



Proteção automatizada de dados Oracle

NetApp database solutions

NetApp
August 18, 2025

Índice

- Proteção automatizada de dados Oracle 1
 - Visão geral da solução 1
 - Proteção de dados automatizada para bancos de dados Oracle 1
- Começando 2
 - AWX/Torre 2
 - Requisitos 2
 - Detalhes de automação 4
 - Parâmetros padrão 6
 - Licença 6
- Procedimento de implantação passo a passo 7
 - Proteção de dados Oracle AWX/Tower 7

Proteção automatizada de dados Oracle

Visão geral da solução

Esta página descreve o método automatizado para implantar o Oracle19c no armazenamento NetApp ONTAP .

Proteção de dados automatizada para bancos de dados Oracle

As organizações estão automatizando seus ambientes para ganhar eficiência, acelerar implantações e reduzir o esforço manual. Ferramentas de gerenciamento de configuração como o Ansible estão sendo usadas para otimizar as operações de banco de dados corporativo. Nesta solução, demonstramos como você pode usar o Ansible para automatizar a proteção de dados do Oracle com o NetApp ONTAP. Ao permitir que administradores de armazenamento, administradores de sistemas e DBAs configurem de forma consistente e rápida a replicação de dados para um data center externo ou para uma nuvem pública, você obtém os seguintes benefícios:

- Elimine complexidades de design e erros humanos e implemente uma implantação consistente e repetível e melhores práticas
- Reduza o tempo de configuração de replicação Intercluster, instanciação de CVO e recuperação de bancos de dados Oracle
- Aumentar a produtividade dos administradores de banco de dados, sistemas e armazenamento
- Fornece fluxo de trabalho de recuperação de banco de dados para facilitar o teste de um cenário de DR.

A NetApp fornece aos clientes módulos e funções Ansible validados para acelerar a implantação, a configuração e o gerenciamento do ciclo de vida do seu ambiente de banco de dados Oracle. Esta solução fornece instruções e código de manual do Ansible para ajudar você a:

Replicação local para local

- Crie vidas intercluster na origem e no destino
- Estabelecer peering de cluster e vserver
- Criar e inicializar o SnapMirror de volumes Oracle
- Crie um cronograma de replicação por meio do AWX/Tower para binários, bancos de dados e logs Oracle
- Restaurar o Oracle DB no destino e colocar o banco de dados online

On Prem para CVO na AWS

- Criar conector AWS
- Criar instância CVO na AWS
- Adicionar cluster local ao Cloud Manager
- Criar vidas intercluster na fonte
- Estabelecer peering de cluster e vserver
- Criar e inicializar o SnapMirror de volumes Oracle
- Crie um cronograma de replicação por meio do AWX/Tower para binários, bancos de dados e logs Oracle
- Restaurar o Oracle DB no destino e colocar o banco de dados online

Depois que estiver pronto, clique "[aqui para começar com a solução](#)".

Começando

Esta solução foi projetada para ser executada em um ambiente AWX/Torre.

AWX/Torre

Para ambientes AWX/Tower, você será orientado na criação de um inventário do gerenciamento de cluster ONTAP e do servidor Oracle (IPs e nomes de host), na criação de credenciais, na configuração de um projeto que extrai o código Ansible do NetApp Automation Github e no modelo de tarefa que inicia a automação.

1. A solução foi projetada para ser executada em um cenário de nuvem privada (local para local) e nuvem híbrida (local para nuvem pública Cloud Volumes ONTAP [CVO])
2. Preencha as variáveis específicas do seu ambiente e copie e cole-as nos campos Extra Vars no seu modelo de trabalho.
3. Depois que as variáveis extras forem adicionadas ao seu modelo de trabalho, você pode iniciar a automação.
4. A automação está definida para ser executada em três fases (configuração, programação de replicação para binários Oracle, banco de dados, logs e programação de replicação apenas para logs) e uma quarta fase para recuperar o banco de dados em um site de DR.
5. Para obter instruções detalhadas sobre como obter as chaves e tokens necessários para a Proteção de Dados do CVO, visite "[Reúna os pré-requisitos para implantações de CVO e Conector](#)".

Requisitos

<strong class="big">No local

Ambiente	Requisitos
Ambiente Ansible	AWX/Torre
	Ansible v.2.10 e superior
	Python 3
	Bibliotecas Python - netapp-lib - xmltodict - jmespath
* ONTAP*	ONTAP versão 9.8 +
	Dois agregados de dados
	NFS vlan e ifgrp criados
Servidor(es) Oracle	RHEL 7/8
	Oracle Linux 7/8
	Interfaces de rede para NFS, pública e gerenciamento opcional
	Ambiente Oracle existente na origem e o sistema operacional Linux equivalente no destino (local de DR ou nuvem pública)

<strong class="big">CVO

Ambiente	Requisitos
Ambiente Ansible	AWX/Torre
	Ansible v.2.10 e superior
	Python 3
	Bibliotecas Python - netapp-lib - xmltodict - jmespath
* ONTAP*	ONTAP versão 9.8 +
	Dois agregados de dados
	NFS vlan e ifgrp criados
Servidor(es) Oracle	RHEL 7/8
	Oracle Linux 7/8
	Interfaces de rede para NFS, pública e gerenciamento opcional
	Ambiente Oracle existente na origem e o sistema operacional Linux equivalente no destino (local de DR ou nuvem pública)
	Defina o espaço de swap apropriado na instância do Oracle EC2, por padrão algumas instâncias do EC2 são implantadas com 0 swap
Gerenciador de Nuvem/AWS	Chave de acesso/secreta da AWS
	Conta do NetApp Cloud Manager
	Token de atualização do NetApp Cloud Manager
	Adicionar lifs intercluster de origem ao grupo de segurança da AWS

<strong class="big">No local

Esta implantação automatizada foi projetada com um único manual do Ansible que consiste em três funções separadas. As funções são para configurações ONTAP, Linux e Oracle. A tabela a seguir descreve quais tarefas estão sendo automatizadas.

Manual de instruções	Tarefas
ontap_setup	Pré-verificação do ambiente ONTAP
	Criação de LIFs Intercluster no cluster de origem (OPCIONAL)
	Criação de LIFs Intercluster no cluster de destino (OPCIONAL)
	Criação de Cluster e Peering SVM
	Criação do SnapMirror de destino e inicialização dos volumes Oracle designados
ora_replication_cg	Habilitar modo de backup para cada banco de dados em /etc/oratab
	Snapshot tirado dos volumes Oracle Binary e Database
	Snapmirror atualizado
	Desative o modo de backup para cada banco de dados em /etc/oratab
ora_replication_log	Alternar o log atual para cada banco de dados em /etc/oratab
	Captura de tela do volume do Oracle Log
	Snapmirror atualizado
ora_recovery	Quebrar SnapMirror
	Habilitar NFS e criar caminho de junção para volumes Oracle no destino
	Configurar o Host Oracle DR
	Montar e verificar volumes Oracle
	Recuperar e iniciar o banco de dados Oracle

<strong class="big">CVO

Esta implantação automatizada foi projetada com um único manual do Ansible que consiste em três funções separadas. As funções são para configurações ONTAP, Linux e Oracle. A tabela a seguir descreve quais tarefas estão sendo automatizadas.

Manual de instruções	Tarefas
configuração_cvo	Pré-verificação do ambiente
	AWS Configure/ID da chave de acesso AWS/Chave secreta/Região padrão
	Criação de função AWS
	Criação de instância do NetApp Cloud Manager Connector na AWS
	Criação de instância do Cloud Volumes ONTAP (CVO) na AWS
	Adicionar cluster ONTAP de origem local ao NetApp Cloud Manager
	Criação do SnapMirror de destino e inicialização dos volumes Oracle designados
ora_replication_cg	Habilitar modo de backup para cada banco de dados em /etc/oratab
	Snapshot tirado dos volumes Oracle Binary e Database
	Snapmirror atualizado
	Desative o modo de backup para cada banco de dados em /etc/oratab
ora_replication_log	Alternar o log atual para cada banco de dados em /etc/oratab
	Captura de tela do volume do Oracle Log
	Snapmirror atualizado
ora_recovery	Quebrar SnapMirror
	Habilitar NFS e criar caminho de junção para volumes Oracle no CVO de destino
	Configurar o Host Oracle DR
	Montar e verificar volumes Oracle
	Recuperar e iniciar o banco de dados Oracle

Parâmetros padrão

Para simplificar a automação, predefinimos muitos parâmetros necessários do Oracle com valores padrão. Geralmente não é necessário alterar os parâmetros padrão para a maioria das implantações. Um usuário mais avançado pode fazer alterações nos parâmetros padrão com cautela. Os parâmetros padrão estão localizados em cada pasta de função, no diretório defaults.

Licença

Você deve ler as informações de licença conforme consta no repositório do Github. Ao acessar, baixar, instalar ou usar o conteúdo deste repositório, você concorda com os termos da licença estabelecida ["aqui"](#).

Observe que há certas restrições quanto à produção e/ou compartilhamento de quaisquer trabalhos derivados do conteúdo deste repositório. Por favor, certifique-se de ler os termos do ["Licença"](#) antes de usar o conteúdo. Se você não concordar com todos os termos, não acesse, baixe ou use o conteúdo deste repositório.

Depois de estar pronto, clique ["aqui para procedimentos detalhados de AWX/Torre"](#).

Procedimento de implantação passo a passo

Esta página descreve a proteção de dados automatizada do Oracle19c no armazenamento NetApp ONTAP .

Proteção de dados Oracle AWX/Tower

Crie o inventário, grupo, hosts e credenciais para seu ambiente

Esta seção descreve a configuração de inventário, grupos, hosts e credenciais de acesso no AWX/Ansible Tower que preparam o ambiente para o consumo de soluções automatizadas da NetApp .

1. Configurar o inventário.
 - a. Navegue até Recursos → Inventário → Adicionar e clique em Adicionar inventário.
 - b. Forneça o nome e os detalhes da organização e clique em Salvar.
 - c. Na página Inventários, clique no inventário criado.
 - d. Navegue até o submenu Grupos e clique em Adicionar.
 - e. Forneça o nome do oráculo para seu primeiro grupo e clique em Salvar.
 - f. Repita o processo para um segundo grupo chamado dr_oracle.
 - g. Selecione o grupo oracle criado, vá para o submenu Hosts e clique em Adicionar novo host.
 - h. Forneça o endereço IP do IP de gerenciamento do host Oracle de origem e clique em Salvar.
 - i. Este processo deve ser repetido para o grupo dr_oracle e adicionar o IP/nome do host de gerenciamento do host DR/Destination Oracle.



Abaixo estão as instruções para criar os tipos de credenciais e credenciais para On-Prem com ONTAP ou CVO na AWS.

No local

1. Configure as credenciais.
2. Criar tipos de credenciais. Para soluções envolvendo o ONTAP, você deve configurar o tipo de credencial para corresponder às entradas de nome de usuário e senha.
 - a. Navegue até Administração → Tipos de credenciais e clique em Adicionar.
 - b. Forneça o nome e a descrição.
 - c. Cole o seguinte conteúdo em Configuração de entrada:

```
fields:
  - id: dst_cluster_username
    type: string
    label: Destination Cluster Username
  - id: dst_cluster_password
    type: string
    label: Destination Cluster Password
    secret: true
  - id: src_cluster_username
    type: string
    label: Source Cluster Username
  - id: src_cluster_password
    type: string
    label: Source Cluster Password
    secret: true
```

- d. Cole o seguinte conteúdo na Configuração do Injetor e clique em Salvar:

```
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. Criar credencial para ONTAP
 - a. Navegue até Recursos → Credenciais e clique em Adicionar.
 - b. Insira o nome e os detalhes da organização para as credenciais do ONTAP
 - c. Selecione o tipo de credencial que foi criado na etapa anterior.
 - d. Em Detalhes do tipo, insira o nome de usuário e a senha para seus clusters de origem e destino.
 - e. Clique em Salvar
4. Criar credencial para Oracle
 - a. Navegue até Recursos → Credenciais e clique em Adicionar.
 - b. Insira o nome e os detalhes da organização para Oracle

- c. Selecione o tipo de credencial Máquina.
- d. Em Detalhes do tipo, insira o nome de usuário e a senha para os hosts Oracle.
- e. Selecione o Método de Escalonamento de Privilégios correto e insira o nome de usuário e a senha.
- f. Clique em Salvar
- g. Repita o processo, se necessário, para uma credencial diferente para o host dr_oracle.

CVO

1. Configure as credenciais.
2. Crie tipos de credenciais. Para soluções envolvendo o ONTAP, você deve configurar o tipo de credencial para corresponder às entradas de nome de usuário e senha. Também adicionaremos entradas para o Cloud Central e a AWS.
 - a. Navegue até Administração → Tipos de credenciais e clique em Adicionar.
 - b. Forneça o nome e a descrição.
 - c. Cole o seguinte conteúdo em Configuração de entrada:

```
fields:
  - id: dst_cluster_username
    type: string
    label: CVO Username
  - id: dst_cluster_password
    type: string
    label: CVO Password
    secret: true
  - id: cvo_svm_password
    type: string
    label: CVO SVM Password
    secret: true
  - id: src_cluster_username
    type: string
    label: Source Cluster Username
  - id: src_cluster_password
    type: string
    label: Source Cluster Password
    secret: true
  - id: regular_id
    type: string
    label: Cloud Central ID
    secret: true
  - id: email_id
    type: string
    label: Cloud Manager Email
    secret: true
  - id: cm_password
    type: string
    label: Cloud Manager Password
    secret: true
  - id: access_key
    type: string
    label: AWS Access Key
    secret: true
  - id: secret_key
    type: string
    label: AWS Secret Key
    secret: true
  - id: token
    type: string
    label: Cloud Central Refresh Token
    secret: true
```

d. Cole o seguinte conteúdo na Configuração do Injetor e clique em Salvar:

```

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. Criar credencial para ONTAP/CVO/AWS

- a. Navegue até Recursos → Credenciais e clique em Adicionar.
- b. Insira o nome e os detalhes da organização para as credenciais do ONTAP
- c. Selecione o tipo de credencial que foi criado na etapa anterior.
- d. Em Detalhes do tipo, insira o nome de usuário e a senha para seus clusters de origem e CVO, Cloud Central/Manager, chave de acesso/secreta da AWS e token de atualização do Cloud Central.
- e. Clique em Salvar

4. Criar credencial para Oracle (fonte)

- a. Navegue até Recursos → Credenciais e clique em Adicionar.
- b. Insira o nome e os detalhes da organização para o host Oracle
- c. Selecione o tipo de credencial Máquina.
- d. Em Detalhes do tipo, insira o nome de usuário e a senha para os hosts Oracle.
- e. Selecione o Método de Escalonamento de Privilégios correto e insira o nome de usuário e a senha.
- f. Clique em Salvar

5. Criar credencial para destino Oracle

- a. Navegue até Recursos → Credenciais e clique em Adicionar.
- b. Insira o nome e os detalhes da organização para o host DR Oracle
- c. Selecione o tipo de credencial Máquina.
- d. Em Detalhes do tipo, insira o nome de usuário (ec2-user ou, se você o alterou do padrão, insira-o) e a chave privada SSH
- e. Selecione o Método de Escalonamento de Privilégios correto (sudo) e insira o nome de usuário e a senha, se necessário.
- f. Clique em Salvar

Criar um projeto

1. Vá para Recursos → Projetos e clique em Adicionar.
 - a. Insira o nome e os detalhes da organização.
 - b. Selecione Git no campo Tipo de credencial de controle de origem.
 - c. digitar `https://github.com/NetApp-Automation/na_oracle19c_data_protection.git` como URL de controle de origem.
 - d. Clique em Salvar.
 - e. O projeto pode precisar ser sincronizado ocasionalmente quando o código-fonte muda.

Configurar variáveis globais

As variáveis definidas nesta seção se aplicam a todos os hosts Oracle, bancos de dados e ao cluster ONTAP .

1. Insira os parâmetros específicos do seu ambiente nas seguintes variáveis globais incorporadas ou no formato vars.



Os itens em azul devem ser alterados para combinar com seu ambiente.

No local

```
# 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"
```

Manuais de Automação

Há quatro manuais separados que precisam ser executados.

1. Manual para configurar seu ambiente, no local ou CVO.
2. Manual para replicar binários e bancos de dados Oracle de acordo com um cronograma
3. Manual para replicar logs do Oracle de acordo com uma programação
4. Manual para recuperar seu banco de dados em um host de destino

Configuração ONTAP/CVO

[.underline]* Configuração ONTAP e CVO*

Configure e inicie o modelo de trabalho.

1. Crie o modelo de trabalho.
 - a. Navegue até Recursos → Modelos → Adicionar e clique em Adicionar modelo de trabalho.
 - b. Digite o nome ONTAP/CVO Setup
 - c. Selecione o tipo de trabalho; Executar configura o sistema com base em um manual.
 - d. Selecione o inventário, o projeto, o manual e as credenciais correspondentes para o manual.
 - e. Selecione o playbook `ontap_setup.yml` para um ambiente local ou selecione o `cvo_setup.yml` para replicar para uma instância CVO.
 - f. Cole as variáveis globais copiadas da etapa 4 no campo Variáveis de modelo na guia YAML.
 - g. Clique em Salvar.
2. Inicie o modelo de trabalho.
 - a. Navegue até Recursos → Modelos.
 - b. Clique no modelo desejado e depois clique em Iniciar.



Usaremos esse modelo e o copiaremos para os outros manuais.

Replicação para volumes binários e de banco de dados

Agendamento do Manual de Replicação Binária e de Banco de Dados

Configure e inicie o modelo de trabalho.

1. Copie o modelo de trabalho criado anteriormente.
 - a. Navegue até Recursos → Modelos.
 - b. Encontre o modelo de configuração ONTAP/CVO e, na extrema direita, clique em Copiar modelo
 - c. Clique em Editar modelo no modelo copiado e altere o nome para Manual de replicação binária e de banco de dados.
 - d. Mantenha o mesmo inventário, projeto e credenciais para o modelo.
 - e. Selecione `ora_replication_cg.yml` como o manual a ser executado.
 - f. As variáveis permanecerão as mesmas, mas o IP do cluster CVO precisará ser definido na variável `dst_cluster_ip`.
 - g. Clique em Salvar.
2. Agende o modelo de trabalho.
 - a. Navegue até Recursos → Modelos.
 - b. Clique no modelo Manual de replicação binária e de banco de dados e, em seguida, clique em Agendamentos no conjunto superior de opções.
 - c. Clique em Adicionar, adicione o Nome Agendado para Replicação Binária e de Banco de Dados, escolha a Data/hora de início no início da hora, escolha seu Fuso horário local e Frequência de execução. A frequência de execução será sempre que a replicação do SnapMirror será atualizada.



Um cronograma separado será criado para a replicação do volume de log, para que ele possa ser replicado em uma cadência mais frequente.

Replicação para volumes de log

Agendamento do Manual de Replicação de Log

Configurar e iniciar o modelo de trabalho

1. Copie o modelo de trabalho criado anteriormente.
 - a. Navegue até Recursos → Modelos.
 - b. Encontre o modelo de configuração ONTAP/CVO e, na extrema direita, clique em Copiar modelo
 - c. Clique em Editar modelo no modelo copiado e altere o nome para Manual de replicação de log.
 - d. Mantenha o mesmo inventário, projeto e credenciais para o modelo.
 - e. Selecione `ora_replication_logs.yml` como o manual a ser executado.
 - f. As variáveis permanecerão as mesmas, mas o IP do cluster CVO precisará ser definido na variável `dst_cluster_ip`.
 - g. Clique em Salvar.
2. Agende o modelo de trabalho.
 - a. Navegue até Recursos → Modelos.
 - b. Clique no modelo Log Replication Playbook e depois clique em Schedules no conjunto superior de opções.
 - c. Clique em Adicionar, adicione o Nome Agendado para Replicação de Log, escolha a Data/hora de início no início da hora, escolha seu Fuso horário local e Frequência de execução. A frequência de execução será sempre que a replicação do SnapMirror será atualizada.



É recomendável definir o agendamento do log para atualizar a cada hora para garantir a recuperação para a última atualização horária.

Restaurar e recuperar banco de dados

Agendamento do Manual de Replicação de Log

Configure e inicie o modelo de trabalho.

1. Copie o modelo de trabalho criado anteriormente.
 - a. Navegue até Recursos → Modelos.
 - b. Encontre o modelo de configuração ONTAP/CVO e, na extrema direita, clique em Copiar modelo
 - c. Clique em Editar modelo no modelo copiado e altere o nome para Manual de restauração e recuperação.
 - d. Mantenha o mesmo inventário, projeto e credenciais para o modelo.
 - e. Selecione `ora_recovery.yml` como o manual a ser executado.
 - f. As variáveis permanecerão as mesmas, mas o IP do cluster CVO precisará ser definido na variável `dst_cluster_ip`.
 - g. Clique em Salvar.



Este manual não será executado até que você esteja pronto para restaurar seu banco de dados no site remoto.

Recuperando o banco de dados Oracle

1. Os volumes de dados dos bancos de dados Oracle de produção local são protegidos por meio da replicação do NetApp SnapMirror para um cluster ONTAP redundante no data center secundário ou no Cloud Volume ONTAP na nuvem pública. Em um ambiente de recuperação de desastres totalmente configurado, as instâncias de computação de recuperação no data center secundário ou na nuvem pública ficam em espera e prontas para recuperar o banco de dados de produção em caso de desastre. As instâncias de computação em espera são mantidas sincronizadas com as instâncias locais por meio da execução de atualizações paralelas no patch do kernel do sistema operacional ou atualização em sincronia.
2. Nesta solução demonstrada, o volume binário do Oracle é replicado no destino e montado na instância de destino para ativar a pilha de software do Oracle. Essa abordagem para recuperar o Oracle tem vantagem sobre uma nova instalação do Oracle de última hora quando ocorre um desastre. Ele garante que a instalação do Oracle esteja totalmente sincronizada com a instalação atual do software de produção local, níveis de patch etc. No entanto, isso pode ou não ter implicações adicionais no licenciamento de software para o volume binário Oracle replicado no site de recuperação, dependendo de como o licenciamento de software é estruturado com a Oracle. É recomendado que o usuário consulte sua equipe de licenciamento de software para avaliar os possíveis requisitos de licenciamento da Oracle antes de decidir usar a mesma abordagem.
3. O host Oracle em espera no destino é configurado com as configurações de pré-requisito do Oracle.
4. Os SnapMirrors são quebrados e os volumes são tornados graváveis e montados no host Oracle em espera.
5. O módulo de recuperação do Oracle executa as seguintes tarefas para recuperar e iniciar o Oracle no site de recuperação depois que todos os volumes do banco de dados são montados na instância de computação em espera.
 - a. Sincronizar o arquivo de controle: implantamos arquivos de controle Oracle duplicados em diferentes volumes de banco de dados para proteger o arquivo de controle crítico do banco de dados. Um está no volume de dados e outro está no volume de log. Como os volumes de dados e logs são replicados em frequências diferentes, eles estarão fora de sincronia no momento da recuperação.
 - b. Revincular binário Oracle: como o binário Oracle é realocado para um novo host, ele precisa ser revinculado.
 - c. Recuperar banco de dados Oracle: O mecanismo de recuperação recupera o último Número de Alteração do Sistema no último log arquivado disponível no volume de log Oracle do arquivo de controle e recupera o banco de dados Oracle para recuperar todas as transações comerciais que puderam ser replicadas no site de DR no momento da falha. O banco de dados é então iniciado em uma nova encarnação para continuar as conexões do usuário e as transações comerciais no site de recuperação.



Antes de executar o manual de recuperação, certifique-se de ter o seguinte: Certifique-se de copiar `/etc/oratab` e `/etc/orainst.loc` do host Oracle de origem para o host de destino

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSAIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES DOCUMENTOS, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.