



Soluções de banco de dados em nuvem híbrida com SnapCenter

NetApp database solutions

NetApp
February 20, 2026

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:

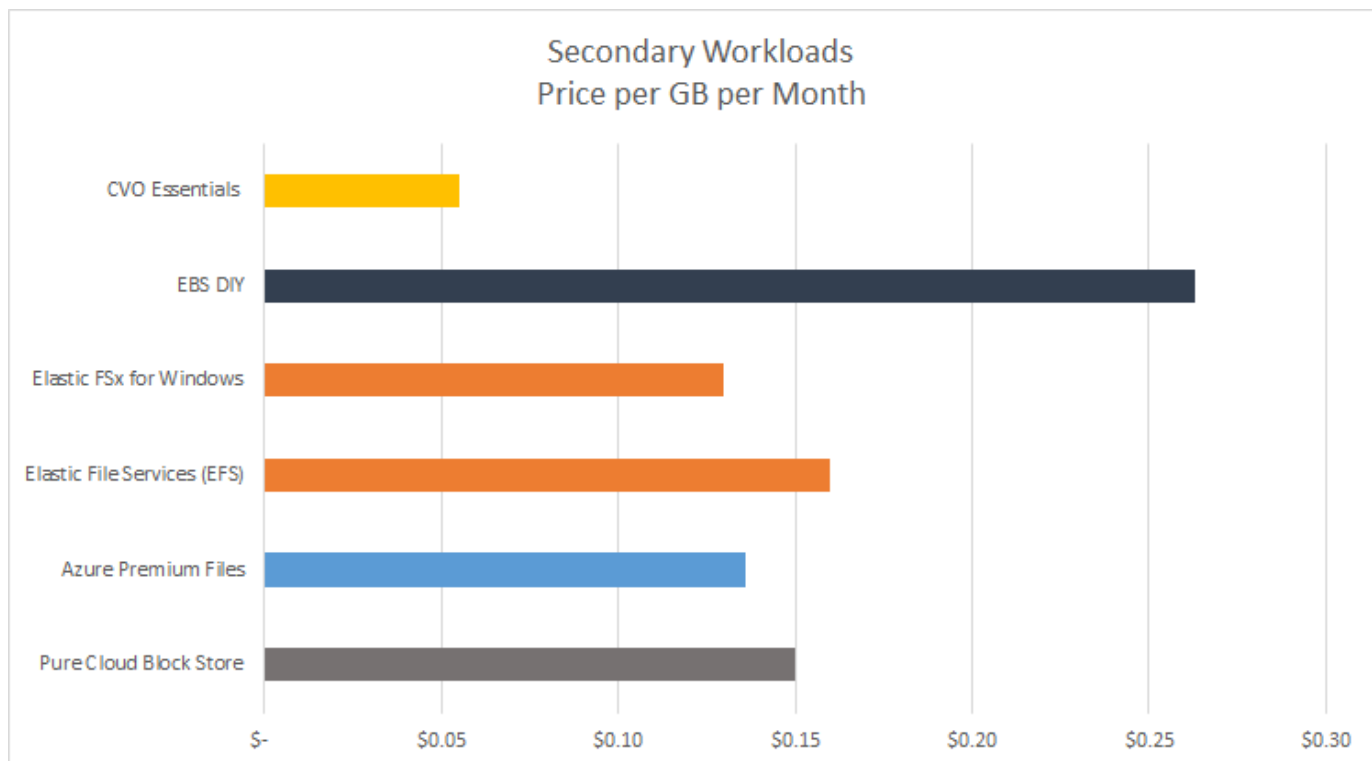
- Operações de desenvolvimento/teste de banco de dados na nuvem híbrida
- Recuperação de desastres de banco de dados na nuvem híbrida

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.

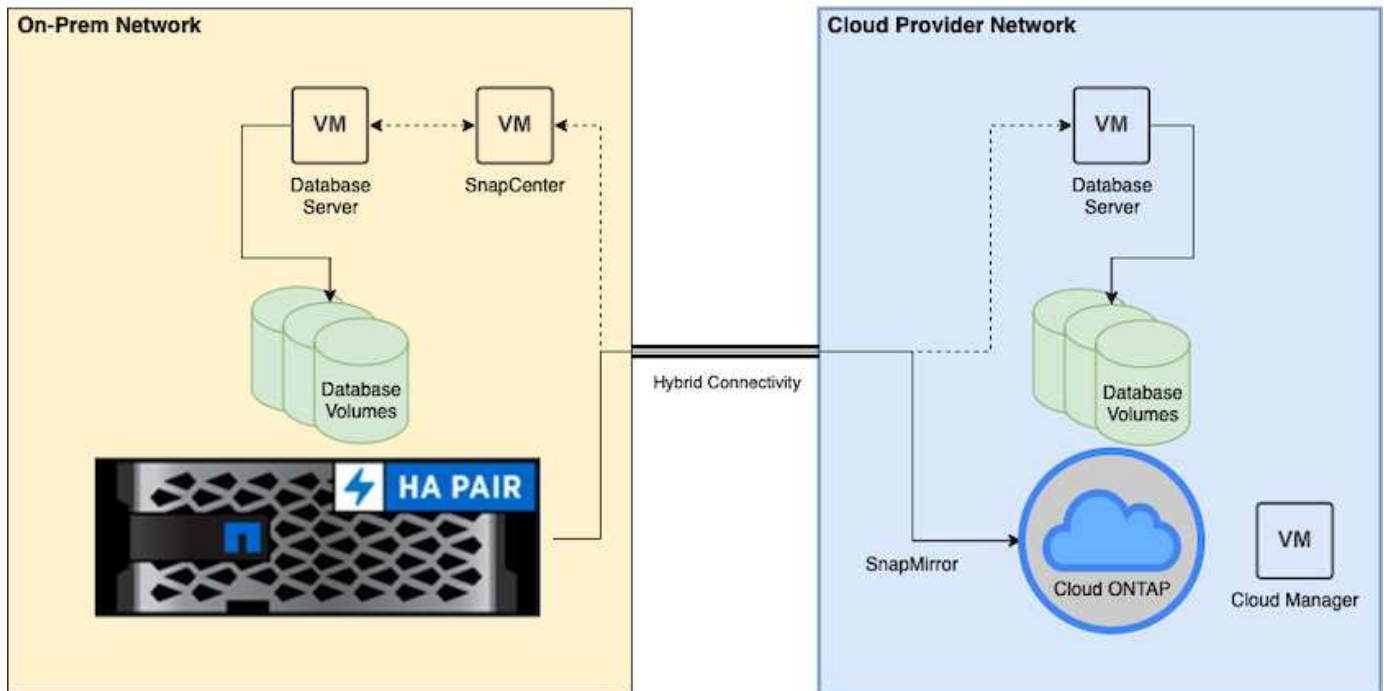
Os vídeos a seguir demonstram o SnapCenter em ação:

- ["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.

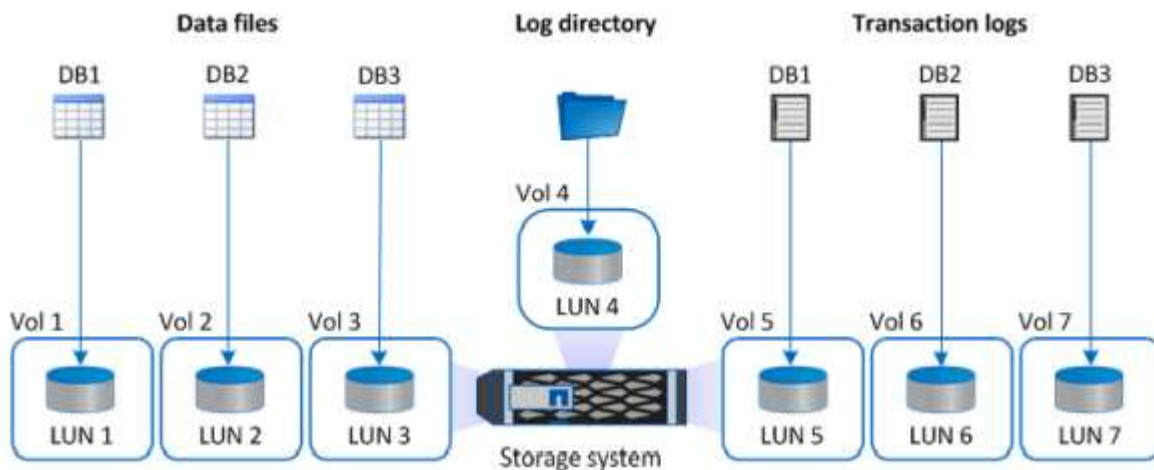
- **Implantação de instância única ou HA.** A implantação de HA fornece redundância no caso de falha de um único servidor de instância do SnapCenter .
- **Resolução de nomes.** O DNS deve ser configurado no servidor SnapCenter para resolver todos os hosts do banco de dados, bem como no SVM de armazenamento 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 .

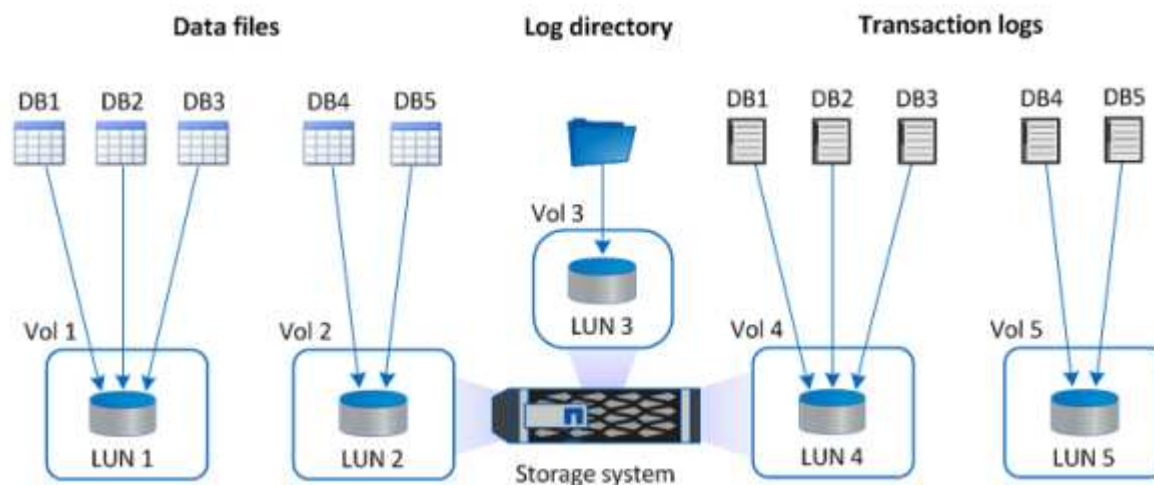
Configuração de armazenamento do servidor de banco de dados local

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

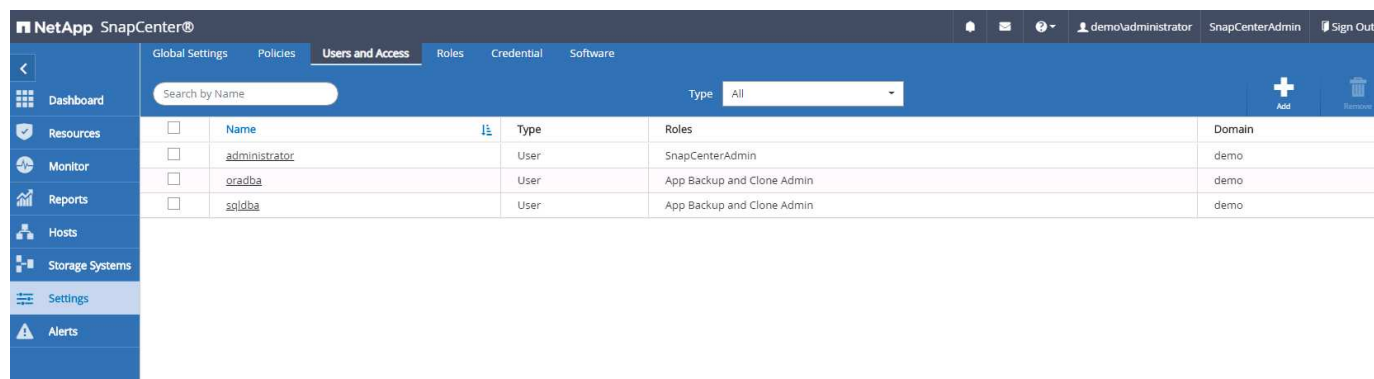
1. Configurar usuário administrador do banco de dados no SnapCenter

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.



Name	Type	Roles	Domain
administrator	User	SnapCenterAdmin	demo
oradbba	User	App Backup and Clone Admin	demo
sqlidba	User	App Backup and Clone Admin	demo

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 plug-ins.
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

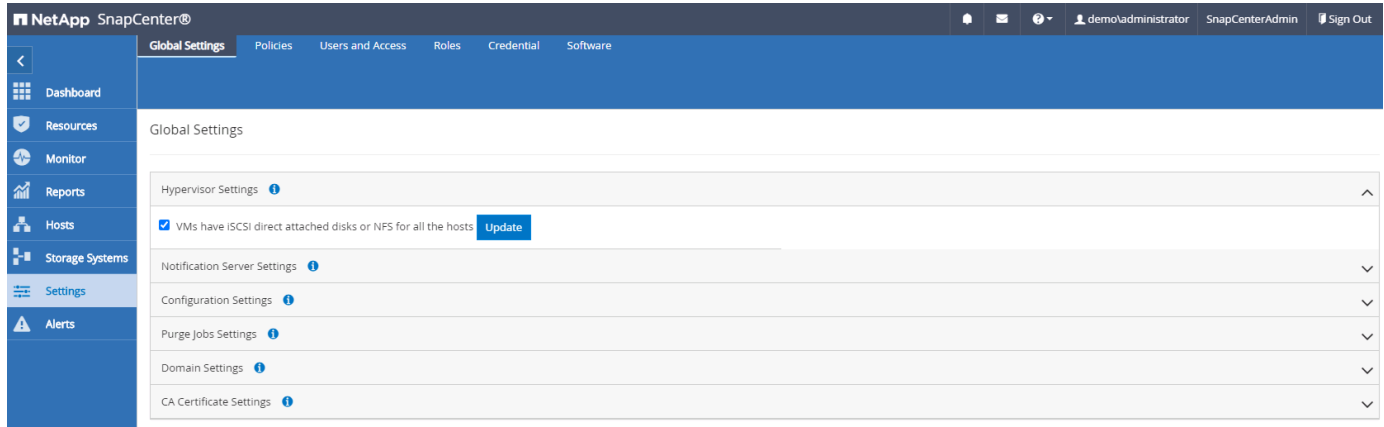


Antes de tentar instalar plug-ins do SnapCenter em instâncias do servidor de banco de dados na nuvem, certifique-se de que todas as etapas de configuração tenham sido concluídas, conforme listado na seção de nuvem relevante para implantação de instância de computação.

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.

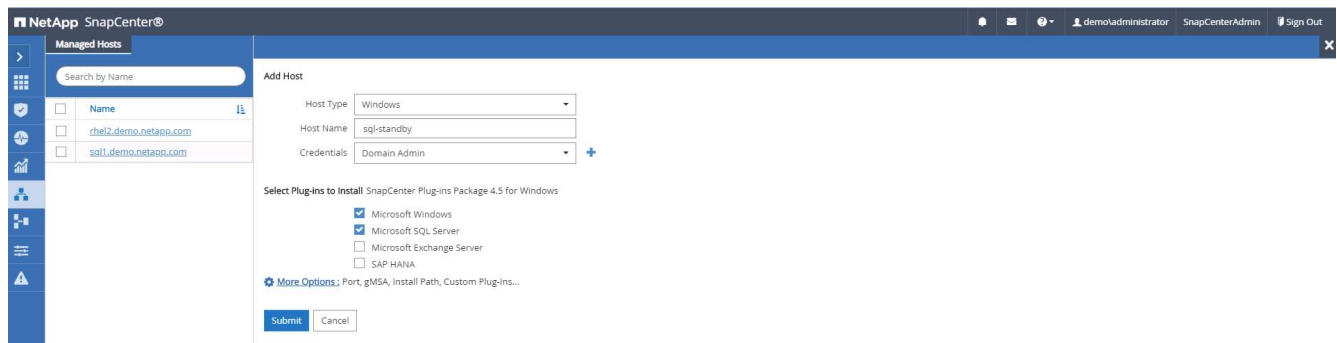
Configurar as configurações globais do SnapCenter VMware

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.

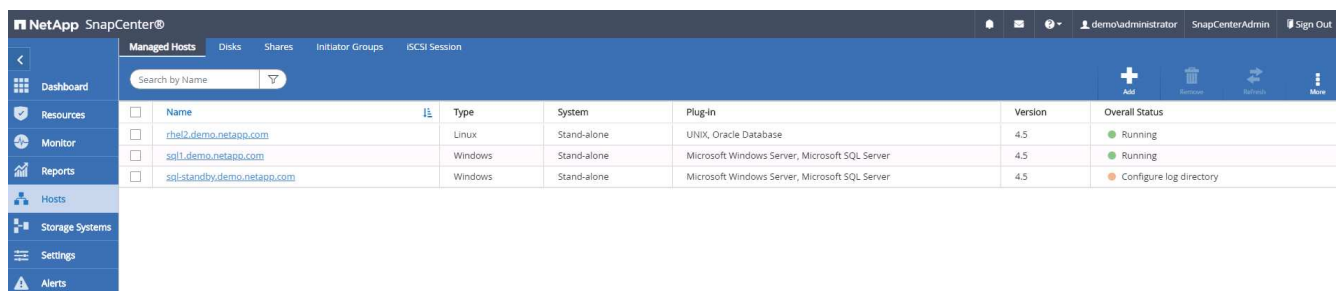


Adicionar host Windows e instalação do plugin no host

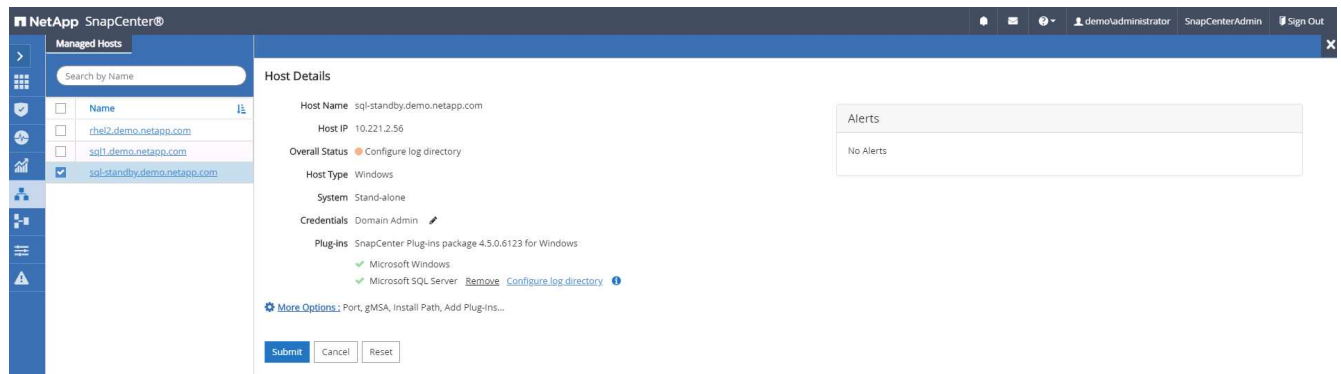
1. Efetue login no SnapCenter com um ID de usuário com privilégios SnapCenterAdmin.
2. Clique na aba Hosts no menu à esquerda e depois clique em Adicionar para abrir o fluxo de trabalho Adicionar Host.
3. Selecione Windows para Tipo de Host; o Nome do Host pode ser um nome de host ou um endereço IP. 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.



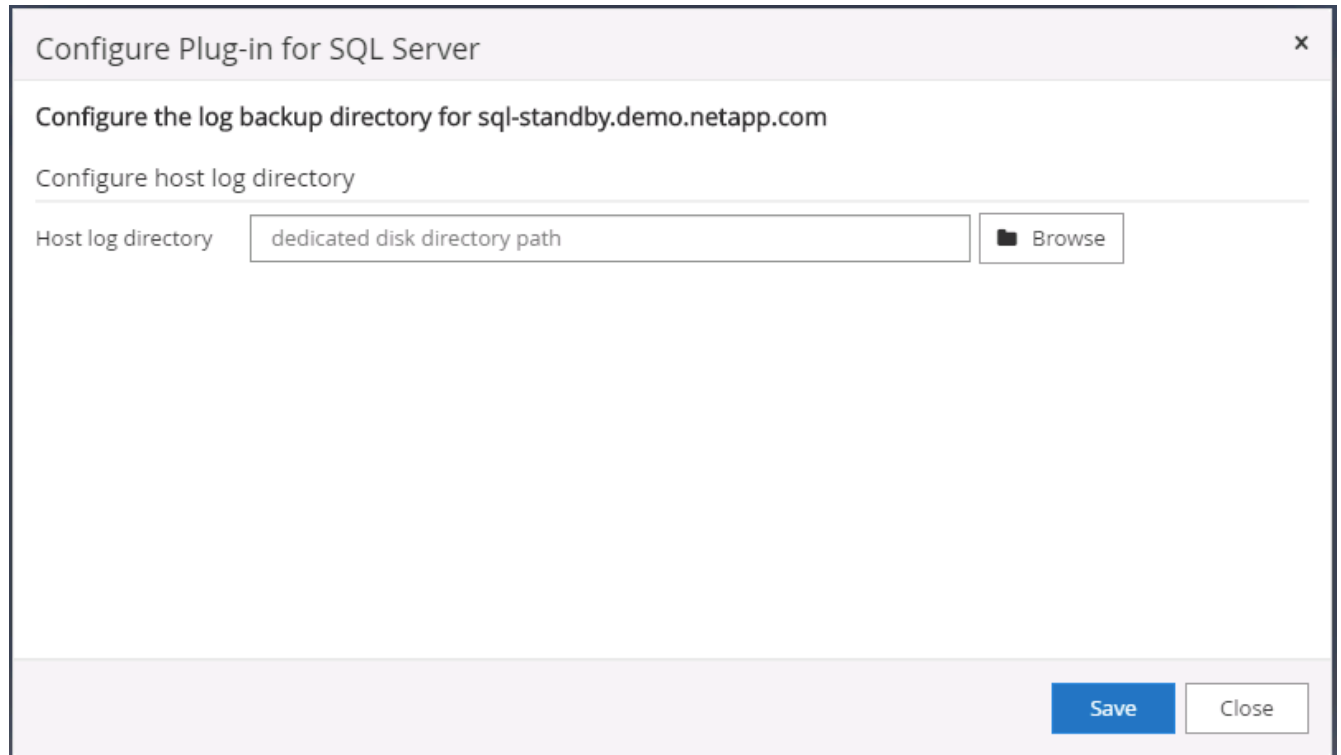
4. Após o plugin ser instalado em um host Windows, seu status geral é exibido como "Configurar diretório de log".



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.

Configure Plug-in for SQL Server

Configure the log backup directory for sql-standby.demo.netapp.com

Configure host log directory

Host log directory

Browse

Choose directory on NetApp Storage

sql-standby.demo.netapp.com

G:\

System Volume Information

Save

Close



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.

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

NetApp SnapCenter®							
Managed Hosts Disks Shares Initiator Groups ISCSI Session							
Search by Name + + + +							
	Name	Type	System	Plug-in	Version	Overall Status	
☐	rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running	
☐	sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running	
☐	sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running	

- 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 sqldb ao qual o host precisa ser atribuído) e clique em Salvar para concluir a atribuição de recursos do host.

NetApp SnapCenter®					
Global Settings Policies Users and Access Roles Credential Software					
Search by Name Type All + +					
	Name	Type	Roles		
☐	administrator	User	SnapCenterAdmin		
☐	oradba	User	App Backup and Clone Admin		
☐	sqldb	User	App Backup and Clone Admin		

Assign Assets

Asset Type
Host
search

☐	Asset Name	☐
☐	rhel2.demo.netapp.com	
☐	sql1.demo.netapp.com	
☒	sql-standby.demo.netapp.com	

Save
Close

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.

demo\administrator
SnapCenterAdmin
Sign Out

Add Host

Host Type
Linux
Host Name
ora-standby
Credentials
admin
+
i

Select Plug-ins to Install SnapCenter Plug-ins Package 4.5 for Linux
☒ Oracle Database
☐ SAP HANA
[More Options](#) Port, Install Path, Custom Plug-ins...

Submit
Cancel

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.

More Options

Port

8145

Installation Path

/opt/NetApp/snapcenter

☒

Skip preinstall checks

☒

Add all hosts in the oracle RAC

Custom Plug-ins

Choose a File

Browse

Upload

No plug-ins found.

Save

Cancel

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

Confirm Fingerprint

Authenticity of the host cannot be determined

Host name	Fingerprint	Valid
ora-standby.demo.netapp.com	ssh-rsa 3072 5C:02:EF:6B:63:54:59:10:84:DF:4D:6B:AB:FB:61:67	

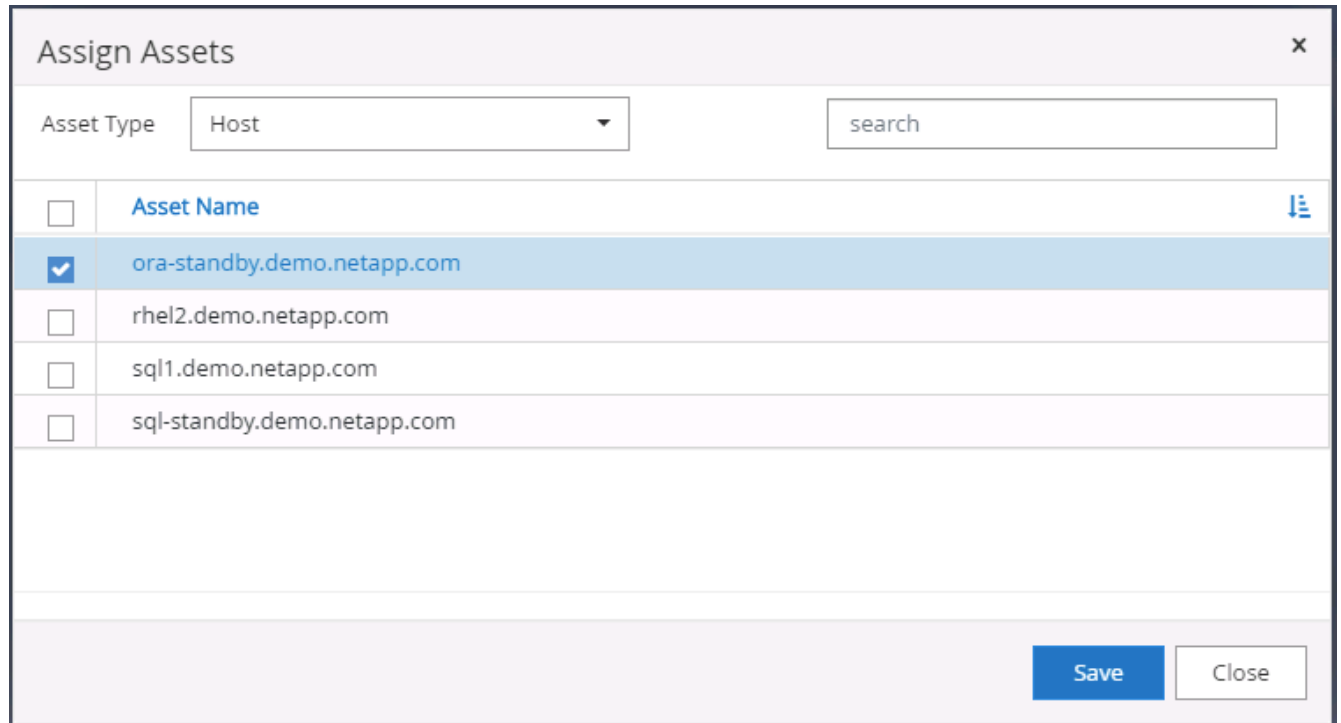
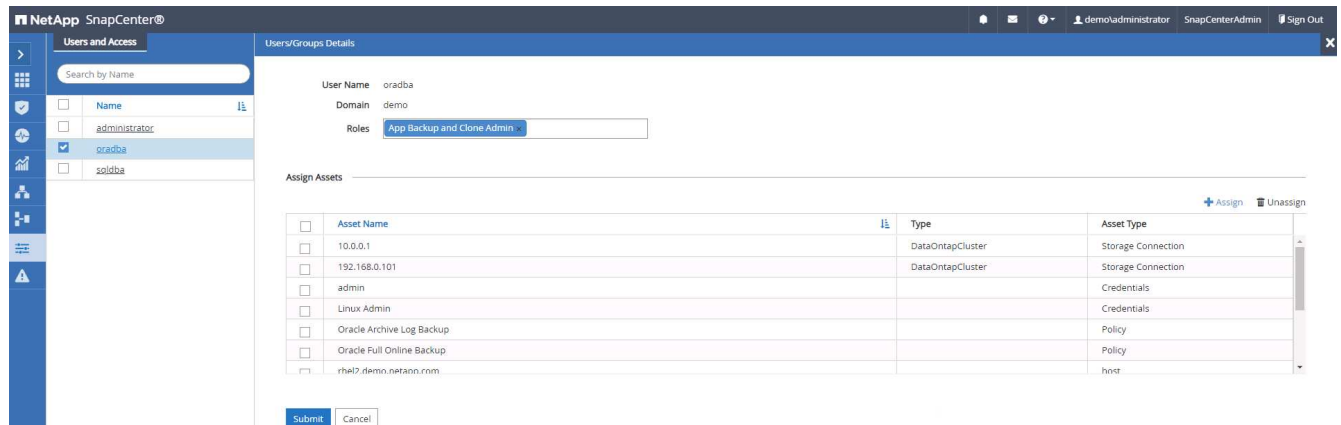
Confirm and Submit

Close

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.

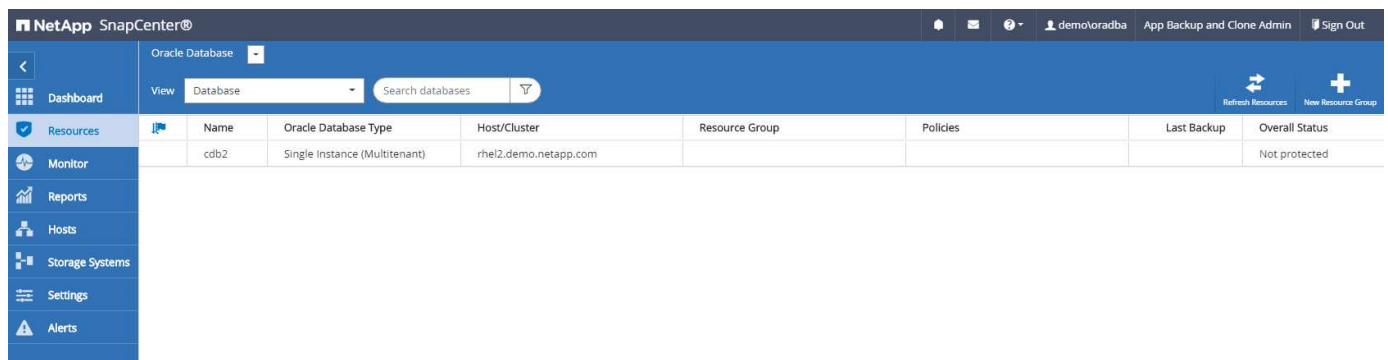
NetApp SnapCenter®							
Managed Hosts							
Search by Name							
	Name	Type	System	Plug-in	Version	Overall Status	
☐	ora-standby.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running	
☐	rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running	
☐	sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running	
☐	sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running	

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.

	Name	Instance	Host	Last Backup	Overall Status	Type
	master	sql1	sql1.demo.netapp.com		Not available for backup	System database
	model	sql1	sql1.demo.netapp.com		Not available for backup	System database
	msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
	tempdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
	tpcc	sql1	sql1.demo.netapp.com	09/14/2021 2:35:07 PM	Backup succeeded	User database

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.

	Name	Host	Resource Groups	Policies	State	Type
	sql-standby	sql-standby.demo.netapp.com			Running	Standalone ()
	sql1	sql1.demo.netapp.com			Running	Standalone (15.0.2000)

Instance - Credentials	
The Microsoft SQL server or Windows credentials are necessary to unlock the selected instance. Click Refresh Resources to run a discovery with the associated Auth.	
Name	sql-standby
Resource Group	None
Policy	None
Selectable	Not available for backup. DB is not on NetApp storage, auto-close is enabled or in recovery mode.

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.

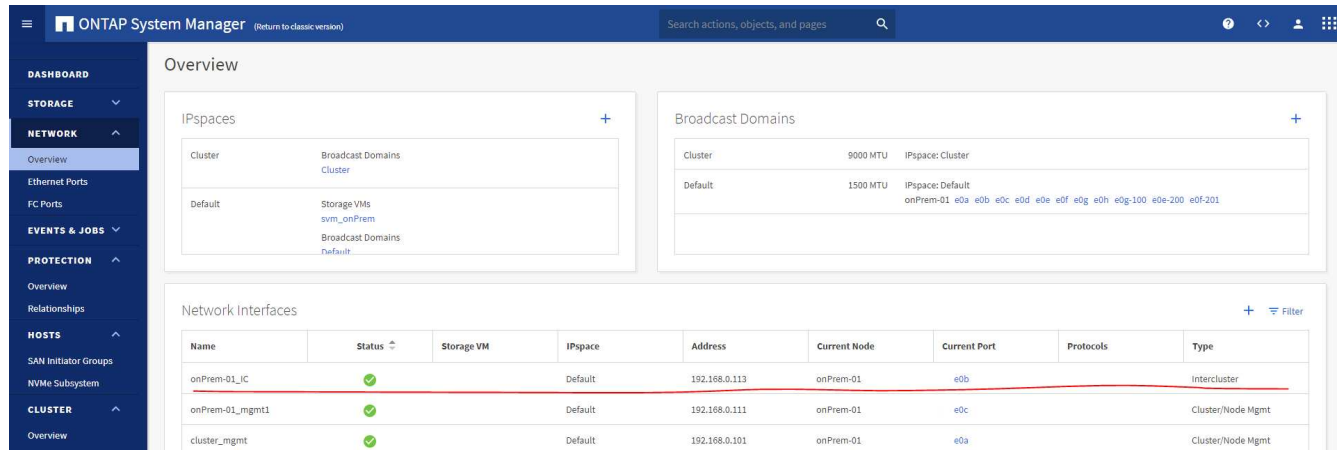
	Name	Host	Resource Groups	Policies	State	Type
	sql1	sql1.demo.netapp.com			Running	Standalone (15.0.2000)
	sql-standby	sql-standby.demo.netapp.com			Running	Standalone (15.0.2000)

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.

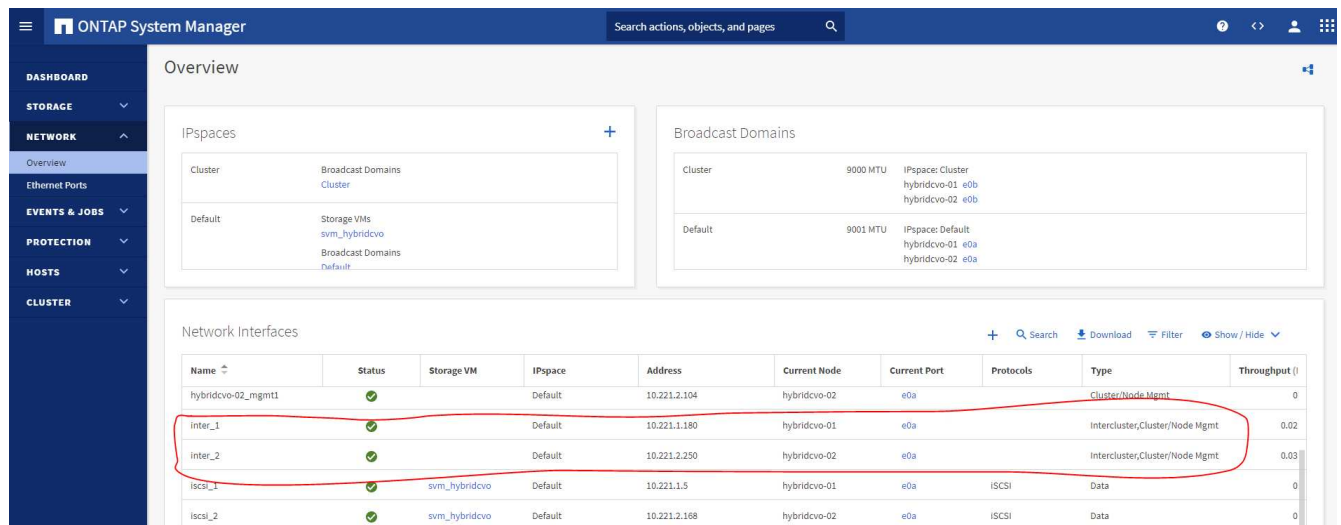
1. Configure LIFs entre clusters para peering de cluster no cluster local e na instância do cluster CVO. Esta etapa pode ser realizada com o ONTAP System Manager. Uma implantação de CVO padrão tem LIFs entre clusters configurados automaticamente.

Cluster local:



Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Protocols	Type
onPrem-01_IC	Up		Default	192.168.0.113	onPrem-01	e0b		Intercluster
onPrem-01_mgmt1	Up		Default	192.168.0.111	onPrem-01	e0c		Cluster/Node Mgmt
cluster_mgmt	Up		Default	192.168.0.101	onPrem-01	e0a		Cluster/Node Mgmt

Cluster CVO alvo:

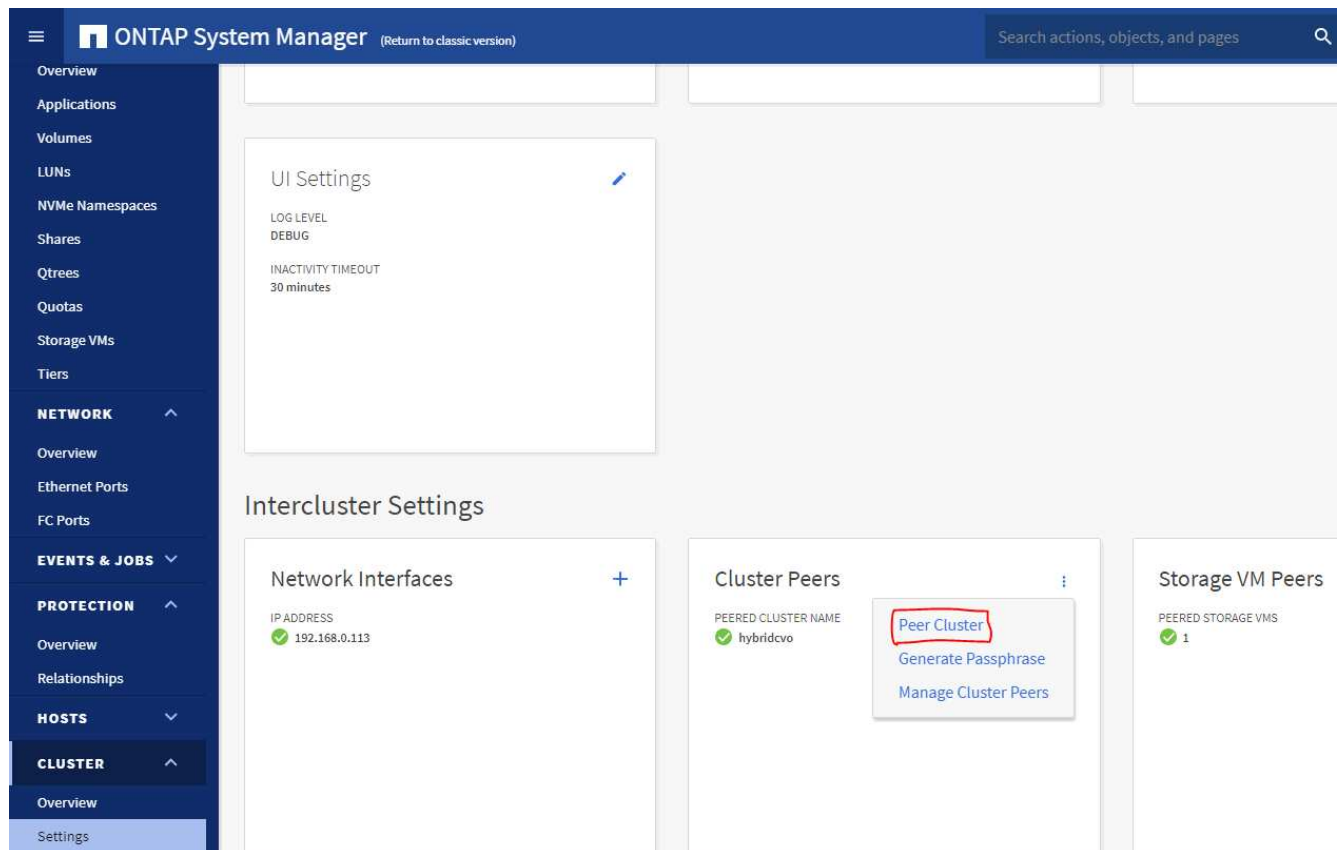


Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Protocols	Type	Throughput (I)
hybridcvo-02_mgmt1	Up		Default	10.221.2.104	hybridcvo-02	e0a		Cluster/Node Mgmt	0
inter_1	Up		Default	10.221.1.180	hybridcvo-01	e0a		Intercluster,Cluster/Node Mgmt	0.02
inter_2	Up		Default	10.221.2.250	hybridcvo-02	e0a		Intercluster,Cluster/Node Mgmt	0.03
iscsi_1	Up	svm_hybridcvo	Default	10.221.1.5	hybridcvo-01	e0a	ISCSI	Data	0
iscsi_2	Up	svm_hybridcvo	Default	10.221.2.168	hybridcvo-02	e0a	ISCSI	Data	0

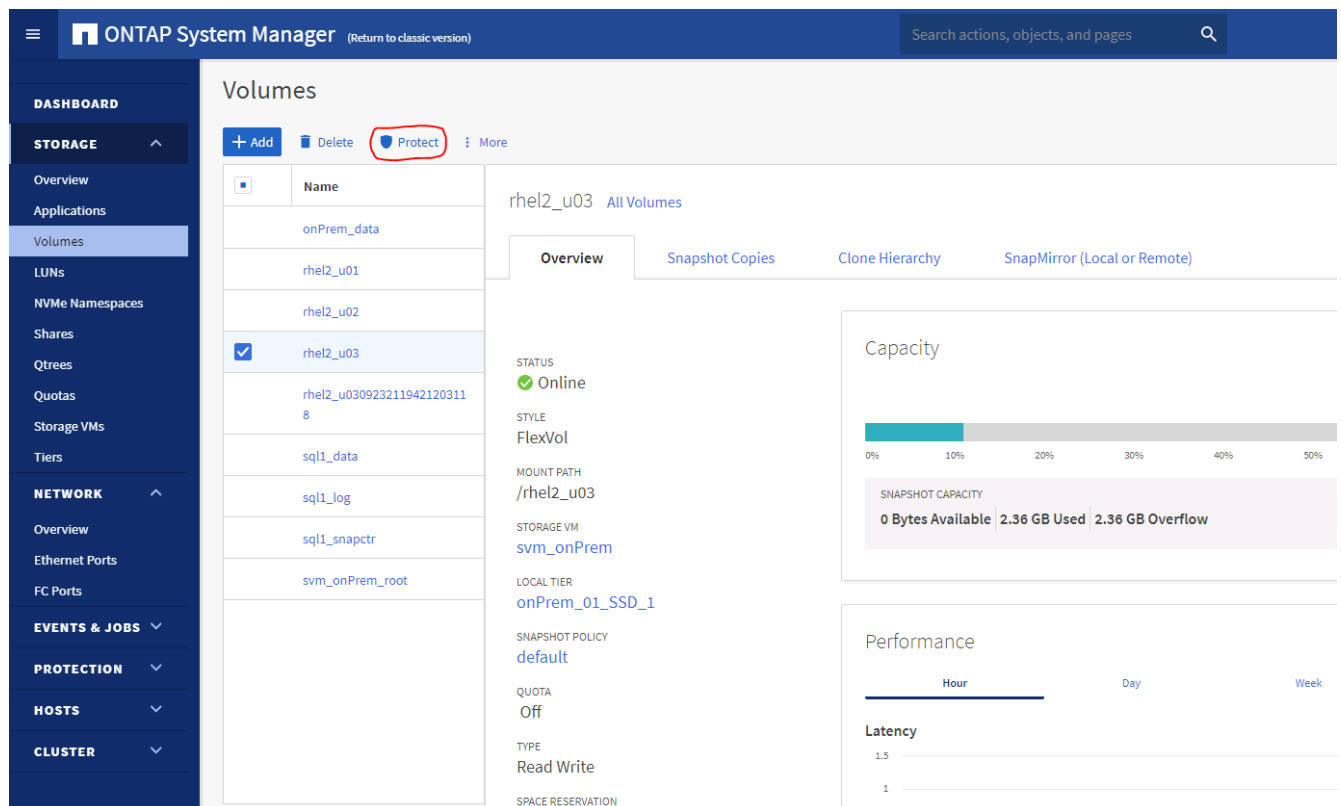
2. Com os LIFs intercluster configurados, o peering de cluster e a replicação de volume podem ser configurados usando arrastar e soltar no NetApp Cloud Manager. Ver ["Introdução - Nuvem Pública da AWS"](#) para mais detalhes.

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.



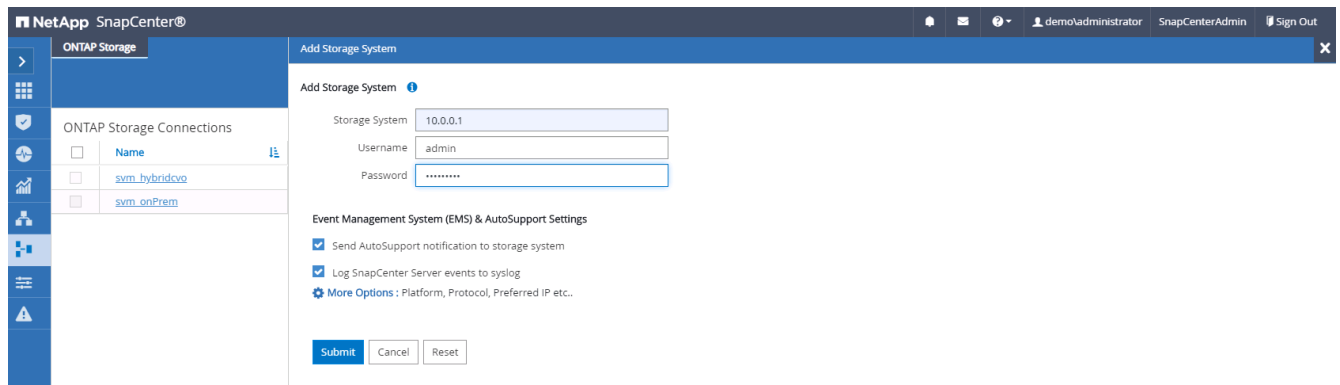
5. Defina a política de proteção como Assíncrona. Selecione o cluster de destino e o SVM de armazenamento.

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

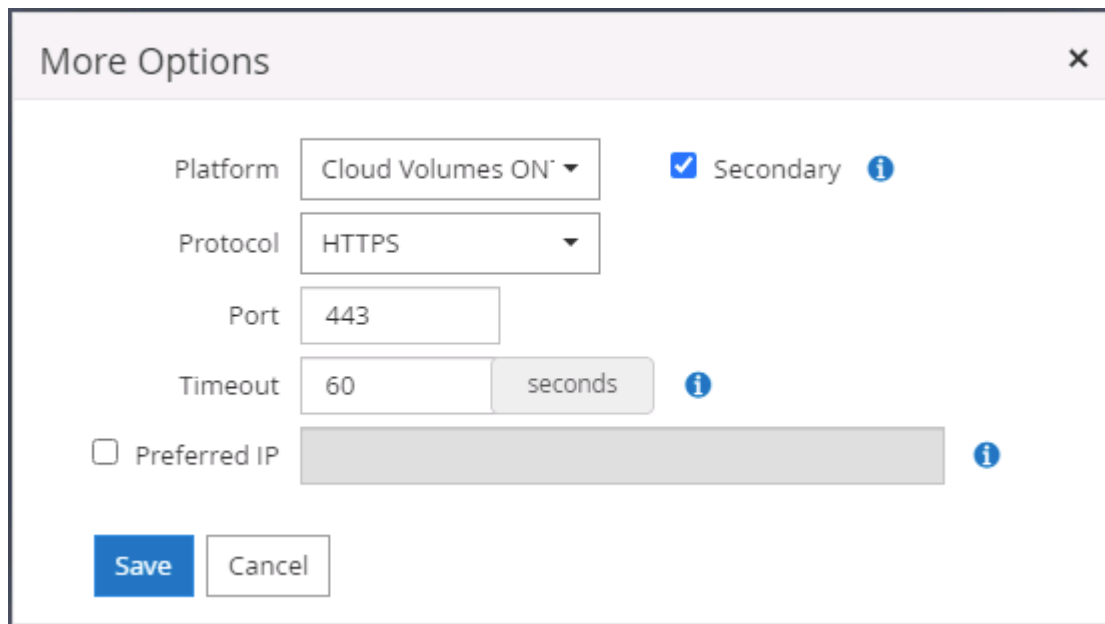
Source	Destination	Protection Policy	Relationship Health	Relationship Status	Lag
svm_onPremorhel2_u03	svm_hybridcvoorhel2_u03_dr	MirrorAllSnapshots	Healthy	Mirrored	12 seconds

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

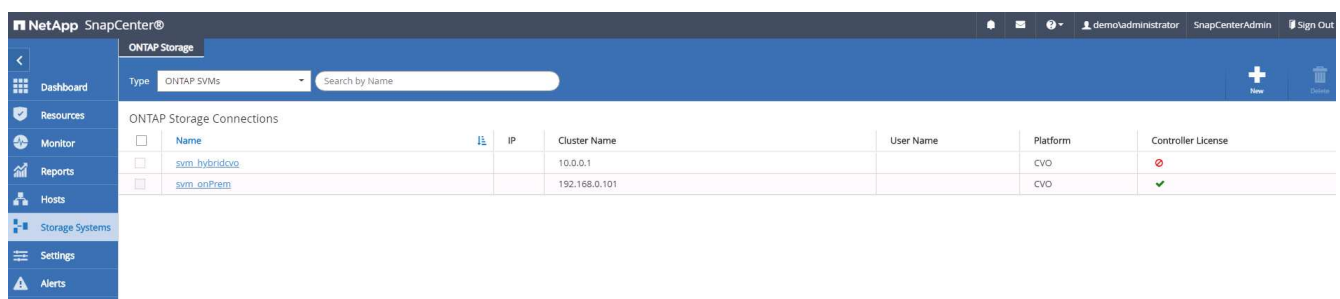
1. Efetue login no SnapCenter com um ID de usuário com privilégios SnapCenterAdmin.
2. Clique na guia Sistema de armazenamento no menu e, em seguida, clique em Novo para adicionar um SVM de armazenamento CVO que hospeda volumes de banco de dados de destino replicados no SnapCenter. Insira o IP de gerenciamento 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 em 3. [Instalação do plugin do host SnapCenter](#).

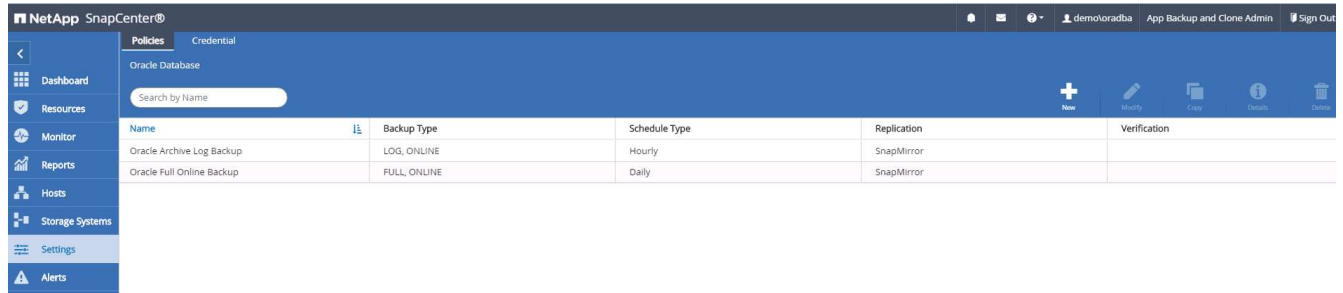


7. Configurar política de backup de banco de dados no SnapCenter

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.

The screenshot shows a 'Modify Oracle Database Backup Policy' dialog box. On the left, there is a vertical list of steps: 1 Name, 2 Backup Type, 3 Retention, 4 Replication, 5 Script, 6 Verification, and 7 Summary. The 'Name' step is currently selected. The main area of the dialog is titled 'Provide a policy name'. It contains two input fields: 'Policy name' with the value 'Oracle Full Online Backup' and 'Details' with the value 'Backup all data and log files'. At the bottom right, there are 'Previous' and 'Next' buttons.

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

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select Oracle database backup options

Choose backup type

☒ Online backup

☒ Datafiles, control files, and archive logs

☐ Datafiles and control files

☐ Archive logs

☐ Offline backup

☒ Mount

☐ Shutdown

☐ Save state of PDBs

Choose schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ On demand

☐ Hourly

☒ Daily

Previous

Next

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

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

Daily retention settings

Data backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

14

days

Archive Log backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

14

days

Previous

Next

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

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Daily

Error retry count

3

Previous

Next

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

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before and after performing a backup job

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Prescript arguments

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Postscript arguments

Script timeout

60

secs

Previous

Next

7. Execute a verificação de backup, se desejar.

29

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.

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

Policy name	Oracle Full Online Backup
Details	Backup all data and log files
Backup type	Online backup
Schedule type	Daily
RMAN catalog backup	Disabled
Archive log pruning	None
On demand data backup retention	None
On demand archive log backup retention	None
Hourly data backup retention	None
Hourly archive log backup retention	None
Daily data backup retention	Delete Snapshot copies older than : 14 days
Daily archive log backup retention	Delete Snapshot copies older than : 14 days
Weekly data backup retention	None
Weekly archive log backup retention	None
Monthly data backup retention	None
Monthly archive log backup retention	None
Replication	SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3

Previous

Finish

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.

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

Details

Oracle Archive Log Backup

Backup Oracle archive logs

Previous

Next

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

32

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select Oracle database backup options

Choose backup type

☒ Online backup

☐ Datafiles, control files, and archive logs

☐ Datafiles and control files

☒ Archive logs

☐ Offline backup

☒ Mount

☐ Shutdown

☐ Save state of PDBs

Choose schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ On demand

☒ Hourly

☐ Daily

Previous

Next

4. Defina o período de retenção do log.

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

Hourly retention settings

Data backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

14 days

Archive Log backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

7 days

Previous

Next

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

34

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Hourly

Error retry count

3

Previous

Next

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

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before and after performing a backup job

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Prescript arguments

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Postscript arguments

Script timeout

60

secs

Previous

Next

7. Especifique quaisquer scripts de verificação de backup.

36

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

60secs

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.

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

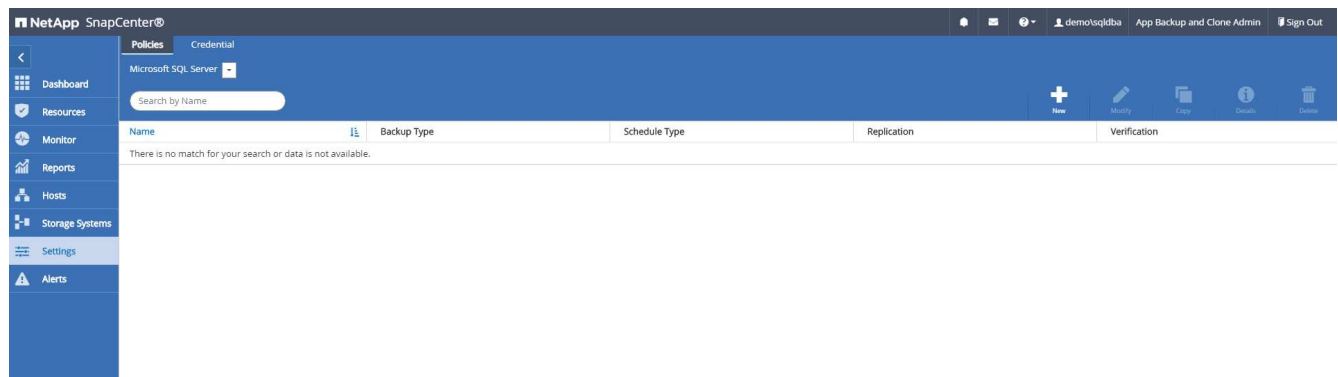
Policy name	Oracle Archive Log Backup
Details	Backup Oracle archive logs
Backup type	Online backup
Schedule type	Hourly
RMAN catalog backup	Disabled
Archive log pruning	None
On demand data backup retention	None
On demand archive log backup retention	None
Hourly data backup retention	None
Hourly archive log backup retention	Delete Snapshot copies older than : 7 days
Daily data backup retention	None
Daily archive log backup retention	None
Weekly data backup retention	None
Weekly archive log backup retention	None
Monthly data backup retention	None
Monthly archive log backup retention	None
Replication	SnapMirror enabled , Secondary policy label: Hourly , Error retry count: 3

Previous

Finish

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.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

SQL Server Full Backup

Details

Backup all data and log files

Previous

Next

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.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select SQL server backup options

Choose backup type

☒ Full backup and log backup

☐ Full backup

☐ Log backup

☐ Copy only backup

Maximum databases backed up per Snapshot copy:

Availability Group Settings

Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ On demand

☐ Hourly

☒ Daily

☐ Weekly

☐ Monthly

Previous

Next

4. Defina o período de retenção do backup.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

Retention settings for up-to-the-minute restore operation ⓘ

☒ Keep log backups applicable to last

7

full backups

☐ Keep log backups applicable to last

14

days

Full backup retention settings ⓘ

Daily

☒ Total Snapshot copies to keep

7

☐ Keep Snapshot copies for

14

days

Previous

Next

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

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Daily

Error retry count

3

Previous

Next

6. 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

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 secs

Previous

Next

8. Resumo.

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

Policy name	SQL Server Full Backup
Details	Backup all data and log files
Backup type	Full backup and log backup
Availability group settings	Backup only on preferred backup replica
Schedule Type	Daily
UTM retention	Total backup copies to retain : 7
Daily Full backup retention	Total backup copies to retain : 7
Replication	SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3
Backup prescript settings	undefined Prescript arguments:
Backup postscript settings	undefined Postscript arguments:
Verification for backup schedule type	none
Verification prescript settings	undefined Prescript arguments:
Verification postscript settings	undefined Postscript arguments:

Previous

Finish

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.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

SQL Server Log Backup

Details

Backup SQL server log

Previous

Next

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.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select SQL server backup options

Choose backup type

☐ Full backup and log backup

☐ Full backup

☒ Log backup

☐ Copy only backup

Maximum databases backed up per Snapshot copy: 100

Availability Group Settings

Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ On demand

☒ Hourly

☐ Daily

☐ Weekly

☐ Monthly

Previous

Next

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

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Log backup retention settings

Up-to-the-minute (UTM) retention settings retains log backups created as part of full backup and full and log backup operations. UTM retention settings also decides for how many full backups the log backups are to be retained. For example, if UTM retention settings is configured to retain log backups of the last 5 full backups, then the log backups of the last 5 full backups are retained and the rest are deleted.

Previous

Next

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

New SQL Server Backup Policy ×

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options ⓘ

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label Hourly ⓘ

Error retry count 3 ⓘ

Previous

Next

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.

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

Policy name	SQL Server Log Backup
Details	Backup SQL server log
Backup type	Log transaction backup
Availability group settings	Backup only on preferred backup replica
Schedule Type	Hourly
Replication	SnapMirror enabled , Secondary policy label: Hourly , Error retry count: 3
Backup prescript settings	undefined Prescript arguments:
Backup postscript settings	undefined Postscript arguments:
Verification for backup schedule type	none
Verification prescript settings	undefined Prescript arguments:
Verification postscript settings	undefined Postscript arguments:

Previous

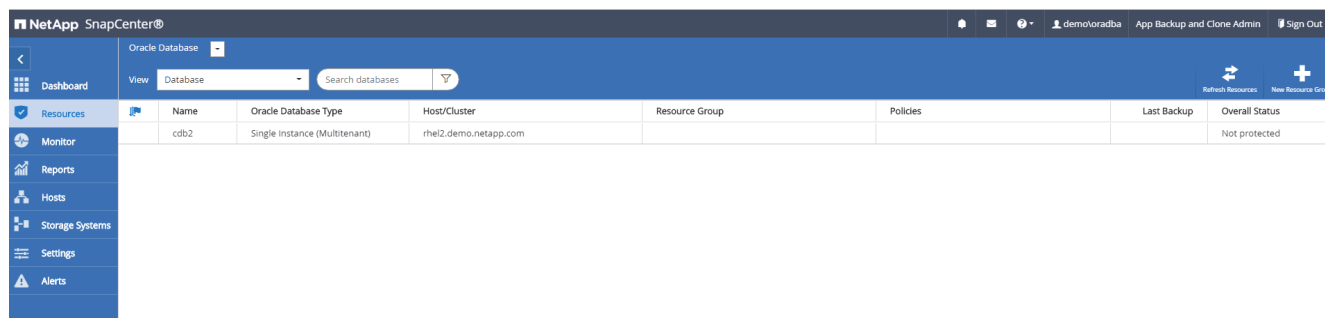
Finish

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.

NetApp SnapCenter®

Oracle Database

Search databases

Name

cdb2

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide a name and tags for the resource group

Name

Tags

☒ Use custom name format for Snapshot copy

Backup settings

Exclude archive log destinations from backup

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

NetApp SnapCenter®

Oracle Database

Search databases

Name

cdb2

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Add resources to Resource Group

Host

Available Resources

search available resources

Selected Resources

cdb2 (rhe12.demo.netapp.com)

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

NetApp SnapCenter®

Oracle Database

Search databases

Name

cdb2

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select one or more policies and configure schedules

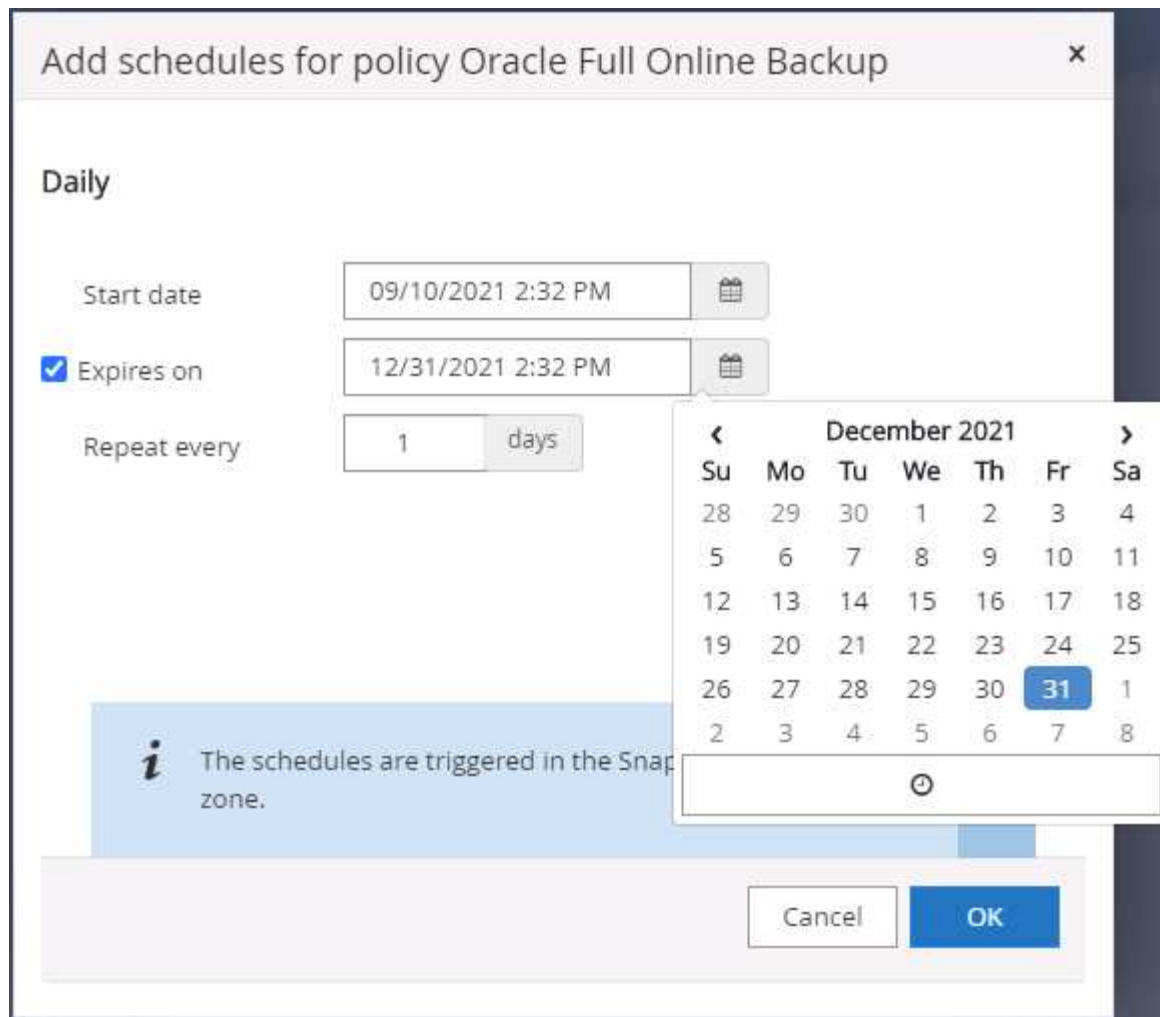
+

Configure schedules for selected policies

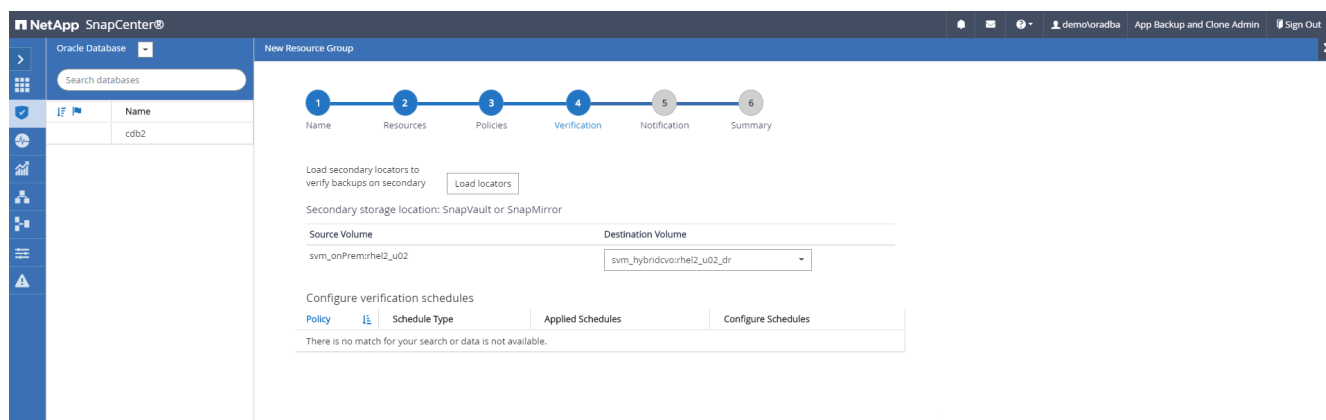
Policy	Applied Schedules	Configure Schedules
Oracle Full Online Backup	None	+

Total 1

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.

Name	Resources	Tags	Policies	Last Backup	Overall Status
rhei2_cdb2	1	orafullbkup	Oracle Full Online Backup		

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.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2_cdb2

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide a name and tags for the resource group

Name: rhel2_cdb2_log

Tags: oragbkup

☒ Use custom name format for Snapshot copy

\$CustomText: rhel2_cdb2_log

Backup settings

Exclude archive log destinations from backup: []

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

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2_cdb2

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Add resources to Resource Group

Host: All

Available Resources

search available resources

Selected Resources

cdb2 (rhel2.demo.netapp.com)

Total 1

Previous Next

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

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2_cdb2

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select one or more policies and configure schedules

Oracle Archive Log Backup

Oracle Full Online Backup

Oracle Archive Log Backup

Policy: Oracle Archive Log Backup

Applied Schedules: None

Configure Schedules: +

Total 1

Previous Next

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

Add schedules for policy Oracle Archive Log Backup

Hourly

Start date

09/10/2021 3:00 PM

☒ Expires on

12/31/2021 3:00 PM

Repeat every

1

hours

0

mins

i

The schedules are triggered in the SnapCenter Server time zone.

Cancel

OK

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

NetApp SnapCenter®

demolatordba App Backup and Clone Admin Sign Out

Oracle Database

New Resource Group

Search resource groups

Name

rhel2_cdb2

Total 1

1

Name

2

Resources

3

Policies

4

Verification

5

Notification

6

Summary

Configure verification schedules

Policy

Schedule Type

Applied Schedules

Configure Schedules

There is no match for your search or data is not available.

Total 0

Previous Next

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

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2_cdb2

Total 1

New Resource Group

If you want to send notifications for scheduled or on demand jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide email settings ⓘ

Select the service accounts or people to notify regarding protection issues.

Email preference: Never

From: From email

To: Email to

Subject: Notification

☐ Attach job report

Previous Next

8. Resumo.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2_cdb2

Total 1

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Resource group name: rhel2_cdb2_log

Tags: oralogbkup

Policy: Oracle Archive Log Backup: Hourly

Plug-in: SnapCenter Plug-in for Oracle Database

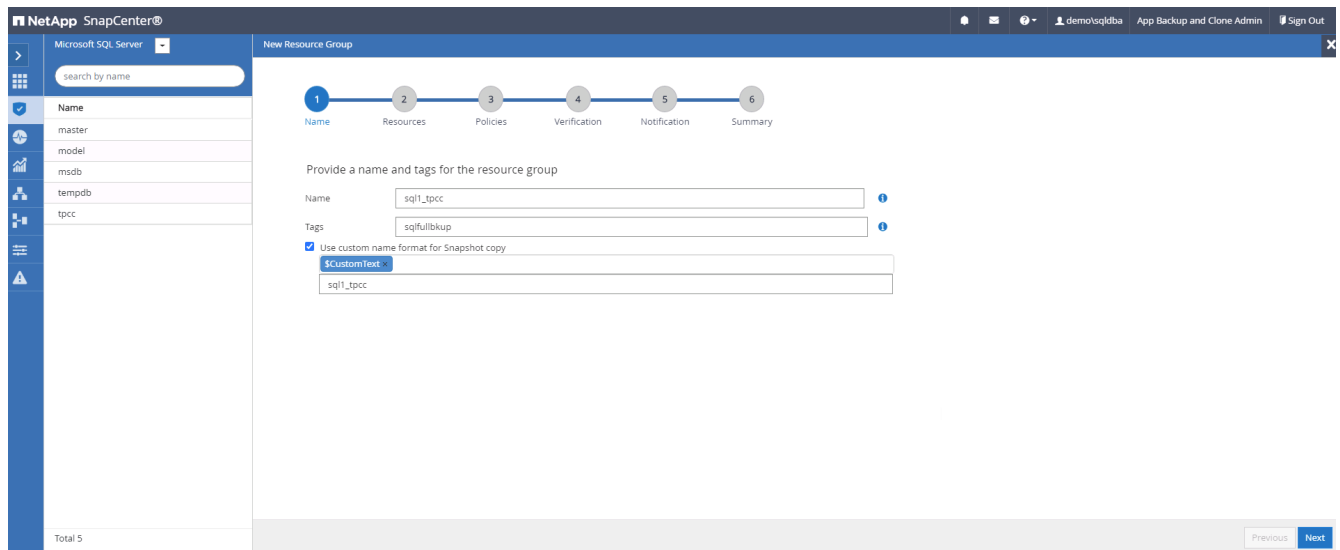
Verification enabled for policy: None

Send email: No

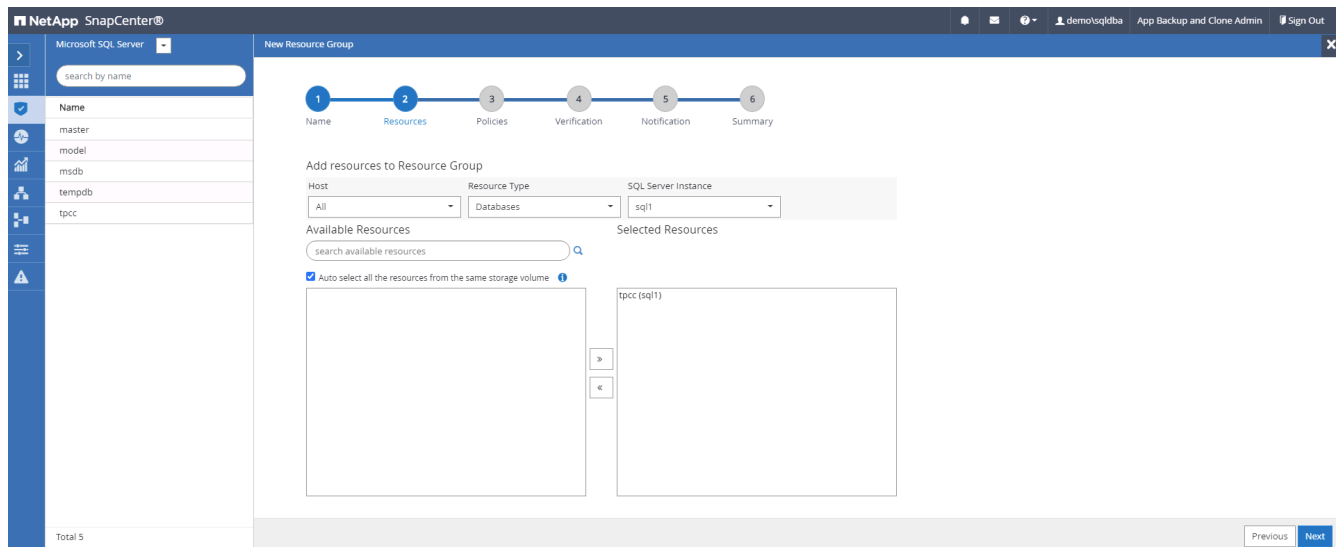
Previous Finish

Crie um grupo de recursos para backup completo do SQL Server

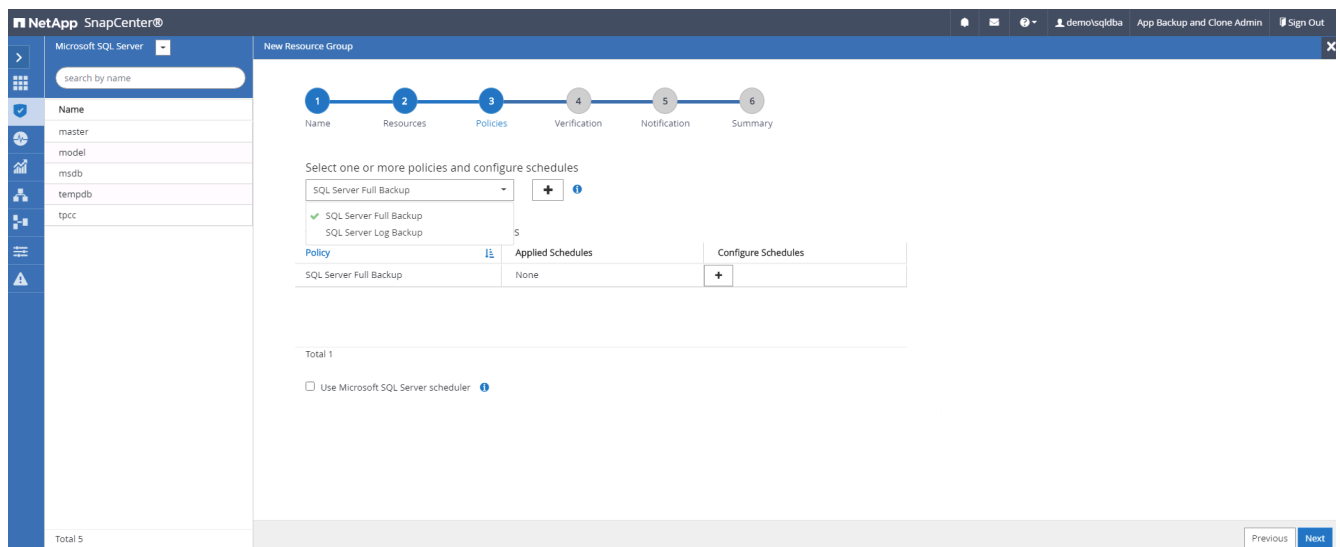
1. Efetue login no SnapCenter com um ID de usuário de gerenciamento de banco de dados e navegue até a guia Recursos. Na lista suspensa Exibir, escolha um Banco de Dados ou Grupo de Recursos para iniciar o fluxo de trabalho de criação do grupo de recursos. Forneça um nome e tags para o grupo de recursos.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

Add schedules for policy SQL Server Full Backup

Daily

Start date

☒ Expires on

Repeat every days

i The schedules are triggered in the SnapCenter Server time zone.

Cancel OK

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.

NetApp SnapCenter®

Microsoft SQL Server

search by name

master

model

msdb

tempdb

tpcc

Total 5

New Resource Group

1 Name

2 Resources

3 Policies

4 Verification

5 Notification

6 Summary

Select the verification servers

Verification server

Load secondary locators to verify backups on secondary

Secondary storage location: SnapVault or SnapMirror

Source Volume

Destination Volume

svm_onPrem:sql1_data

svm_hybridcvosql1_data_dr

svm_onPrem:sql1_log

svm_hybridcvosql1_log_dr

Configure verification schedules

Policy ☒ Schedule Type ☐ Applied Schedules ☐ Configure Schedules ☐

There is no match for your search or data is not available.

Previous Next

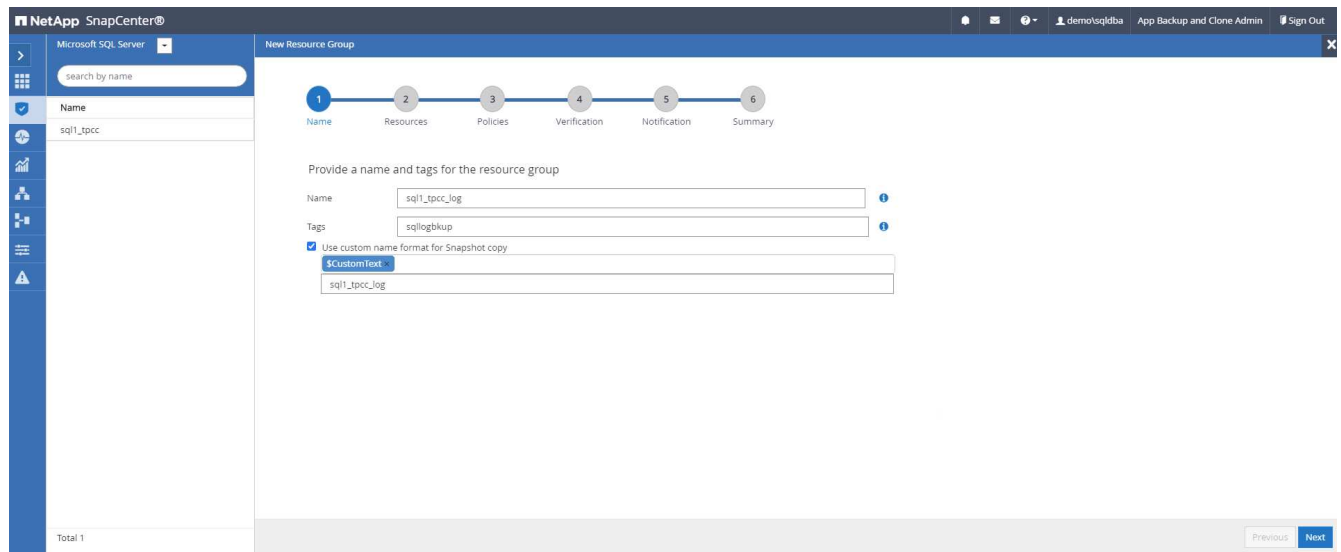
6. Configure o servidor SMTP para notificação por email, se desejar.

59

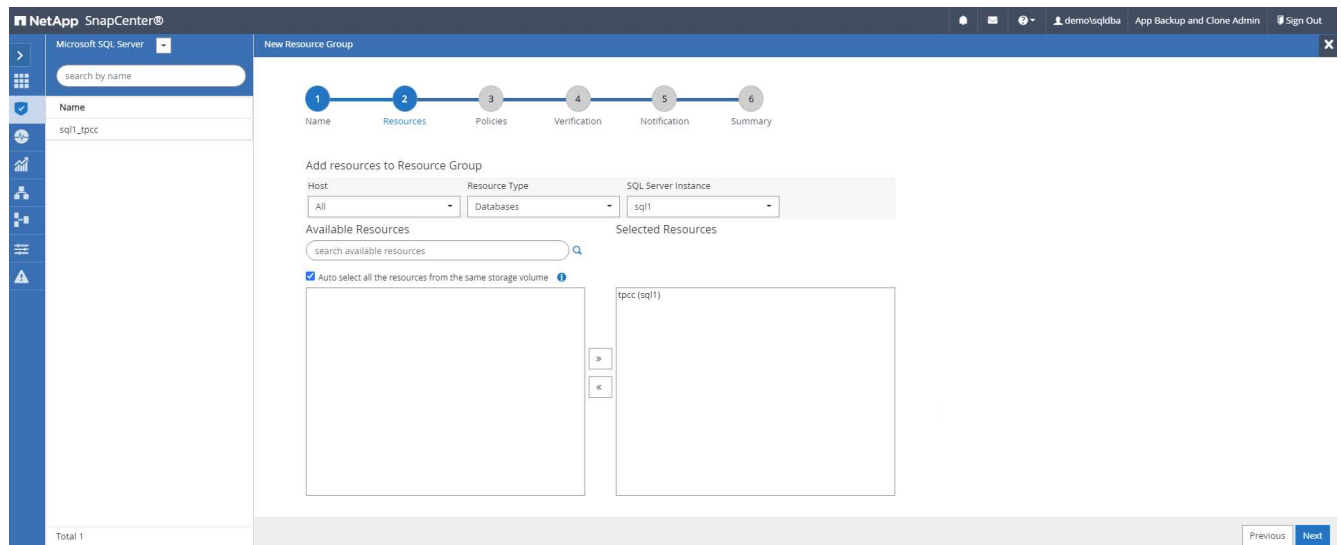
7. Resumo.

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

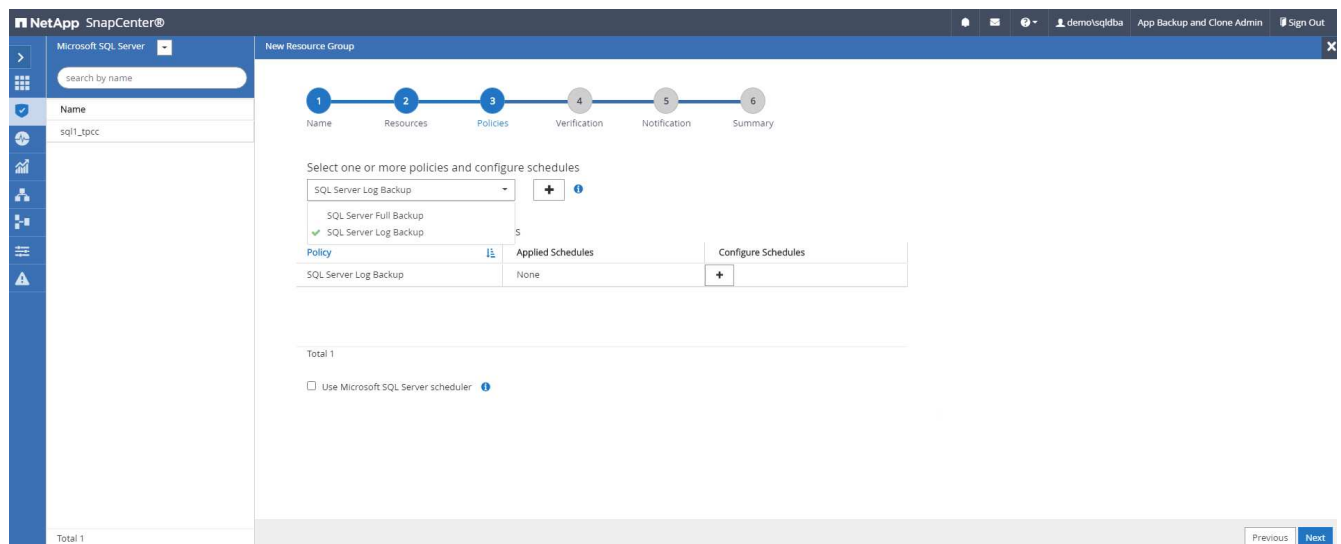
1. Efetue login no SnapCenter com um ID de usuário de gerenciamento de banco de dados e navegue até a guia Recursos. Na lista suspensa Exibir, escolha um Banco de Dados ou Grupo de Recursos para iniciar o fluxo de trabalho de criação do grupo de recursos. Forneça o nome e as tags para o grupo de recursos.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

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

sql1_tpcc

Total 1

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select one or more policies and configure schedules

SQL Server Log Backup

Configure schedules for selected policies

Policy	Applied Schedules	Configure Schedules
SQL Server Log Backup	Hourly: Repeat every 1 hours	✎ ✕

Total 1

☐ Use Microsoft SQL Server scheduler

Previous Next

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.

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

sql1_tpcc

Total 1

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select the verification servers

Verification server: Select one or more servers

Load secondary locators to verify backups on secondary

Load locators

Secondary storage location: SnapVault or SnapMirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridv:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridv:sql1_log_dr

Configure verification schedules

Policy Schedule Type Applied Schedules Configure Schedules

There is no match for your search or data is not available.

Previous Next

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

NetApp SnapCenter®

Microsoft SQL Server

search by name

sql1_tpcc

Total 1

New Resource Group

If you want to send notifications for scheduled or on demand jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide email settings

Select the service accounts or people to notify regarding protection issues.

Email preference: Never

From: From email

To: Email to

Subject: Notification

☐ Attach job report

Previous Next

7. Resumo.

NetApp SnapCenter®

Microsoft SQL Server

search by name

sql1_tpcc

Total 1

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Resource group name: sql1_tpcc_log

Tags: sqllogbkup

Policy: SQL Server Log Backup: Hourly

Plug-in: SnapCenter Plug-in for Microsoft SQL Server

Verification Server: None

Verification enabled for policy: None

Send email: No

Previous Finish

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.

NetApp SnapCenter®

Jobs Schedules Events Logs

search by name

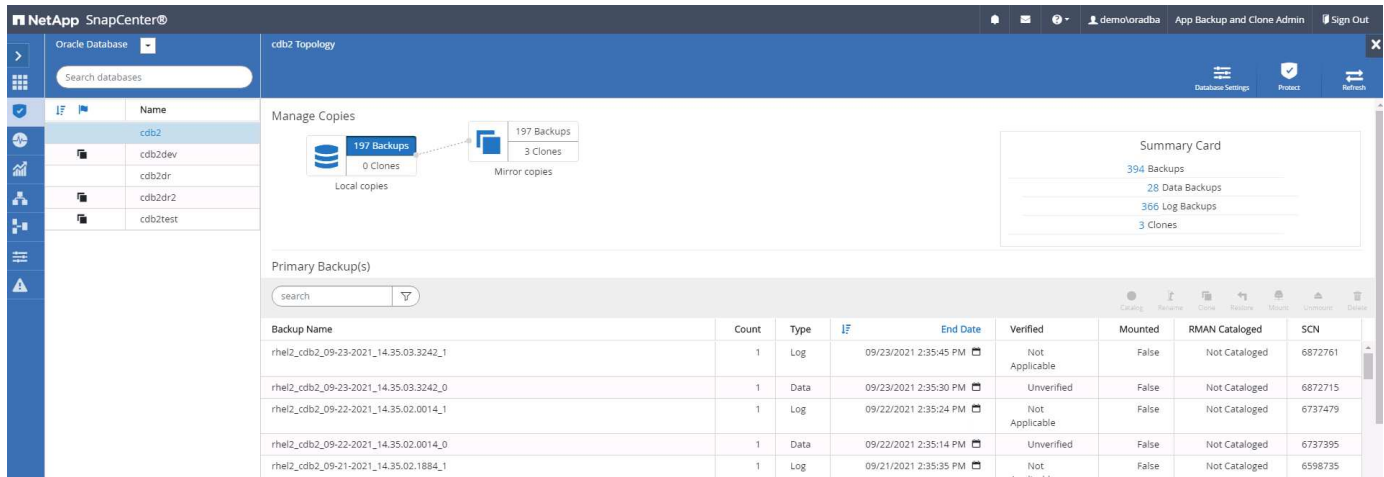
Dashboard Resources Monitor Reports Hosts Storage Systems Settings Alerts

Jobs - Filter

ID	Status	Name	Start date	End date	Owner
532	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 8:35:01 PM	09/14/2021 8:37:10 PM	demo/sqldba
528	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 7:35:01 PM	09/14/2021 7:37:09 PM	demo/sqldba
524	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 6:35:01 PM	09/14/2021 6:37:08 PM	demo/sqldba
521	✓	Backup of Resource Group 'sql1_tpcc' with policy 'SQL Server Full Backup'	09/14/2021 6:25:01 PM	09/14/2021 6:27:14 PM	demo/sqldba
517	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 5:35:01 PM	09/14/2021 5:37:09 PM	demo/sqldba
513	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 4:35:01 PM	09/14/2021 4:37:08 PM	demo/sqldba
509	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 3:35:01 PM	09/14/2021 3:37:10 PM	demo/sqldba
503	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 2:35:01 PM	09/14/2021 2:37:09 PM	demo/sqldba

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.



Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_09-23-2021_14.35.03.3242_1	1	Log	09/23/2021 2:35:45 PM	Not Applicable	False	Not Cataloged	6872761
rhel2_cdb2_09-23-2021_14.35.03.3242_0	1	Data	09/23/2021 2:35:30 PM	Unverified	False	Not Cataloged	6872715
rhel2_cdb2_09-22-2021_14.35.02.0014_1	1	Log	09/22/2021 2:35:24 PM	Not Applicable	False	Not Cataloged	6737479
rhel2_cdb2_09-22-2021_14.35.02.0014_0	1	Data	09/22/2021 2:35:14 PM	Unverified	False	Not Cataloged	6737395
rhel2_cdb2_09-21-2021_14.35.02.1884_1	1	Log	09/21/2021 2:35:35 PM	Not Applicable	False	Not Cataloged	6598735

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.



[Continue to Cloud Manager](#)

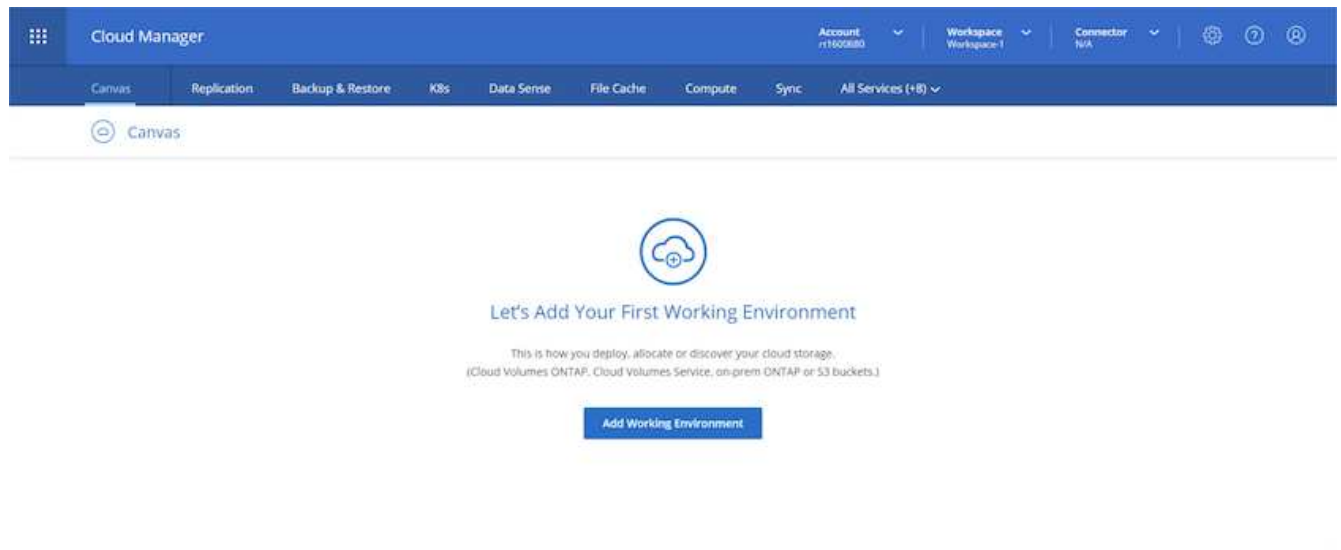
Log In to NetApp Cloud Central

Don't have an account yet? [Sign Up](#)

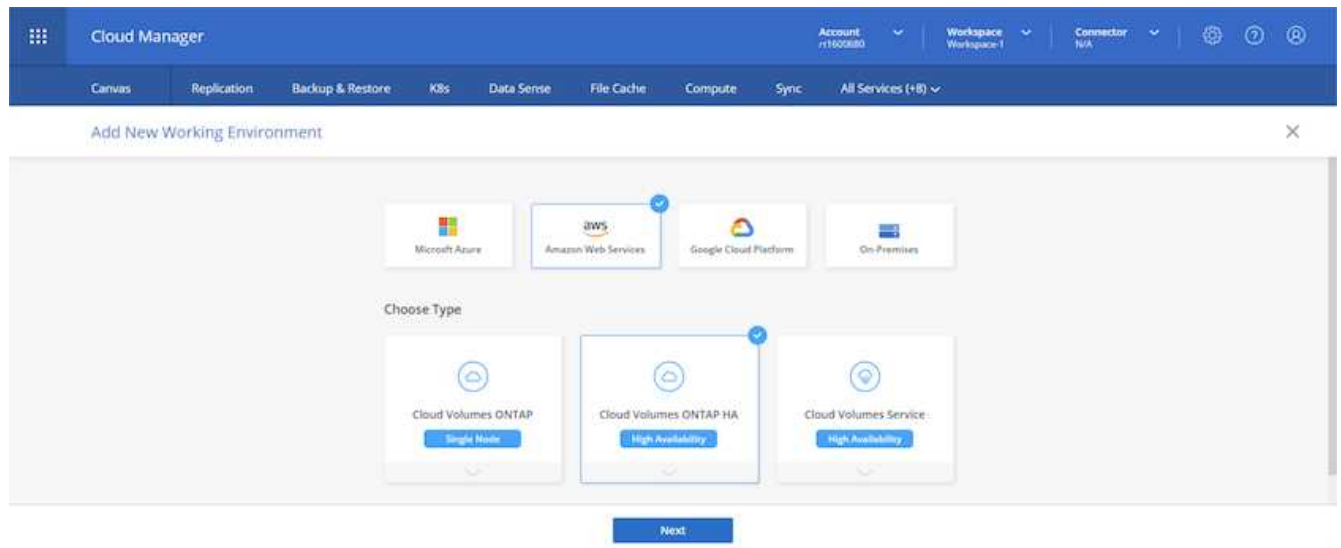
LOGIN

[Forgot your password?](#)

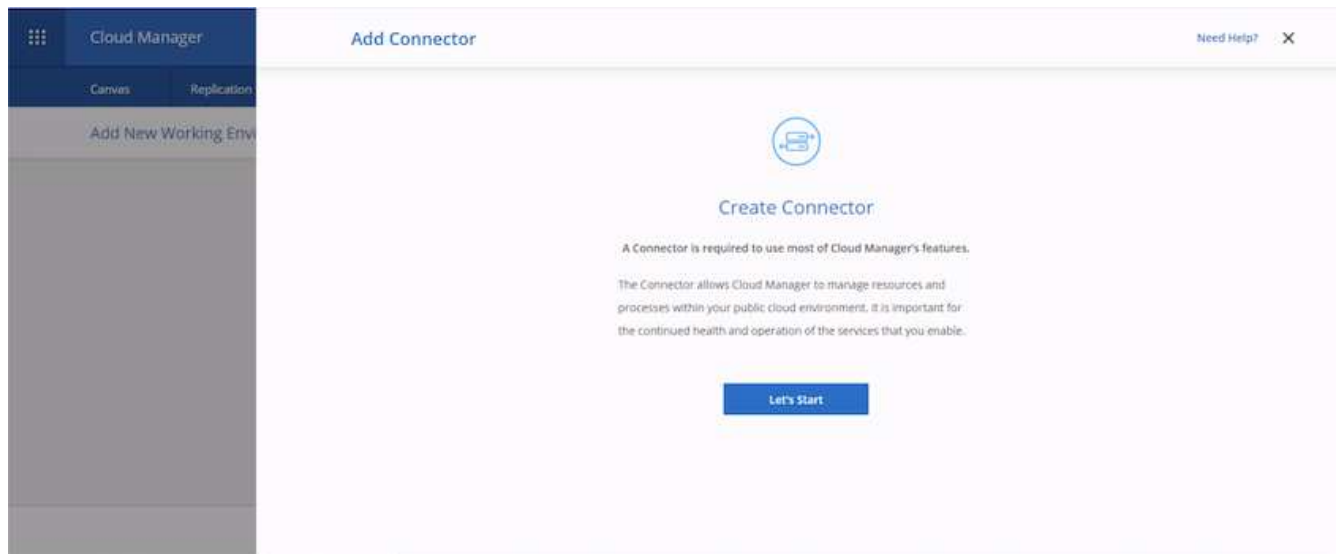
2. Após efetuar login, você será levado ao Canvas.



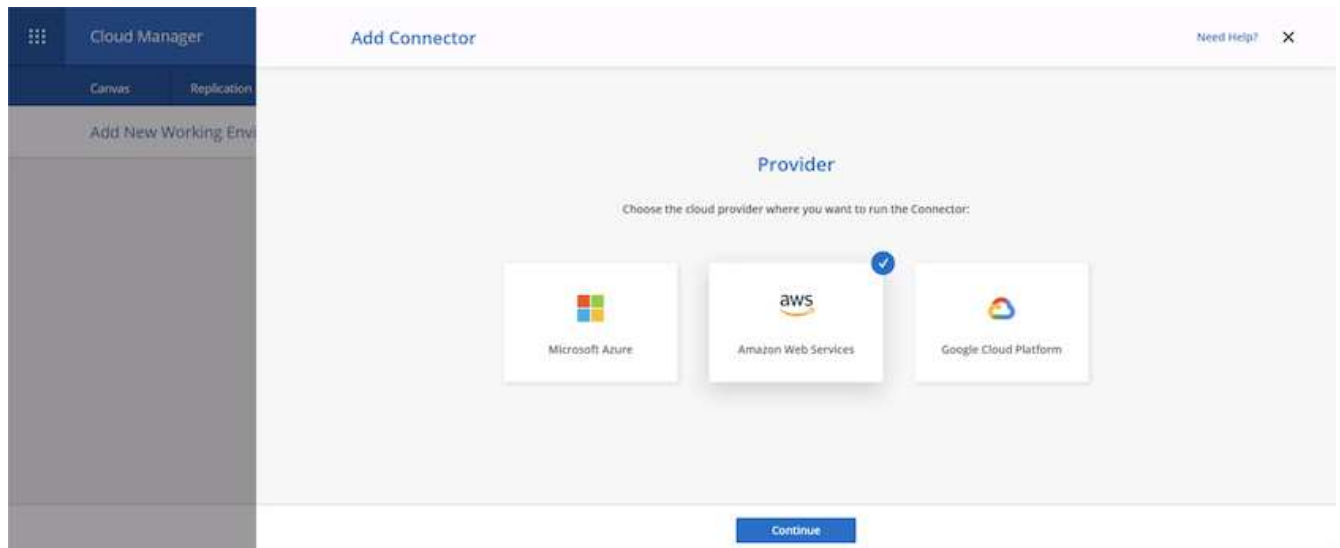
3. Clique em "Adicionar ambiente de trabalho" e escolha Cloud Volumes ONTAP na AWS. Aqui, você também escolhe se deseja implantar um sistema de nó único ou um par de alta disponibilidade. Optei por implantar um par de alta disponibilidade.



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](#)".

Cloud Manager

Add Connector

Need Help? X

Get Ready AWS Credentials Details Network Security Group Review

AWS Credentials

AWS Access Key

AWS Access Key is required

AWS Secret Key

Region

us-east-1 | US East (N. Virginia)

Want to launch an instance without AWS Credentials?

Previous Next

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.

Cloud Manager

Add Connector

Need Help? X

Get Ready AWS Credentials Details Network Security Group Review

Details

Connector Instance Name

awscloudmanager

Connector Role

Create Role Select an existing Role

Add Tags to Connector Instance

Role Name

Cloud-Manager-Operator-IBHt24j

Previous Next

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

Add Connector

Get Ready AWS Credentials Details **Network** Security Group Review

Connectivity

VPC: vpc-083fcbd79f75dfb6e - 10.221.0.0/16

Subnet: 10.221.4.0/24 | publicSN_us-east-1a_rt1600680

Key Pair: rt1600680

Public IP: Enable

Proxy Configuration (Optional)

HTTP Proxy: Example: https://172.16.254.1:8080

Define Credentials for this Proxy

Upload a root certificate

Previous Next

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

Add Connector

Get Ready AWS Credentials Details Network **Security Group** Review

The security group must allow inbound HTTP, HTTPS and SSH access.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

HTTP (Port 80)

Source Type: My IP

Source (CIDR): 216.240.31.145/32

HTTPS (Port 443)

Source Type: My IP

Source (CIDR): 216.240.31.145/32

SSH (Port 22)

Source Type: My IP

Source (CIDR): 216.240.31.145/32

Previous Next

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

Add Connector

Get Ready AWS Credentials Details Network Security Group **Review**

Code for Terraform Automation

Connector Name: awscloudmanager

Region: us-east-1

VPC: vpc-083fcbd79f75dfb6e - 10.221.0.0/16

Subnet: 10.221.4.0/24 | publicSN_us-east-1a_rt1600680

Key Pair: rt1600680

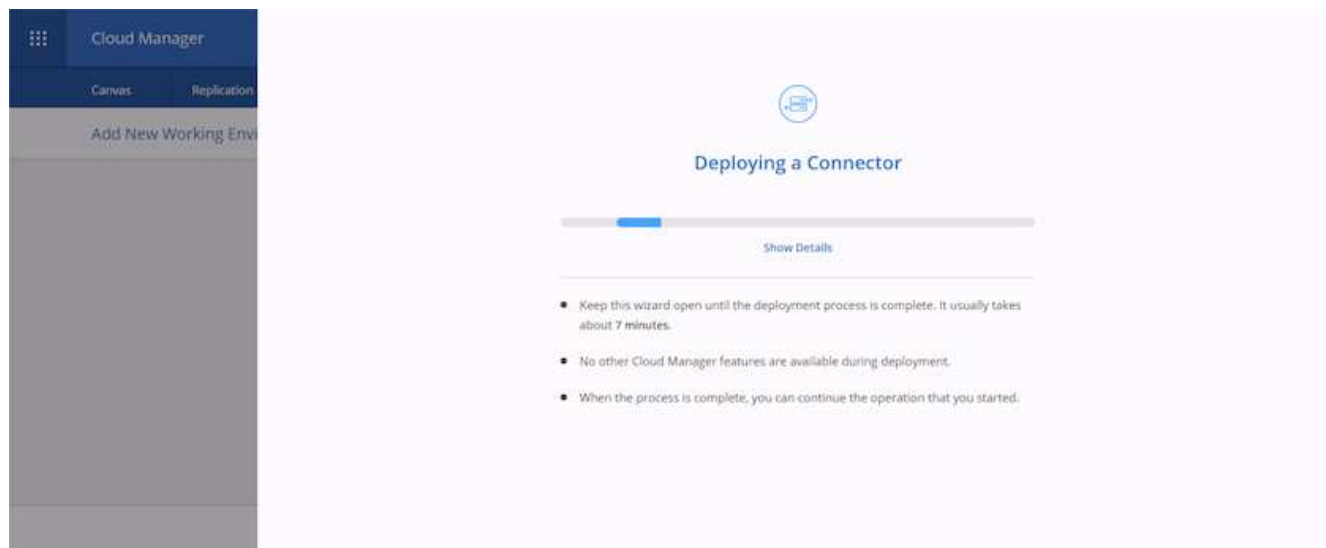
Public IP: Enable

Proxy: None

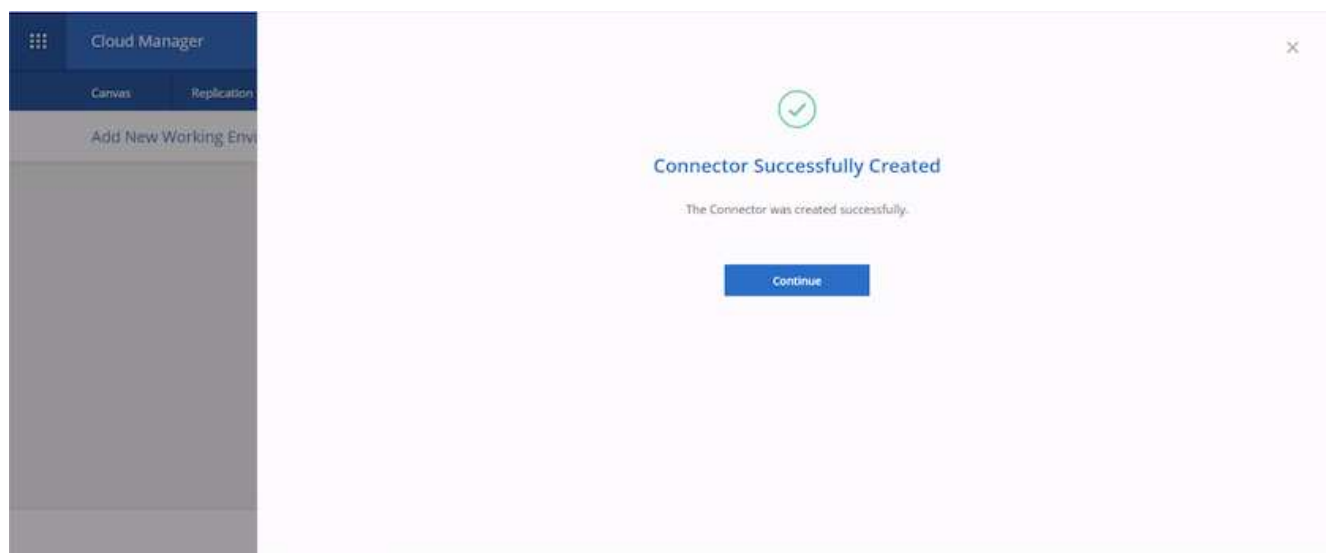
Security Group: HTTP: 216.240.31.145/32, HTTPS: 216.240.31.145/32, SSH: 216.240.31.145/32

Previous Add

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

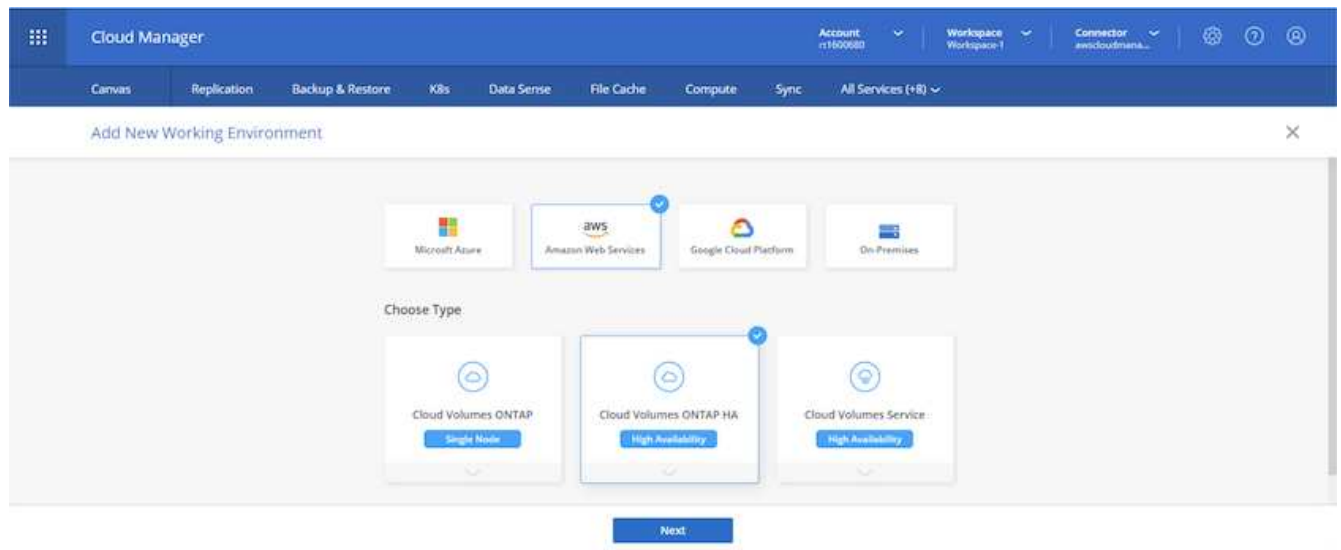


12. Quando a implantação estiver concluída, uma página de sucesso será exibida.

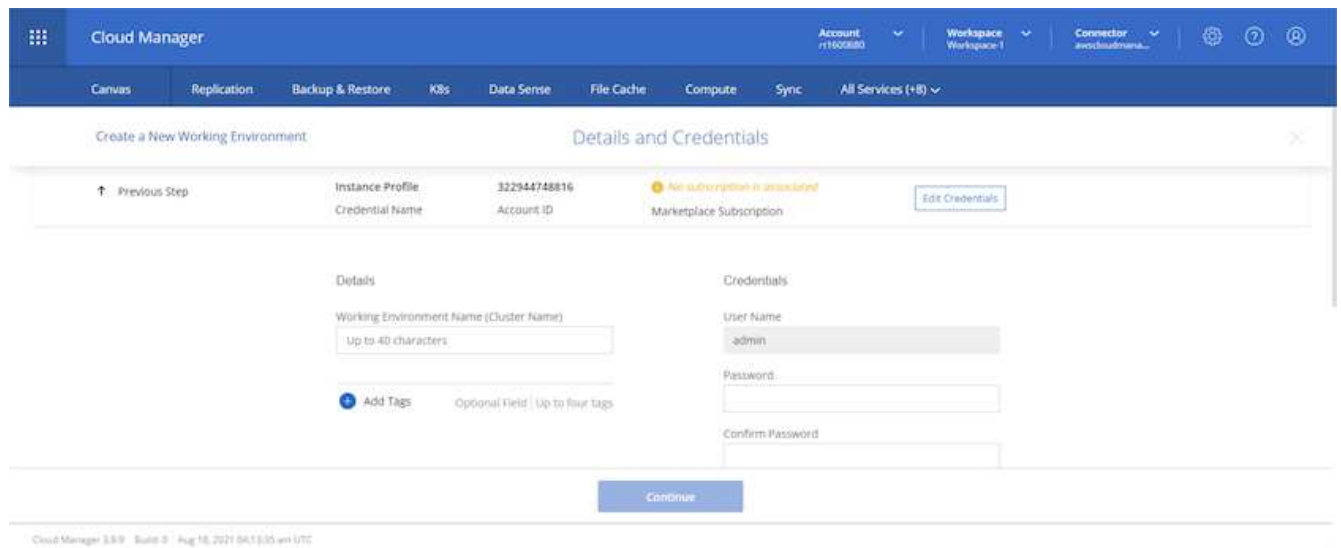


Implantar Cloud Volumes ONTAP

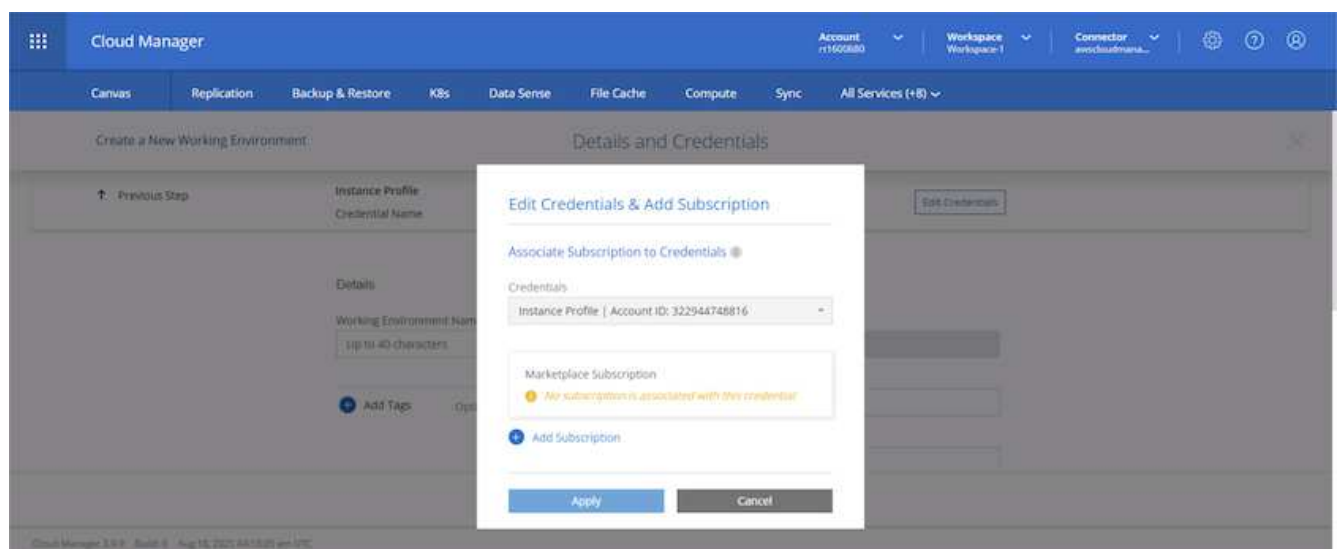
1. Selecione AWS e o tipo de implantação com base em seus requisitos.



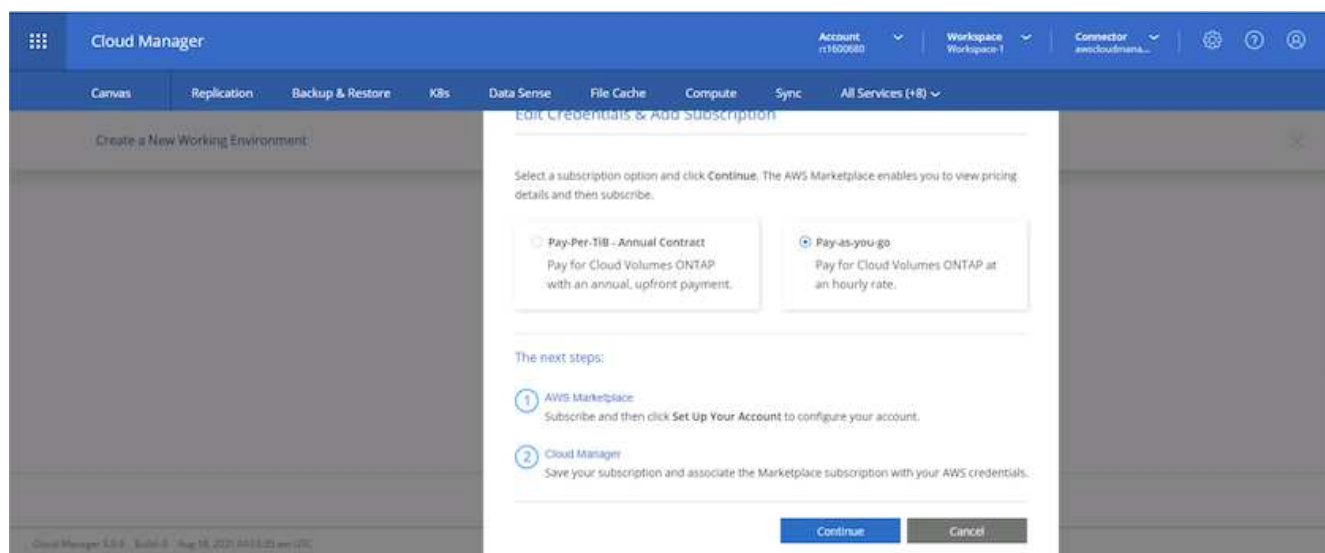
2. Se nenhuma assinatura foi atribuída e você deseja comprar com o PAYGO, escolha Editar credenciais.



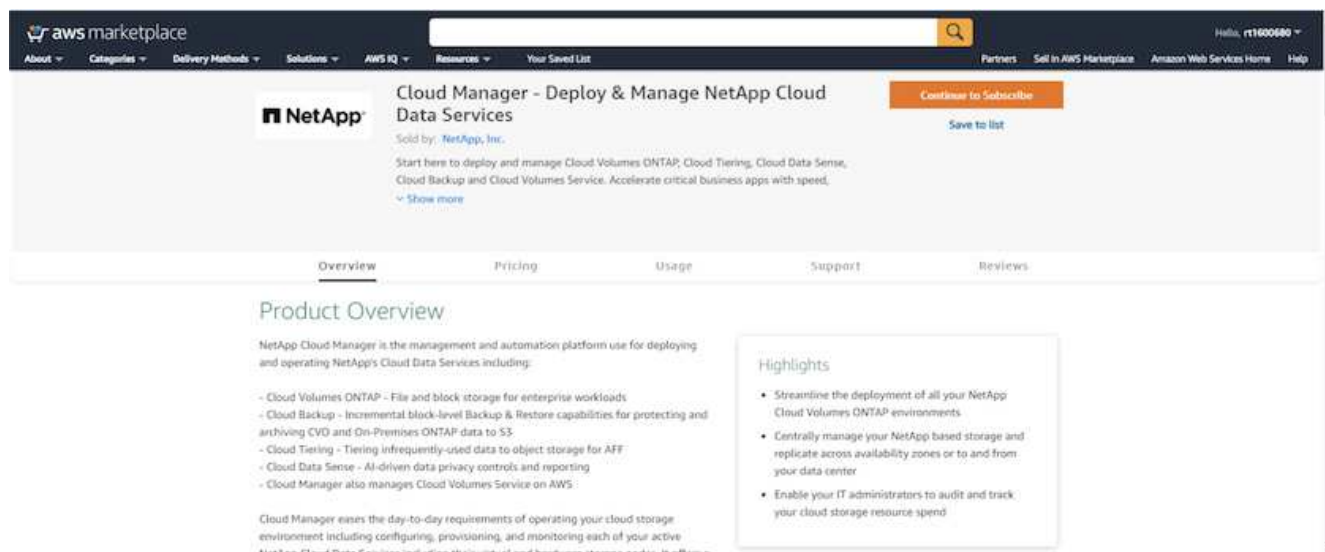
3. Selecione Adicionar assinatura.



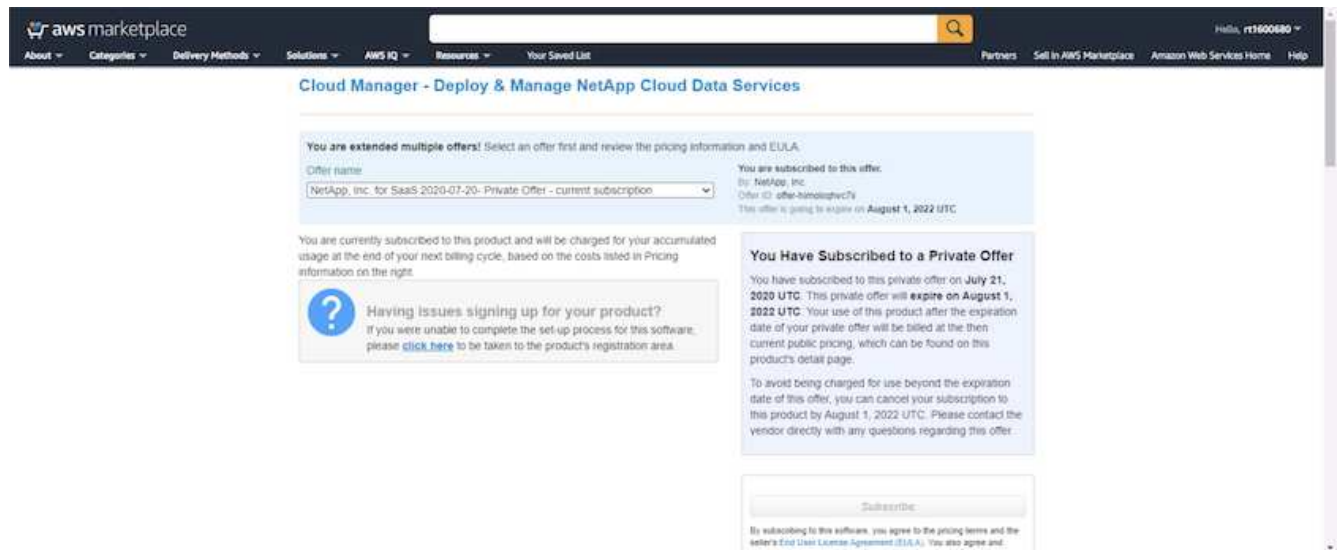
4. Selecione o tipo de contrato que deseja assinar. Eu escolhi o pagamento conforme o uso.



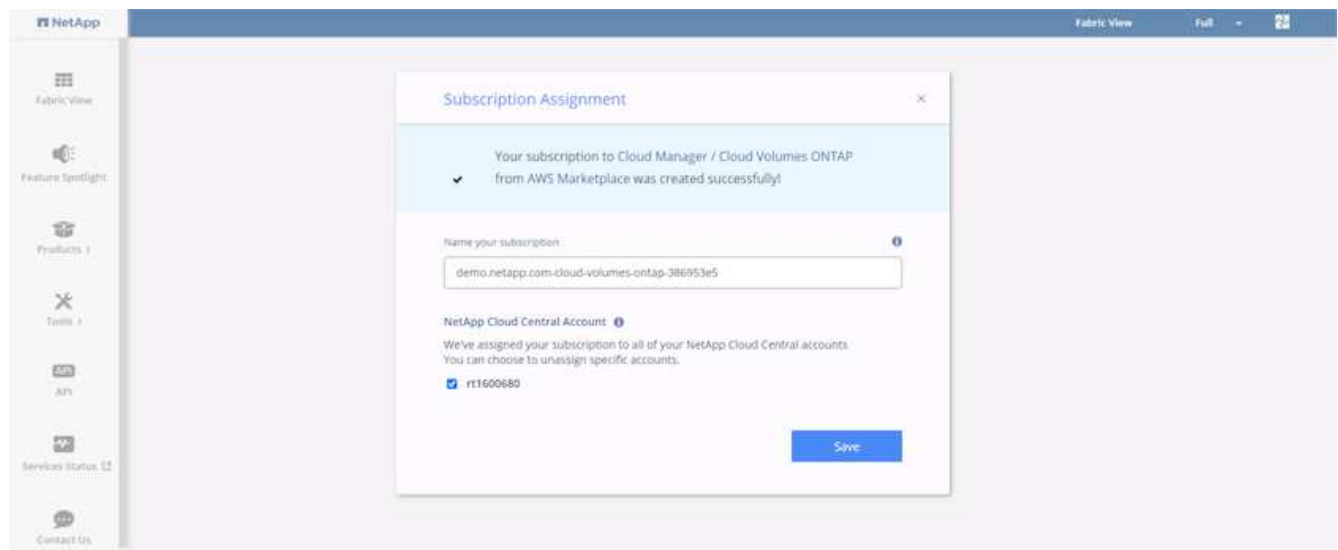
5. Você será redirecionado para a AWS; escolha Continuar para assinar.



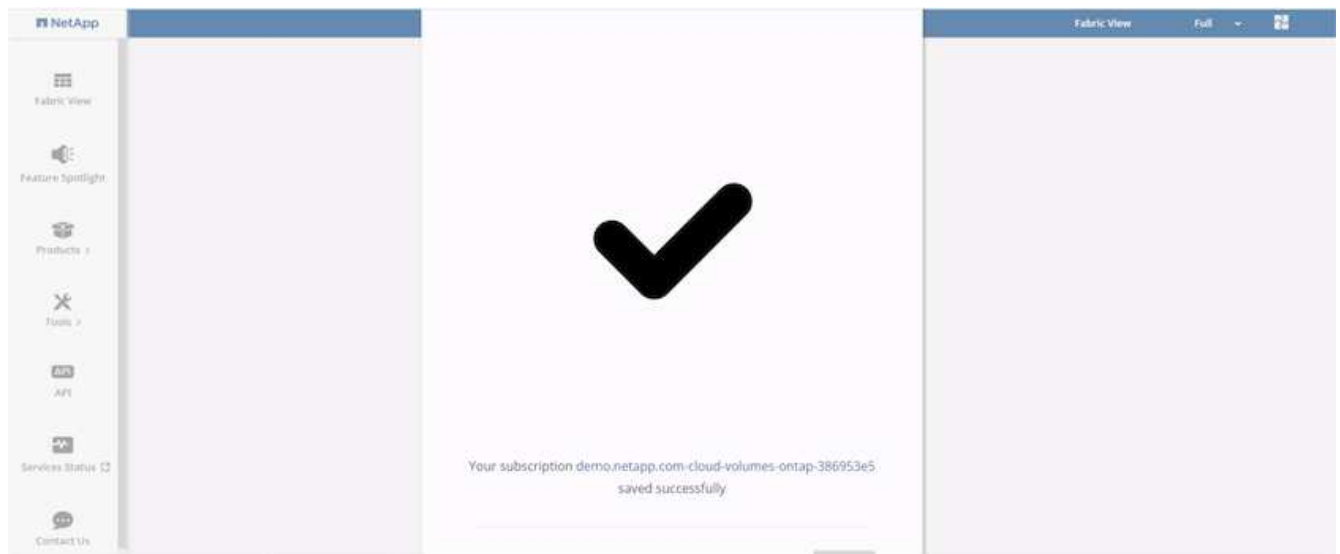
6. Assine e você será redirecionado de volta ao NetApp Cloud Central. Se você já se inscreveu e não for redirecionado, escolha o link "Clique aqui".



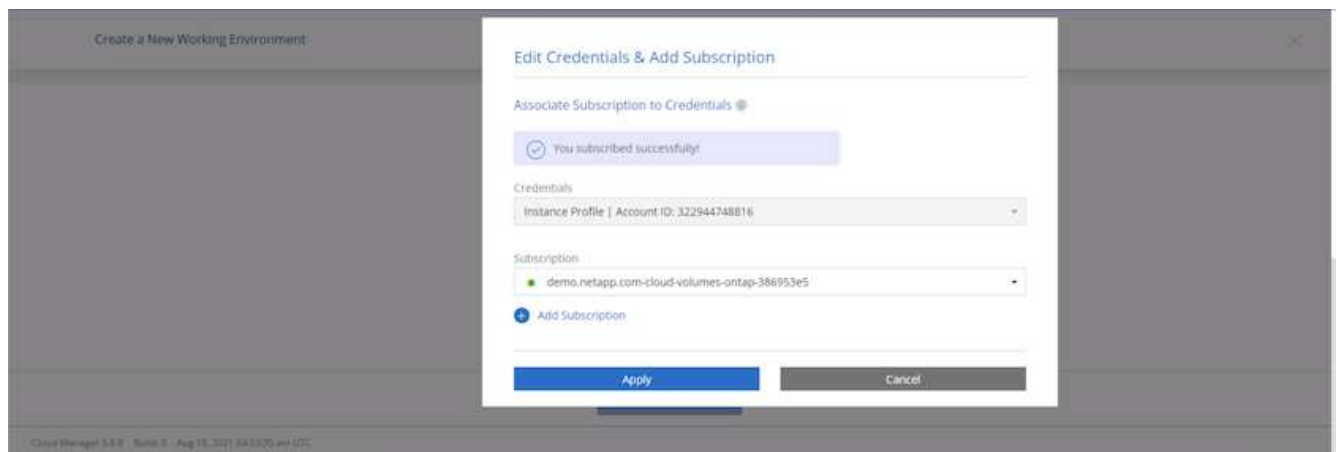
7. Você será redirecionado para o Cloud Central, onde deverá nomear sua assinatura e atribuí-la à sua conta do Cloud Central.



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)

The screenshot shows the 'Details and Credentials' step in the Cloud Manager interface. The top navigation bar includes 'Cloud Manager', 'Account: r1600880', 'Workspace: Workspace 1', and 'Connector: awscloudmana...'. The main navigation menu lists 'Canvas', 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'File Cache', 'Compute', 'Sync', and 'All Services (+8)'. The 'Create a New Working Environment' window is open, showing a 'Previous Step' button and a table with the following details:

Instance Profile	322944748816	demo.netapp.com-cloud-vol...
Credential Name	Account ID	Marketplace Subscription

Below the table, there are two sections: 'Details' and 'Credentials'. The 'Details' section has a 'Working Environment Name (Cluster Name)' field with the value 'hybridawsco' and an 'Add Tags' button. The 'Credentials' section has 'User Name' (admin), 'Password' (masked), and 'Confirm Password' (masked) fields. A 'Continue' button is at the bottom. The footer indicates 'Cloud Manager 3.9.9 - Build 0 - Aug 18, 2021 06:13:35 am UTC'.

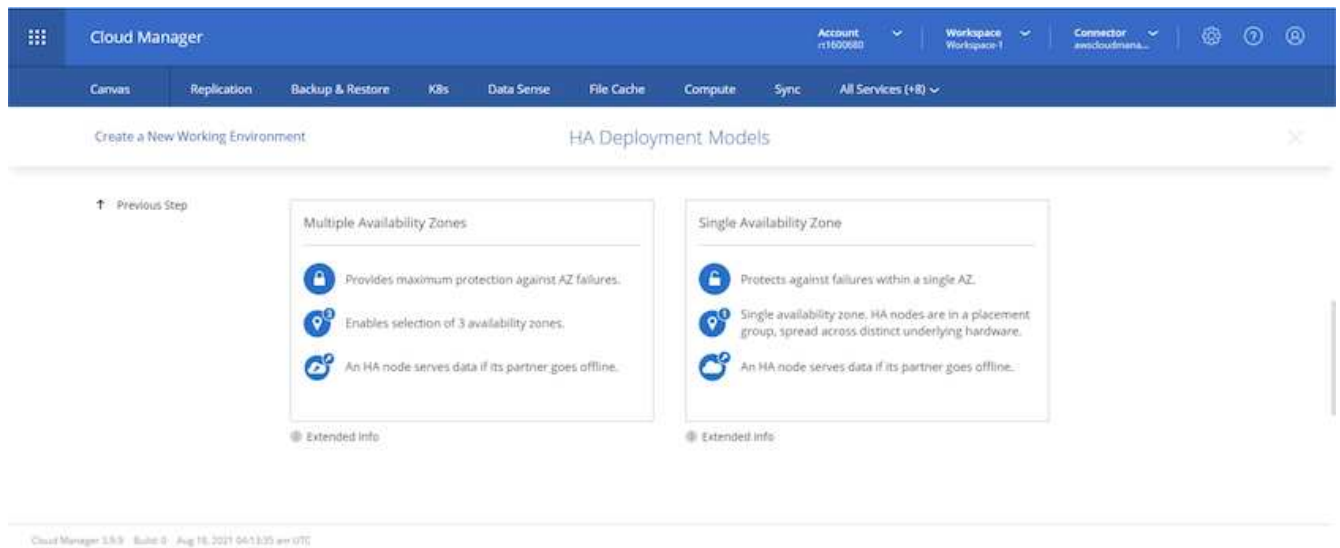
- Escolha quais serviços adicionais você gostaria de implantar. Para saber mais sobre esses serviços, visite o ["BlueXP: Operações modernas de propriedade de dados simplificadas"](#).

The screenshot shows the 'Services' step in the Cloud Manager interface. The top navigation bar and main navigation menu are the same as in the previous screenshot. The 'Create a New Working Environment' window is open, showing a 'Previous Step' button and a list of services with toggle switches and dropdown menus:

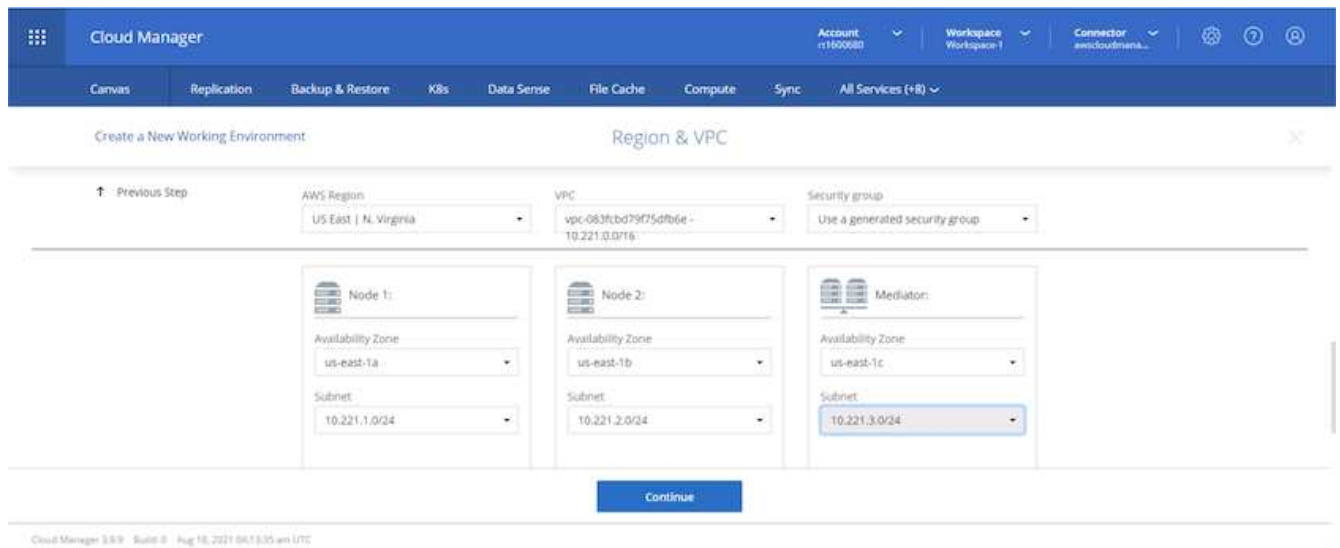
- Data Sense & Compliance
- Backup to Cloud
- Monitoring

A 'Continue' button is at the bottom. The footer indicates 'Cloud Manager 3.9.9 - Build 0 - Aug 18, 2021 06:13:35 am UTC'.

- 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.

Cloud Manager

Account: rt1600680 | Workspace: Workspace 1 | Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8)

Create a New Working Environment | Connectivity & SSH Authentication

Previous Step

Nodes

SSH Authentication Method: Password

Mediator

Security Group: Use a generated security group

Key Pair Name: rt1600680

Internet Connection Method: Public IP address

Continue

Cloud Manager 3.8.9 | Build 2 | Aug 18, 2021 06:13:35 am UTC



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"](#).

Cloud Manager

Account: rt1618349 | Workspace: Workspace-1 | Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8)

Create a New Working Environment | Floating IPs

Previous Step

Floating IP addresses are required for cluster and SVM access and for NFS and CIFS data access. These floating IPs can migrate between HA nodes if failures occur. To access the data from outside the VPC, you can set up an AWS transit gateway.

You must specify IP addresses that are outside of the CIDR blocks for all VPCs in the selected AWS region.

Floating IP address for cluster management: 10.222.0.200

Floating IP address 1 for NFS and CIFS data: 10.222.0.201

Floating IP address 2 for NFS and CIFS data: 10.222.0.202

Floating IP address for SVM management (Optional): Enter Floating IP Address

Continue

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.

Cloud Manager

Account: r1600680 Workspace: Workspace 1 Connector: #wicloudmana...

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8)

Create a New Working Environment Route Tables

Previous Step

Select the route tables that should include routes to the floating IP addresses. This enables client access to the Cloud Volumes ONTAP HA pair. If you leave a route table unselected, clients that are associated with the route table cannot access the HA pair.

Additional information ⓘ

☒	Name	Main	ID	Associate with Subnet	Tags
☒	private_rt_r1600680	No	rtb-08b4cb88f5c826a5	3 Subnets	1 Tags
☒	public_rt_r1600680	Yes	rtb-0e46720d0da10c593	1 Subnets	1 Tags

2 Route Tables | The main route table is the default for the VPC

Continue

Cloud Manager 3.8.9 Build 0 Aug 18, 2021 06:13:35 am UTC

- 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 .

Cloud Manager

Account: r1600680 Workspace: Workspace 1 Connector: #wicloudmana...

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8)

Create a New Working Environment Data Encryption

Previous Step

 AWS Managed Encryption

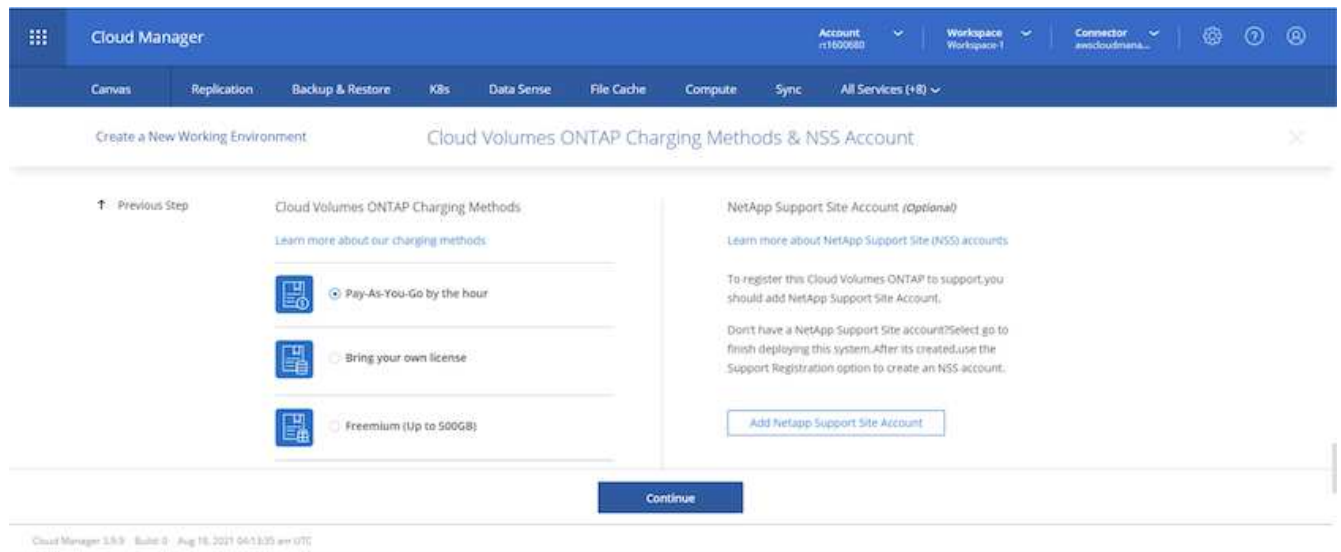
AWS is responsible for data encryption and decryption operations. Key management is handled by AWS key management services.

Default Master Key: aws/ebs

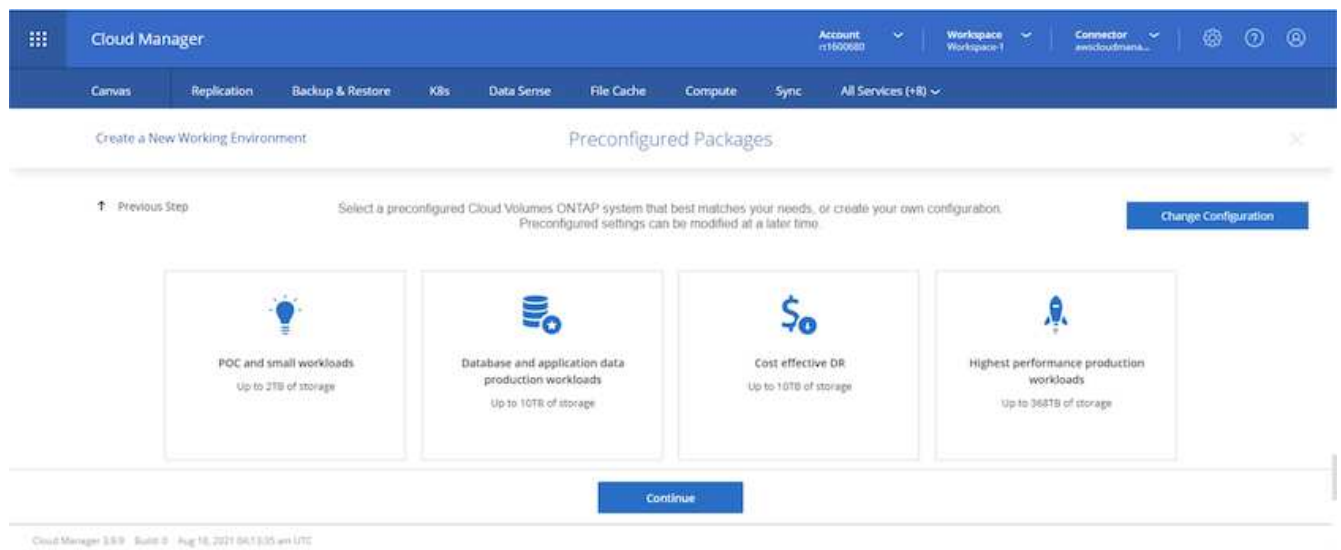
Continue

Cloud Manager 3.8.9 Build 0 Aug 18, 2021 06:13:35 am UTC

- 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.

Cloud Manager

Account: r1600880 | Workspace: Workspace 1 | Connector: #workspace...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8)

Create a New Working Environment | Create Volume

Previous Step

Details & Protection

Volume Name: | Size (GB): | Volume size:

Snapshot Policy: | Default Policy

Protocol

NFS | CIFS | iSCSI

Access Control:

Custom export policy:

Advanced options:

Continue | Skip

Cloud Manager 3.9.9 | Build 9 | Aug 18, 2021 04:13:35 am UTC

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.

Cloud Manager

Account: r1600880 | Workspace: Workspace 1 | Connector: #workspace...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8)

Create a New Working Environment | Review & Approve

Previous Step | hybridawscvo | Show API request

☒ I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp. [More information >](#)

☒ I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements. [More information >](#)

Overview | Networking | Storage

Storage System: Cloud Volumes ONTAP HA | HA Deployment Model: Multiple Availability Zones

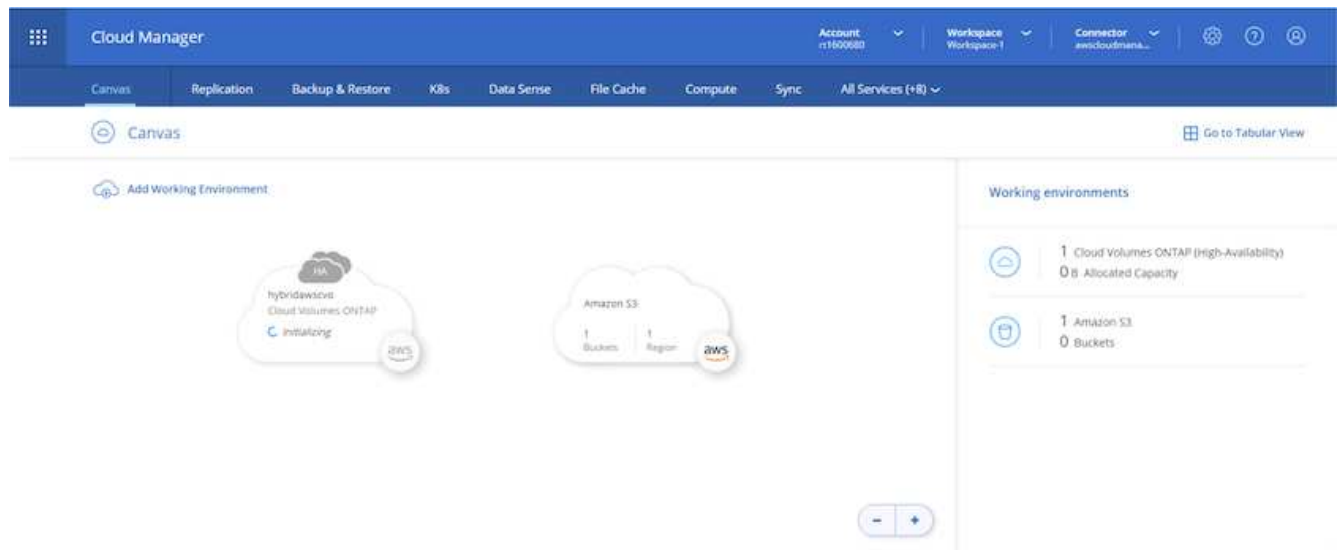
License Type: Cloud Volumes ONTAP Standard | Encryption: AWS Managed

Capacity Limit: 10TB | Customer Master Key: aws/ebc

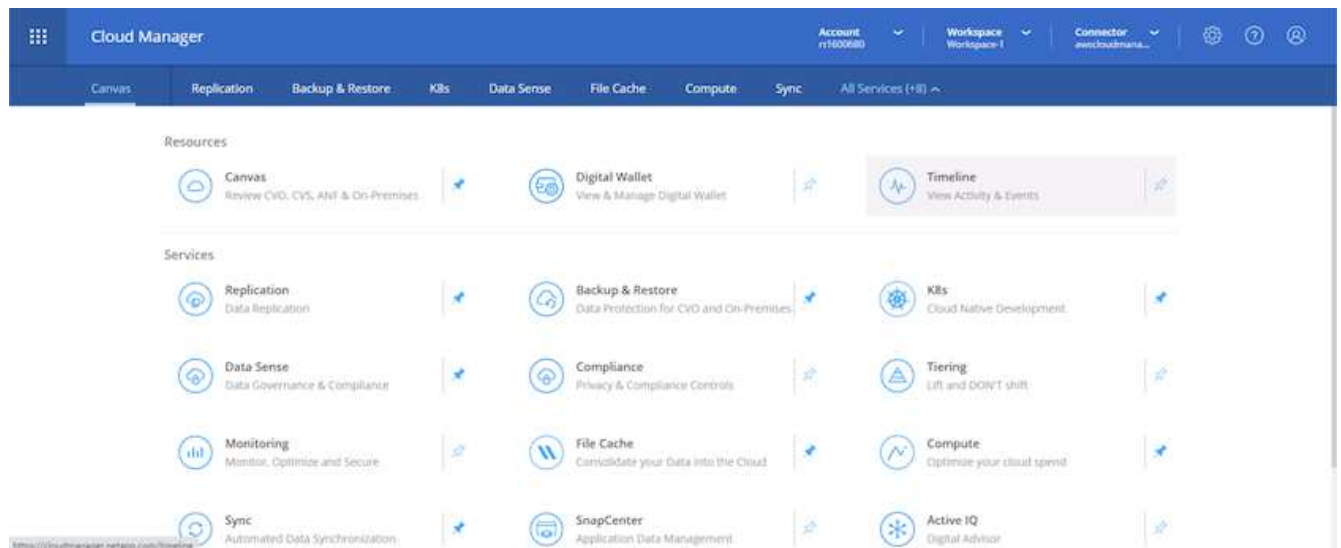
Go

Cloud Manager 3.9.9 | Build 9 | Aug 18, 2021 04:13:35 am UTC

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.

Cloud Manager

Account: r1600680 | Workspace: Workspace-1 | Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8)

Timeline

Filters: Time (1) | Service | Action | Agent (1) | Resource | User | Status | Reset

Time	Action	Service	Agent	Resource	User	Status
Aug 18 2021, 9:42:32 pm	Check Connectivity	Cloud Manager	awscloudman...	hybridawsco	Full Name	Success
Aug 18 2021, 9:42:00 pm	Create Aws Ha Working Environment	Cloud Manager	awscloudma...	hybridawsco	Full Name	Pending
Aug 18 2021, 10:09:39 pm	Describe Operation Status					Success
Aug 18 2021, 10:00:03 pm	Describe Operation Status					Success

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.

Cloud Manager

Account: r1600680 | Workspace: Workspace-1 | Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8)

Canvas

Add Working Environment

Working environments

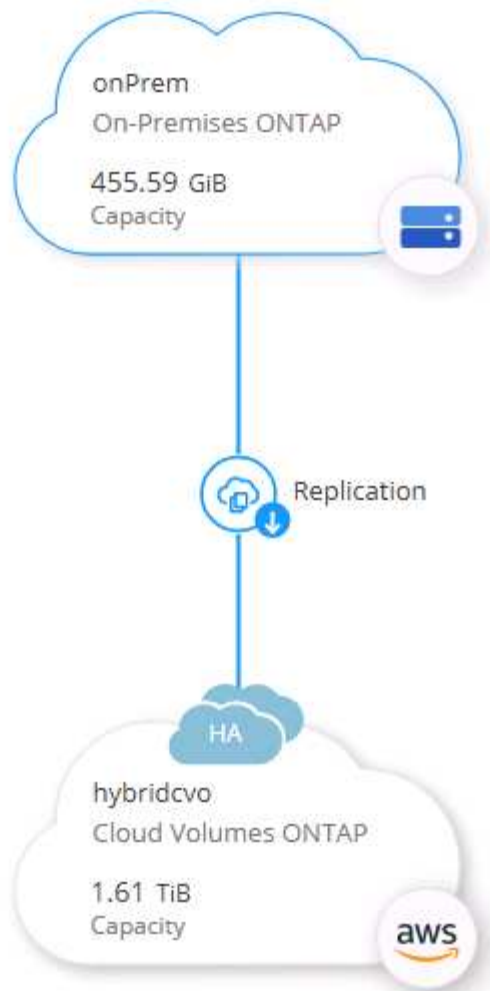
- 1 Cloud Volumes ONTAP (High-Availability)
1 GB Allocated Capacity
- 1 Amazon S3
0 Buckets

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.

SERVICES



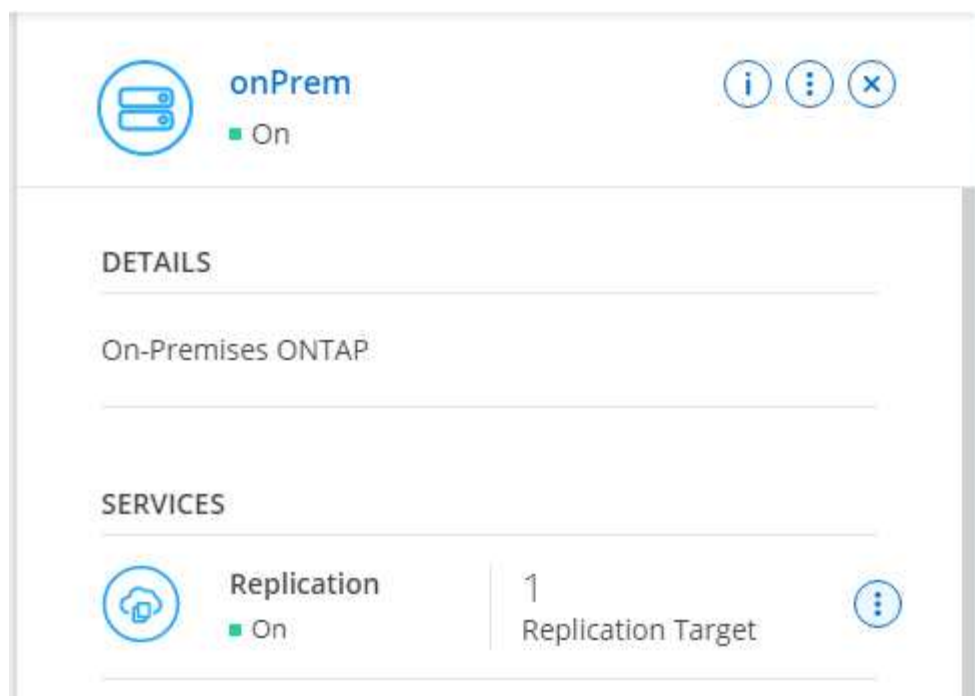
Replication

■ Off

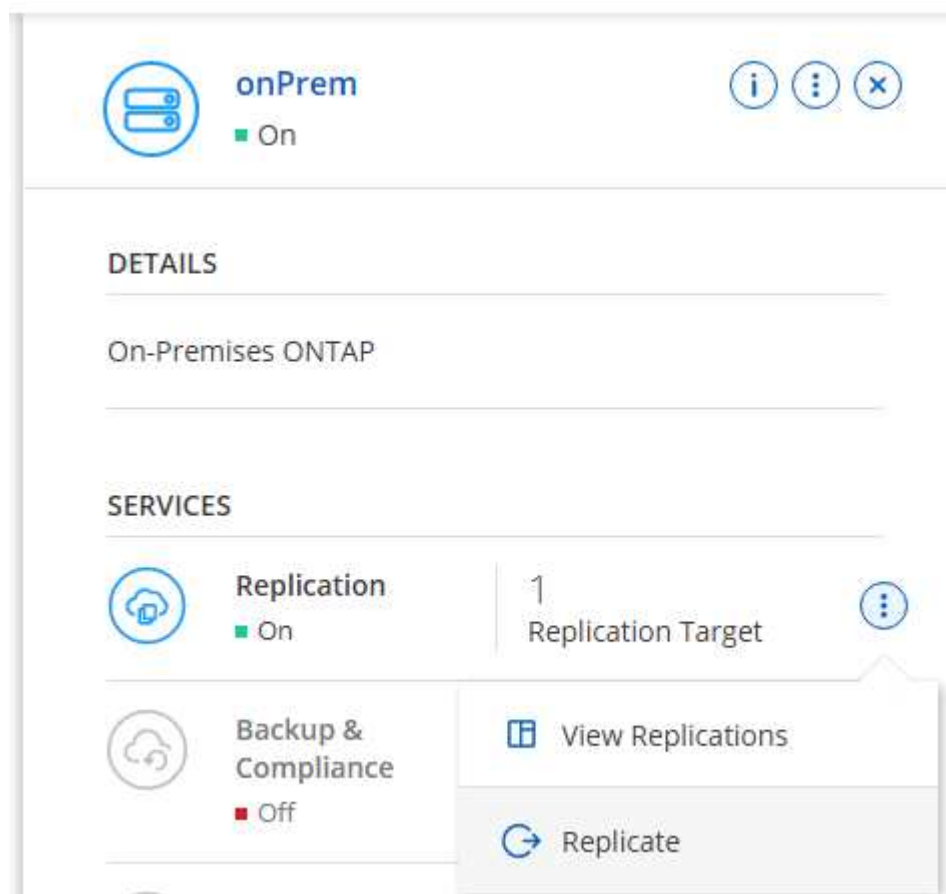
Enable



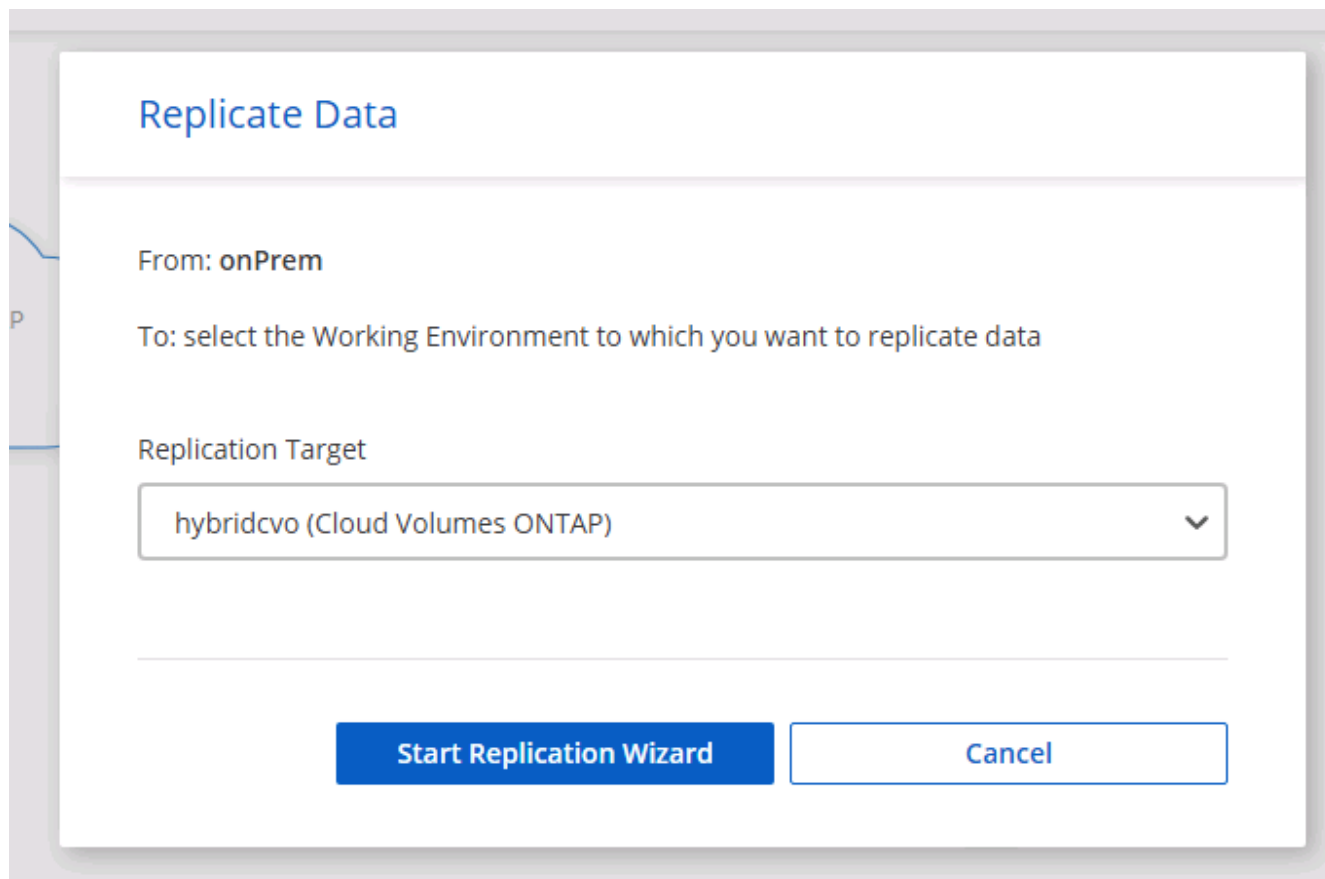
Ou Opções.



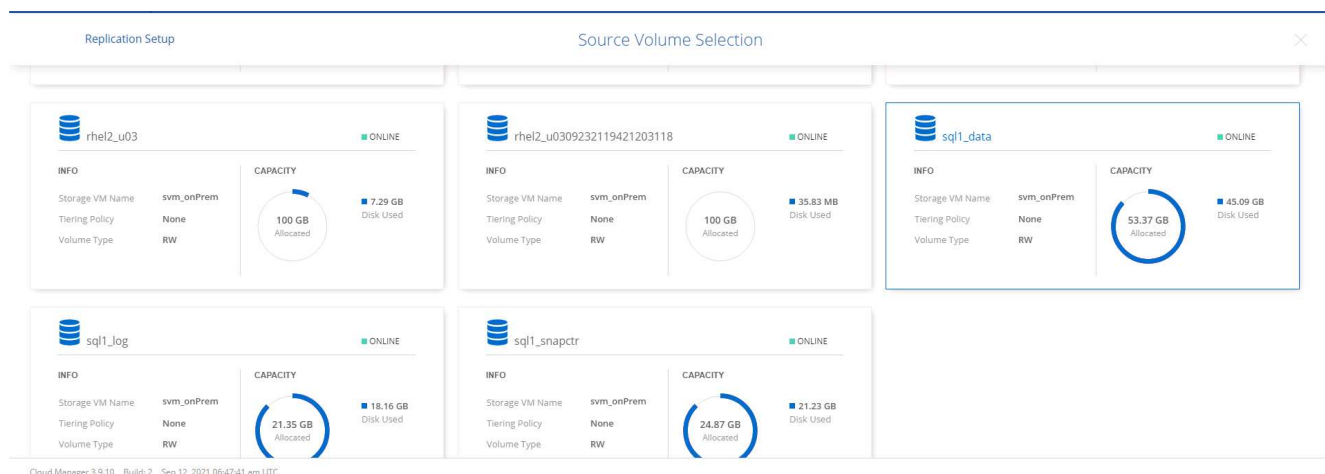
Replicar.



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



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



- 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.

Replication Setup

Destination Disk Type and Tiering

↑ Previous Step

Destination Disk Type

General Purpose SSD

General Purpose SSD - Dynamic Performance

Throughput Optimized HDD

S3 Tiering [What are storage tiers?](#)

☒ Enabled ☐ Disabled

Note: If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.

Continue

Cloud Manager 3.9.10 Build: 2 Sep 12, 2021 06:47:41 am UTC

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

Destination Volume Name

`sql1_data_dr`

Destination Aggregate

Automatically select the best aggregate

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.

Max Transfer Rate

You should limit the transfer rate. An unlimited rate might negatively impact the performance of other applications and it might impact your Internet performance.

☒ Limited to: MB/s

☐ Unlimited (recommended for DR only machines)

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.

Replication Policy

Default Policies

Additional Policies

 Mirror

Typically used for disaster recovery

[More info](#)

 Mirror and Backup (1 month retention)

Configures disaster recovery and long-term retention of backups on the same destination volume

[More info](#)

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.

Replication Setup

Schedule

Previous Step

Select a replication schedule

One-time copy

No schedule

10min

Every hour
Minutes: 0th, 10th, 20th, 3...

12-hourly

Every day
Hours: 12 AM and 12 PM
Minutes: 15th minute

5min

Every hour
Minutes: 0th, 5th, 10th, 15t...

6-hourly

Every day
Hours: 12 AM, 6 AM, 12 PM...
Minutes: 15th minute

8hour

Every day
Hours: 2 AM, 10 AM and 6 ...
Minutes: 15th minute

daily

Every day
Hours: 12 AM
Minutes: 10th minute

hourly

Every hour
Minutes: 5th minute

monthly

Every month
Days: 2nd
Hours: 12 AM
Minutes: 20th minute

pg-15-minutely

Every hour

pg-6-hourly

Every day

pg-daily

Every day

pg-daily-set2

Every day

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 .

Replication Setup

Review & Approve

Previous Step

Review your selection and start the replication process

Source

onPrem

sql1_data

Destination

hybridcvo

sql1_data_copy

☒ I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements.
 [More Information >](#)

Source Volume Allocated Size:

53.37 GB

Source Volume Used Size:

45.09 GB

Source Thin Provisioning:

Yes

Destination Volume Allocated Size:

53.37 GB

Destination Volume Disk Type:

General Purpose SSD (...)

Capacity Tiering:

S3

Destination Thin Provisioning:

Yes

Destination Aggregate:

aggr1 (Automatically s...

Destination Storage VM:

svm_hybridcvo

Max Transfer Rate:

100 MB/s

SnapMirror Policy:

Mirror

Replication Schedule:

daily

Go

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.

Replication

7 Volume Relationships

153.32 GiB Replicated Capacity

0 Currently Transferring

7 Healthy

0 Failed

7 Volume Relationships

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer	
✓	rhel2_u01 onPrem	rhel2_u01_dr hybridcvo	43 minutes 43 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:50 AI 19.73 MiB	...
✓	rhel2_u02 onPrem	rhel2_u02_dr hybridcvo	1 hour 37 minutes 59 seconds	idle	snapmirrored	Sep 30, 2021, 2:37:08 PM 239.78 MiB	...
✓	rhel2_u03 onPrem	rhel2_u03_dr hybridcvo	16 hours 1 minute 9 seconds	idle	snapmirrored	Sep 30, 2021, 4:07:14 PM 225.37 KiB	...
✓	sql1_data onPrem	sql1_data_dr hybridcvo	1 hour 6 minutes 50 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:28 AI 24.56 KiB	...

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.

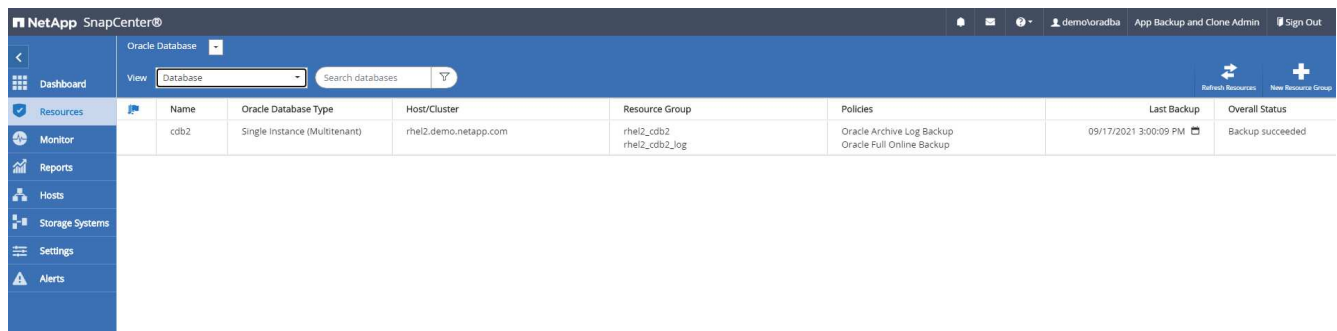
1. Recupere a senha do administrador do Windows para efetuar login em uma instância via RDP.
2. Desabilite o firewall do Windows, junte o host ao domínio do Windows SnapCenter e adicione a instância ao servidor DNS para resolução de nomes.
3. Provisione um volume de log do SnapCenter para armazenar arquivos 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

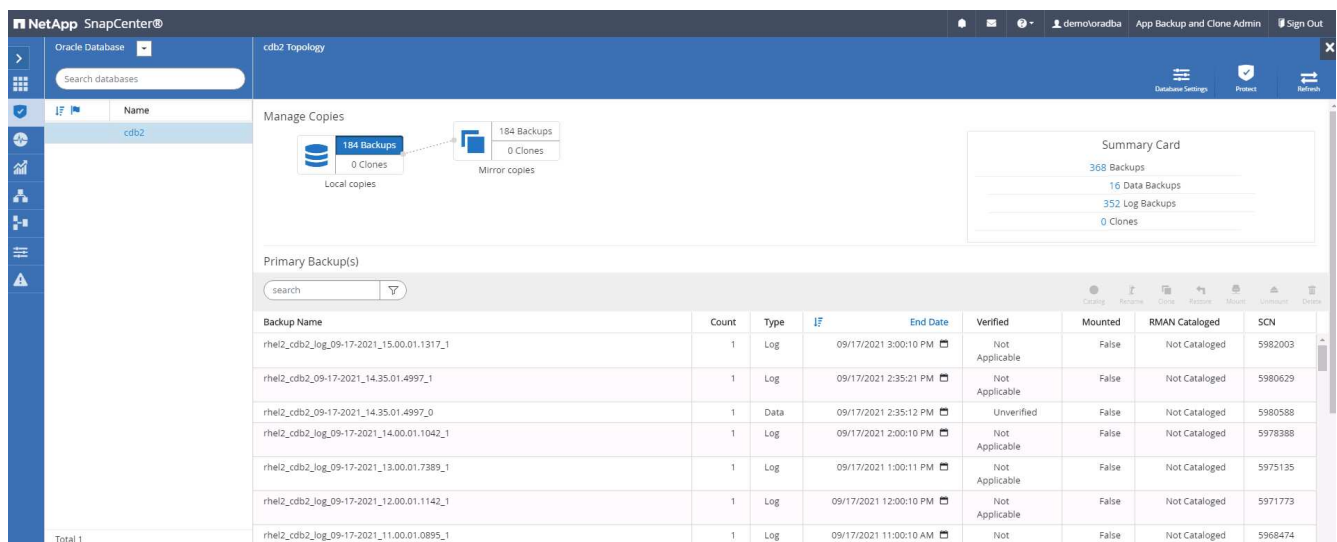
A agilidade da nuvem pública, o tempo de retorno e a economia de custos são propostas de valor significativas para empresas que adotam a nuvem pública para desenvolvimento de aplicativos de banco de dados e esforços de teste. Não há ferramenta melhor que o SnapCenter para tornar isso realidade. O SnapCenter 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).

NetApp SnapCenter®

Oracle Database

Search databases

cdb2

Manage Copies

184 Backups
0 Clones
Local copies

184 Backups
0 Clones
Mirror copies

Summary Card

368 Backups
16 Data Backups
352 Log Backups
0 Clones

Secondary Mirror Backup(s)

search

Backup Name	Count	Type	if	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log		09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	False	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data		09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log		09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388
rhel2_cdb2_log_09-17-2021_13.00.01.7389_1	1	Log		09/17/2021 1:00:11 PM	Not Applicable	False	Not Cataloged	5975135
rhel2_cdb2_log_09-17-2021_12.00.01.1142_1	1	Log		09/17/2021 12:00:10 PM	Not Applicable	False	Not Cataloged	5971773
rhel2_cdb2_log_09-17-2021_11.00.01.0895_1	1	Log		09/17/2021 11:00:10 AM	Not Applicable	False	Not Cataloged	5968474
Total 1								

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.

Mount backups

Choose the host to mount the backup

ora-standby.demo.netapp.com

Mount path : /var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_09-17-2021_14.35.01.4997_1/cdb2

Secondary storage location : Snap Vault / Snap Mirror

Source Volume

svm_onPrem:rhel2_u03

Destination Volume

svm_hybridcvo:rhel2_u03_dr

Mount Cancel

NetApp SnapCenter®

Oracle Database

Search databases

cdb2 Topology

Manage Copies

184 Backups
0 Clones
Local copies

184 Backups
1 Clone
Mirror copies

Summary Card

368 Backups
16 Data Backups
352 Log Backups
1 Clone

Secondary Mirror Backup(s)

search

Backup Name	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log		09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log		09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_log_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	True	Not Cataloged	5980629
rhel2_cdb2_log_09-17-2021_14.35.01.4997_0	1	Data		09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log		09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388



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.

cdb2 Topology

search

Backup Name	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log		09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log		09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_log_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	True	Not Cataloged	5980629
rhel2_cdb2_log_09-17-2021_14.35.01.4997_0	1	Data		09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log		09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388

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

Clone from cdb2

1

Name

2

Locations

3

Credentials

4

PreOps

5

PostOps

6

Notification

7

Summary

☒ Complete Database Clone

Clone SID

cdb2test

Exclude PDBs

Type to find PDBs

☐ PDB Clone

Secondary storage location : Snap Vault / Snap Mirror

Data

Source Volume

svm_onPrem:rhel2_u02

Destination Volume

svm_hybridcvo:rhel2_u02_dr

Logs

Source Volume

svm_onPrem:rhel2_u03

Destination Volume

svm_hybridcvo:rhel2_u03_dr

Previous

Next

- 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.

Clone from cdb2

1

Name

2

Locations

3

Credentials

4

PreOps

5

PostOps

6

Notification

7

Summary

Select the host to create a clone

Clone host
ora-standby.demo.netapp.com

Datafile locations ⓘ

/u02_cdb2test
Reset

Control files ⓘ

/u02_cdb2test/cdb2test/control/control01.ctl
/u02_cdb2test/cdb2test/control/control02.ctl
Reset

Redo logs ⓘ

Group	Size	Unit	Number of files
RedoGroup 1	200	MB	1
/u02_cdb2test/cdb2test/redolog/redo03.log			
RedoGroup 2	200	MB	1

Previous
Next

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.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Database Credentials for the clone

Credential name for sys user

None

+

i

Database port

1521

Oracle Home Settings

i

Oracle Home

/u01/app/oracle/product/19800/cdb2

Oracle OS User

oracle

Oracle OS Group

oinstall

Previous

Next

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.

Clone from cdb2

1

Name

2

Locations

3

Credentials

4

5

6

7

Specify scripts to run before clone operation ⓘ

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Arguments

Script timeout

60

secs

Database Parameter settings

processes	320	×
remote_login_passwordfile	EXCLUSIVE	×
sga_target	4311744512	×
undo_tablespace	UNDOTBS1	×

+

Reset

Previous

Next

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.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

☒ Recover Database

☐ Until Cancel

☐ Date and Time

☒ Until SCN (System Change Number)

5980629

Specify external archive log locations

/var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_09-17-2021_14.35.01.4997_1/cdb2/1/orareco/CDB2/archivelog/

☒ Create new DBID

☒ Create tempfile for temporary tablespace

☐ Enter SQL queries to apply when clone is created

☐ Enter scripts to run after clone operation

Previous

Next

```

oracle@ora-standby/tmp$ ls /var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_09-17-2021_14.35.01.4997_1/cdb2/1/orareco/CDB2/archivelog/
2021_08_26 2021_08_28 2021_08_30 2021_09_01 2021_09_03 2021_09_05 2021_09_07 2021_09_09 2021_09_11 2021_09_13 2021_09_15 2021_09_17
2021_08_27 2021_08_29 2021_08_31 2021_09_02 2021_09_04 2021_09_06 2021_09_08 2021_09_10 2021_09_12 2021_09_14 2021_09_16
oracle@ora-standby/tmp$

```

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

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Provide email settings ⓘ

Email preference

Never

From

From email

To

Email to

Subject

Notification

☐ Attach job report

⚠

If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

✕

Previous

Next

12. Resumo do clone.

Clone from cdb2

1 Name
2 Locations
3 Credentials
4 PreOps
5 PostOps
6 Notification
7 Summary

Summary

Clone from backup	rhel2_cdb2_09-17-2021_14.35.01.4997_0
Clone SID	cdb2test
Clone server	ora-standby.demo.netapp.com
Exclude PDBs	none
Oracle home	/u01/app/oracle/product/19800/cdb2
Oracle OS user	oracle
Oracle OS group	oinstall
Datafile mountpaths	/u02_cdb2test
Control files	/u02_cdb2test/cdb2test/control/control01.ctl /u02_cdb2test/cdb2test/control/control02.ctl
Redo groups	RedoGroup =1 TotalSize =200 Path =/u02_cdb2test/cdb2test/redolog/redo03.log RedoGroup =2 TotalSize =200 Path =/u02_cdb2test/cdb2test/redolog/redo02.log RedoGroup =3 TotalSize =200 Path =/u02_cdb2test/cdb2test/redolog/redo01.log
Recovery scope	Until SCN 5980629
Prescript full path	none
Prescript arguments	
Postscript full path	none
Postscript arguments	

Previous

Finish

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.

```

oracle@ora-standby/tmp$ export ORACLE_SID=cdb2test
[oracle@ora-standby tmp]$ export ORACLE_HOME=/u01/app/oracle/product/19800/cdb2
[oracle@ora-standby tmp]$ export PATH=$PATH:$ORACLE_HOME/bin
[oracle@ora-standby tmp]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Sep 17 17:49:29 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> select name, log_mode from v$database;

NAME          LOG MODE
-----
CDB2TEST      ARCHIVELOG

SQL> select instance_name, host_name from v$instance;

INSTANCE_NAME
HOST_NAME
-----
cdb2test
ora-standby.demo.netapp.com

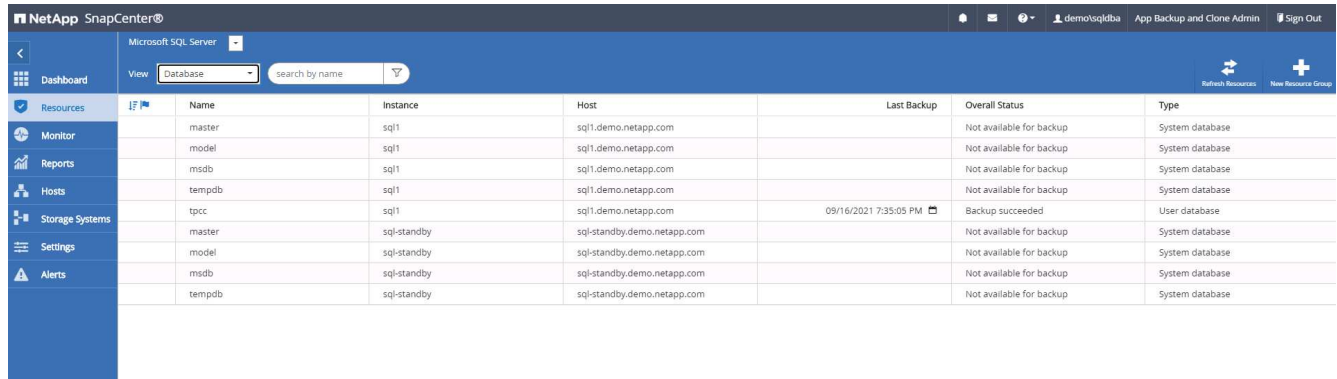
SQL> show pdbs

  CON_ID CON_NAME              OPEN MODE RESTRICTED
  -----
2 PDB$SEED                  READ ONLY NO
3 CDB2_PDB1                  READ WRITE NO
4 CDB2_PDB2                  READ WRITE NO
5 CDB2_PDB3                  READ WRITE NO
SQL>

```

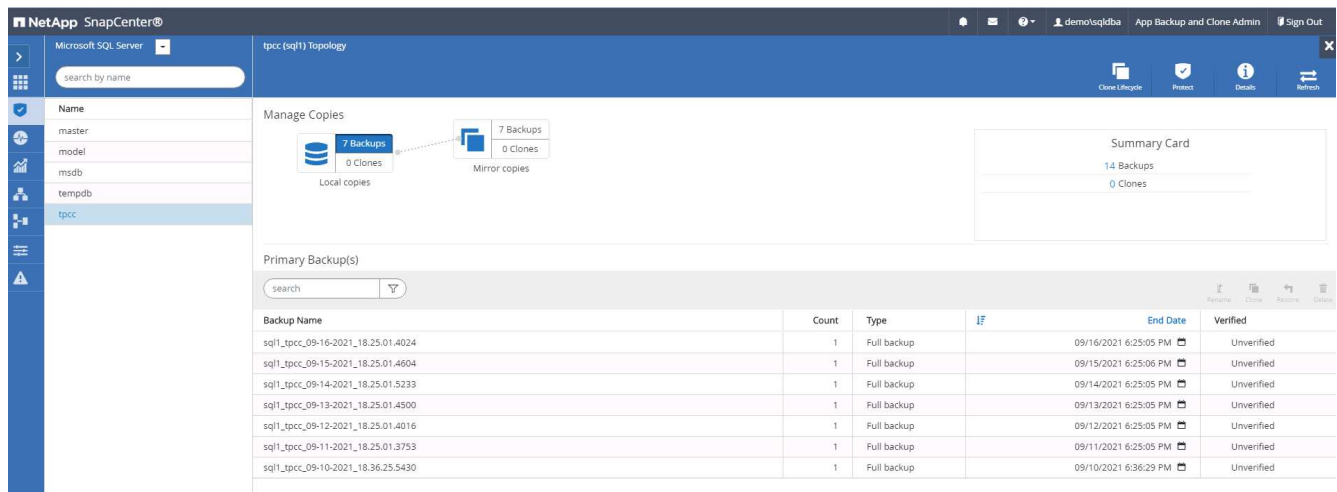
Clonar um banco de dados SQL para desenvolvimento/teste a partir de um backup de Snapshot replicado

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.



	Name	Instance	Host	Last Backup	Overall Status	Type
	master	sql1	sql1.demo.netapp.com		Not available for backup	System database
	model	sql1	sql1.demo.netapp.com		Not available for backup	System database
	msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
	tempdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
	tpcc	sql1	sql1.demo.netapp.com	09/16/2021 7:35:05 PM	Backup succeeded	User database
	master	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database
	model	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database
	msdb	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database
	tempdb	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database

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.



tpcc (sql1) Topology

Manage Copies

Local copies: 7 Backups, 0 Clones. Mirror copies: 7 Backups, 0 Clones.

Summary Card

14 Backups, 0 Clones

Primary Backup(s)

Backup Name	Count	Type	End Date	Verified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup	09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup	09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup	09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup	09/13/2021 6:25:05 PM	Unverified
sql1_tpcc_09-12-2021_18.25.01.4016	1	Full backup	09/12/2021 6:25:05 PM	Unverified
sql1_tpcc_09-11-2021_18.25.01.3753	1	Full backup	09/11/2021 6:25:05 PM	Unverified
sql1_tpcc_09-10-2021_18.36.25.5430	1	Full backup	09/10/2021 6:36:29 PM	Unverified

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.

NetApp SnapCenter®

Microsoft SQL Server

tpcc (sql1) Topology

search by name

Manage Copies

Local copies: 7 Backups, 0 Clones

Mirror copies: 7 Backups, 0 Clones

Summary Card

14 Backups

0 Clones

Secondary Mirror Backup(s)

Backup Name	Count	Type	if	End Date	Verified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup		09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup		09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup		09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup		09/13/2021 6:25:05 PM	Unverified
sql1_tpcc_09-12-2021_18.25.01.4016	1	Full backup		09/12/2021 6:25:05 PM	Unverified
sql1_tpcc_09-11-2021_18.25.01.3753	1	Full backup		09/11/2021 6:25:05 PM	Unverified
sql1_tpcc_09-10-2021_18.36.25.5430	1	Full backup		09/10/2021 6:36:29 PM	Unverified

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

NetApp SnapCenter®

Microsoft SQL Server

tpcc (sql1) Topology

search by name

Manage Copies

Local copies: 7 Backups, 0 Clones

Mirror copies: 7 Backups, 1 Clone

Summary Card

14 Backups

1 Clone

Secondary Mirror Backup(s)

Backup Name	Count	Type	if	End Date	Verified
sql1_tpcc_09-19-2021_18.25.01.4134	1	Full backup		09/19/2021 6:25:05 PM	Unverified
sql1_tpcc_09-18-2021_18.25.01.3963	1	Full backup		09/18/2021 6:25:05 PM	Unverified
sql1_tpcc_09-17-2021_18.25.01.4218	1	Full backup		09/17/2021 6:25:05 PM	Unverified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup		09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup		09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup		09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup		09/13/2021 6:25:05 PM	Unverified

Clone from backup

1

Clone Options

2

Logs

3

Script

4

Notification

5

Summary

Clone settings

Clone server

Choose

i

Clone instance

Nothing selected

i

Clone name

tpcc

Choose mount option

☒
Auto assign mount point

i

☐
Auto assign volume mount point under path

full file path

i

Secondary storage location : Snap Vault / Snap Mirror

Source Volume

Destination Volume

svm_onPrem:sql1_data

svm_hybridcvo:sql1_data_dr

svm_onPrem:sql1_log

svm_hybridcvo:sql1_log_dr

Previous

Next

- 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.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Clone settings

Clone server

sql-standby.demo.netapp.com

Clone instance

sql-standby

Clone name

tpcc_clone

Choose mount option

☒ Auto assign mount point

☐ Auto assign volume mount point under path

full file path

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcvo:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcvo:sql1_log_dr

Previous

Next

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

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Choose logs

☐ All log backups

☒ By log backups until

9/17/2021 6:25:10 PM

☐ By specific date until

09/17/2021 6:25:05 PM

☐ None

Previous

Next

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

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Specify optional scripts to run before and after performing a clone from backup job

Prescript full path

Prescript arguments

Choose optional arguments...

Postscript full path

Postscript arguments

Choose optional arguments...

Script timeout

60

secs

Previous

Next

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

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Provide email settings ⓘ

Email preference

Never

From

From email

To

Email to

Subject

Notification

☐ Attach Job Report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

✕

Previous

Next

9. Resumo do clone.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Summary

Clone server	sql-standby.demo.netapp.com
Clone instance	sql-standby
Clone name	tpcc_dev
Mount option	Auto assign volume mount point under custom path
Prescript full path	None
Prescript arguments	
Postscript full path	None
Postscript arguments	
Send email	No

Previous

Finish

- 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.

NetApp SnapCenter®						
Jobs - Filter						
ID	Status	Name	Start date	End date	Owner	
766	✓	Clone from backup 'sql1_tpcc-09-16-2021_18.25.01.4024'	09/16/2021 8:05:25 PM	09/16/2021 8:06:17 PM	demo:sqlqdba	
763	✓	Discover resources for all hosts	09/16/2021 7:56:49 PM	09/16/2021 7:56:54 PM	demo:sqlqdba	
761	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 7:35:00 PM	09/16/2021 7:37:08 PM	demo:sqlqdba	
760	⚠	Discover resources for all hosts	09/16/2021 7:19:05 PM	09/16/2021 7:19:09 PM	demo:sqlqdba	
759	⚠	Discover resources for all hosts	09/16/2021 7:18:43 PM	09/16/2021 7:18:48 PM	demo:sqlqdba	
756	⚠	Discover resources for all hosts	09/16/2021 6:59:51 PM	09/16/2021 6:59:56 PM	demo:sqlqdba	
753	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 6:35:00 PM	09/16/2021 6:37:07 PM	demo:sqlqdba	
750	✓	Backup of Resource Group 'sql1_tpcc' with policy 'SQL Server Full Backup'	09/16/2021 6:25:01 PM	09/16/2021 6:27:14 PM	demo:sqlqdba	
749	✓	Discover resources for host 'sql-standby.demo.netapp.com'	09/16/2021 6:19:00 PM	09/16/2021 6:19:05 PM	DemoAdministrator	
745	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 5:35:00 PM	09/16/2021 5:37:08 PM	demo:sqlqdba	

Configuração pós-clone

- 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.
- Configure um listener Oracle ou registre o banco de dados recém-cloneado com um listener existente para acesso do usuário.
- 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?

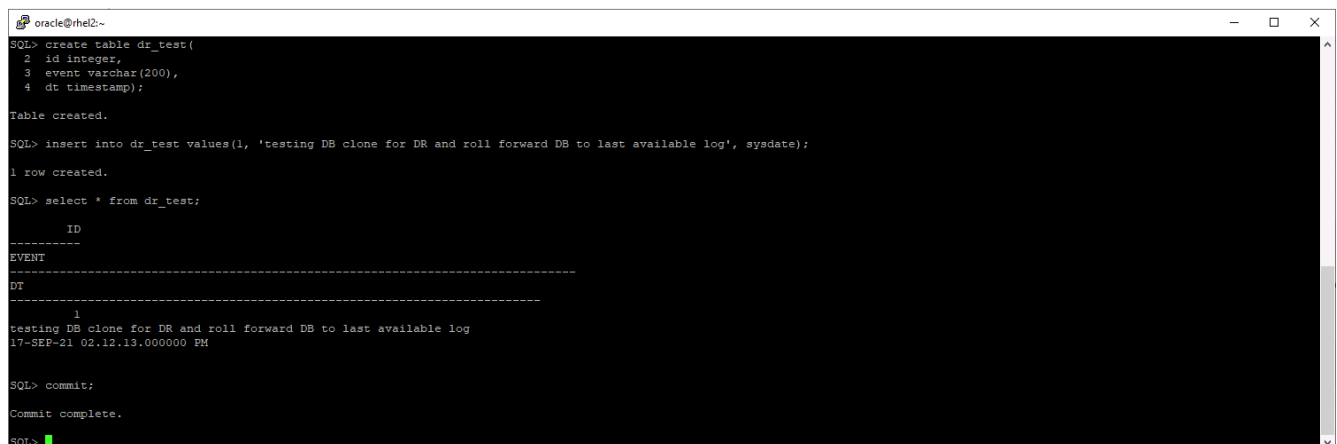
Se precisar de ajuda com esta solução e casos de uso, junte-se a ["Canal do Slack de suporte da comunidade de automação de soluções da NetApp"](#) e procure o canal de automação de soluções para postar suas dúvidas ou perguntas.

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.

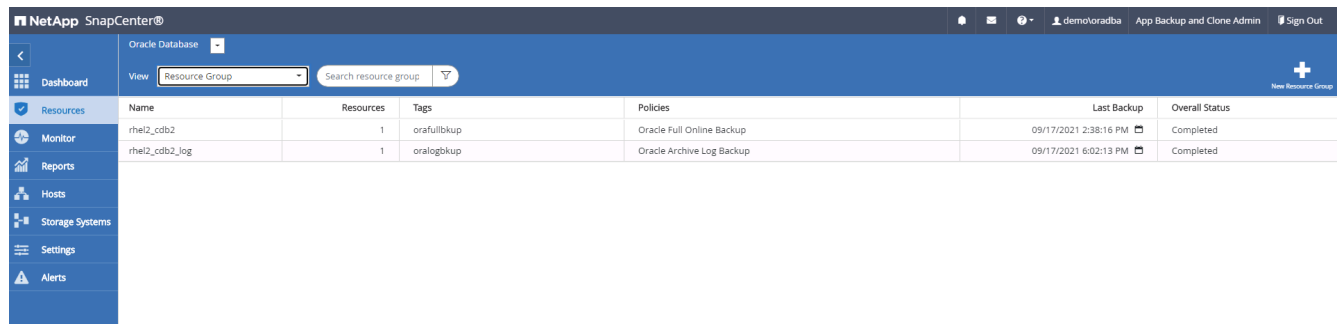
Clonar um banco de dados de produção Oracle local para a nuvem para recuperação de desastres

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.



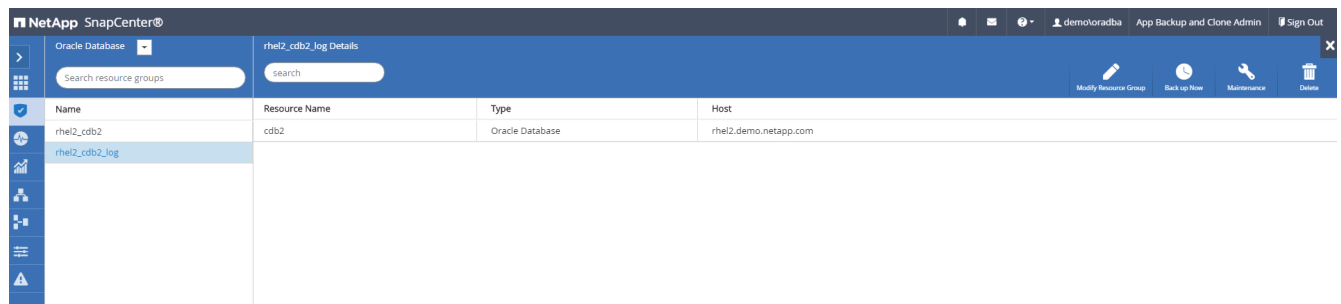
```
oracle@rhel2~  
SQL> create table dr_test(  
  2 id integer,  
  3 event varchar(200),  
  4 dt timestamp);  
  
Table created.  
  
SQL> insert into dr_test values(1, 'testing DB clone for DR and roll forward DB to last available log', sysdate);  
  
1 row created.  
  
SQL> select * from dr_test;  
  
      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> commit;  
  
Commit complete.  
  
SQL>
```

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.



Name	Resources	Tags	Policies	Last Backup	Overall Status
rhel2_cdb2	1	orafullbkup	Oracle Full Online Backup	09/17/2021 2:38:16 PM	Completed
rhel2_cdb2_log	1	oralogbkup	Oracle Archive Log Backup	09/17/2021 6:02:13 PM	Completed

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.



Name	Resource Name	Type	Host
rhel2_cdb2	cdb2	Oracle Database	rhel2.demo.netapp.com
rhel2_cdb2_log			

Backup

Create a backup for the selected resource group

Resource Group

rhel2_cdb2_log

Policy

Oracle Archive Log Backup

Cancel

Backup



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.

The screenshot shows the NetApp SnapCenter interface for an Oracle Database. The left sidebar lists databases: cdb2, cdb2dev, and cdb2test. The main area displays 'Manage Copies' with a visual representation of 185 Backups (Local copies) and 185 Backups (Mirror copies) with 2 Clones. A 'Summary Card' on the right shows: 370 Backups, 16 Data Backups, 354 Log Backups, and 2 Clones. Below this is a table of 'Secondary Mirror Backup(s)'. The table has columns: Backup Name, Count, Type, ID, End Date, Verified, Mounted, RMAN Cataloged, and SCN. The data rows show log backups for rhel2_cdb2_log_09-17-2021_18.20.04.1177_1, rhel2_cdb2_log_09-17-2021_18.00.01.2424_1, and rhel2_cdb2_log_09-17-2021_17.00.01.1566_1.

Backup Name	Count	Type	ID	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_18.20.04.1177_1	1	Log		09/17/2021 6:20:13 PM	Not Applicable	False	Not Cataloged	5994710
rhel2_cdb2_log_09-17-2021_18.00.01.2424_1	1	Log		09/17/2021 6:00:09 PM	Not Applicable	False	Not Cataloged	5992079
rhel2_cdb2_log_09-17-2021_17.00.01.1566_1	1	Log		09/17/2021 5:00:20 PM	Not Applicable	False	Not Cataloged	5988842

The 'Mount backups' dialog box is shown. It includes a dropdown for 'Choose the host to mount the backup' with the value 'ora-standby.demo.netapp.com'. The 'Mount path' is '/var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_log_09-17-2021_18.20.04.1177_1/cdb2'. Below this, the 'Secondary storage location' is set to 'Snap Vault / Snap Mirror'. A table shows the mapping from 'Source Volume' (svm_onPrem:rhel2_u03) to 'Destination Volume' (svm_hybridcvo:rhel2_u03_dr). At the bottom right are 'Mount' and 'Cancel' buttons.

Source Volume	Destination Volume
svm_onPrem:rhel2_u03	svm_hybridcvo:rhel2_u03_dr

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

NetApp SnapCenter®

Oracle Database

Search databases

cdb2 Topology

Manage Copies

Local copies: 185 Backups, 0 Clones

Mirror copies: 185 Backups, 2 Clones

Summary Card

- 370 Backups
- 16 Data Backups
- 354 Log Backups
- 2 Clones

Secondary Mirror Backup(s)

Backup Name	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_18.20.04.1177_1	1	Log		09/17/2021 6:20:13 PM	Not Applicable	True	Not Cataloged	5994710
rhel2_cdb2_log_09-17-2021_18.00.01.2424_1	1	Log		09/17/2021 6:00:09 PM	Not Applicable	False	Not Cataloged	5992079
rhel2_cdb2_log_09-17-2021_17.00.01.1566_1	1	Log		09/17/2021 5:00:20 PM	Not Applicable	False	Not Cataloged	5988842
rhel2_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log		09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log		09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_log_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	False	Not Cataloged	5980629
rhel2_cdb2_log_09-17-2021_14.35.01.4997_0	1	Data		09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588

Total 3

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

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

☒ Complete Database Clone

Clone SID:

Exclude PDBs:

☐ PDB Clone

Secondary storage location : Snap Vault / Snap Mirror

☒ Data

Source Volume: svm_onPrem:rhel2_u02

Destination Volume:

☒ Logs

Source Volume: svm_onPrem:rhel2_u03

Destination Volume:

Previous Next

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.

≡

ONTAP System Manager

Search actions, objects, and pages

🔍

DASHBOARD

STORAGE

Overview

Applications

Volumes

LUNS

Shares

Qtrees

Quotas

Storage VMs

Tiers

NETWORK

EVENTS & JOBS

PROTECTION

HOSTS

Volumes

+ Add

⋮ More

☐	Name	Storage VM	Status	Capacity
☐	ora_standby_u01	svm_hybridcvo	Online	31.6 GB 12.3 GB used 17.7 GB available
☐	rhel2_u01_dr	svm_hybridcvo	Online	31.6 GB
☐	rhel2_u02_dr	svm_hybridcvo	Online	31.6 GB
☐	rhel2_u02_dr0917211608119360	svm_hybridcvo	Online	31.6 GB
☐	rhel2_u02_dr0917211703534863	svm_hybridcvo	Online	31.6 GB
☐	rhel2_u03_dr	svm_hybridcvo	Online	31.6 GB
☐	rhel2_u03_dr0917211824574775	svm_hybridcvo	Online	31.6 GB

Add Volume

NAME

ora_standby_u03

CAPACITY

20

GB

More Options

Cancel

Save



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

Clone from cdb2

1 Name
2 Locations
3 Credentials
4 PreOps
5 PostOps
6 Notification
7 Summary

Select the host to create a clone

Clone host
ora-standby.demo.netapp.com

Datafile locations ⓘ

/u02_cdb2dr
Reset

Control files ⓘ

/u02_cdb2dr/cdb2dr/control/control01.ctl
/u03_cdb2dr/cdb2dr/control/control02.ctl
Reset

Redo logs ⓘ

Group	Size	Unit	Number of files
RedoGroup 1	200	MB	1
/u03_cdb2dr/cdb2dr/redolog/redo03.log			
RedoGroup 2	200	MB	1

Previous
Next

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

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Database Credentials for the clone

Credential name for sys user

None

+

i

Database port

1521

Oracle Home Settings

i

Oracle Home

/u01/app/oracle/product/19800/cdb2

Oracle OS User

oracle

Oracle OS Group

oinstall

Previous

Next

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

Clone from cdb2

1

Name

2

Locations

3

Credentials

4

PreOps

5

6

7

Specify scripts to run before clone operation ⓘ

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Arguments

Script timeout

60

secs

Database Parameter settings

+
Reset

Previous

Next

- 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.

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

☒ Recover Database

☒ Until Cancel

☐ Date and Time

Date-time format: MM/DD/YYYY hh:mm:ss

☐ Until SCN (System Change Number)

Specify external archive log locations

/var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_log_09-17-2021_18.20.04.1177_1/cdb2/1/orareco/CDB2/archivelog/

☒

Create new DBID

☒

Create tempfile for temporary tablespace

☐

Enter SQL queries to apply when clone is created

☐

Enter scripts to run after clone operation

Previous

Next

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

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Provide email settings ⓘ

Email preference

Never

From

From email

To

Email to

Subject

Notification

☐ Attach job report

⚠

If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

✕

Previous

Next

13. Resumo do clone DR.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Summary

Clone from backup

rhe12_cdb2_09-17-2021_14.35.01.4997_0

Clone SID

cdb2dr

Clone server

ora-standby.demo.netapp.com

Exclude PDBs

none

Oracle home

/u01/app/oracle/product/19800/cdb2

Oracle OS user

oracle

Oracle OS group

oinstall

Datafile mountpaths

/u02_cdb2dr

Control files

/u02_cdb2dr/cdb2dr/control/control01.ctl
/u03_cdb2dr/cdb2dr/control/control02.ctl

Redo groups

RedoGroup =1 TotalSize =200 Path =/u03_cdb2dr/cdb2dr/redolog/redo03.log
RedoGroup =2 TotalSize =200 Path =/u03_cdb2dr/cdb2dr/redolog/redo02.log
RedoGroup =3 TotalSize =200 Path =/u03_cdb2dr/cdb2dr/redolog/redo01.log

Recovery scope

Until Cancel

Prescript full path

none

Prescript arguments

Postscript full path

none

Postscript arguments

Previous

Finish

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

NetApp SnapCenter®								
Oracle Database View Database Search databases								
	Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status	
	cdb2	Single Instance (Multitenant)	rhe12.demo.netapp.com	rhe12_cdb2 rhe12_cdb2_log	Oracle Archive Log Backup Oracle Full Online Backup	09/17/2021 7:00:10 PM	Backup succeeded	
	cdb2dev	Single Instance (Multitenant)	ora-standby.demo.netapp.com				Not protected	
	cdb2dr	Single Instance (Multitenant)	ora-standby.demo.netapp.com				Not protected	
	cdb2test	Single Instance (Multitenant)	ora-standby.demo.netapp.com				Not protected	

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:db]$ 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    /u03_cdb2dr/cdb2dr
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.

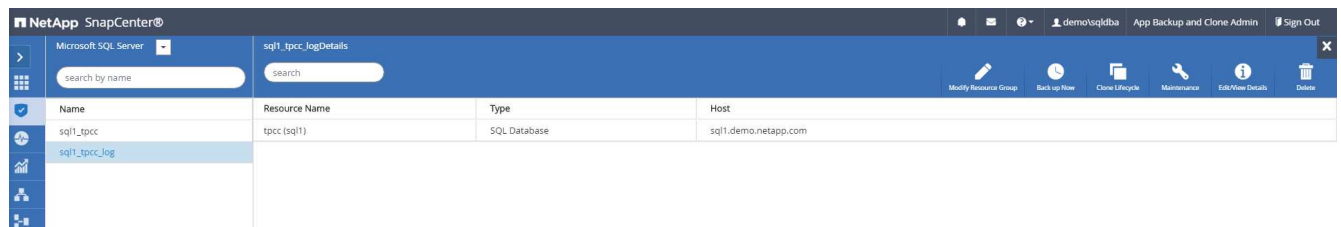
Clonar um banco de dados de produção SQL local para a nuvem para recuperação de desastres

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.

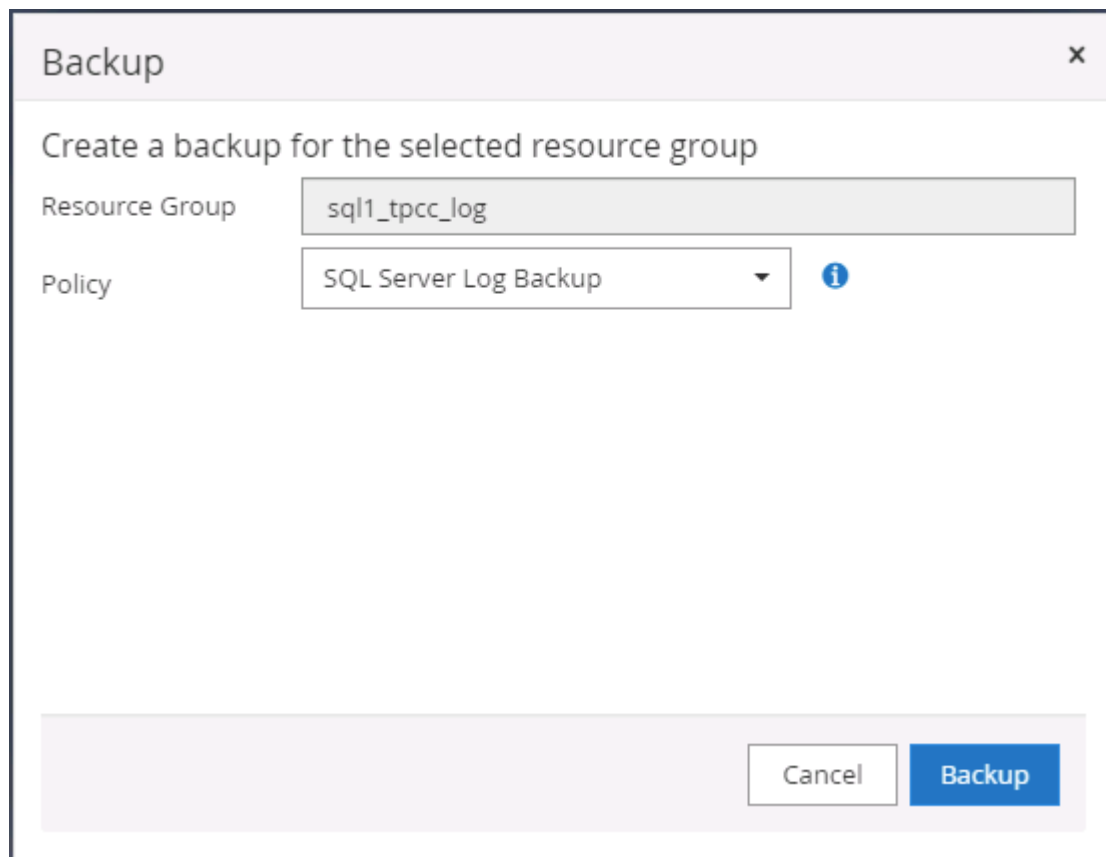
```
Administrator Command Prompt - sqlcmd - SQLCMD
C:\Users\administrator.DEMO>sqlcmd
1> select host_name()
2> go

-----
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.

Backup Name	Count	Type	if	End Date	Verified
sql1_tpcc_09-19-2021_18.25.01.4134	1	Full backup		09/19/2021 6:25:05 PM	Unverified
sql1_tpcc_09-18-2021_18.25.01.3963	1	Full backup		09/18/2021 6:25:05 PM	Unverified
sql1_tpcc_09-17-2021_18.25.01.4218	1	Full backup		09/17/2021 6:25:05 PM	Unverified

- 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.

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcvo:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcvo:sql1_log_dr

- Selecione todos os backups de log a serem aplicados.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Choose logs

☒ All log backups

☐ By log backups until

9/19/2021 6:25:10 PM

☐ By specific date until

09/19/2021 6:25:05 PM

☐ None

Previous

Next

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

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Specify optional scripts to run before and after performing a clone from backup job

Prescript full path

Prescript arguments

Choose optional arguments...

Postscript full path

Postscript arguments

Choose optional arguments...

Script timeout

60

secs

Previous

Next

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

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Provide email settings ⓘ

Email preference

Never

From

From email

To

Email to

Subject

Notification

☐ Attach Job Report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

×

Previous

Next

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

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Summary

Clone server

sql-standby.demo.netapp.com

Clone instance

sql-standby

Clone name

tpcc_dr

Mount option

Auto Mount

Prescript full path

None

Prescript arguments

Postscript full path

None

Postscript arguments

Send email

No

Previous

Finish

NetApp SnapCenter®							
Microsoft SQL Server							
View Database search by name							
Resources	Name	Instance	Host	Last Backup	Overall Status	Type	
Monitor	master	sql1	sql1.demo.netapp.com		Not available for backup	System database	
Reports	model	sql1	sql1.demo.netapp.com		Not available for backup	System database	
Hosts	msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database	
Storage Systems	tempdb	sql1	sql1.demo.netapp.com		Not available for backup	System database	
Settings	tpcc	sql1	sql1.demo.netapp.com	09/22/2021 5:35:08 PM	Backup failed, Schedules on hold	User database	
Alerts	master	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database	
	model	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database	
	msdb	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database	
	tempdb	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database	
	tpcc_clone	sql-standby	sql-standby.demo.netapp.com		Not protected	User database	
	tpcc_dev	sql-standby	sql-standby.demo.netapp.com		Not protected	User database	
	tpcc_dr	sql-standby	sql-standby.demo.netapp.com		Not protected	User database	

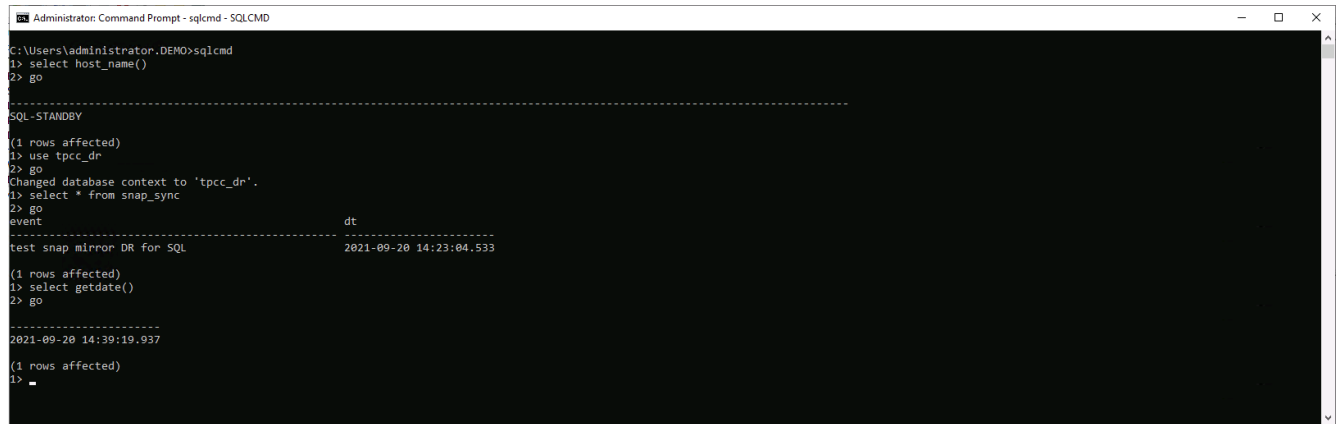
Validação e configuração do clone pós-DR para SQL

1. Monitore o status do trabalho de clonagem.

NetApp SnapCenter®							
Jobs Schedules Events Logs							
search by name							
Resources	Jobs - Filter						
Monitor	ID	Status	Name	Start date	End date	Owner	
Reports	1052	✓	Clone from backup 'sql1_tpcc_09-19-2021_18.25.01.4134'	09/20/2021 2:36:17 PM	09/20/2021 2:37:06 PM	demo/sqlqdba	
Hosts	1047	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 2:35:01 PM	09/20/2021 2:37:08 PM	demo/sqlqdba	
Storage Systems	1045	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 2:28:17 PM	09/20/2021 2:30:25 PM	demo/sqlqdba	
Settings	1044	✓	Clone from backup 'sql1_tpcc_09-17-2021_18.25.01.4218'	09/20/2021 1:39:24 PM	09/20/2021 1:40:09 PM	demo/sqlqdba	
	1042	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 1:35:01 PM	09/20/2021 1:37:08 PM	demo/sqlqdba	
	1040	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 12:35:01 PM	09/20/2021 12:37:08 PM	demo/sqlqdba	

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 © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

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

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