Soluções de banco de dados em nuvem híbrida com SnapCenter

NetApp database solutions

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/pt-br/netapp-solutions-databases/dbops/hybrid-dbops-snapcenter-usecases.html on August 18, 2025. Always check docs.netapp.com for the latest.

Índice

Soluções de banco de dados em nuvem híbrida com SnapCenter . . . 1
- TR-4908: Visão geral de soluções de banco de dados em nuvem híbrida com SnapCenter . . . 1
- Arquitetura da Solução . . . 2
- Requisitos do SnapCenter . . . 3
  - Requisitos . . . 3
- Configuração de pré-requisitos . . . 4
  - Configuração de pré-requisitos . . . 4
  - Pré-requisitos no local . . . 5
  - Pré-requisitos para a nuvem pública . . . 10
- Visão geral de introdução . . . 11
  - Visão geral de introdução . . . 11
  - Começando no local . . . 12
  - Introdução à nuvem pública da AWS . . . 64
- Fluxo de trabalho para expansão de desenvolvimento/teste para a nuvem . . . 90
  - Clonar um banco de dados Oracle para desenvolvimento/teste a partir de um backup de snapshot replicado . . . 90
  - Clonar um banco de dados SQL para desenvolvimento/teste a partir de um backup de Snapshot replicado . . . 100
  - Configuração pós-clone . . . 107
  - Atualizar banco de dados clone . . . 108
  - Onde procurar ajuda? . . . 108
- Fluxo de trabalho de recuperação de desastres . . . 108
  - Clonar um banco de dados de produção Oracle local para a nuvem para recuperação de desastres . . . 108
  - Validação e configuração de clone pós-DR para Oracle . . . 118
  - Clonar um banco de dados de produção SQL local para a nuvem para recuperação de desastres . . . 119
  - Validação e configuração do clone pós-DR para SQL . . . 125
  - Onde procurar ajuda? . . . 126

Soluções de banco de dados em nuvem híbrida com SnapCenter

TR-4908: Visão geral de soluções de banco de dados em nuvem híbrida com SnapCenter

Alan Cao, Felix Melligan, NetApp

Esta solução fornece ao campo e aos clientes da NetApp instruções e orientações para configurar, operar e migrar bancos de dados para um ambiente de nuvem híbrida usando a ferramenta baseada em GUI do NetApp SnapCenter e o serviço de armazenamento CVO da NetApp em nuvens públicas para os seguintes casos de uso:

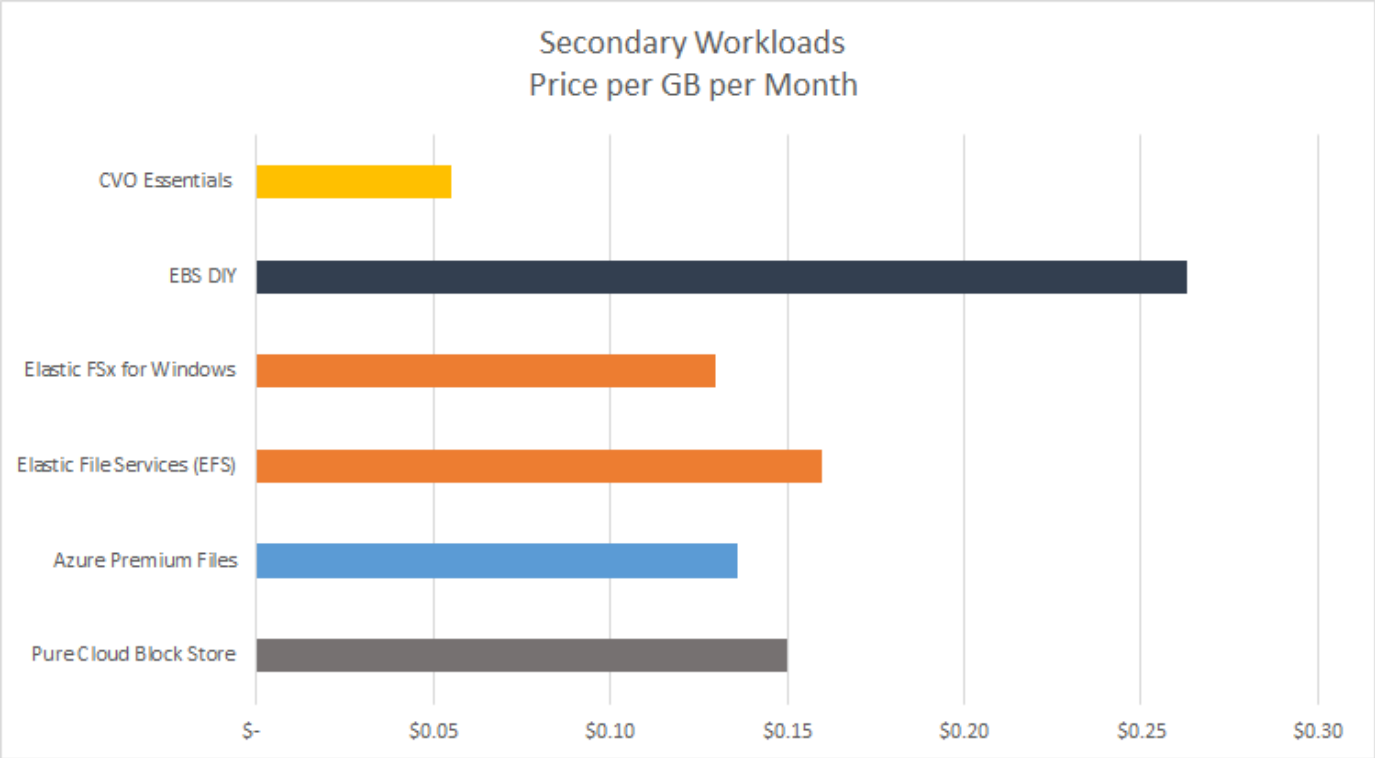
- Operações de desenvolvimento/teste de banco de dados na nuvem híbrida
- Recuperação de desastres de banco de dados na nuvem híbrida

Hoje, muitos bancos de dados empresariais ainda residem em data centers corporativos privados por motivos de desempenho, segurança e/ou outros. Esta solução de banco de dados em nuvem híbrida permite que as empresas operem seus bancos de dados primários no local enquanto usam uma nuvem pública para operações de banco de dados de desenvolvimento/teste, bem como para recuperação de desastres, a fim de reduzir custos operacionais e de licenciamento.

Muitos bancos de dados corporativos, como Oracle, SQL Server, SAP HANA e assim por diante, têm altos custos operacionais e de licenciamento. Muitos clientes pagam uma taxa de licença única, bem como custos anuais de suporte com base no número de núcleos de computação em seu ambiente de banco de dados, independentemente de os núcleos serem usados para desenvolvimento, teste, produção ou recuperação de desastres. Muitos desses ambientes podem não ser totalmente utilizados durante o ciclo de vida do aplicativo.

As soluções oferecem uma opção para os clientes reduzirem potencialmente sua contagem de núcleos licenciáveis movendo seus ambientes de banco de dados dedicados ao desenvolvimento, teste ou recuperação de desastres para a nuvem. Ao usar escala de nuvem pública, redundância, alta disponibilidade e um modelo de cobrança baseado no consumo, a economia de custos com licenciamento e operação pode ser substancial, sem sacrificar a usabilidade ou disponibilidade do aplicativo.

Além da potencial economia nos custos de licença do banco de dados, o modelo de licença CVO baseado em capacidade da NetApp permite que os clientes economizem nos custos de armazenamento por GB, ao mesmo tempo em que oferece alto nível de capacidade de gerenciamento de banco de dados que não está disponível em serviços de armazenamento concorrentes. O gráfico a seguir mostra uma comparação de custos de armazenamento de serviços de armazenamento populares disponíveis na nuvem pública.



Esta solução demonstra que, usando a ferramenta de software baseada em GUI SnapCenter e a tecnologia NetApp SnapMirror , as operações de banco de dados em nuvem híbrida podem ser facilmente configuradas, implementadas e operadas.

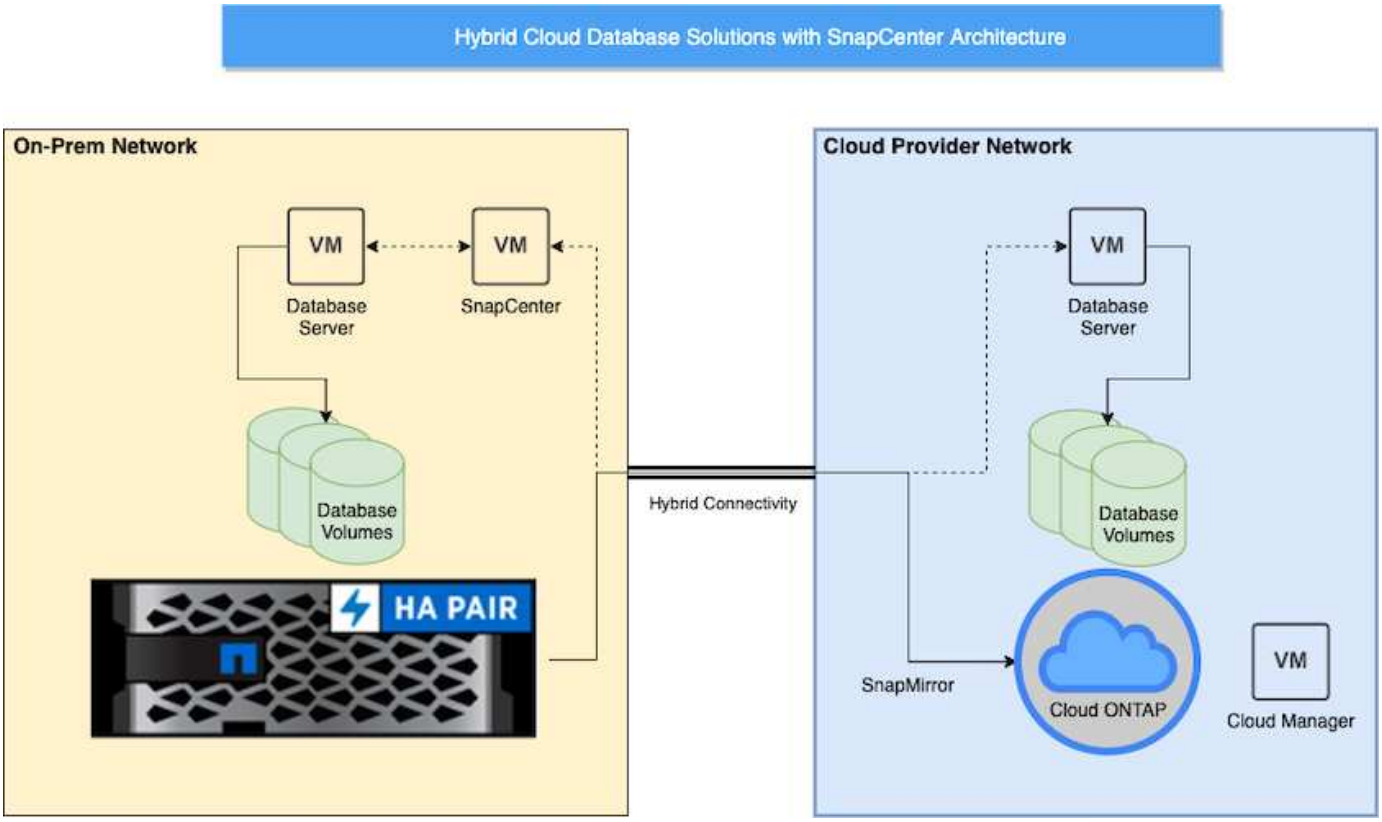
Os vídeos a seguir demonstram o SnapCenter em ação:

- "Backup de um banco de dados Oracle em uma nuvem híbrida usando SnapCenter"
- "SnapCenter- Clonar DEV/TEST para AWS Cloud para um banco de dados Oracle"

Notavelmente, embora as ilustrações ao longo deste documento mostrem o CVO como uma instância de armazenamento de destino na nuvem pública, a solução também é totalmente validada para a nova versão do mecanismo de armazenamento FSx ONTAP para AWS.

Arquitetura da Solução

O diagrama de arquitetura a seguir ilustra uma implementação típica de operação de banco de dados corporativo em uma nuvem híbrida para operações de desenvolvimento/teste e recuperação de desastres.



Em operações comerciais normais, volumes de banco de dados sincronizados na nuvem podem ser clonados e montados em instâncias de banco de dados de desenvolvimento/teste para desenvolvimento ou teste de aplicativos. Em caso de falha, os volumes de banco de dados sincronizados na nuvem podem ser ativados para recuperação de desastres.

Requisitos do SnapCenter

Esta solução foi projetada em um ambiente de nuvem híbrida para oferecer suporte a bancos de dados de produção locais que podem ser expandidos para todas as nuvens públicas populares para operações de desenvolvimento/teste e recuperação de desastres.

Esta solução oferece suporte a todos os bancos de dados atualmente suportados pelo SnapCenter, embora apenas bancos de dados Oracle e SQL Server sejam demonstrados aqui. Esta solução é validada com cargas de trabalho de bancos de dados virtualizados, embora cargas de trabalho bare-metal também sejam suportadas.

Presumimos que os servidores de banco de dados de produção sejam hospedados no local com volumes de banco de dados apresentados aos hosts de banco de dados de um cluster de armazenamento ONTAP . O SnapCenter software é instalado no local para backup de banco de dados e replicação de dados para a nuvem. Um controlador Ansible é recomendado, mas não obrigatório, para automação de implantação de banco de dados ou sincronização de kernel do sistema operacional e configuração de banco de dados com uma instância de DR em espera ou instâncias de desenvolvimento/teste na nuvem pública.

Requisitos

Ambiente	Requisitos
No local	Quaisquer bancos de dados e versões suportados pelo SnapCenter
	SnapCenter v4.4 ou superior
	Ansible v2.09 ou superior
	Cluster ONTAP 9.x
	LIFs intercluster configurados
	Conectividade do local para uma VPC na nuvem (VPN, interconexão e assim por diante)
	Portas de rede abertas - ssh 22 - tcp 8145, 8146, 10000, 11104, 11105
Nuvem - AWS	"Conector do Gerenciador de Nuvem"
	"Cloud Volumes ONTAP"
	Correspondência de instâncias do DB OS EC2 com o On-prem
Nuvem - Azure	"Conector do Gerenciador de Nuvem"
	"Cloud Volumes ONTAP"
	Correspondência de máquinas virtuais do Azure do DB OS com o local
Nuvem - GCP	"Conector do Gerenciador de Nuvem"
	"Cloud Volumes ONTAP"
	Correspondência de instâncias do Google Compute Engine do sistema operacional DB com instâncias locais

Configuração de pré-requisitos

Configuração de pré-requisitos

Certos pré-requisitos devem ser configurados no local e na nuvem antes da execução de cargas de trabalho de banco de dados em nuvem híbrida. A seção a seguir fornece um resumo de alto nível desse processo, e os links a seguir fornecem mais informações sobre a configuração necessária do sistema.

No local

- Instalação e configuração do SnapCenter
- Configuração de armazenamento do servidor de banco de dados local
- Requisitos de licenciamento
- Rede e segurança
- Automação

Nuvem pública

- Um login do NetApp Cloud Central

- Acesso à rede a partir de um navegador da web para vários terminais
- Um local de rede para um conector
- Permissões do provedor de nuvem
- Networking para serviços individuais

Considerações importantes:

1. Onde implantar o Cloud Manager Connector?
2. Dimensionamento e arquitetura do Cloud Volume ONTAP
3. Nó único ou alta disponibilidade?

Os links a seguir fornecem mais detalhes:

"No local"

"Nuvem Pública"

Pré-requisitos no local

As seguintes tarefas devem ser concluídas no local para preparar o ambiente de carga de trabalho do banco de dados de nuvem híbrida SnapCenter .

Instalação e configuração do SnapCenter

A ferramenta NetApp SnapCenter é um aplicativo baseado no Windows que normalmente é executado em um ambiente de domínio do Windows, embora a implantação em grupo de trabalho também seja possível. Ele é baseado em uma arquitetura multicamadas que inclui um servidor de gerenciamento centralizado (o servidor SnapCenter) e um plug-in SnapCenter nos hosts do servidor de banco de dados para cargas de trabalho do banco de dados. Aqui estão algumas considerações importantes para a implantação de nuvem híbrida.

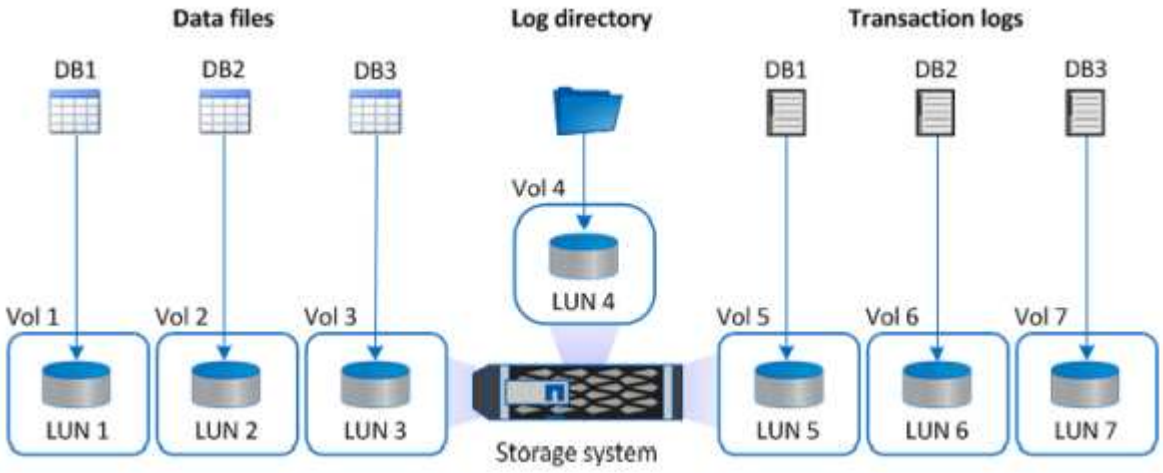
- **Implantação de instância única ou HA.** A implantação de HA fornece redundância no caso de falha de um único servidor de instância do SnapCenter .
- **Resolução de nomes.** O DNS deve ser configurado no servidor SnapCenter para resolver todos os hosts do banco de dados, bem como no SVM de armazenamento para pesquisa direta e reversa. O DNS também deve ser configurado em servidores de banco de dados para resolver o servidor SnapCenter e o SVM de armazenamento para pesquisa direta e reversa.
- **Configuração de controle de acesso baseado em função (RBAC).** Para cargas de trabalho de bancos de dados mistos, talvez você queira usar o RBAC para segregar a responsabilidade de gerenciamento para diferentes plataformas de banco de dados, como um administrador para o banco de dados Oracle ou um administrador para o SQL Server. Permissões necessárias devem ser concedidas ao usuário administrador do banco de dados.
- **Habilite a estratégia de backup baseada em políticas.** Para garantir a consistência e a confiabilidade do backup.
- **Abra as portas de rede necessárias no firewall.** Para que o servidor SnapCenter local se comunique com agentes instalados no host do banco de dados na nuvem.
- **As portas devem estar abertas para permitir o tráfego do SnapMirror entre o local e a nuvem pública.** O servidor SnapCenter depende do ONTAP SnapMirror para replicar backups de Snapshot no local para SVMs de armazenamento CVO em nuvem.

Após cuidadoso planejamento e consideração da pré-instalação, clique aqui"Pré-requisitos de instalação do SnapCenter" para obter detalhes sobre a instalação e configuração do SnapCenter .

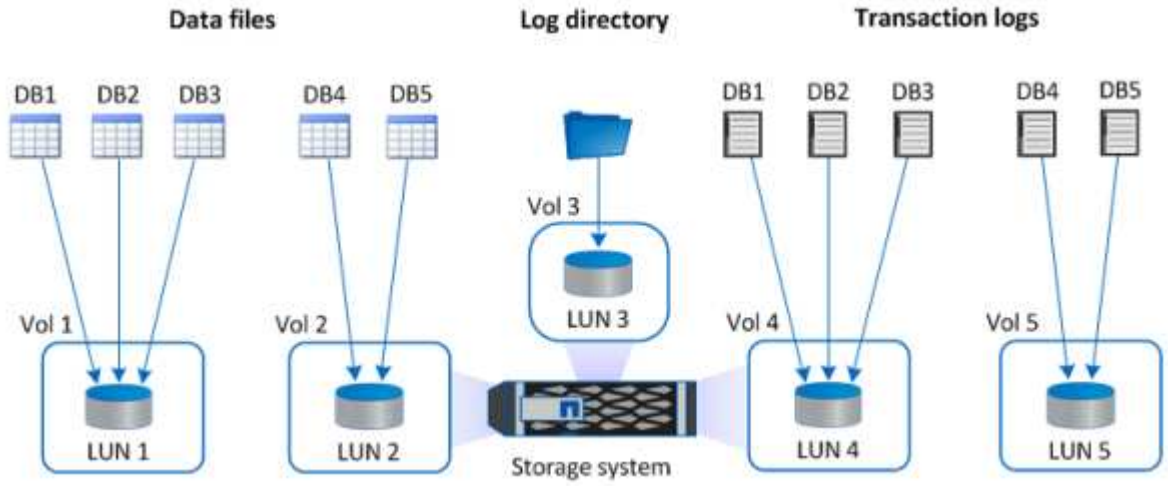
Configuração de armazenamento do servidor de banco de dados local

O desempenho do armazenamento desempenha um papel importante no desempenho geral de bancos de dados e aplicativos. Um layout de armazenamento bem projetado pode não apenas melhorar o desempenho do banco de dados, mas também facilitar o gerenciamento do backup e da recuperação do banco de dados. Vários fatores devem ser considerados ao definir seu layout de armazenamento, incluindo o tamanho do banco de dados, a taxa de alteração de dados esperada para o banco de dados e a frequência com que você executa backups.

Anexar LUNs de armazenamento diretamente à VM convidada por NFS ou iSCSI para cargas de trabalho de banco de dados virtualizado geralmente fornece melhor desempenho do que o armazenamento alocado via VMDK. A NetApp recomenda o layout de armazenamento para um grande banco de dados SQL Server em LUNs ilustrado na figura a seguir.



A figura a seguir mostra o layout de armazenamento recomendado pela NetApp para bancos de dados SQL Server pequenos ou médios em LUNs.

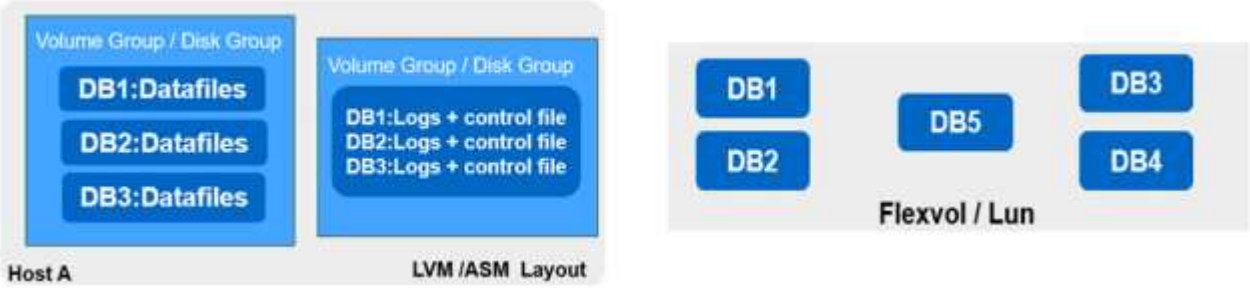


O diretório Log é dedicado ao SnapCenter para executar o rollup do log de transações para recuperação do banco de dados. Para um banco de dados extra grande, vários LUNs podem ser alocados a um volume para melhor desempenho.

Para cargas de trabalho de banco de dados Oracle, o SnapCenter oferece suporte a ambientes de banco de dados apoiados pelo armazenamento ONTAP que são montados no host como dispositivos físicos ou virtuais. Você pode hospedar o banco de dados inteiro em um ou vários dispositivos de armazenamento, com base na criticidade do ambiente. Normalmente, os clientes isolam arquivos de dados em armazenamento dedicado de todos os outros arquivos, como arquivos de controle, arquivos de refazer e arquivos de log de arquivamento. Isso ajuda os administradores a restaurar rapidamente (SnapRestore de arquivo único ONTAP) ou clonar um grande banco de dados crítico (escala de petabytes) usando a tecnologia Snapshot em poucos segundos ou minutos.

Para cargas de trabalho de missão crítica que são sensíveis à latência, um volume de armazenamento dedicado deve ser implantado em diferentes tipos de arquivos Oracle para atingir a melhor latência possível. Para um banco de dados grande, vários LUNs (a NetApp recomenda até oito) por volume devem ser alocados para arquivos de dados.

Para bancos de dados Oracle menores, o SnapCenter oferece suporte a layouts de armazenamento compartilhado nos quais você pode hospedar vários bancos de dados ou parte de um banco de dados no mesmo volume de armazenamento ou LUN. Como exemplo desse layout, você pode hospedar arquivos de dados para todos os bancos de dados em um grupo de discos +DATA ASM ou em um grupo de volumes. O restante dos arquivos (refazer, log de arquivamento e arquivos de controle) podem ser hospedados em outro grupo de discos dedicado ou grupo de volumes (LVM). Um cenário de implantação como esse é ilustrado abaixo.



Para facilitar a realocação de bancos de dados Oracle, o binário Oracle deve ser instalado em um LUN separado, incluído na política de backup regular. Isso garante que, no caso de realocação do banco de dados para um novo host de servidor, a pilha Oracle possa ser iniciada para recuperação sem quaisquer problemas potenciais devido a um binário Oracle fora de sincronia.

Requisitos de licenciamento

SnapCenter é um software licenciado da NetApp. Geralmente está incluído em uma licença ONTAP local. No entanto, para implantação em nuvem híbrida, uma licença de nuvem para o SnapCenter também é necessária para adicionar o CVO ao SnapCenter como um destino de replicação de dados. Revise os links a seguir para obter detalhes sobre a licença baseada em capacidade padrão do SnapCenter :

"Licenças baseadas em capacidade padrão do SnapCenter"

Rede e segurança

Em uma operação de banco de dados híbrido que requer um banco de dados de produção local que possa ser expandido para a nuvem para desenvolvimento/teste e recuperação de desastres, a rede e a segurança são fatores importantes a serem considerados ao configurar o ambiente e conectar-se à nuvem pública a partir de um data center local.

Nuvens públicas normalmente usam uma nuvem privada virtual (VPC) para isolar diferentes usuários dentro de uma plataforma de nuvem pública. Dentro de uma VPC individual, a segurança é controlada usando medidas como grupos de segurança que são configuráveis com base nas necessidades do usuário para o bloqueio de uma VPC.

A conectividade do data center local com a VPC pode ser protegida por meio de um túnel VPN. No gateway VPN, a segurança pode ser reforçada usando regras de NAT e firewall que bloqueiam tentativas de estabelecer conexões de rede de hosts na Internet para hosts dentro do data center corporativo.

Para considerações de rede e segurança, revise as regras de CVO de entrada e saída relevantes para sua nuvem pública de escolha:

- "Regras de grupo de segurança para CVO - AWS"
- "Regras de grupo de segurança para CVO - Azure"
- "Regras de firewall para CVO - GCP"

Usando a automação do Ansible para sincronizar instâncias de banco de dados entre o local e a nuvem - opcional

Para simplificar o gerenciamento de um ambiente de banco de dados de nuvem híbrida, a NetApp recomenda, mas não exige, que você implante um controlador Ansible para automatizar algumas tarefas de gerenciamento, como manter instâncias de computação locais e na nuvem sincronizadas. Isso é particularmente importante porque uma instância de computação fora de sincronia na nuvem pode tornar o banco de dados recuperado na nuvem sujeito a erros devido a pacotes de kernel ausentes e outros problemas.

O recurso de automação de um controlador Ansible também pode ser usado para aumentar o SnapCenter em determinadas tarefas, como dividir a instância do SnapMirror para ativar a cópia de dados de DR para produção.

Siga estas instruções para configurar seu nó de controle Ansible para máquinas RedHat ou CentOS:

1. Requisitos para o nó de controle do Ansible:
    a. Uma máquina RHEL/CentOS com os seguintes pacotes instalados:
        i. Python3
        ii. Pip3

iii. Ansible (versão superior a 2.10.0)
iv. Git

Se você tiver uma máquina RHEL/CentOS nova sem os requisitos acima instalados, siga as etapas abaixo para configurar essa máquina como o nó de controle do Ansible:

1. Habilitar o repositório Ansible para RHEL-8/RHEL-7
   a. Para RHEL-8 (execute o comando abaixo como root)

```
subscription-manager repos --enable ansible-2.9-for-rhel-8-x86_64-
rpms
```

   b. Para RHEL-7 (execute o comando abaixo como root)

```
subscription-manager repos --enable rhel-7-server-ansible-2.9-rpms
```

2. Cole o conteúdo abaixo no Terminal

```
sudo yum -y install python3 >> install.log
sudo yum -y install python3-pip >> install.log
python3 -W ignore -m pip --disable-pip-version-check install ansible >>
install.log
sudo yum -y install git >> install.log
```

Siga estas instruções para configurar seu nó de controle Ansible para máquinas Ubuntu ou Debian:

1. Requisitos para o nó de controle do Ansible:
   a. Uma máquina Ubuntu/Debian com os seguintes pacotes instalados:
      i. Python3
      ii. Pip3
      iii. Ansible (versão superior a 2.10.0)
      iv. Git

Se você tiver uma máquina Ubuntu/Debian nova sem os requisitos acima instalados, siga os passos abaixo para configurar essa máquina como o nó de controle do Ansible:

1. Cole o conteúdo abaixo no terminal

```
sudo apt-get -y install python3 >> outputlog.txt
sudo apt-get -y install python3-pip >> outputlog.txt
python3 -W ignore -m pip --disable-pip-version-check install ansible >>
outputlog.txt
sudo apt-get -y install git >> outputlog.txt
```

Pré-requisitos para a nuvem pública

Antes de instalar o conector Cloud Manager e o Cloud Volumes ONTAP e configurar o SnapMirror, precisamos realizar alguma preparação para nosso ambiente de nuvem. Esta página descreve o trabalho que precisa ser feito, bem como as considerações ao implantar o Cloud Volumes ONTAP.

Lista de verificação de pré-requisitos para implantação do Cloud Manager e do Cloud Volumes ONTAP

- Um login do NetApp Cloud Central
- Acesso à rede a partir de um navegador da web para vários terminais
- Um local de rede para um conector
- Permissões do provedor de nuvem
- Networking para serviços individuais

Para obter mais informações sobre o que você precisa para começar, visite nosso "documentação da nuvem" .

Considerações

1. O que é um conector do Cloud Manager?

Na maioria dos casos, um administrador de conta do Cloud Central deve implantar um conector na sua rede local ou na nuvem. O conector permite que o Cloud Manager gerencie recursos e processos dentro do seu ambiente de nuvem pública.

Para mais informações sobre Conectores, visite nosso "documentação da nuvem" .

2. Dimensionamento e arquitetura do Cloud Volumes ONTAP

Ao implantar o Cloud Volumes ONTAP, você pode escolher entre um pacote predefinido ou a criação de sua própria configuração. Embora muitos desses valores possam ser alterados posteriormente sem interrupções, há algumas decisões importantes que precisam ser tomadas antes da implantação com base nas cargas de trabalho a serem implantadas na nuvem.

Cada provedor de nuvem tem diferentes opções de implantação e quase toda carga de trabalho tem suas próprias propriedades exclusivas. A NetApp tem uma "Calculadora de TCO" que pode ajudar a dimensionar implantações corretamente com base na capacidade e no desempenho, mas foi criado em torno de alguns conceitos básicos que valem a pena considerar:

- Capacidade necessária
- Capacidade de rede da máquina virtual em nuvem

- Características de desempenho do armazenamento em nuvem

O segredo é planejar uma configuração que não apenas satisfaça os requisitos atuais de capacidade e desempenho, mas também considere o crescimento futuro. Isso é geralmente conhecido como capacidade de sobra e desempenho de sobra.

Se desejar mais informações, leia a documentação sobre o planejamento correto para "AWS" , "Azul" , e "GCP" .

3. Nó único ou alta disponibilidade?

Em todas as nuvens, há a opção de implantar o CVO em um único nó ou em um par de alta disponibilidade em cluster com dois nós. Dependendo do caso de uso, você pode querer implantar um único nó para economizar custos ou um par de HA para fornecer mais disponibilidade e redundância.

Para um caso de uso de DR ou para criar armazenamento temporário para desenvolvimento e teste, nós únicos são comuns, pois o impacto de uma interrupção repentina de zona ou infraestrutura é menor. No entanto, para qualquer caso de uso de produção, quando os dados estão em apenas um local ou quando o conjunto de dados precisa ter mais redundância e disponibilidade, a alta disponibilidade é recomendada.

Para obter mais informações sobre a arquitetura da versão de alta disponibilidade de cada nuvem, visite a documentação para "AWS" , "Azul" e "GCP" .

Visão geral de introdução

Visão geral de introdução

Esta seção fornece um resumo das tarefas que devem ser concluídas para atender aos requisitos pré-requisitos descritos na seção anterior. A seção a seguir fornece uma lista de tarefas de alto nível para operações locais e na nuvem pública. Os processos e procedimentos detalhados podem ser acessados clicando nos links relevantes.

No local

- Configurar usuário administrador do banco de dados no SnapCenter
- Pré-requisitos de instalação do plugin SnapCenter
- Instalação do plugin do host SnapCenter
- Descoberta de recursos de banco de dados
- Configurar peering de cluster de armazenamento e replicação de volume de banco de dados
- Adicionar armazenamento de banco de dados CVO SVM ao SnapCenter
- Configurar política de backup de banco de dados no SnapCenter
- Implementar política de backup para proteger o banco de dados
- Validar backup

Nuvem pública da AWS

- Verificação pré-voo
- Etapas para implantar o Cloud Manager e o Cloud Volumes ONTAP na AWS

- Implantar instância de computação EC2 para carga de trabalho de banco de dados

Clique nos links a seguir para obter detalhes:

"No local","Nuvem Pública - AWS"

Começando no local

A ferramenta NetApp SnapCenter usa controle de acesso baseado em função (RBAC) para gerenciar o acesso a recursos do usuário e concessões de permissão, e a instalação do SnapCenter cria funções pré-preenchidas. Você também pode criar funções personalizadas com base em suas necessidades ou aplicativos.

No local

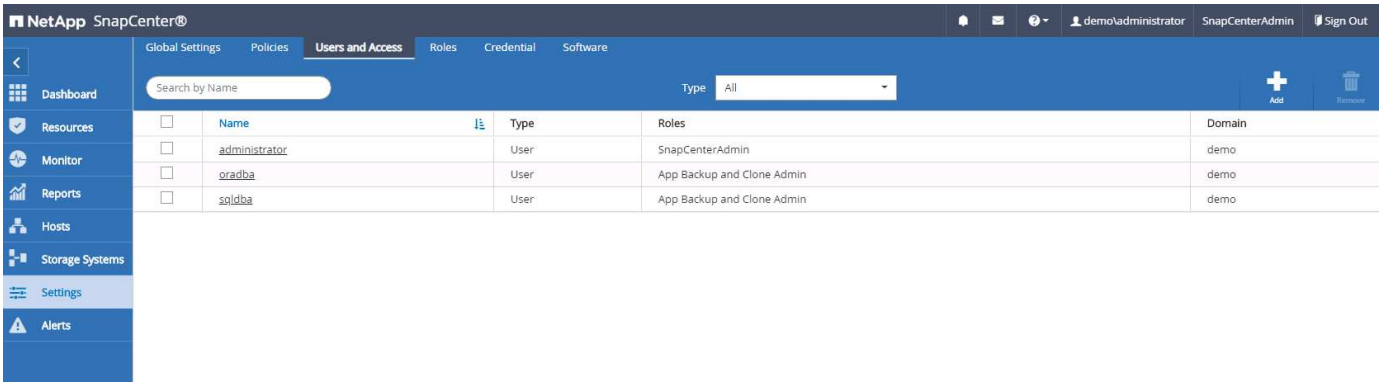
1. Configurar usuário administrador do banco de dados no SnapCenter

Faz sentido ter um ID de usuário administrador dedicado para cada plataforma de banco de dados suportada pelo SnapCenter para backup de banco de dados, restauração e/ou recuperação de desastres. Você também pode usar um único ID para gerenciar todos os bancos de dados. Em nossos casos de teste e demonstração, criamos um usuário administrador dedicado para Oracle e SQL Server, respectivamente.

Certos recursos do SnapCenter só podem ser provisionados com a função SnapCenterAdmin. Os recursos podem então ser atribuídos a outros IDs de usuários para acesso.

Em um ambiente SnapCenter local pré-instalado e configurado, as seguintes tarefas podem já ter sido concluídas. Caso contrário, as etapas a seguir criam um usuário administrador de banco de dados:

1. Adicione o usuário administrador ao Windows Active Directory.
2. Efetue login no SnapCenter usando uma ID concedida com a função SnapCenterAdmin.
3. Navegue até a aba Acesso em Configurações e Usuários e clique em Adicionar para adicionar um novo usuário. O novo ID de usuário é vinculado ao usuário administrador criado no Windows Active Directory na etapa 1. . Atribua a função adequada ao usuário, conforme necessário. Atribua recursos ao usuário administrador, conforme aplicável.



2. Pré-requisitos de instalação do plugin SnapCenter

O SnapCenter executa backup, restauração, clonagem e outras funções usando um agente de plug-in em execução nos hosts do banco de dados. Ele se conecta ao host do banco de dados e ao banco de dados por meio de credenciais configuradas na guia Configurações e credenciais para instalação de plug-ins e outras funções de gerenciamento. Há requisitos de privilégios específicos com base no tipo de host de destino, como

Linux ou Windows, bem como no tipo de banco de dados.

As credenciais dos hosts do BD devem ser configuradas antes da instalação do plugin SnapCenter . Geralmente, você deseja usar contas de usuário de administrador no host do banco de dados como suas credenciais de conexão de host para instalação do plugin. Você também pode conceder o mesmo ID de usuário para acesso ao banco de dados usando autenticação baseada em sistema operacional. Por outro lado, você também pode empregar autenticação de banco de dados com diferentes IDs de usuário de banco de dados para acesso de gerenciamento de banco de dados. Se você decidir usar a autenticação baseada no sistema operacional, o ID do usuário administrador do sistema operacional deverá receber acesso ao banco de dados. Para instalação do SQL Server baseado em domínio do Windows, uma conta de administrador de domínio pode ser usada para gerenciar todos os SQL Servers dentro do domínio.

Host Windows para servidor SQL:

1. Se estiver usando credenciais do Windows para autenticação, você deverá configurar suas credenciais antes de instalar plug-ins.
2. Se estiver usando uma instância do SQL Server para autenticação, você deverá adicionar as credenciais após instalar os plugins.
3. Se você tiver habilitado a autenticação SQL ao configurar as credenciais, a instância ou o banco de dados descoberto será exibido com um ícone de cadeado vermelho. Se o ícone de cadeado aparecer, você deverá especificar as credenciais da instância ou do banco de dados para adicionar com sucesso a instância ou o banco de dados a um grupo de recursos.
4. Você deve atribuir a credencial a um usuário RBAC sem acesso de administrador de sistema quando as seguintes condições forem atendidas:
    - A credencial é atribuída a uma instância SQL.
    - A instância ou host do SQL é atribuído a um usuário RBAC.
    - O usuário administrador do RBAC DB deve ter privilégios de grupo de recursos e de backup.

Host Unix para Oracle:

1. Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root editando sshd.conf e reiniciando o serviço sshd. A autenticação SSH baseada em senha na instância da AWS é desativada por padrão.
2. Configure os privilégios sudo para que o usuário não root instale e inicie o processo do plugin. Após instalar o plugin, os processos são executados como um usuário root efetivo.
3. Crie credenciais com o modo de autenticação Linux para o usuário de instalação.
4. Você deve instalar o Java 1.8.x (64 bits) no seu host Linux.
5. A instalação do plugin do banco de dados Oracle também instala o plugin SnapCenter para Unix.

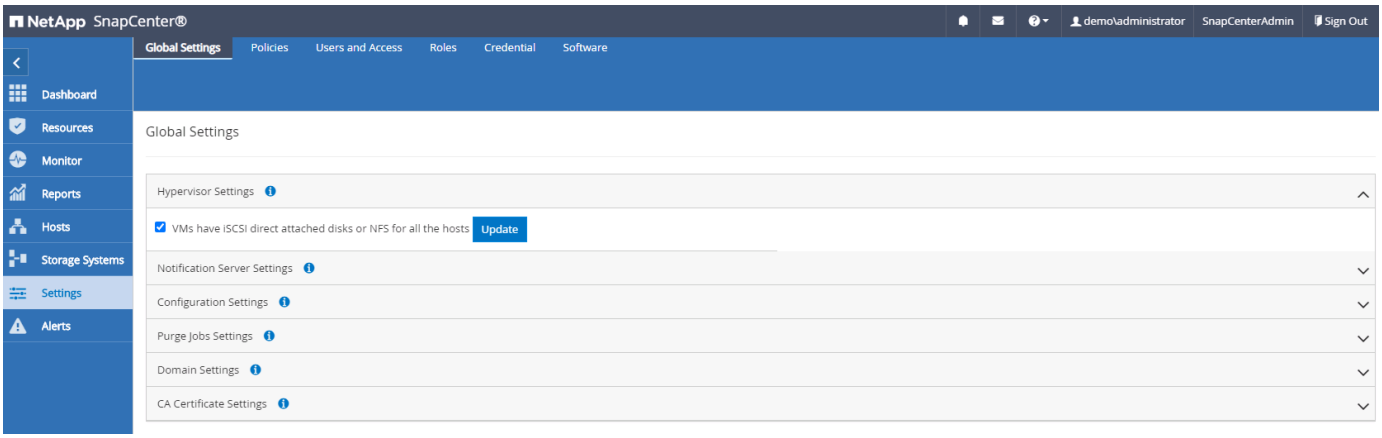
3. Instalação do plugin do host SnapCenter

> Antes de tentar instalar plug-ins do SnapCenter em instâncias do servidor de banco de dados na nuvem, certifique-se de que todas as etapas de configuração tenham sido concluídas, conforme listado na seção de nuvem relevante para implantação de instância de computação.

As etapas a seguir ilustram como um host de banco de dados é adicionado ao SnapCenter enquanto um plug-in do SnapCenter é instalado no host. O procedimento se aplica à adição de hosts locais e hosts na nuvem. A demonstração a seguir adiciona um host Windows ou Linux residente na AWS.

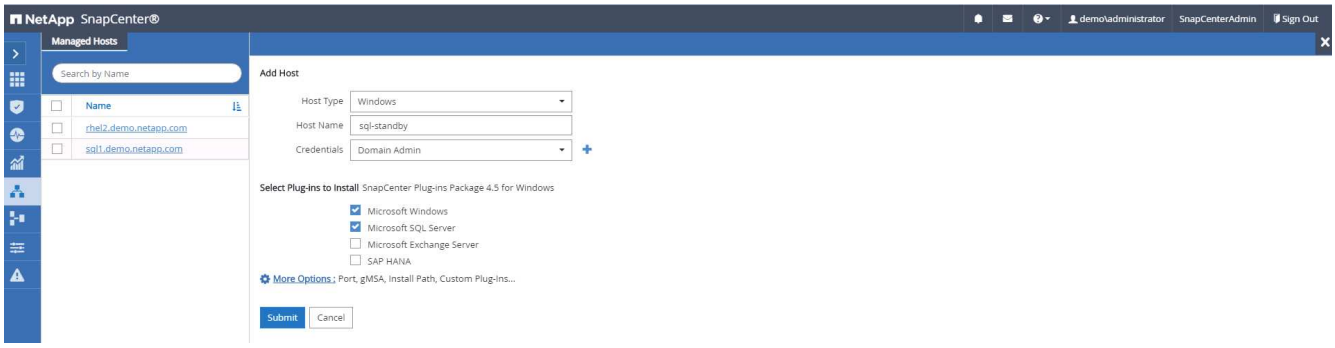
Configurar as configurações globais do SnapCenter VMware

Navegue até Configurações > Configurações globais. Selecione "As VMs têm discos iSCSI conectados diretamente ou NFS para todos os hosts" em Configurações do hipervisor e clique em Atualizar.



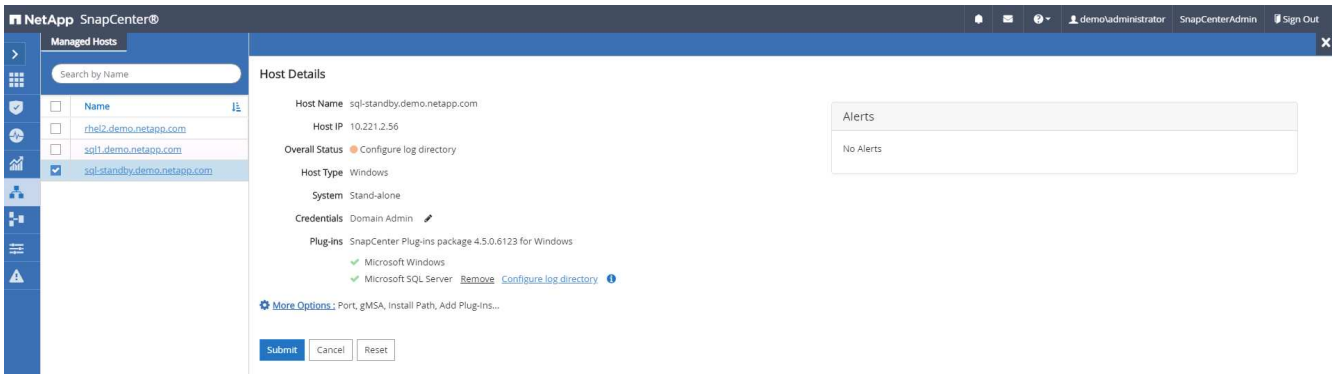
Adicionar host Windows e instalação do plugin no host

1. Efetue login no SnapCenter com um ID de usuário com privilégios SnapCenterAdmin.
2. Clique na aba Hosts no menu à esquerda e depois clique em Adicionar para abrir o fluxo de trabalho Adicionar Host.
3. Selecione Windows para Tipo de Host; o Nome do Host pode ser um nome de host ou um endereço IP. O nome do host deve ser resolvido para o endereço IP do host correto do host SnapCenter . Escolha as credenciais do host criadas na etapa 2. Escolha Microsoft Windows e Microsoft SQL Server como os pacotes de plugin a serem instalados.

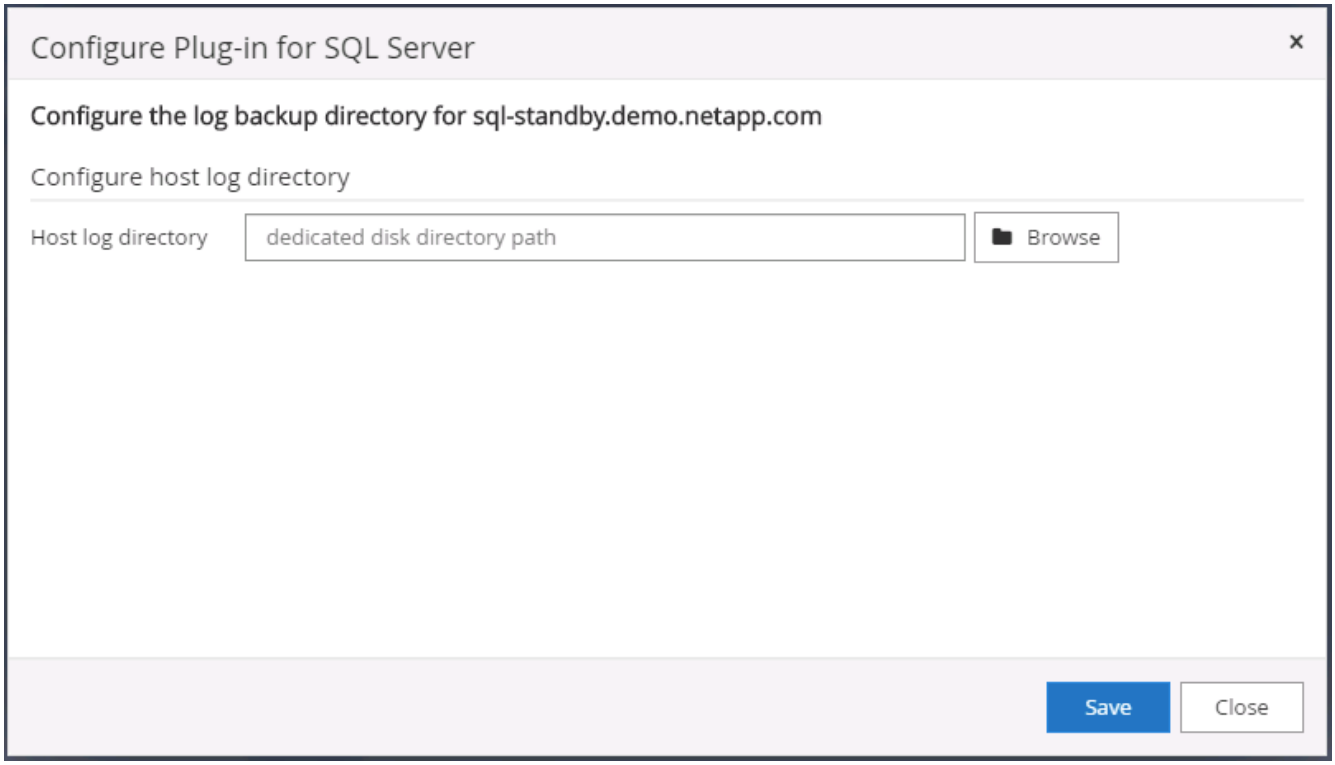


4. Após o plugin ser instalado em um host Windows, seu status geral é exibido como "Configurar diretório de log".

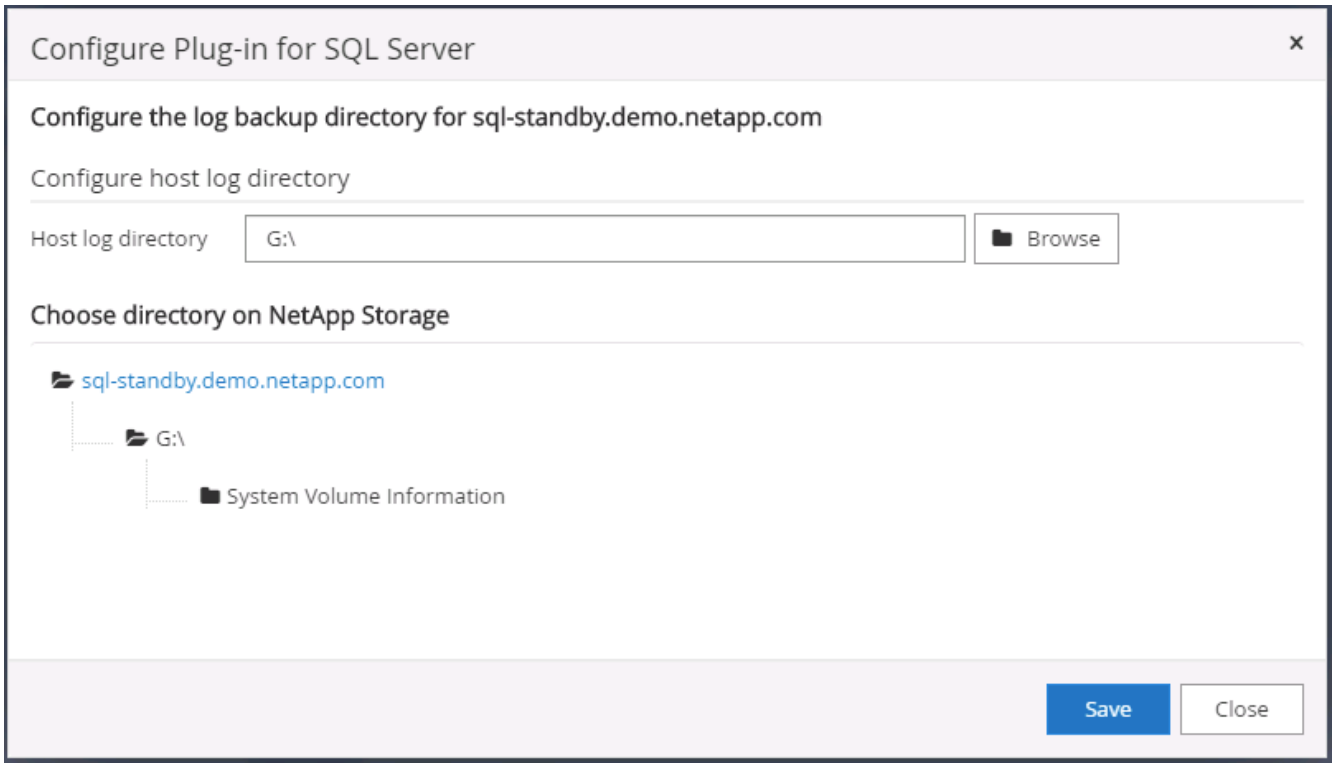
5. Clique no nome do host para abrir a configuração do diretório de log do SQL Server.



6. Clique em "Configurar diretório de log" para abrir "Configurar plug-in para SQL Server".

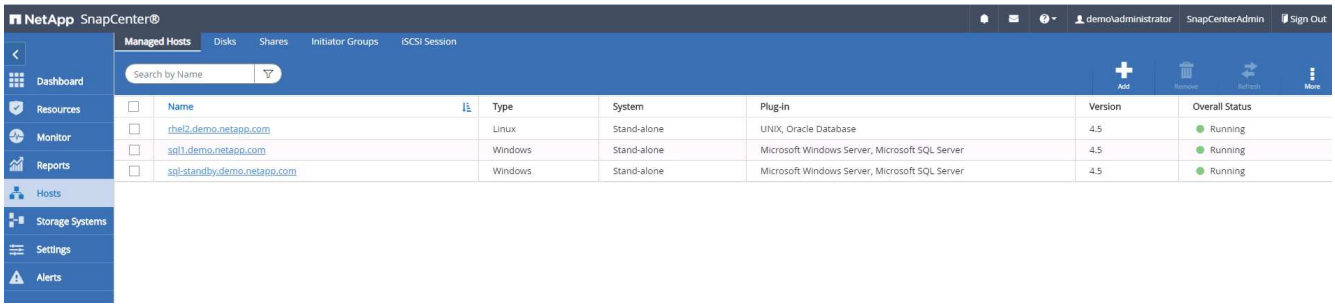


7. Clique em Procurar para descobrir o armazenamento do NetApp para que um diretório de log possa ser definido; o SnapCenter usa esse diretório de log para acumular os arquivos de log de transações do servidor SQL. Em seguida, clique em Salvar.

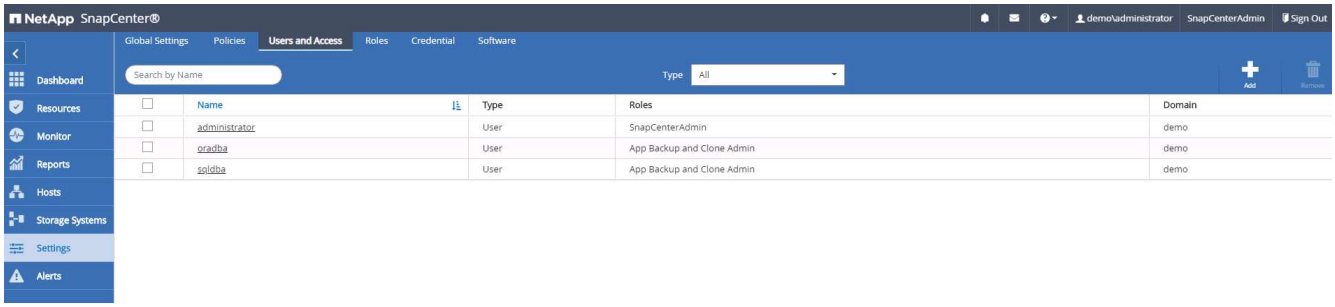


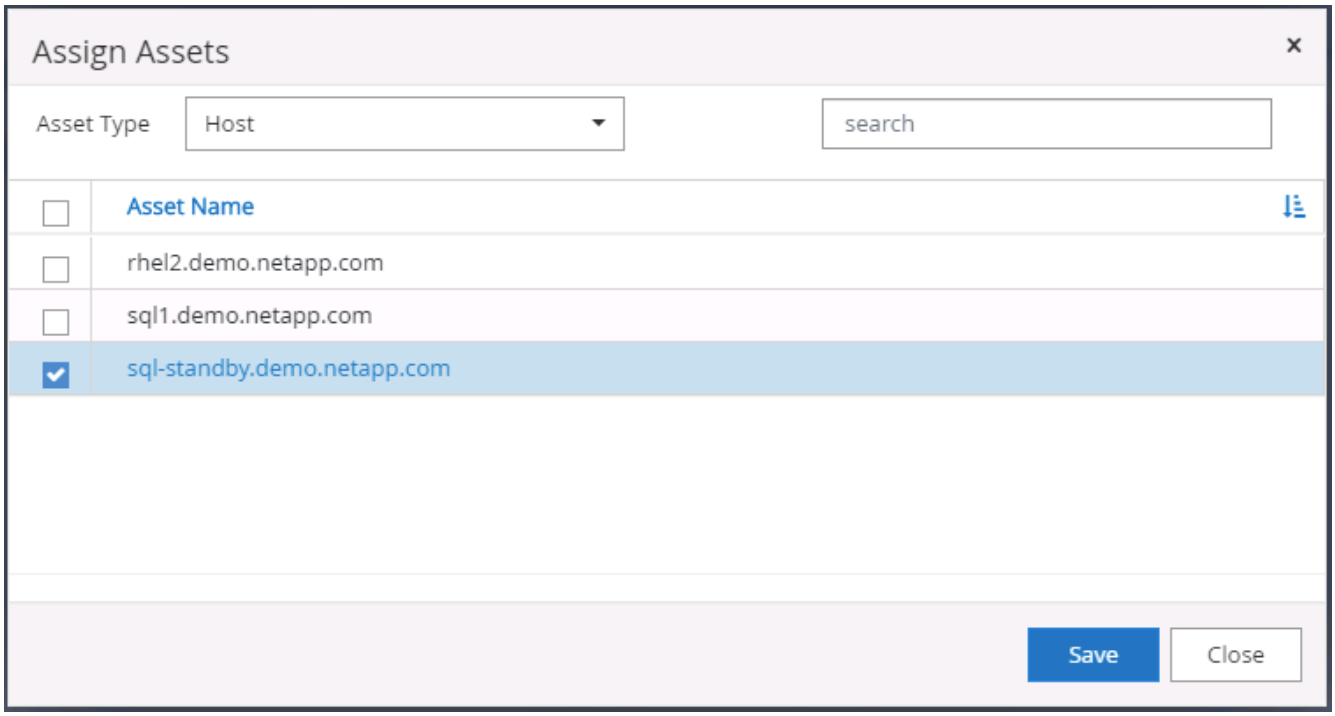
Para que o armazenamento NetApp provisionado em um host de banco de dados seja descoberto, o armazenamento (local ou CVO) deve ser adicionado ao SnapCenter, conforme ilustrado na etapa 6 para o CVO como exemplo.

8. Após a configuração do diretório de log, o Status geral do plugin do host do Windows é alterado para Em execução.



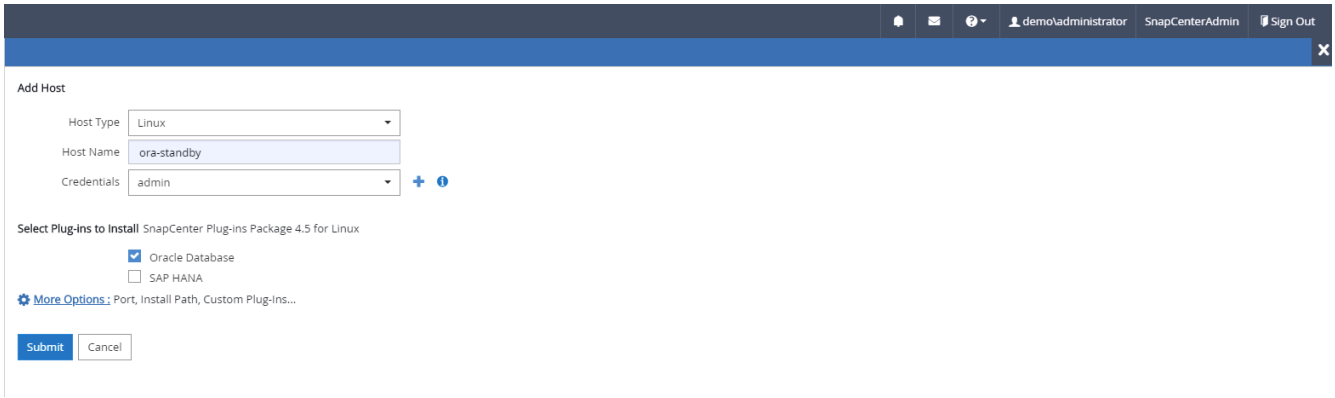
9. Para atribuir o host ao ID de usuário de gerenciamento de banco de dados, navegue até a guia Acesso em Configurações e Usuários, clique no ID de usuário de gerenciamento de banco de dados (no nosso caso, o sqldba ao qual o host precisa ser atribuído) e clique em Salvar para concluir a atribuição de recursos do host.



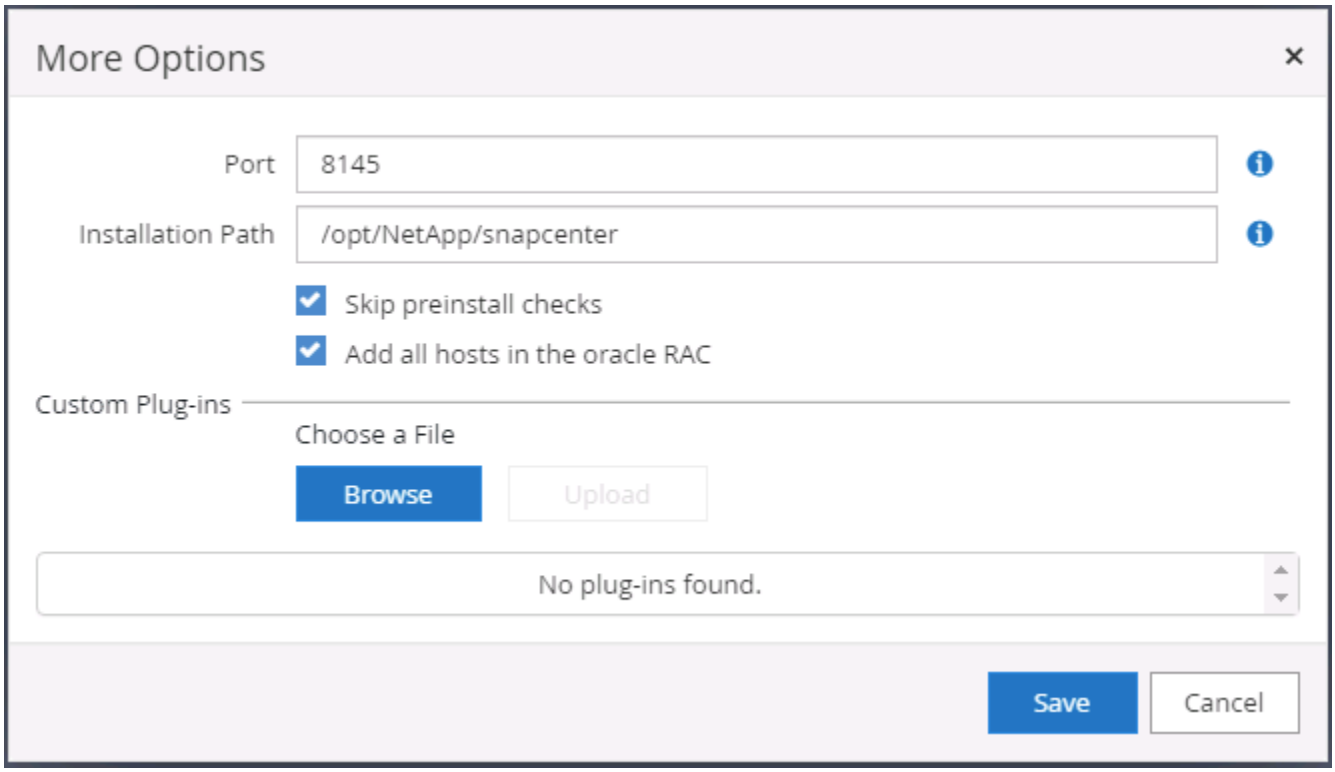


Adicionar host Unix e instalação do plugin no host

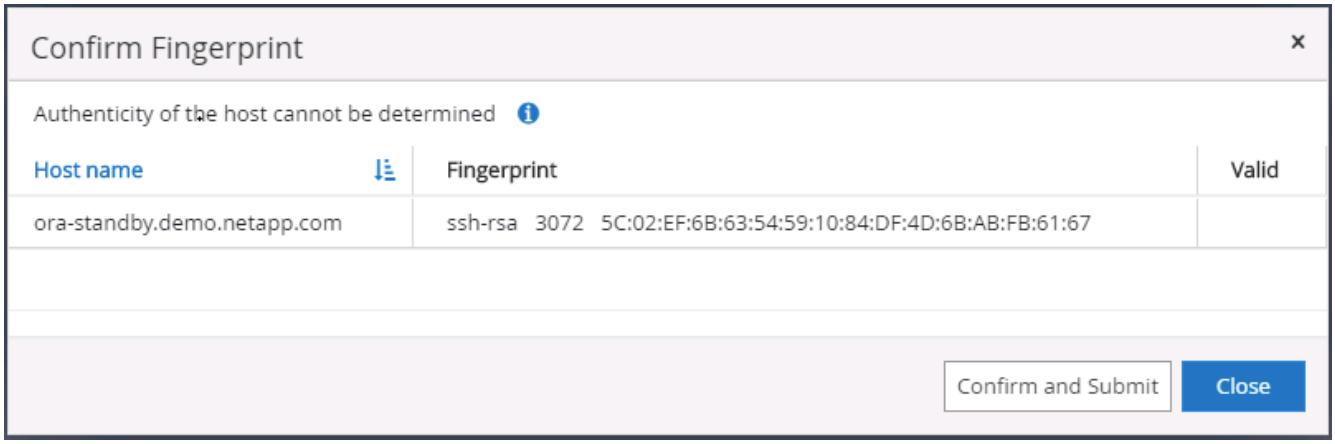
1. Efetue login no SnapCenter com um ID de usuário com privilégios SnapCenterAdmin.
2. Clique na aba Hosts no menu à esquerda e clique em Adicionar para abrir o fluxo de trabalho Adicionar Host.
3. Escolha Linux como o tipo de host. O nome do host pode ser o nome do host ou um endereço IP. No entanto, o nome do host deve ser resolvido para corrigir o endereço IP do host do SnapCenter . Escolha as credenciais do host criadas na etapa 2. As credenciais do host exigem privilégios sudo. Marque o Oracle Database como o plug-in a ser instalado, que instala os plug-ins do host Oracle e Linux.



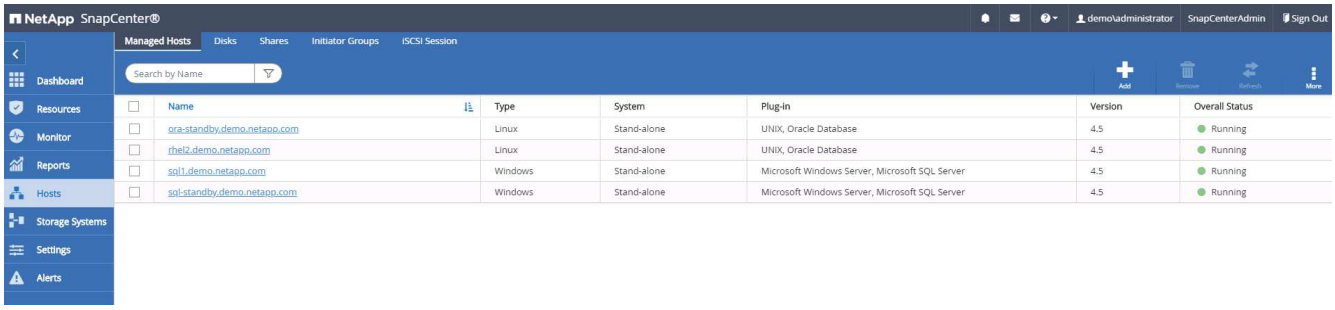
4. Clique em Mais opções e selecione "Ignorar verificações de pré-instalação". Você será solicitado a confirmar que deseja ignorar a verificação de pré-instalação. Clique em Sim e depois em Salvar.



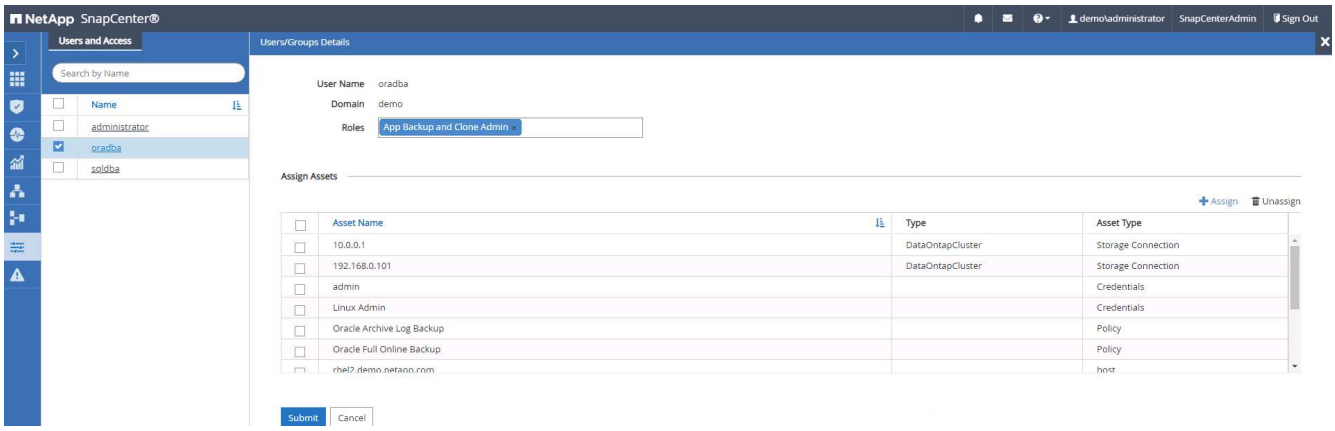
5. Clique em Enviar para iniciar a instalação do plugin. Você será solicitado a confirmar a impressão digital, conforme mostrado abaixo.

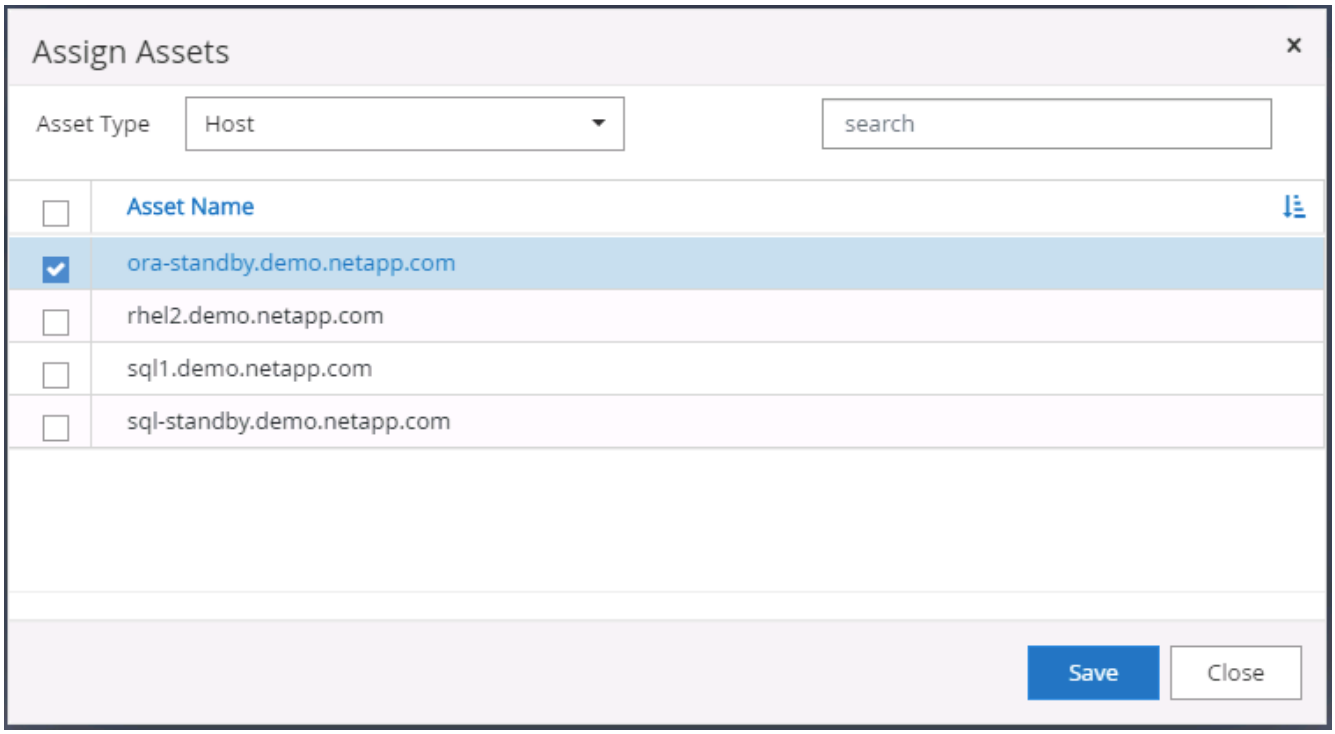


6. O SnapCenter executa a validação e o registro do host e, em seguida, o plugin é instalado no host Linux. O status é alterado de Instalando plugin para Em execução.



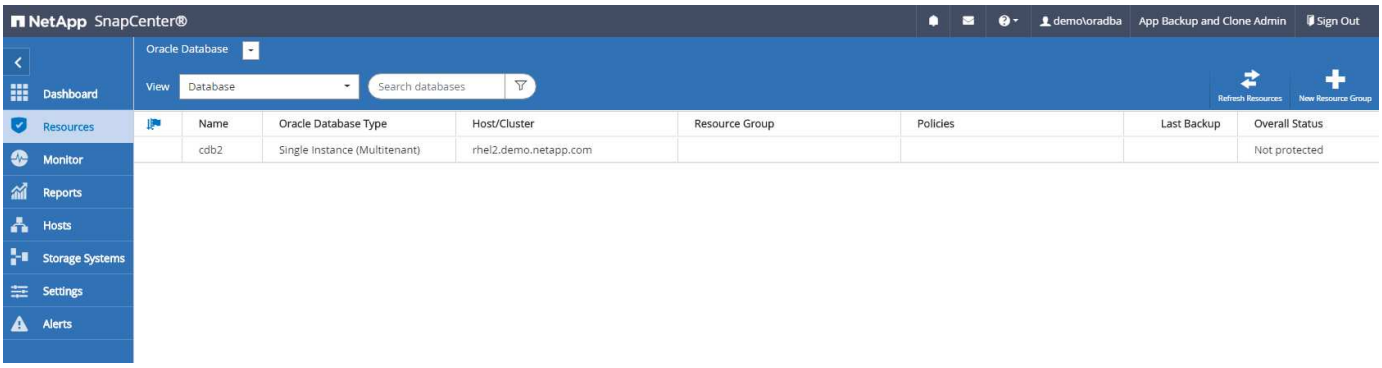
7. Atribua o host recém-adicionado ao ID de usuário de gerenciamento de banco de dados apropriado (no nosso caso, oradba).





4. Descoberta de recursos de banco de dados

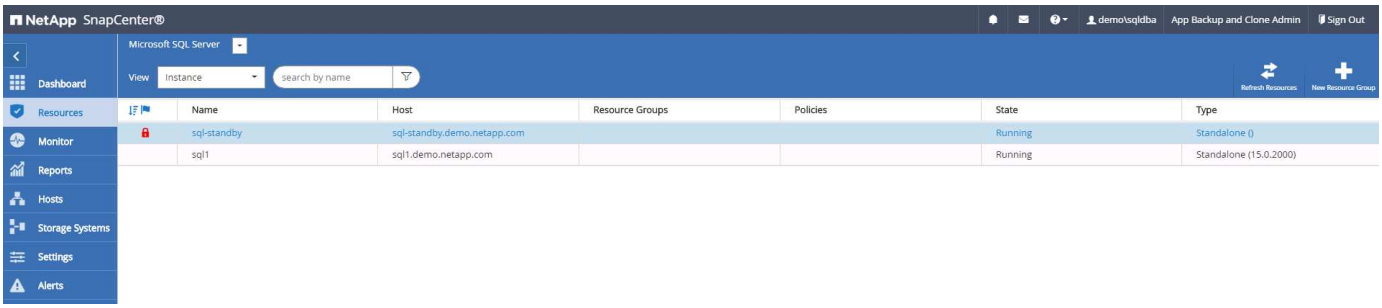
Com a instalação bem-sucedida do plugin, os recursos do banco de dados no host podem ser descobertos imediatamente. Clique na aba Recursos no menu à esquerda. Dependendo do tipo de plataforma de banco de dados, várias visualizações estão disponíveis, como banco de dados, grupo de recursos e assim por diante. Talvez seja necessário clicar na guia Atualizar recursos se os recursos no host não forem descobertos e exibidos.

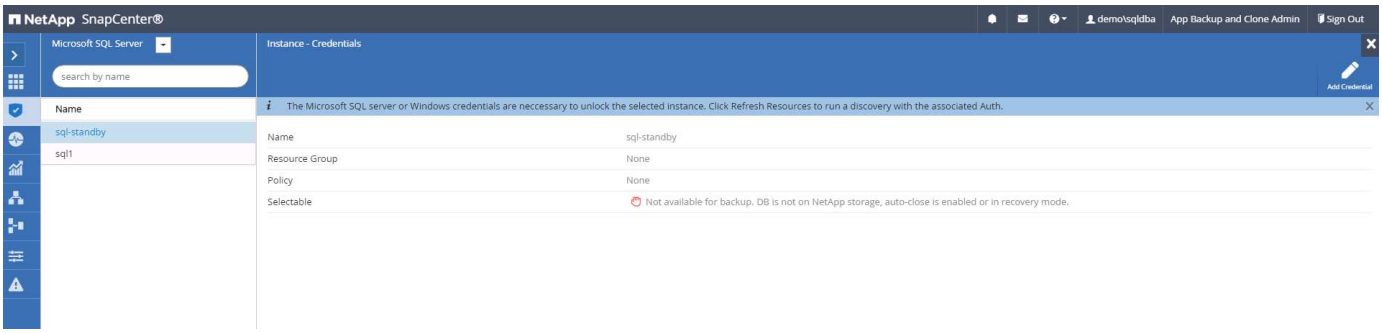


Quando o banco de dados é descoberto inicialmente, o status geral é mostrado como "Não protegido". A captura de tela anterior mostra um banco de dados Oracle ainda não protegido por uma política de backup.

Quando uma configuração ou política de backup é definida e um backup é executado, o Status geral do banco de dados mostra o status do backup como "Backup bem-sucedido" e o registro de data e hora do último backup. A captura de tela a seguir mostra o status do backup de um banco de dados de usuário do SQL Server.

Se as credenciais de acesso ao banco de dados não estiverem configuradas corretamente, um botão de cadeado vermelho indicará que o banco de dados não está acessível. Por exemplo, se as credenciais do Windows não tiverem acesso de administrador de sistema a uma instância de banco de dados, as credenciais do banco de dados deverão ser reconfiguradas para desbloquear o cadeado vermelho.





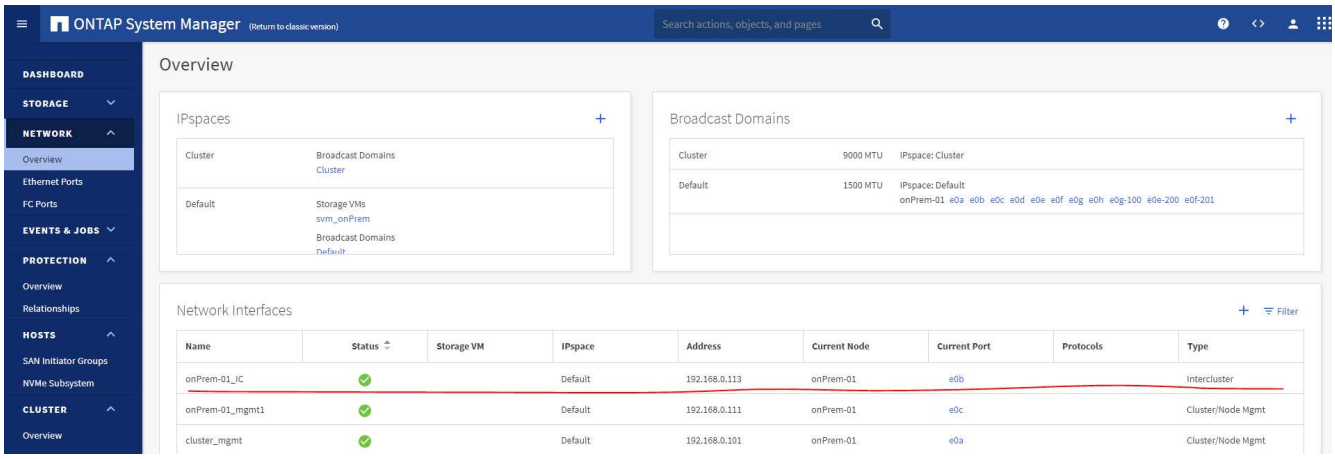
Depois que as credenciais apropriadas são configuradas no nível do Windows ou no nível do banco de dados, o cadeado vermelho desaparece e as informações do tipo SQL Server são coletadas e revisadas.

5. Configurar peering de cluster de armazenamento e replicação de volumes de banco de dados

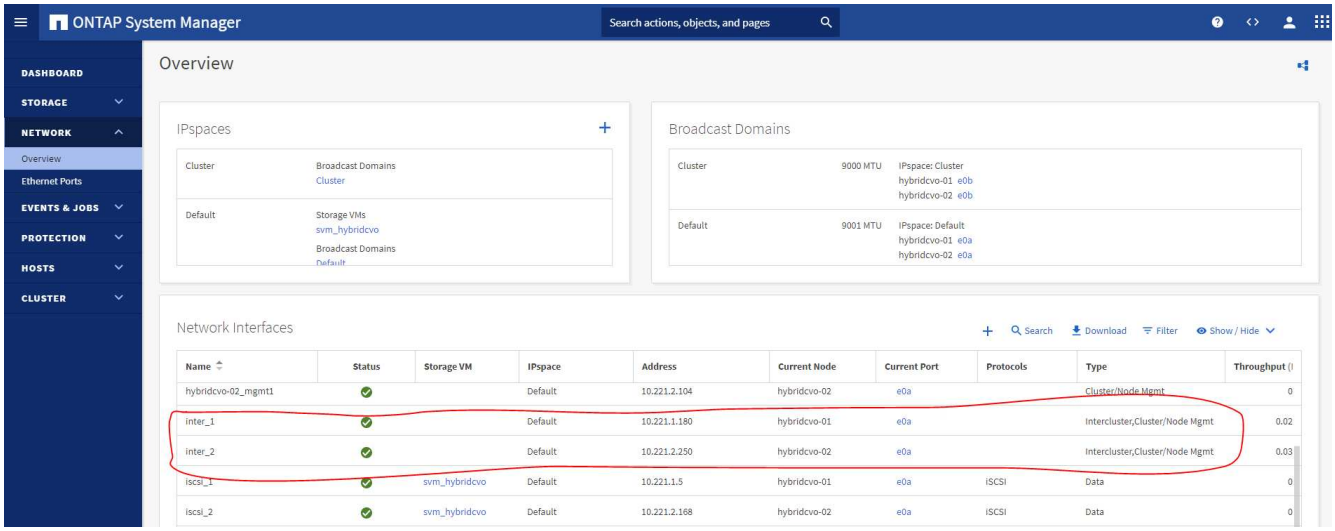
Para proteger os dados do seu banco de dados local usando uma nuvem pública como destino, os volumes de banco de dados de cluster ONTAP local são replicados para o CVO na nuvem usando a tecnologia NetApp SnapMirror . Os volumes de destino replicados podem então ser clonados para DEV/OPS ou recuperação de desastres. As etapas de alto nível a seguir permitem que você configure o peering de cluster e a replicação de volumes de banco de dados.

1. Configure LIFs entre clusters para peering de cluster no cluster local e na instância do cluster CVO. Esta etapa pode ser realizada com o ONTAP System Manager. Uma implantação de CVO padrão tem LIFs entre clusters configurados automaticamente.

   Cluster local:



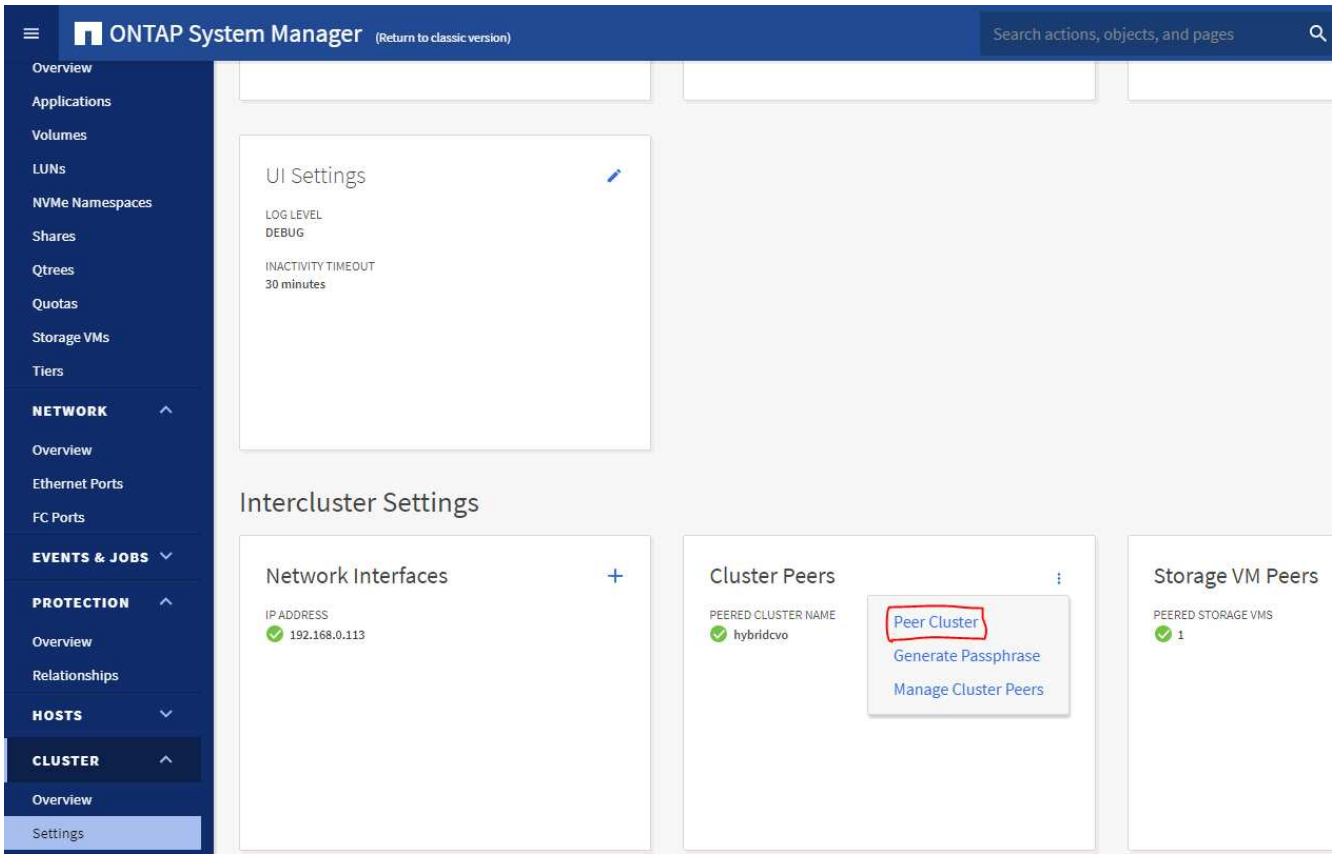
   Cluster CVO alvo:



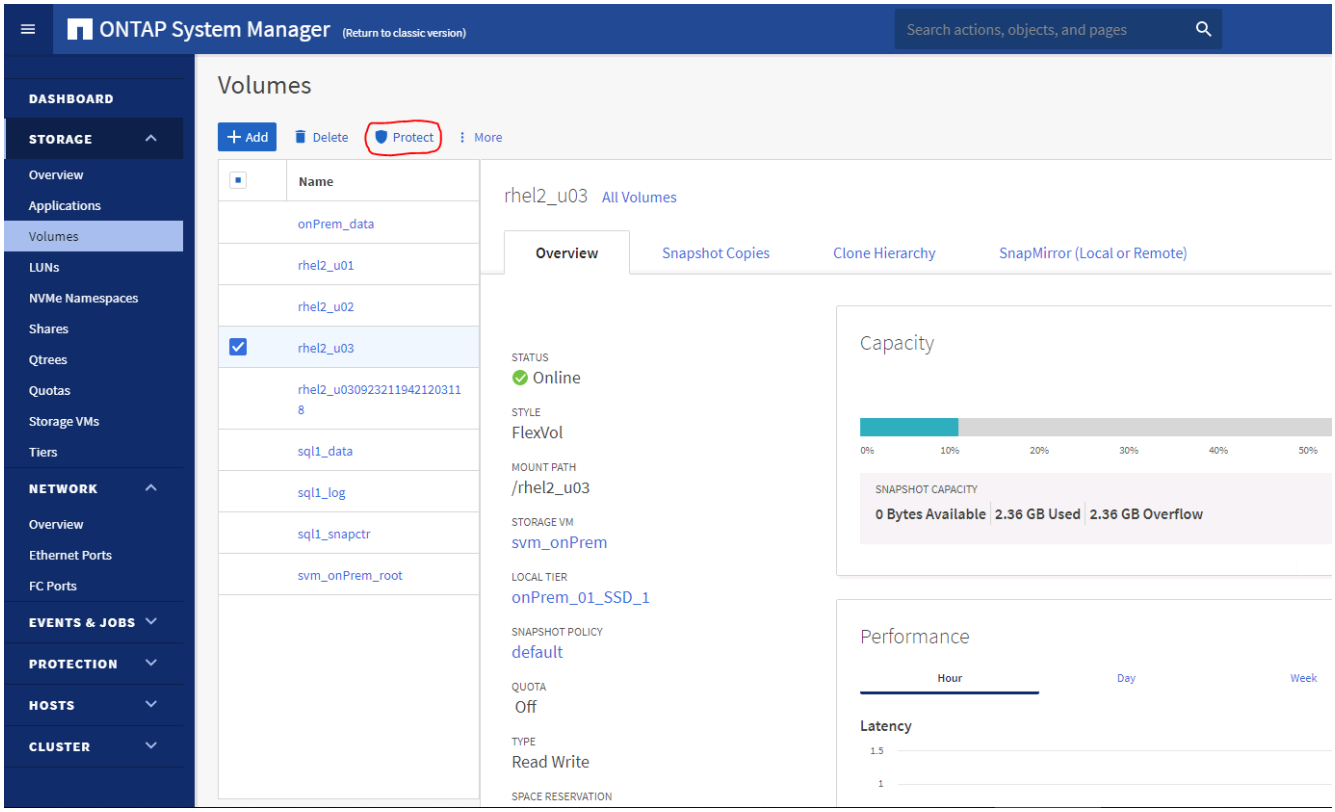
2. Com os LIFs intercluster configurados, o peering de cluster e a replicação de volume podem ser configurados usando arrastar e soltar no NetApp Cloud Manager. Ver"Introdução - Nuvem Pública da AWS" para mais detalhes.

   Como alternativa, o peering de cluster e a replicação de volume de banco de dados podem ser executados usando o ONTAP System Manager da seguinte maneira:

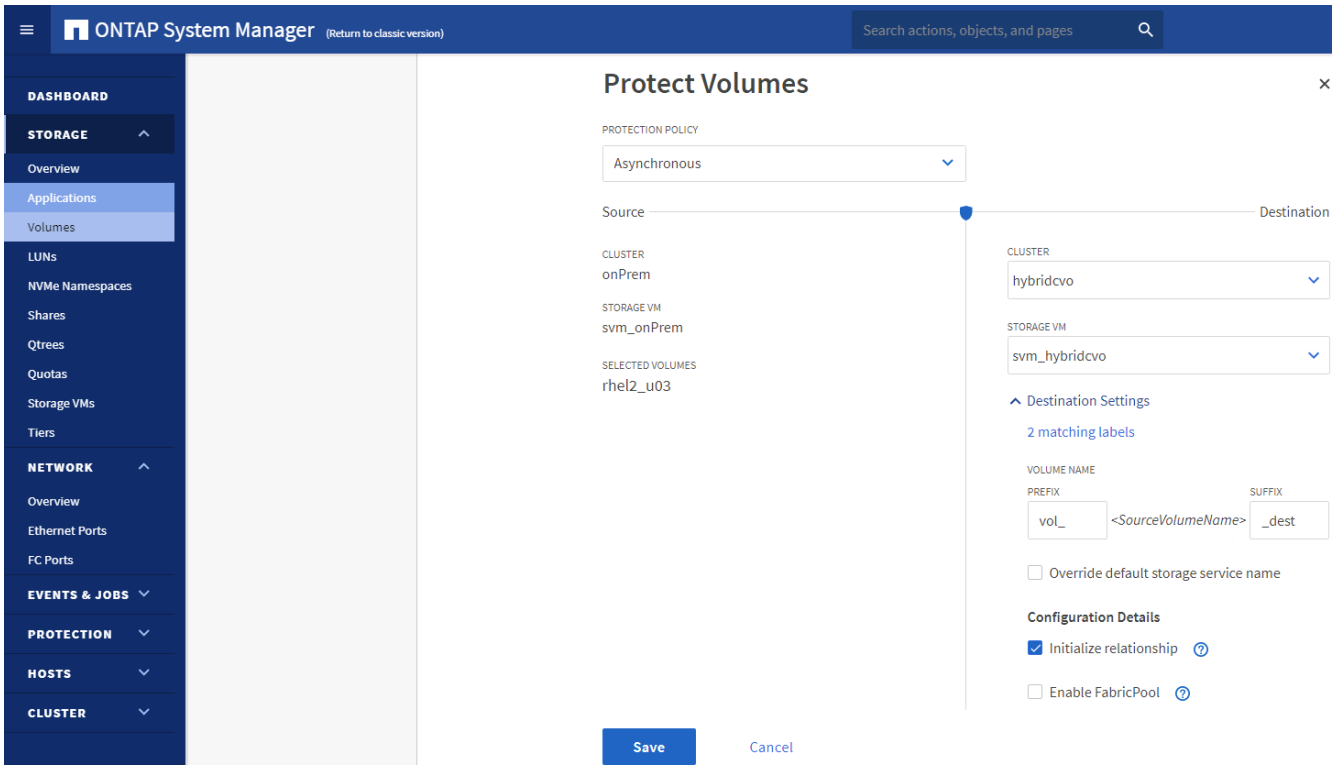
3. Efetue login no ONTAP System Manager. Navegue até Cluster > Configurações e clique em Cluster de pares para configurar o peering de cluster com a instância do CVO na nuvem.



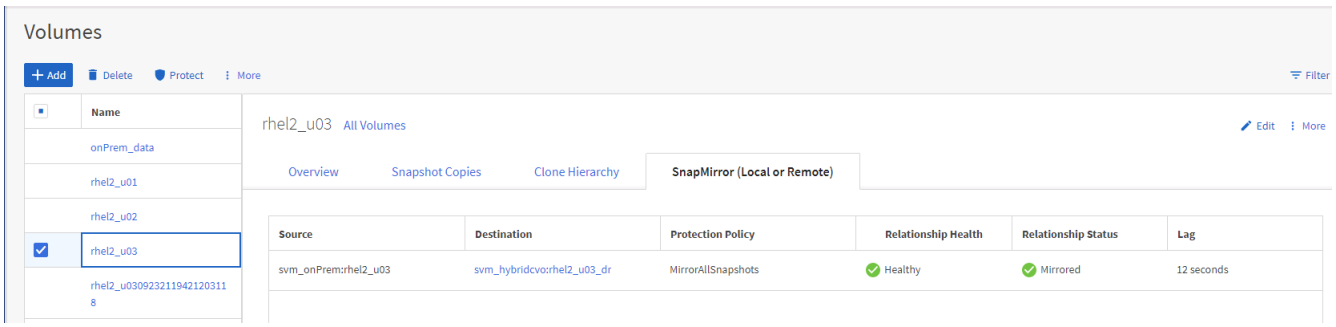
4. Vá para a aba Volumes. Selecione o volume do banco de dados a ser replicado e clique em Proteger.



5. Defina a política de proteção como Assíncrona. Selecione o cluster de destino e o SVM de armazenamento.

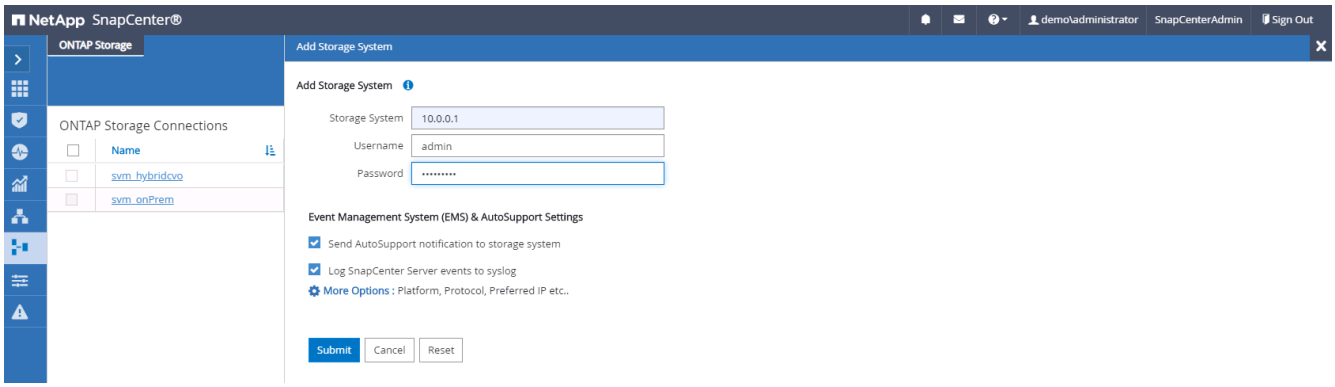


6. Valide se o volume está sincronizado entre a origem e o destino e se o relacionamento de replicação está saudável.

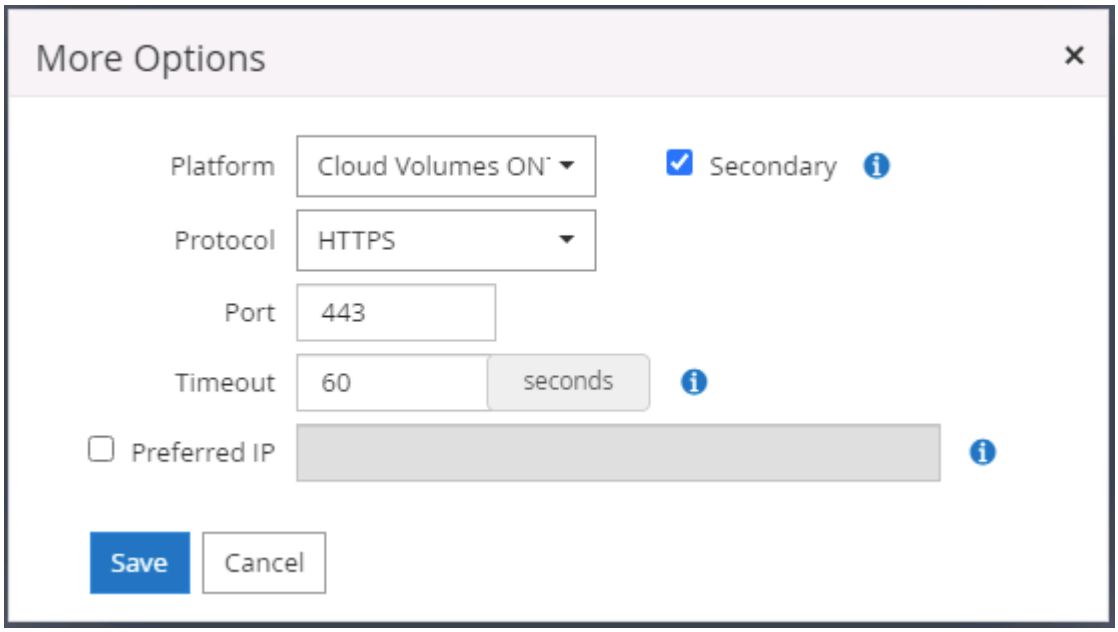


6. Adicionar armazenamento de banco de dados CVO SVM ao SnapCenter

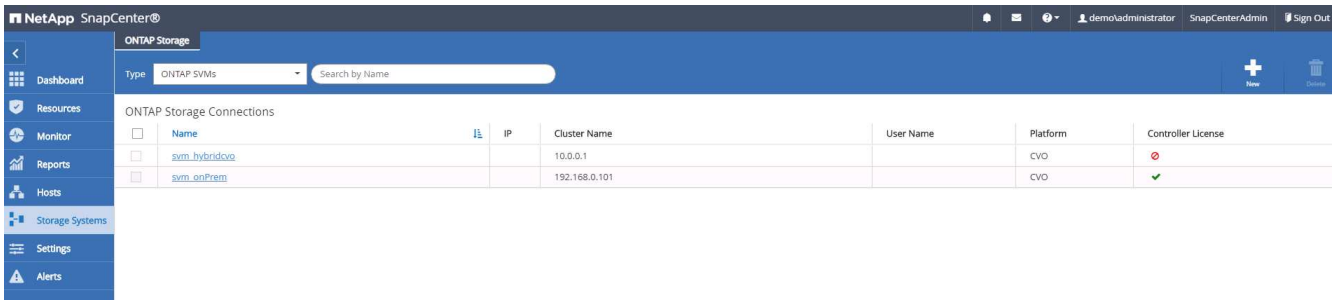
1. Efetue login no SnapCenter com um ID de usuário com privilégios SnapCenterAdmin.
2. Clique na guia Sistema de armazenamento no menu e, em seguida, clique em Novo para adicionar um SVM de armazenamento CVO que hospeda volumes de banco de dados de destino replicados no SnapCenter. Insira o IP de gerenciamento do cluster no campo Sistema de armazenamento e insira o nome de usuário e a senha apropriados.



3. Clique em Mais opções para abrir opções adicionais de configuração de armazenamento. No campo Plataforma, selecione Cloud Volumes ONTAP, marque Secundário e clique em Salvar.



4. Atribua os sistemas de armazenamento aos IDs de usuário de gerenciamento de banco de dados SnapCenter , conforme mostrado em3. Instalação do plugin do host SnapCenter .

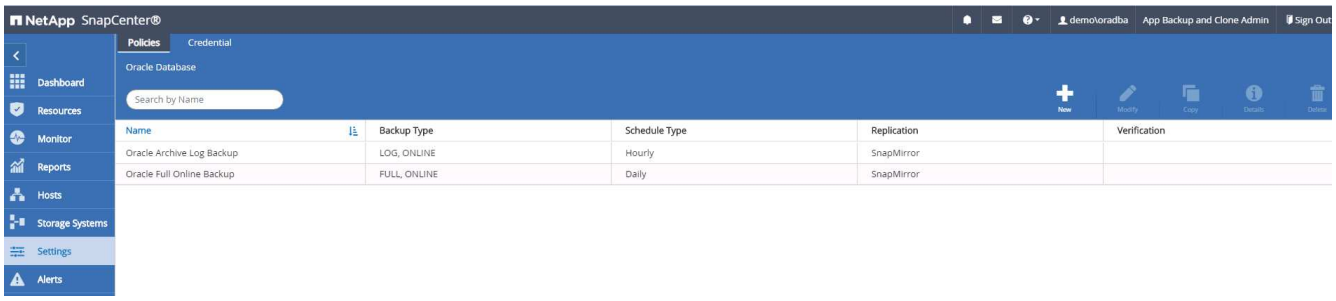


7. Configurar política de backup de banco de dados no SnapCenter

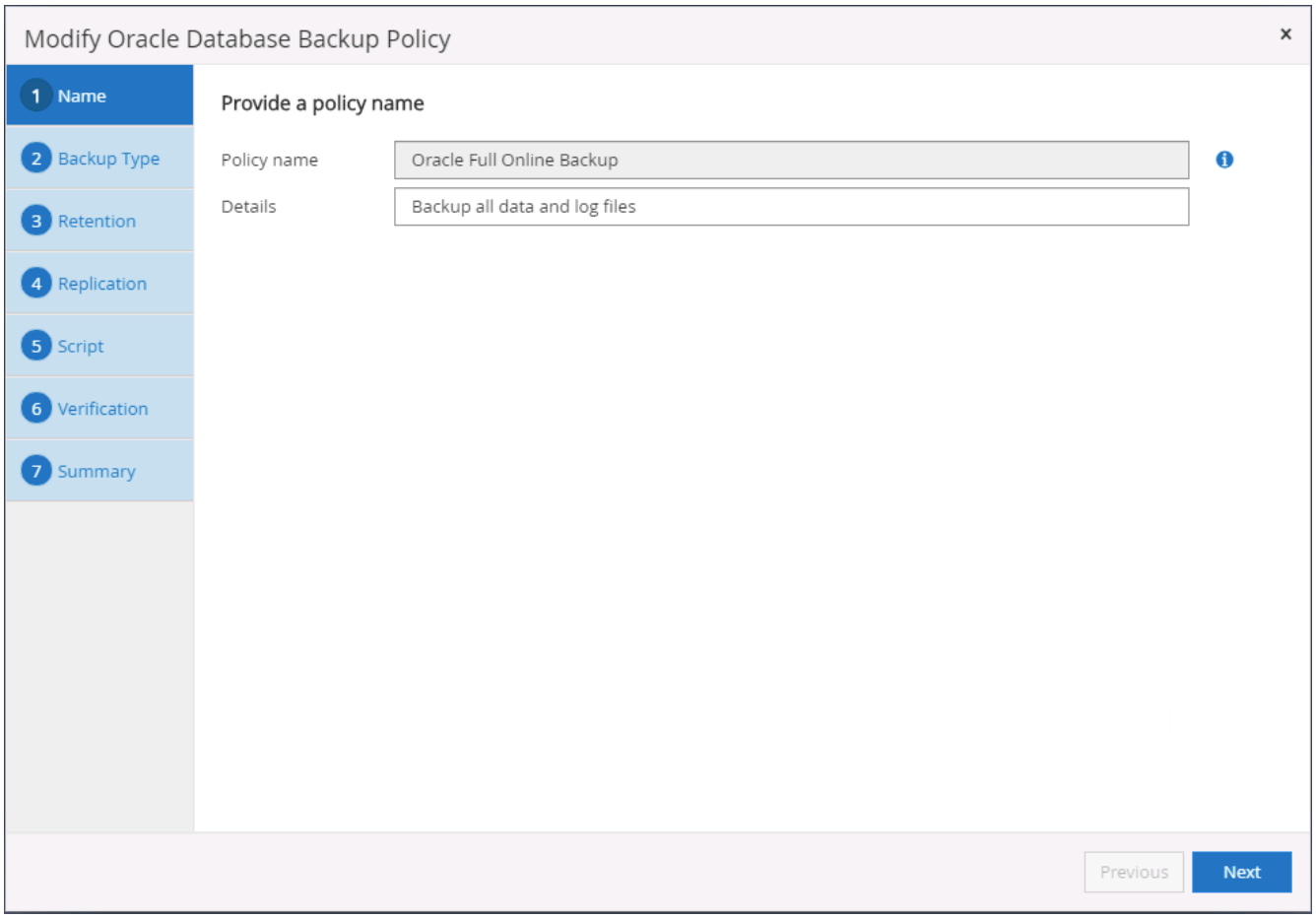
Os procedimentos a seguir demonstram como criar uma política de backup completa de banco de dados ou arquivo de log. A política pode então ser implementada para proteger os recursos dos bancos de dados. O objetivo do ponto de recuperação (RPO) ou objetivo de tempo de recuperação (RTO) determina a frequência dos backups de banco de dados e/ou log.

Crie uma política de backup de banco de dados completa para Oracle

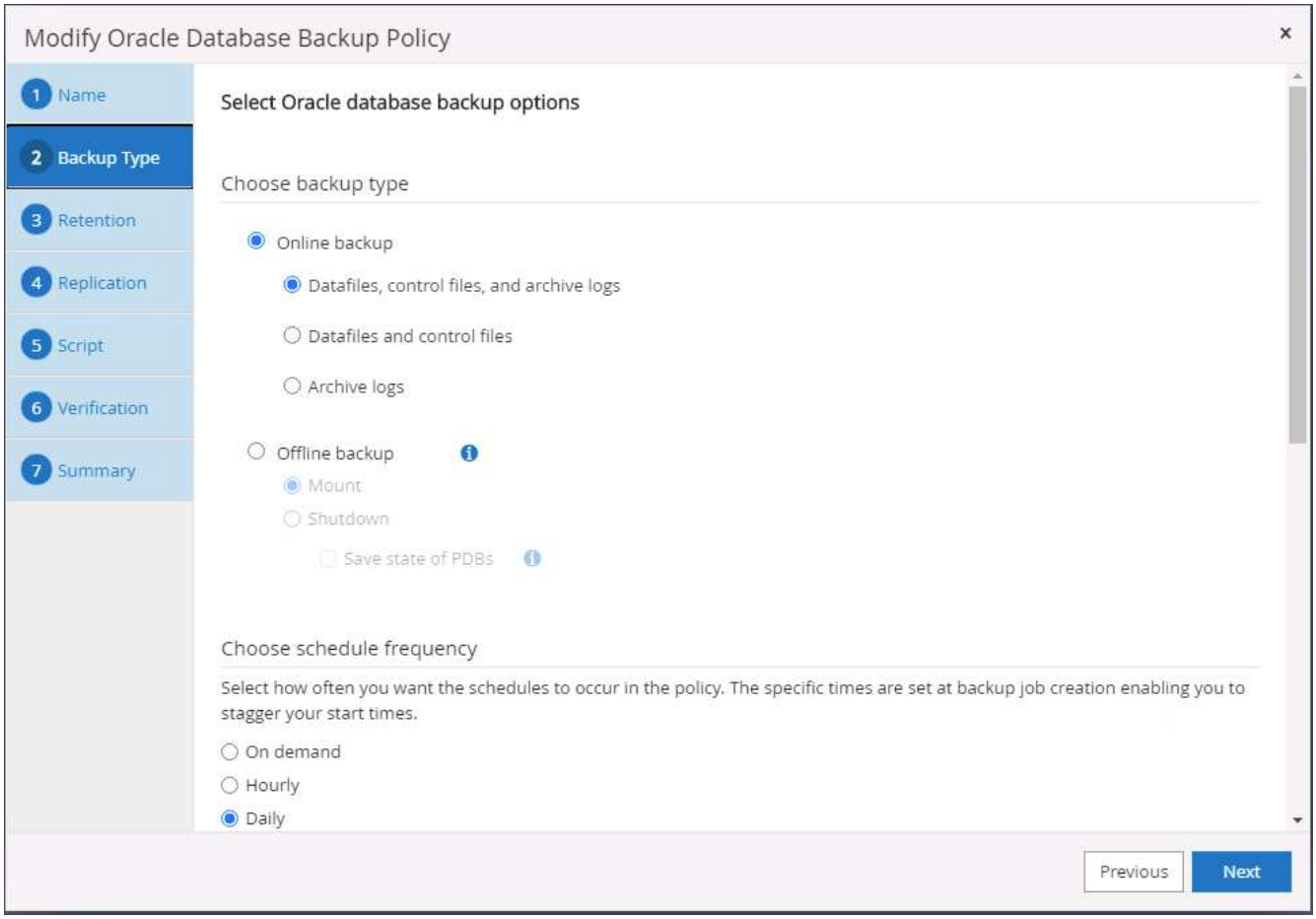
1. Efetue login no SnapCenter como um ID de usuário de gerenciamento de banco de dados, clique em Configurações e depois em Políticas.



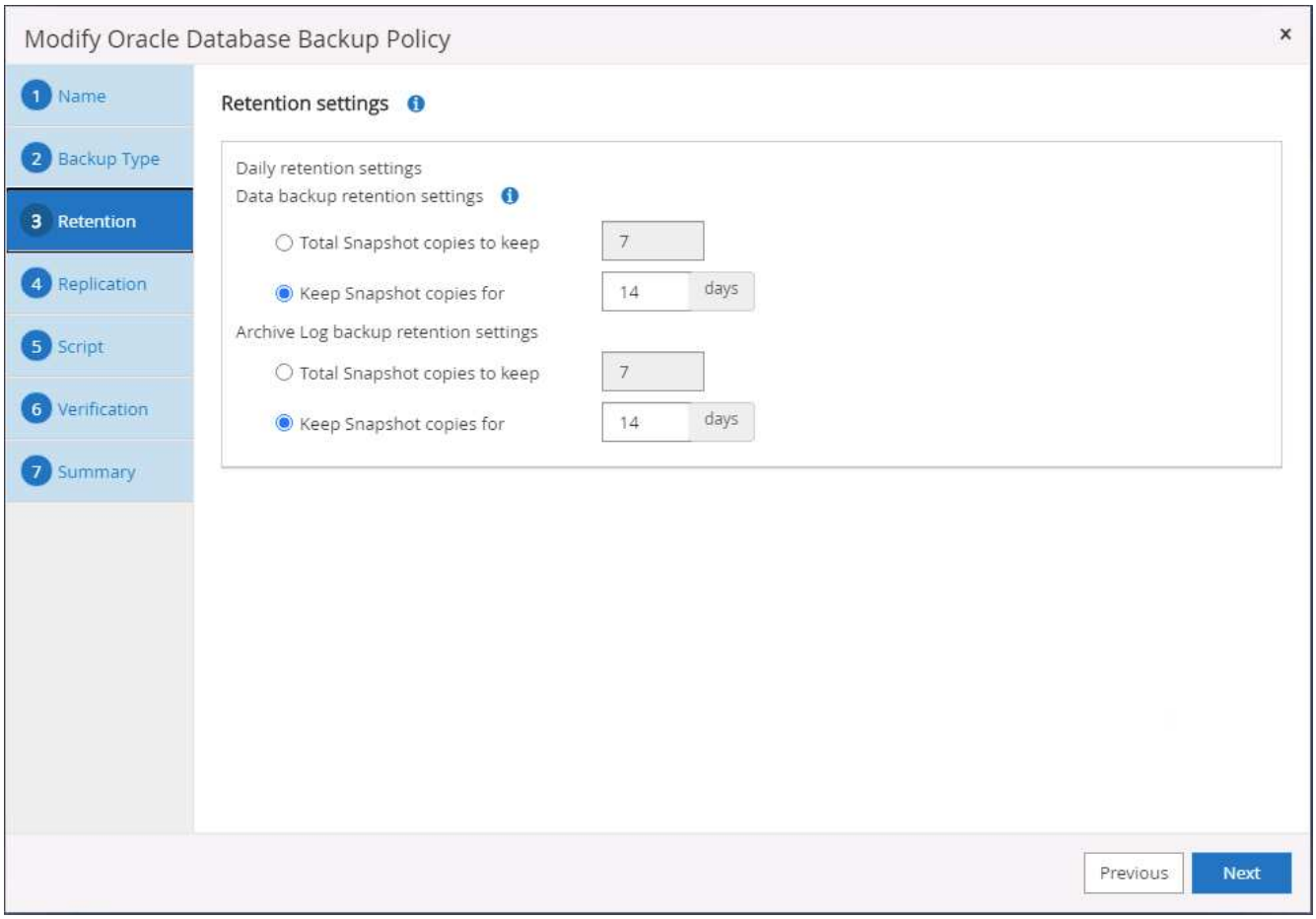
2. Clique em Novo para iniciar um novo fluxo de trabalho de criação de política de backup ou escolha uma política existente para modificação.



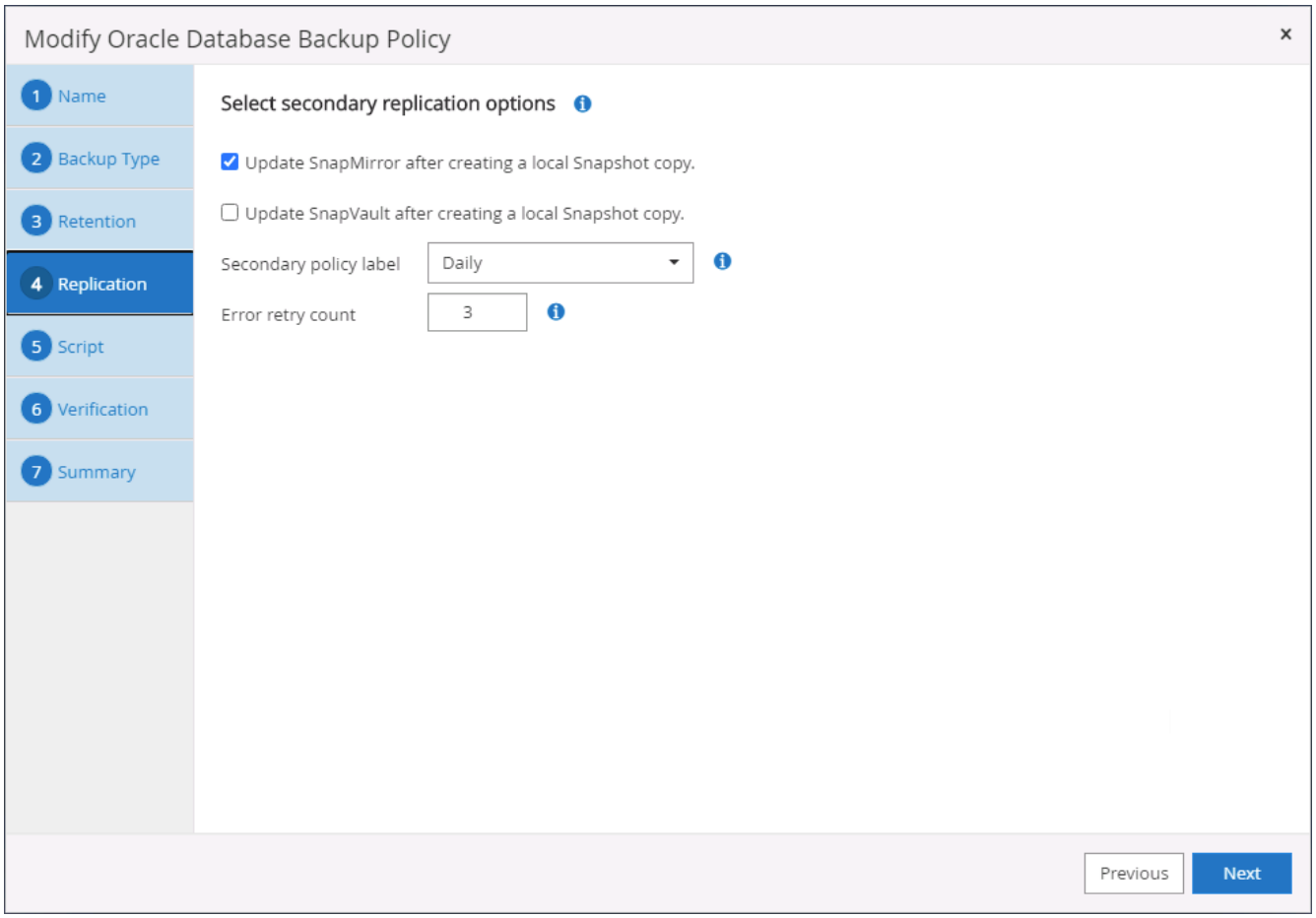
3. Selecione o tipo de backup e a frequência agendada.



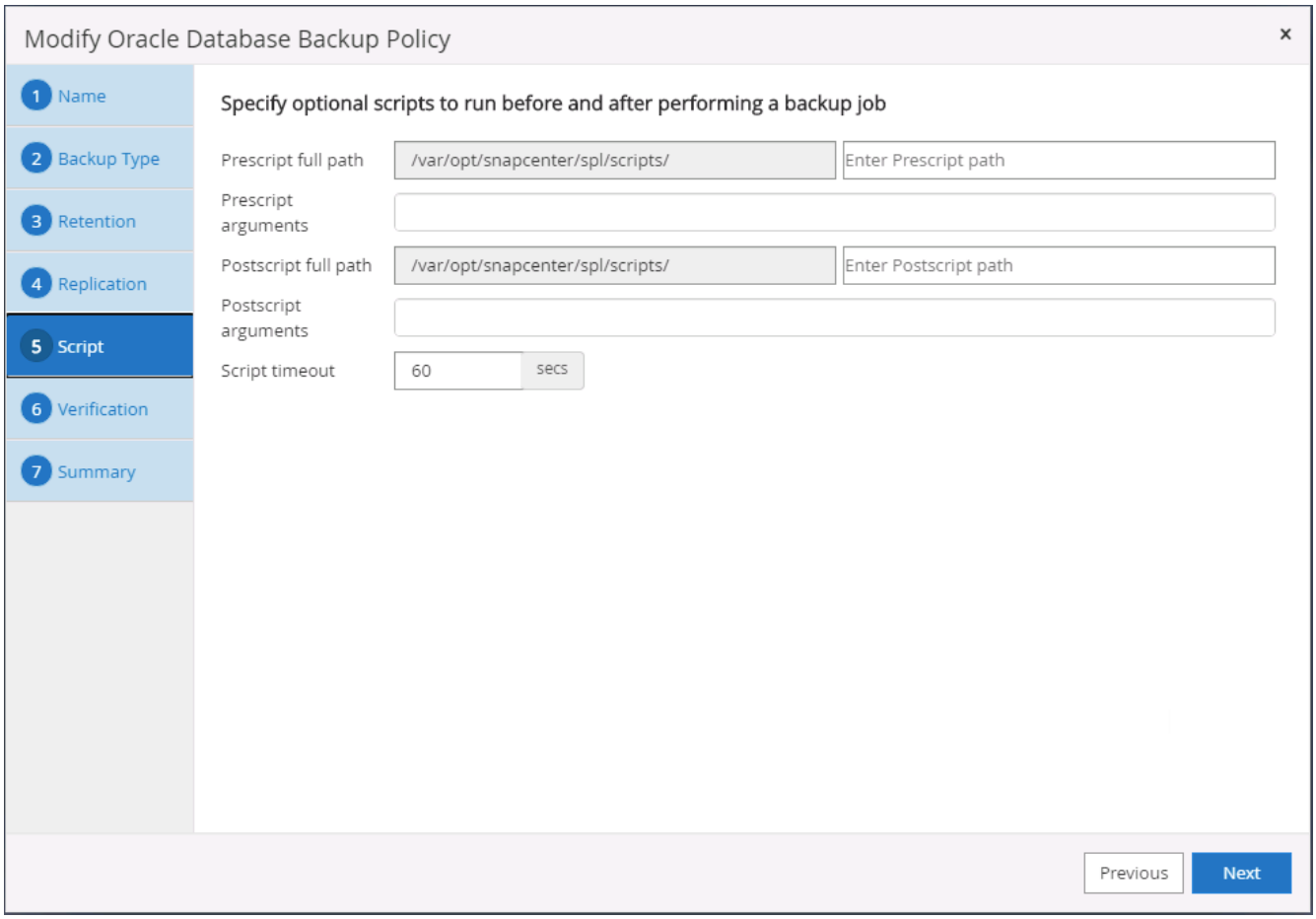
4. Defina a configuração de retenção de backup. Isso define quantas cópias completas de backup do banco de dados manter.



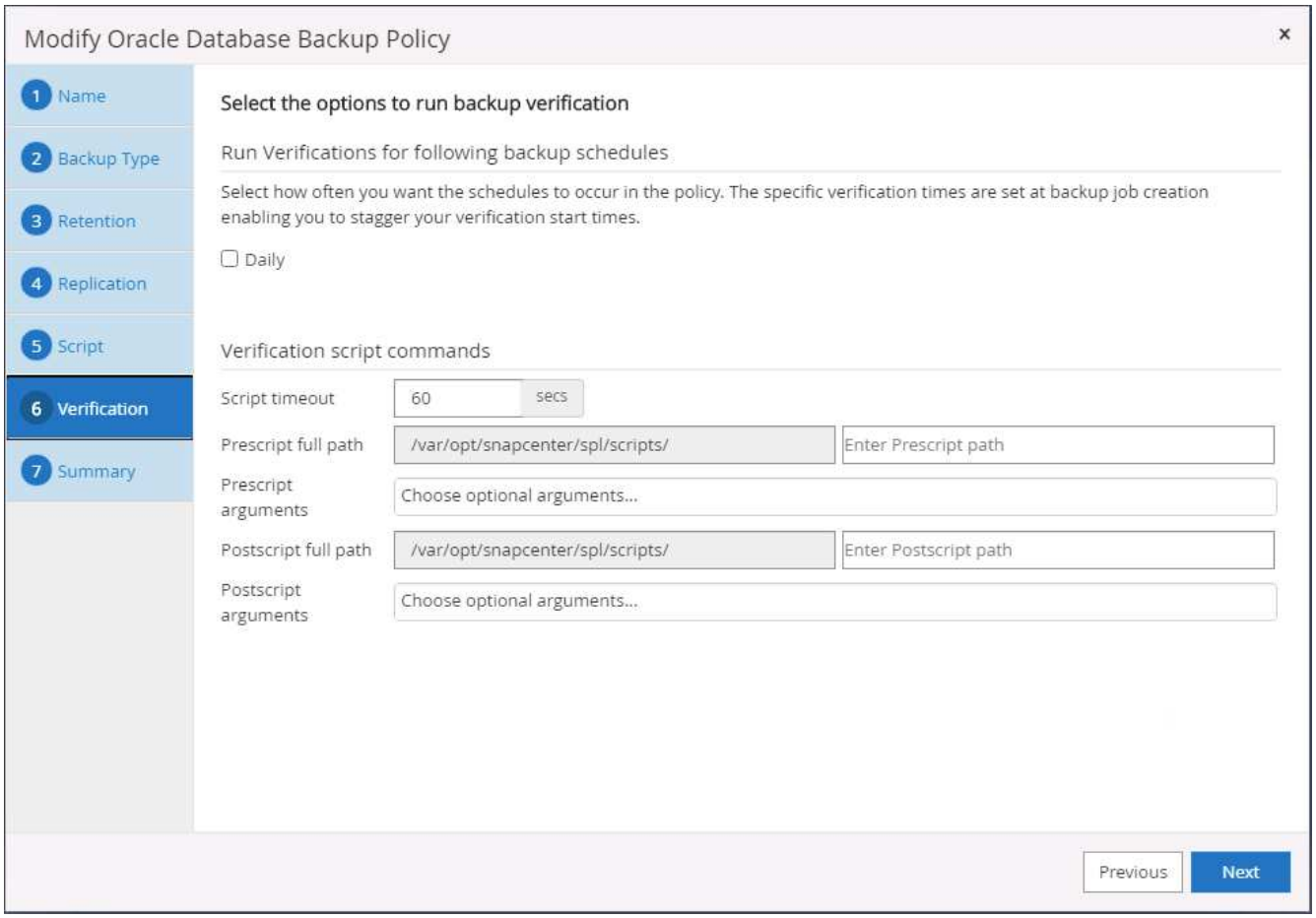
5. Selecione as opções de replicação secundária para enviar backups de instantâneos primários locais para serem replicados em um local secundário na nuvem.



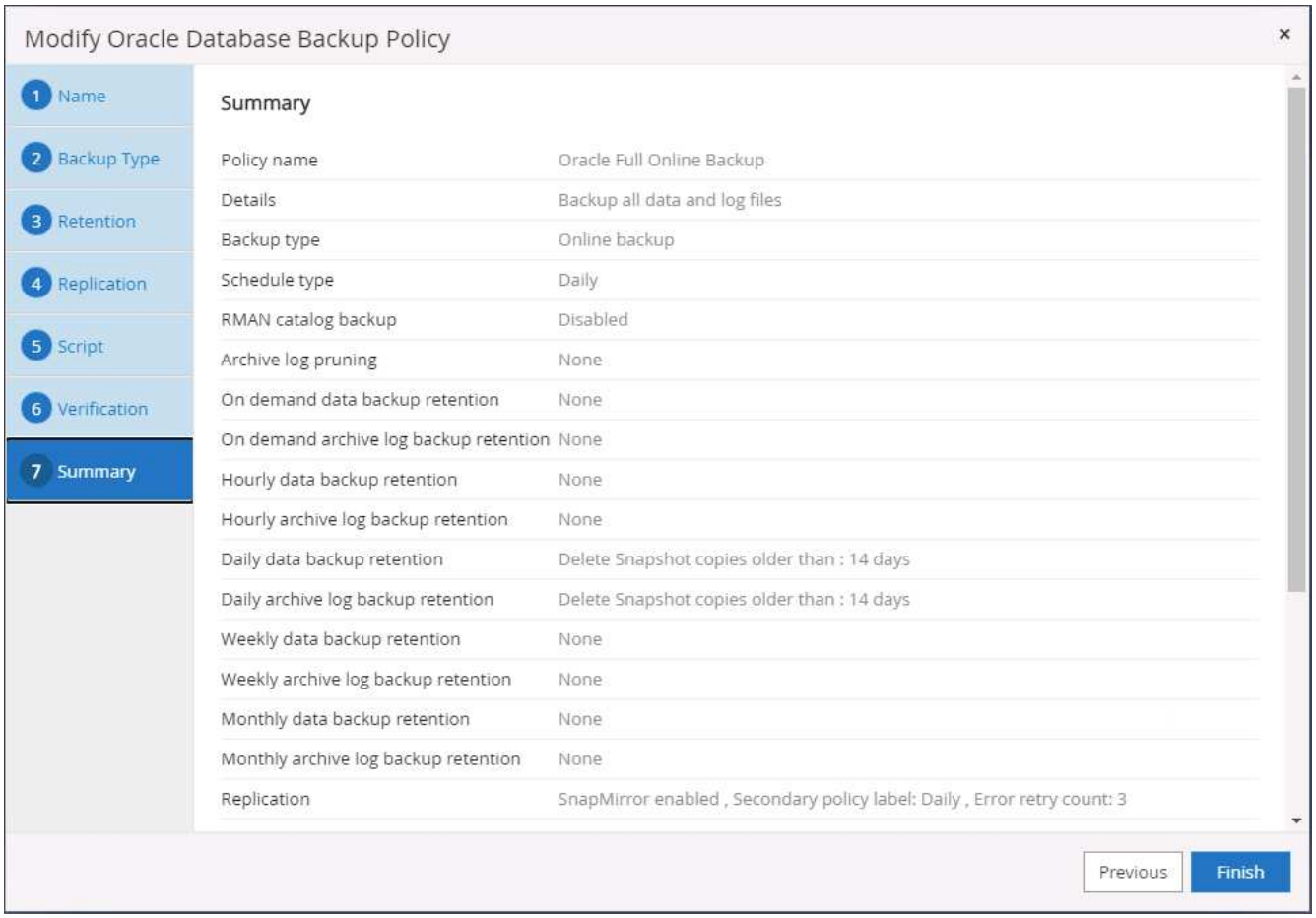
6. Especifique qualquer script opcional para ser executado antes e depois de uma execução de backup.



7. Execute a verificação de backup, se desejar.

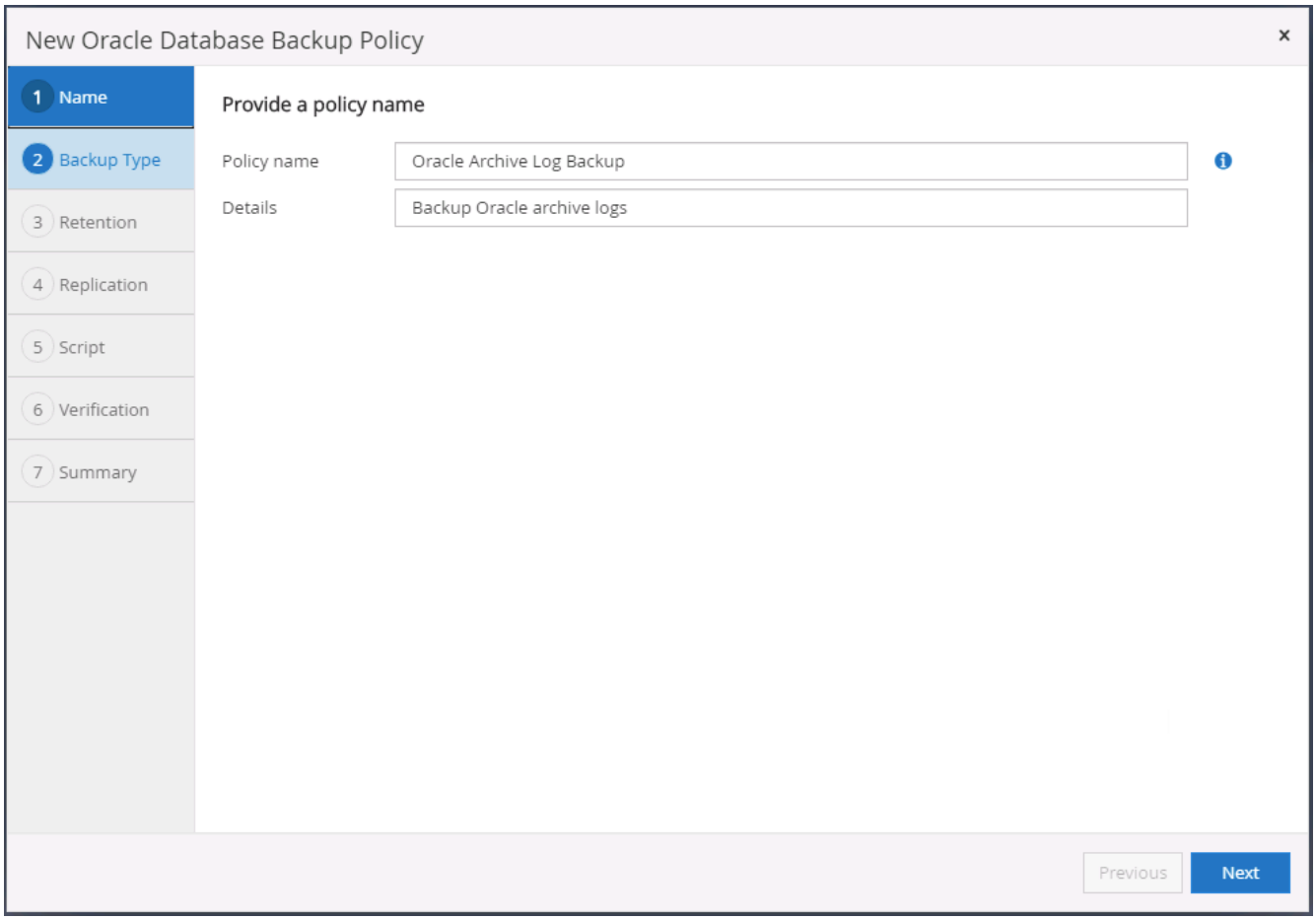

Modify Oracle Database Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run Verifications for following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.
Daily
Verification script commands
Script timeout
60
secs
Prescript full path
/var/opt/snapcenter/spl/scripts/
Enter Prescript path
Prescript arguments
Choose optional arguments...
Postscript full path
/var/opt/snapcenter/spl/scripts/
Enter Postscript path
Postscript arguments
Choose optional arguments...
Previous
Next

8. Resumo.

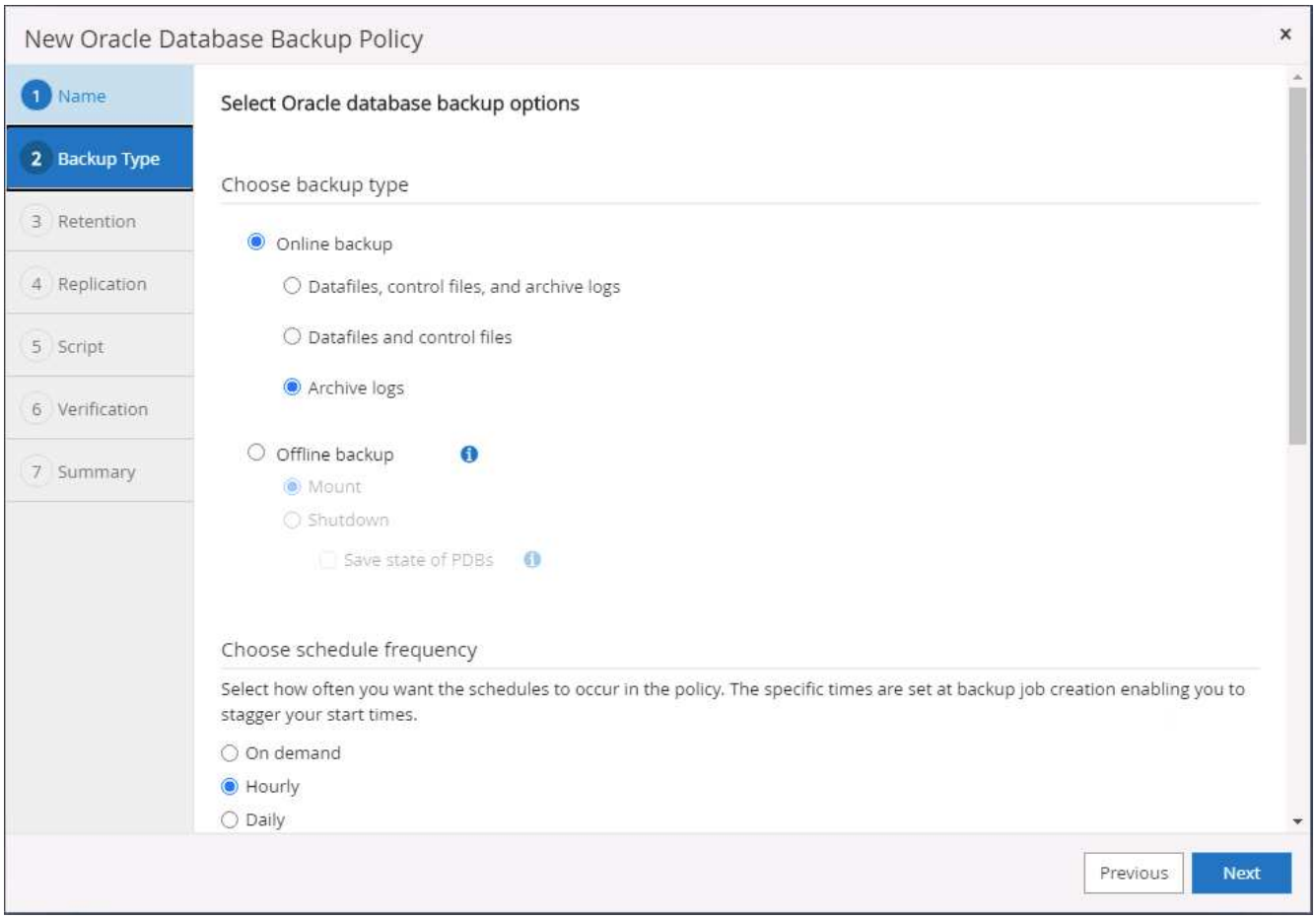


Crie uma política de backup de log de banco de dados para Oracle

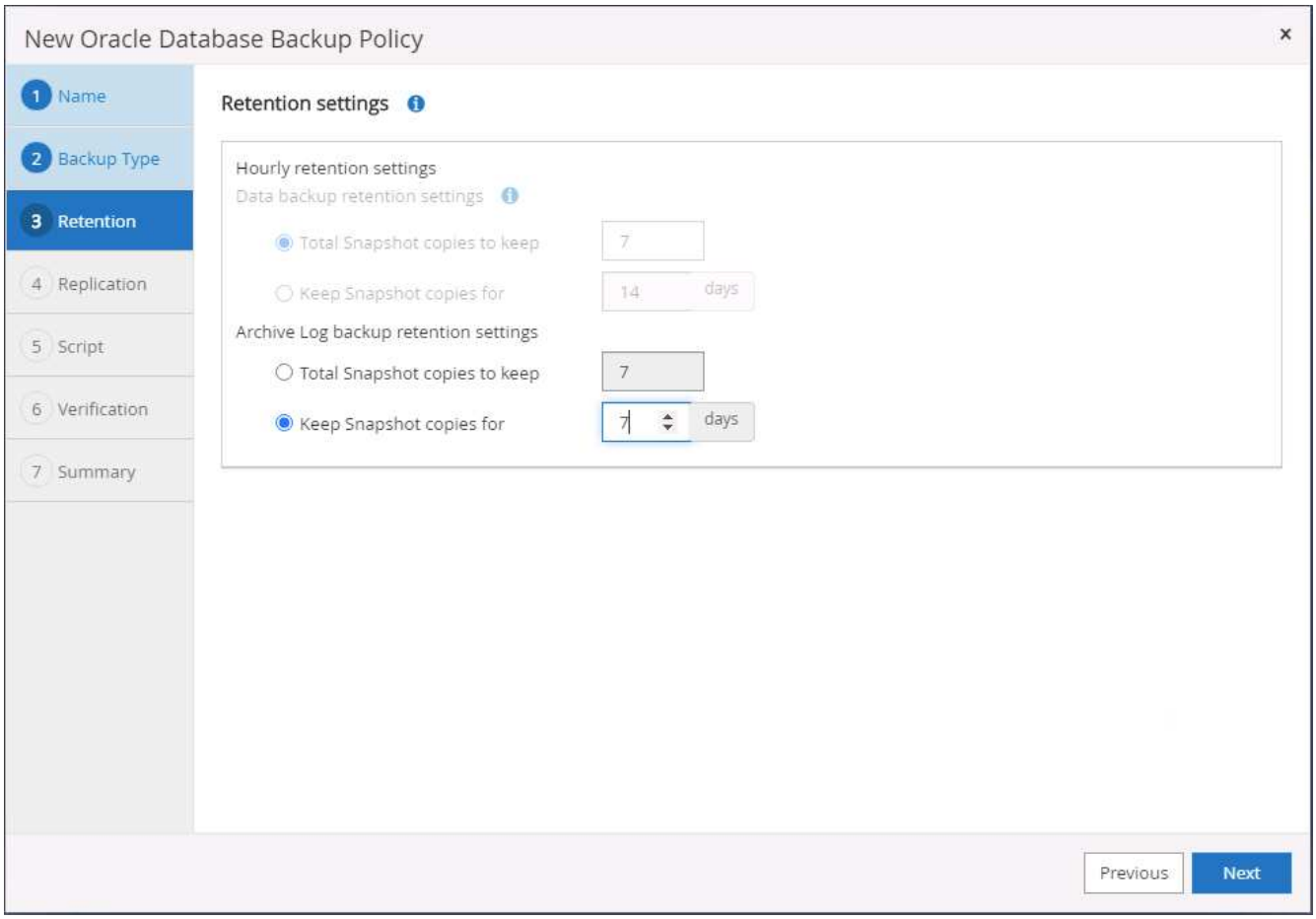
1. Efetue login no SnapCenter com um ID de usuário de gerenciamento de banco de dados, clique em Configurações e depois em Políticas.
2. Clique em Novo para iniciar um novo fluxo de trabalho de criação de política de backup ou escolha uma política existente para modificação.



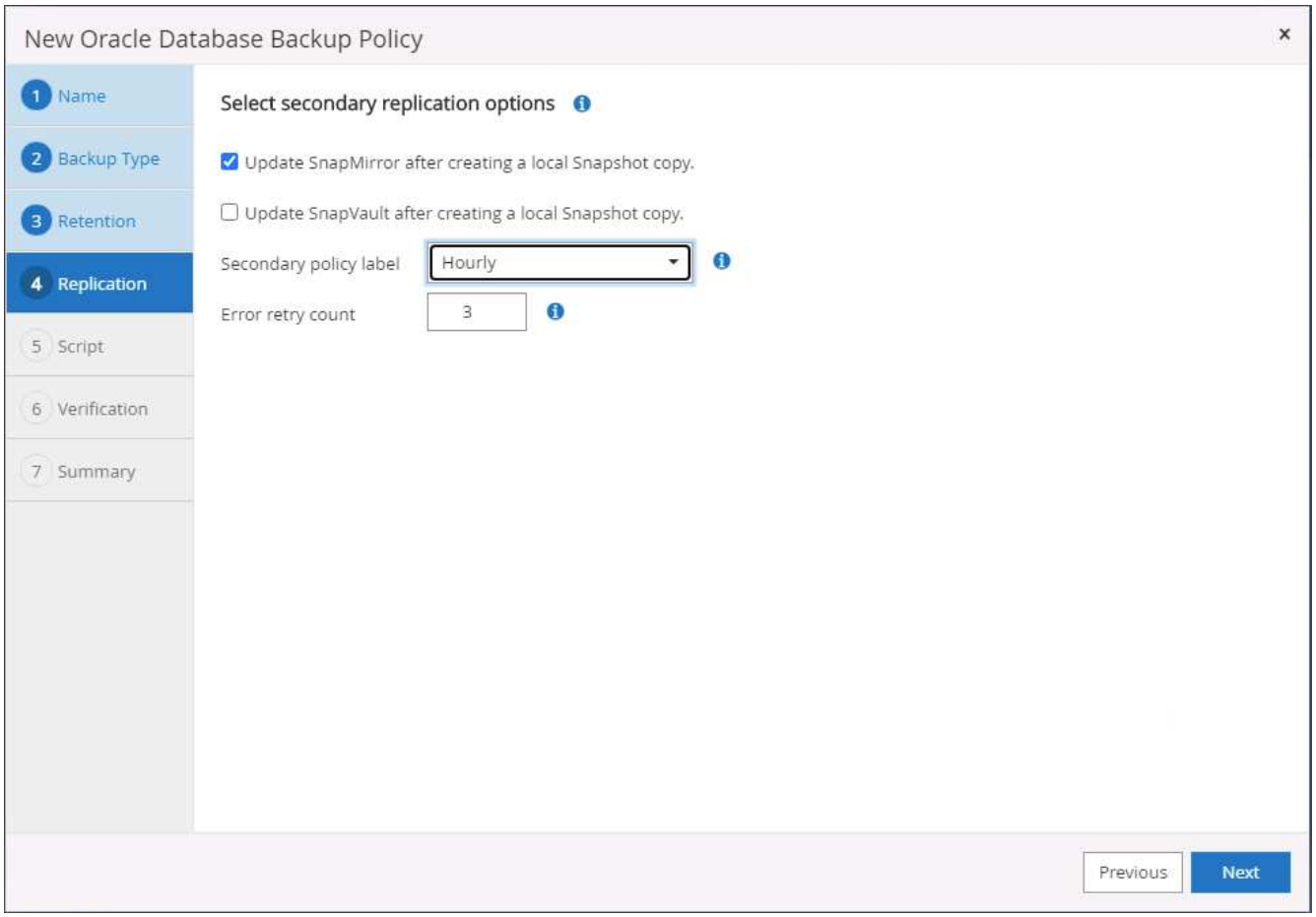
3. Selecione o tipo de backup e a frequência agendada.



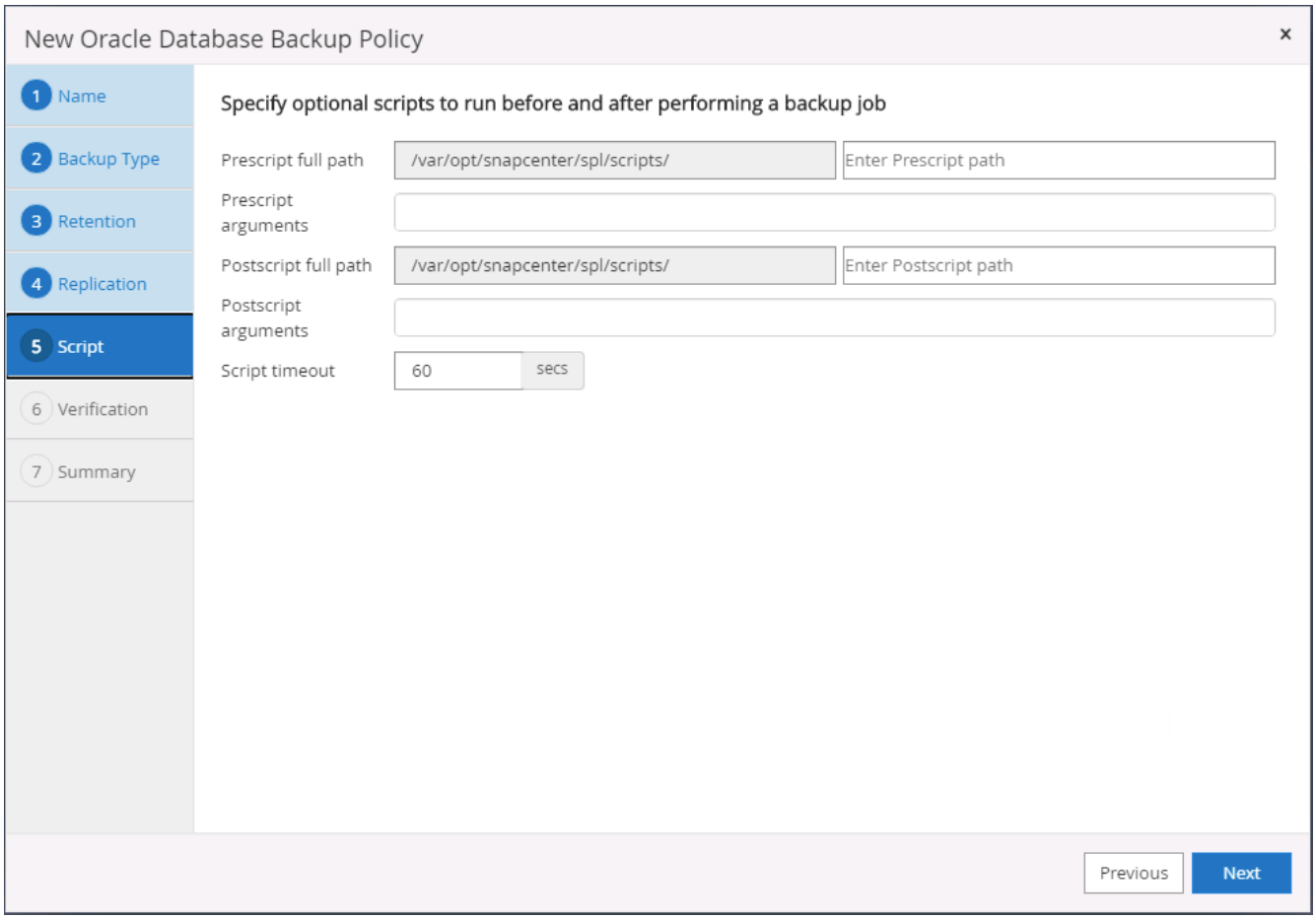
4. Defina o período de retenção do log.



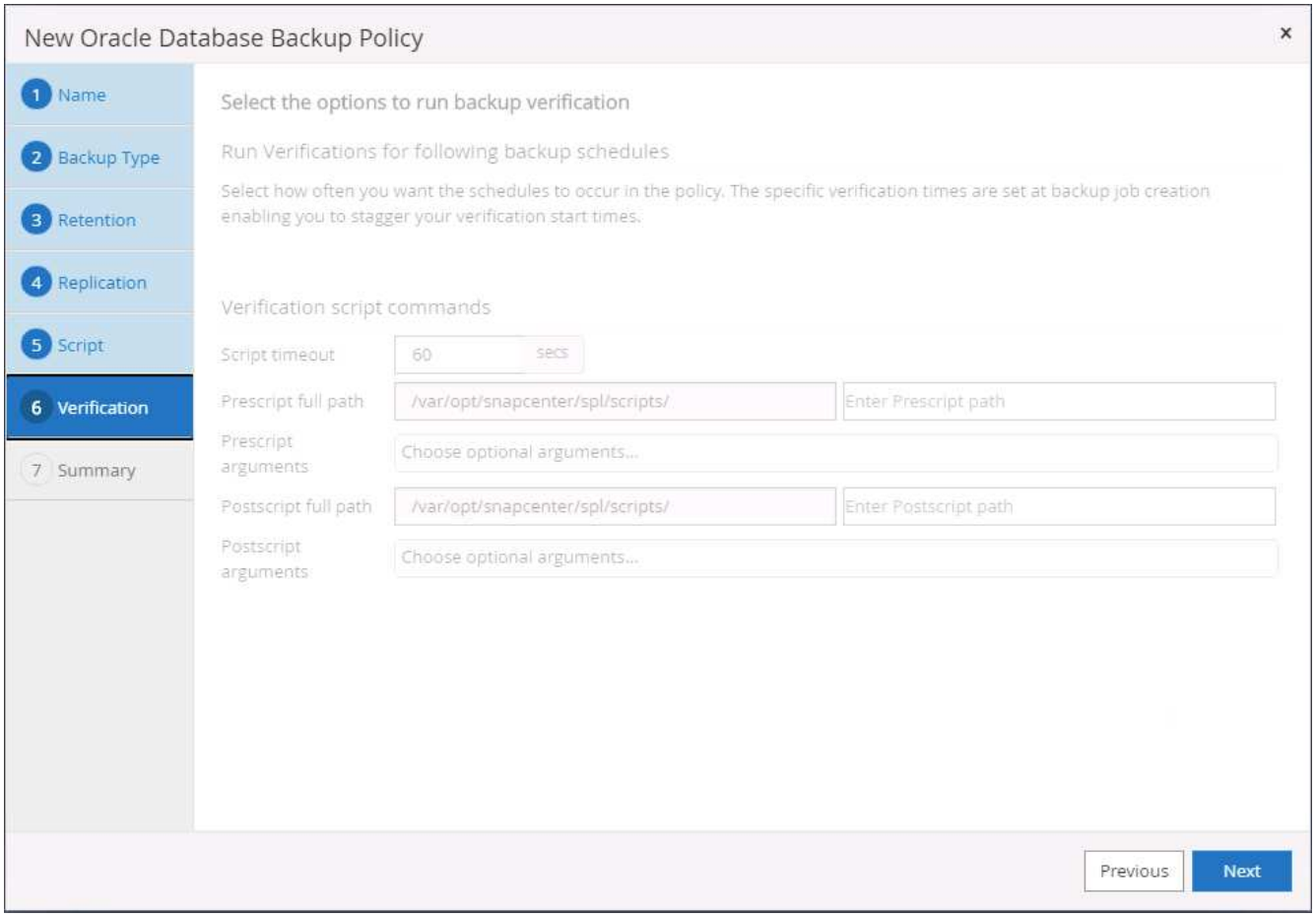
5. Habilite a replicação para um local secundário na nuvem pública.



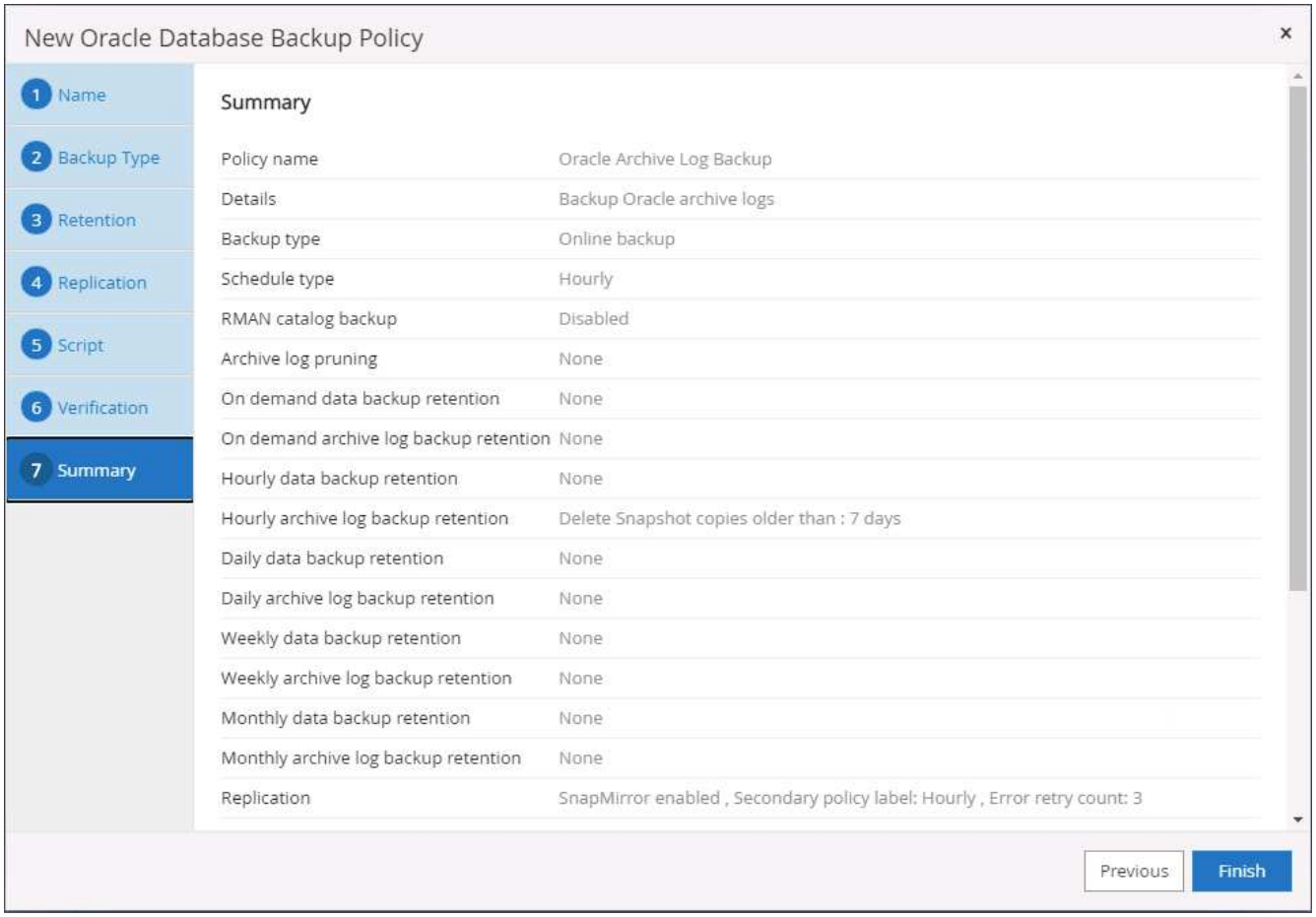
6. Especifique quaisquer scripts opcionais a serem executados antes e depois do backup do log.



7. Especifique quaisquer scripts de verificação de backup.

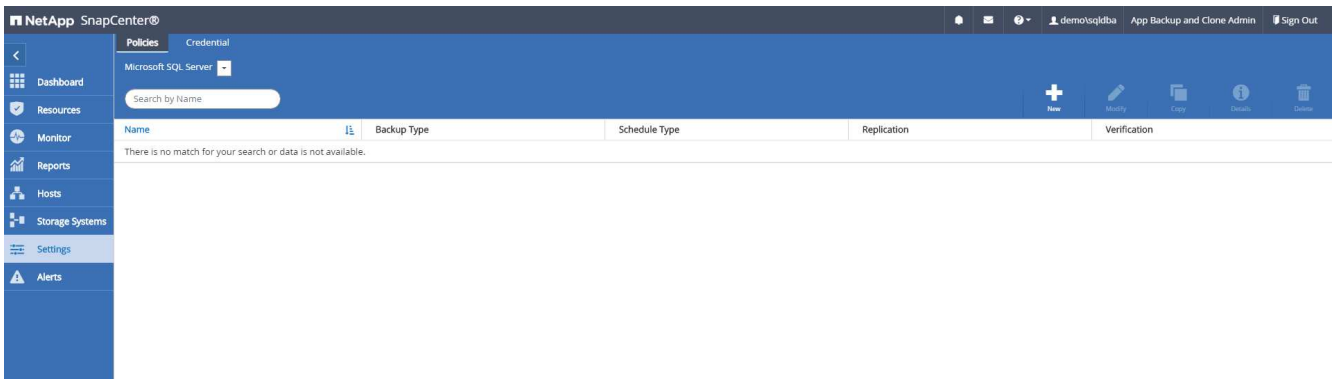

New Oracle Database Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run Verifications for following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.
Verification script commands
Script timeout
60
secs
Prescript full path
/var/opt/snapcenter/spl/scripts/
Enter Prescript path
Prescript arguments
Choose optional arguments...
Postscript full path
/var/opt/snapcenter/spl/scripts/
Enter Postscript path
Postscript arguments
Choose optional arguments...
Previous
Next

8. Resumo.

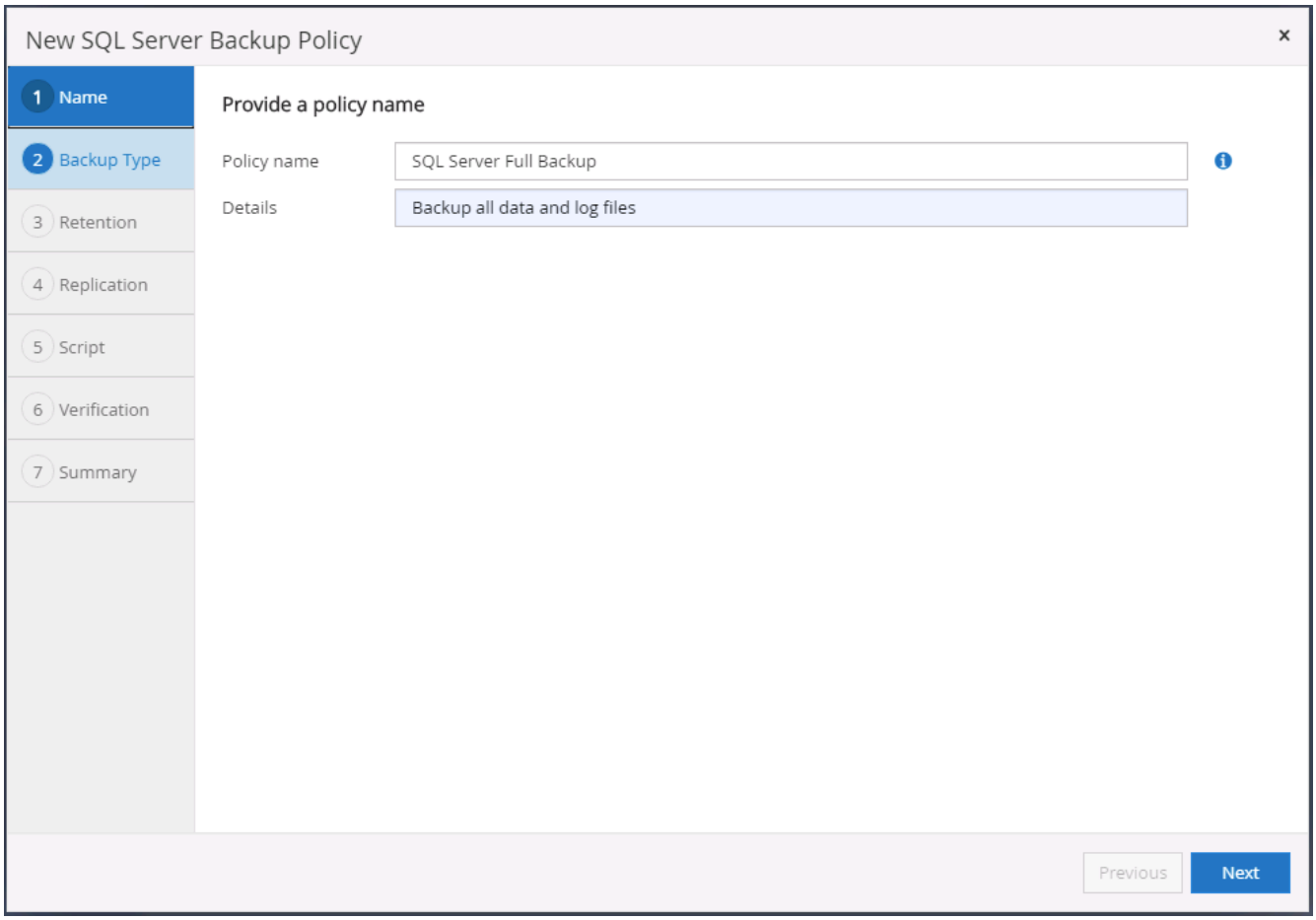


Crie uma política de backup de banco de dados completa para SQL

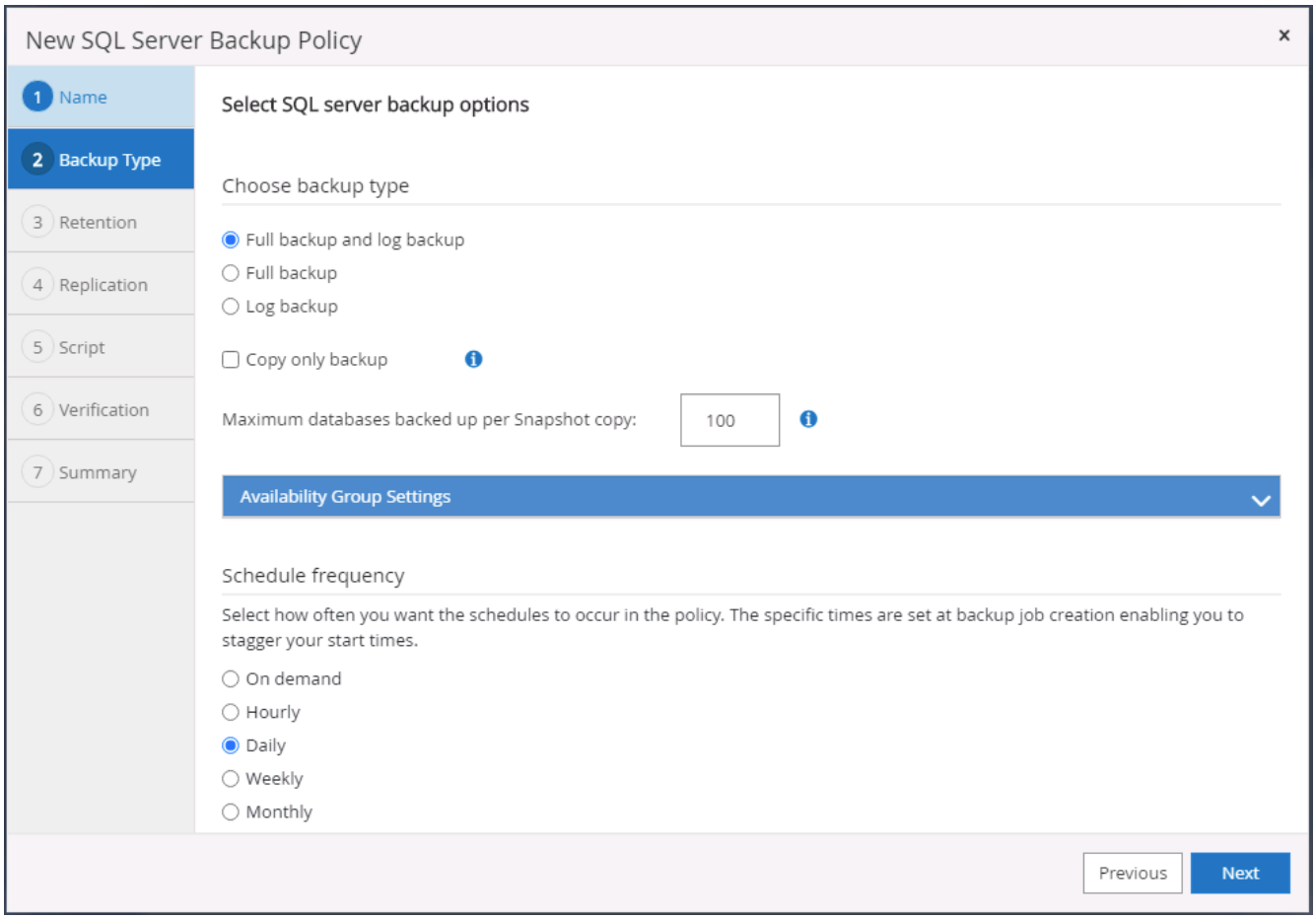
1. Efetue login no SnapCenter com um ID de usuário de gerenciamento de banco de dados, clique em Configurações e depois em Políticas.



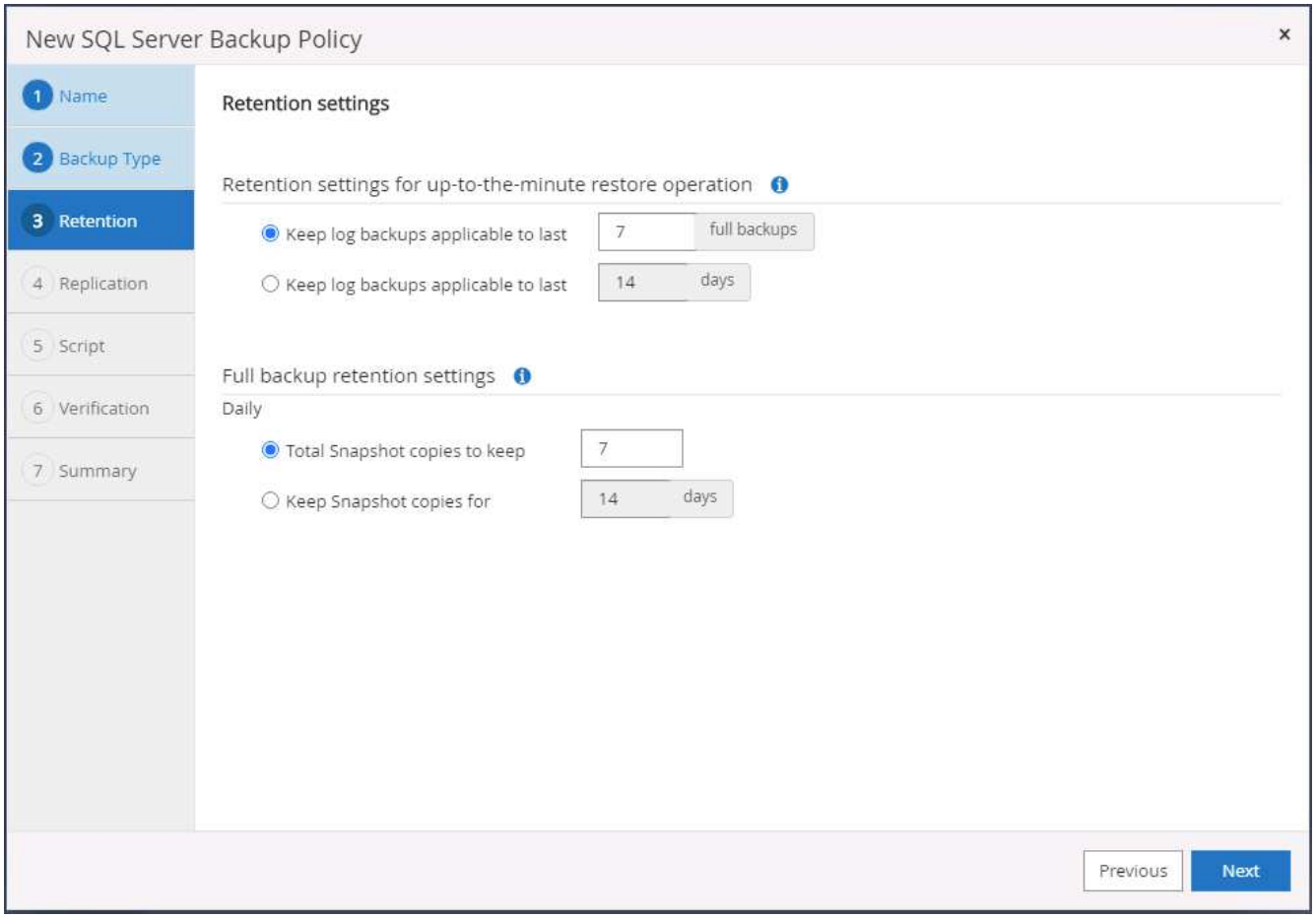
2. Clique em Novo para iniciar um novo fluxo de trabalho de criação de política de backup ou escolha uma política existente para modificação.



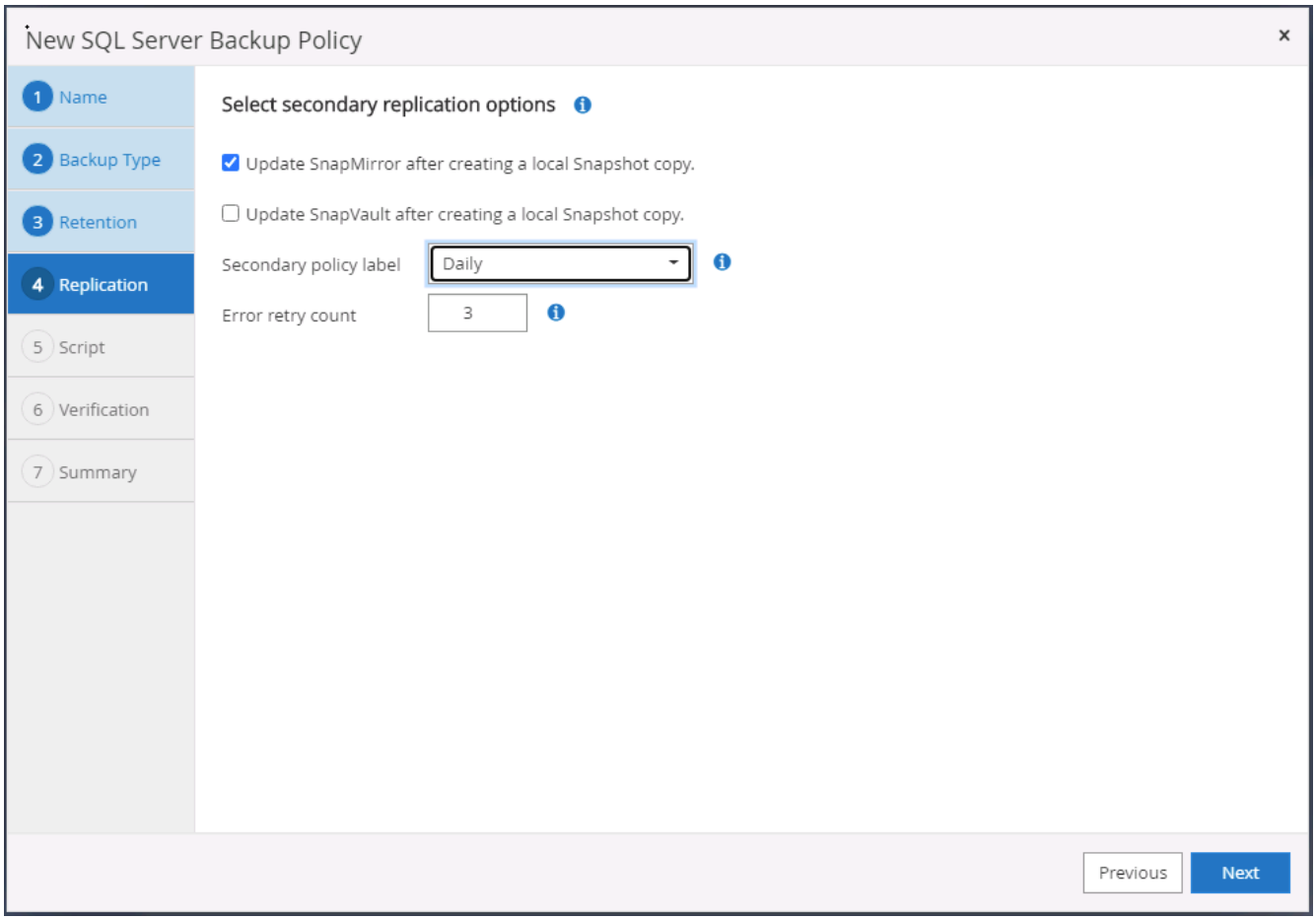
3. Defina a opção de backup e agende a frequência. Para o SQL Server configurado com um grupo de disponibilidade, uma réplica de backup preferencial pode ser definida.



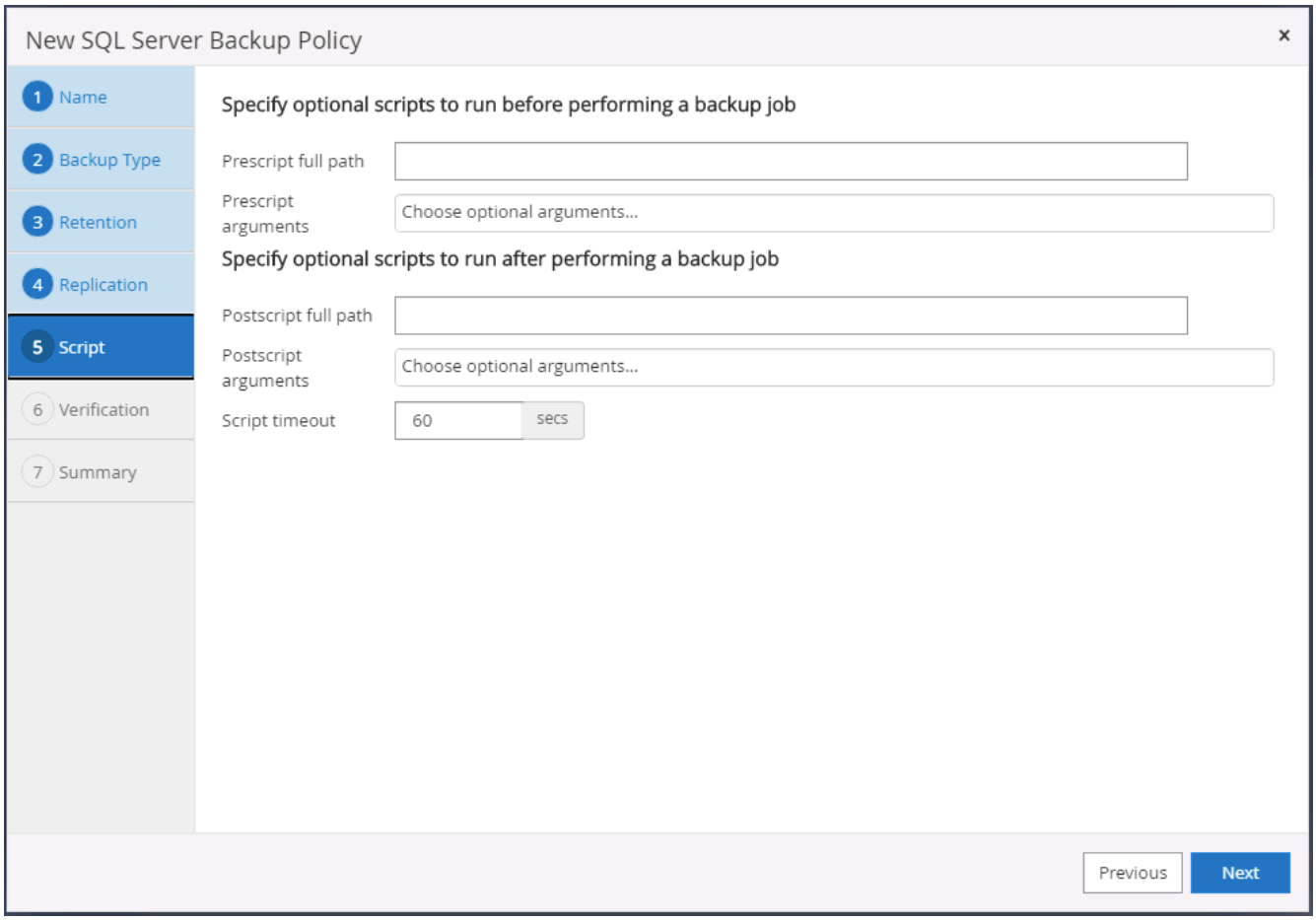
4. Defina o período de retenção do backup.



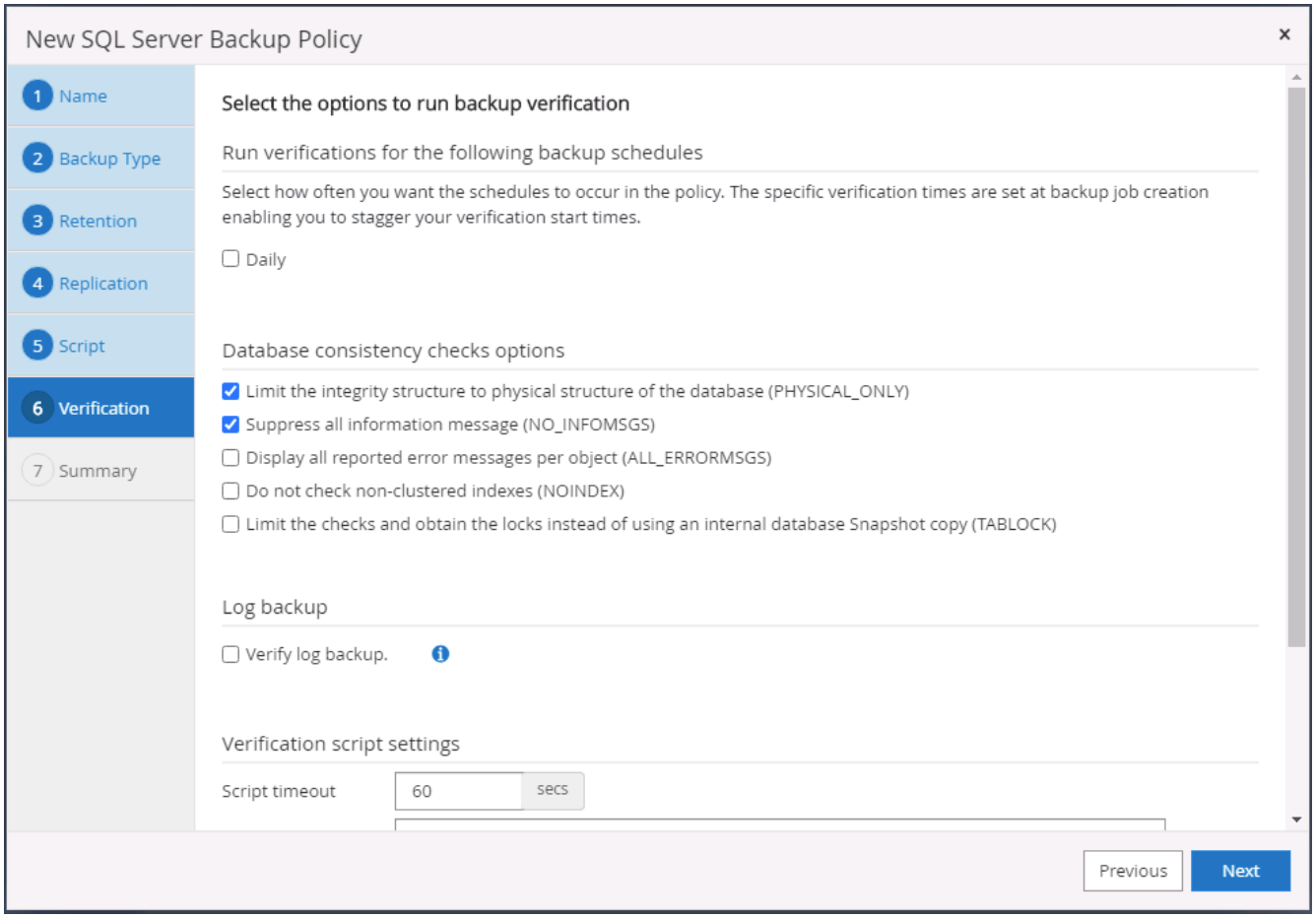
5. Habilite a replicação de cópias de backup para um local secundário na nuvem.



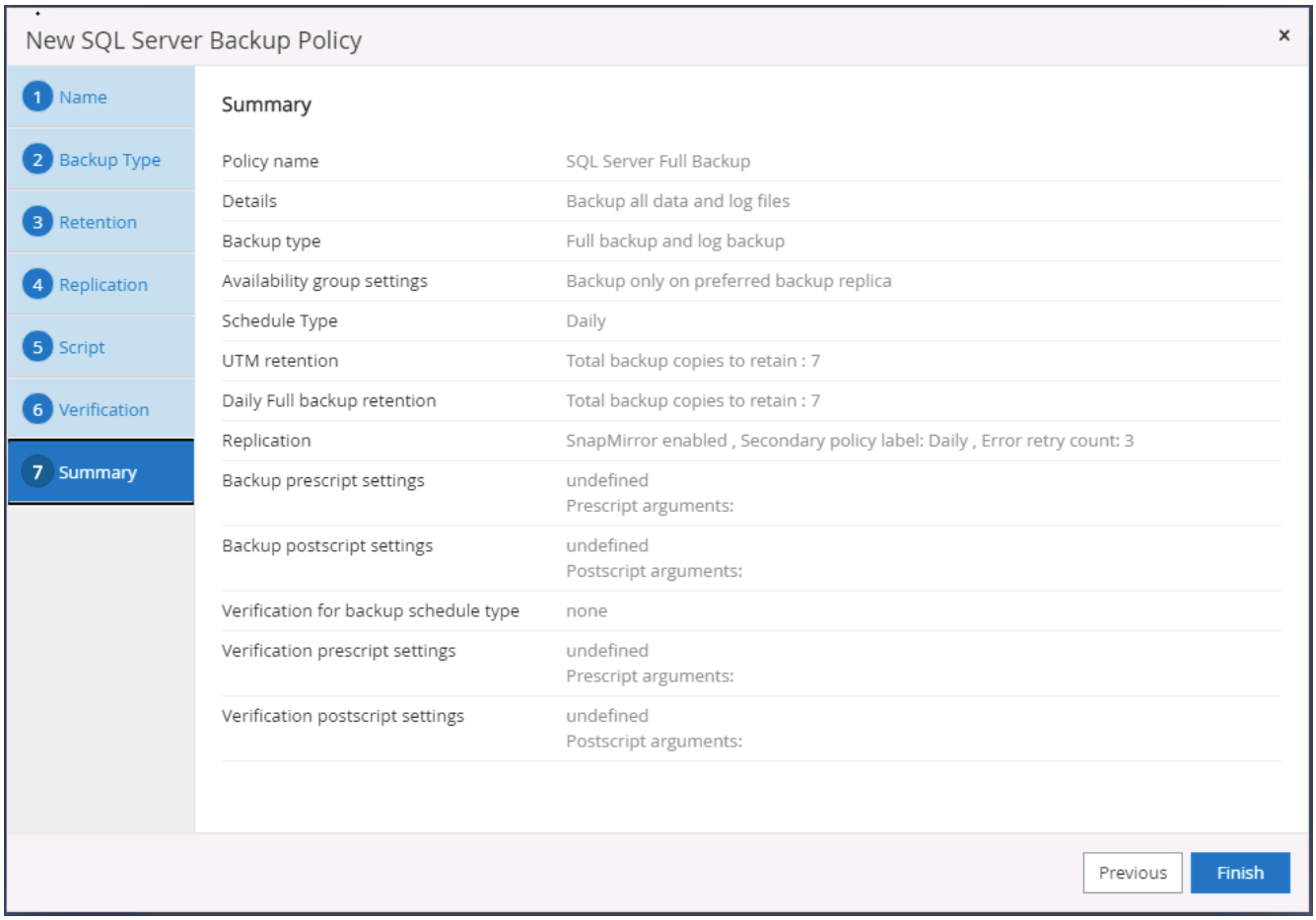
6. Especifique quaisquer scripts opcionais a serem executados antes ou depois de uma tarefa de backup.



7. Especifique as opções para executar a verificação de backup.

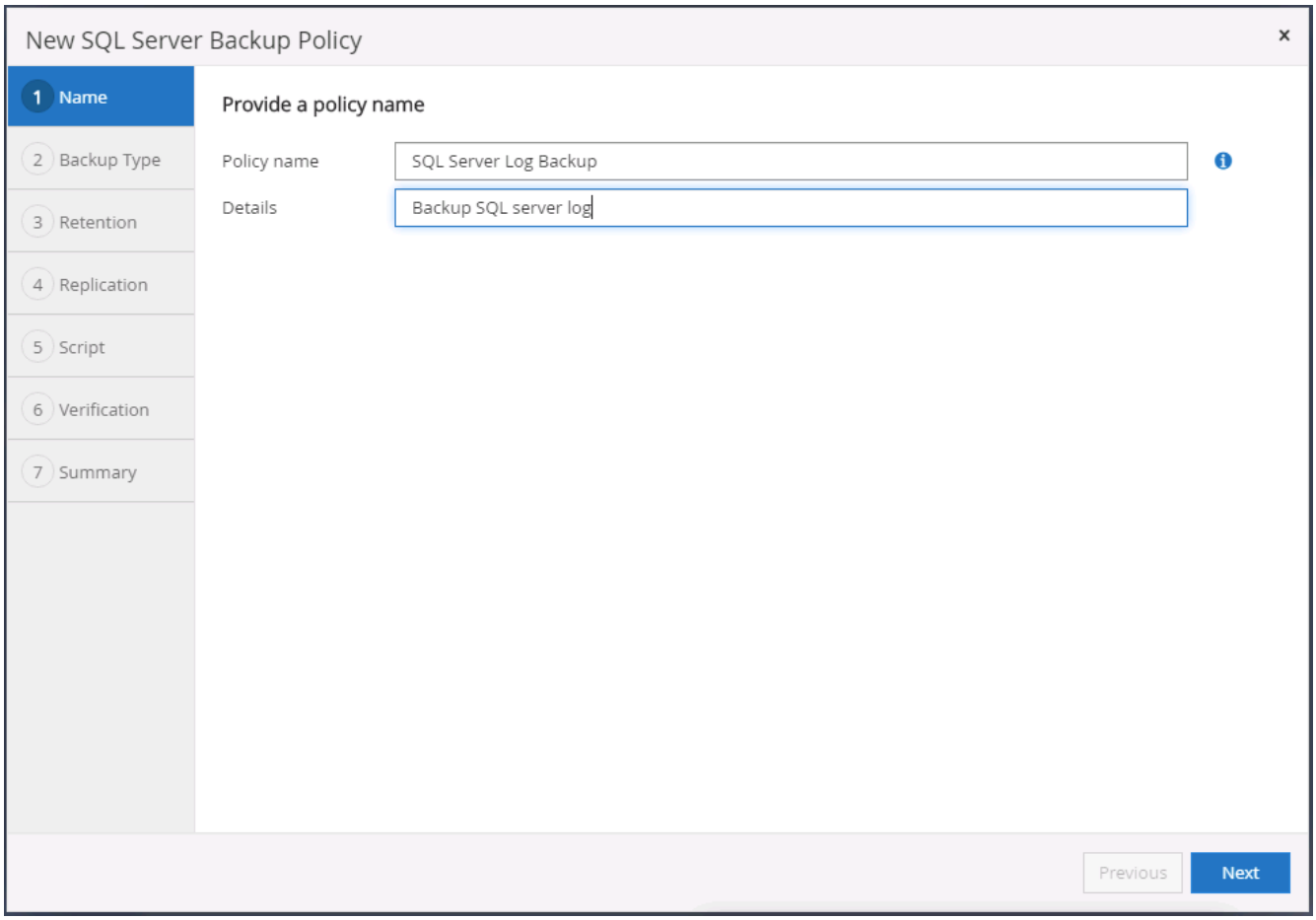

New SQL Server Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run verifications for the following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.
Daily
Database consistency checks options
Limit the integrity structure to physical structure of the database (PHYSICAL_ONLY)
Suppress all information message (NO_INFOMSGS)
Display all reported error messages per object (ALL_ERRORMSGS)
Do not check non-clustered indexes (NOINDEX)
Limit the checks and obtain the locks instead of using an internal database Snapshot copy (TABLOCK)
Log backup
Verify log backup.
Verification script settings
Script timeout
60
secs
Previous
Next

8. Resumo.

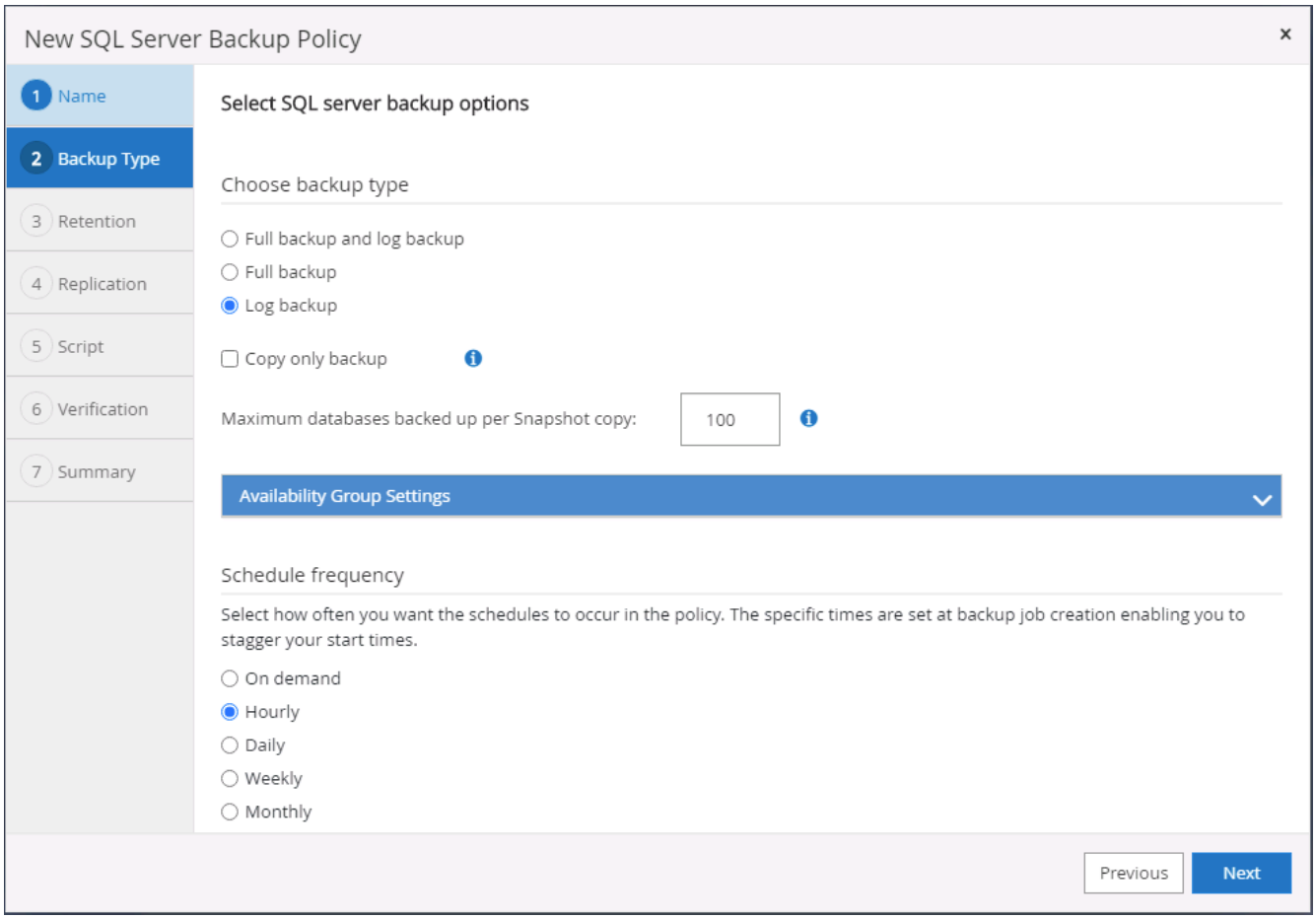


Crie uma política de backup de log de banco de dados para SQL.

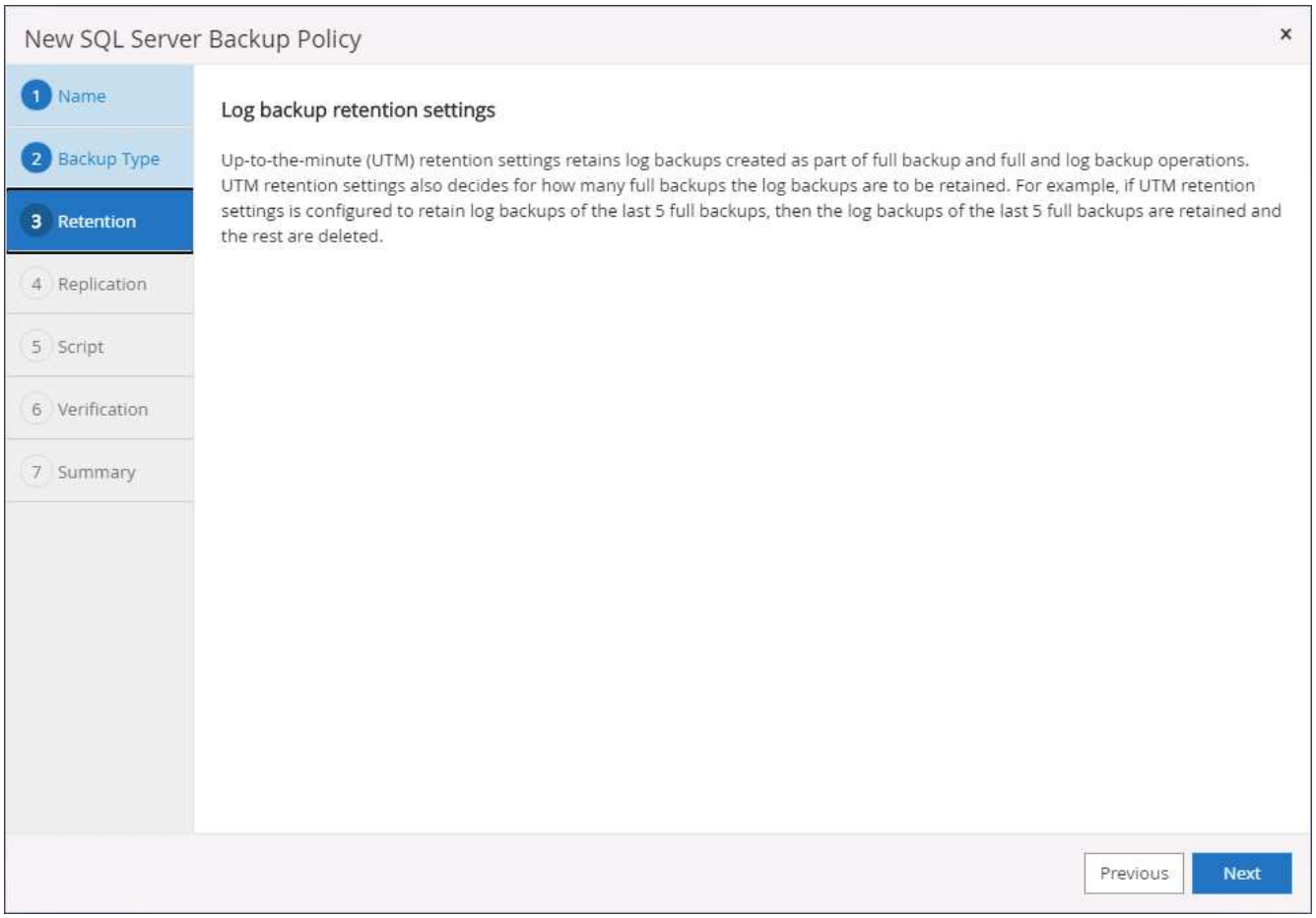
1. Efetue login no SnapCenter com um ID de usuário de gerenciamento de banco de dados, clique em Configurações > Políticas e depois em Novo para iniciar um novo fluxo de trabalho de criação de políticas.



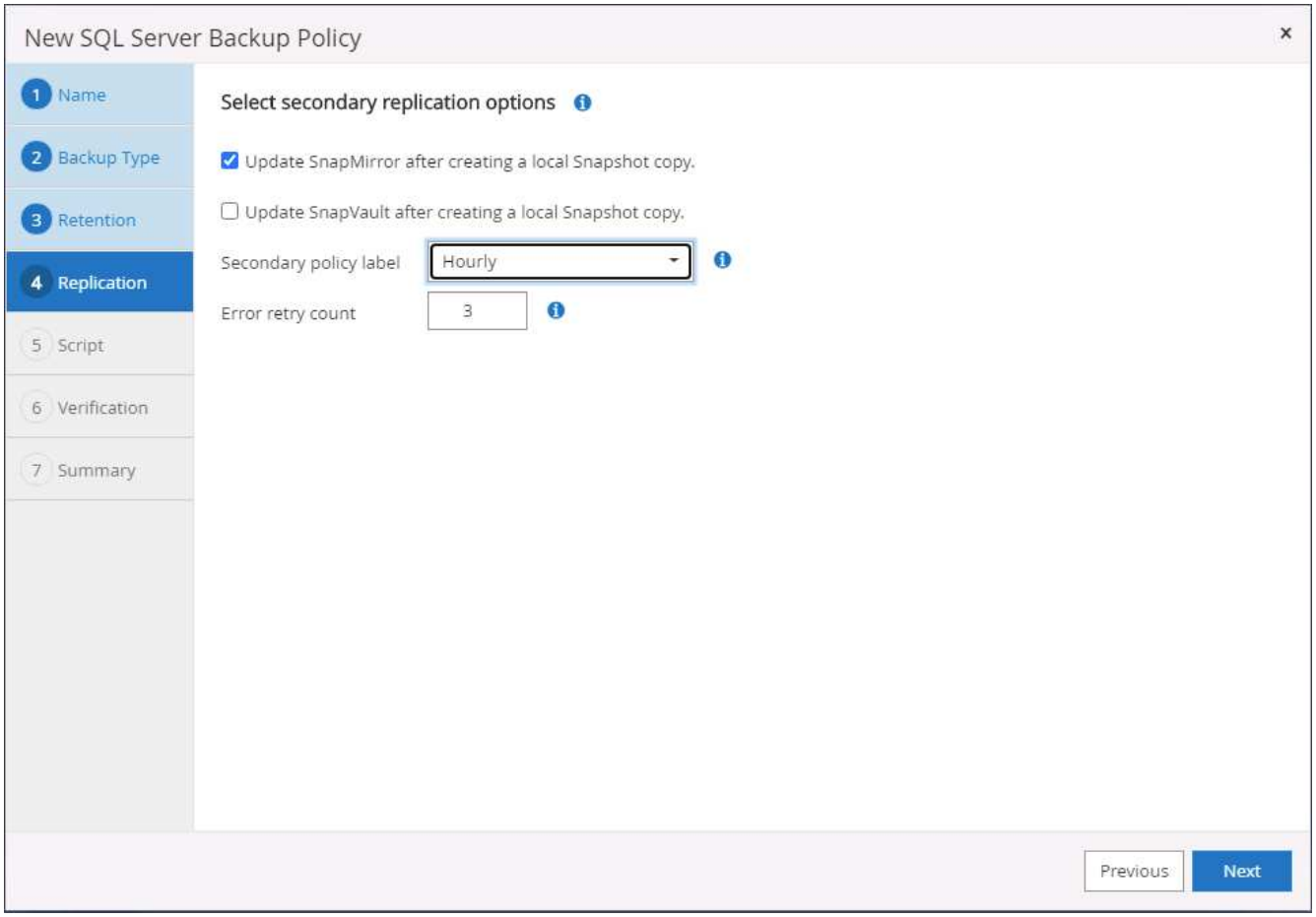
2. Defina a opção de backup de log e agende a frequência. Para o SQL Server configurado com um grupo de disponibilidade, uma réplica de backup preferencial pode ser definida.



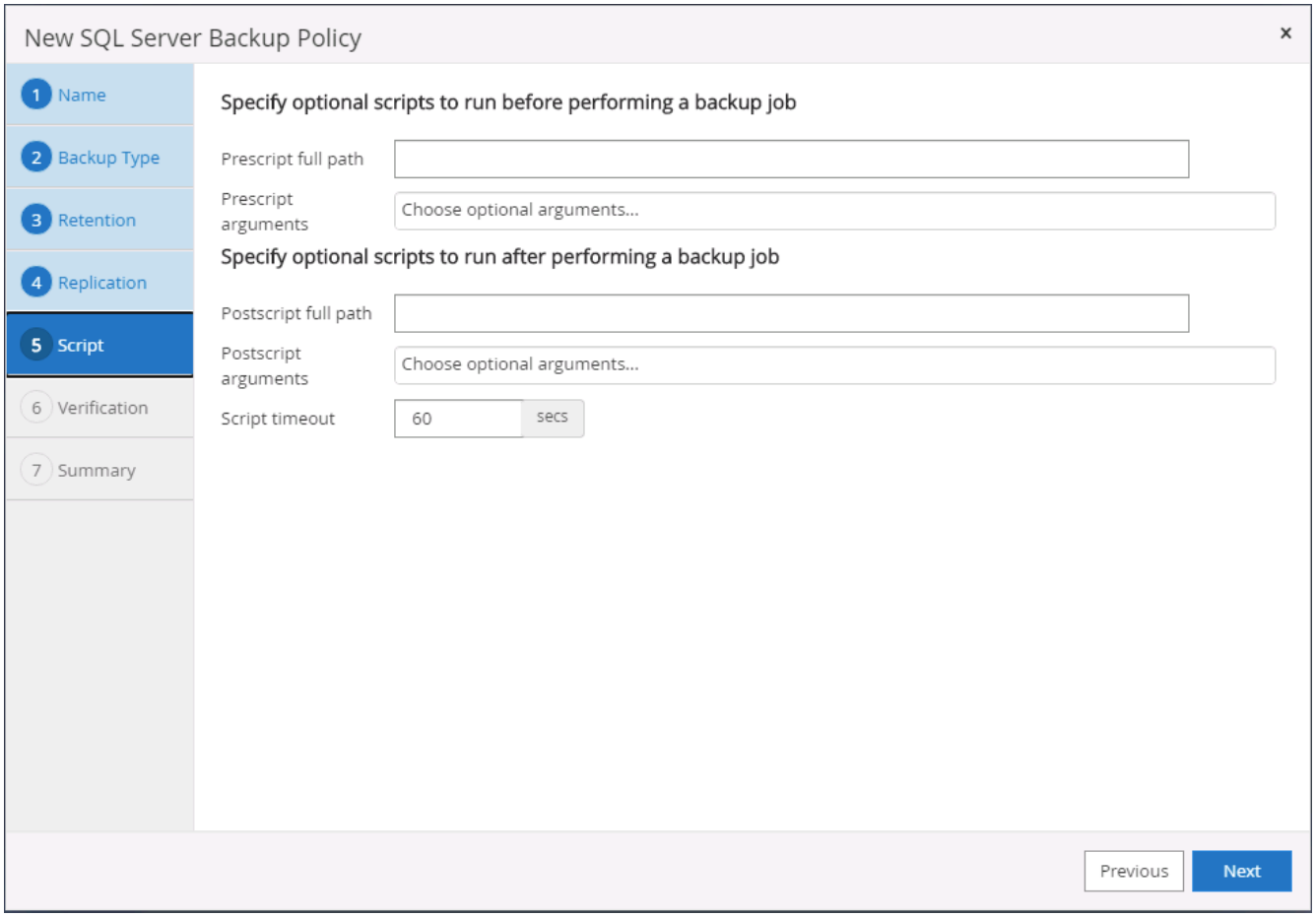
3. A política de backup de dados do servidor SQL define a retenção do backup de log; aceite os padrões aqui.



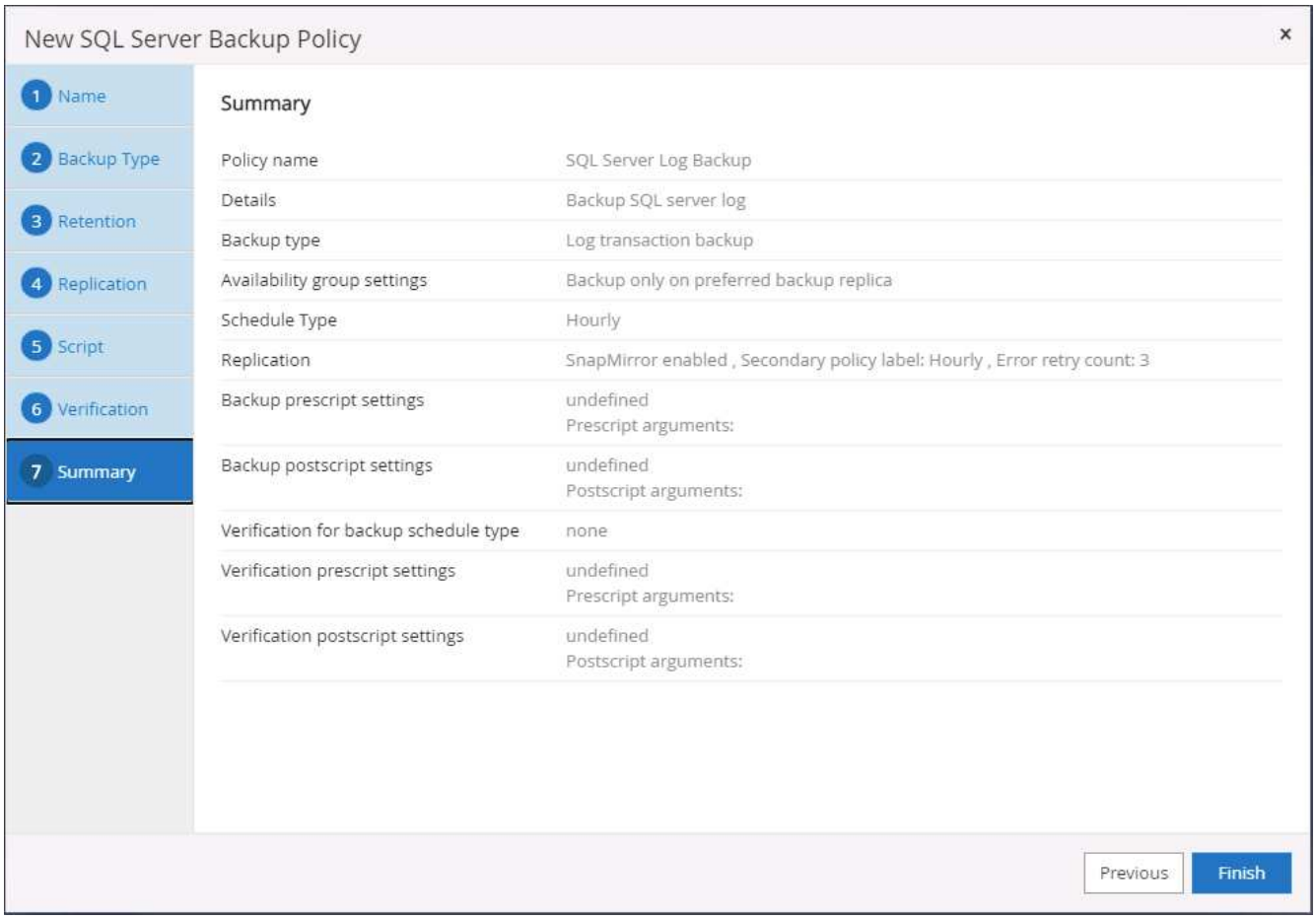
4. Habilite a replicação de backup de log para secundário na nuvem.



5. Especifique quaisquer scripts opcionais a serem executados antes ou depois de uma tarefa de backup.


New SQL Server Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Specify optional scripts to run before performing a backup job
Prescript full path
Prescript arguments
Choose optional arguments...
Specify optional scripts to run after performing a backup job
Postscript full path
Postscript arguments
Choose optional arguments...
Script timeout
60
secs
Previous
Next

6. Resumo.

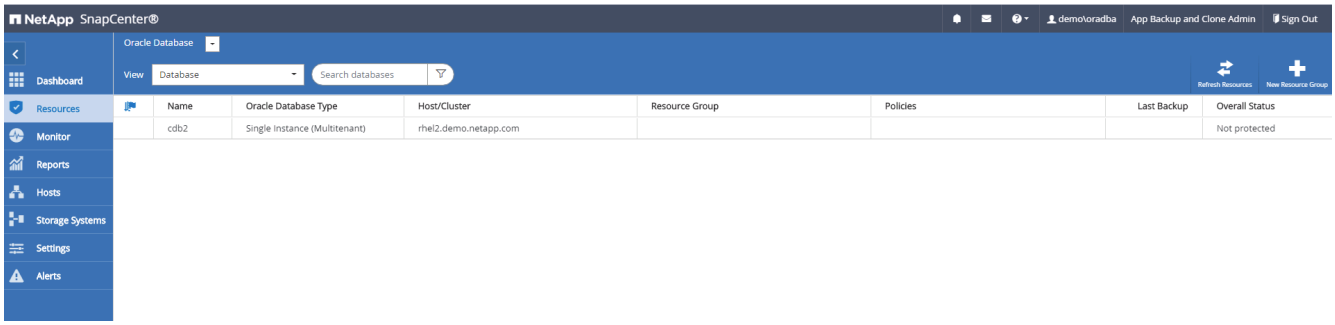


8. Implementar política de backup para proteger o banco de dados

O SnapCenter usa um grupo de recursos para fazer backup de um banco de dados em um agrupamento lógico de recursos de banco de dados, como vários bancos de dados hospedados em um servidor, um banco de dados compartilhando os mesmos volumes de armazenamento, vários bancos de dados dando suporte a um aplicativo comercial e assim por diante. Proteger um único banco de dados cria um grupo de recursos próprio. Os procedimentos a seguir demonstram como implementar uma política de backup criada na seção 7 para proteger bancos de dados Oracle e SQL Server.

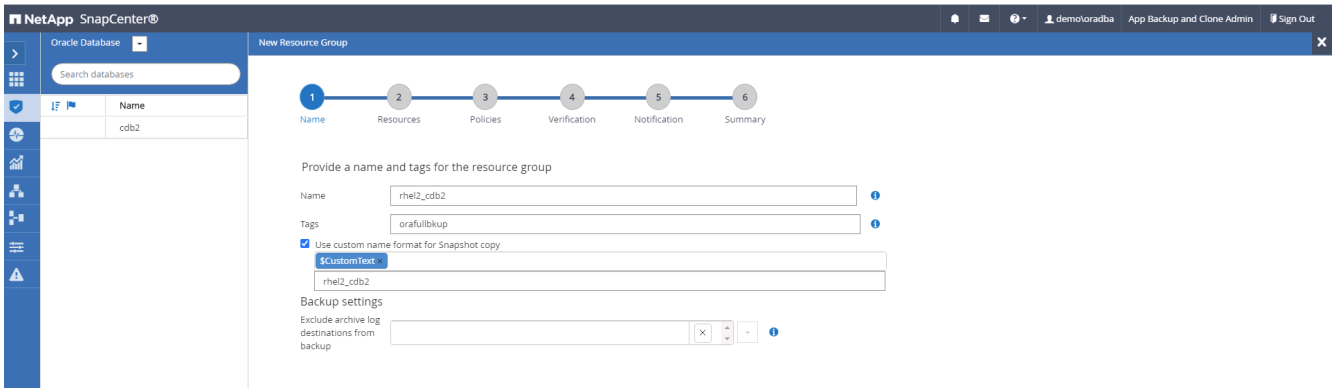
Crie um grupo de recursos para backup completo do Oracle

1. Efetue login no SnapCenter com um ID de usuário de gerenciamento de banco de dados e navegue até a guia Recursos. Na lista suspensa Exibir, escolha Banco de Dados ou Grupo de Recursos para iniciar o fluxo de trabalho de criação do grupo de recursos.

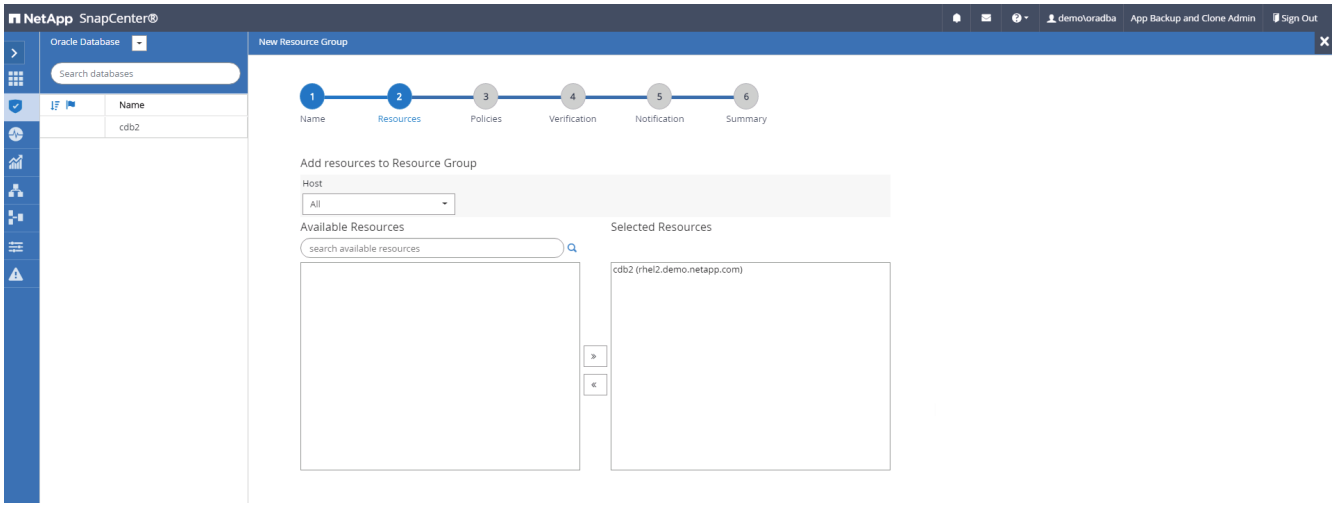


2. Forneça um nome e tags para o grupo de recursos. Você pode definir um formato de nomenclatura para a

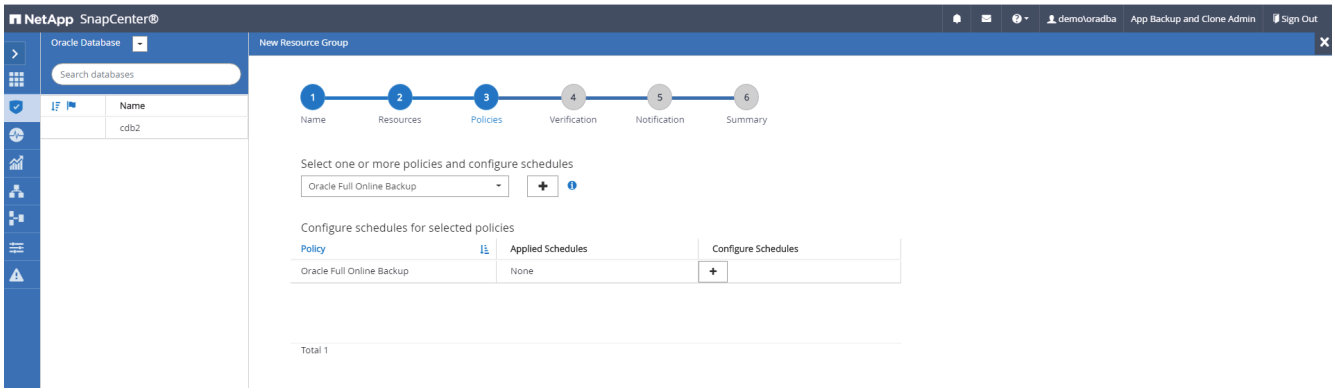
cópia do Snapshot e ignorar o destino do log de arquivamento redundante, se configurado.



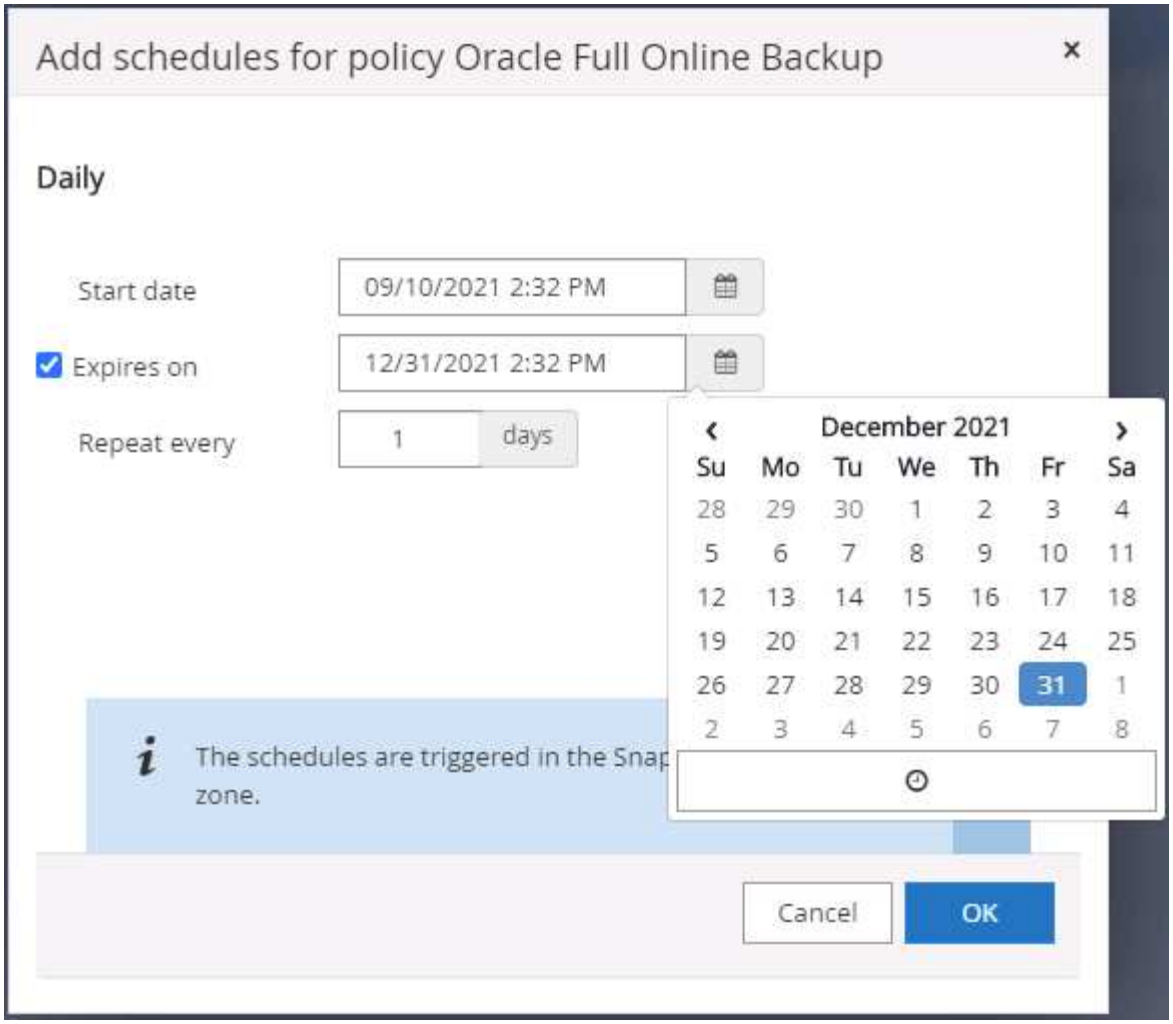
3. Adicione recursos de banco de dados ao grupo de recursos.



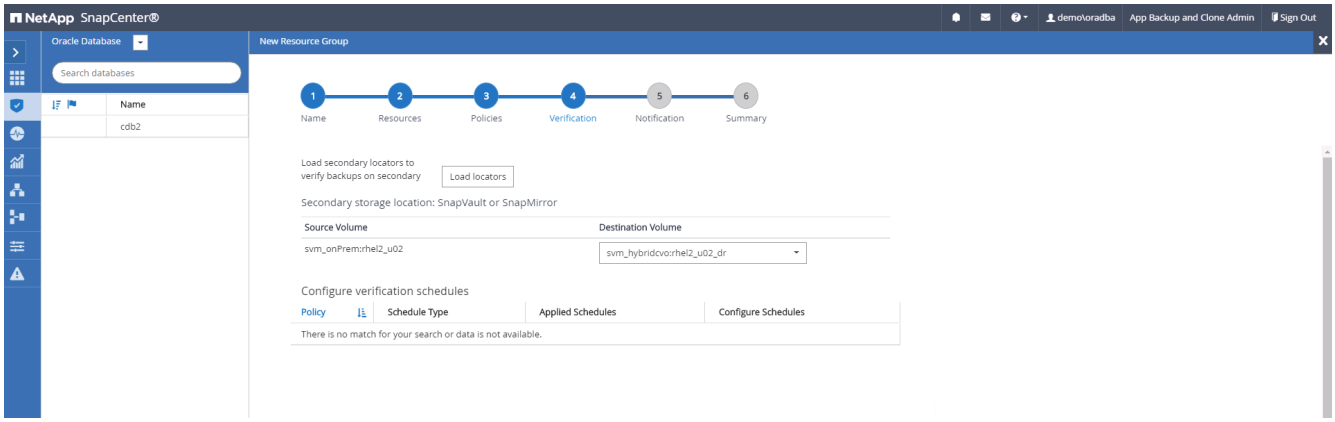
4. Selecione uma política de backup completa criada na seção 7 na lista suspensa.



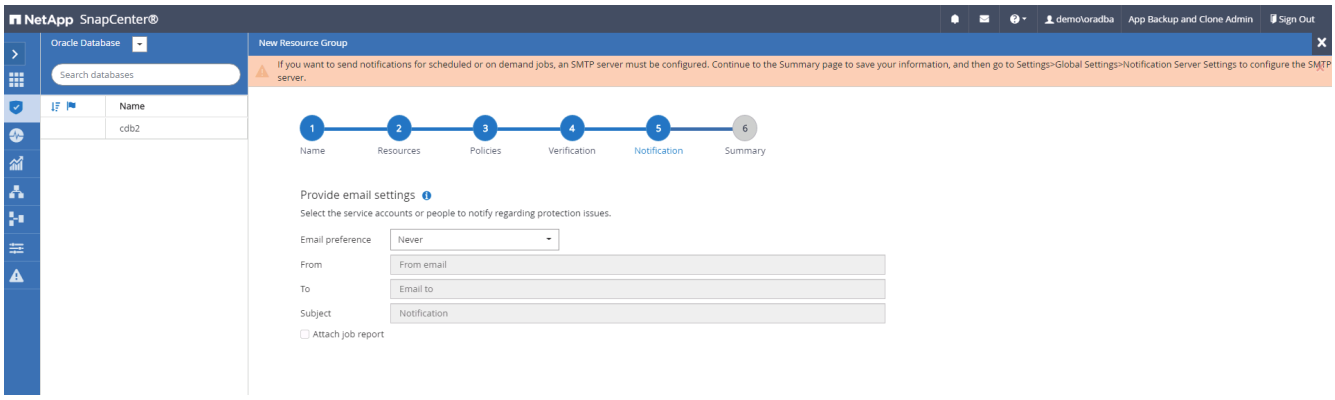
5. Clique no sinal (+) para configurar o agendamento de backup desejado.



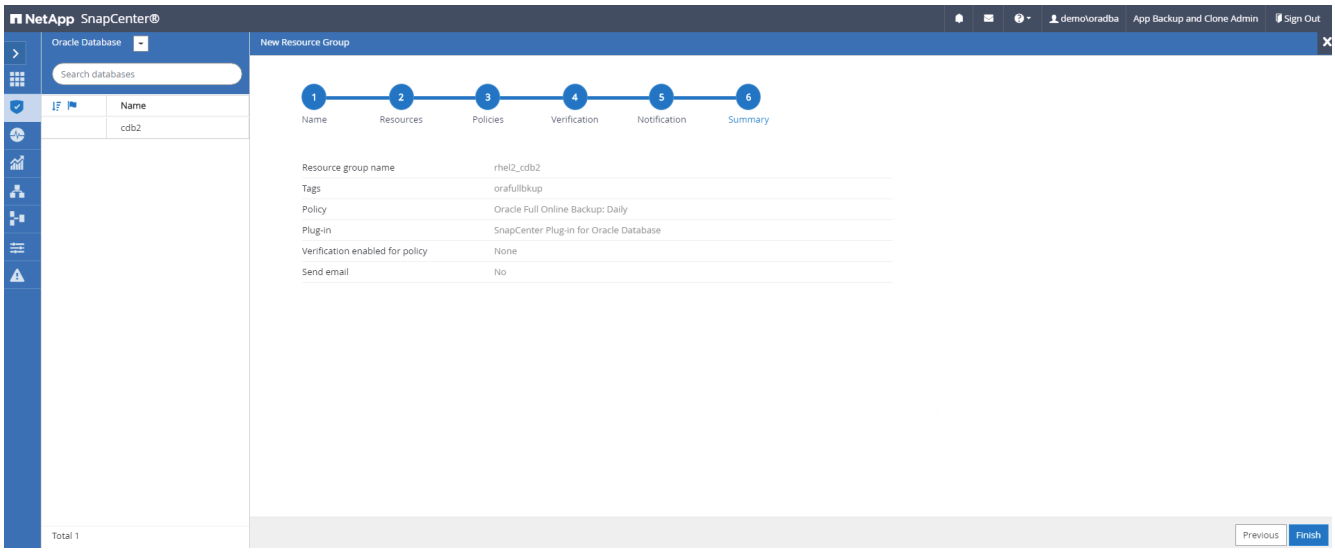
6. Clique em Carregar localizadores para carregar o volume de origem e destino.



7. Configure o servidor SMTP para notificação por email, se desejar.

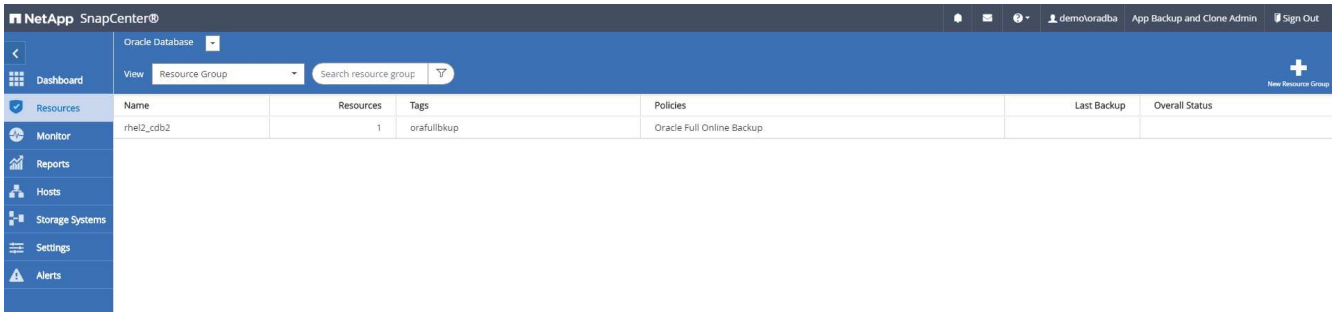


8. Resumo.

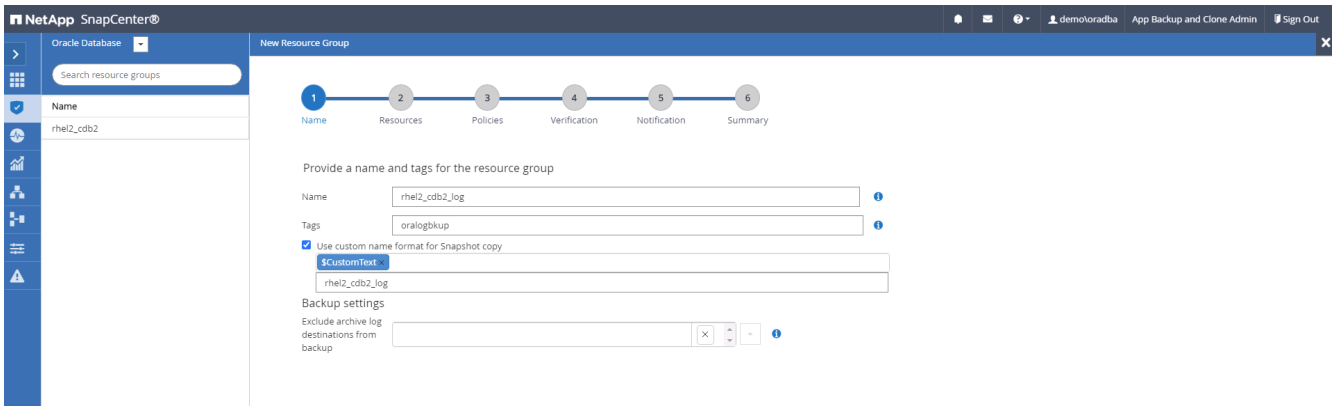


Crie um grupo de recursos para backup de log do Oracle

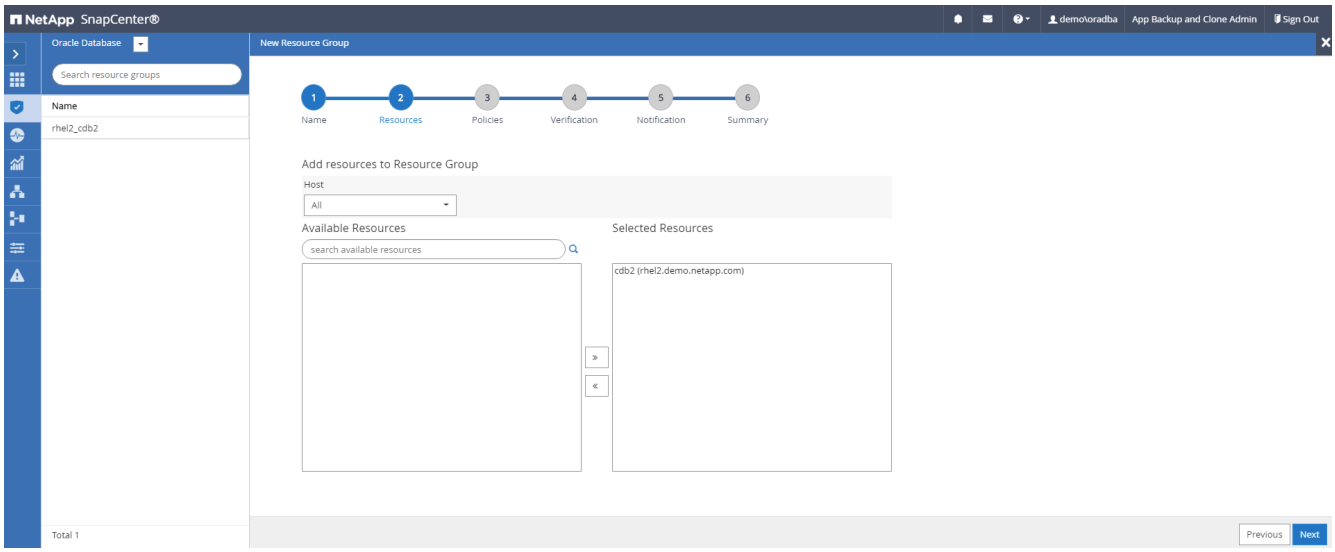
1. Efetue login no SnapCenter com um ID de usuário de gerenciamento de banco de dados e navegue até a guia Recursos. Na lista suspensa Exibir, escolha Banco de Dados ou Grupo de Recursos para iniciar o fluxo de trabalho de criação do grupo de recursos.



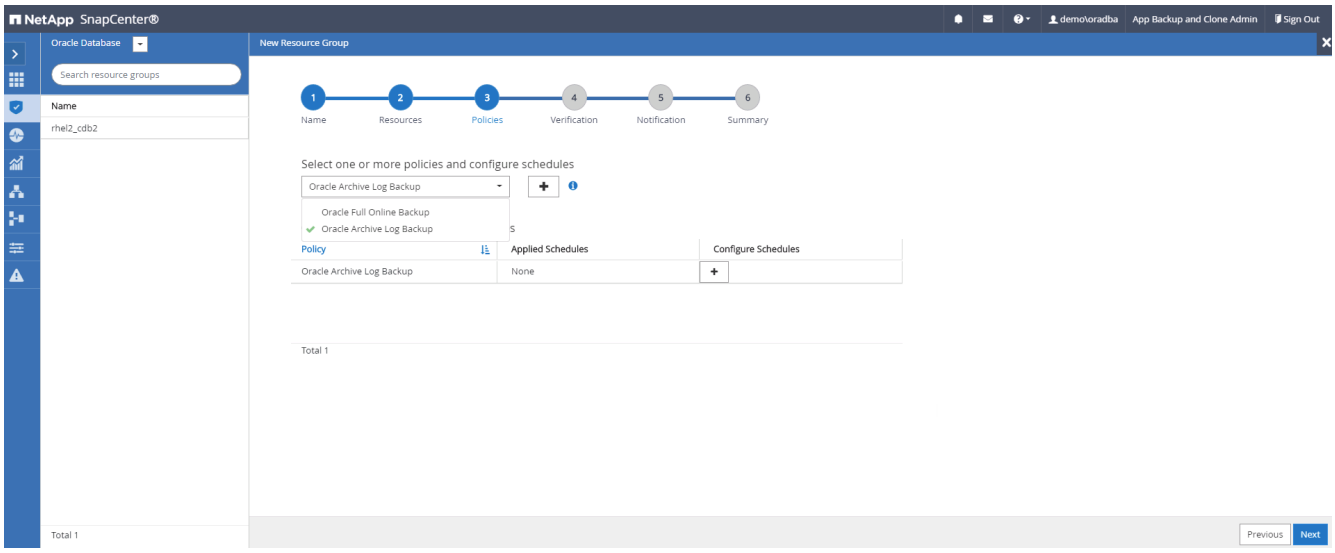
2. Forneça um nome e tags para o grupo de recursos. Você pode definir um formato de nomenclatura para a cópia do Snapshot e ignorar o destino do log de arquivamento redundante, se configurado.



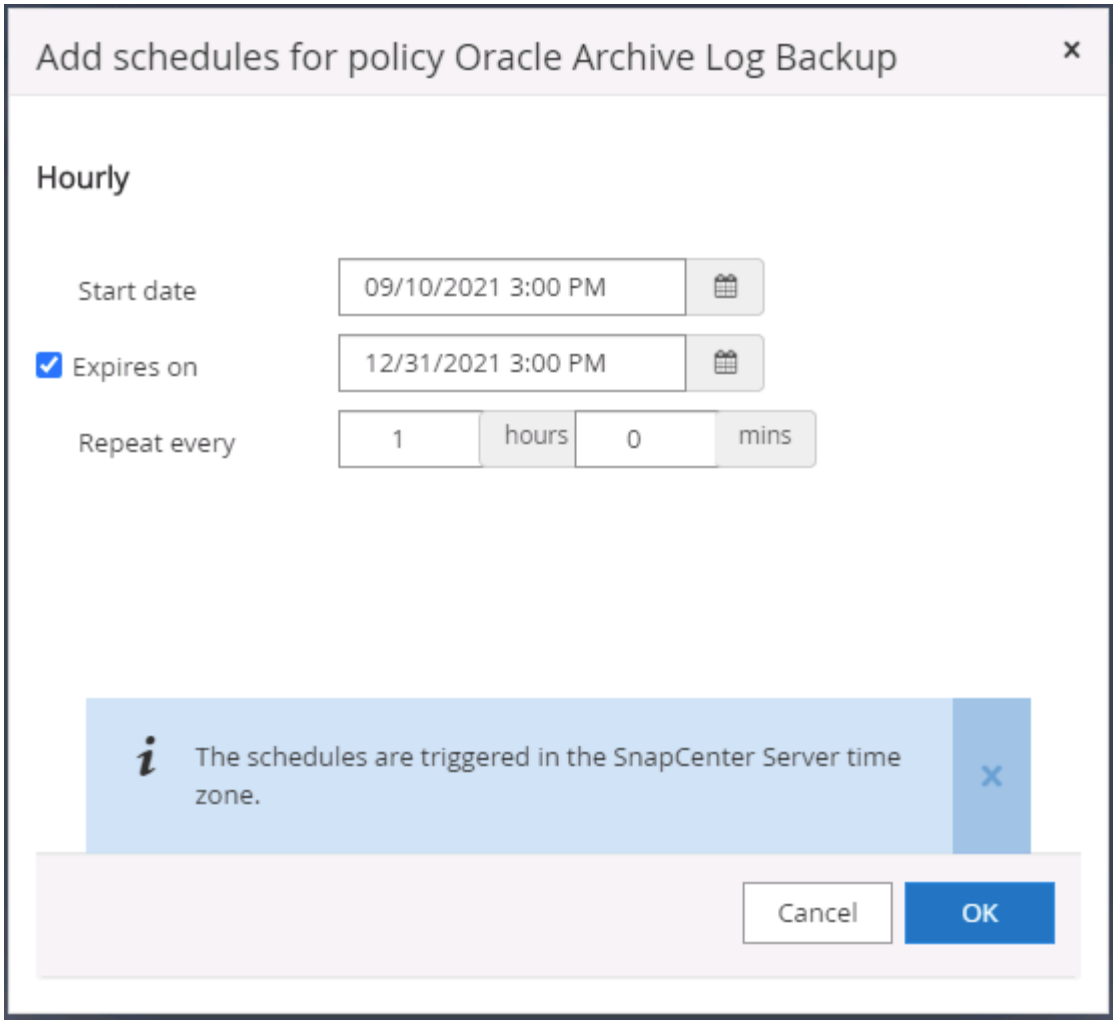
3. Adicione recursos de banco de dados ao grupo de recursos.



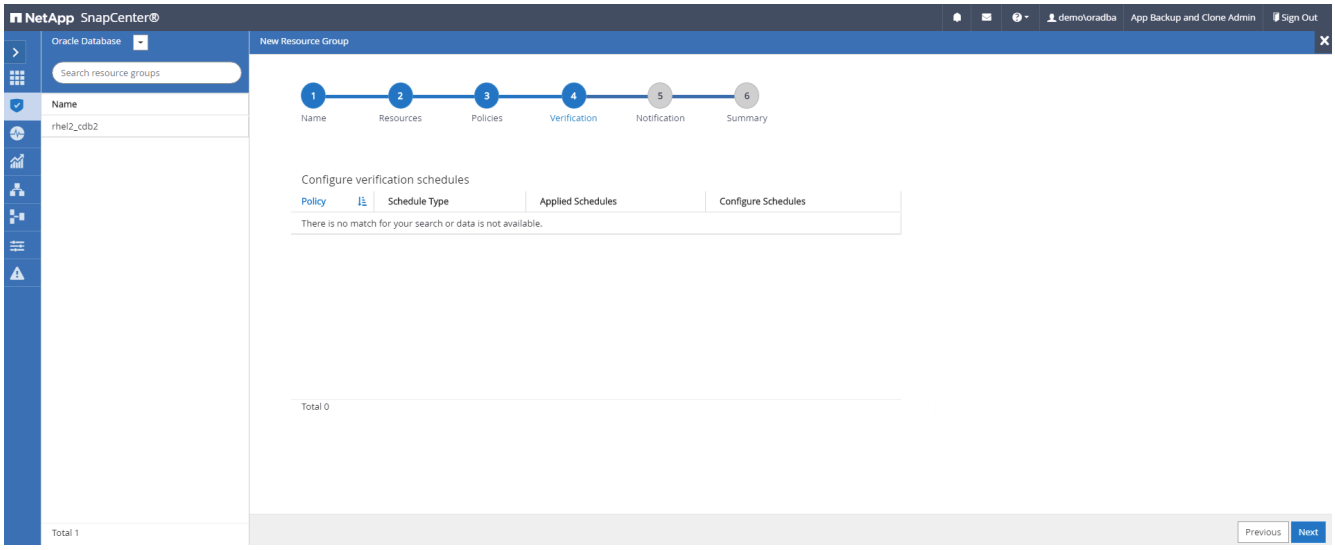
4. Selecione uma política de backup de log criada na seção 7 na lista suspensa.



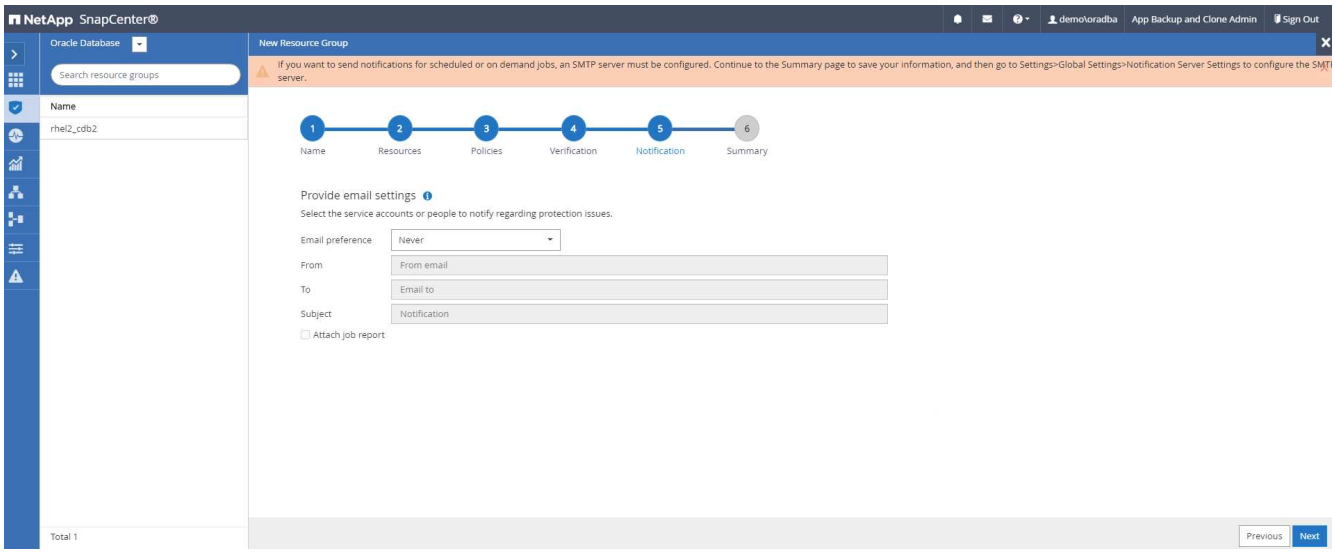
5. Clique no sinal (+) para configurar o agendamento de backup desejado.



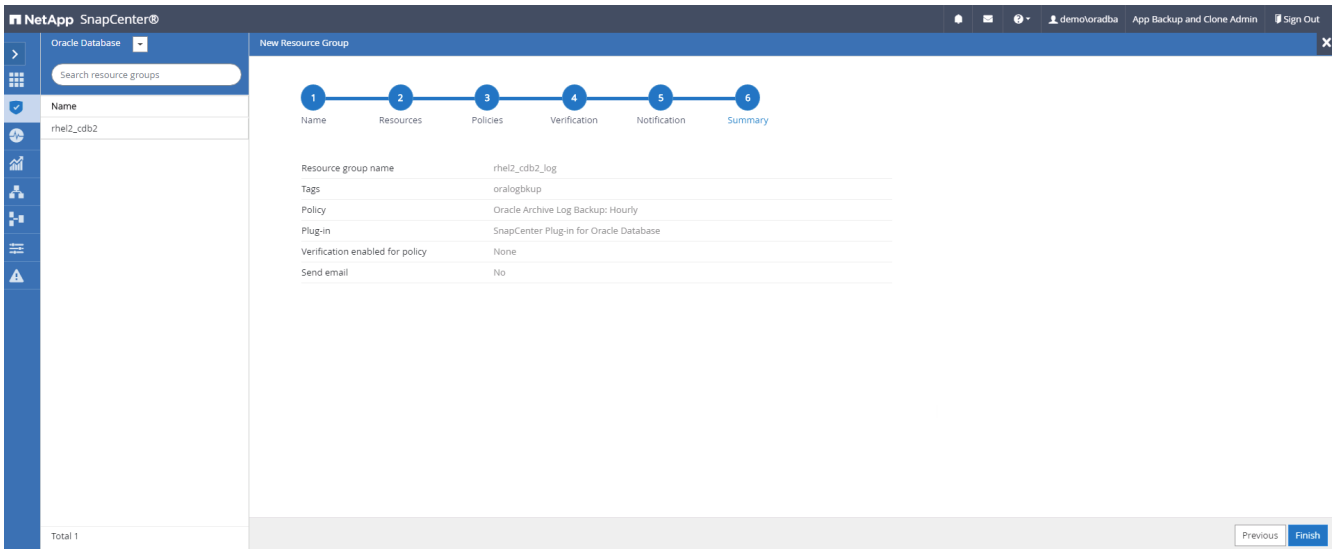
6. Se a verificação de backup estiver configurada, ela será exibida aqui.



7. Configure um servidor SMTP para notificação por email, se desejar.

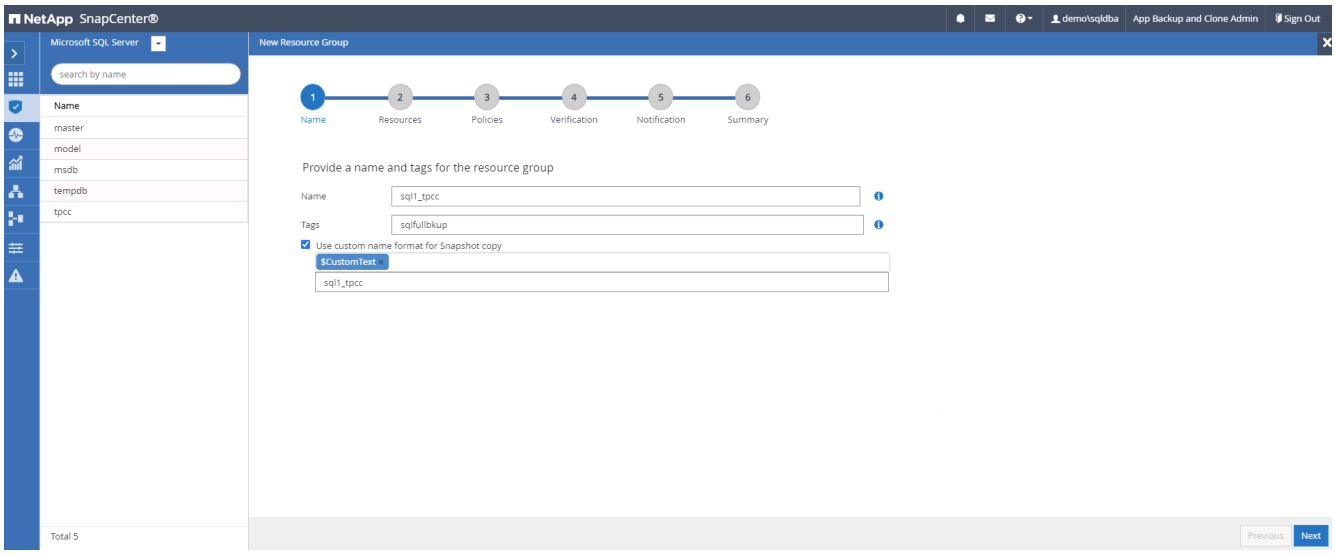


8. Resumo.

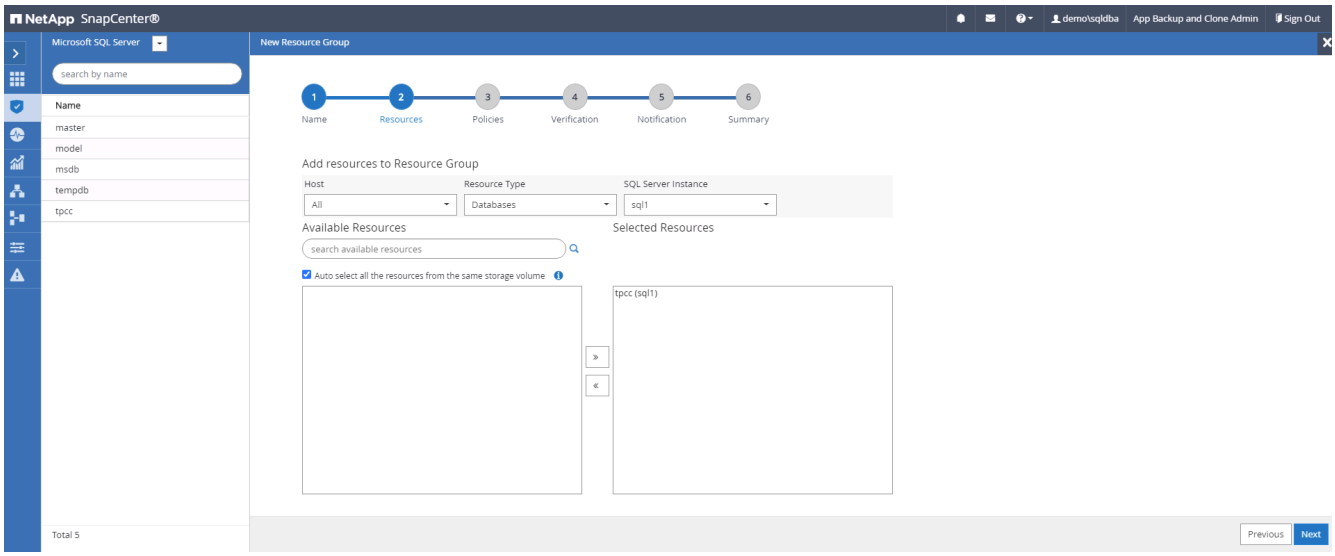


Crie um grupo de recursos para backup completo do SQL Server

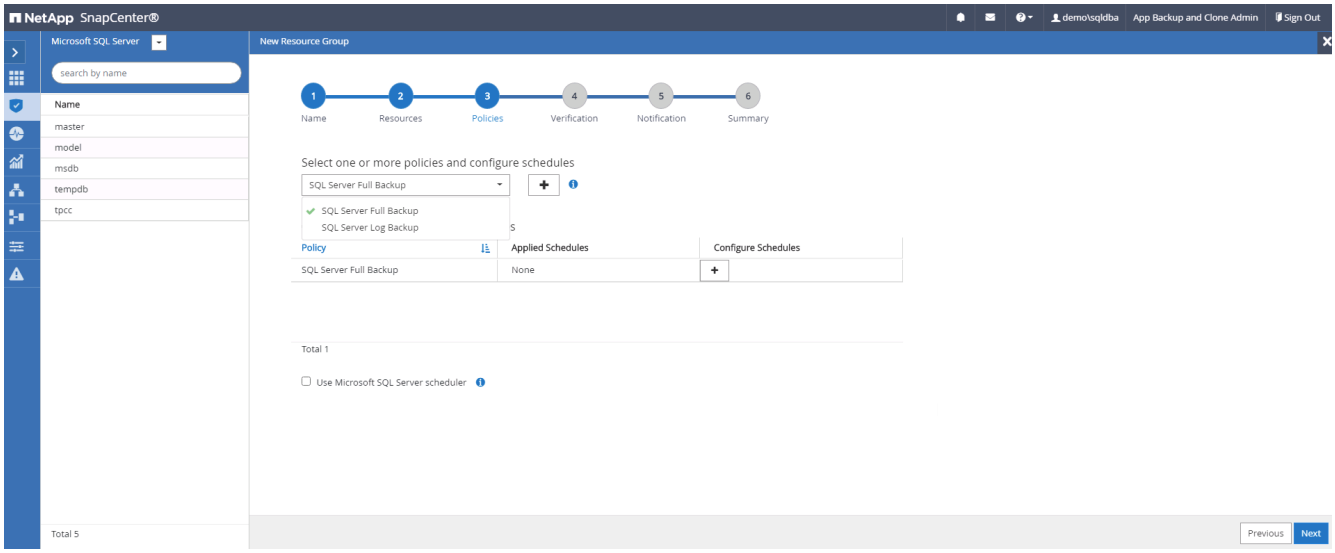
1. Efetue login no SnapCenter com um ID de usuário de gerenciamento de banco de dados e navegue até a guia Recursos. Na lista suspensa Exibir, escolha um Banco de Dados ou Grupo de Recursos para iniciar o fluxo de trabalho de criação do grupo de recursos. Forneça um nome e tags para o grupo de recursos. Você pode definir um formato de nomenclatura para a cópia do Snapshot.



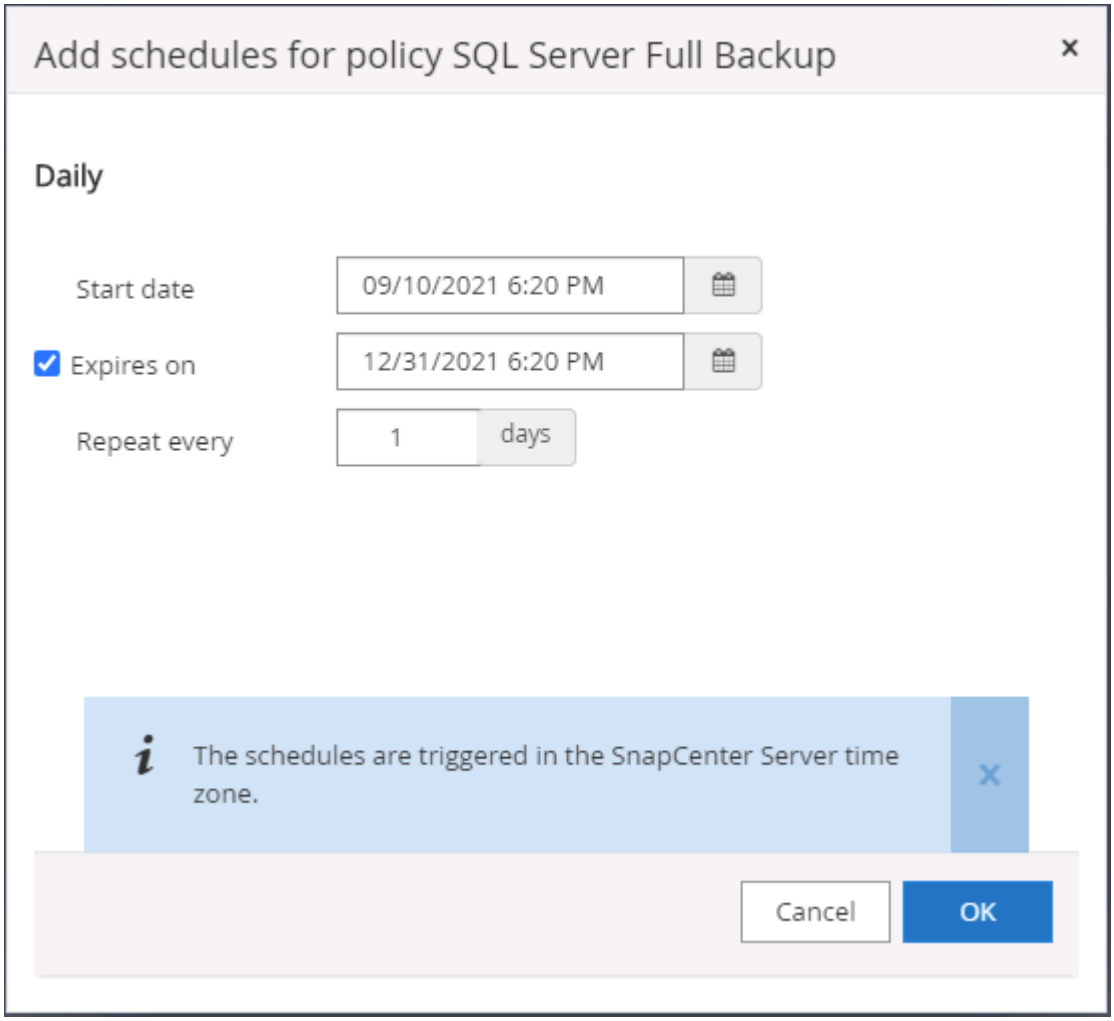
2. Selecione os recursos do banco de dados a serem copiados.



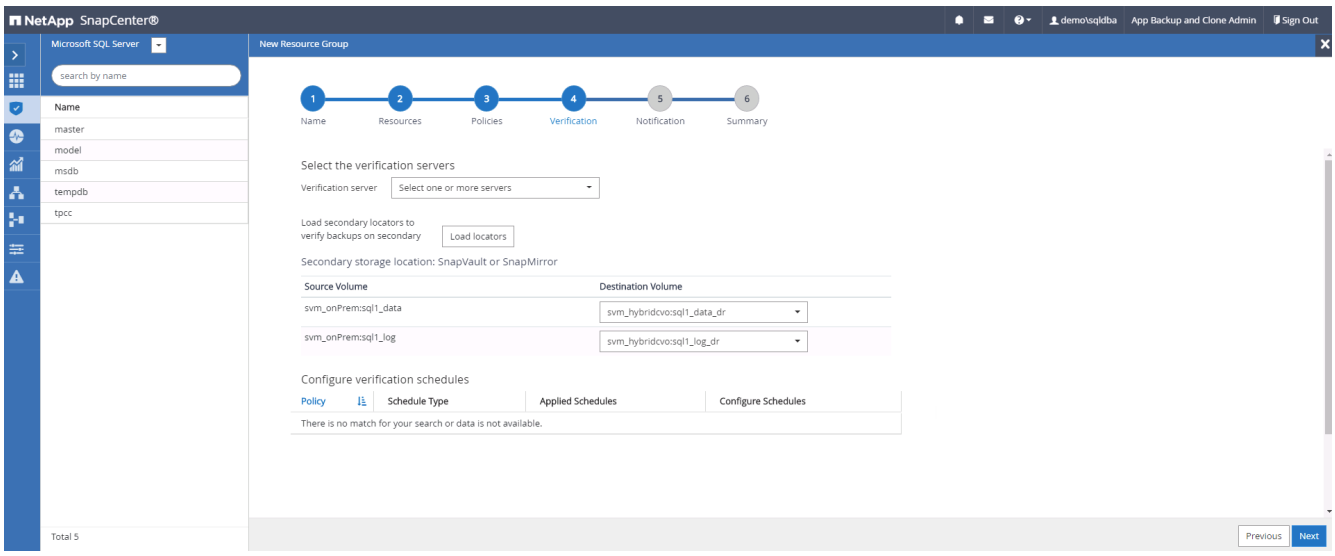
3. Selecione uma política de backup SQL completa criada na seção 7.



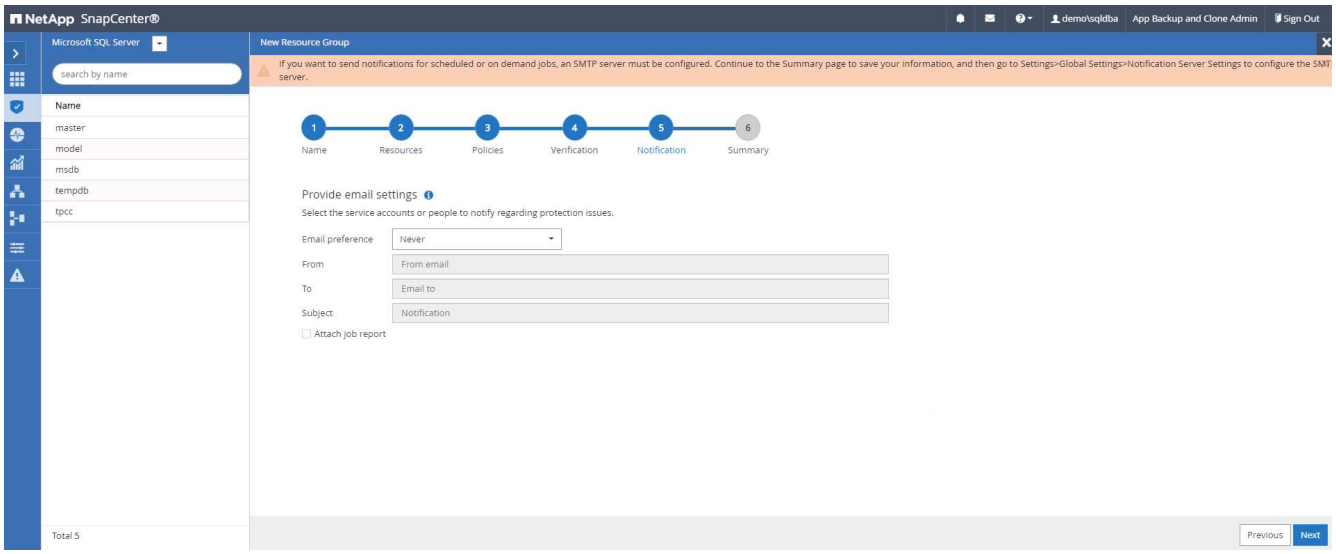
4. Adicione o tempo exato para backups, bem como a frequência.



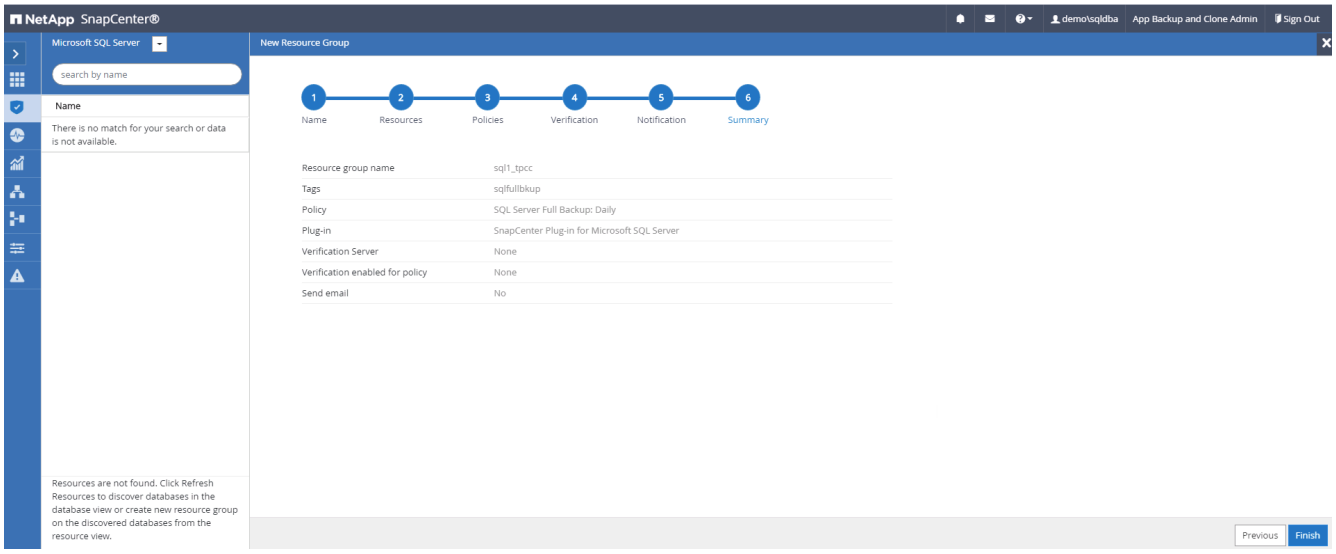
5. Escolha o servidor de verificação para o backup no secundário se a verificação do backup for realizada. Clique em Carregar Localizador para preencher o local de armazenamento secundário.



6. Configure o servidor SMTP para notificação por email, se desejar.

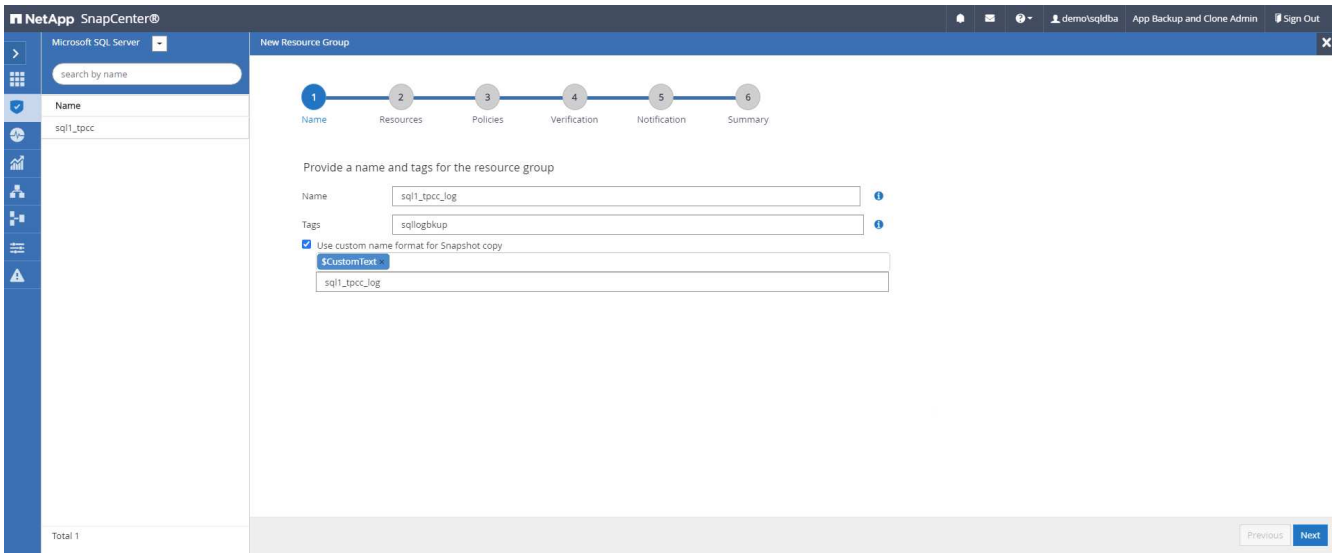


7. Resumo.

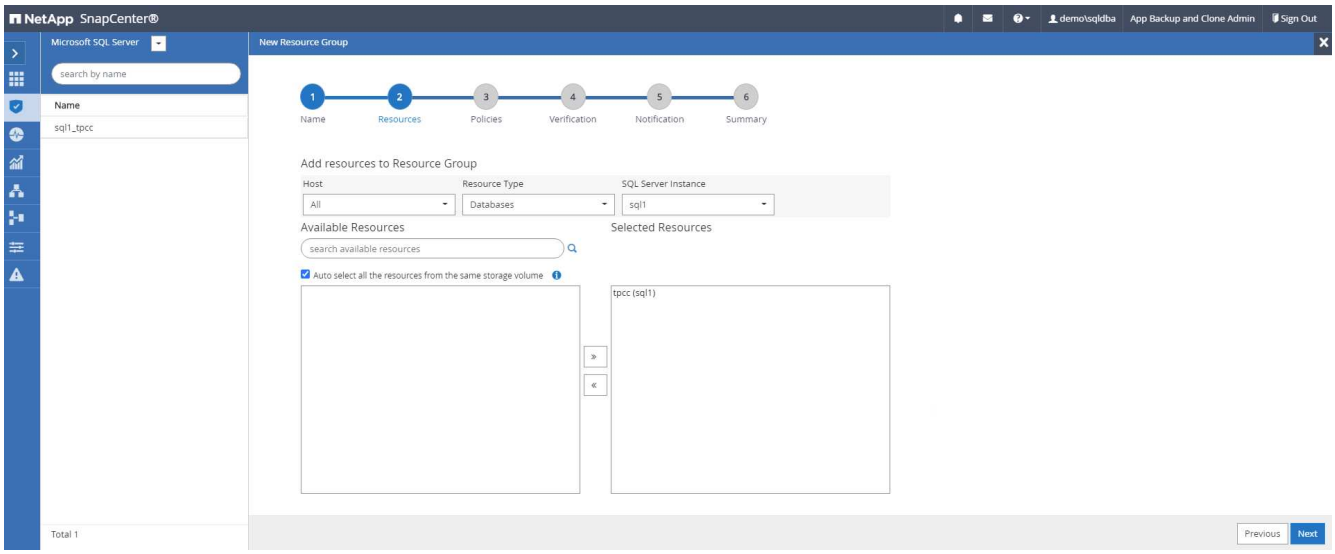


Crie um grupo de recursos para backup de log do SQL Server

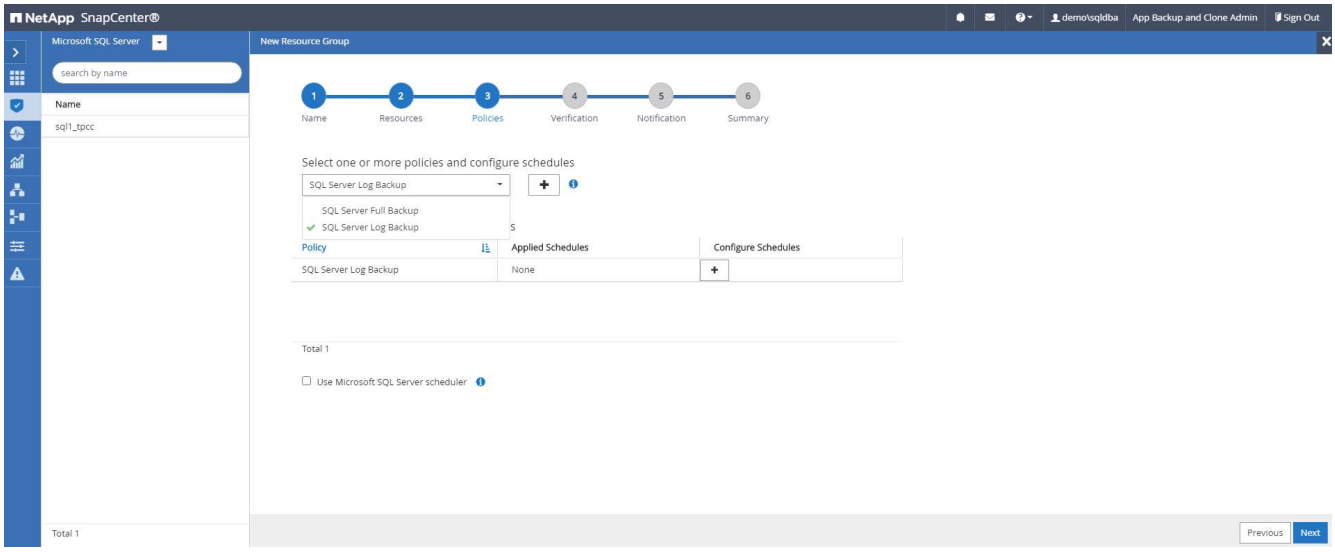
1. Efetue login no SnapCenter com um ID de usuário de gerenciamento de banco de dados e navegue até a guia Recursos. Na lista suspensa Exibir, escolha um Banco de Dados ou Grupo de Recursos para iniciar o fluxo de trabalho de criação do grupo de recursos. Forneça o nome e as tags para o grupo de recursos. Você pode definir um formato de nomenclatura para a cópia do Snapshot.



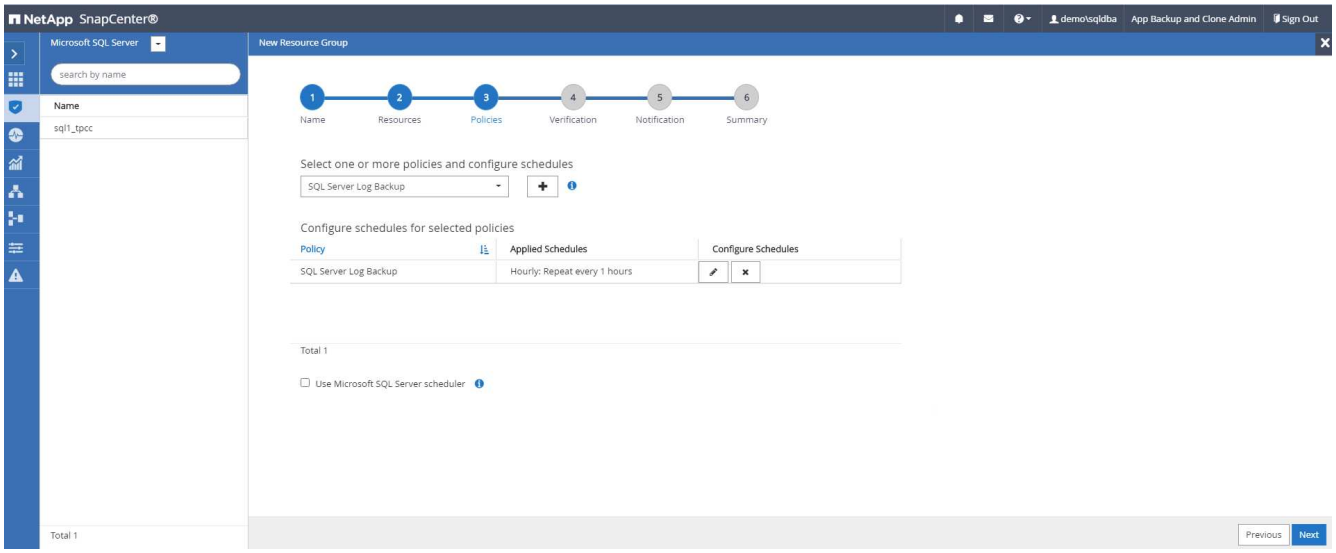
2. Selecione os recursos do banco de dados a serem copiados.



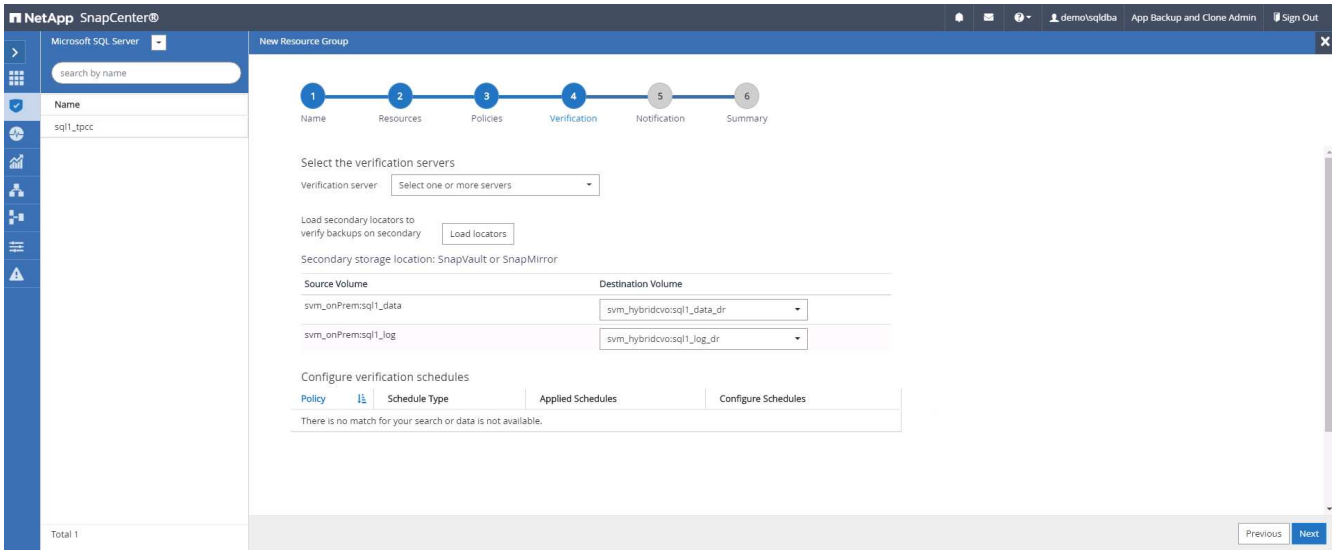
3. Selecione uma política de backup de log SQL criada na seção 7.



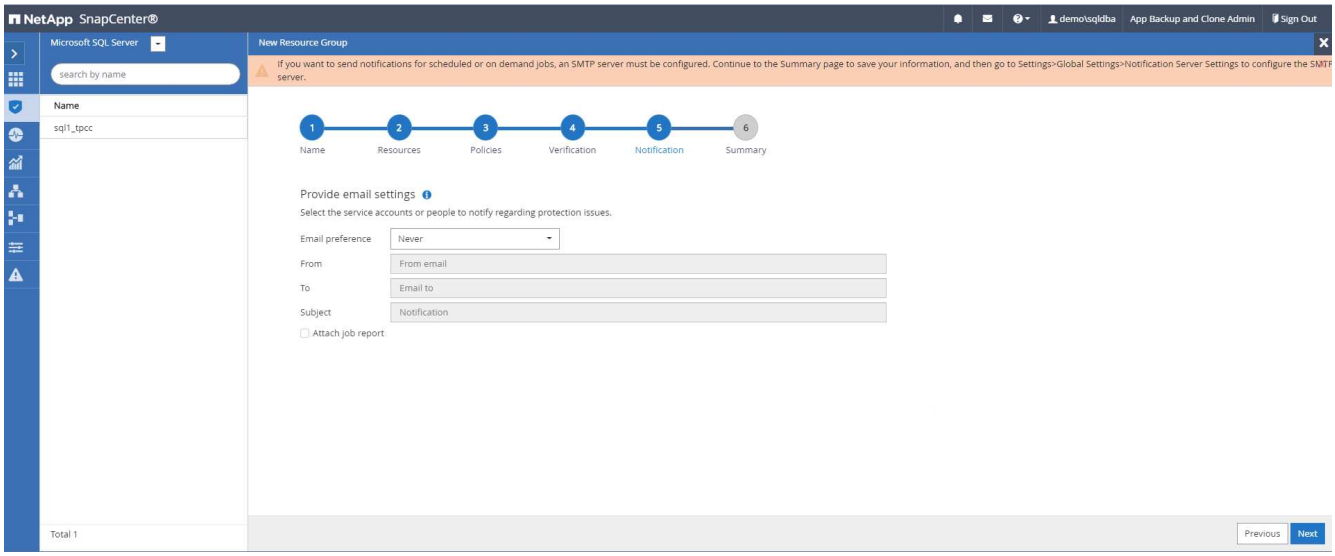
4. Adicione o tempo exato para o backup, bem como a frequência.



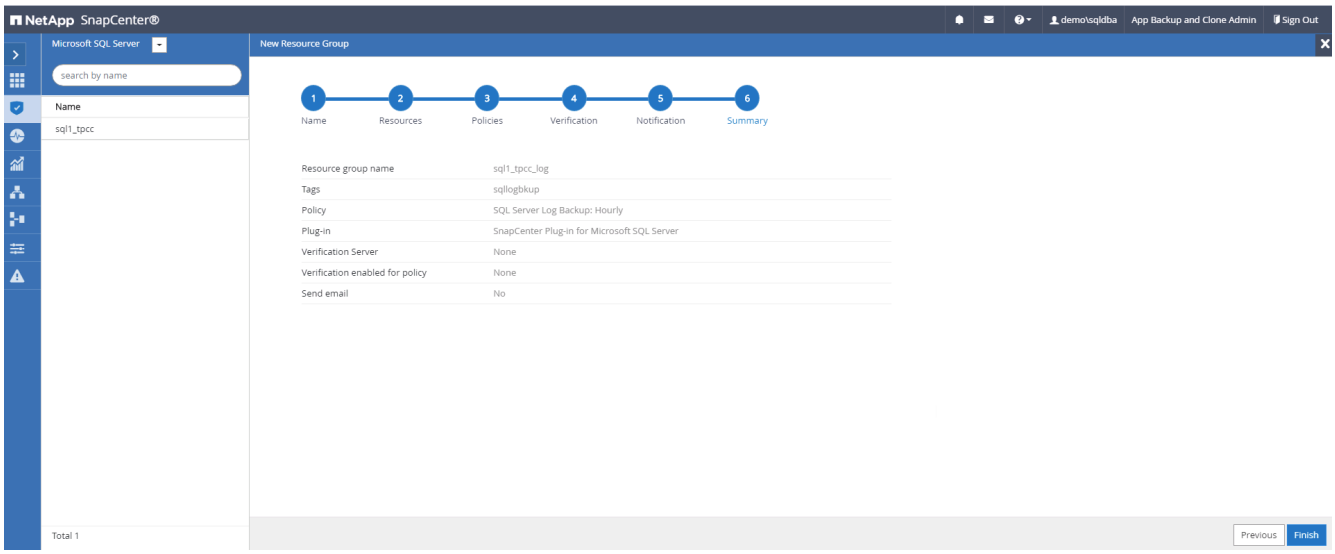
5. Escolha o servidor de verificação para o backup no secundário se a verificação do backup for realizada. Clique no Localizador de carga para preencher o local de armazenamento secundário.



6. Configure o servidor SMTP para notificação por email, se desejar.

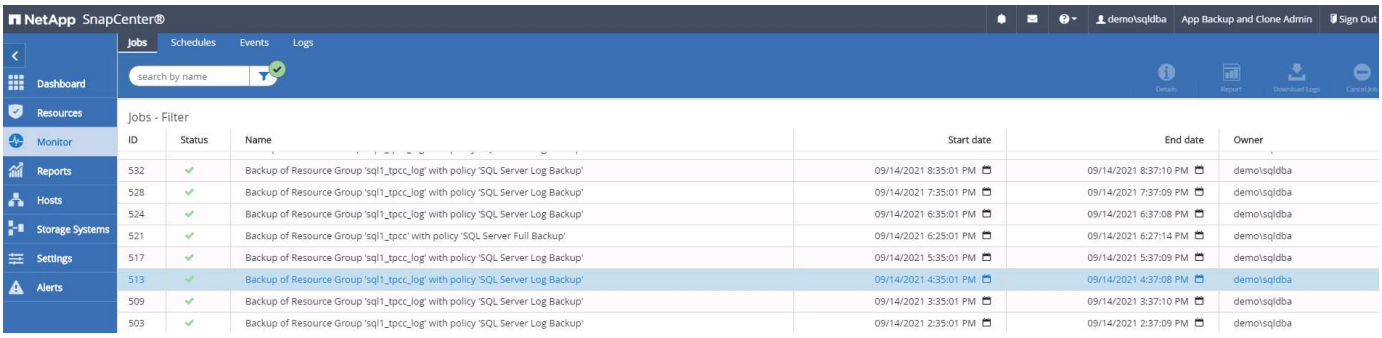


7. Resumo.



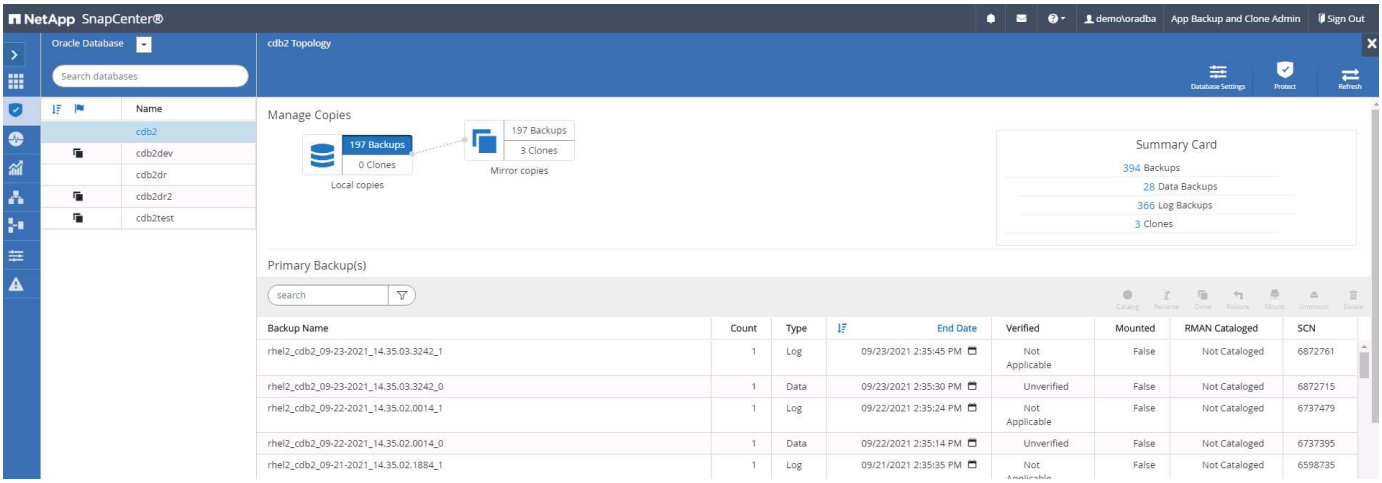
9. Validar backup

Depois que os grupos de recursos de backup do banco de dados são criados para proteger os recursos do banco de dados, as tarefas de backup são executadas de acordo com o cronograma predefinido. Verifique o status de execução do trabalho na guia Monitor.



Acesse a guia Recursos, clique no nome do banco de dados para visualizar detalhes do backup do banco de dados e alterne entre cópias locais e cópias espelhadas para verificar se os backups de instantâneos são

replicados para um local secundário na nuvem pública.



Neste ponto, as cópias de backup do banco de dados na nuvem estão prontas para clonagem para executar processos de desenvolvimento/teste ou para recuperação de desastres no caso de uma falha primária.

Introdução à nuvem pública da AWS

Esta seção descreve o processo de implantação do Cloud Manager e do Cloud Volumes ONTAP na AWS.

Nuvem pública da AWS

> Para facilitar o acompanhamento, criamos este documento com base em uma implantação na AWS. No entanto, o processo é muito semelhante para Azure e GCP.

1. Verificação pré-voo

Antes da implantação, certifique-se de que a infraestrutura esteja pronta para permitir a implantação no próximo estágio. Isso inclui o seguinte:

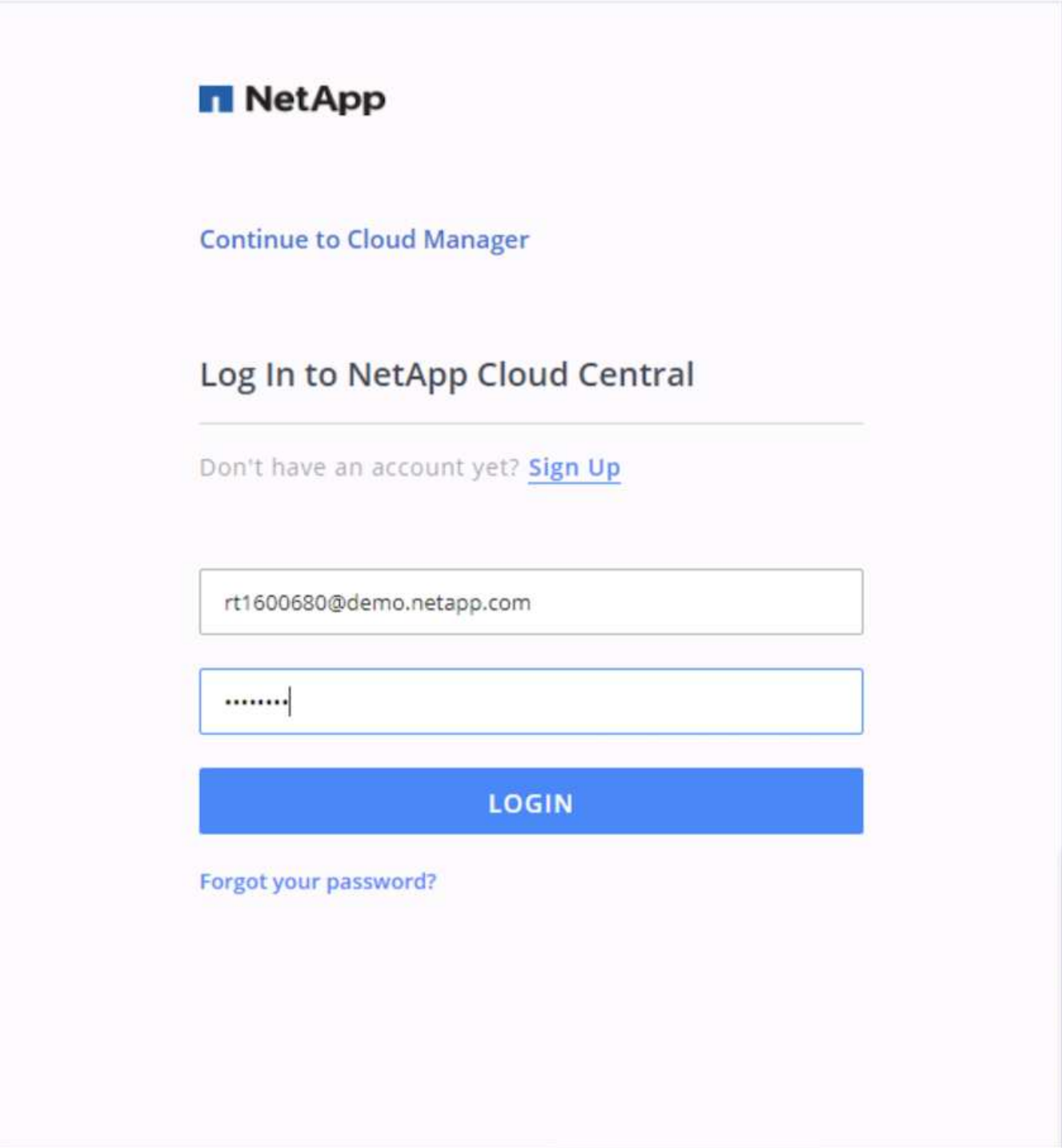
- Conta AWS
- VPC na região de sua escolha
- Sub-rede com acesso à internet pública
- Permissões para adicionar funções do IAM à sua conta da AWS
- Uma chave secreta e uma chave de acesso para seu usuário AWS

2. Etapas para implantar o Cloud Manager e o Cloud Volumes ONTAP na AWS

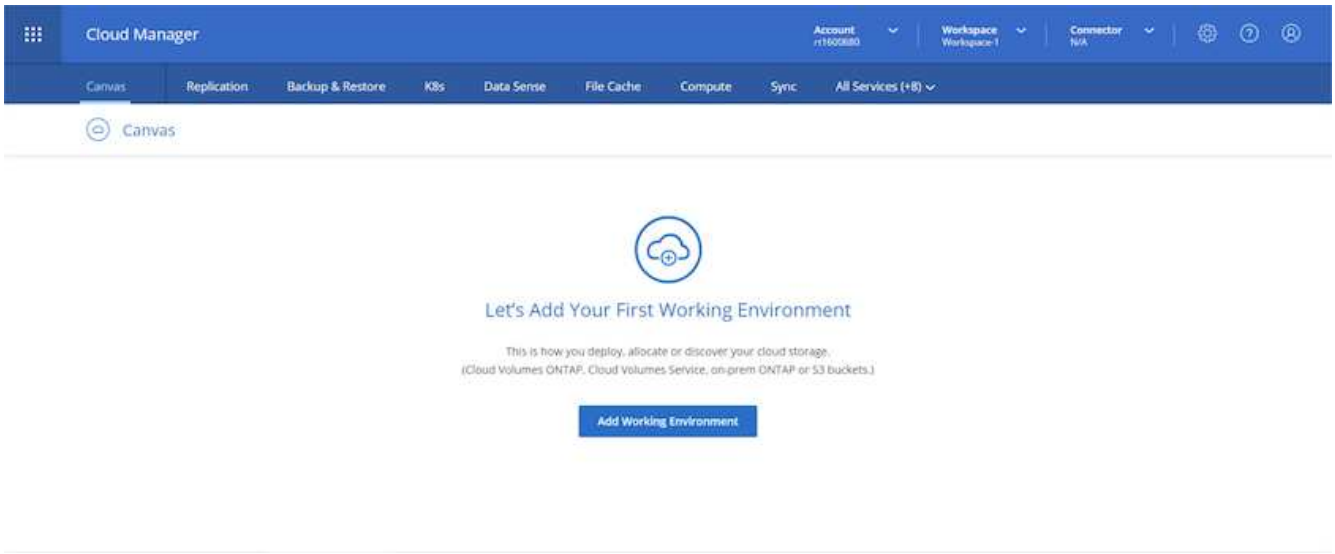
> Há muitos métodos para implantar o Cloud Manager e o Cloud Volumes ONTAP; este método é o mais simples, mas requer mais permissões. Se este método não for apropriado para o seu ambiente AWS, consulte o "Documentação do NetApp Cloud" .

Implantar o conector do Cloud Manager

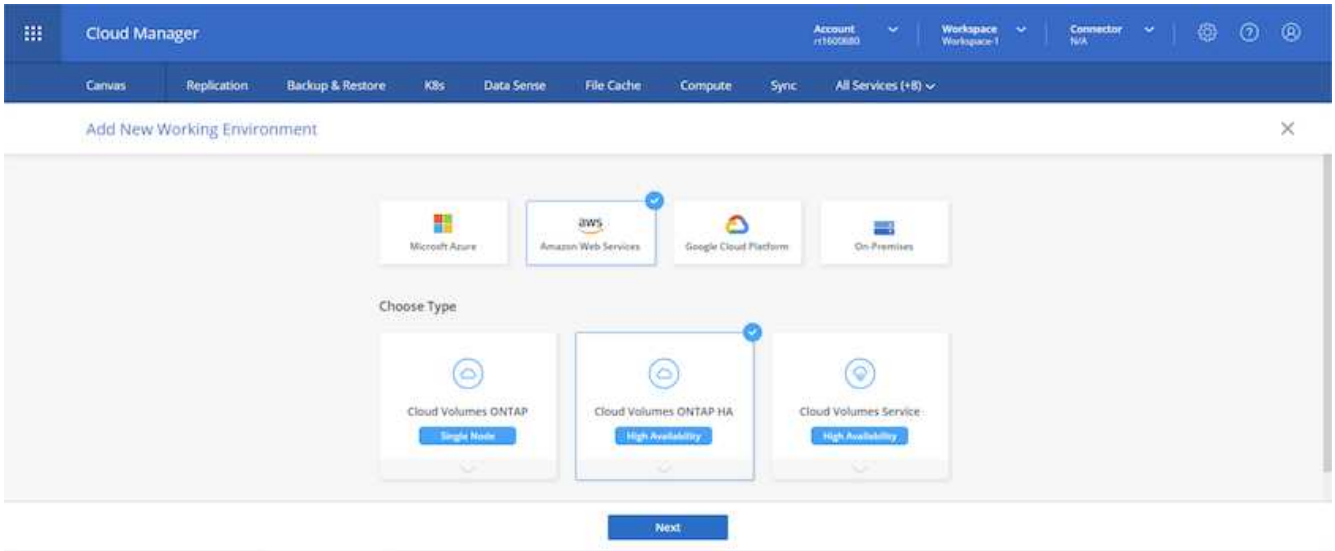
1. Navegar para "NetApp BlueXP" e faça login ou registre-se.



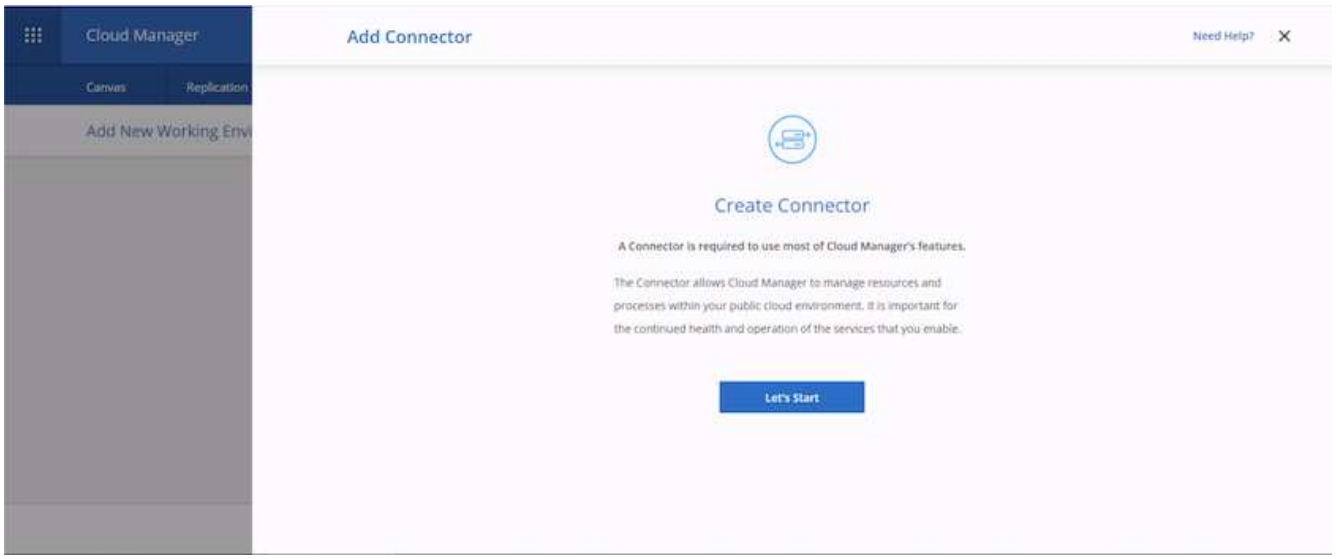
2. Após efetuar login, você será levado ao Canvas.



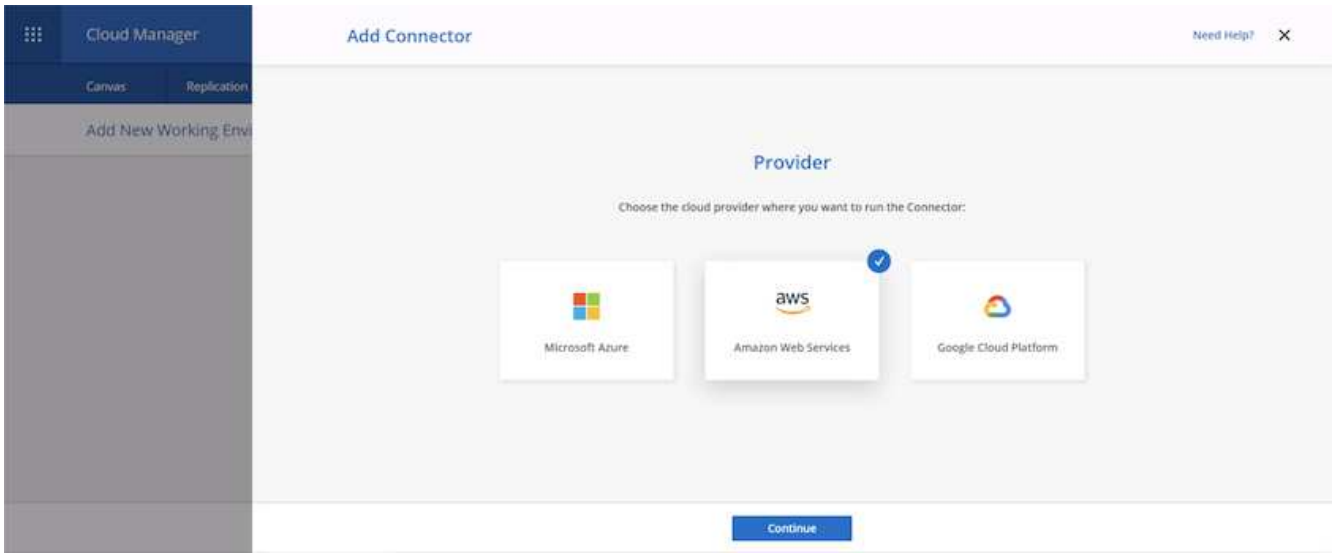
3. Clique em "Adicionar ambiente de trabalho" e escolha Cloud Volumes ONTAP na AWS. Aqui, você também escolhe se deseja implantar um sistema de nó único ou um par de alta disponibilidade. Optei por implantar um par de alta disponibilidade.



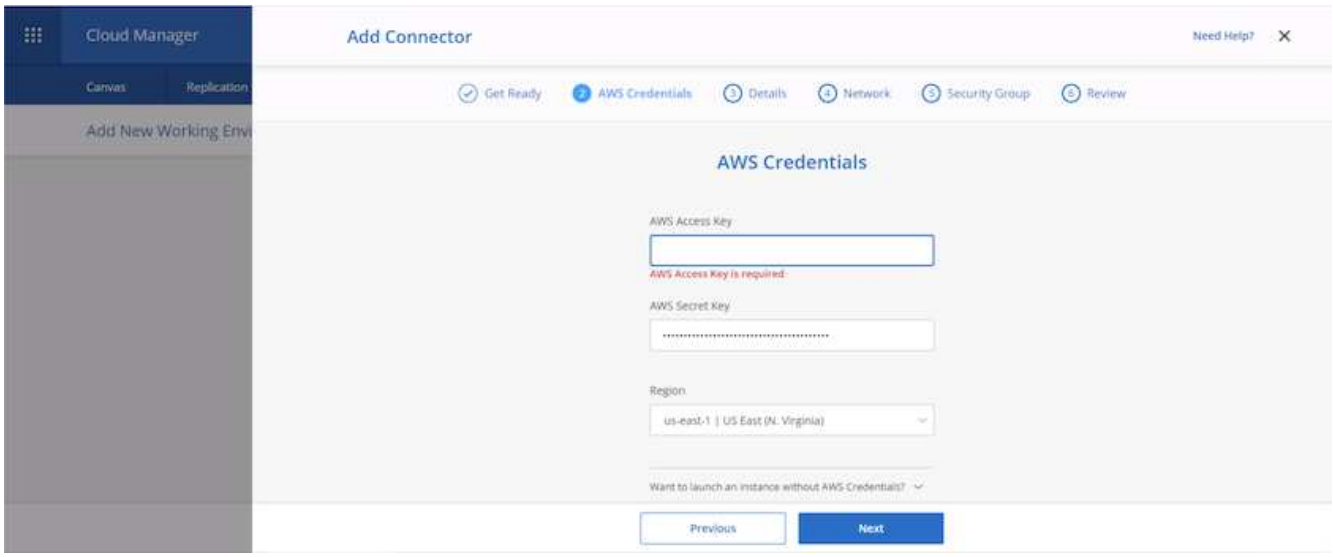
4. Se nenhum conector tiver sido criado, um pop-up aparecerá solicitando que você crie um conector.



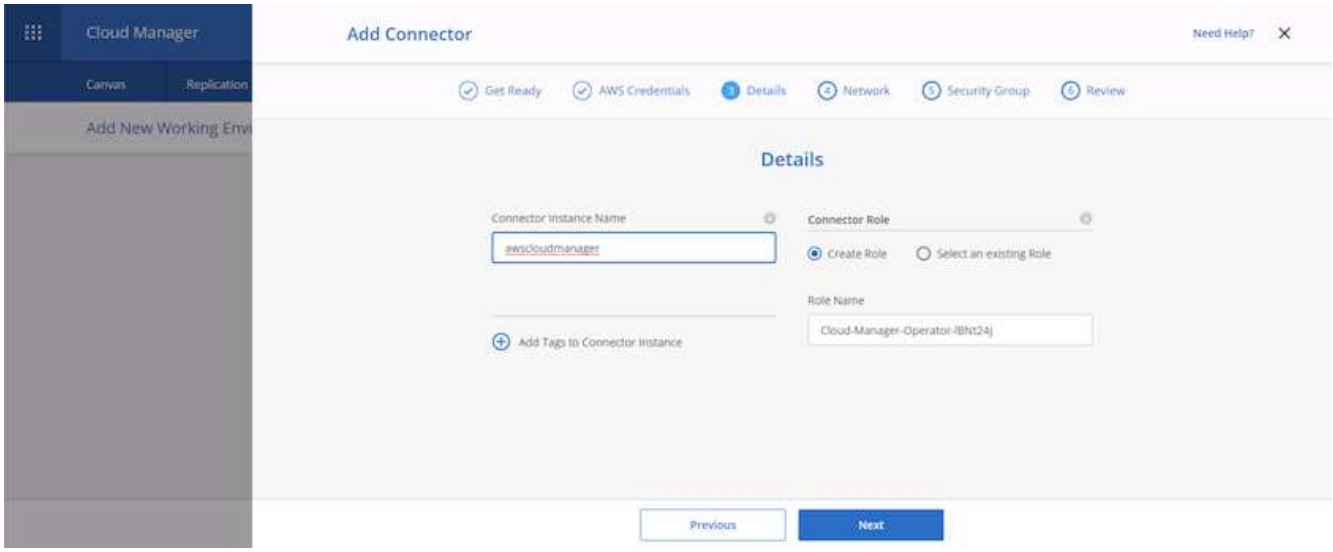
5. Clique em Vamos começar e depois escolha AWS.



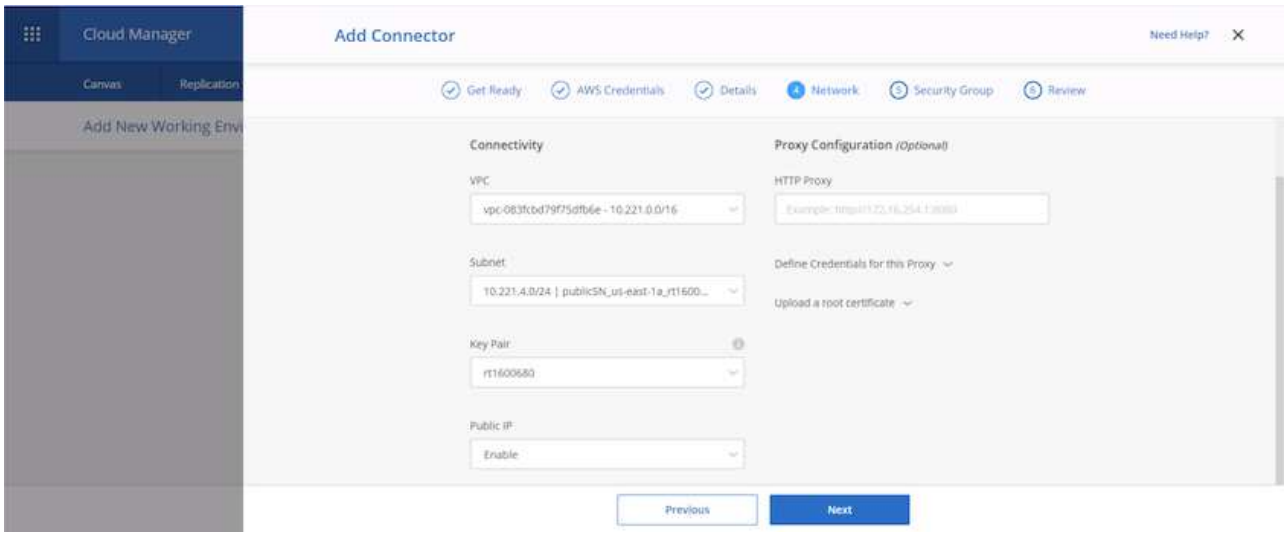
6. Digite sua chave secreta e chave de acesso. Certifique-se de que seu usuário tenha as permissões corretas descritas no "Página de políticas da NetApp" .



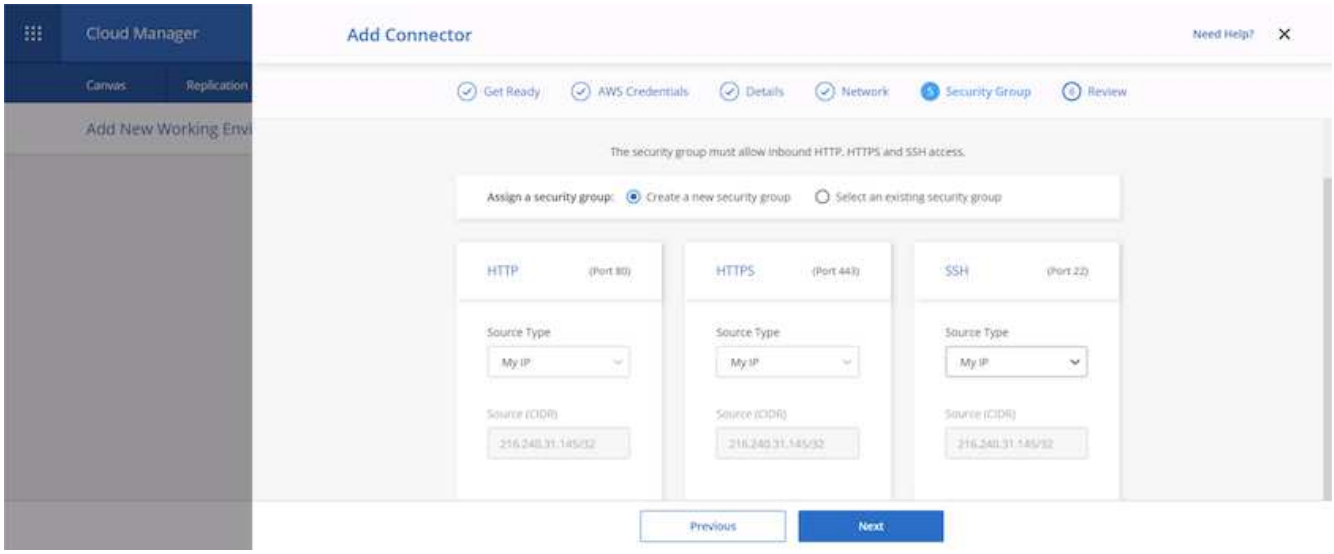
7. Dê um nome ao conector e use uma função predefinida conforme descrito na "Página de políticas da NetApp" ou peça ao Cloud Manager para criar a função para você.



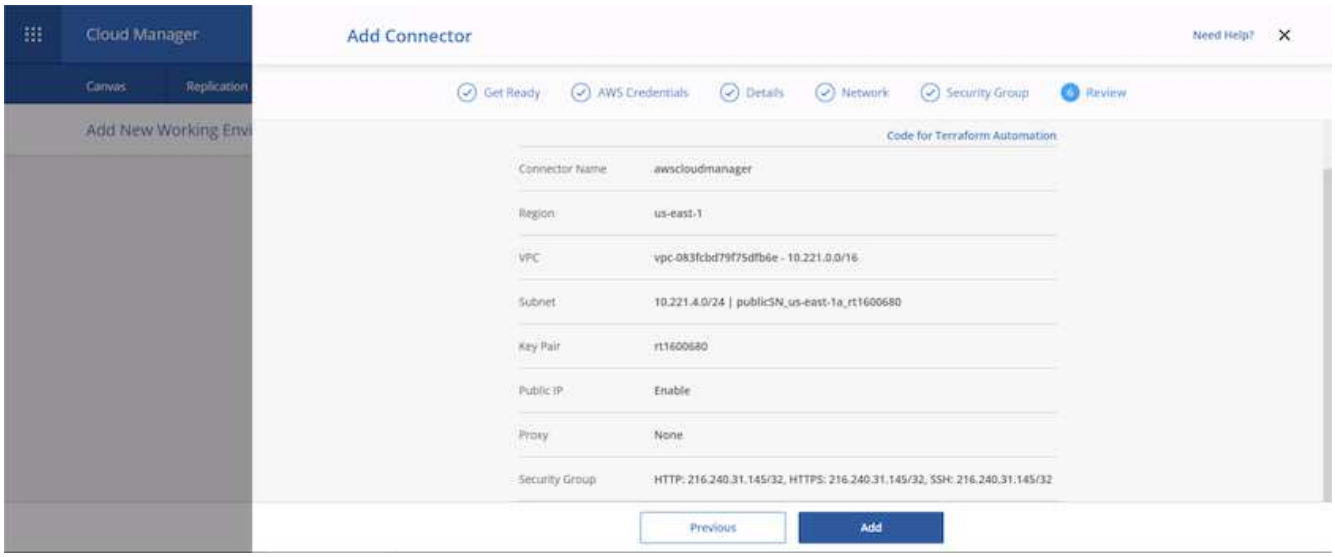
8. Forneça as informações de rede necessárias para implantar o conector. Verifique se o acesso de saída à Internet está habilitado por:
   a. Atribuindo ao conector um endereço IP público
   b. Fornecendo ao conector um proxy para trabalhar
   c. Fornecendo ao conector uma rota para a Internet pública por meio de um Gateway de Internet



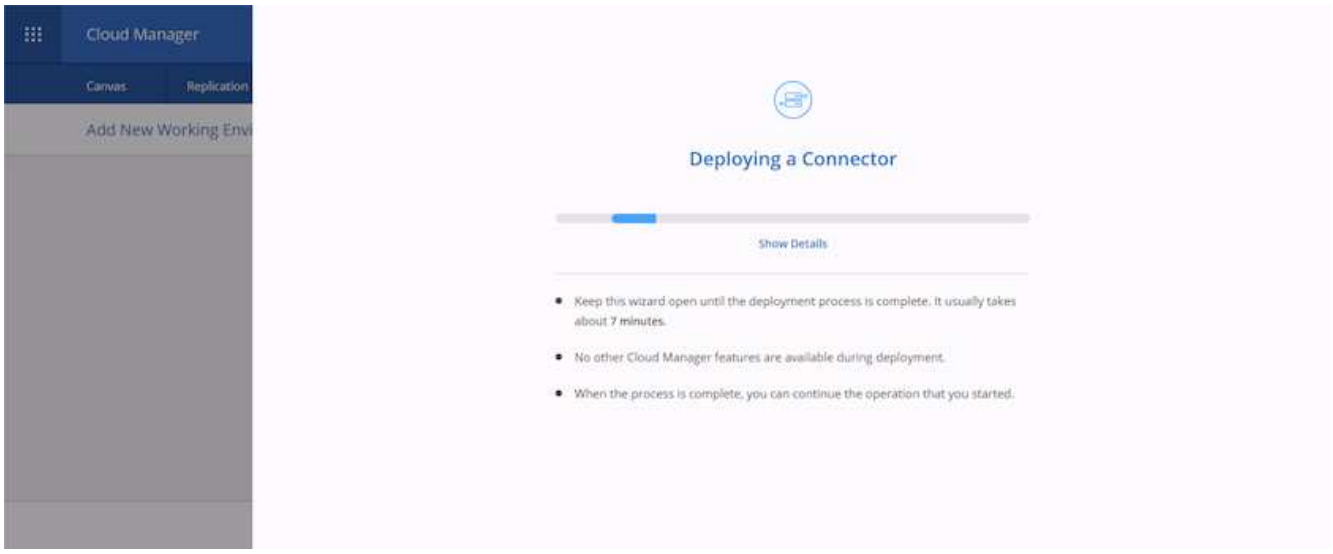
9. Forneça comunicação com o conector via SSH, HTTP e HTTPs, fornecendo um grupo de segurança ou criando um novo grupo de segurança. Habilitei o acesso ao conector somente a partir do meu endereço IP.



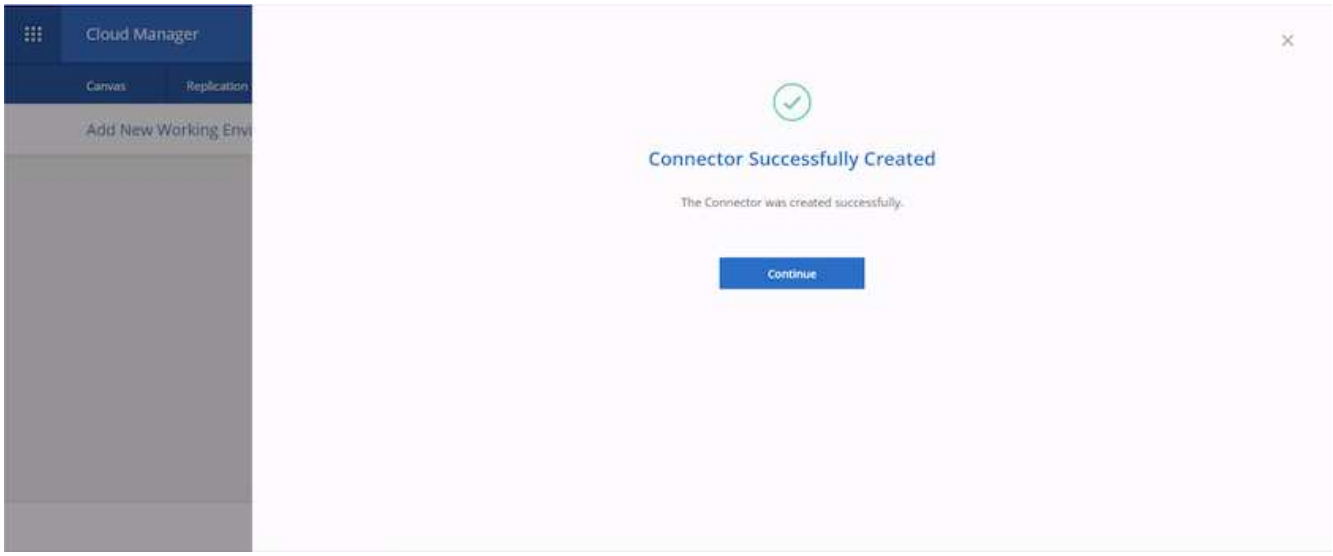
10. Revise as informações na página de resumo e clique em Adicionar para implantar o conector.



11. O conector agora é implantado usando uma pilha de formação de nuvem. Você pode monitorar o progresso pelo Cloud Manager ou pela AWS.

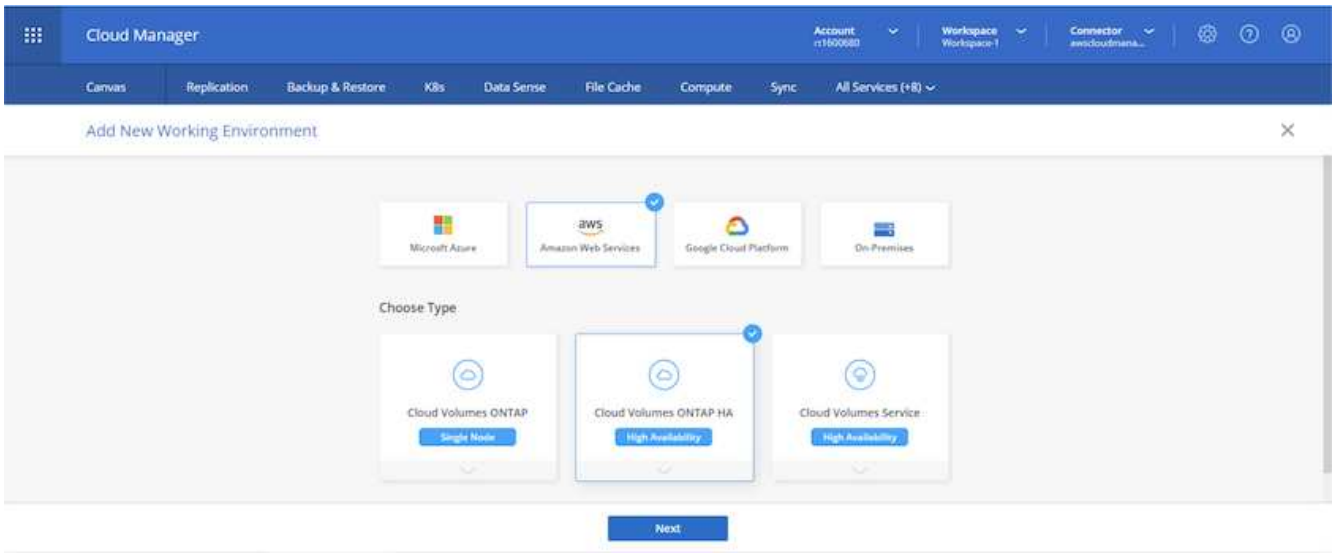


12. Quando a implantação estiver concluída, uma página de sucesso será exibida.

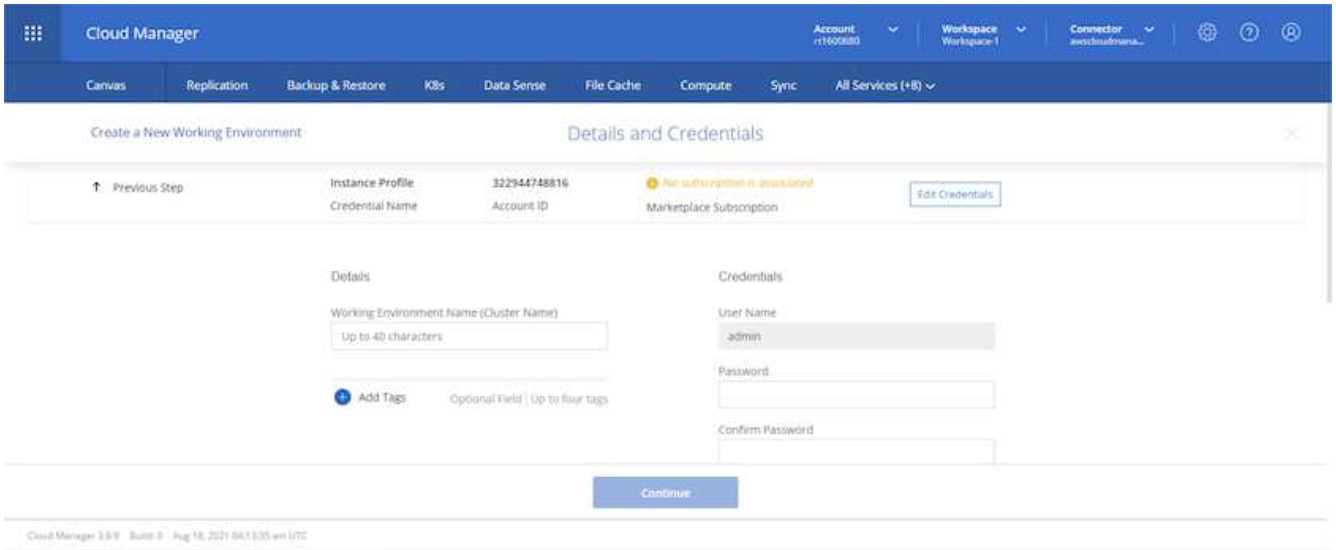


Implantar Cloud Volumes ONTAP

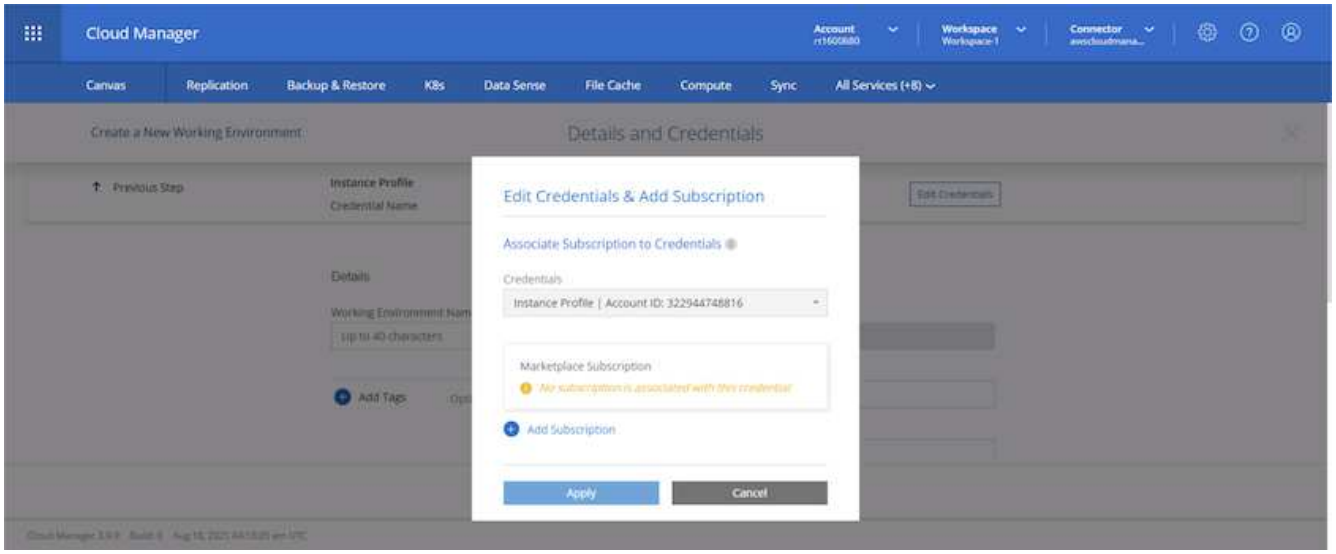
1. Selecione AWS e o tipo de implantação com base em seus requisitos.



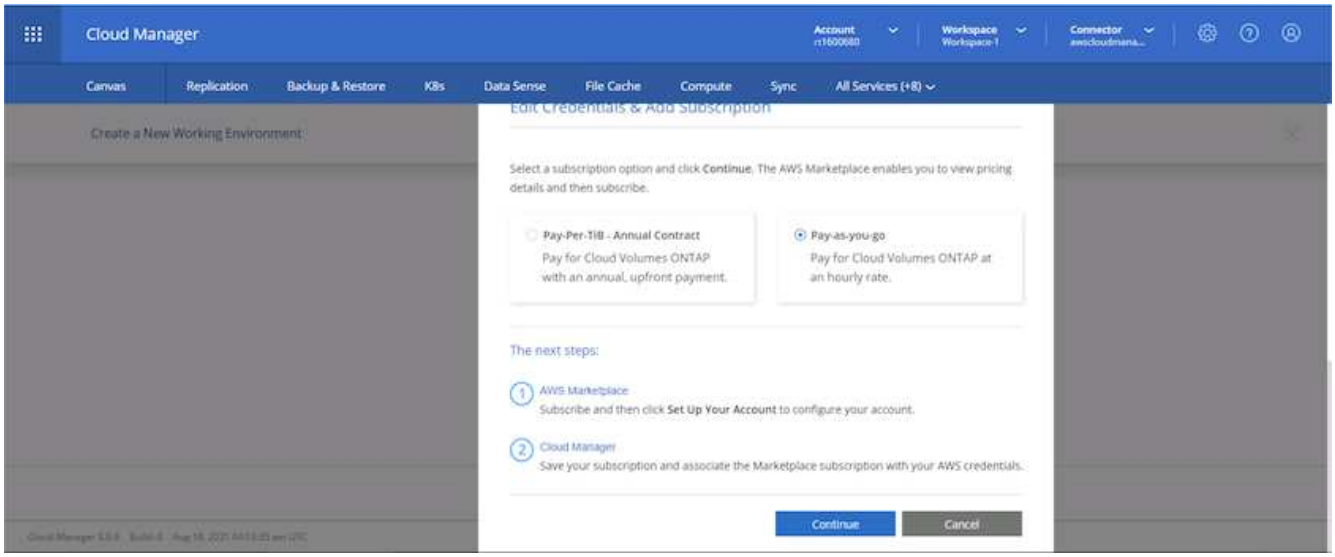
2. Se nenhuma assinatura foi atribuída e você deseja comprar com o PAYGO, escolha Editar credenciais.



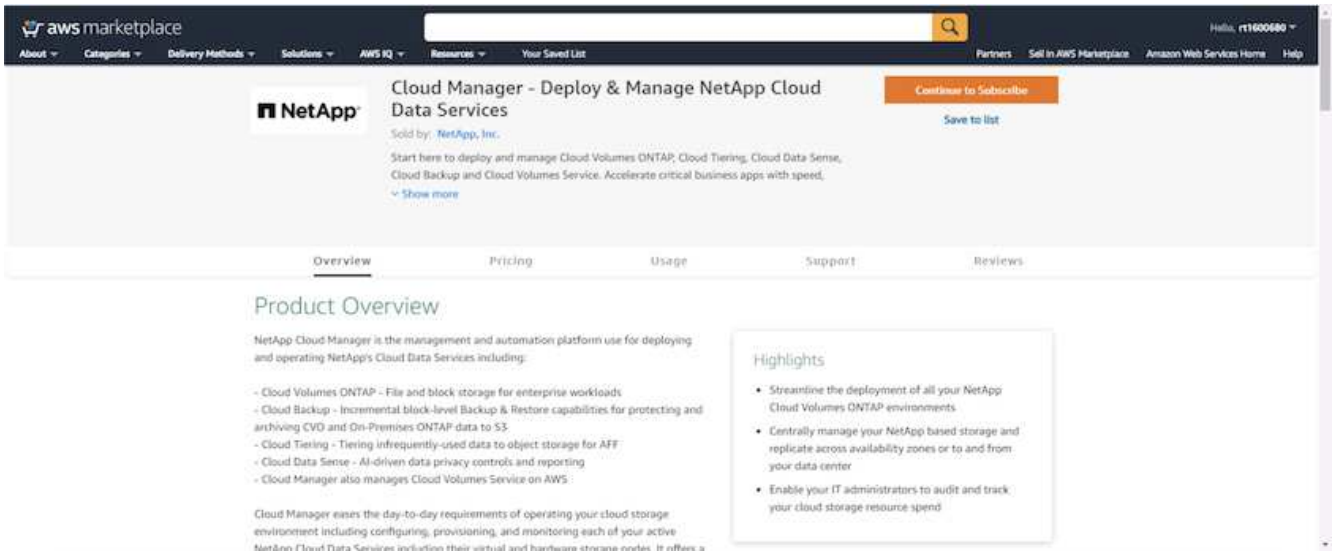
3. Selecione Adicionar assinatura.



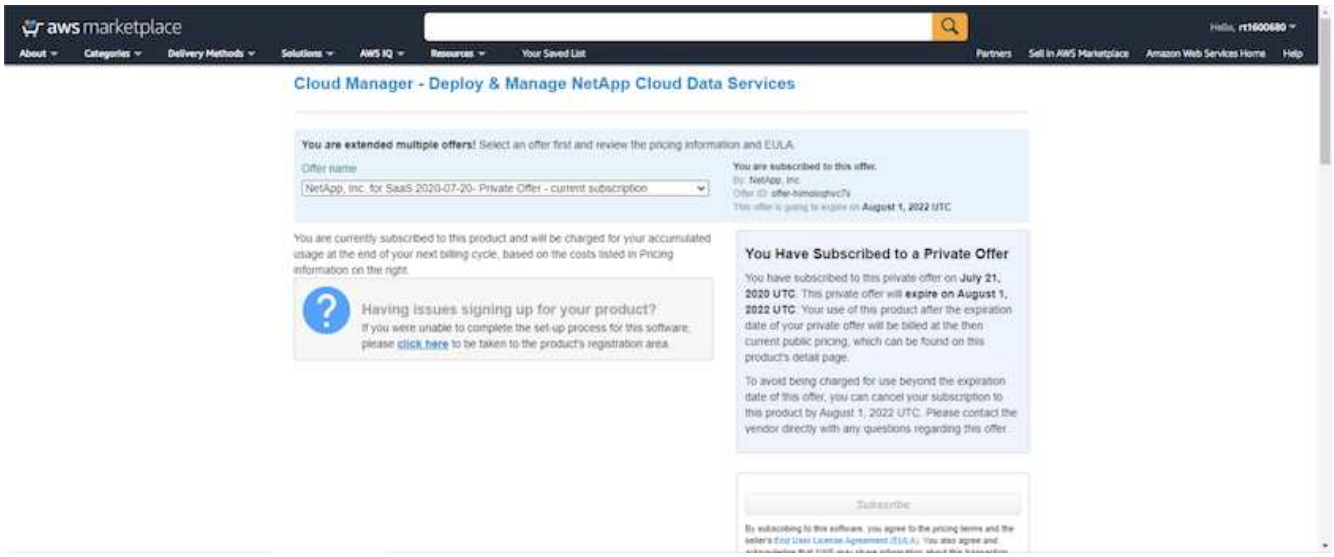
4. Selecione o tipo de contrato que deseja assinar. Eu escolhi o pagamento conforme o uso.



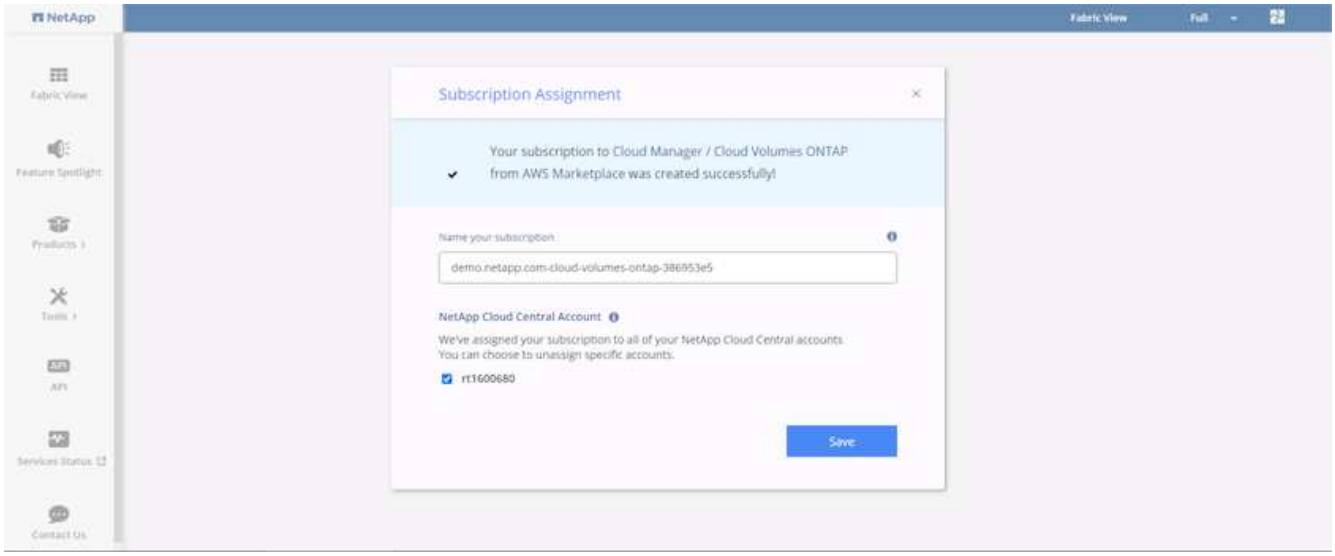
5. Você será redirecionado para a AWS; escolha Continuar para assinar.



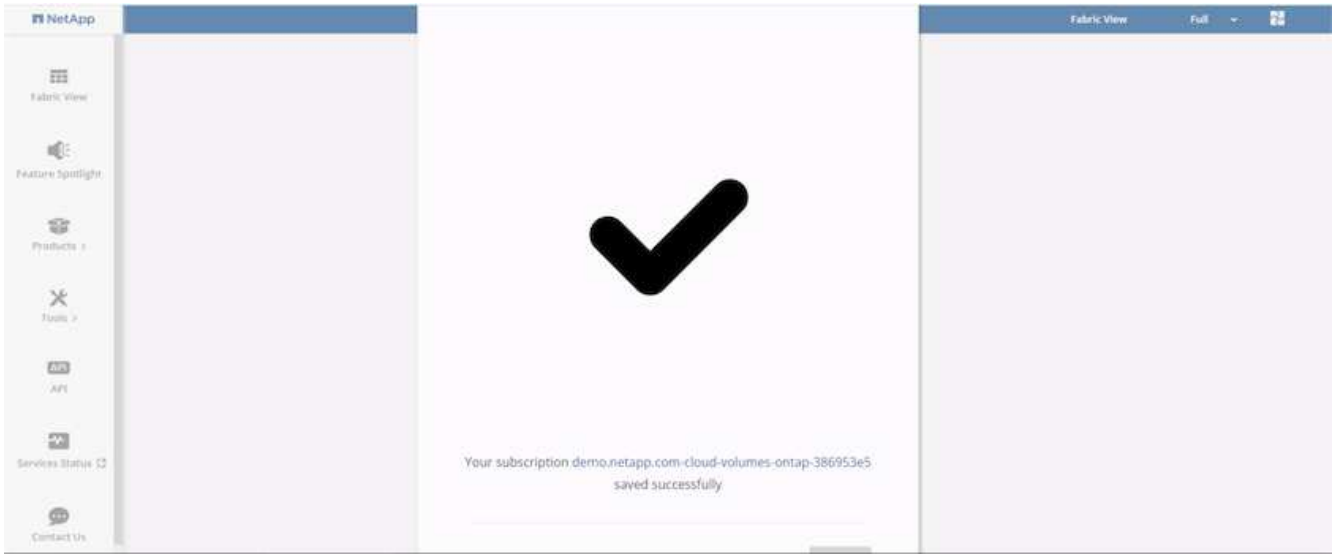
6. Assine e você será redirecionado de volta ao NetApp Cloud Central. Se você já se inscreveu e não for redirecionado, escolha o link "Clique aqui".



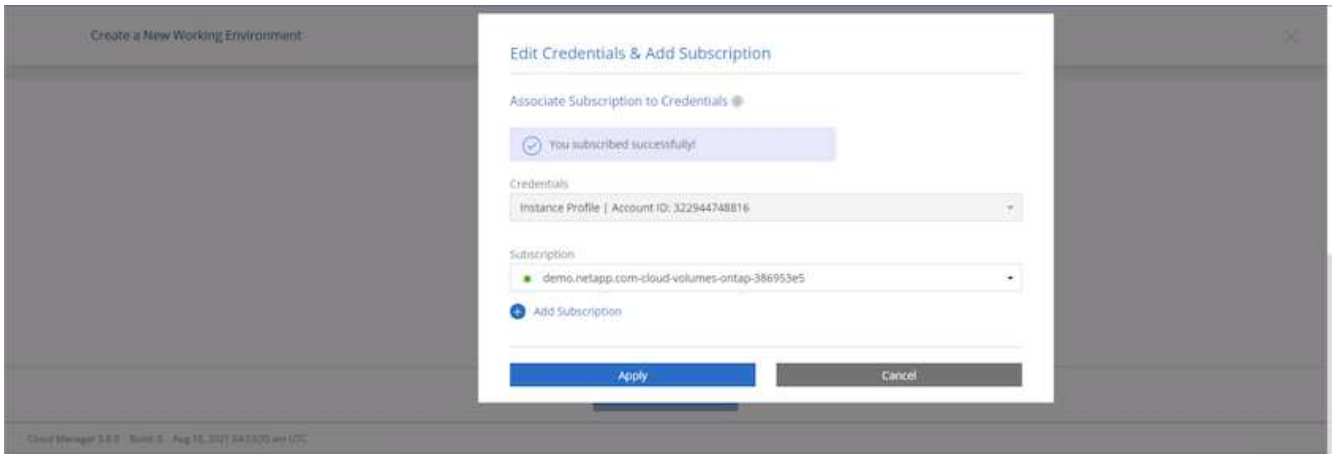
7. Você será redirecionado para o Cloud Central, onde deverá nomear sua assinatura e atribuí-la à sua conta do Cloud Central.



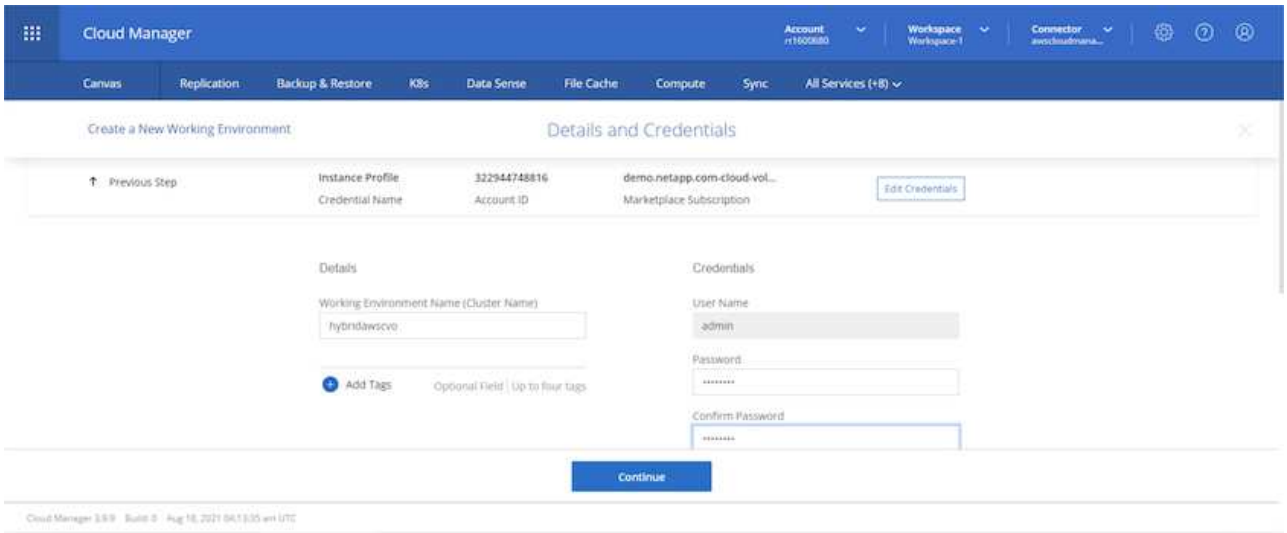
8. Quando bem-sucedido, uma página de marca de seleção é exibida. Navegue de volta para a aba Gerenciador de Nuvem.



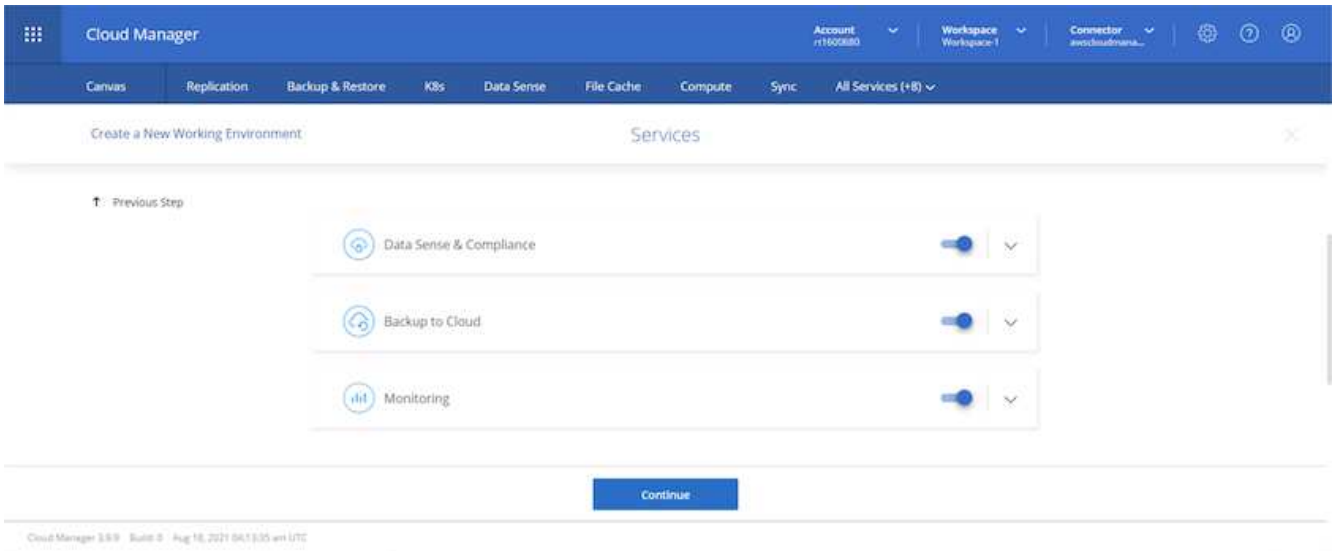
9. A assinatura agora aparece no Cloud Central. Clique em Aplicar para continuar.



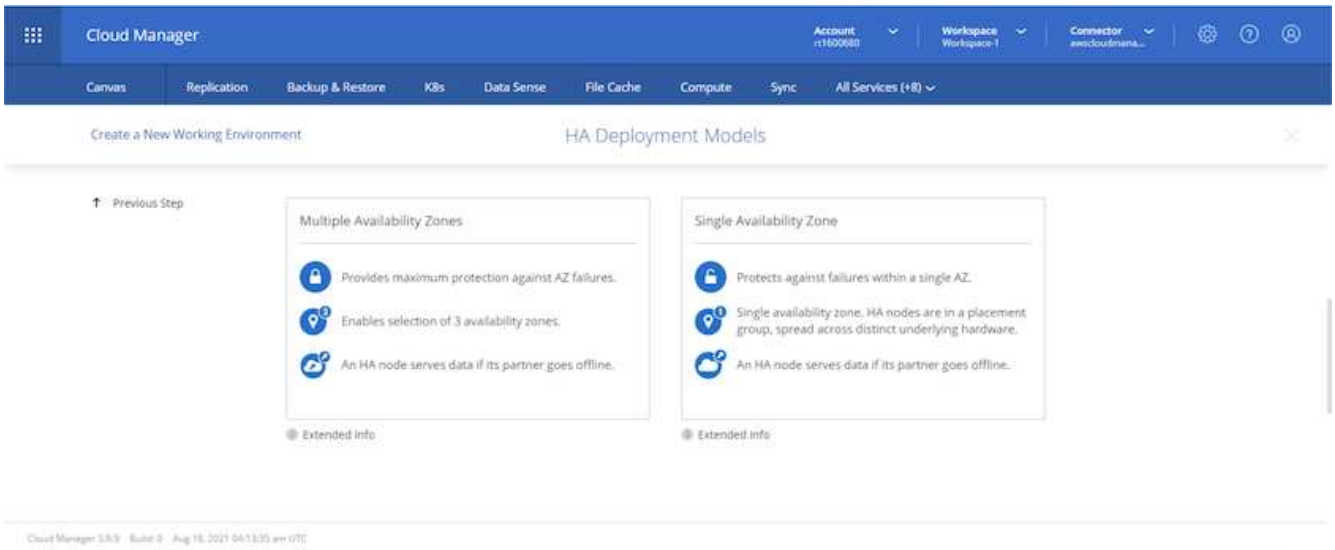
10. Insira os detalhes do ambiente de trabalho, como:
    a. Nome do cluster
    b. Senha do cluster
    c. Tags AWS (opcional)



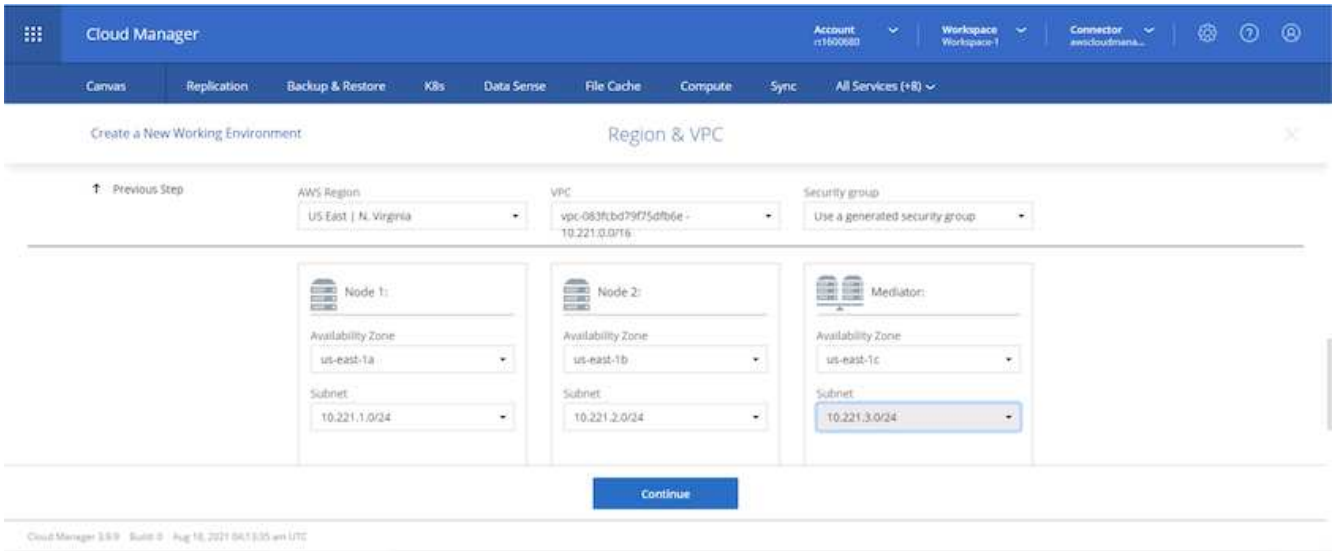
11. Escolha quais serviços adicionais você gostaria de implantar. Para saber mais sobre esses serviços, visite o "BlueXP: Operações modernas de propriedade de dados simplificadas" .



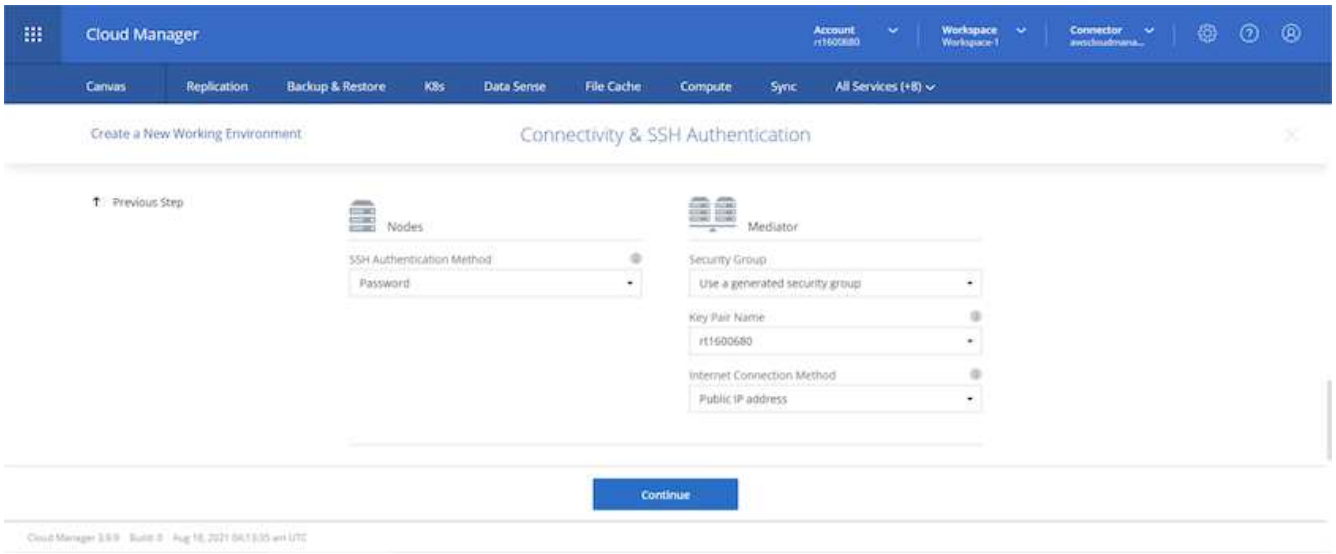
12. Escolha se deseja implantar em várias zonas de disponibilidade (requer três sub-redes, cada uma em uma AZ diferente) ou em uma única zona de disponibilidade. Eu escolhi várias AZs.



13. Escolha a região, a VPC e o grupo de segurança para o cluster ser implantado. Nesta seção, você também atribui as zonas de disponibilidade por nó (e mediador), bem como as sub-redes que elas ocupam.

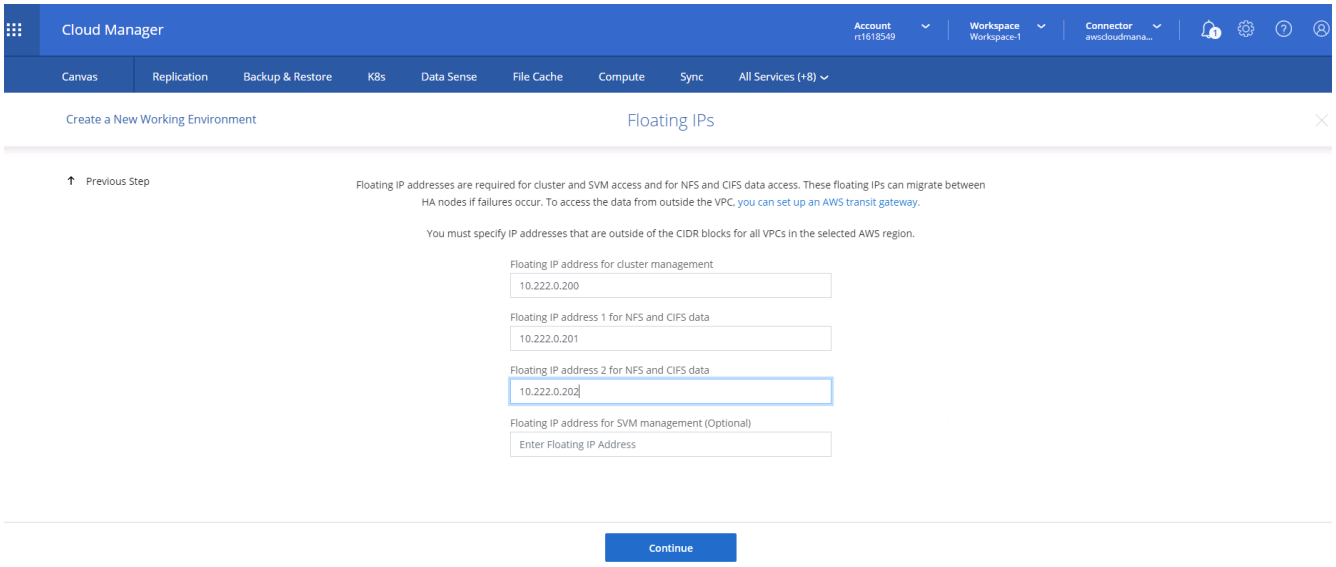


14. Escolha os métodos de conexão para os nós, bem como o mediador.

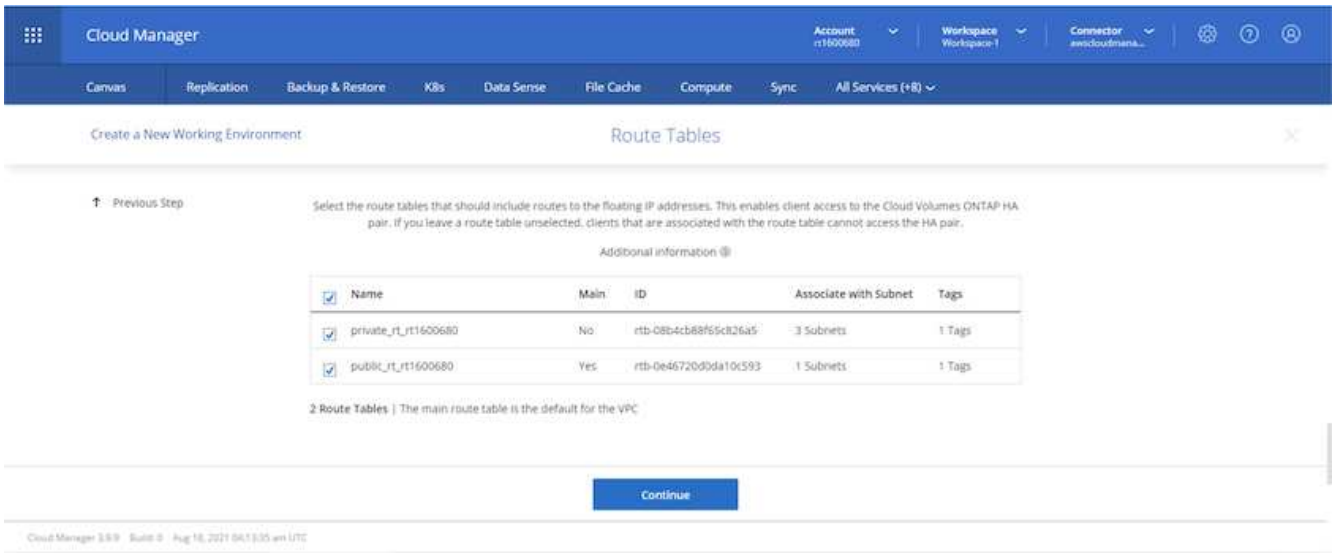


O mediador requer comunicação com as APIs da AWS. Um endereço IP público não é necessário, desde que as APIs possam ser acessadas após a implantação da instância do mediador EC2.

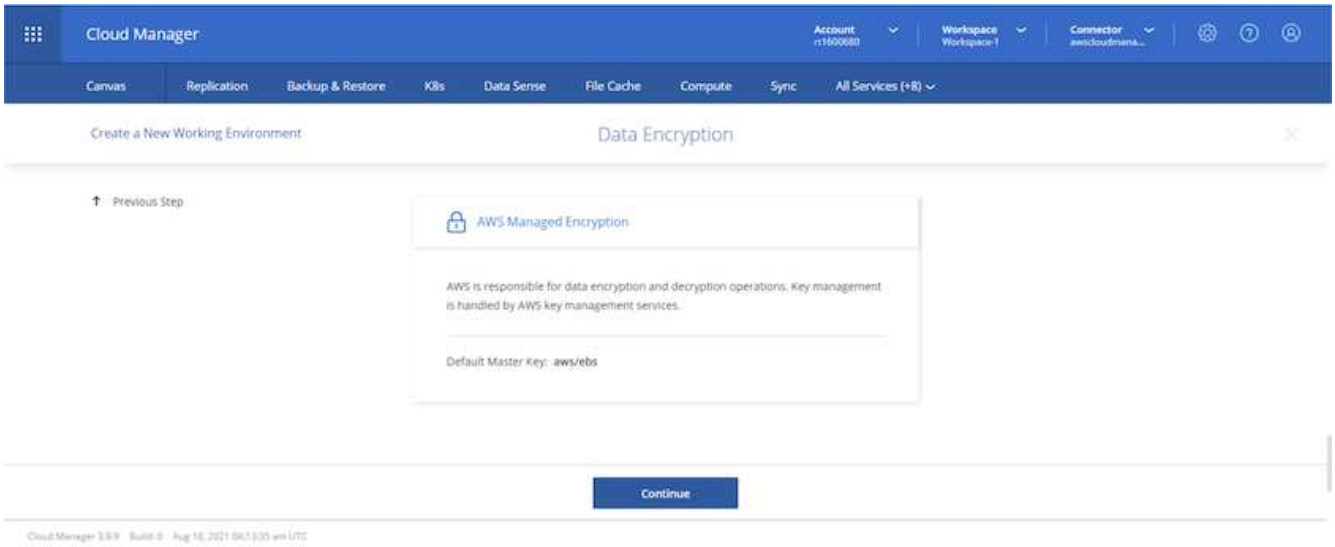
1. Endereços IP flutuantes são usados para permitir acesso aos vários endereços IP que o Cloud Volumes ONTAP usa, incluindo gerenciamento de cluster e IPs de serviço de dados. Esses devem ser endereços que ainda não são roteáveis na sua rede e são adicionados às tabelas de roteamento no seu ambiente AWS. Eles são necessários para habilitar endereços IP consistentes para um par de HA durante o failover. Mais informações sobre endereços IP flutuantes podem ser encontradas em "Documentação do NetApp Cloud" .



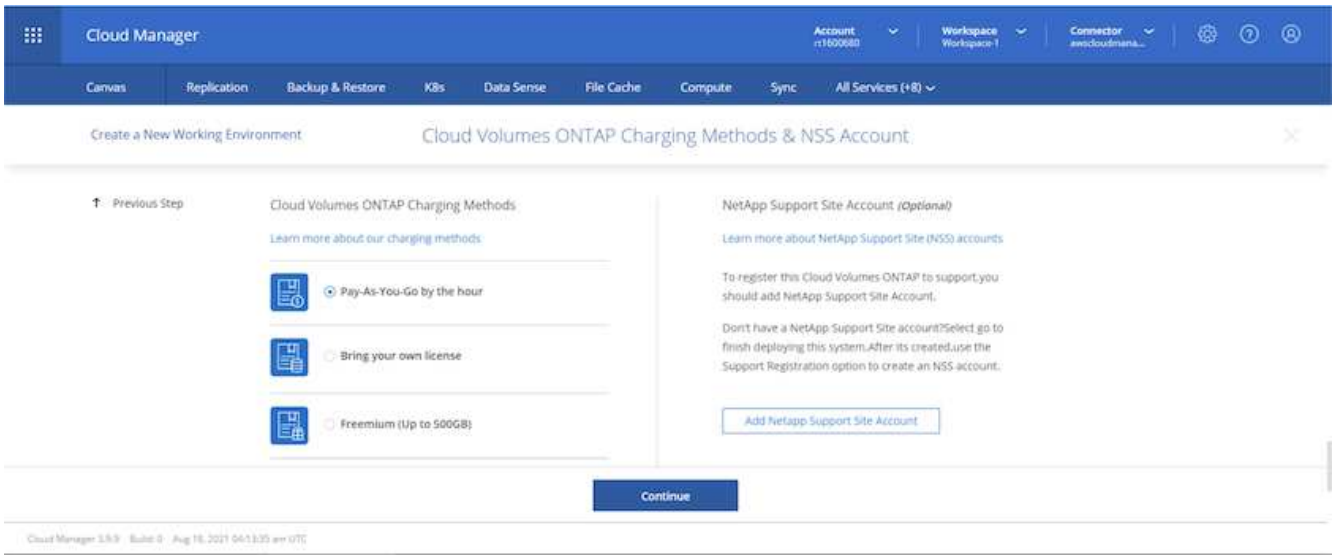
2. Selecione em quais tabelas de rotas os endereços IP flutuantes serão adicionados. Essas tabelas de rotas são usadas pelos clientes para se comunicar com o Cloud Volumes ONTAP.



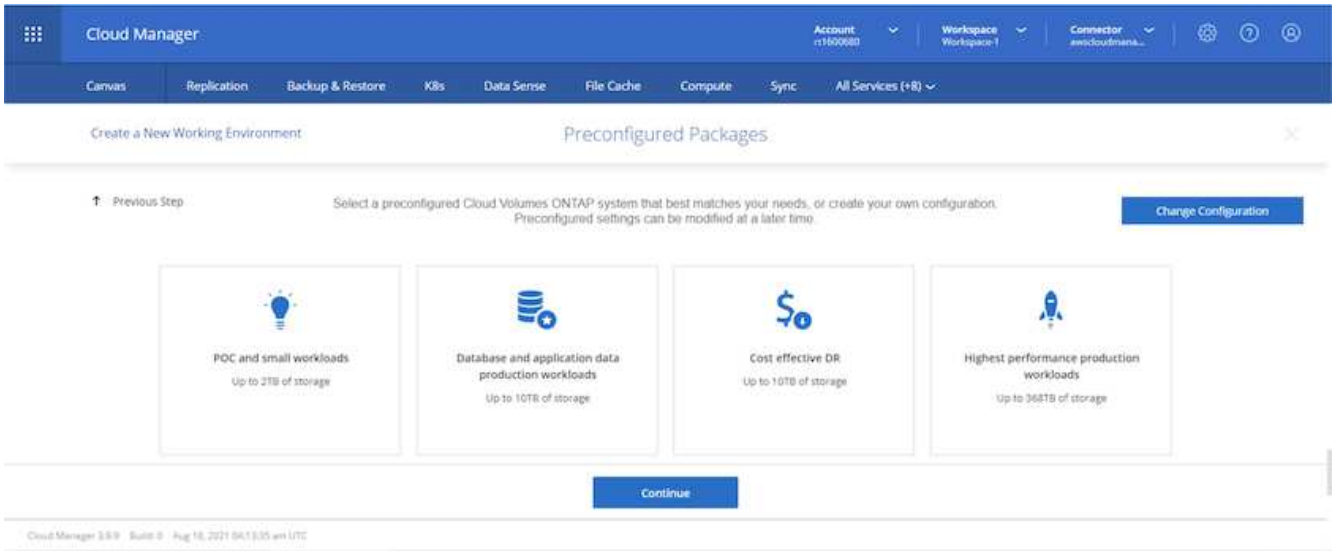
3. Escolha se deseja habilitar a criptografia gerenciada pela AWS ou o AWS KMS para criptografar os discos raiz, de inicialização e de dados do ONTAP .



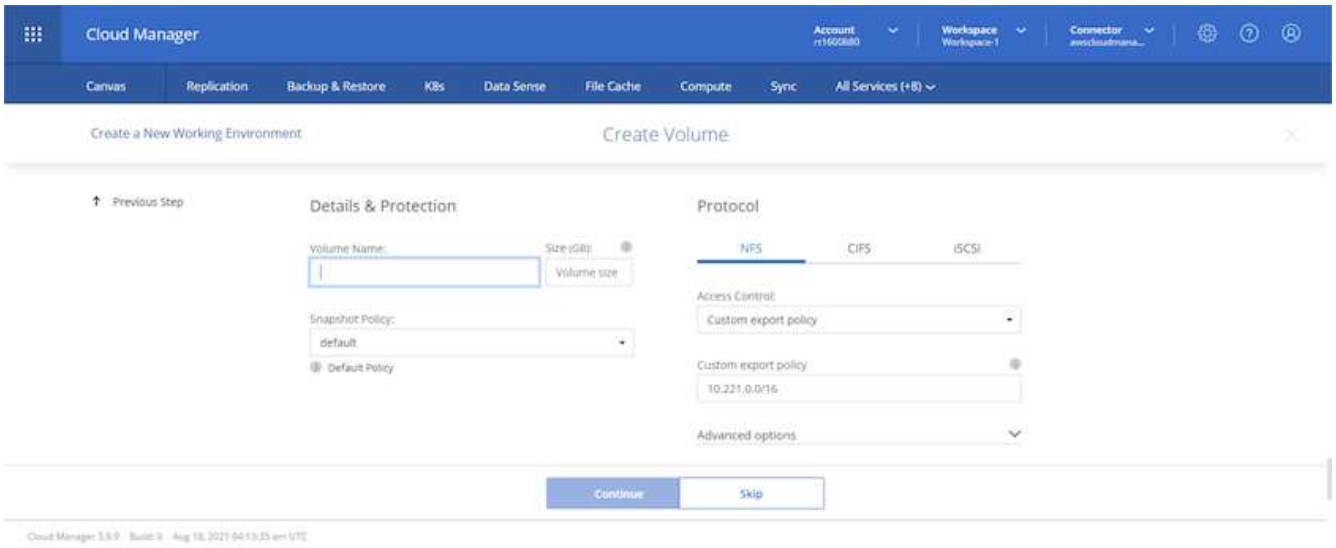
4. Escolha seu modelo de licenciamento. Se você não souber qual escolher, entre em contato com seu representante da NetApp .



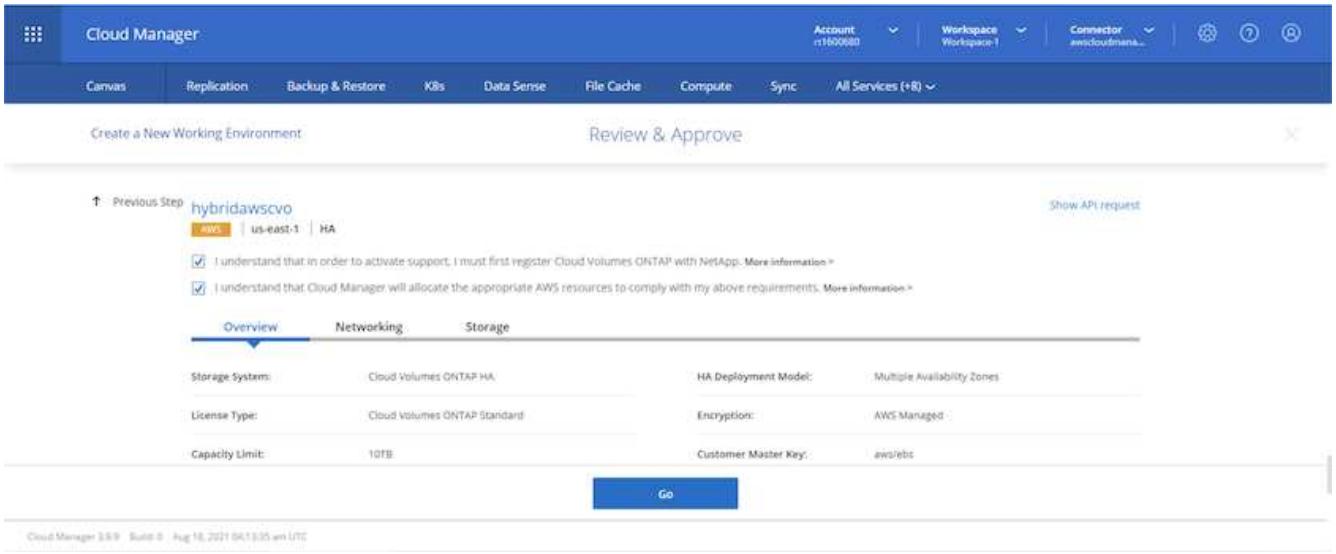
5. Selecione a configuração mais adequada ao seu caso de uso. Isso está relacionado às considerações de dimensionamento abordadas na página de pré-requisitos.



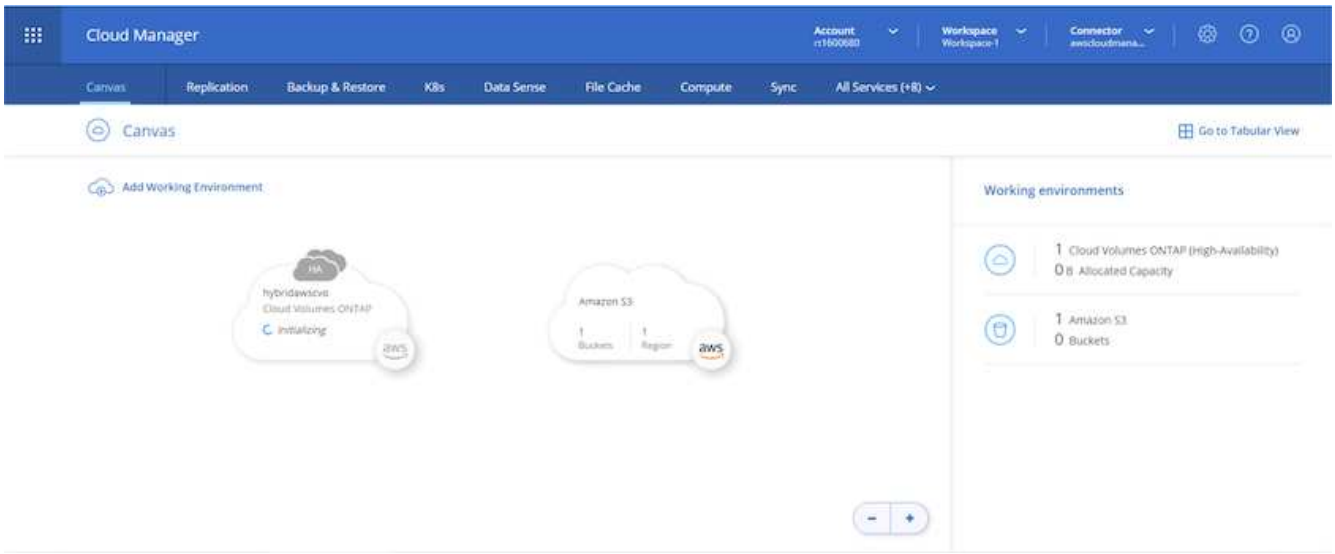
6. Opcionalmente, crie um volume. Isso não é necessário, porque as próximas etapas usam o SnapMirror, que cria os volumes para nós.



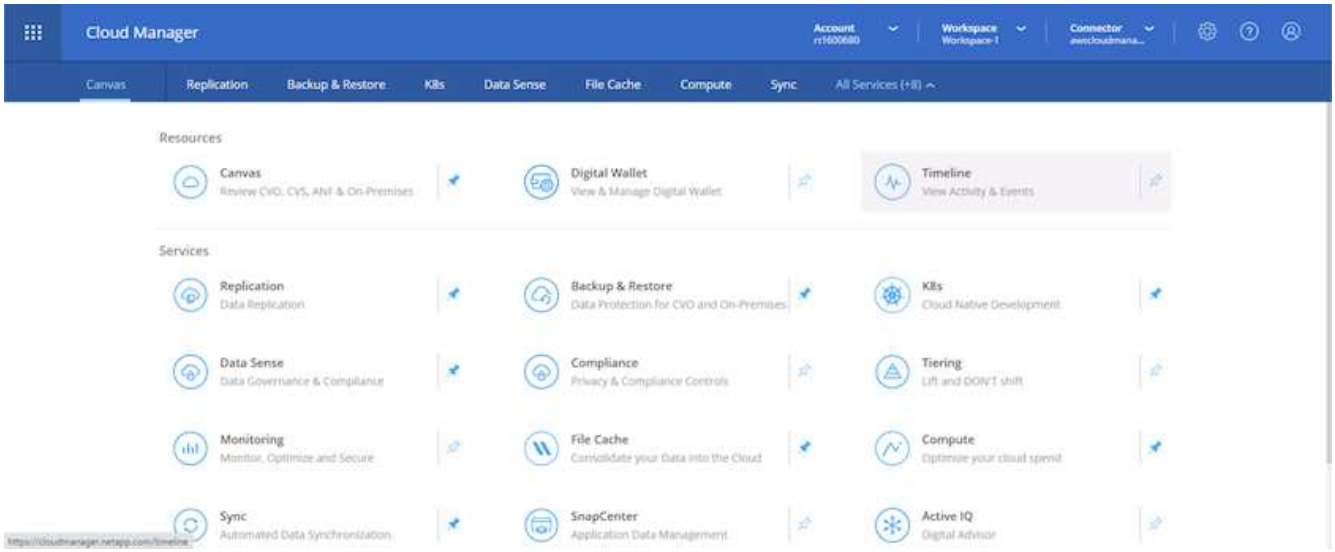
7. Revise as seleções feitas e marque as caixas para verificar se você entende que o Cloud Manager implanta recursos no seu ambiente da AWS. Quando estiver pronto, clique em Ir.



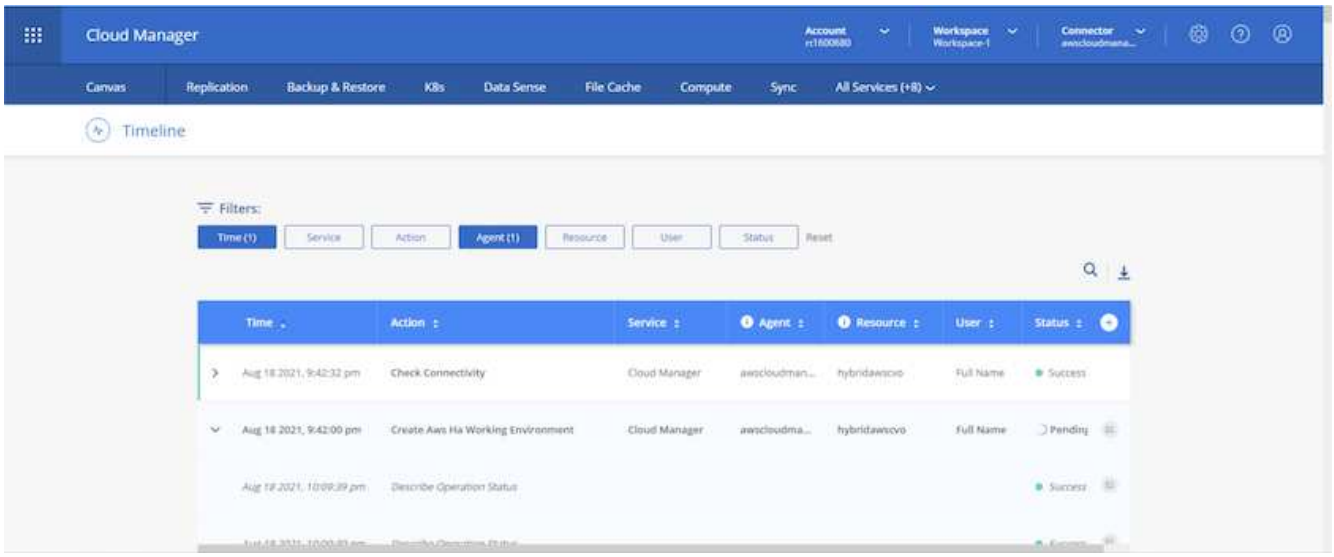
8. O Cloud Volumes ONTAP agora inicia seu processo de implantação. O Cloud Manager usa APIs da AWS e pilhas de formação de nuvem para implantar o Cloud Volumes ONTAP. Em seguida, ele configura o sistema de acordo com suas especificações, fornecendo um sistema pronto para uso que pode ser utilizado instantaneamente. O tempo para esse processo varia dependendo das seleções feitas.



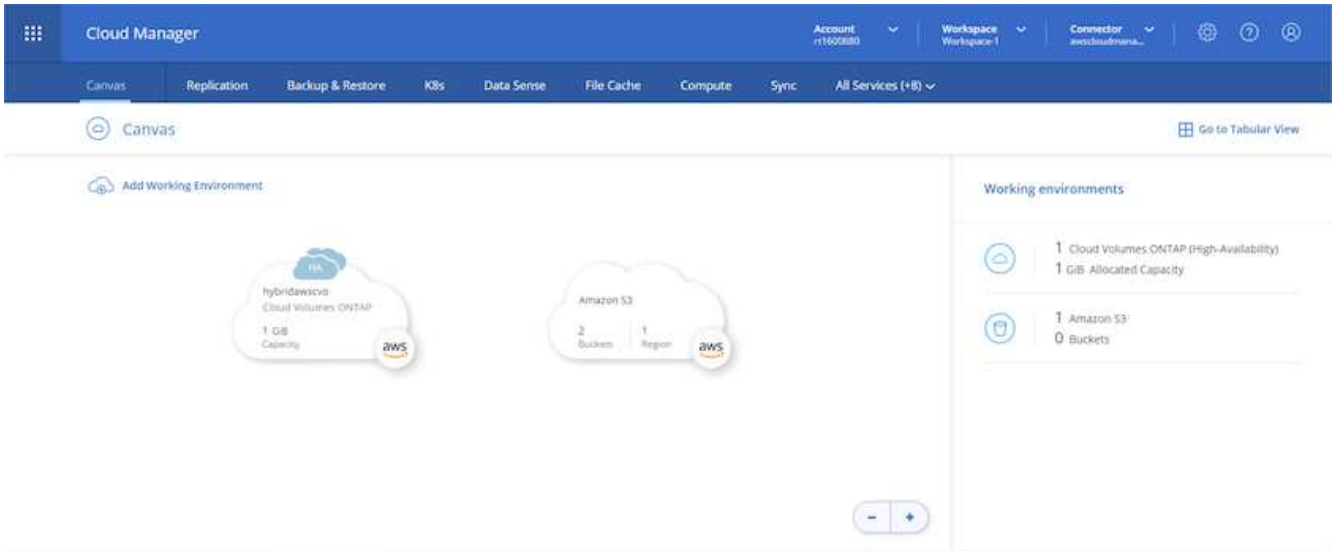
9. Você pode monitorar o progresso navegando até a Linha do tempo.



10. A Linha do Tempo atua como uma auditoria de todas as ações realizadas no Cloud Manager. Você pode visualizar todas as chamadas de API feitas pelo Cloud Manager durante a configuração tanto na AWS quanto no cluster ONTAP . Isso também pode ser usado efetivamente para solucionar quaisquer problemas que você enfrente.



11. Após a conclusão da implantação, o cluster CVO aparece no Canvas, com a capacidade atual. O cluster ONTAP em seu estado atual está totalmente configurado para permitir uma experiência real e pronta para uso.

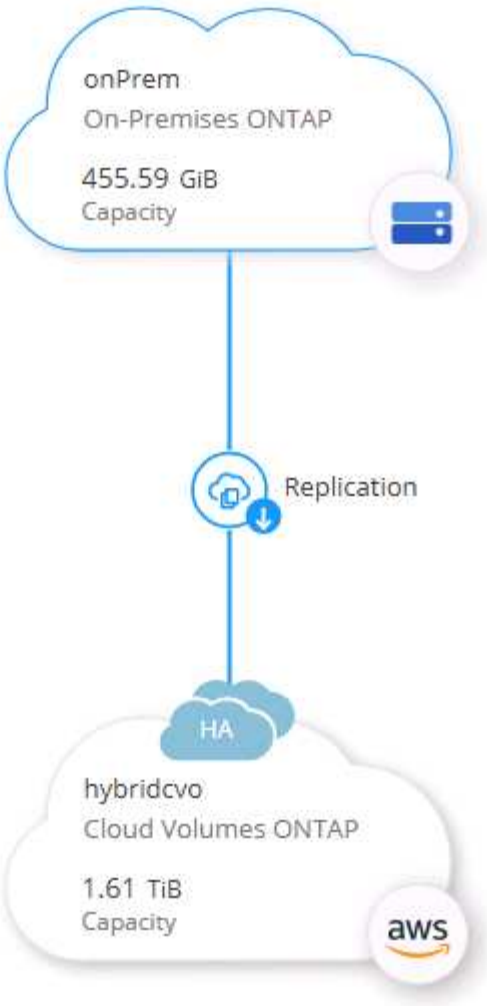


Configurar o SnapMirror do local para a nuvem

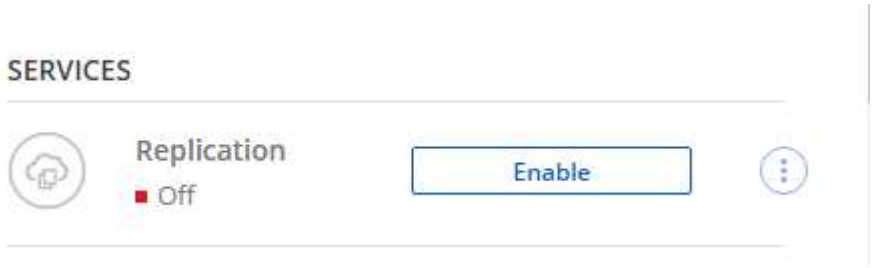
Agora que você tem um sistema ONTAP de origem e um sistema ONTAP de destino implantados, você pode replicar volumes contendo dados de banco de dados na nuvem.

Para obter um guia sobre versões ONTAP compatíveis com SnapMirror, consulte o "Matriz de compatibilidade do SnapMirror" .

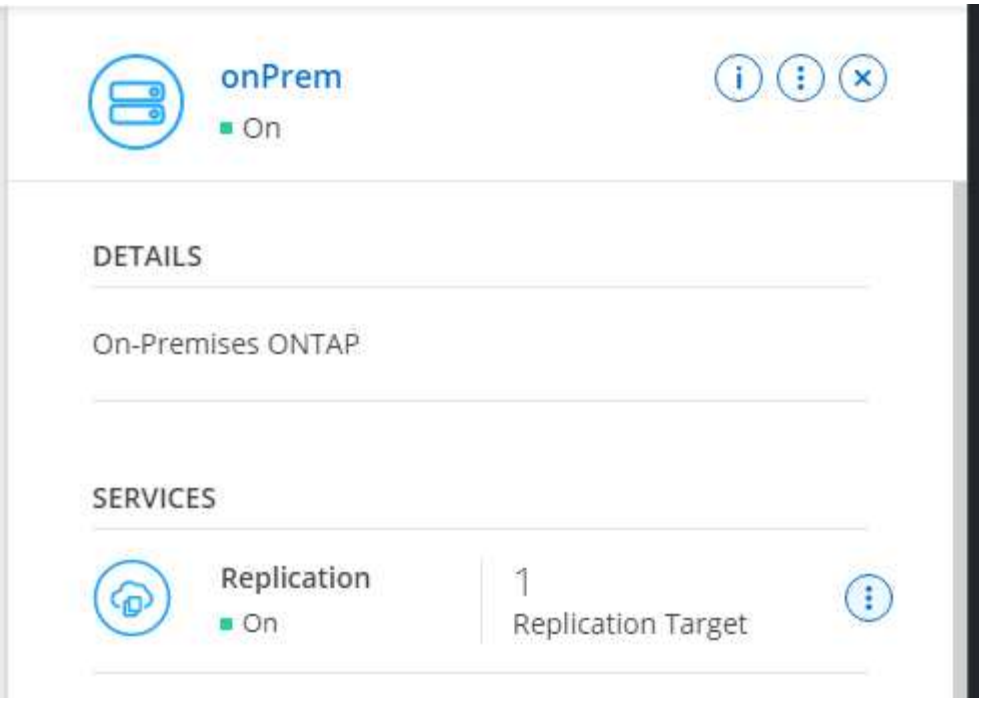
1. Clique no sistema ONTAP de origem (local) e arraste-o e solte-o no destino, selecione Replicação > Habilitar ou selecione Replicação > Menu > Replicar.



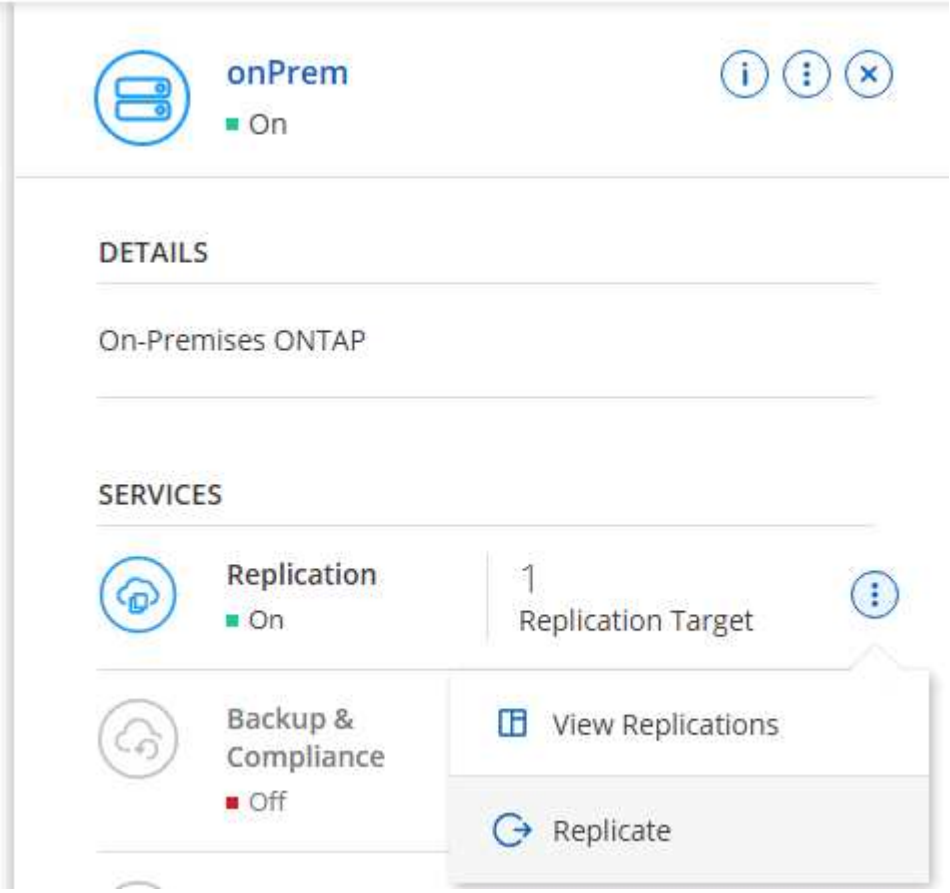
Selecione Habilitar.



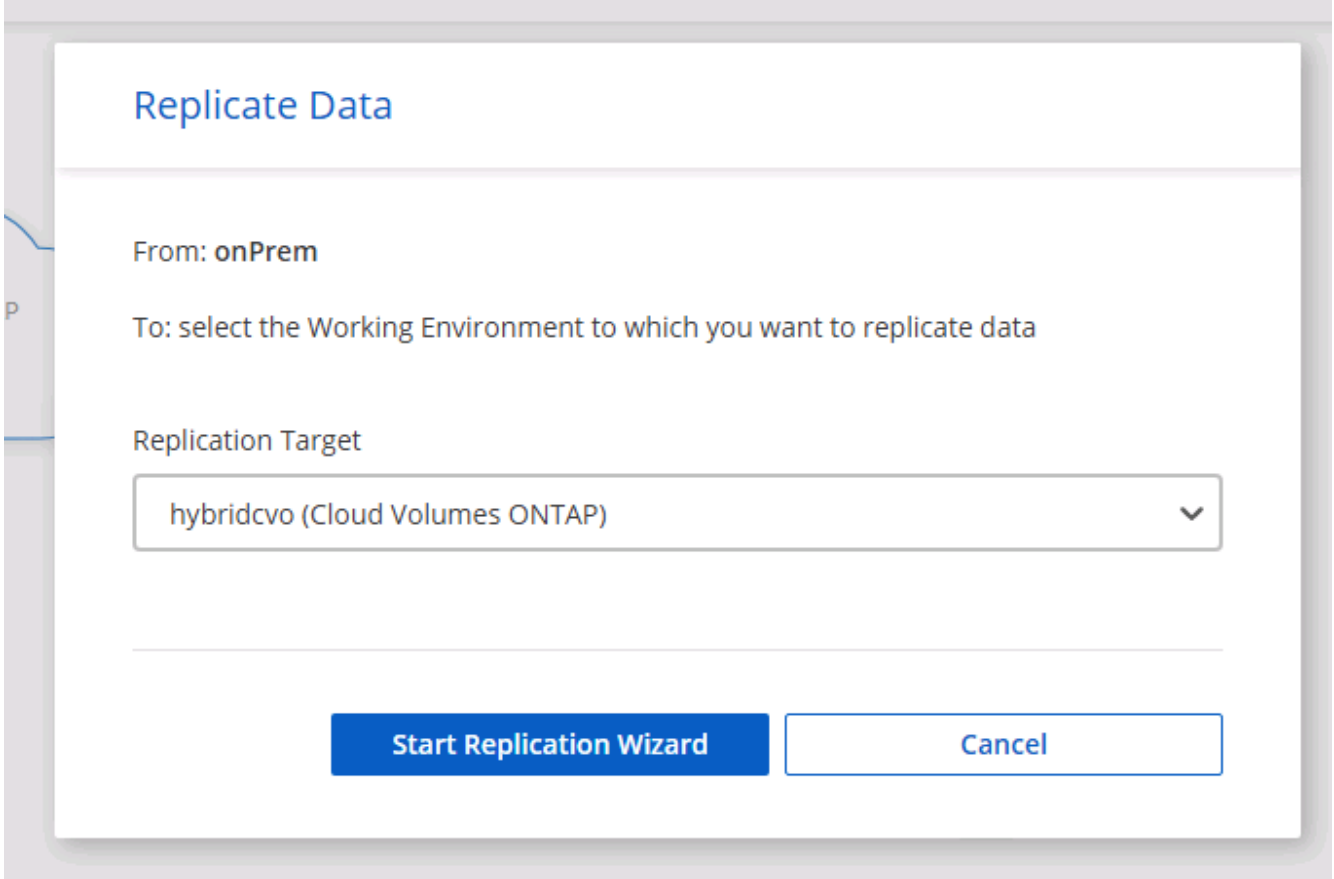
Ou Opções.



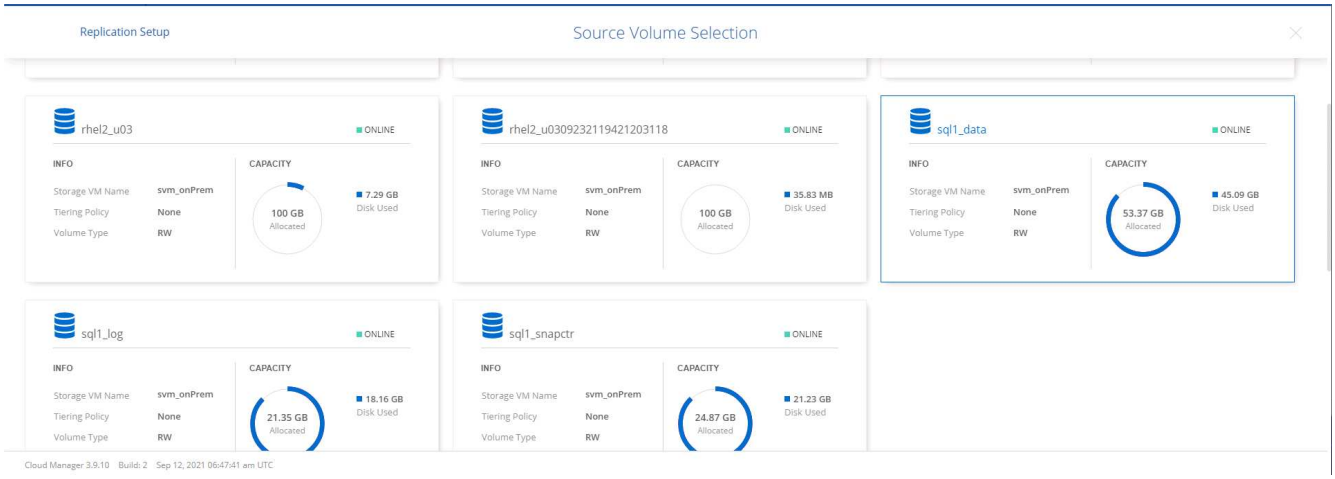
Replicar.



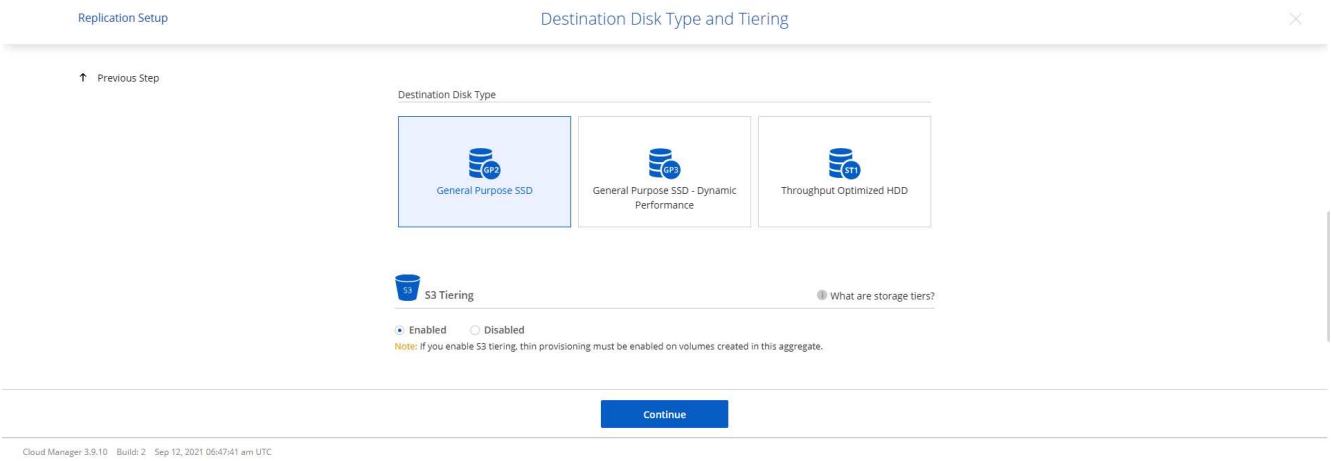
2. Se você não arrastou e soltou, escolha o cluster de destino para replicar.



3. Escolha o volume que você gostaria de replicar. Replicamos os dados e todos os volumes de log.

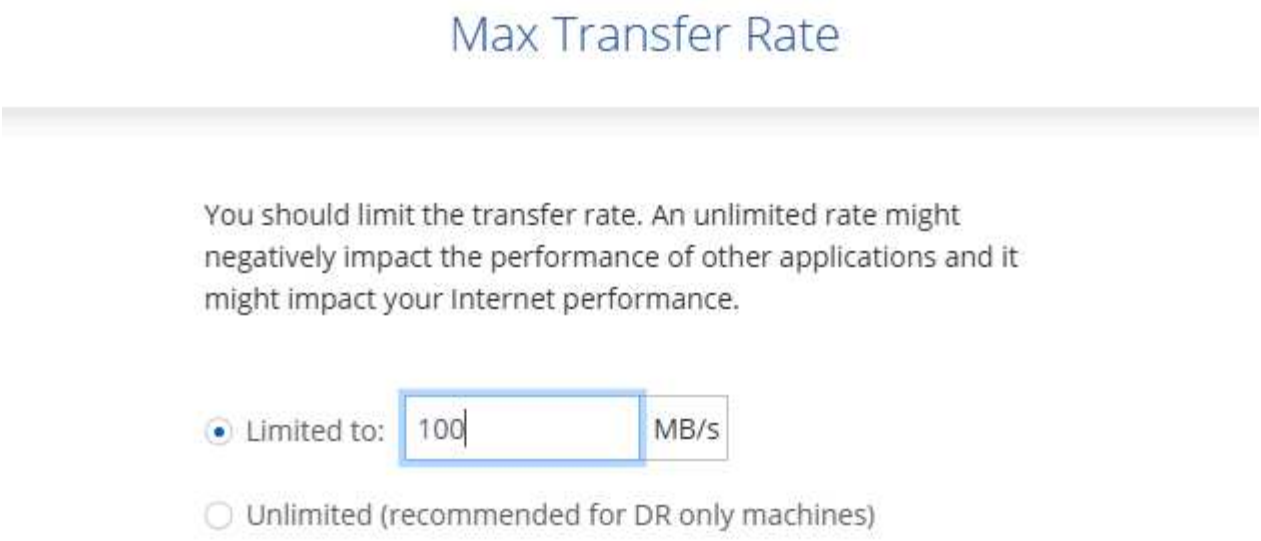


4. Escolha o tipo de disco de destino e a política de camadas. Para recuperação de desastres, recomendamos um SSD como tipo de disco e para manter a hierarquização dos dados. A hierarquização de dados coloca os dados espelhados em armazenamento de objetos de baixo custo e economiza dinheiro em discos locais. Quando você quebra o relacionamento ou clona o volume, os dados usam o armazenamento local rápido.

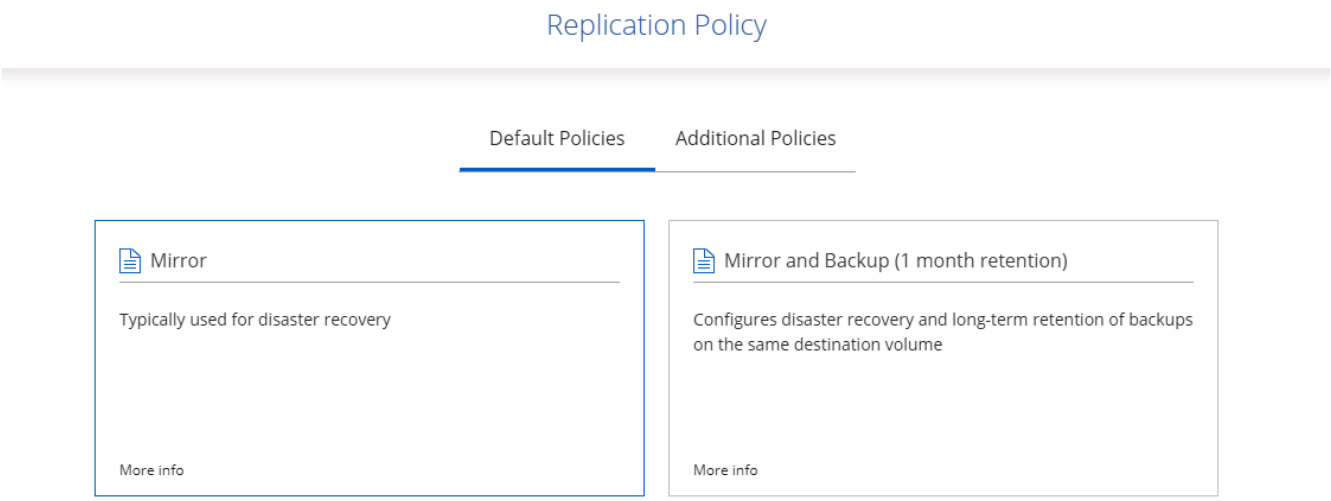


5. Selecione o nome do volume de destino: escolhemos `[source_volume_name]_dr`.

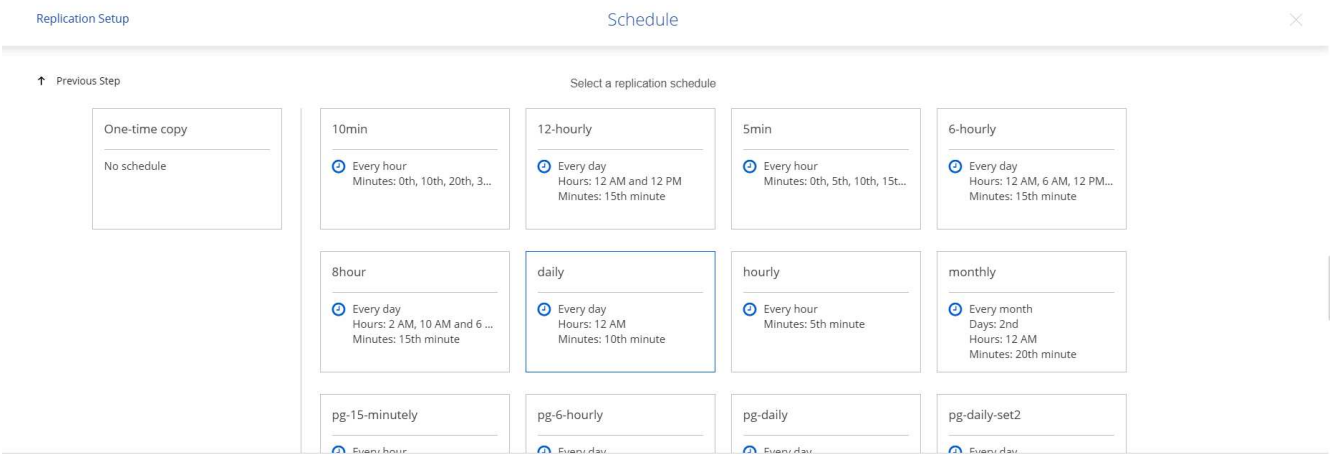
6. Selecione a taxa de transferência máxima para a replicação. Isso permite que você economize largura de banda caso tenha uma conexão de baixa largura de banda com a nuvem, como uma VPN.



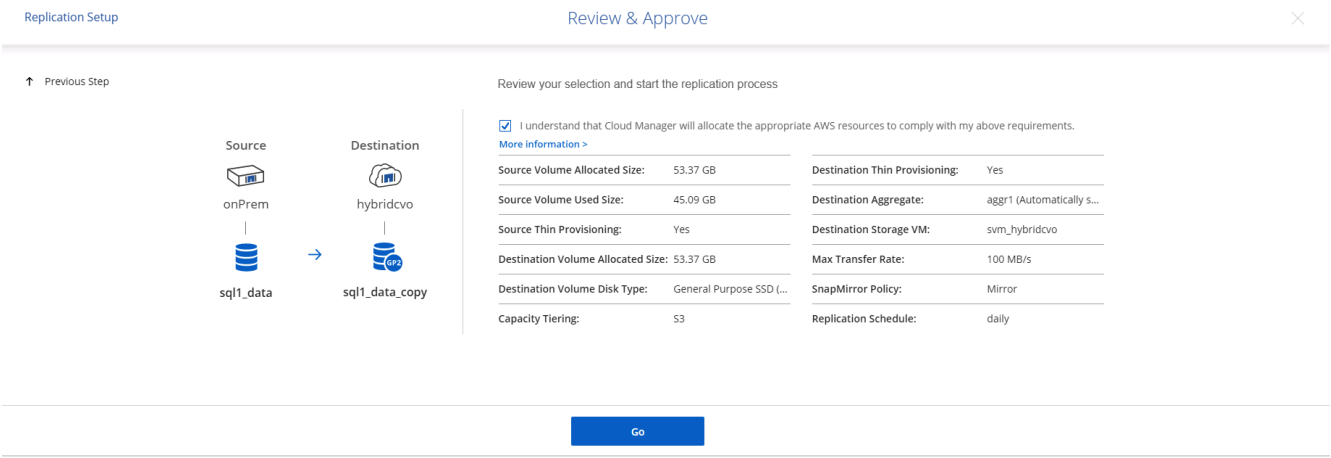
7. Defina a política de replicação. Escolhemos um Mirror, que pega o conjunto de dados mais recente e o replica no volume de destino. Você também pode escolher uma política diferente com base em suas necessidades.



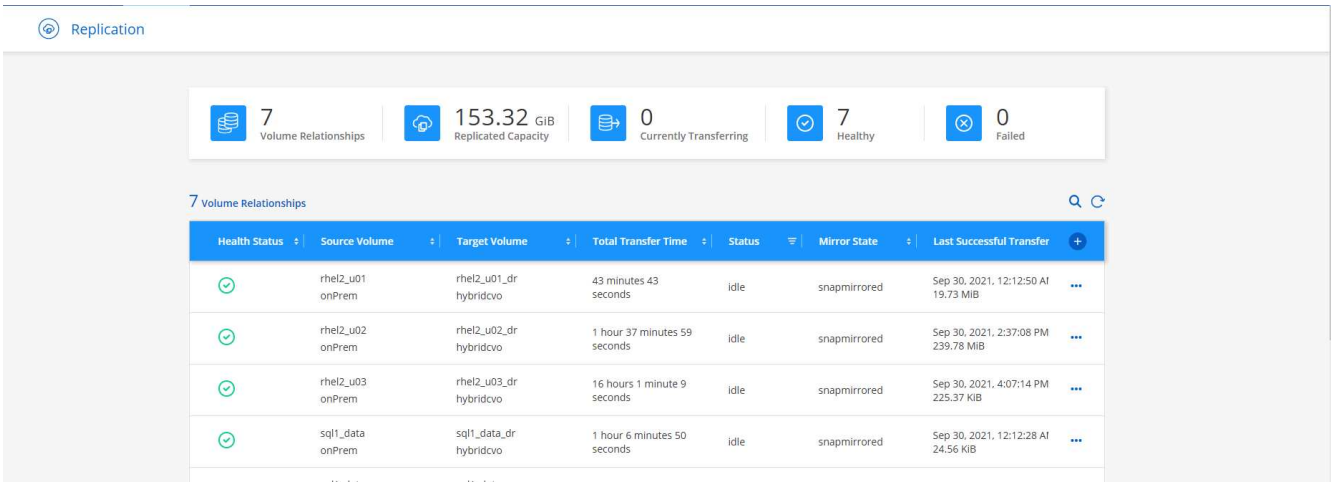
8. Escolha o agendamento para acionar a replicação. A NetApp recomenda definir uma programação "diária" para o volume de dados e uma programação "horária" para os volumes de log, embora isso possa ser alterado com base nos requisitos.



9. Revise as informações inseridas, clique em Ir para acionar o peer do cluster e o peer do SVM (se esta for a primeira vez que você replica entre os dois clusters) e, em seguida, implemente e inicialize o relacionamento SnapMirror .



10. Continue esse processo para volumes de dados e volumes de log.
11. Para verificar todos os seus relacionamentos, navegue até a guia Replicação dentro do Cloud Manager. Aqui você pode gerenciar seus relacionamentos e verificar o status deles.



12. Depois que todos os volumes forem replicados, você estará em um estado estável e pronto para passar para os fluxos de trabalho de recuperação de desastres e desenvolvimento/teste.

3. Implantar instância de computação do EC2 para carga de trabalho do banco de dados

A AWS pré-configurou instâncias de computação do EC2 para várias cargas de trabalho. A escolha do tipo de instância determina o número de núcleos de CPU, a capacidade de memória, o tipo e a capacidade de armazenamento e o desempenho da rede. Para os casos de uso, com exceção da partição do sistema operacional, o armazenamento principal para executar a carga de trabalho do banco de dados é alocado do CVO ou do mecanismo de armazenamento FSx ONTAP . Portanto, os principais fatores a serem considerados são a escolha dos núcleos da CPU, a memória e o nível de desempenho da rede. Tipos típicos de instâncias do AWS EC2 podem ser encontrados aqui: "Tipo de instância EC2" .

Dimensionando a instância de computação

1. Selecione o tipo de instância correto com base na carga de trabalho necessária. Os fatores a serem considerados incluem o número de transações comerciais a serem suportadas, o número de usuários simultâneos, o dimensionamento do conjunto de dados e assim por diante.
2. A implantação da instância do EC2 pode ser iniciada por meio do Painel do EC2. Os procedimentos exatos de implantação estão além do escopo desta solução. Ver "Amazon EC2" para mais detalhes.

Configuração de instância Linux para carga de trabalho Oracle

Esta seção contém etapas de configuração adicionais após a implantação de uma instância do EC2 Linux.

1. Adicione uma instância de standby do Oracle ao servidor DNS para resolução de nomes dentro do domínio de gerenciamento do SnapCenter .
2. Adicione um ID de usuário de gerenciamento do Linux como credenciais do SnapCenter OS com permissões sudo sem senha. Habilite o ID com autenticação de senha SSH na instância EC2. (Por padrão, a autenticação de senha SSH e o sudo sem senha são desativados em instâncias EC2.)
3. Configure a instalação do Oracle para corresponder à instalação local do Oracle, como patches do sistema operacional, versões e patches do Oracle e assim por diante.
4. As funções de automação do NetApp Ansible DB podem ser aproveitadas para configurar instâncias do EC2 para casos de uso de desenvolvimento/teste de banco de dados e recuperação de desastres. O código de automação pode ser baixado do site público do GitHub da NetApp : "Implantação automatizada do Oracle 19c" . O objetivo é instalar e configurar uma pilha de software de banco de dados em uma instância EC2 para corresponder às configurações do sistema operacional e do banco de dados local.

Configuração de instância do Windows para carga de trabalho do SQL Server

Esta seção lista etapas de configuração adicionais após uma instância do EC2 Windows ser implantada inicialmente.

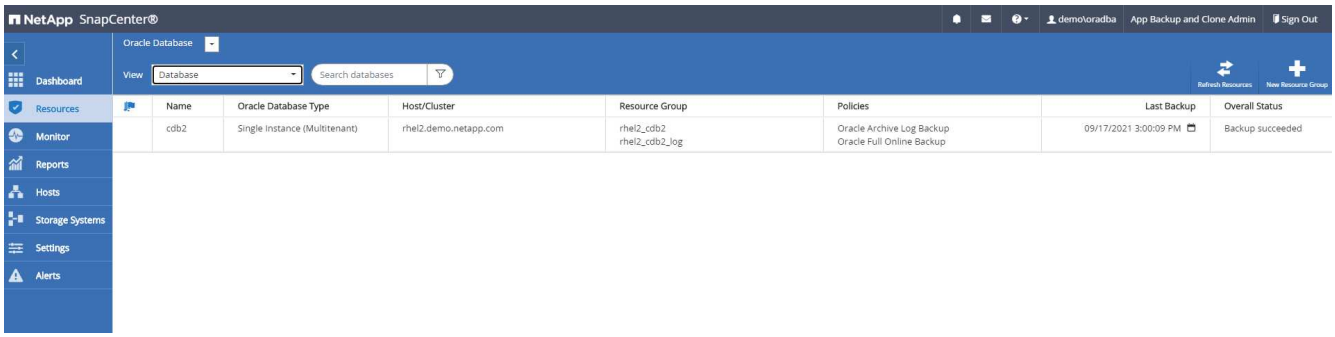
1. Recupere a senha do administrador do Windows para efetuar login em uma instância via RDP.
2. Desabilite o firewall do Windows, junte o host ao domínio do Windows SnapCenter e adicione a instância ao servidor DNS para resolução de nomes.
3. Provisione um volume de log do SnapCenter para armazenar arquivos de log do SQL Server.
4. Configure o iSCSI no host Windows para montar o volume e formatar a unidade de disco.
5. Novamente, muitas das tarefas anteriores podem ser automatizadas com a solução de automação da NetApp para SQL Server. Confira o site público do GitHub de automação da NetApp para funções e soluções recém-publicadas: "Automação NetApp" .

Fluxo de trabalho para expansão de desenvolvimento/teste para a nuvem

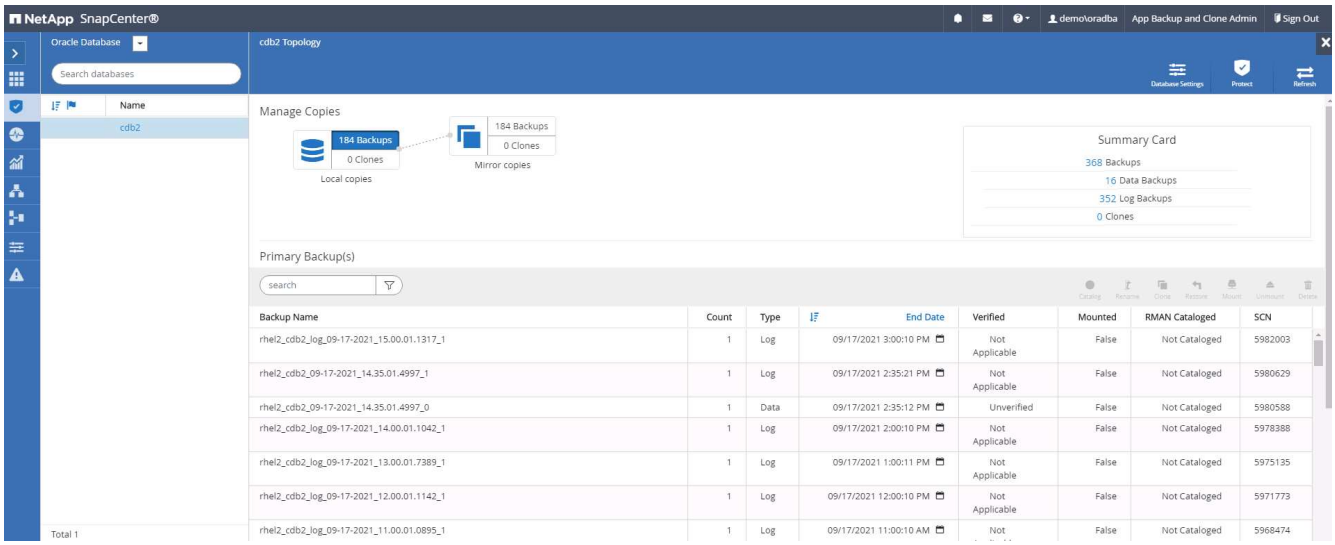
A agilidade da nuvem pública, o tempo de retorno e a economia de custos são propostas de valor significativas para empresas que adotam a nuvem pública para desenvolvimento de aplicativos de banco de dados e esforços de teste. Não há ferramenta melhor que o SnapCenter para tornar isso realidade. O SnapCenter não só pode proteger seu banco de dados de produção local, mas também pode clonar rapidamente uma cópia para desenvolvimento de aplicativos ou testes de código na nuvem pública, consumindo muito pouco armazenamento extra. A seguir estão os detalhes dos processos passo a passo para usar esta ferramenta.

Clonar um banco de dados Oracle para desenvolvimento/teste a partir de um backup de snapshot replicado

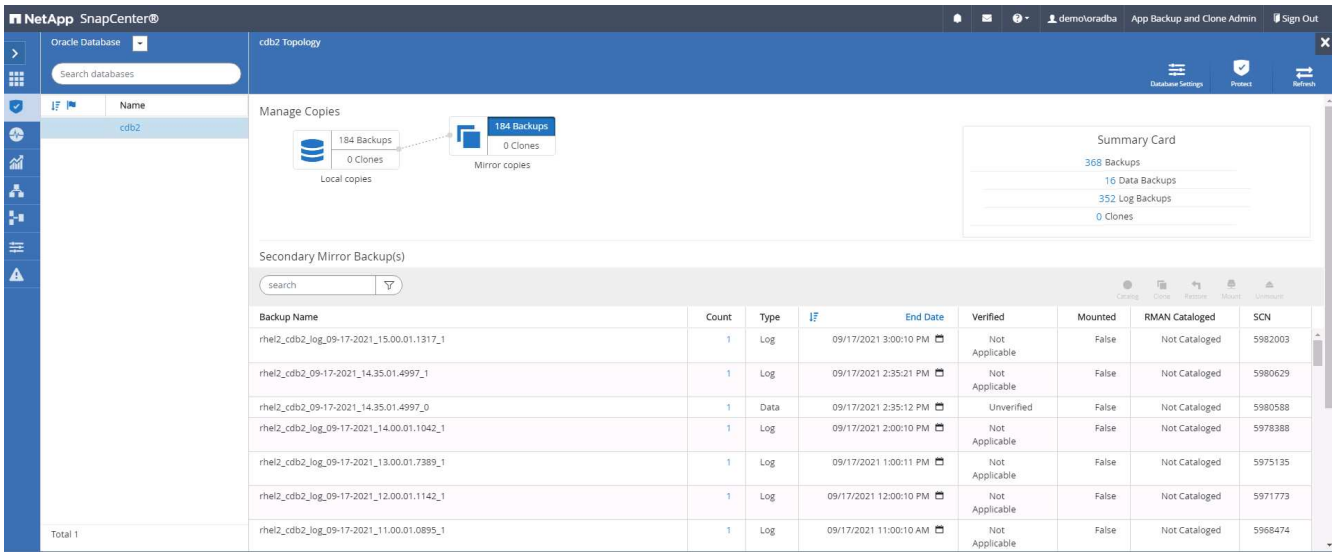
1. Efetue login no SnapCenter com um ID de usuário de gerenciamento de banco de dados do Oracle. Navegue até a guia Recursos, que mostra os bancos de dados Oracle sendo protegidos pelo SnapCenter.



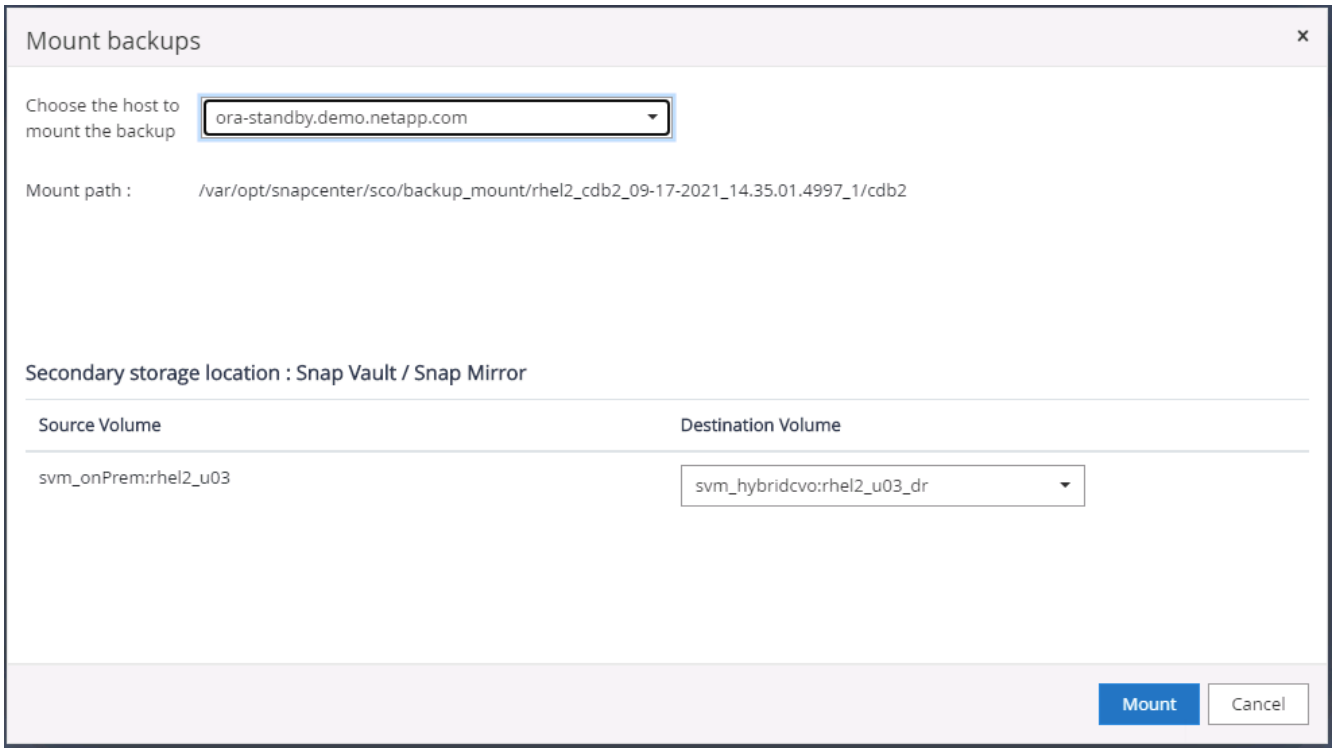
2. Clique no nome do banco de dados local pretendido para a topologia de backup e a visualização detalhada. Se um local replicado secundário estiver habilitado, ele mostrará backups espelhados vinculados.

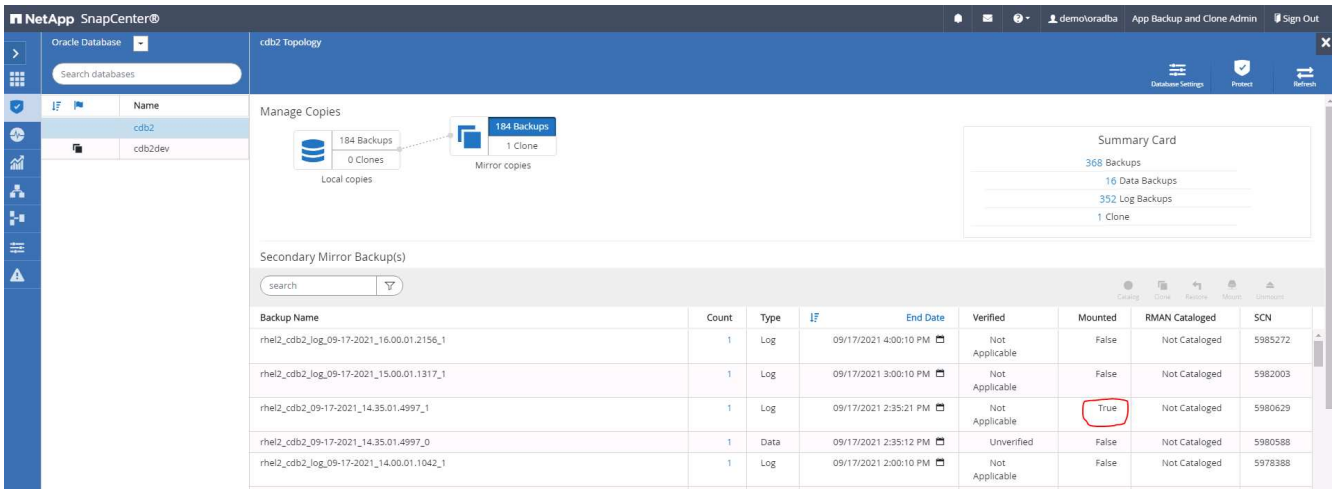


3. Alterne para a visualização de backups espelhados clicando em backups espelhados. O(s) backup(es) do espelho secundário é(são) então exibido(s).



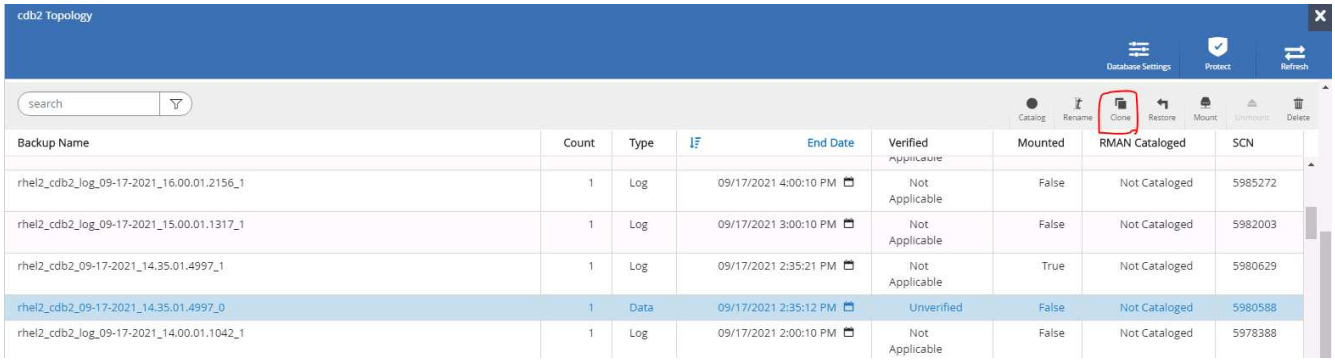
4. Escolha uma cópia de backup do banco de dados secundário espelhado a ser clonada e determine um ponto de recuperação por hora e número de alteração do sistema ou por SCN. Geralmente, o ponto de recuperação deve estar atrás do tempo de backup completo do banco de dados ou do SCN a ser clonado. Depois que um ponto de recuperação for definido, o backup do arquivo de log necessário deverá ser montado para recuperação. O backup do arquivo de log deve ser montado no servidor de banco de dados de destino onde o banco de dados clone será hospedado.



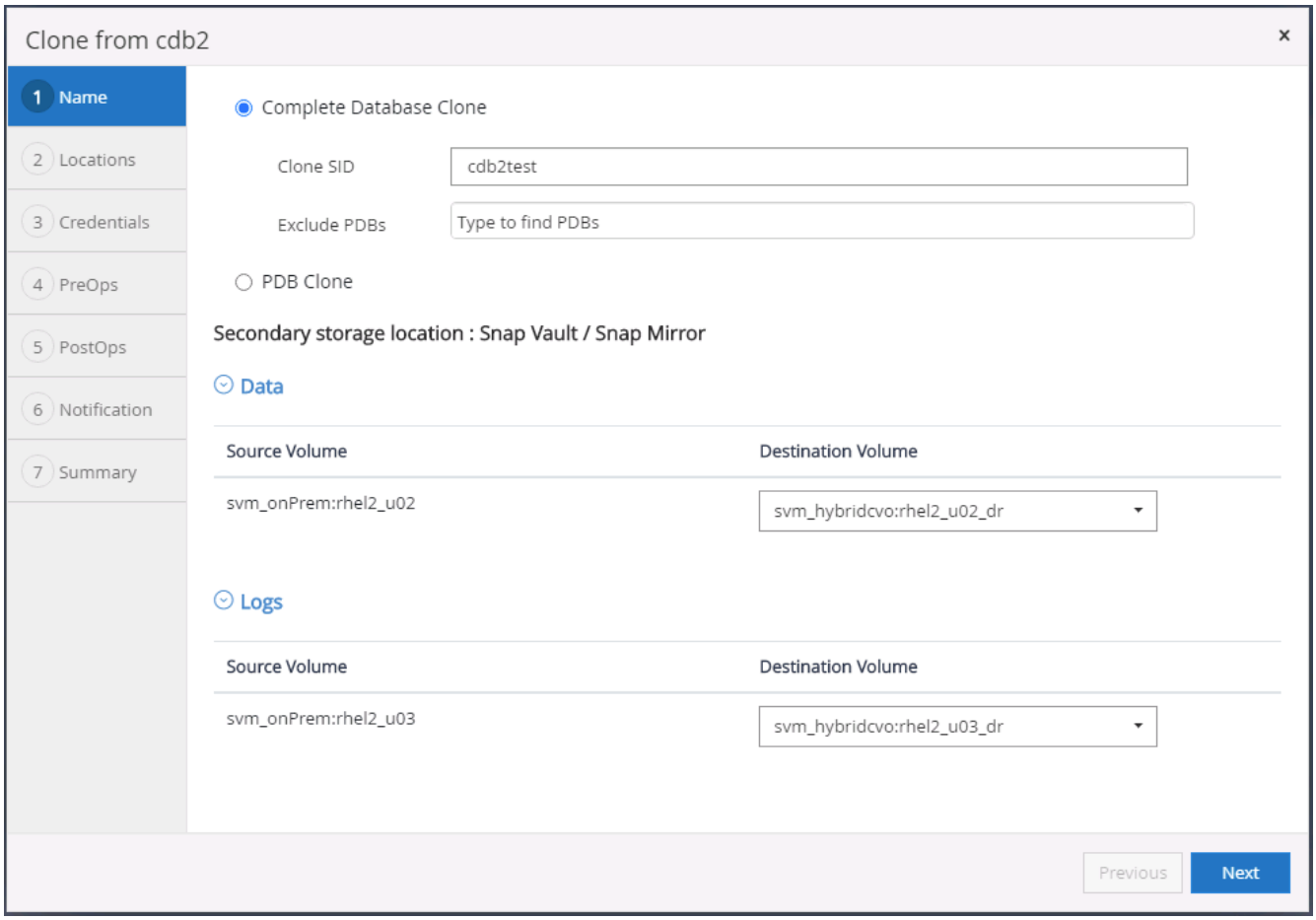


Se a remoção de log estiver habilitada e o ponto de recuperação for estendido além da última remoção de log, vários backups de log de arquivamento poderão precisar ser montados.

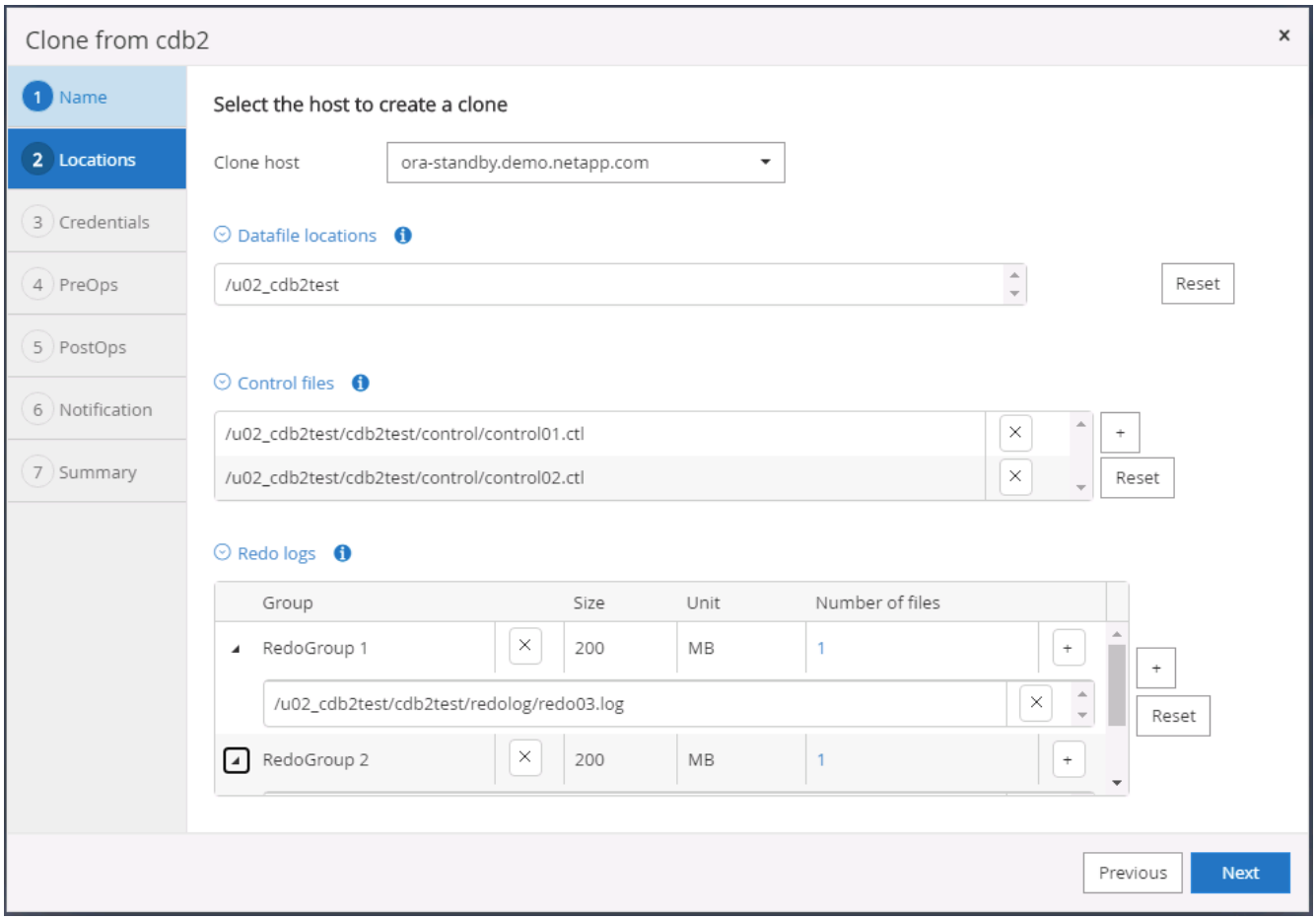
5. Realce a cópia de backup completa do banco de dados a ser clonada e clique no botão clonar para iniciar o fluxo de trabalho de clonagem do banco de dados.



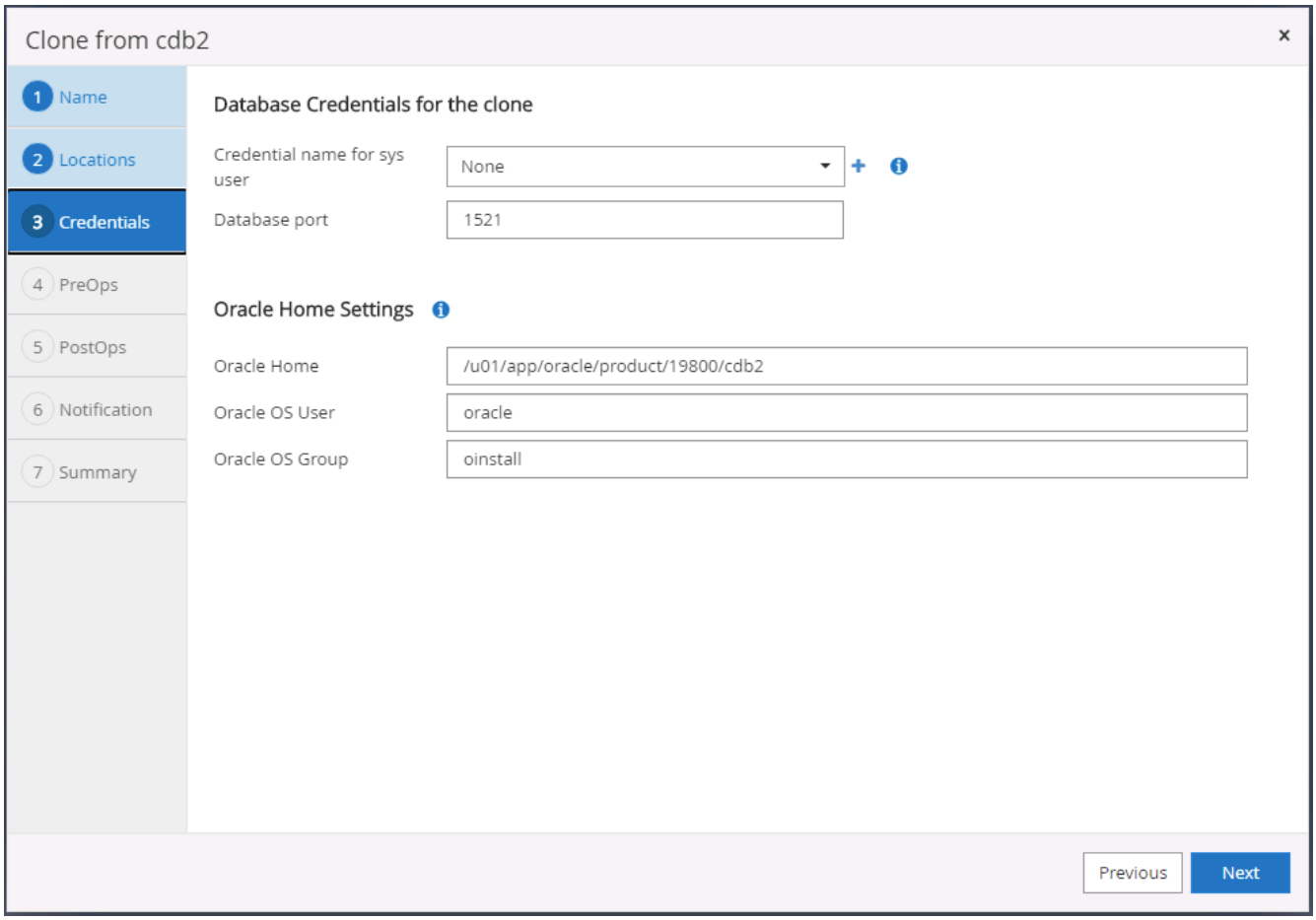
6. Escolha um SID de banco de dados clone adequado para um banco de dados de contêiner completo ou clone de CDB.



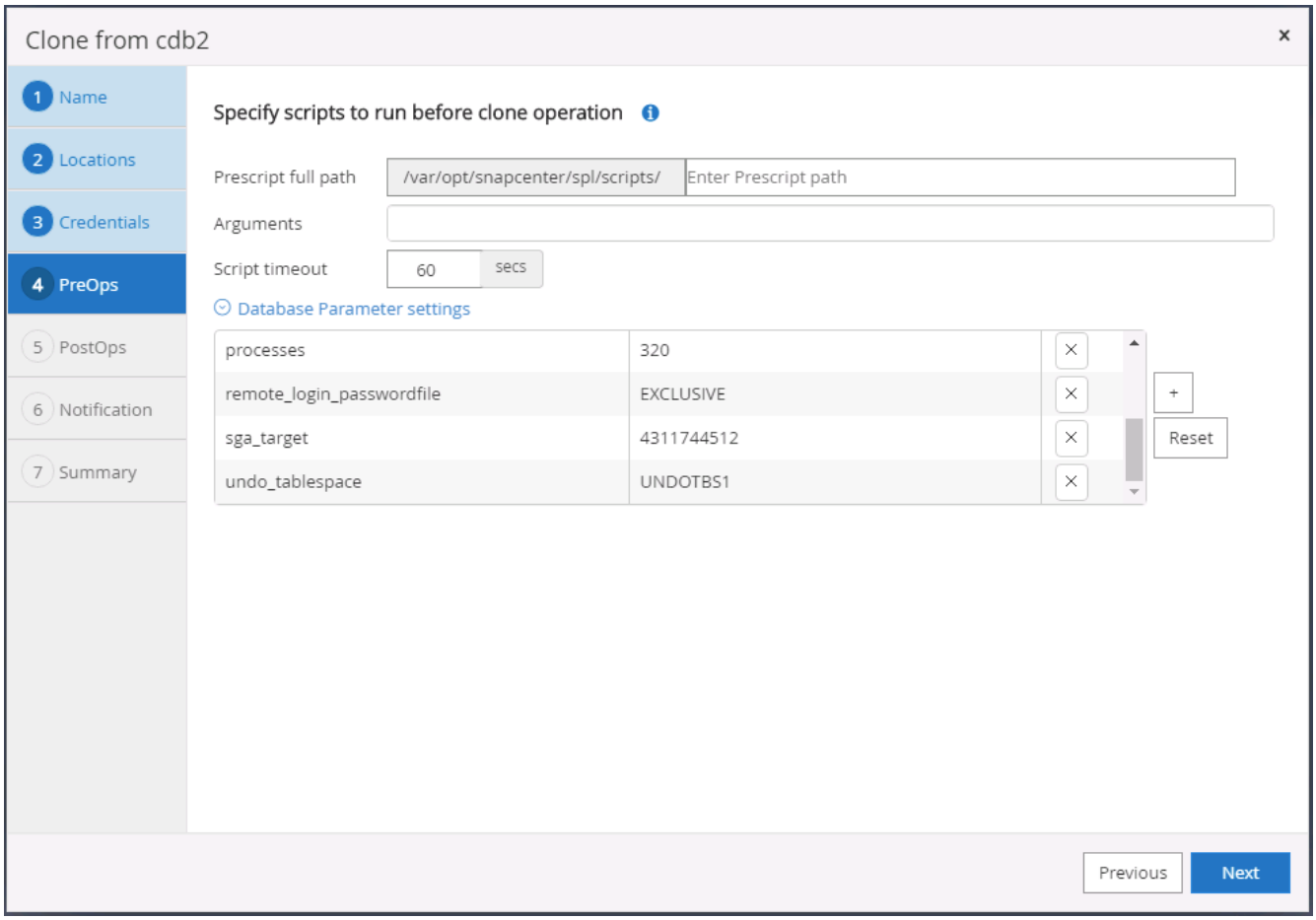
7. Selecione o host do clone de destino na nuvem, e os diretórios de arquivo de dados, arquivo de controle e log de refazer serão criados pelo fluxo de trabalho do clone.



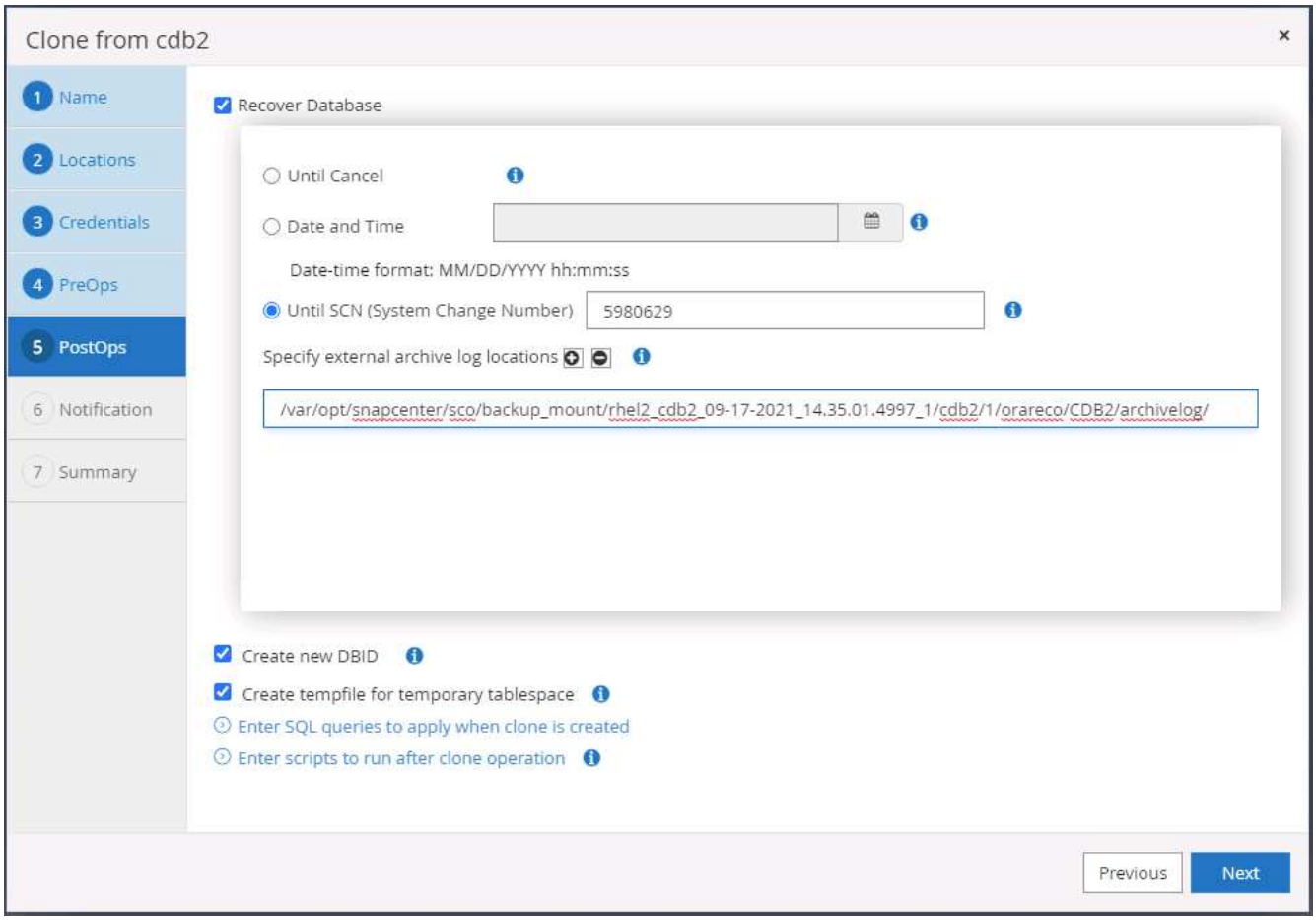
8. O nome de credencial Nenhum é usado para autenticação baseada em sistema operacional, o que torna a porta do banco de dados irrelevante. Preencha o Oracle Home, o Oracle OS User e o Oracle OS Group adequados, conforme configurado no servidor de banco de dados clone de destino.

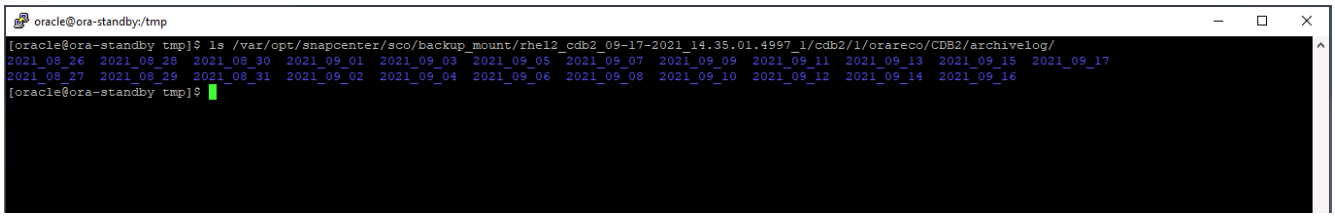


9. Especifique os scripts a serem executados antes da operação de clonagem. Mais importante, o parâmetro da instância do banco de dados pode ser ajustado ou definido aqui.

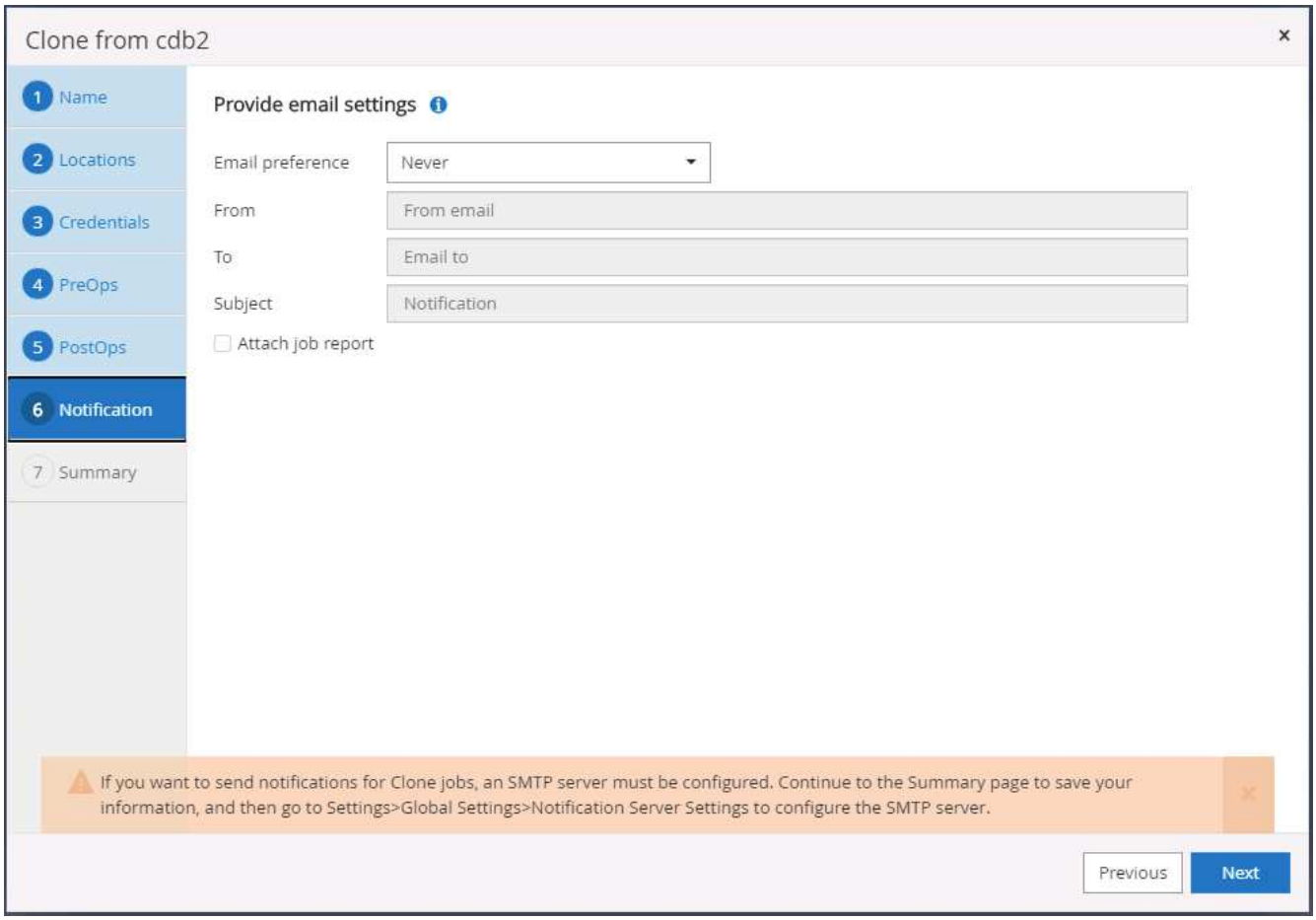


10. Especifique o ponto de recuperação por data e hora ou SCN. Até Cancelar recupera o banco de dados até os logs de arquivo disponíveis. Especifique o local do log de arquivamento externo do host de destino onde o volume do log de arquivamento está montado. Se o proprietário do servidor de destino Oracle for diferente do servidor de produção local, verifique se o diretório de log de arquivamento pode ser lido pelo proprietário do servidor de destino Oracle.

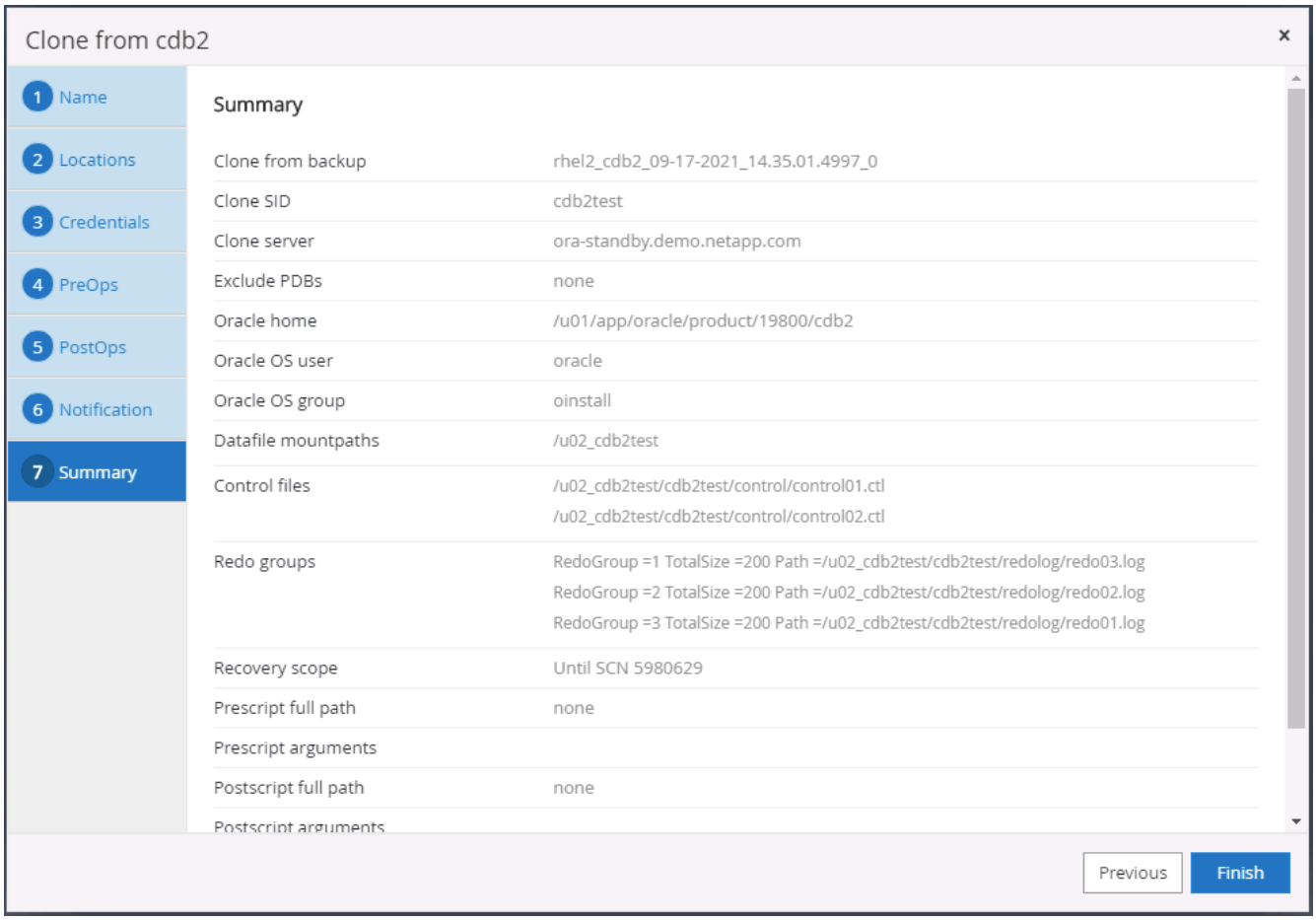




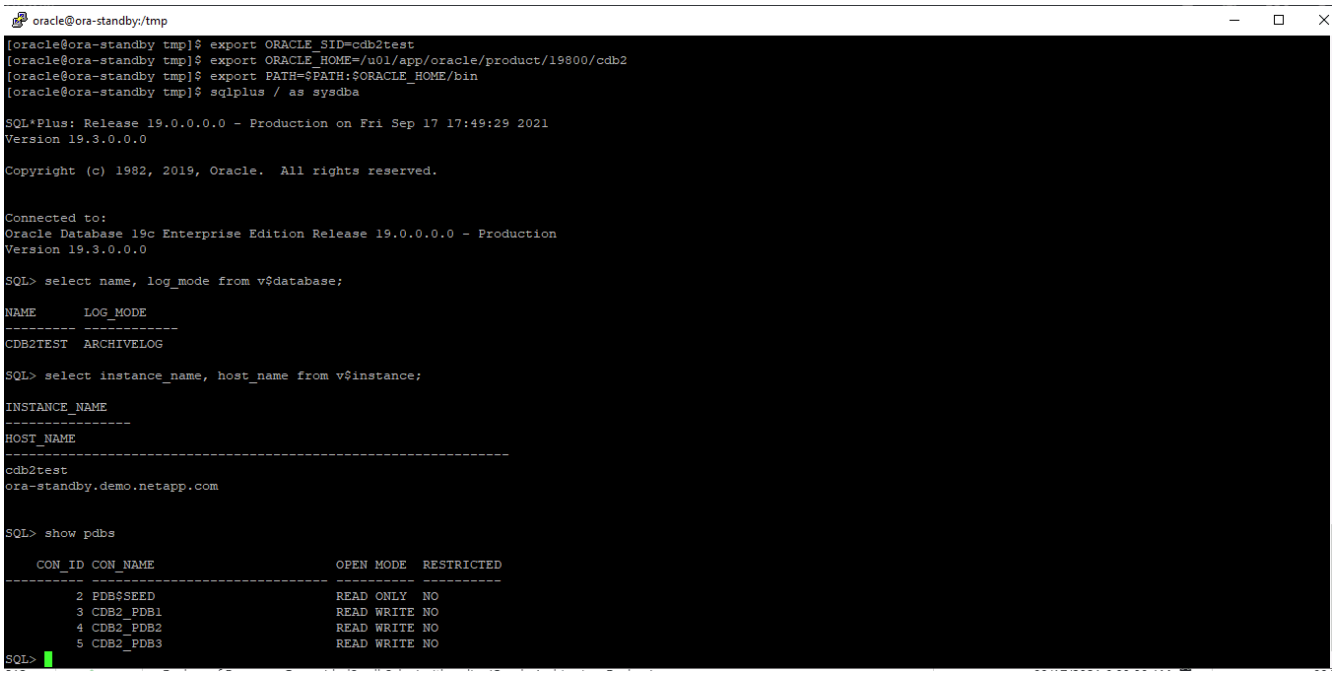
11. Configure o servidor SMTP para notificação por email, se desejar.



12. Resumo do clone.

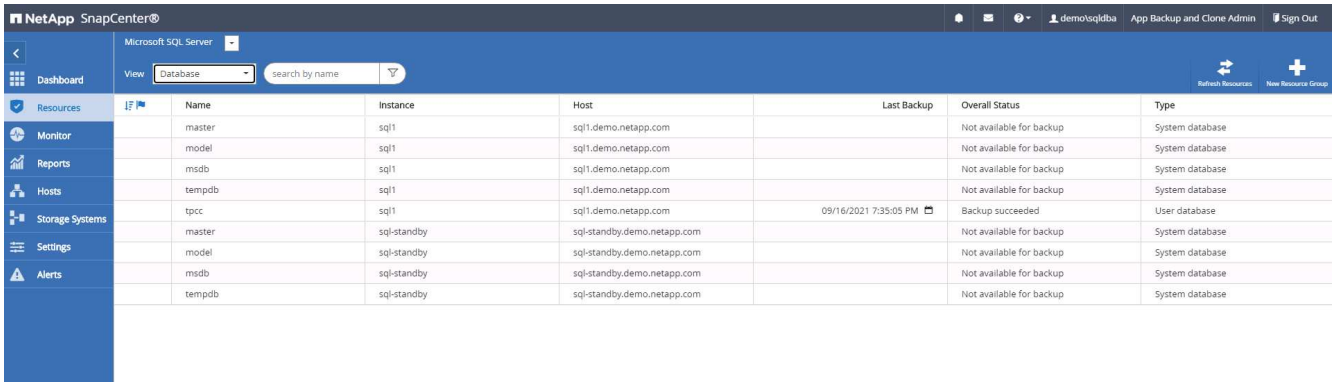


13. Você deve validar após a clonagem para ter certeza de que o banco de dados clonado está operacional. Algumas tarefas adicionais, como iniciar o listener ou desativar o modo de arquivamento de log do BD, podem ser executadas no banco de dados dev/test.

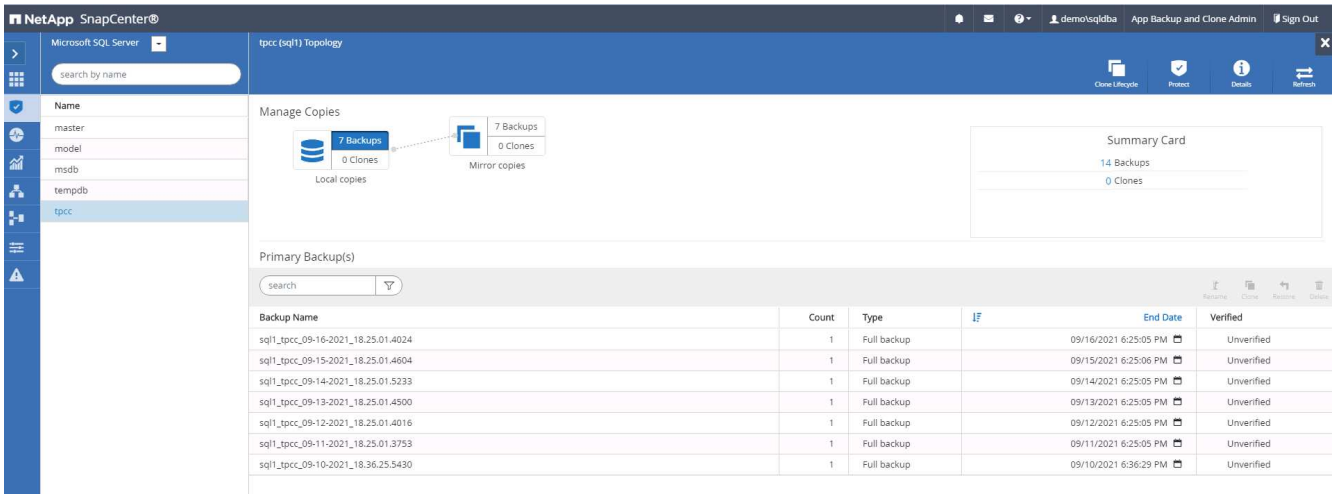


Clonar um banco de dados SQL para desenvolvimento/teste a partir de um backup de Snapshot replicado

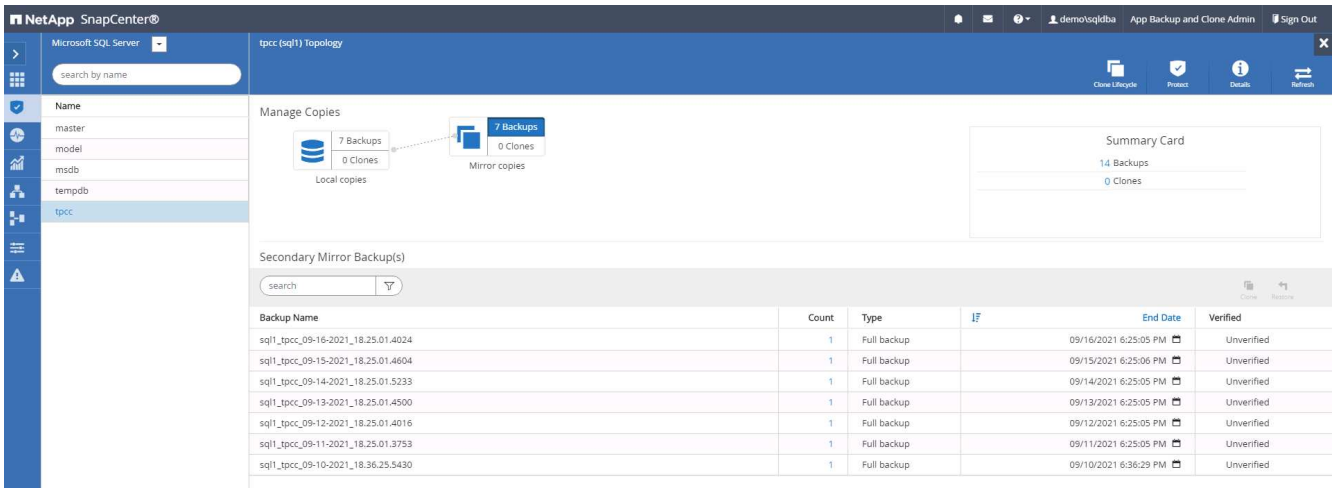
1. Efetue login no SnapCenter com uma ID de usuário de gerenciamento de banco de dados do SQL Server. Navegue até a guia Recursos, que mostra os bancos de dados do usuário do SQL Server sendo protegidos pelo SnapCenter e uma instância SQL de espera de destino na nuvem pública.



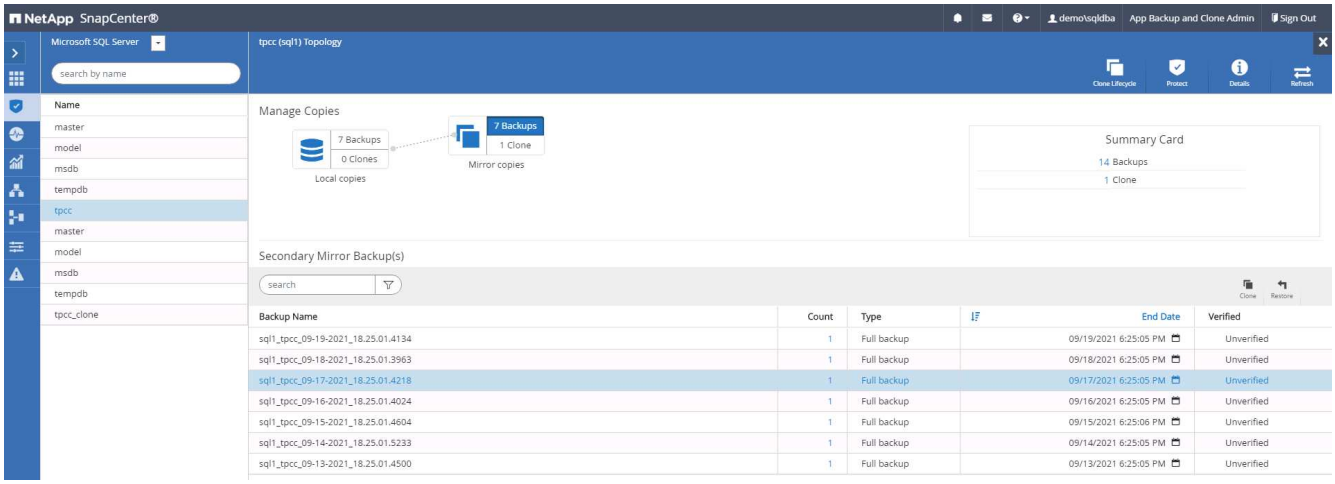
2. Clique no nome do banco de dados do usuário do SQL Server local pretendido para obter a topologia dos backups e a exibição detalhada. Se um local replicado secundário estiver habilitado, ele mostrará backups espelhados vinculados.

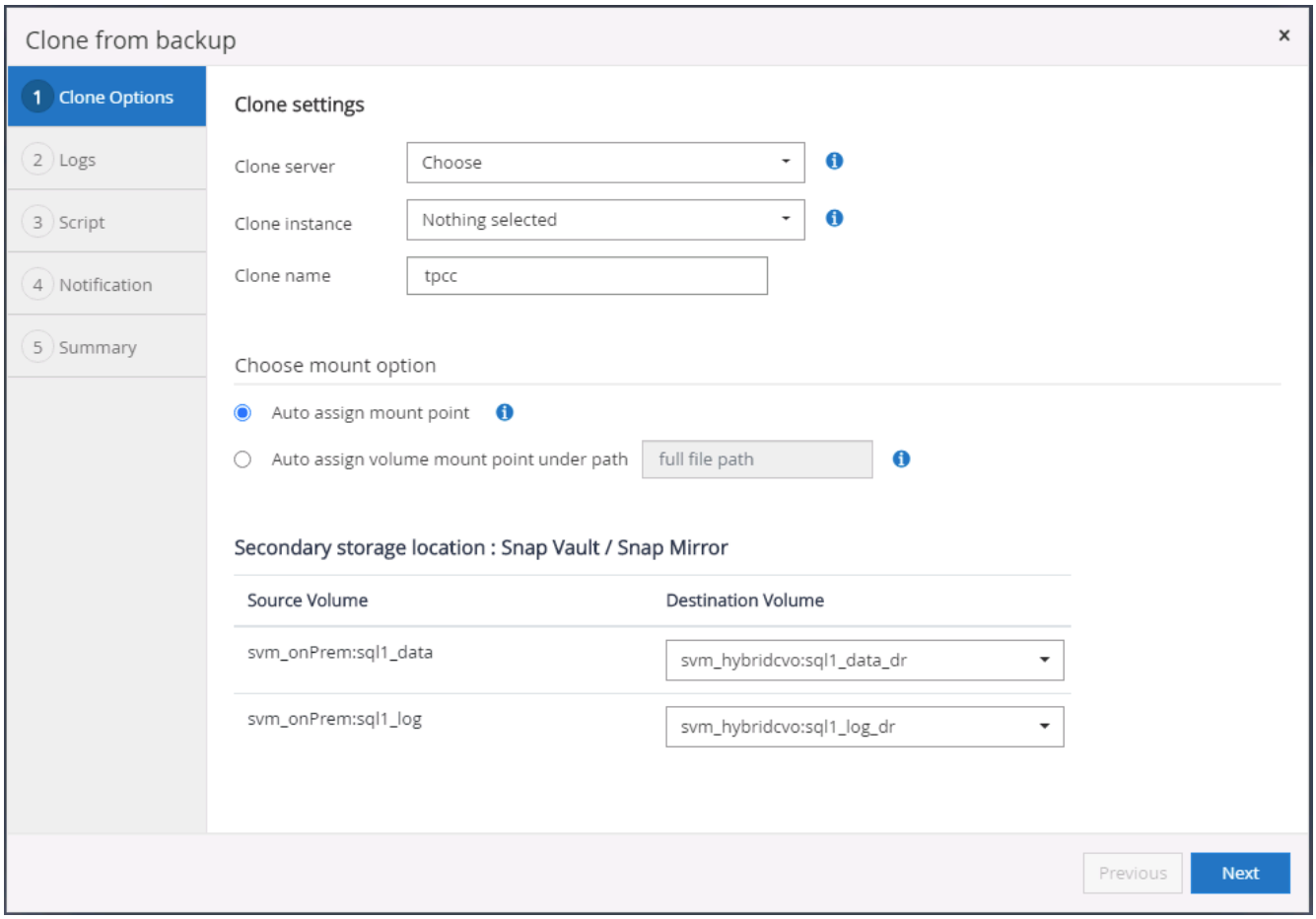


3. Alterne para a visualização Backups espelhados clicando em Backups espelhados. Os backups do espelho secundário são exibidos. Como o SnapCenter faz backup do log de transações do SQL Server em uma unidade dedicada para recuperação, somente backups completos do banco de dados são exibidos aqui.

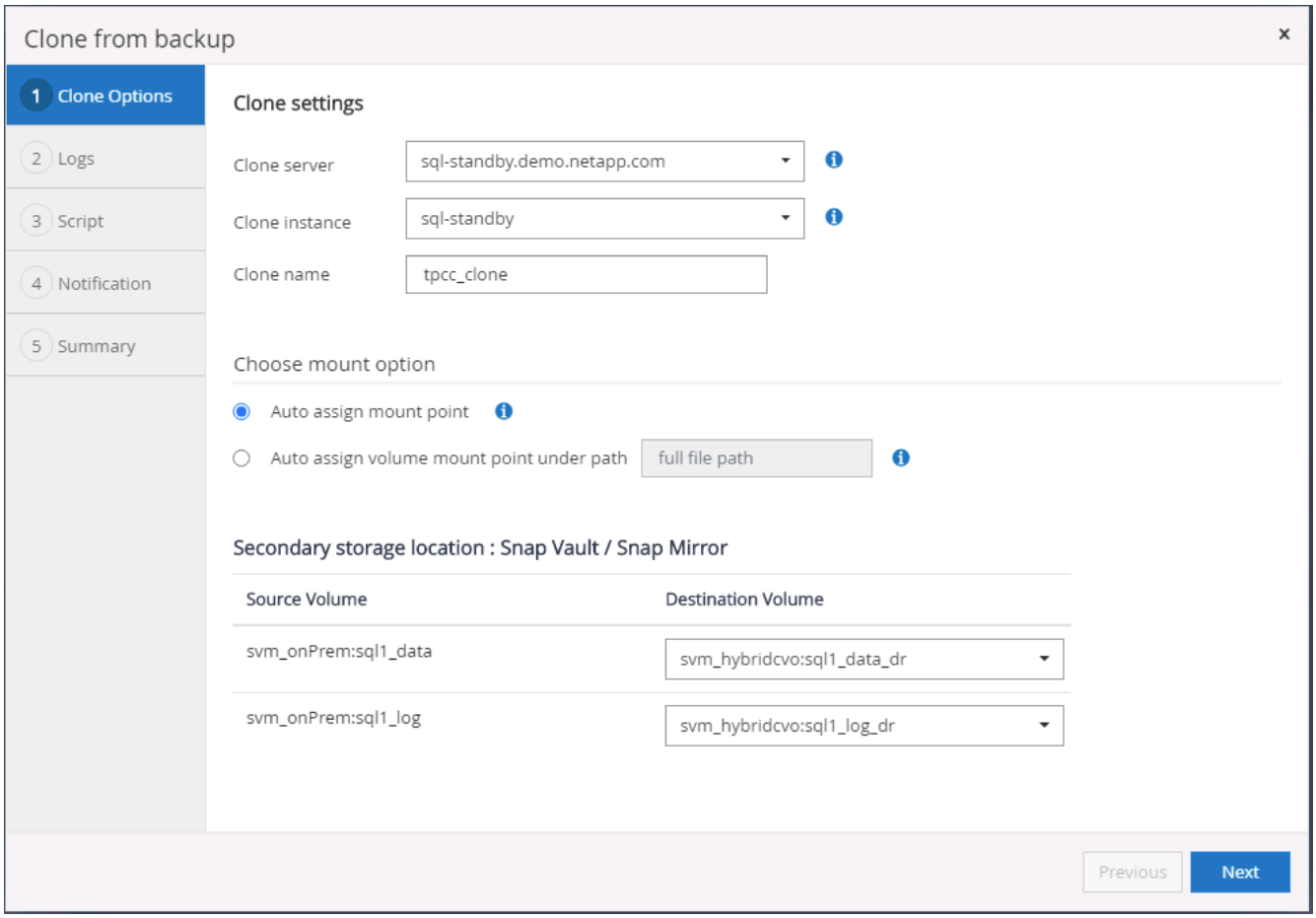


4. Escolha uma cópia de backup e clique no botão Clonar para iniciar o fluxo de trabalho Clonar do backup.

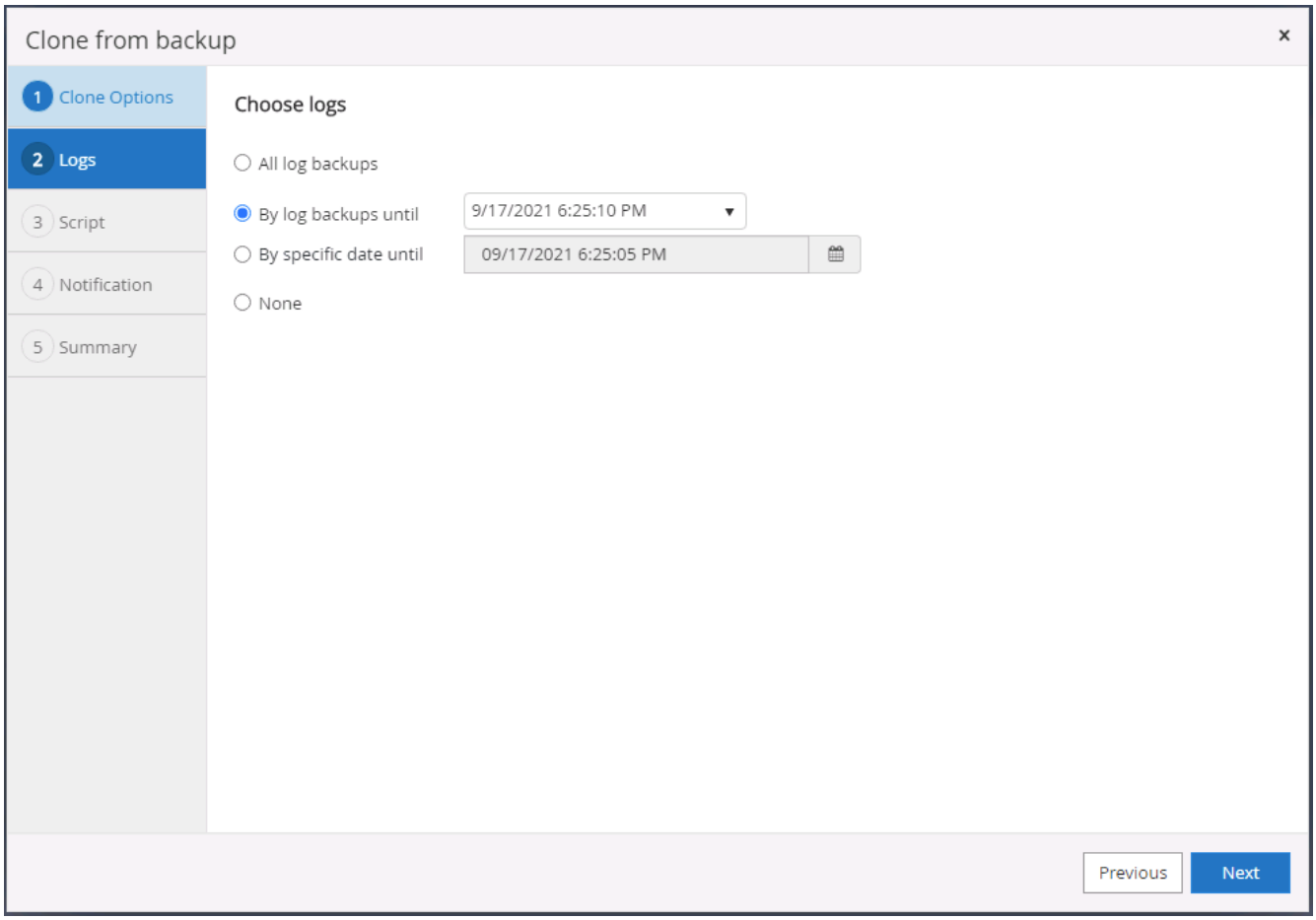




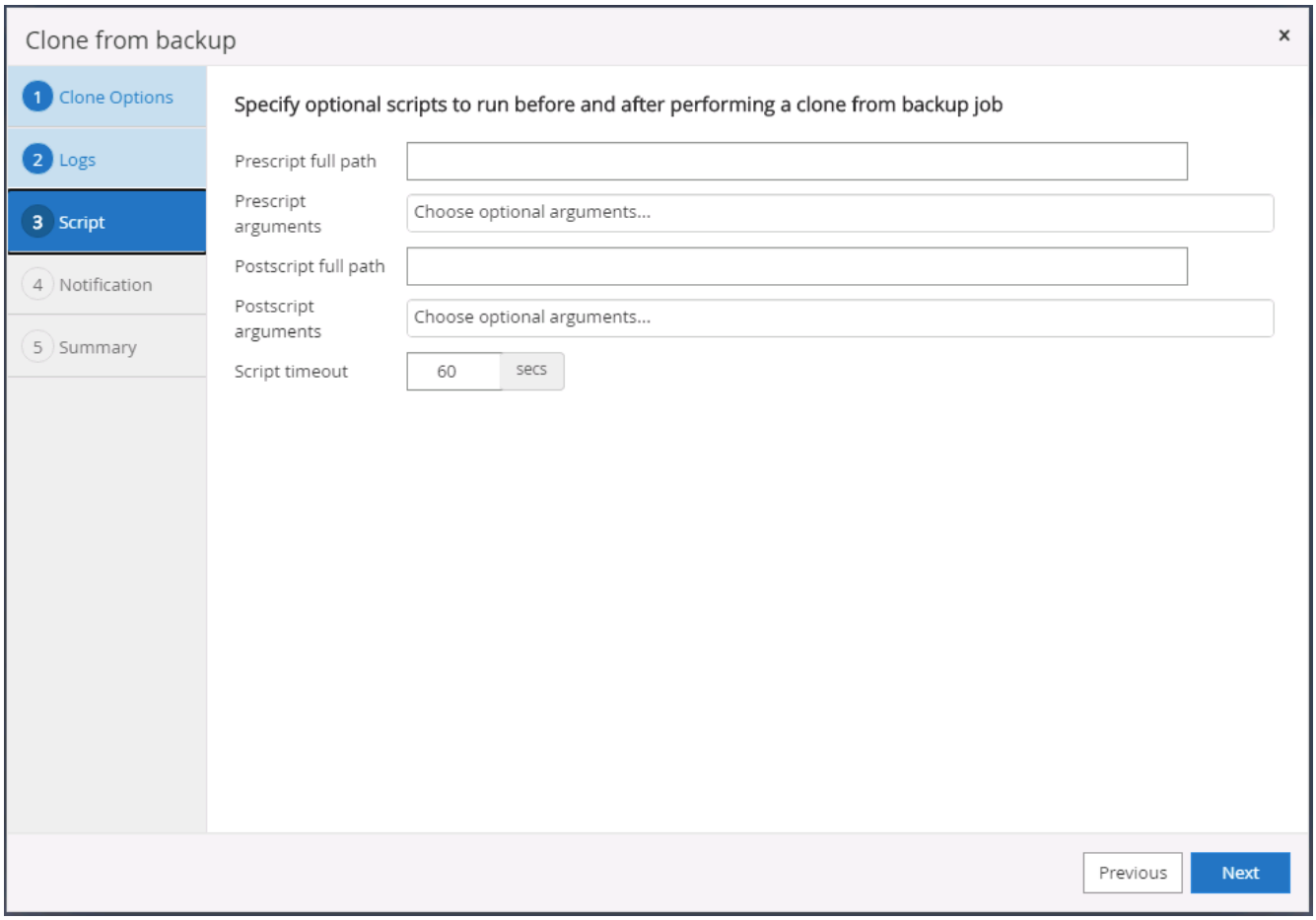
5. Selecione um servidor de nuvem como o servidor clone de destino, o nome da instância clone e o nome do banco de dados clone. Escolha um ponto de montagem de atribuição automática ou um caminho de ponto de montagem definido pelo usuário.



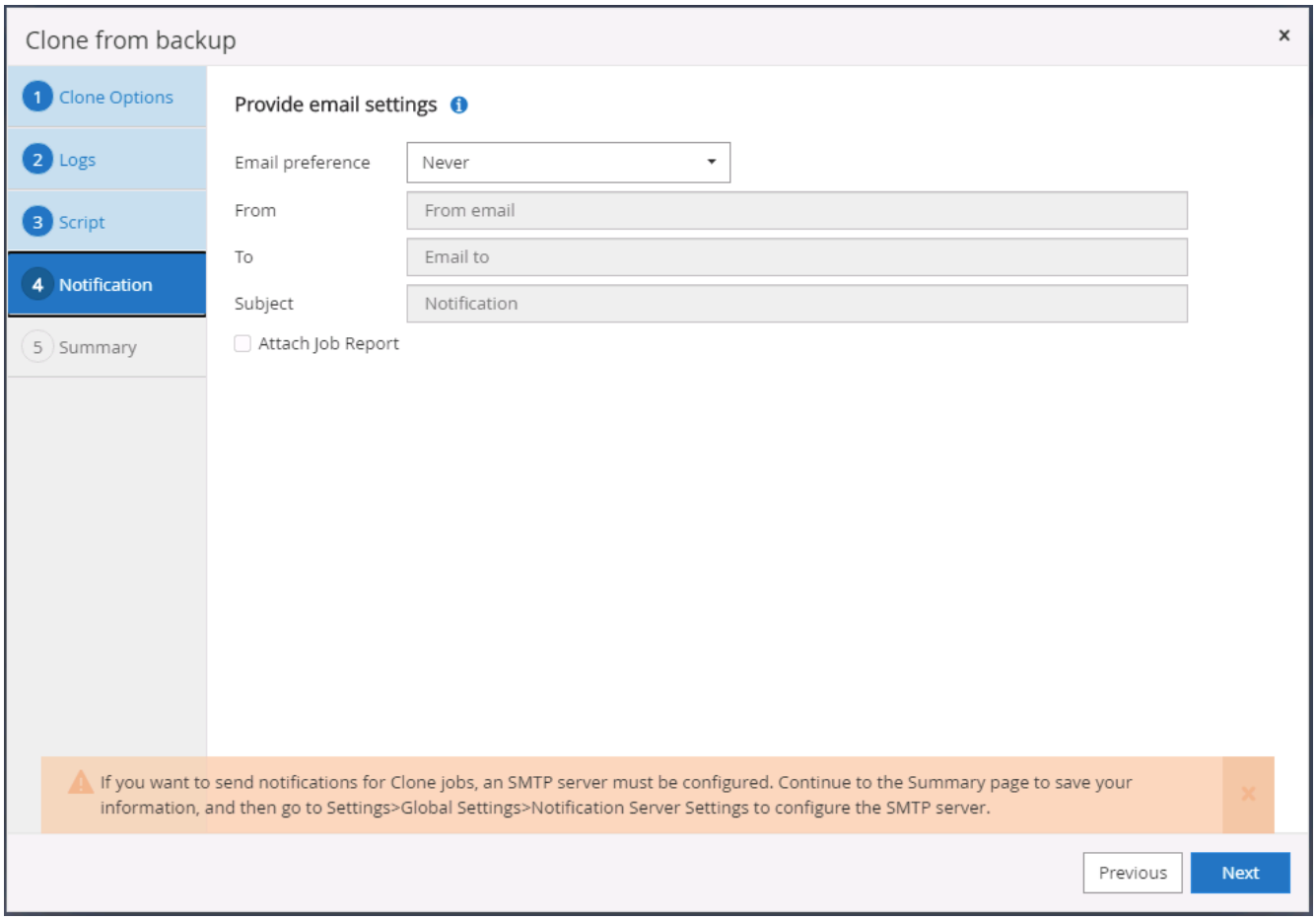
6. Determine um ponto de recuperação por um horário de backup de log ou por uma data e hora específicas.



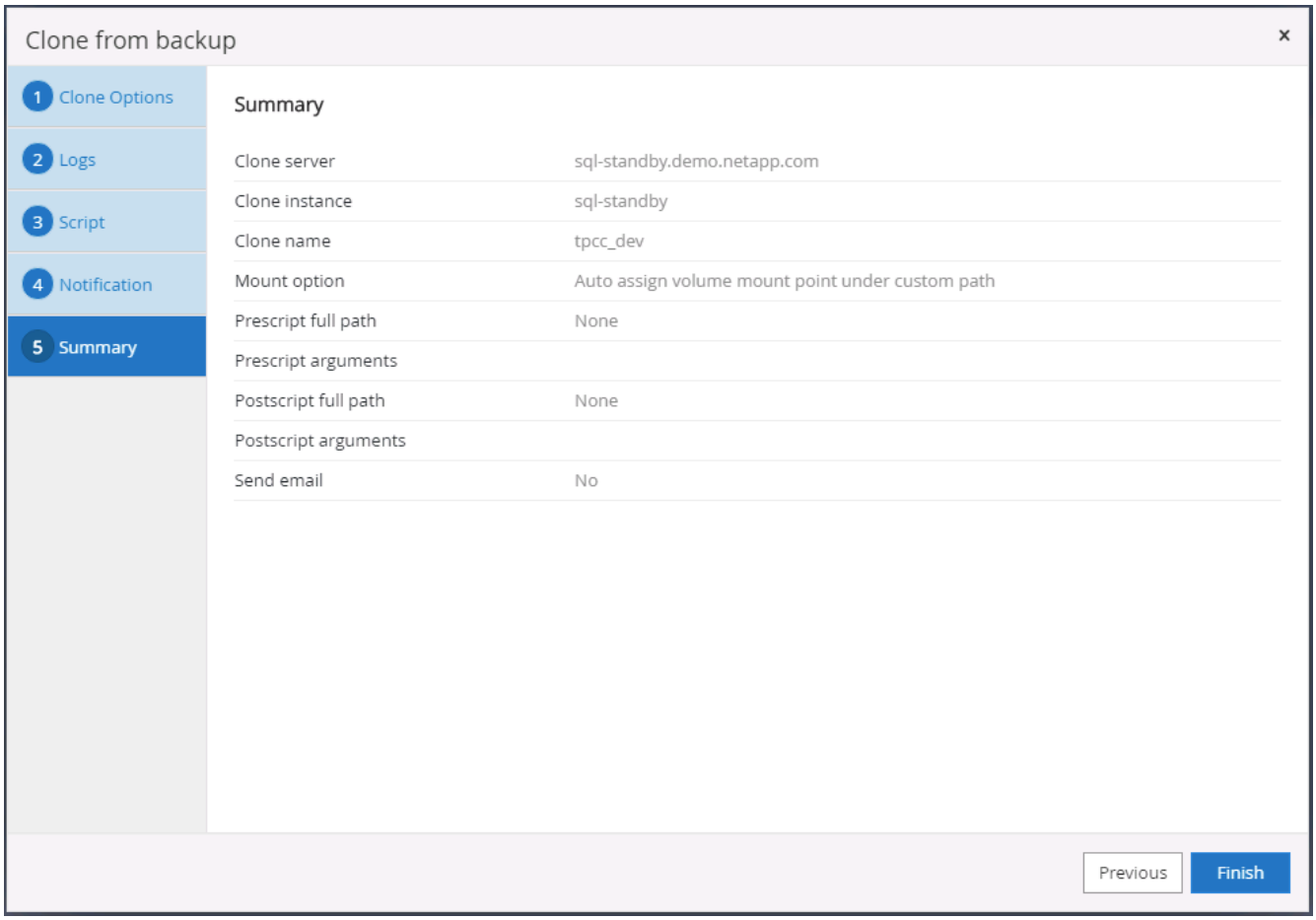
7. Especifique scripts opcionais para serem executados antes e depois da operação de clonagem.



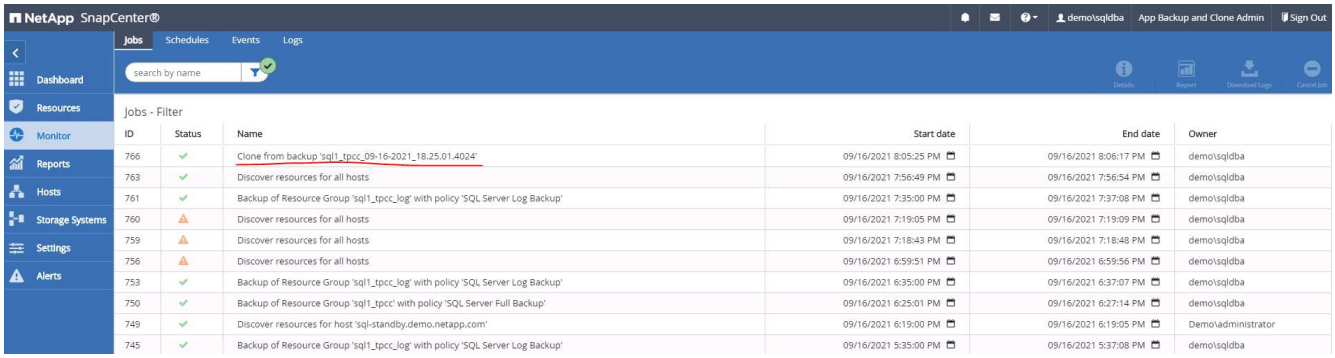
8. Configure um servidor SMTP se desejar receber notificações por e-mail.



9. Resumo do clone.



10. Monitore o status do trabalho e valide se o banco de dados do usuário pretendido foi anexado a uma instância SQL de destino no servidor clone da nuvem.



Configuração pós-clone

1. Um banco de dados de produção Oracle local geralmente é executado no modo de arquivamento de log. Este modo não é necessário para um banco de dados de desenvolvimento ou teste. Para desativar o modo de arquivamento de log, efetue login no Oracle DB como sysdba, execute um comando de alteração do modo de log e inicie o banco de dados para acesso.
2. Configure um listener Oracle ou registre o banco de dados recém-clonado com um listener existente para acesso do usuário.
3. Para o SQL Server, altere o modo de log de Completo para Fácil para que o arquivo de log de desenvolvimento/teste do SQL Server possa ser facilmente reduzido quando estiver preenchendo o volume de log.

Atualizar banco de dados clone

1. Elimine bancos de dados clonados e limpe o ambiente do servidor de banco de dados na nuvem. Em seguida, siga os procedimentos anteriores para clonar um novo banco de dados com dados atualizados. Leva apenas alguns minutos para clonar um novo banco de dados.
2. Desligue o banco de dados clone e execute um comando de atualização do clone usando a CLI. Consulte a seguinte documentação do SnapCenter para obter detalhes:"Atualizar um clone" .

Onde procurar ajuda?

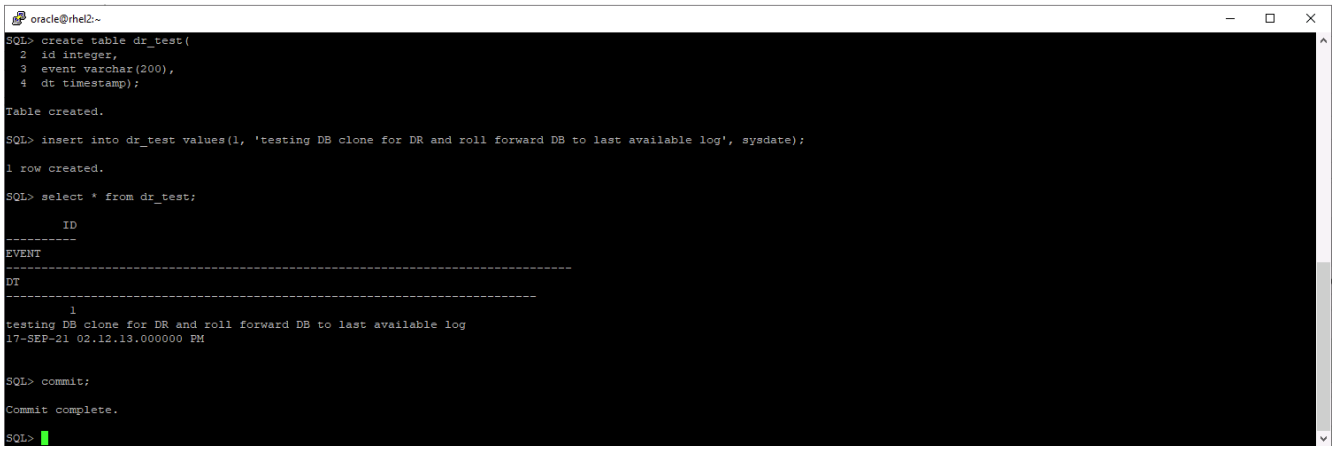
Se precisar de ajuda com esta solução e casos de uso, junte-se a"Canal do Slack de suporte da comunidade de automação de soluções da NetApp" e procure o canal de automação de soluções para postar suas dúvidas ou perguntas.

Fluxo de trabalho de recuperação de desastres

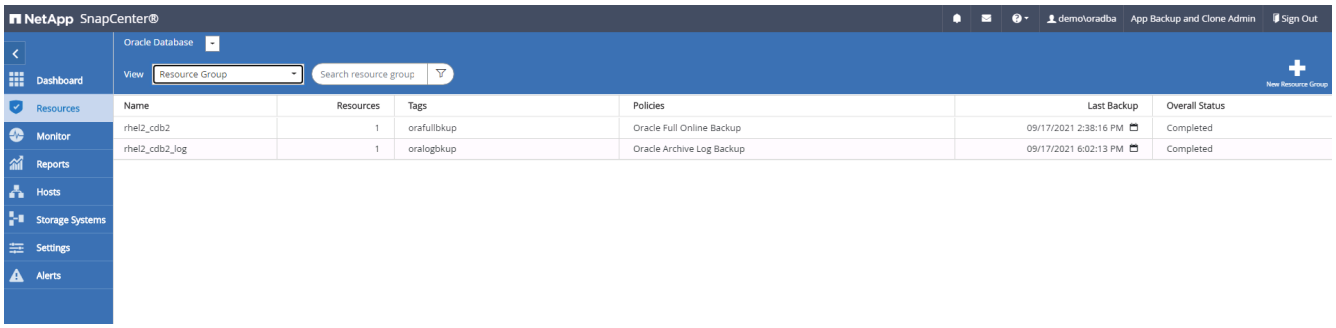
As empresas adotaram a nuvem pública como um recurso viável e destino para recuperação de desastres. O SnapCenter torna esse processo o mais simples possível. Este fluxo de trabalho de recuperação de desastres é muito semelhante ao fluxo de trabalho de clone, mas a recuperação do banco de dados é executada no último log disponível que foi replicado na nuvem para recuperar todas as transações comerciais possíveis. No entanto, há etapas adicionais de pré-configuração e pós-configuração específicas para recuperação de desastres.

Clonar um banco de dados de produção Oracle local para a nuvem para recuperação de desastres

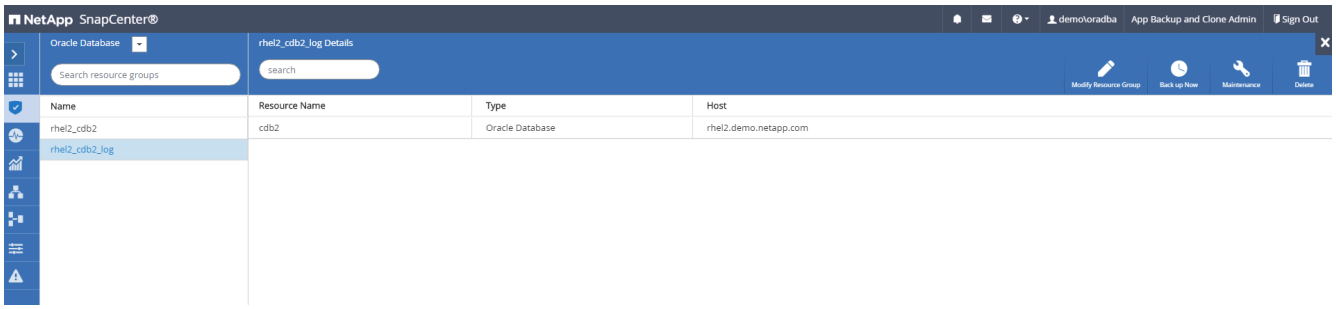
1. Para validar se a recuperação do clone é executada pelo último log disponível, criamos uma pequena tabela de teste e inserimos uma linha. Os dados de teste seriam recuperados após uma recuperação completa do último log disponível.

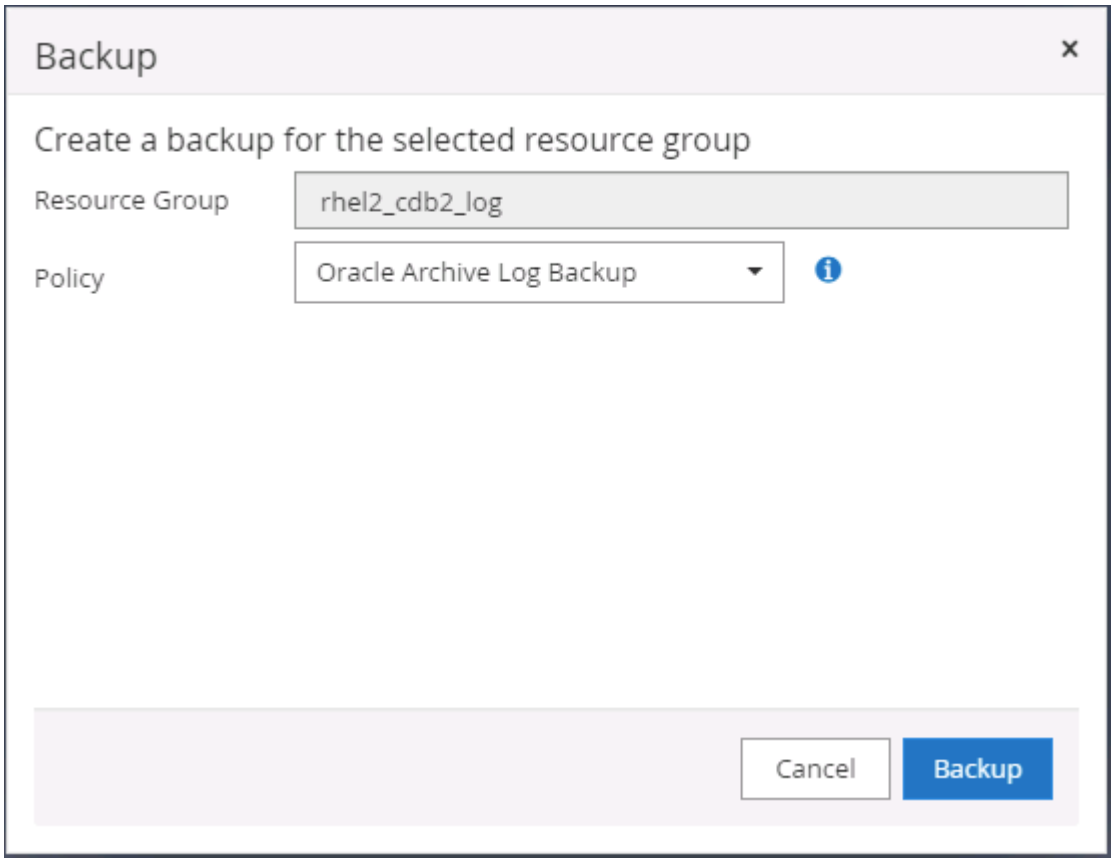


2. Efetue login no SnapCenter como um ID de usuário de gerenciamento de banco de dados do Oracle. Navegue até a guia Recursos, que mostra os bancos de dados Oracle sendo protegidos pelo SnapCenter.



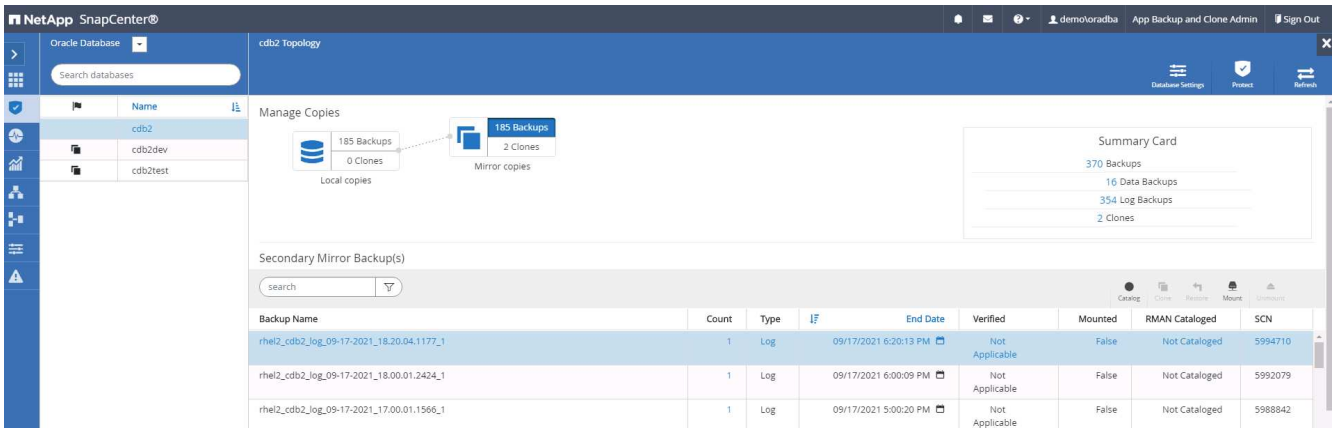
3. Selecione o grupo de recursos de log do Oracle e clique em Fazer backup agora para executar manualmente um backup de log do Oracle para liberar a transação mais recente para o destino na nuvem. Em um cenário de DR real, a última transação recuperável depende da frequência de replicação do volume de log do banco de dados para a nuvem, que por sua vez depende da política de RTO ou RPO da empresa.

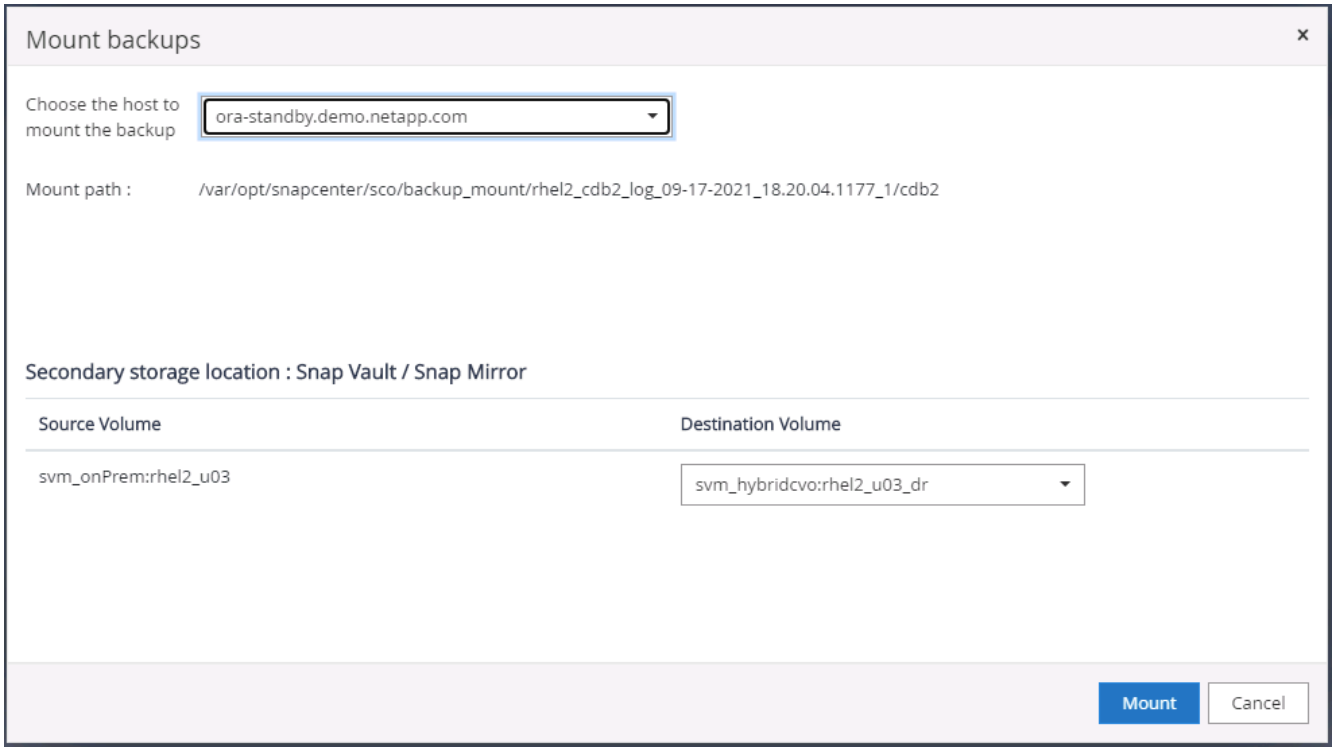




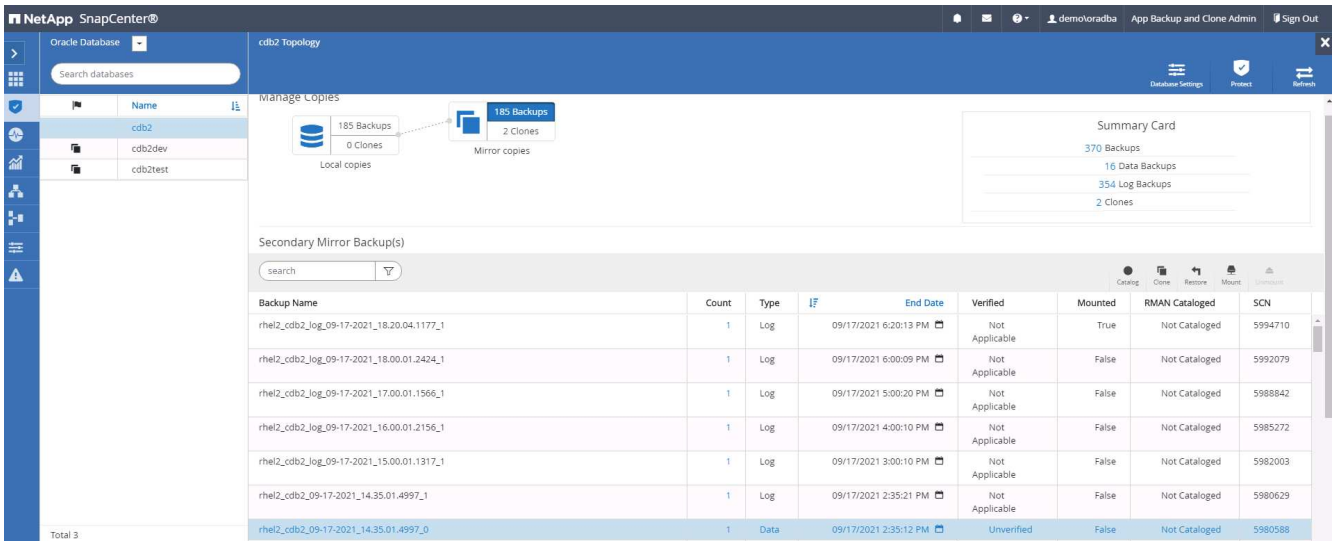
O SnapMirror assíncrono perde dados que não chegaram ao destino na nuvem no intervalo de backup do log do banco de dados em um cenário de recuperação de desastre. Para minimizar a perda de dados, é possível agendar backups de log mais frequentes. No entanto, há um limite para a frequência de backup de log que é tecnicamente possível.

4. Selecione o último backup de log no(s) Backup(s) de Espelho Secundário e monte o backup de log.

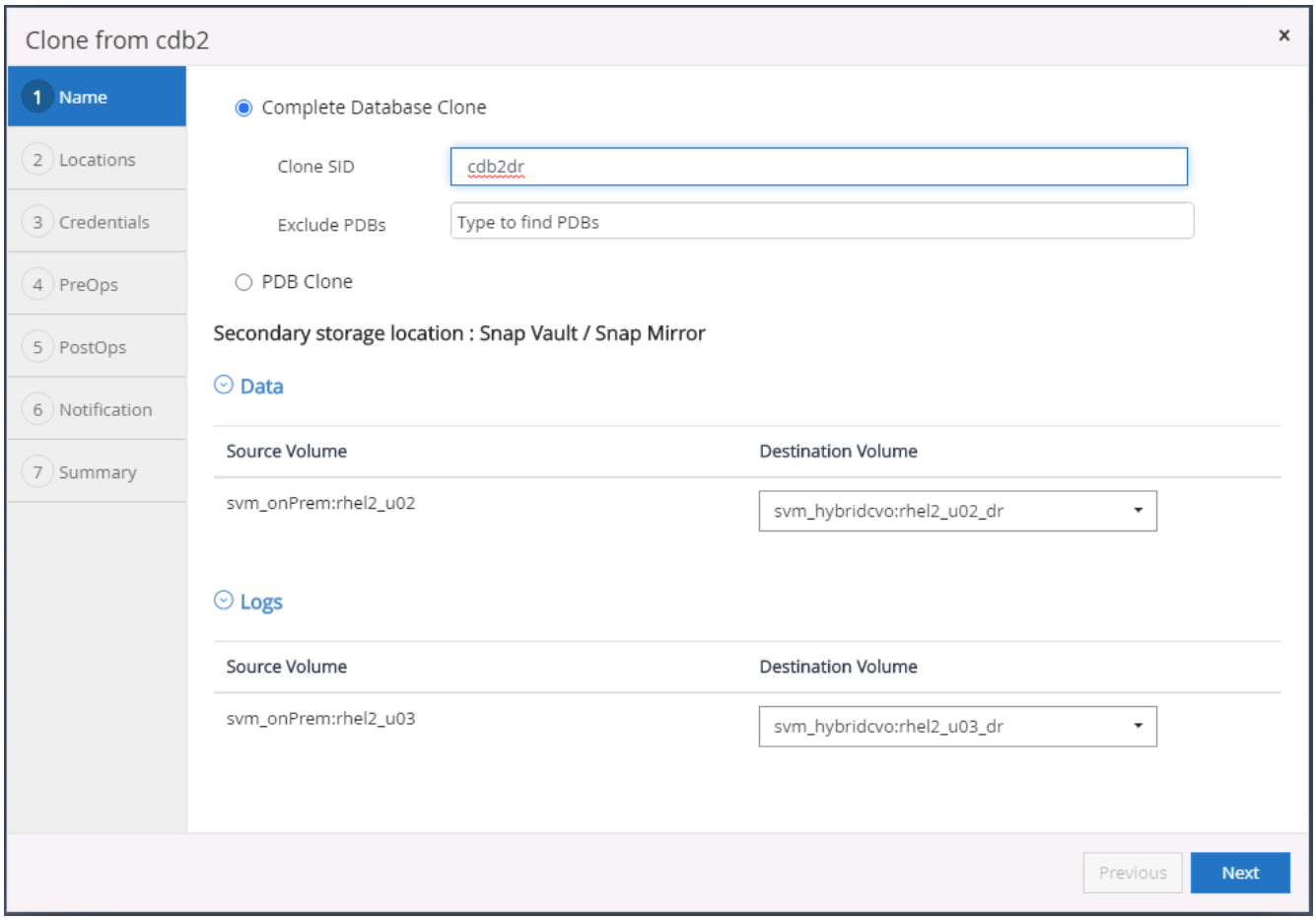




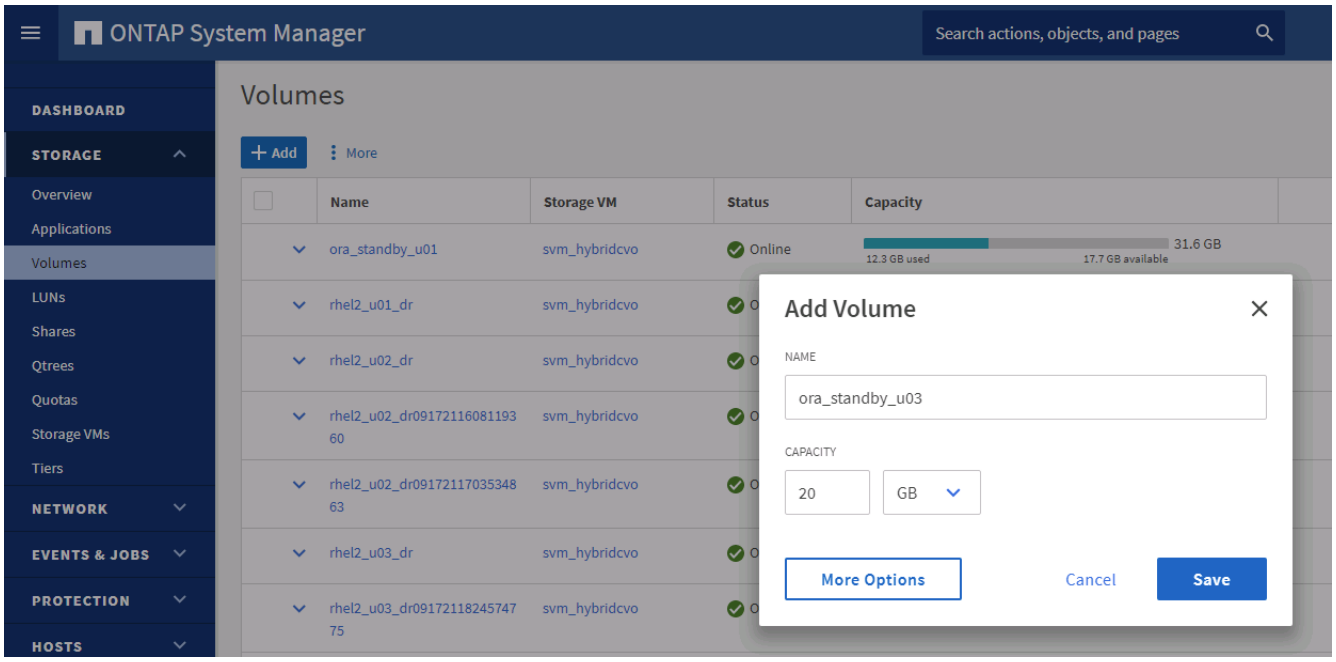
5. Selecione o último backup completo do banco de dados e clique em Clonar para iniciar o fluxo de trabalho de clonagem.

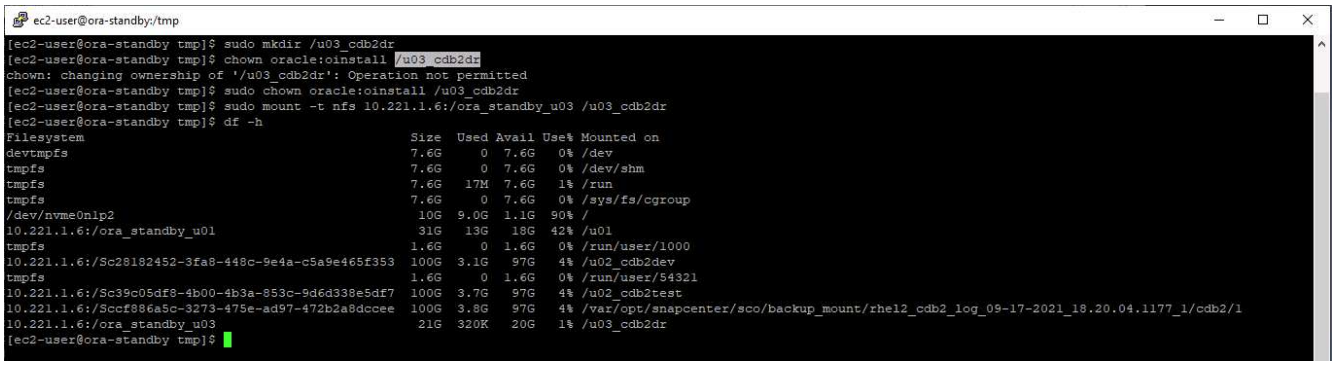


6. Selecione um ID de banco de dados clone exclusivo no host.



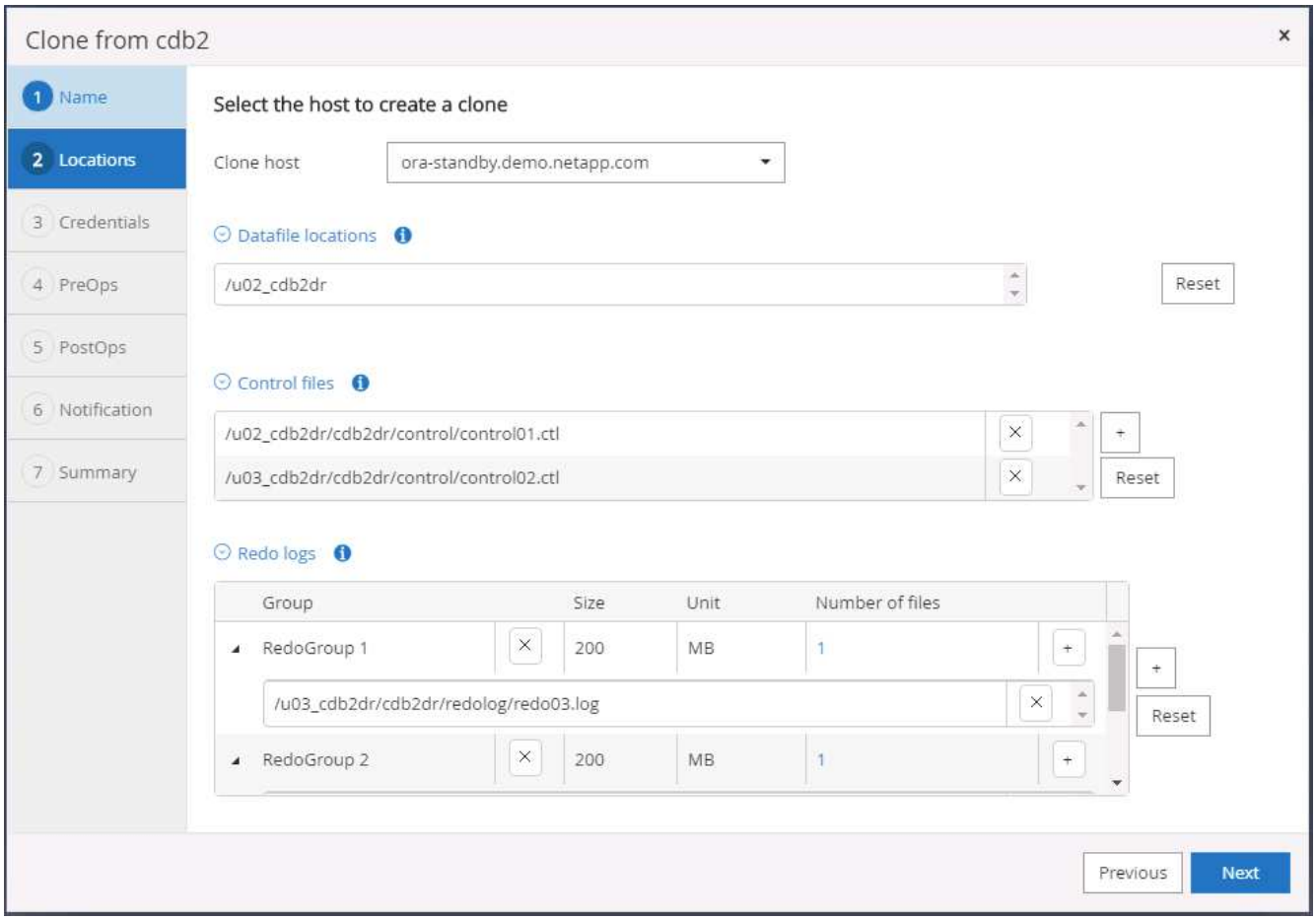
7. Provisione um volume de log e monte-o no servidor DR de destino para a área de recuperação flash do Oracle e logs on-line.



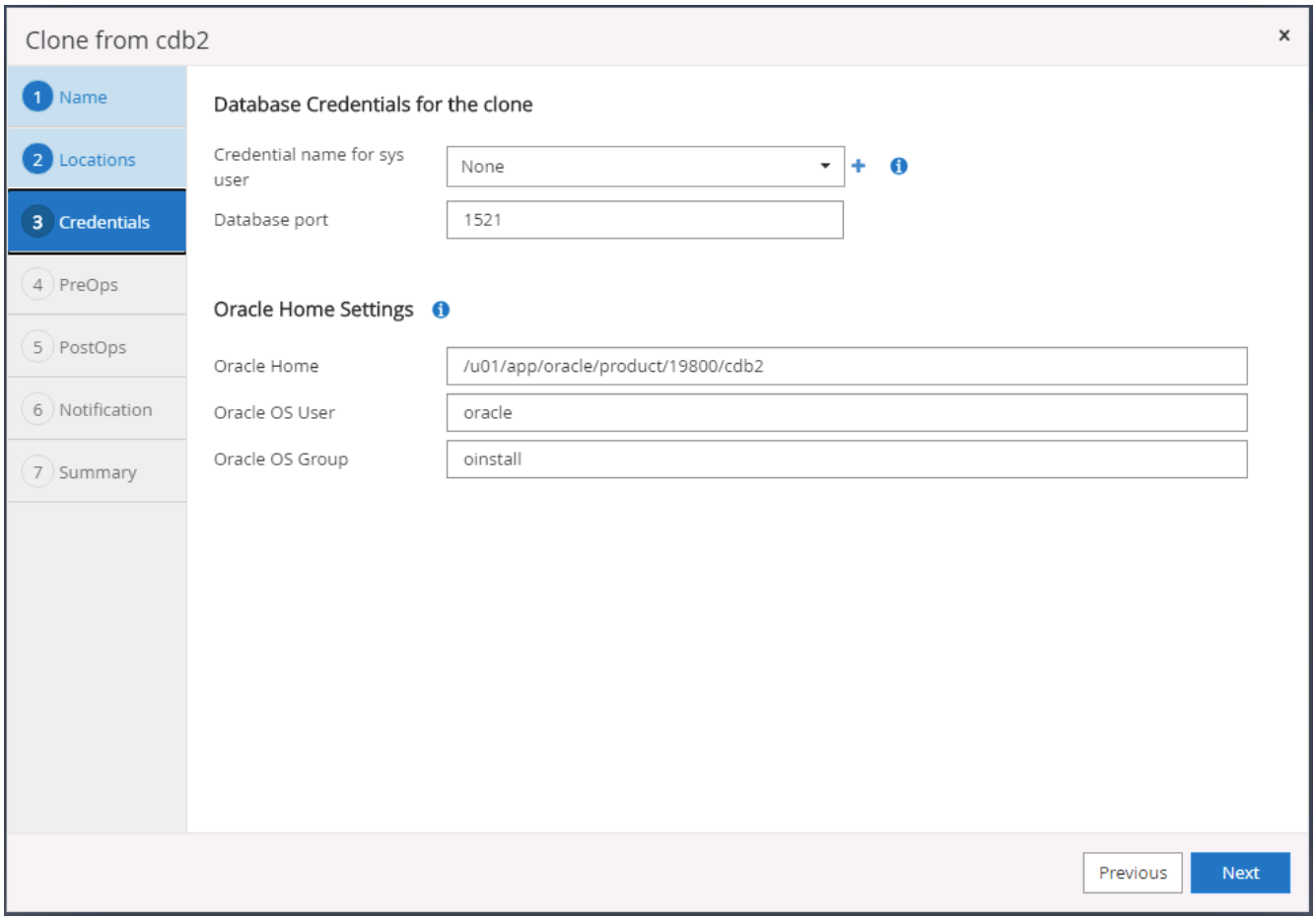


> O procedimento de clonagem do Oracle não cria um volume de log, que precisa ser provisionado no servidor DR antes da clonagem.

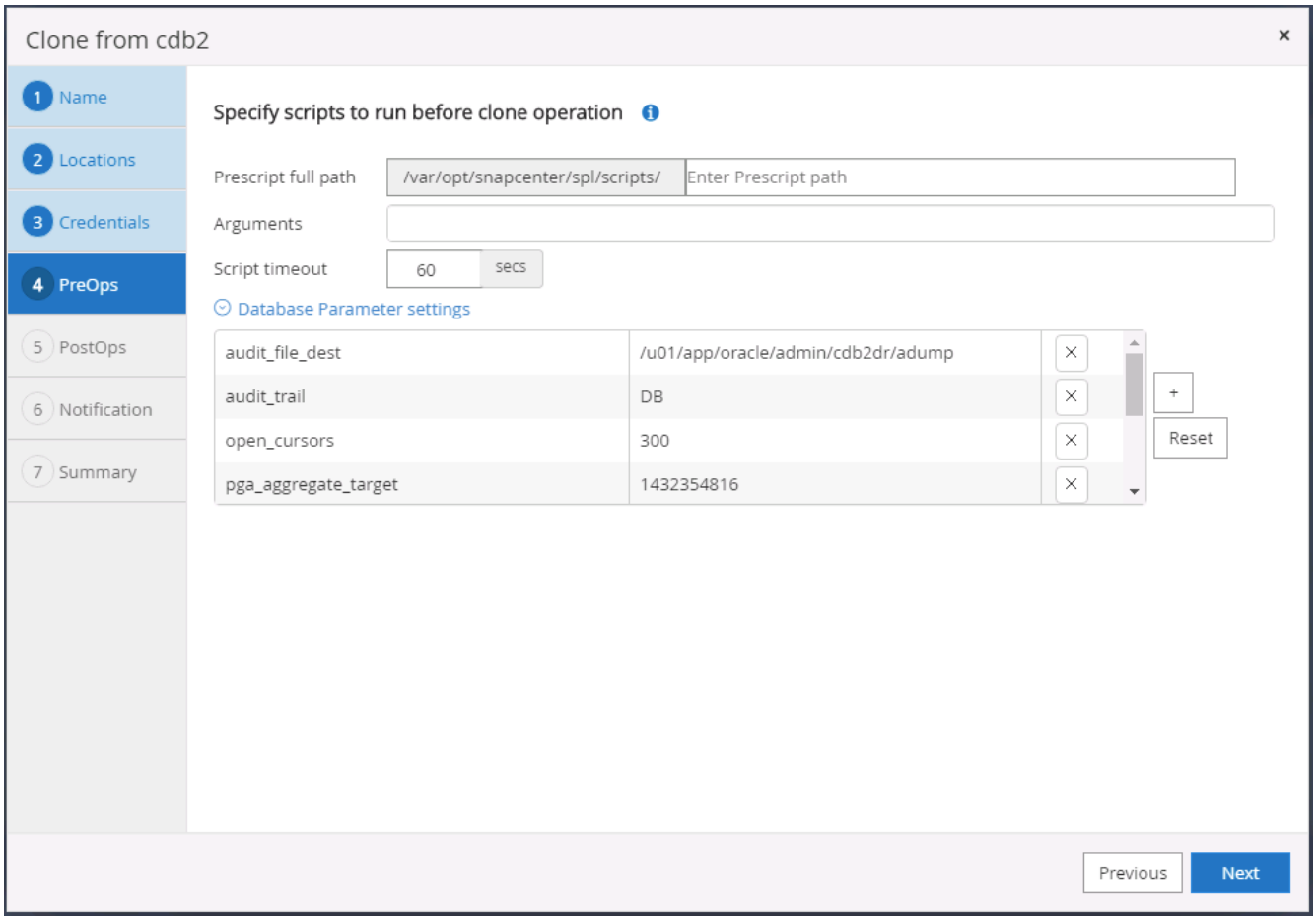
8. Selecione o host do clone de destino e o local para colocar os arquivos de dados, arquivos de controle e logs de refazer.



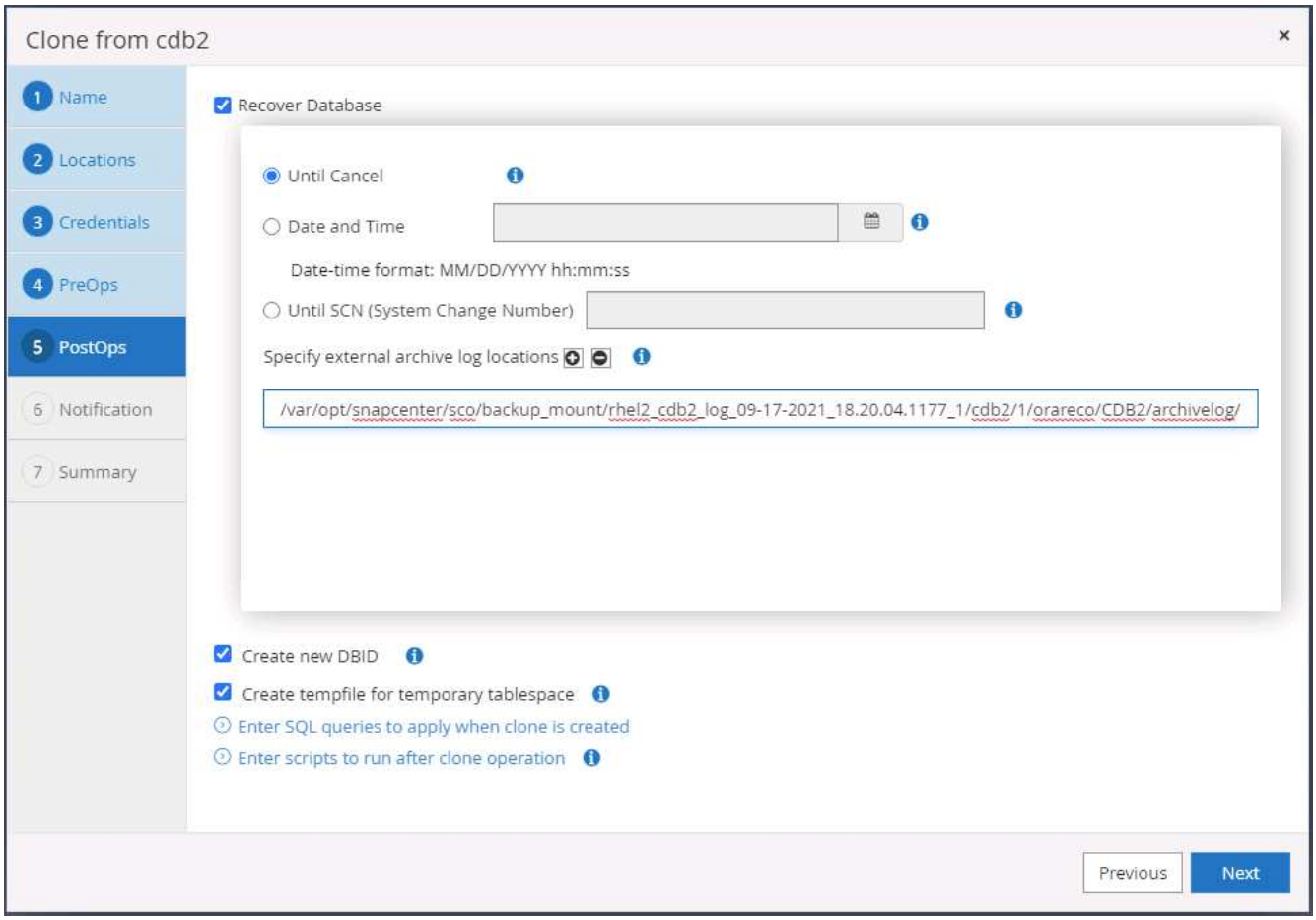
9. Selecione as credenciais para o clone. Preencha os detalhes da configuração inicial do Oracle no servidor de destino.



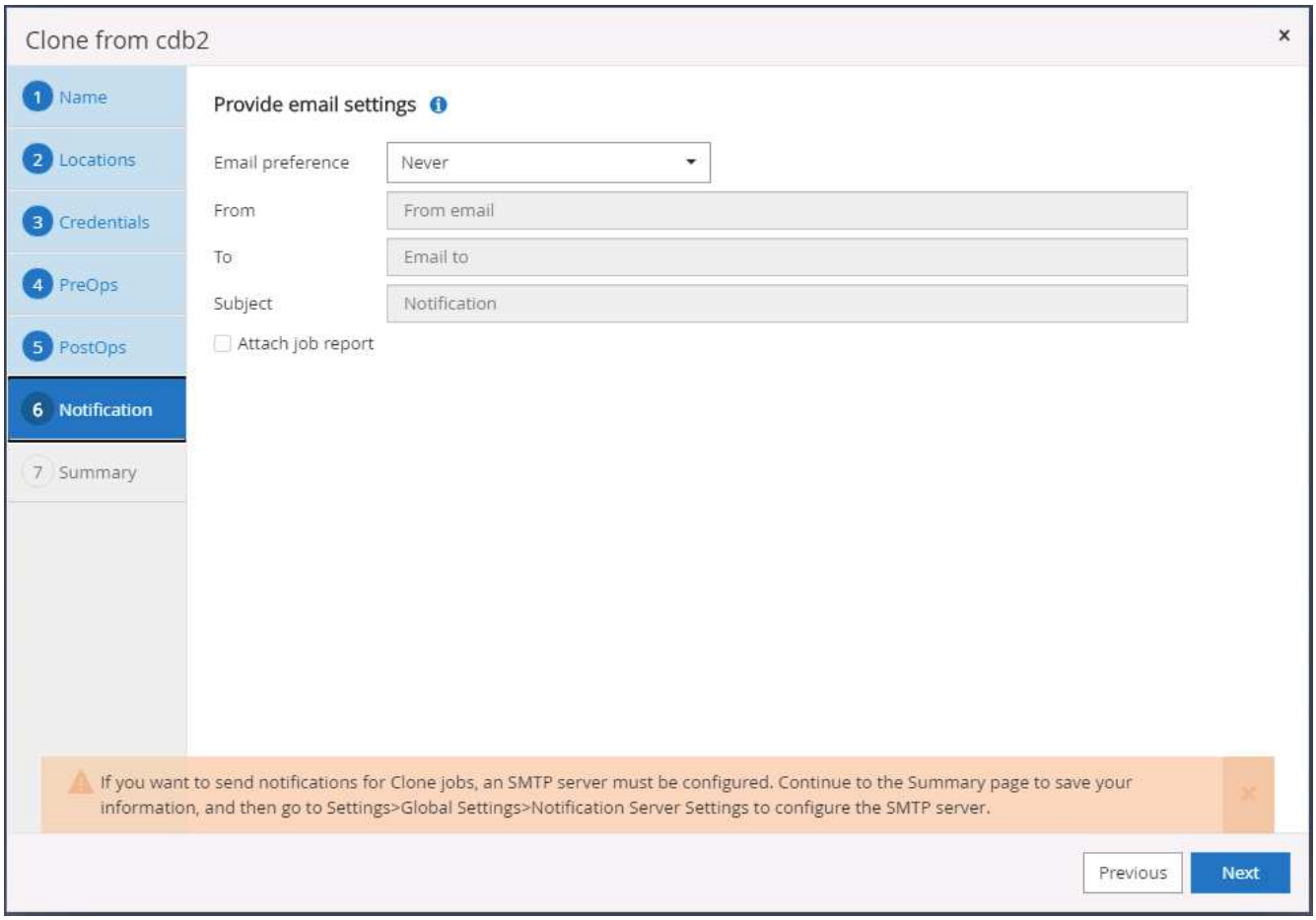
10. Especifique os scripts a serem executados antes da clonagem. Os parâmetros do banco de dados podem ser ajustados, se necessário.



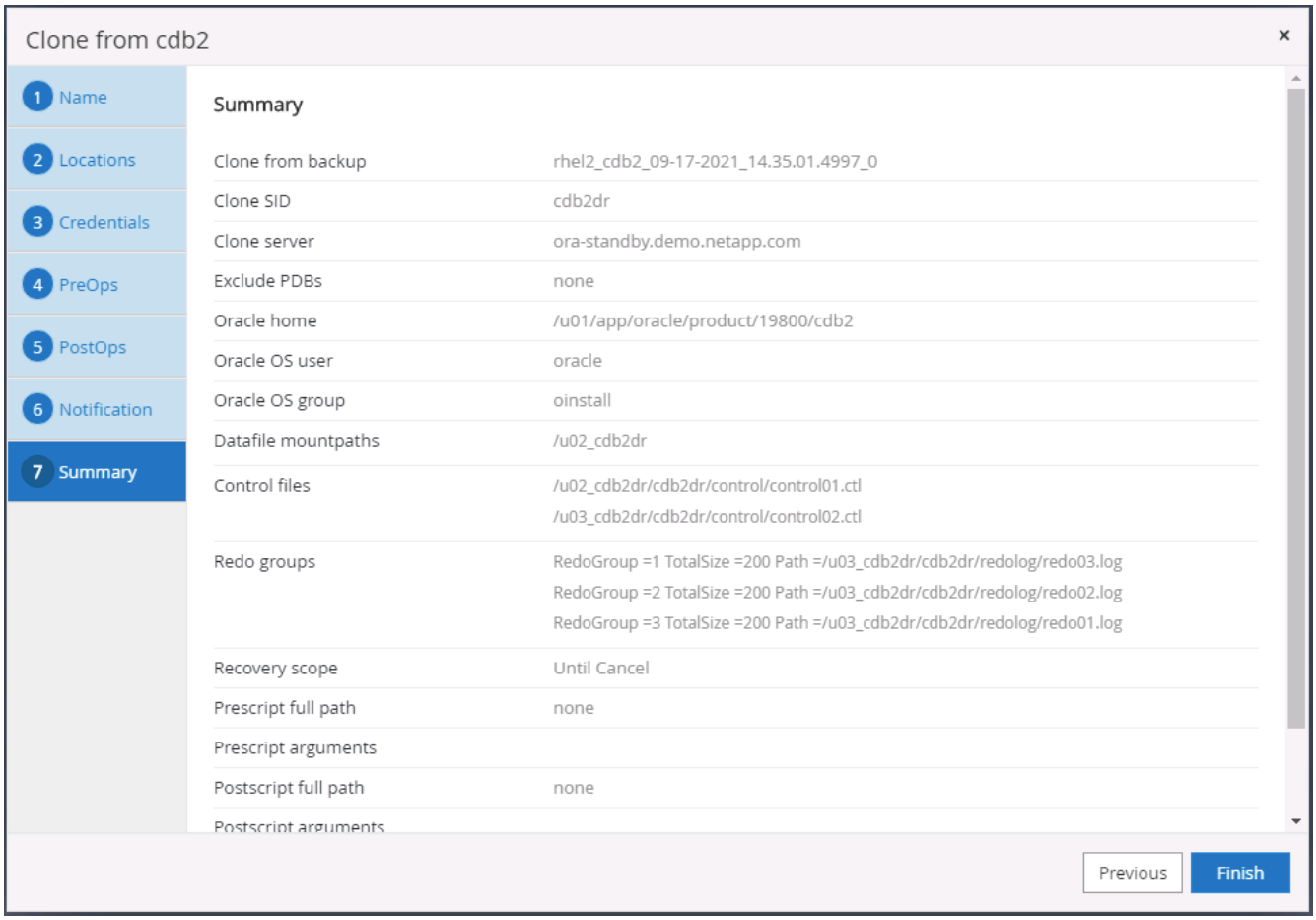
11. Selecione Até Cancelar como a opção de recuperação para que a recuperação seja executada em todos os logs de arquivamento disponíveis para recuperar a última transação replicada no local da nuvem secundária.



12. Configure o servidor SMTP para notificação por email, se necessário.



13. Resumo do clone DR.



14. Os bancos de dados clonados são registrados no SnapCenter imediatamente após a conclusão da clonagem e ficam então disponíveis para proteção de backup.

Validação e configuração de clone pós-DR para Oracle

1. Valide a última transação de teste que foi liberada, replicada e recuperada no local de DR na nuvem.

```
oracle@ora-standby:/u01/app/oracle/product/19800/cdb2/dbs
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> set lin 200
SQL> select instance_name, host_name from v$instance;

INSTANCE_NAME    HOST_NAME
---------------- ----------------------------------------------------------------
cdb2dr           ora-standby.demo.netapp.com

SQL> alter pluggable database cdb2_pdb1 open;

Pluggable database altered.

SQL> alter session set container=cdb2_pdb1;

Session altered.

SQL> select * from pdbadmin.dr_test;

        ID
----------
EVENT
--------------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------
DT
---------------------------------------------------------------------------
         1
testing DB clone for DR and roll forward DB to last available log
17-SEP-21 02.12.13.000000 PM


SQL>
```

2. Configure a área de recuperação do flash.

```
oracle@ora-standby:/u01/app/oracle/product/19800/cdb2/dbs
[oracle@ora-standby dbs]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Sep 17 22:07:11 2021
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> show parameter db_recovery_file_dest

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
db_recovery_file_dest                string
db_recovery_file_dest_size           big integer 17208M
SQL> alter system set db_recovery_file_dest='/u03_cdb2dr/cdb2dr' scope=both;

System altered.

SQL> show parameter db_recovery_file_dest

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
db_recovery_file_dest                string      /u03_cdb2dr/cdb2dr
db_recovery_file_dest_size           big integer 17208M
SQL>
```

3. Configure o ouvinte Oracle para acesso do usuário.
4. Divida o volume clonado do volume de origem replicado.
5. Reverta a replicação da nuvem para o local e reconstrua o servidor de banco de dados local com falha.

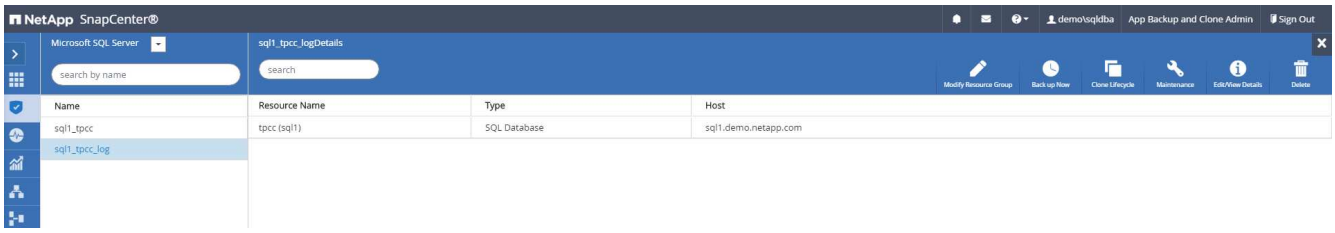
> A divisão de clones pode incorrer em utilização temporária de espaço de armazenamento muito maior que a operação normal. No entanto, depois que o servidor de banco de dados local for reconstruído, espaço extra poderá ser liberado.

Clonar um banco de dados de produção SQL local para a nuvem para recuperação de desastres

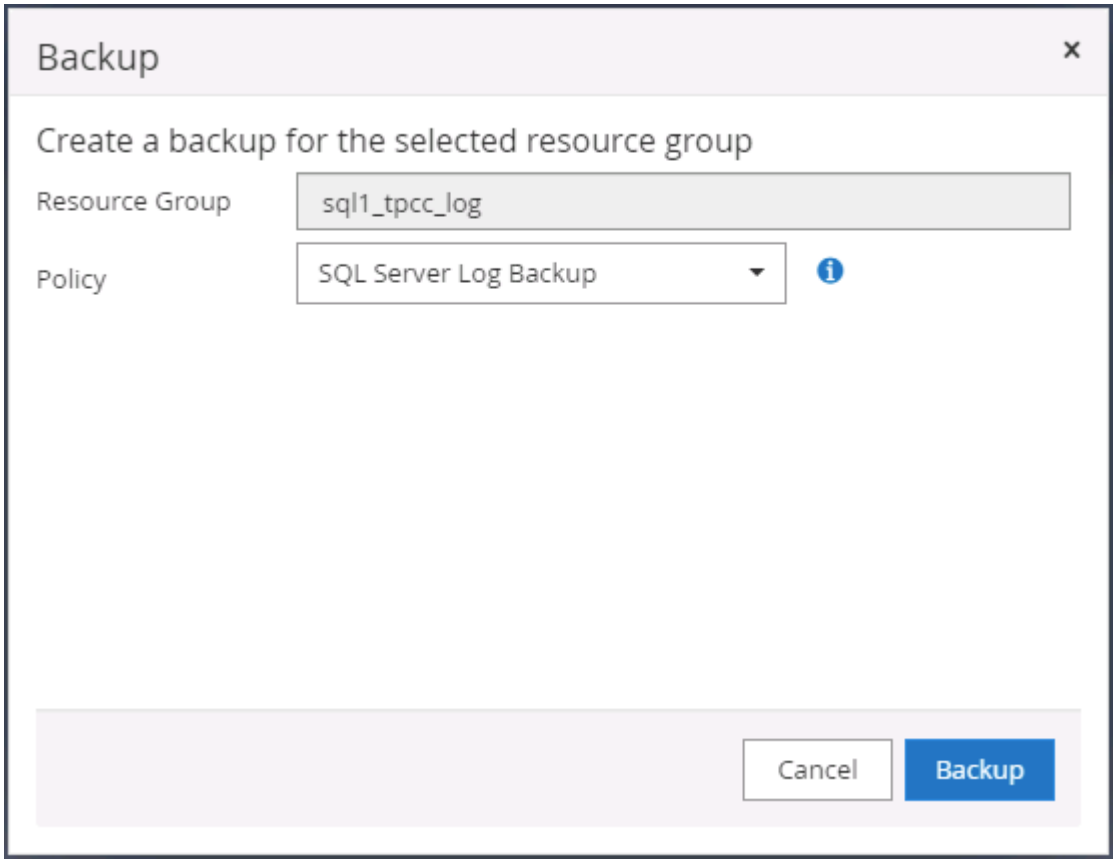
1. Da mesma forma, para validar se a recuperação do clone SQL foi executada no último log disponível, criamos uma pequena tabela de teste e inserimos uma linha. Os dados de teste seriam recuperados após uma recuperação completa do último log disponível.

```
Administrator: Command Prompt - sqlcmd - SQLCMD

C:\Users\administrator.DEMO>sqlcmd
1> select host_name()
2> go

------------------------------------------------------------------------------------------------------------------------------------
SQL1

(1 rows affected)
1> use tpcc
2> go
Changed database context to 'tpcc'.
1> insert into snap_sync values ('test snap mirror DR for SQL', getdate())
2> go

(1 rows affected)
1> select * from snap_sync
2> go
event                                              dt
-------------------------------------------------- -----------------------
test snap mirror DR for SQL                        2021-09-20 14:23:04.533

(1 rows affected)
1>
```

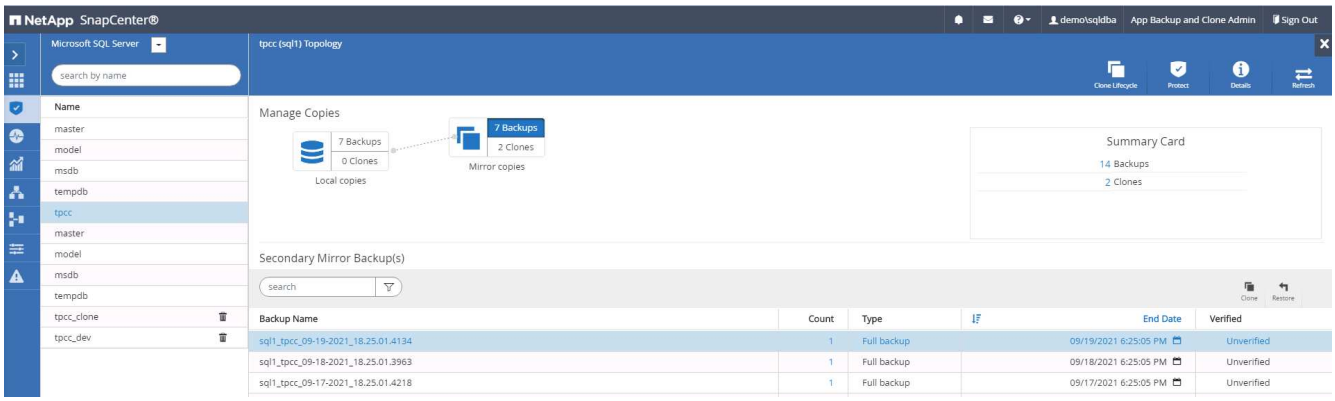
2. Efetue login no SnapCenter com uma ID de usuário de gerenciamento de banco de dados do SQL Server. Navegue até a guia Recursos, que mostra o grupo de recursos de proteção do SQL Server.



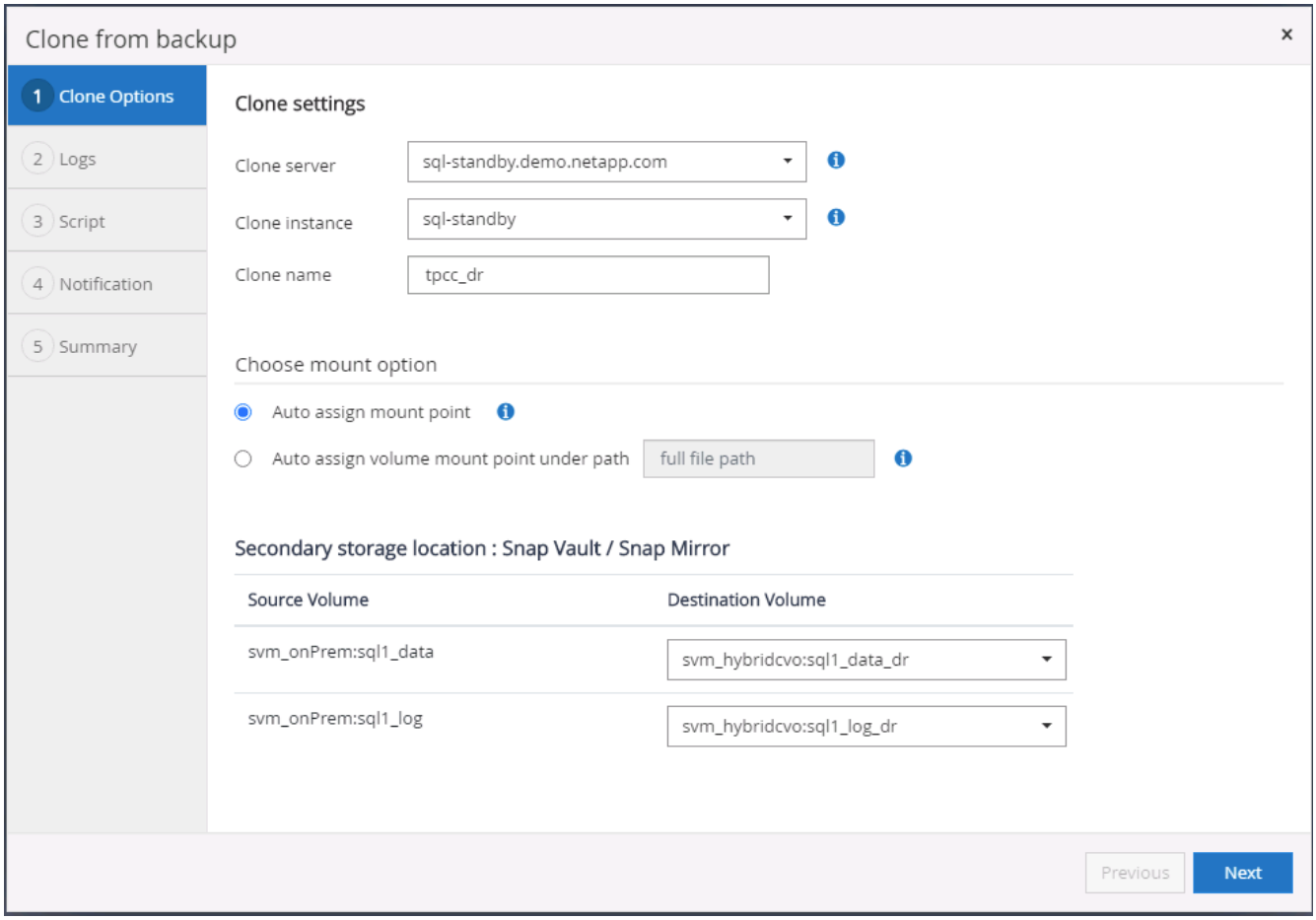
3. Execute manualmente um backup de log para liberar a última transação a ser replicada no armazenamento secundário na nuvem pública.



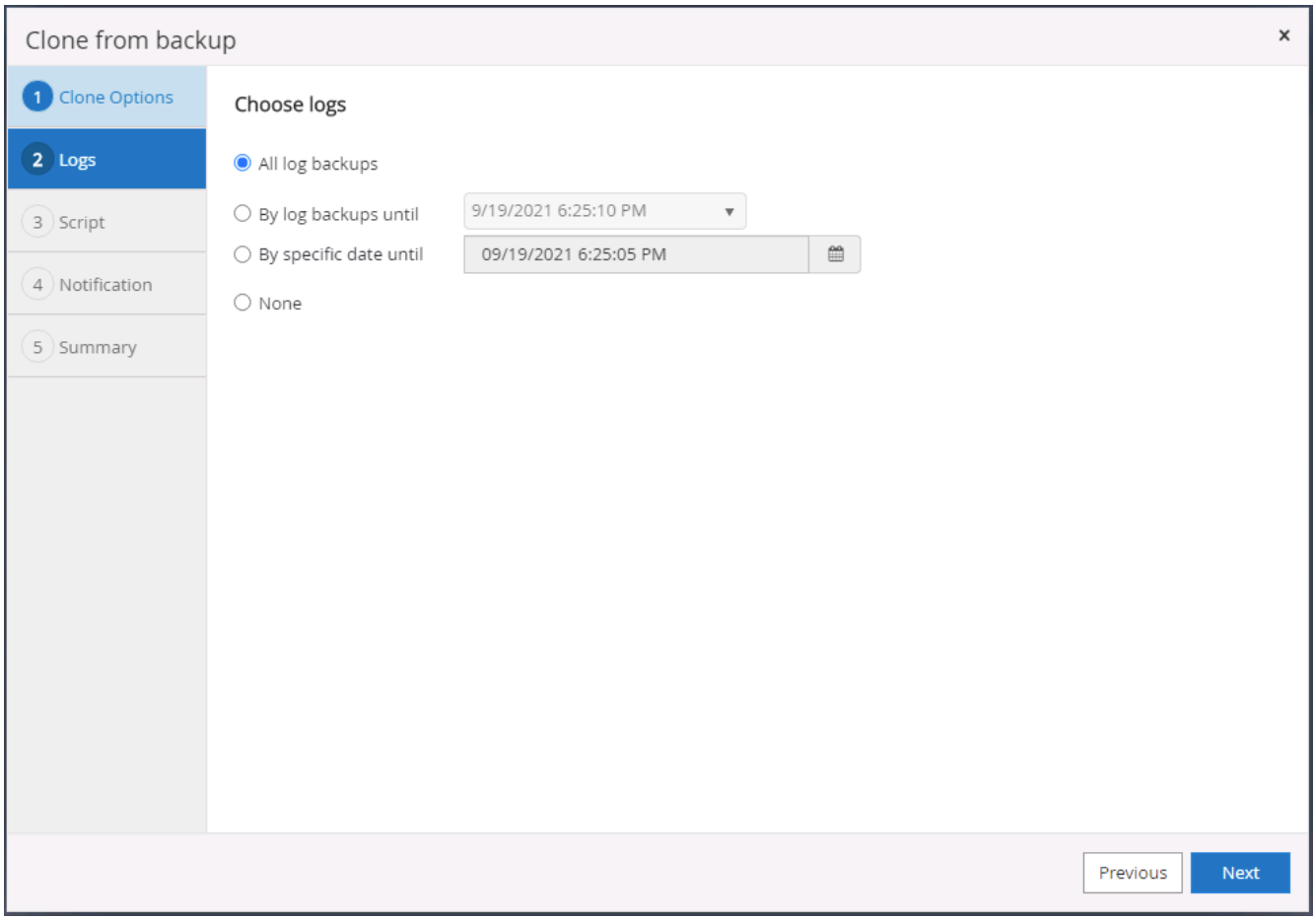
4. Selecione o último backup completo do SQL Server para o clone.



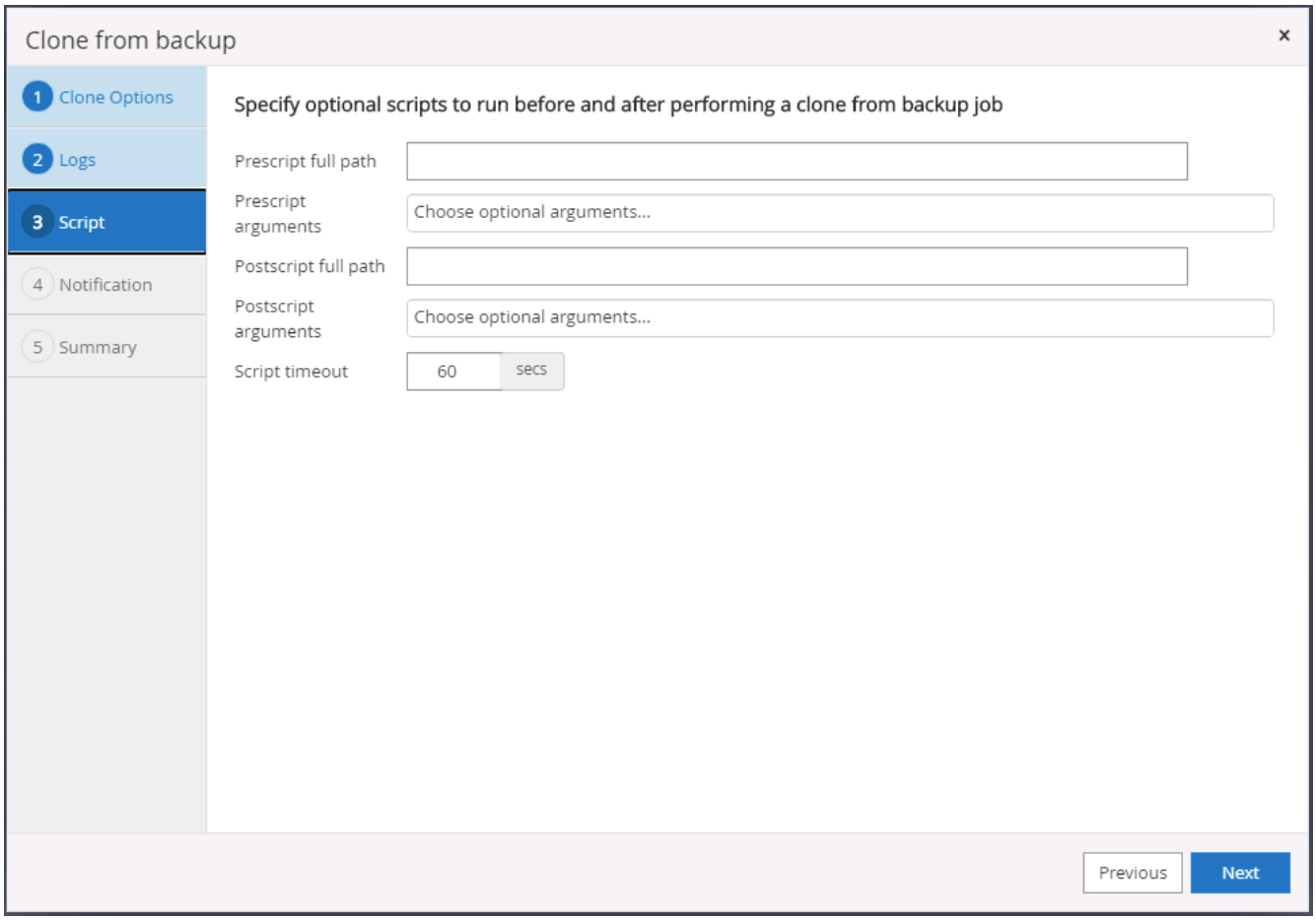
5. Defina as configurações de clone, como Servidor clone, Instância clone, Nome clone e opção de montagem. O local de armazenamento secundário onde a clonagem é realizada é preenchido automaticamente.



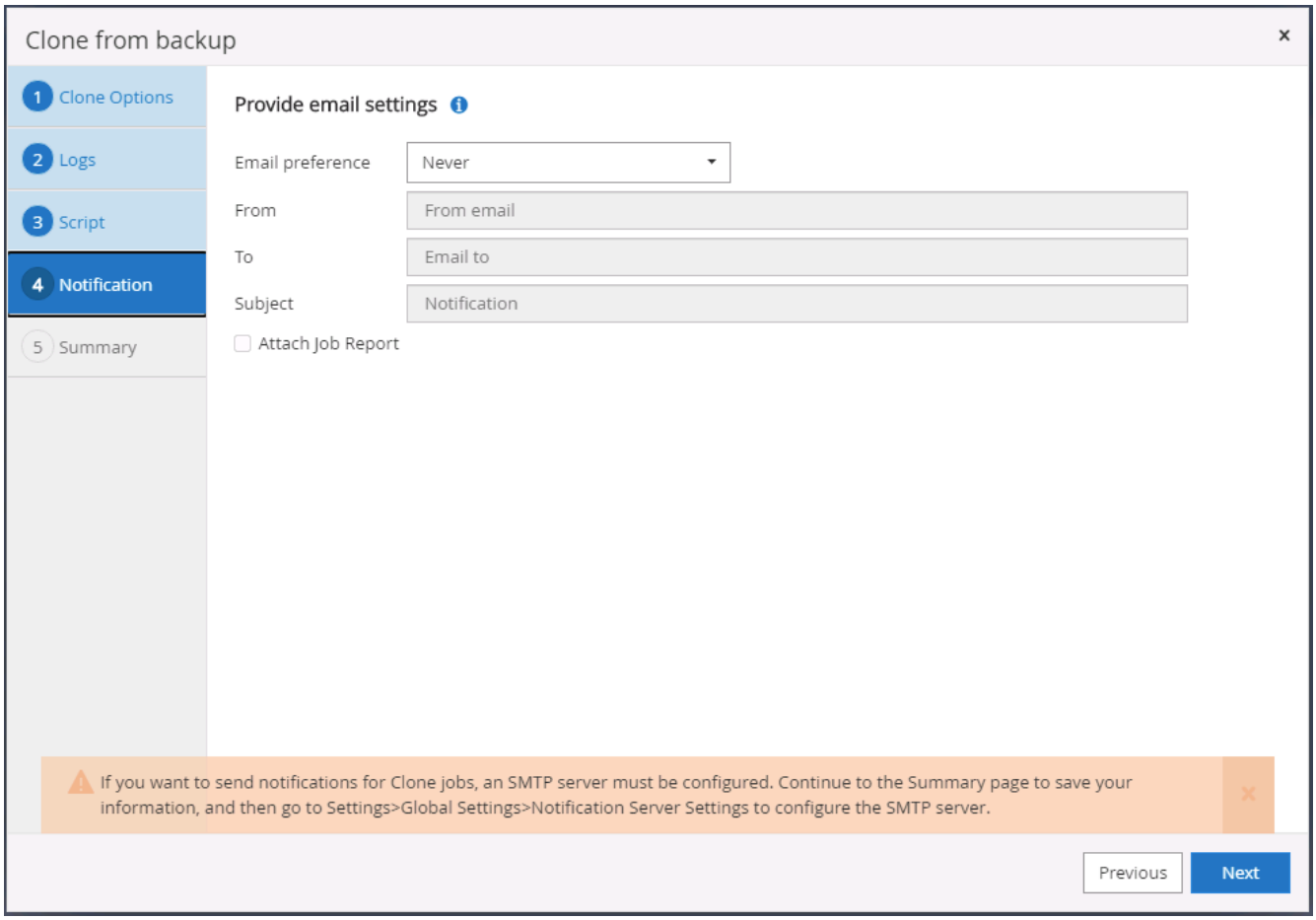
6. Selecione todos os backups de log a serem aplicados.



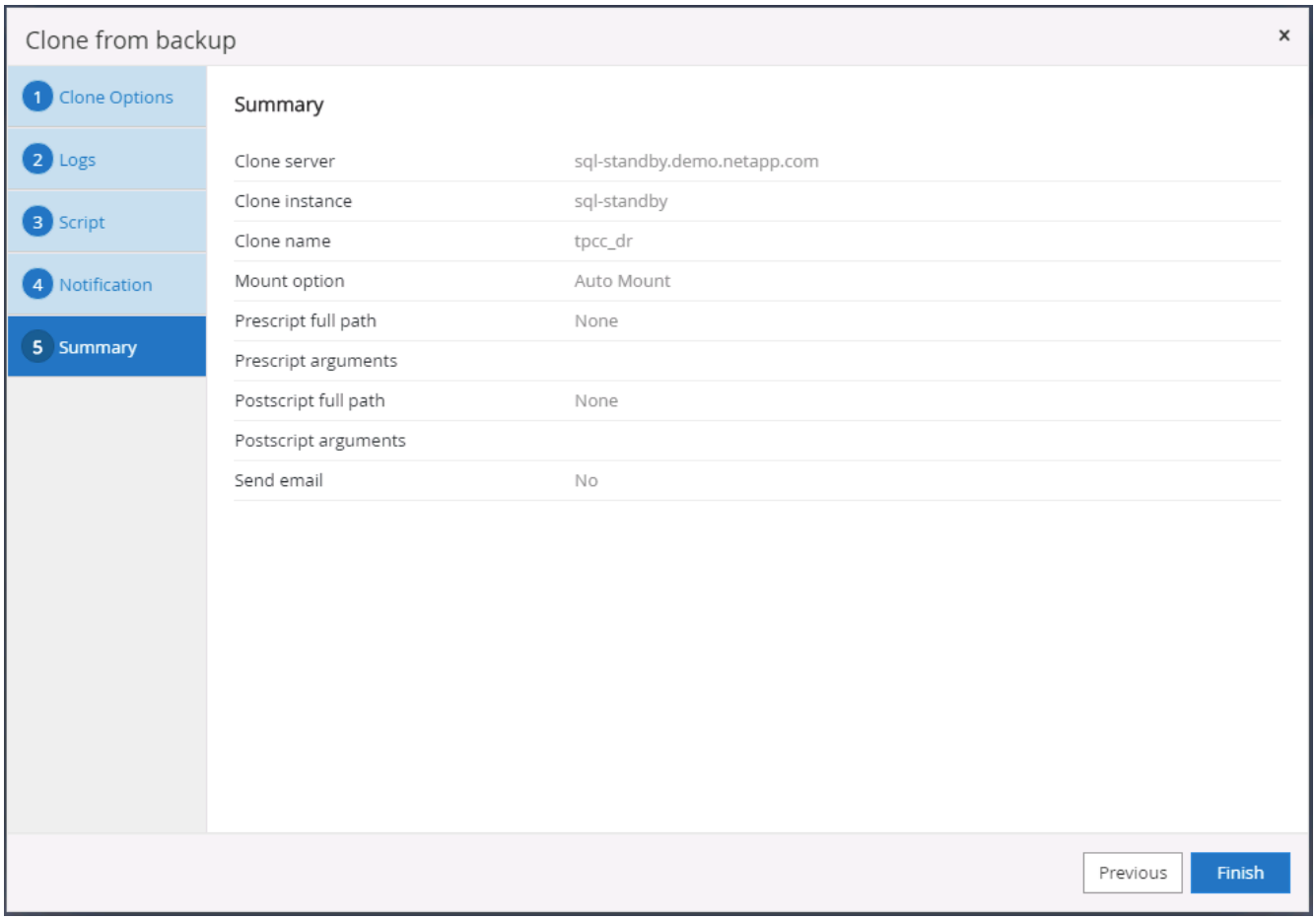
7. Especifique quaisquer scripts opcionais a serem executados antes ou depois da clonagem.

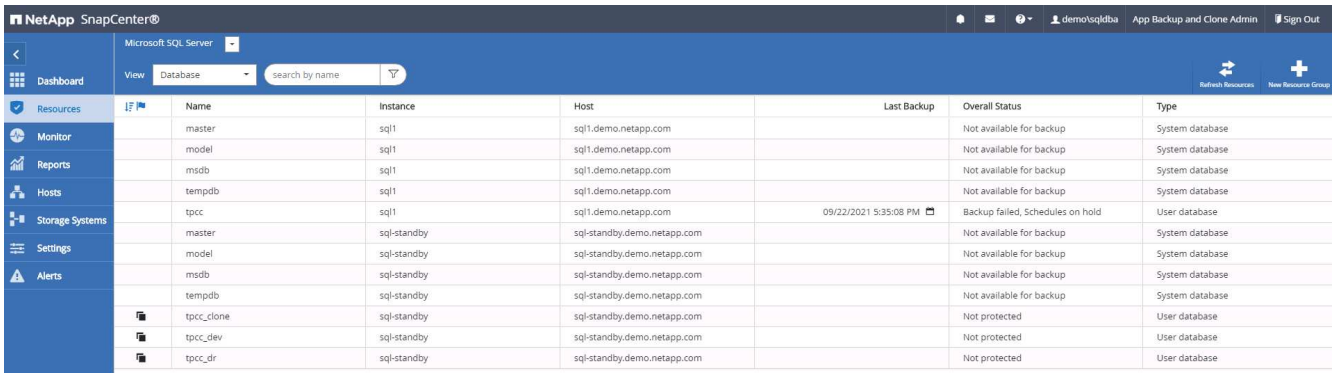


8. Especifique um servidor SMTP se desejar receber notificação por e-mail.



9. Resumo do clone DR. Bancos de dados clonados são imediatamente registrados no SnapCenter e ficam disponíveis para proteção de backup.





Validação e configuração do clone pós-DR para SQL

1. Monitore o status do trabalho de clonagem.

2. Valide se a última transação foi replicada e recuperada com todos os clones de arquivos de log e

recuperação.

```
Administrator: Command Prompt - sqlcmd - SQLCMD

C:\Users\administrator.DEMO>sqlcmd
1> select host_name()
2> go

----------------------------------------------------------------------------------------------------------------------------
SQL-STANDBY

(1 rows affected)
1> use tpcc_dr
2> go
Changed database context to 'tpcc_dr'.
1> select * from snap_sync
2> go
event                                              dt
-------------------------------------------------- -----------------------
test snap mirror DR for SQL                        2021-09-20 14:23:04.533

(1 rows affected)
1> select getdate()
2> go

-----------------------
2021-09-20 14:39:19.937

(1 rows affected)
1>
```

3. Configure um novo diretório de log do SnapCenter no servidor DR para backup de log do SQL Server.
4. Divida o volume clonado do volume de origem replicado.
5. Reverta a replicação da nuvem para o local e reconstrua o servidor de banco de dados local com falha.

Onde procurar ajuda?

Se precisar de ajuda com esta solução e casos de uso, junte-se a nós"Canal do Slack de suporte da comunidade de automação de soluções da NetApp" e procure o canal de automação de soluções para postar suas dúvidas ou perguntas.

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 DESTE DOCUMENTO. 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 SOBRESSALENTES; 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 DESTE SOFTWARE, 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.