen → Hinzufügen und klicken Sie auf Jobvorlage hinzufügen.
   b. Geben Sie den Namen ONTAP/CVO Setup ein
   c. Wählen Sie den Jobtyp aus. „Ausführen“ konfiguriert das System basierend auf einem Playbook.
   d. Wählen Sie das entsprechende Inventar, Projekt, Playbook und die Anmeldeinformationen für das Playbook aus.
   e. Wählen Sie das Playbook ontap_setup.yml für eine On-Prem-Umgebung oder wählen Sie cvo_setup.yml für die Replikation auf eine CVO-Instanz.
   f. Fügen Sie die aus Schritt 4 kopierten globalen Variablen in das Feld „Vorlagenvariablen“ unter der Registerkarte „YAML“ ein.
   g. Klicken Sie auf Speichern.
2. Starten Sie die Jobvorlage.
   a. Navigieren Sie zu Ressourcen → Vorlagen.
   b. Klicken Sie auf die gewünschte Vorlage und dann auf „Starten“.

   Wir werden diese Vorlage verwenden und sie für die anderen Playbooks kopieren.

Replikation für Binär- und Datenbankvolumes

Planung des Playbooks für Binär- und Datenbankreplikation

Konfigurieren und starten Sie die Jobvorlage.

1. Kopieren Sie die zuvor erstellte Jobvorlage.
   a. Navigieren Sie zu Ressourcen → Vorlagen.
   b. Suchen Sie die ONTAP/CVO-Setup-Vorlage und klicken Sie ganz rechts auf „Vorlage kopieren“.
   c. Klicken Sie in der kopierten Vorlage auf „Vorlage bearbeiten“ und ändern Sie den Namen in „Binary and Database Replication Playbook“.
   d. Behalten Sie dasselbe Inventar, Projekt und dieselben Anmeldeinformationen für die Vorlage bei.
   e. Wählen Sie „ora_replication_cg.yml“ als auszuführendes Playbook aus.
   f. Die Variablen bleiben gleich, aber die CVO-Cluster-IP muss in der Variable dst_cluster_ip festgelegt werden.
   g. Klicken Sie auf Speichern.
2. Planen Sie die Jobvorlage.
   a. Navigieren Sie zu Ressourcen → Vorlagen.
   b. Klicken Sie auf die Playbook-Vorlage für Binär- und Datenbankreplikation und dann im oberen Optionssatz auf Zeitpläne.

c. Klicken Sie auf „Hinzufügen“, fügen Sie „Zeitplan für Binär- und Datenbankreplikation“ hinzu, wählen Sie „Startdatum/-zeit zu Beginn der Stunde“, wählen Sie Ihre lokale Zeitzone und die Ausführungshäufigkeit. Die Ausführungshäufigkeit ist, wie oft die SnapMirror -Replikation aktualisiert wird.

> Für die Replikation des Protokollvolumes wird ein separater Zeitplan erstellt, sodass die Replikation in kürzeren Abständen erfolgen kann.

Replikation für Protokollvolumes

Planung des Playbooks zur Protokollreplikation

Jobvorlage konfigurieren und starten

1. Kopieren Sie die zuvor erstellte Jobvorlage.
   a. Navigieren Sie zu Ressourcen → Vorlagen.
   b. Suchen Sie die ONTAP/CVO-Setup-Vorlage und klicken Sie ganz rechts auf „Vorlage kopieren“.
   c. Klicken Sie in der kopierten Vorlage auf „Vorlage bearbeiten“ und ändern Sie den Namen in „Log Replication Playbook“.
   d. Behalten Sie dasselbe Inventar, Projekt und dieselben Anmeldeinformationen für die Vorlage bei.
   e. Wählen Sie „ora_replication_logs.yml“ als auszuführendes Playbook aus.
   f. Die Variablen bleiben gleich, aber die CVO-Cluster-IP muss in der Variable dst_cluster_ip festgelegt werden.
   g. Klicken Sie auf Speichern.
2. Planen Sie die Jobvorlage.
   a. Navigieren Sie zu Ressourcen → Vorlagen.
   b. Klicken Sie auf die Playbook-Vorlage für die Protokollreplikation und dann im oberen Optionssatz auf „Zeitpläne“.
   c. Klicken Sie auf „Hinzufügen“, fügen Sie „Zeitplan für die Protokollreplikation“ hinzu, wählen Sie „Startdatum/-zeit“ zu Beginn der Stunde, wählen Sie Ihre lokale Zeitzone und die Ausführungshäufigkeit. Die Ausführungshäufigkeit ist, wie oft die SnapMirror -Replikation aktualisiert wird.

> Es wird empfohlen, den Protokollzeitplan so einzustellen, dass er stündlich aktualisiert wird, um die Wiederherstellung bis zur letzten stündlichen Aktualisierung sicherzustellen.

Datenbank wiederherstellen

Planung des Playbooks zur Protokollreplikation

Konfigurieren und starten Sie die Jobvorlage.

1. Kopieren Sie die zuvor erstellte Jobvorlage.
   a. Navigieren Sie zu Ressourcen → Vorlagen.
   b. Suchen Sie die ONTAP/CVO-Setup-Vorlage und klicken Sie ganz rechts auf „Vorlage kopieren“.
   c. Klicken Sie in der kopierten Vorlage auf „Vorlage bearbeiten“ und ändern Sie den Namen in

„Wiederherstellungs- und Recovery-Playbook“.

d. Behalten Sie dasselbe Inventar, Projekt und dieselben Anmeldeinformationen für die Vorlage bei.

e. Wählen Sie ora_recovery.yml als auszuführendes Playbook aus.

f. Die Variablen bleiben gleich, aber die CVO-Cluster-IP muss in der Variable dst_cluster_ip festgelegt werden.

g. Klicken Sie auf Speichern.

Dieses Playbook wird erst ausgeführt, wenn Sie bereit sind, Ihre Datenbank am Remote-Standort wiederherzustellen.

Wiederherstellen der Oracle-Datenbank

1. Die Datenvolumes der Oracle-Produktionsdatenbanken vor Ort werden durch die NetApp SnapMirror -Replikation entweder auf einem redundanten ONTAP -Cluster im sekundären Rechenzentrum oder auf Cloud Volume ONTAP in der öffentlichen Cloud geschützt. In einer vollständig konfigurierten Notfallwiederherstellungsumgebung stehen Wiederherstellungs-Compute-Instanzen im sekundären Rechenzentrum oder in der öffentlichen Cloud bereit, um im Katastrophenfall die Produktionsdatenbank wiederherzustellen. Die Standby-Compute-Instanzen werden mit den lokalen Instanzen synchronisiert, indem parallele Updates für OS-Kernel-Patches oder Upgrades im Gleichschritt ausgeführt werden.
2. In dieser gezeigten Lösung wird das Oracle-Binärvolume auf das Ziel repliziert und in der Zielinstanz gemountet, um den Oracle-Software-Stack zu starten. Dieser Ansatz zur Wiederherstellung von Oracle hat Vorteile gegenüber einer Neuinstallation von Oracle in letzter Minute, wenn ein Desaster eingetreten ist. Dadurch wird gewährleistet, dass die Oracle-Installation vollständig mit der aktuellen Installation der Produktionssoftware vor Ort und den Patch-Levels usw. synchronisiert ist. Dies kann jedoch je nach der Struktur der Softwarelizenzierung bei Oracle zusätzliche Auswirkungen auf die Softwarelizenzierung des replizierten Oracle-Binärvolumes am Wiederherstellungsstandort haben oder nicht. Dem Benutzer wird empfohlen, sich bei seinem Softwarelizenzierungspersonal zu erkundigen, um die potenziellen Oracle-Lizenzanforderungen einzuschätzen, bevor er sich für die Verwendung desselben Ansatzes entscheidet.
3. Der Standby-Oracle-Host am Ziel ist mit den erforderlichen Oracle-Konfigurationen konfiguriert.
4. Die SnapMirrors werden beschädigt und die Volumes werden beschreibbar gemacht und auf dem Standby-Oracle-Host gemountet.
5. Das Oracle-Wiederherstellungsmodul führt die folgenden Aufgaben aus, um Oracle am Wiederherstellungsstandort wiederherzustellen und zu starten, nachdem alle DB-Volumes in der Standby-Compute-Instanz gemountet wurden.
   a. Synchronisieren Sie die Steuerdatei: Wir haben doppelte Oracle-Steuerdateien auf verschiedenen Datenbankvolumes bereitgestellt, um wichtige Datenbank-Steuerdateien zu schützen. Eines befindet sich auf dem Datenvolumen und ein anderes auf dem Protokollvolumen. Da Daten- und Protokollvolumes mit unterschiedlicher Häufigkeit repliziert werden, sind sie zum Zeitpunkt der Wiederherstellung nicht synchron.
   b. Oracle-Binärdatei neu verknüpfen: Da die Oracle-Binärdatei auf einen neuen Host verschoben wird, ist eine Neuverknüpfung erforderlich.
   c. Oracle-Datenbank wiederherstellen: Der Wiederherstellungsmechanismus ruft die letzte Systemänderungsnummer im letzten verfügbaren archivierten Protokoll im Oracle-Protokollvolume aus der Steuerdatei ab und stellt die Oracle-Datenbank wieder her, um alle Geschäftstransaktionen wiederherzustellen, die zum Zeitpunkt des Fehlers an den DR-Standort repliziert werden konnten. Die Datenbank wird dann in einer neuen Version gestartet, um Benutzerverbindungen und Geschäftstransaktionen am Wiederherstellungsstandort fortzusetzen.

Bevor Sie das Wiederherstellungs-Playbook ausführen, stellen Sie sicher, dass Sie über Folgendes verfügen: Stellen Sie sicher, dass /etc/oratab und /etc/oraInst.loc vom Oracle-Quellhost auf den Zielhost kopiert werden