



Proteger bancos de dados Oracle

SnapCenter Software 4.9

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/pt-br/snapcenter-49/protect-sco/concept_what_you_can_do_with_the_snapcenter_plug_in_for_oracle_database.html on September 26, 2025. Always check docs.netapp.com for the latest.

Índice

Proteger bancos de dados Oracle	1
Visão geral do plug-in SnapCenter para banco de dados Oracle	1
O que você pode fazer com o Plug-in para Oracle Database	1
Recursos do Plug-in para banco de dados Oracle	1
Tipos de armazenamento suportados pelo Plug-in para Oracle Database	3
Preparar sistemas de storage para replicação SnapMirror e SnapVault para plug-in para Oracle	5
Mínimo de ONTAP Privileges necessário para plug-in para Oracle	5
Instale o plug-in do SnapCenter para o banco de dados Oracle	7
Fluxo de trabalho de instalação do plug-in SnapCenter para banco de dados Oracle	7
Pré-requisitos para adicionar hosts e instalar o pacote Plug-ins para Linux ou AIX	8
Adicione hosts e instale o pacote Plug-ins para Linux ou AIX usando GUI	17
Maneiras alternativas de instalar o pacote Plug-ins para Linux ou AIX	21
Configure o serviço SnapCenter Plug-in Loader	24
Configure o certificado CA com o serviço SnapCenter Plug-in Loader (SPL) no host Linux	27
Ative certificados de CA para plug-ins	29
Importar dados do SnapManager para Oracle e SnapManager para SAP para SnapCenter	30
Instale o plug-in do SnapCenter para VMware vSphere	36
Implantar certificado CA	36
Configure o arquivo CRL	36
Prepare-se para proteger bancos de dados Oracle	36
Faça backup de bancos de dados Oracle	38
Visão geral do procedimento de backup	38
Informações de configuração de backup	39
Requisitos para fazer backup de um banco de dados Oracle	52
Descubra os bancos de dados Oracle disponíveis para backup	52
Criar políticas de backup para bancos de dados Oracle	54
Crie grupos de recursos e anexe políticas para bancos de dados Oracle	59
Faça backup dos recursos Oracle	61
Faça backup de grupos de recursos de banco de dados Oracle	63
Monitorar o backup do banco de dados Oracle	64
Outras operações de backup	66
Montar e desmontar backups de bancos de dados	69
Montar um backup de banco de dados	70
Desmontar um backup de banco de dados	71
Restaurar e recuperar bancos de dados Oracle	71
Restaure o fluxo de trabalho	71
Definir uma estratégia de restauração e recuperação para bancos de dados Oracle	72
Variáveis de ambiente predefinidas para restaurar prescrição específica e postscript	77
Requisitos para restaurar um banco de dados Oracle	78
Restaurar e recuperar banco de dados Oracle	79
Restaure e recupere espaços de tablespaces usando recuperação ponto no tempo	84
Restaurar e recuperar banco de dados conetável usando recuperação pontual	86
Restaure e recupere bancos de dados Oracle usando comandos UNIX	88

Monitorar operações de restauração de banco de dados Oracle	89
Cancelar operações de restauração de banco de dados Oracle	90
Clonar banco de dados Oracle	90
Fluxo de trabalho clone	90
Definir uma estratégia de clone para bancos de dados Oracle	91
Variáveis de ambiente predefinidas para o prescritor específico de clone e postscript	92
Requisitos para clonar um banco de dados Oracle	94
Clonar um backup de banco de dados Oracle	96
Clone um banco de dados conectável	105
Clonar backups de bancos de dados Oracle usando comandos UNIX	109
Divida um clone do banco de dados Oracle	110
Clone dividido de um banco de dados conectável	111
Monitorar operações de clone de banco de dados Oracle	111
Atualize um clone	112
Excluir clone de um banco de dados conectável	113
Gerenciar volumes de aplicações	114
Adicionar volumes de aplicações	114
Volumes de aplicações de backup	115
Clone o backup de volume de aplicativo	117

Proteger bancos de dados Oracle

Visão geral do plug-in SnapCenter para banco de dados Oracle

O que você pode fazer com o Plug-in para Oracle Database

O plug-in SnapCenter para banco de dados Oracle é um componente do lado do host do software NetApp SnapCenter que permite o gerenciamento de proteção de dados com reconhecimento de aplicações de bancos de dados Oracle.

O plug-in para banco de dados Oracle automatiza o backup, catalogação e desinstalação com o Oracle Recovery Manager (RMAN), verificação, montagem, desmontagem, restauração, recuperação e clonagem de bancos de dados Oracle em seu ambiente SnapCenter. O plug-in para banco de dados Oracle instala o plug-in do SnapCenter para UNIX para executar todas as operações de proteção de dados.

Você pode usar o Plug-in para Oracle Database para gerenciar backups de bancos de dados Oracle que executam aplicativos SAP. No entanto, a integração SAP BR*Tools não é suportada.

- Faça backup de arquivos de dados, arquivos de controle e arquivos de log de arquivamento.

A cópia de segurança é suportada apenas no nível da base de dados de contentores (CDB).

- Restauração e recuperação de bancos de dados, CDBs e bancos de dados conetáveis (PDBs).

A recuperação incompleta de PDBs não é suportada.

- Crie clones de bancos de dados de produção até um ponto no tempo.

A clonagem é suportada apenas no nível CDB.

- Verifique os backups imediatamente.
- Monte e desmonte os backups de dados e log para operação de recuperação.
- Agendar operações de backup e verificação.
- Monitorar todas as operações.
- Exibir relatórios para operações de backup, restauração e clone.

Recursos do Plug-in para banco de dados Oracle

O plug-in para banco de dados Oracle se integra ao banco de dados Oracle no host Linux ou AIX e com tecnologias NetApp no sistema de armazenamento.

- Interface gráfica do usuário unificada

A interface do SnapCenter fornece padronização e consistência em plug-ins e ambientes. A interface do SnapCenter permite concluir operações consistentes de backup, restauração, recuperação e clone em plug-ins, usar relatórios centralizados, usar visualizações de dashboard rápidas, configurar controle de acesso baseado em funções (RBAC) e monitorar tarefas em todos os plug-ins.

- Administração central automatizada

Você pode agendar operações de backup e clone, configurar a retenção de backup baseada em política e executar operações de restauração. Você também pode monitorar proativamente seu ambiente configurando o SnapCenter para enviar alertas por e-mail.

- Tecnologia de cópia Snapshot sem interrupções NetApp

O SnapCenter usa a tecnologia de cópia Snapshot do NetApp com o plug-in para banco de dados Oracle e plug-in para UNIX para fazer backup de bancos de dados. As cópias Snapshot consomem espaço mínimo de storage.

O Plug-in para Oracle Database também oferece os seguintes benefícios:

- Suporte para fluxos de trabalho de backup, restauração, clonagem, montagem, desmontagem e verificação
- Descoberta automática de bancos de dados Oracle configurados no host
- Suporte para catalogação e descatalogação usando o Oracle Recovery Manager (RMAN)
- Delegação de funções centralizada e segurança compatível com RBAC

Você também pode definir as credenciais para que os usuários autorizados do SnapCenter tenham permissões no nível do aplicativo.

- Suporte para gerenciamento de logs de arquivamento (ALM) para operações de restauração e clonagem
- Criação de cópias pontuais e com uso eficiente de espaço de bancos de dados de produção para teste ou extração de dados usando a tecnologia NetApp FlexClone

É necessária uma licença FlexClone no sistema de storage onde você deseja criar o clone.

- Suporte ao recurso de grupo de consistência (CG) do ONTAP como parte da criação de backups em ambientes SAN e ASM
- Verificação de backup sem interrupções e automatizada
- Funcionalidade de executar vários backups simultaneamente em vários hosts de banco de dados

Em uma única operação, as cópias Snapshot são consolidadas quando os bancos de dados em um único host compartilham o mesmo volume.

- Suporte para infraestruturas físicas e virtualizadas
- Suporte para NFS, iSCSI, Fibre Channel (FC), RDM, VMDK em NFS e VMFS, e ASM em NFS, SAN, RDM e VMDK
- Suporte para o recurso de mapa LUN seletivo (SLM) do ONTAP

Habilitado por padrão, o recurso SLM detecta periodicamente os LUNs que não têm caminhos otimizados e os corrige. Você pode configurar o SLM modificando os parâmetros no arquivo `scu.properties` localizado em `/var/opt/SnapCenter/scu/etc`.

- Você pode desativar isso definindo o valor do parâmetro `ENABLE_LUNPATH_MONITORING` como `false`.
- Você pode especificar a frequência em que os caminhos LUN serão corrigidos automaticamente atribuindo o valor (em horas) ao parâmetro `LUNPATH_MONITORING_INTERVAL`. Para obter informações sobre o SLM, consulte ["Guia de administração de SAN ONTAP 9"](#).

- Suporte para memória não volátil Express (NVMe) no Linux

- O NVMe útil deve ser instalado no host.

É necessário instalar o NVMe util para clonar ou montar em um host alternativo.

- Operações de backup, restauração, clone, montagem, desmontagem, catálogo, descátalo e verificação são compatíveis com o hardware NVMe, exceto para ambientes virtualizados como VMDK e RDM.

As operações acima são suportadas em dispositivos sem partições ou com partição única.



Você pode configurar a solução multipathing para dispositivos NVMe definindo a opção multipathing nativa no kernel. O multipathing do Mapeador de dispositivos (DM) não é suportado.

- Suporta qualquer usuário não padrão em vez de oracle e Grid.

Para oferecer suporte aos usuários não padrão, você deve definir os usuários não padrão modificando os valores dos parâmetros no arquivo **sco.properties** localizado em *file /var/opt/SnapCenter/SCO/etc/*.

Os valores padrão dos parâmetros são definidos como oracle e Grid.

- DB_USER: oracle
- DB_GROUP
- GI_USER_grid
- GI_GROUP: Instalação

Tipos de armazenamento suportados pelo Plug-in para Oracle Database

O SnapCenter oferece suporte a uma ampla variedade de tipos de armazenamento em máquinas físicas e virtuais. Você deve verificar o suporte para seu tipo de storage antes de instalar o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do SnapCenter para AIX.

O SnapCenter não oferece suporte ao provisionamento de storage para Linux e AIX.

Tipos de armazenamento compatíveis com Linux

A tabela a seguir lista os tipos de armazenamento suportados no Linux.

Máquina	Tipo de armazenamento
Servidor físico	• LUNs conectados a FC • LUNs ligados ao iSCSI • Volumes conectados a NFS

Máquina	Tipo de armazenamento
VMware ESXi	- LUNs RDM conectados por um FC ou iSCSI ESXi HAScanning de adaptadores de barramento de host (HBAs) pode levar muito tempo para ser concluído porque o SnapCenter verifica todos os adaptadores de barramento de host presentes no host. Você pode editar o arquivo LinuxConfig.pm localizado em <code>/opt/NetApp/SnapCenter/spl/plugins/scu/scucore/modules/SCU/Config</code> para definir o valor do parâmetro SCSI_HOSTS_OPTIMIZED_RESCAN para 1 para reexaminar somente os HBA listados em HBA_DRIVER_NAMES. - iSCSI LUNs ligados diretamente ao sistema convidado pelo iniciador iSCSI - VMDKs em armazenamentos de dados VMFS ou NFS - Volumes NFS conectados diretamente ao sistema convidado

Tipos de storage compatíveis com AIX

A tabela a seguir lista os tipos de armazenamento suportados no AIX.

Máquina	Tipo de armazenamento
Servidor físico	- LUNs conectados a FC e iSCSI. Em um ambiente SAN, os sistemas de arquivos ASM, LVM e SAN são compatíveis.  NFS no AIX e no sistema de arquivos não é suportado. - Sistema de arquivos Journaled aprimorado (JFS2) Suporta log in-line em sistemas de arquivos SAN e layout LVM.

O ["Ferramenta de Matriz de interoperabilidade do NetApp"](#) contém as informações mais recentes sobre as versões suportadas.

Preparar sistemas de storage para replicação SnapMirror e SnapVault para plug-in para Oracle

Você pode usar um plug-in do SnapCenter com a tecnologia ONTAP SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e com a tecnologia ONTAP SnapVault para executar replicação de backup disco a disco para conformidade com os padrões e outros fins relacionados à governança. Antes de executar essas tarefas, você deve configurar uma relação de proteção de dados entre os volumes de origem e destino e inicializar a relação.

O SnapCenter executa as atualizações para o SnapMirror e o SnapVault após concluir a operação de cópia Snapshot. As atualizações SnapMirror e SnapVault são executadas como parte da tarefa SnapCenter; não crie uma agenda ONTAP separada.



Se você estiver vindo para o SnapCenter de um produto NetApp SnapManager e estiver satisfeito com as relações de proteção de dados que configurou, ignore esta seção.

Uma relação de proteção de dados replica dados no storage primário (o volume de origem) para o storage secundário (o volume de destino). Ao inicializar a relação, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.



O SnapCenter não suporta relações em cascata entre volumes SnapMirror e SnapVault (**Primary > Mirror > Vault**). Você deve usar relacionamentos de fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis de versão e como configurá-los, consulte "[Documentação do ONTAP](#)".



O SnapCenter não suporta replicação **Sync_mirror**.

Mínimo de ONTAP Privileges necessário para plug-in para Oracle

Os ONTAP Privileges mínimos necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

- Comandos All-Access: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior
 - event generate-AutoSupport-log
 - mostra o histórico de trabalhos
 - paragem do trabalho
 - lun
 - show de atributo lun
 - lun criar
 - eliminação lun
 - geometria lun
 - lun igrop add
 - lun igrop criar

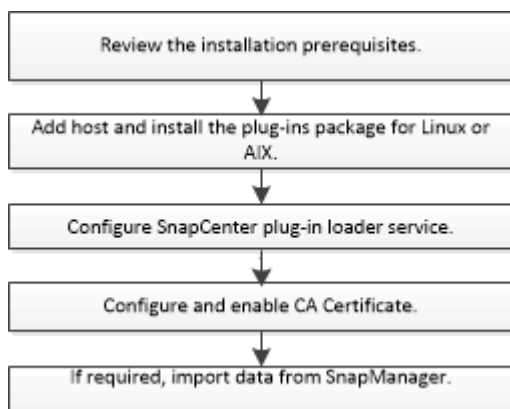
- eliminação do agrupamento lun
- mudar o nome do grupo lun
- show de grupos de lun
- nós complementares de mapeamento de lun
- mapeamento lun criar
- eliminação do mapeamento lun
- mapeamento lun remove-reporting-nonos
- mostra de mapeamento lun
- modificação de lun
- movimentação de lun no volume
- lun offline
- lun online
- limpeza da reserva persistente de lun
- redimensionar lun
- série lun
- mostra lun
- regra adicional de política do SnapMirror
- regra de modificação de política do SnapMirror
- regra de remoção da política do SnapMirror
- SnapMirror policy show
- restauração de SnapMirror
- SnapMirror show
- SnapMirror show-history
- atualização do SnapMirror
- SnapMirror update-ls-set
- SnapMirror lista-destinos
- versão
- clone de volume criar
- show de clone de volume
- início da divisão do clone de volume
- paragem dividida clone volume
- criar volume
- destruição de volume
- clone de arquivo de volume criar
- show-disk-use do arquivo de volume
- volume off-line
- volume online

- modificação do volume
- criar qtree de volume
- eliminação de qtree de volume
- modificação de qtree de volume
- apresentação de qtree de volume
- restrição de volume
- apresentação do volume
- criar instantâneo de volume
- eliminar instantâneo do volume
- modificação do instantâneo do volume
- mudar o nome do instantâneo do volume
- restauração de snapshot de volume
- restauração de arquivo de snapshot de volume
- apresentação de instantâneo do volume
- desmontar o volume
- svm
- svm cifs
- apresentação do shadowcopy cifs de svm
- mostra o svm
- interface de rede
- mostra da interface de rede
- MetroCluster show

Instale o plug-in do SnapCenter para o banco de dados Oracle

Fluxo de trabalho de instalação do plug-in SnapCenter para banco de dados Oracle

Você deve instalar e configurar o plug-in do SnapCenter para o banco de dados Oracle se quiser proteger os bancos de dados Oracle.



Pré-requisitos para adicionar hosts e instalar o pacote Plug-ins para Linux ou AIX

Antes de adicionar um host e instalar os pacotes de plug-ins, você deve completar todos os requisitos.

- Se estiver a utilizar iSCSI, o serviço iSCSI tem de estar em execução.
- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.

O plug-in do SnapCenter para banco de dados Oracle pode ser instalado por um usuário não-root. No entanto, você deve configurar o sudo Privileges para que o usuário não-root instale e inicie o processo de plug-in. Depois de instalar o plug-in, os processos serão executados como um usuário não-root eficaz.

- Se você estiver instalando o pacote de plug-ins do SnapCenter para AIX no host AIX, você deverá ter resolvido manualmente os links simbólicos no nível do diretório.

O pacote de plug-ins do SnapCenter para AIX resolve automaticamente o link simbólico no nível do arquivo, mas não os links simbólicos no nível do diretório para obter o caminho absoluto JAVA_HOME.

- Crie credenciais com o modo de autenticação como Linux ou AIX para o usuário de instalação.
- Você deve ter instalado Java 1,8.x ou Java 11, 64-bit, em seu host Linux ou AIX.



Certifique-se de ter instalado apenas a edição certificada DO Java 11 no host Linux.

Para obter informações sobre O download DO JAVA, consulte:

- ["Downloads Java para todos os sistemas operacionais"](#)
- ["IBM Java para AIX"](#)
- Para bancos de dados Oracle que estão sendo executados em um host Linux ou AIX, você deve instalar o plug-in SnapCenter para banco de dados Oracle e o plug-in SnapCenter para UNIX.



Você também pode usar o Plug-in para Oracle Database para gerenciar bancos de dados Oracle para SAP. No entanto, a integração SAP BR*Tools não é suportada.

- Se você estiver usando o banco de dados Oracle 11.2.0.3 ou posterior, você deve instalar o patch 13366202 Oracle.



O mapeamento UUID no arquivo /etc/fstab não é suportado pelo SnapCenter.

- Você deve ter **bash** como o shell padrão para instalação do plug-in.

Requisitos de Host Linux

Você deve garantir que o host atenda aos requisitos antes de instalar o pacote de plug-ins do SnapCenter para Linux.

Item	Requisitos
Sistemas operacionais	• Red Hat Enterprise Linux • Oracle Linux  Se você estiver usando o banco de dados Oracle no LVM em sistemas operacionais Oracle Linux ou Red Hat Enterprise Linux 6,6 ou 7,0, instale a versão mais recente do Logical volume Manager (LVM). • SUSE Linux Enterprise Server (SLES)
RAM mínima para o plug-in SnapCenter no host	2 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	2 GB  Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registros. O espaço de registro necessário varia consoante o número de entidades a proteger e a frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	• Java 1,8.x (64-bit) Oracle Java e OpenJDK sabores • Java 11 (64 bits) versões Oracle Java e OpenJDK  Certifique-se de ter instalado apenas a edição certificada DO Java 11 no host Linux. Se você atualizou O JAVA para a versão mais recente, você deve garantir que a opção JAVA_HOME localizada em /var/opt/SnapCenter/spl/etc/spl.properties esteja definida para a versão JAVA correta e o caminho correto.

Para obter as informações mais recentes sobre versões suportadas, consulte o ["Ferramenta de Matriz de interoperabilidade do NetApp"](#).

Configure sudo Privileges para usuários não-root para host Linux

O SnapCenter 2,0 e versões posteriores permitem que um usuário não root instale o pacote de plug-ins do SnapCenter para Linux e inicie o processo de plug-in. Os processos de plug-in serão executados como um usuário não-root eficaz. Você deve configurar o sudo Privileges para que o usuário não-root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Edite o arquivo `/etc/ssh/sshd_config` para configurar os algoritmos de código de autenticação de mensagem: Macs hmac-SHA2-256 e MACs hmac-SHA2-512.

Reinicie o serviço sshd depois de atualizar o arquivo de configuração.

Exemplo:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

Sobre esta tarefa

Você deve configurar o sudo Privileges para que o usuário não-root forneça acesso aos seguintes caminhos:

- `/Home/Linux_USER/.SC_NetApp/SnapCenter_linux_host_plugin.bin`
- `/Custom_location/NetApp/SnapCenter/spl/installation/plugins/uninstall`
- `/Custom_location/NetApp/SnapCenter/spl/bin/spl`

Passos

1. Faça login no host Linux no qual você deseja instalar o pacote de plug-ins do SnapCenter para Linux.
2. Adicione as seguintes linhas ao arquivo `/etc/sudoers` usando o utilitário visudo Linux.

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



Se você estiver tendo uma configuração RAC, juntamente com os outros comandos permitidos, você deve adicionar o seguinte ao arquivo `/etc/sudoers`:

```
'/<crs_home>/bin/olsnodes'
```

Você pode obter o valor de `crs_Home` do arquivo `/etc/oracle/olr.loc`.

`LINUX_USER` é o nome do usuário não-root que você criou.

Você pode obter o `checksum_value` a partir do arquivo **oracle_checksum.txt**, que está localizado em `C:/NetApp/SnapCenter/Repository`.

Se tiver especificado uma localização personalizada, a localização será `custom_path/NetApp/SnapCenter/Package Repository`.



O exemplo deve ser usado apenas como referência para criar seus próprios dados.

Requisitos de anfitrião do AIX

Você deve garantir que o host atenda aos requisitos antes de instalar o pacote de plug-ins do SnapCenter para AIX.



O plug-in do SnapCenter para UNIX, que faz parte do pacote de plug-ins do SnapCenter para AIX, não suporta grupos de volume simultâneos.

Item	Requisitos
Sistemas operacionais	AIX 7,1 ou posterior

Item	Requisitos
RAM mínima para o plug-in SnapCenter no host	4 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	2 GB  Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	• Java 1,8.x (64 bits) IBM Java • Java 11 (64 bits) IBM Java Se você atualizou O JAVA para a versão mais recente, você deve garantir que a opção JAVA_HOME localizada em /var/opt/SnapCenter/spl/etc/spl.properties esteja definida para a versão JAVA correta e o caminho correto.

Para obter as informações mais recentes sobre versões suportadas, consulte o ["Ferramenta de Matriz de interoperabilidade do NetApp"](#).

Configure sudo Privileges para usuários não-root para host AIX

O SnapCenter 4,4 e posterior permite que um usuário não root instale o pacote de plug-ins do SnapCenter para AIX e inicie o processo de plug-in. Os processos de plug-in serão executados como um usuário não-root eficaz. Você deve configurar o sudo Privileges para que o usuário não-root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Edite o arquivo `/etc/ssh/sshd_config` para configurar os algoritmos de código de autenticação de mensagem: Macs hmac-SHA2-256 e MACs hmac-SHA2-512.

Reinicie o serviço sshd depois de atualizar o arquivo de configuração.

Exemplo:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

Sobre esta tarefa

Você deve configurar o sudo Privileges para que o usuário não-root forneça acesso aos seguintes caminhos:

- /Home/AIX_USER/.SC_NetApp/SnapCenter_aix_host_plugin.bsx
- /Custom_location/NetApp/SnapCenter/spl/installation/plugins/uninstall,
- /Custom_location/NetApp/SnapCenter/spl/bin/spl

Passos

1. Faça login no host AIX no qual você deseja instalar o pacote de plug-ins do SnapCenter para AIX.
2. Adicione as seguintes linhas ao arquivo /etc/sudoers usando o utilitário visudo Linux.

```
Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```



Se você estiver tendo uma configuração RAC, juntamente com os outros comandos permitidos, você deve adicionar o seguinte ao arquivo /etc/sudoers:
'<crs_home>/bin/olsnodes'

Você pode obter o valor de `crs_Home` do arquivo `/etc/oracle/olr.loc`.

`AIX_USER` é o nome do usuário não-root que você criou.

Você pode obter o `checksum_value` a partir do arquivo **oracle_checksum.txt**, que está localizado em `C:/NetApp/SnapCenter/Repository`.

Se tiver especificado uma localização personalizada, a localização será `custom_path/NetApp/SnapCenter/Package Repository`.



O exemplo deve ser usado apenas como referência para criar seus próprios dados.

Configurar credenciais

O SnapCenter usa credenciais para autenticar usuários para operações do SnapCenter. Você deve criar credenciais para instalar o pacote plug-in em hosts Linux ou AIX.

Sobre esta tarefa

As credenciais são criadas para o usuário raiz ou para um usuário não-root que tenha sudo Privileges para instalar e iniciar o processo de plug-in.

Para obter informações, consulte: [Configure sudo Privileges para usuários não-root para host Linux](#) Ou [Configure sudo Privileges para usuários não-root para host AIX](#)

Prática recomendada: embora você tenha permissão para criar credenciais após implantar hosts e instalar plug-ins, a prática recomendada é criar credenciais após adicionar SVMs, antes de implantar hosts e instalar plug-ins.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credential**.
3. Clique em **novo**.
4. Na página Credential (credencial), insira as informações da credencial:

Para este campo...	Faça isso...
Nome da credencial	Introduza um nome para as credenciais.

Para este campo...	Faça isso...
Nome de utilizador/Palavra-passe	Introduza o nome de utilizador e a palavra-passe a utilizar para a autenticação. - Administrador de domínio Especifique o administrador de domínio no sistema no qual você está instalando o plug-in SnapCenter. Os formatos válidos para o campo Nome de usuário são: <i>NetBIOS_username</i> <i>Domain FQDN_username</i> - Administrador local (apenas para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local incorporado no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host. O formato válido para o campo Nome de usuário é: <i>Nome de usuário</i>
Modo de autenticação	Selecione o modo de autenticação que pretende utilizar. Dependendo do sistema operacional do host plug-in, selecione Linux ou AIX.
Use sudo Privileges	Marque a caixa de seleção Use sudo Privileges se estiver criando credenciais para um usuário que não seja root.

5. Clique em **OK**.

Depois de concluir a configuração das credenciais, você pode querer atribuir a manutenção de credenciais a um usuário ou grupo de usuários na página **Usuário e Acesso**.

Configurar credenciais para um banco de dados Oracle

Você deve configurar credenciais usadas para executar operações de proteção de dados em bancos de dados Oracle.

Sobre esta tarefa

Você deve rever os diferentes métodos de autenticação suportados para o banco de dados Oracle. Para obter

informações, "[Métodos de autenticação para suas credenciais](#)" consulte .

Se você configurar credenciais para grupos de recursos individuais e o nome de usuário não tiver Privileges de administrador completo, o nome de usuário deve ter, pelo menos, Privileges de grupo de recursos e backup.

Se você ativou a autenticação do banco de dados Oracle, um ícone de cadeado vermelho será exibido na exibição recursos. Você deve configurar credenciais de banco de dados para poder proteger o banco de dados ou adicioná-lo ao grupo de recursos para executar operações de proteção de dados.



Se você especificar detalhes incorretos durante a criação de uma credencial, uma mensagem de erro será exibida. Você deve clicar em **Cancelar** e tentar novamente.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** na lista **Exibir**.
3. Clique  em e selecione o nome do host e o tipo de banco de dados para filtrar os recursos.

Em seguida, pode clicar  para fechar o painel de filtro.

4. Selecione o banco de dados e clique em **Configurações do banco de dados > Configurar banco de dados**.
5. Na seção Configurar configurações do banco de dados, na lista suspensa **usar credencial existente**, selecione a credencial que deve ser usada para executar tarefas de proteção de dados no banco de dados Oracle.



O usuário Oracle deve ter sysdba Privileges.

Você também pode criar uma credencial clicando  em .

6. Na seção Configurar configurações ASM, na lista suspensa **usar credencial existente**, selecione a credencial que deve ser usada para executar tarefas de proteção de dados na instância ASM.



O usuário ASM deve ter privilégio sysasm.

Você também pode criar uma credencial clicando  em .

7. Na seção Configurar configurações do catálogo RMAN, na lista suspensa **usar credencial existente**, selecione a credencial que deve ser usada para executar tarefas de proteção de dados no banco de dados de catálogo do Oracle Recovery Manager (RMAN).

Você também pode criar uma credencial clicando  em .

No campo **TNSName**, insira o nome do arquivo do substrato de rede transparente (TNS) que será usado pelo servidor SnapCenter para se comunicar com o banco de dados.

8. No campo **Preferred RAC Nodes**, especifique os nós do Real Application Cluster (RAC) preferidos para backup.

Os nós preferidos podem ser um ou todos os nós de cluster onde as instâncias de banco de dados RAC estão presentes. A operação de backup é acionada somente nesses nós preferenciais na ordem de

preferência.

No RAC One Node, apenas um nó é listado nos nós preferenciais e esse nó preferido é o nó onde o banco de dados está hospedado atualmente.

Após o failover ou realocação do banco de dados RAC de um nó, a atualização de recursos na página recursos do SnapCenter removerá o host da lista **Preferred RAC Nodes**, onde o banco de dados foi hospedado anteriormente. O nó RAC onde o banco de dados é realocado será listado em **nós RAC** e precisará ser configurado manualmente como o nó RAC preferido.

Para obter mais informações, "[Nós preferenciais na configuração RAC](#)" consulte .

9. Clique em **OK**.

Adicione hosts e instale o pacote Plug-ins para Linux ou AIX usando GUI

Você pode usar a página Adicionar host para adicionar hosts e, em seguida, instalar o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do SnapCenter para AIX. Os plug-ins são instalados automaticamente nos hosts remotos.

Sobre esta tarefa

Você pode adicionar um host e instalar pacotes de plug-in para um host individual ou para um cluster. Se você estiver instalando o plug-in em um cluster (Oracle RAC), o plug-in será instalado em todos os nós do cluster. Para Oracle RAC One Node, você deve instalar o plug-in em nós ativos e passivos.

Você deve ser atribuído a uma função que tenha as permissões de instalação e desinstalação do plug-in, como a função Administrador do SnapCenter.



Não é possível adicionar um servidor SnapCenter como um host plug-in a outro servidor SnapCenter.

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Verifique se a guia **hosts gerenciados** está selecionada na parte superior.
3. Clique em **Add**.
4. Na página hosts, execute as seguintes ações:

Para este campo...	Faça isso...
Tipo de host	Selecione Linux ou AIX como o tipo de host. O servidor SnapCenter adiciona o host e, em seguida, instala o plug-in para banco de dados Oracle e o plug-in para UNIX se os plug-ins ainda não estiverem instalados no host.

Para este campo...	Faça isso...
Nome do host	Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração adequada do DNS. Portanto, a melhor prática é entrar no FQDN. Você pode inserir os endereços IP ou FQDN de um dos seguintes: • Anfitrião independente • Qualquer nó no ambiente do Oracle Real Application clusters (RAC)  O nó VIP ou IP de digitalização não é suportado Se você estiver adicionando um host usando o SnapCenter e o host fizer parte de um subdomínio, você deverá fornecer o FQDN.
Credenciais	Selecione o nome da credencial que você criou ou crie novas credenciais. A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte as informações sobre como criar credenciais. Você pode exibir detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você especificou.  O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar host.

5. Na seção Selecionar plug-ins para instalar, selecione os plug-ins a instalar.

6. (Opcional) clique em **mais opções**.

Para este campo...	Faça isso...
Porta	Guarde o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o servidor SnapCenter tiver sido instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão.  Se você instalou manualmente os plug-ins e especificou uma porta personalizada, você deve especificar a mesma porta. Caso contrário, a operação falha.
Caminho de instalação	O caminho padrão é <code>/opt/NetApp/SnapCenter</code>. Opcionalmente, você pode personalizar o caminho.
Adicione todos os hosts no Oracle RAC	Marque essa caixa de seleção para adicionar todos os nós de cluster em um Oracle RAC. Em uma configuração do Flex ASM, todos os nós, independentemente de ser um nó Hub ou Leaf, serão adicionados.
Ignorar verificações de pré-instalação opcionais	Marque essa caixa de seleção se você já instalou os plug-ins manualmente e não deseja validar se o host atende aos requisitos para instalar o plug-in.

7. Clique em **Enviar**.

Se você não tiver selecionado a caixa de seleção Ignorar pré-verificações, o host será validado para verificar se o host atende aos requisitos para instalar o plug-in.



O script de pré-verificação não valida o status do firewall da porta do plug-in se for especificado nas regras de rejeição do firewall.

Mensagens de erro ou aviso apropriadas são exibidas se os requisitos mínimos não forem atendidos. Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo `web.config` localizado em `_C: SnapCenter NetApp` para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deve corrigir o problema.



Em uma configuração de HA, se você estiver atualizando o arquivo `web.config`, será necessário atualizar o arquivo em ambos os nós.

8. Verifique a impressão digital e clique em **Confirm and Submit**.

Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós no cluster.



O SnapCenter não suporta o algoritmo ECDSA.



A verificação de impressões digitais é obrigatória mesmo que o mesmo host tenha sido adicionado anteriormente ao SnapCenter e a impressão digital tenha sido confirmada.

9. Monitorize o progresso da instalação.

Os arquivos de log específicos da instalação estão localizados em `/custom_location/SnapCenter/logs`.

Resultado

Todos os bancos de dados no host são automaticamente descobertos e exibidos na página recursos. Se nada for exibido, clique em **Atualizar recursos**.

Monitorar o status da instalação

Pode monitorizar o progresso da instalação do pacote de plug-ins do SnapCenter utilizando a página trabalhos. Você pode querer verificar o andamento da instalação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

-  Em curso
-  Concluído com êxito
-  Falha
-  Preenchido com avisos ou não foi possível iniciar devido a avisos
-  Em fila de espera

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, para filtrar a lista de modo a que apenas as operações de instalação de plug-in sejam listadas, faça o seguinte:
 - a. Clique em **filtro**.
 - b. Opcional: Especifique a data de início e fim.
 - c. No menu suspenso tipo, selecione **Instalação Plug-in**.
 - d. No menu suspenso Status, selecione o status da instalação.
 - e. Clique em **aplicar**.
4. Selecione o trabalho de instalação e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Visualizar logs**.

Maneiras alternativas de instalar o pacote Plug-ins para Linux ou AIX

Você também pode instalar o pacote Plug-ins para Linux ou AIX manualmente usando os cmdlets ou CLIs.

Antes de instalar o plug-in manualmente, você deve validar a assinatura do pacote binário usando a chave **SnapCenter_public_key.pub** e **SnapCenter_linux_host_plugin.bin.SIG** localizada em *C:\ProgramData\NetApp\SnapCenter Package\Repository*.



Certifique-se de que **OpenSSL 1,0.2g** esteja instalado no host onde você deseja instalar o plug-in.

Valide a assinatura do pacote binário executando o comando:

- Para host Linux: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bin.sig snapcenter_linux_host_plugin.bin`
- Para o host AIX: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bsx.sig snapcenter_linux_host_plugin.bsx`

Instale em vários hosts remotos usando cmdlets

Você deve usar o cmdlet *Install-SmHostPackage* PowerShell para instalar o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do SnapCenter para AIX em vários hosts.

O que você vai precisar

Você deve estar conectado ao SnapCenter como um usuário de domínio com direitos de administrador local em cada host no qual deseja instalar o pacote de plug-in.

Passos

1. Inicie o PowerShell.
2. No host do servidor SnapCenter, estabeleça uma sessão usando o cmdlet *Open-SmConnection* e insira suas credenciais.
3. Instale o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do SnapCenter para AIX usando o cmdlet *Install-SmHostPackage* e os parâmetros necessários.

Você pode usar a opção *-skipprecheck* quando já tiver instalado os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.



O script de pré-verificação não valida o status do firewall da porta do plug-in se for especificado nas regras de rejeição do firewall.

4. Insira suas credenciais para instalação remota.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *get-Help command_name*. Em alternativa, pode também consultar o ["Guia de referência de cmdlet do software SnapCenter"](#).

Instalar no host do cluster

Você deve instalar o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do SnapCenter para AIX em ambos os nós do host do cluster.

Cada um dos nós do host do cluster tem dois IPs. Um dos IPs será o IP público dos respectivos nós e o segundo IP será o IP do cluster compartilhado entre ambos os nós.

Passos

1. Instale o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do SnapCenter para AIX nos dois nós do host do cluster.
2. Valide que os valores corretos para os parâmetros `SnapCenter_SERVER_HOST`, `SPL_PORT`, `SnapCenter_SERVER_PORT` e `SPL_ENABLED_PLUGINS` são especificados no arquivo `spl.properties` localizado em `/var/opt/SnapCenter/spl/etc/`.

Se `SPL_ENABLED_PLUGINS` não for especificado no `spl.properties`, você pode adicioná-lo e atribuir o valor `SCO,SCU`.

3. No host do servidor SnapCenter, estabeleça uma sessão usando o cmdlet *Open-SmConnection* e insira suas credenciais.
4. Em cada um dos nós, defina os IPs preferidos do nó usando o comando *set-PreferredHostIPsInStorageExportPolicy* `sccli` e os parâmetros necessários.
5. No host do servidor SnapCenter, adicione uma entrada para o IP do cluster e o nome DNS correspondente em `C:/Windows/System32/drivers/etc/hosts`.
6. Adicione o nó ao servidor SnapCenter usando o cmdlet *Add-SmHost* especificando o IP do cluster para o nome do host.

Descubra o banco de dados Oracle no nó 1 (supondo que o IP do cluster esteja hospedado no nó 1) e crie um backup do banco de dados. Se ocorrer um failover, você poderá usar o backup criado no nó 1 para restaurar o banco de dados no nó 2. Você também pode usar o backup criado no nó 1 para criar um clone no nó 2.



Haverá volumes, diretórios e arquivos de bloqueio obsoletos se o failover ocorrer enquanto quaisquer outras operações do SnapCenter estiverem em execução.

Instale o pacote Plug-ins para Linux no modo silencioso

Você pode instalar o pacote de plug-ins do SnapCenter para Linux no modo silencioso usando a interface de linha de comando (CLI).

O que você vai precisar

- Você deve rever os pré-requisitos para instalar o pacote de plug-ins.
- Você deve garantir que a variável de ambiente de EXIBIÇÃO não esteja definida.

Se a variável de ambiente DE EXIBIÇÃO estiver definida, você deverá executar A EXIBIÇÃO não definida e, em seguida, tentar instalar manualmente o plug-in.

Sobre esta tarefa

Você é obrigado a fornecer as informações de instalação necessárias durante a instalação no modo console, enquanto na instalação do modo silencioso você não precisa fornecer nenhuma informação de instalação.

Passos

1. Faça o download do pacote de plug-ins do SnapCenter para Linux a partir do local de instalação do servidor SnapCenter.

O caminho de instalação padrão é *C:/ProgramData/NetApp/SnapCenter/PackageRepository*. Este caminho é acessível a partir do host onde o servidor SnapCenter está instalado.

2. No prompt de comando, navegue até o diretório onde você baixou o arquivo de instalação.
3. Executar

```
./SnapCenter_linux_host_plugin.bin -i silent-DPORT=8145-  
DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-  
DUSER_INSTALL_DIR=/opt/custom_path
```

4. Edite o arquivo *spl.properties* localizado em */var/opt/SnapCenter/spl/etc/* para adicionar *SPL_ENABLED_PLUGINS SCO,SCU* e, em seguida, reinicie o serviço SnapCenter Plug-in Loader.



A instalação do pacote plug-ins Registra os plug-ins no host e não no servidor SnapCenter. Você deve Registrar os plug-ins no servidor SnapCenter adicionando o host usando a GUI do SnapCenter ou cmdlet do PowerShell. Ao adicionar o host, selecione "nenhum" como a credencial. Depois que o host é adicionado, os plug-ins instalados são descobertos automaticamente.

Instale o pacote Plug-ins para AIX no modo silencioso

Você pode instalar o pacote de plug-ins do SnapCenter para AIX no modo silencioso usando a interface de linha de comando (CLI).

O que você vai precisar

- Você deve rever os pré-requisitos para instalar o pacote de plug-ins.
- Você deve garantir que a variável de ambiente de EXIBIÇÃO não esteja definida.

Se a variável de ambiente DE EXIBIÇÃO estiver definida, você deverá executar A EXIBIÇÃO não definida e, em seguida, tentar instalar manualmente o plug-in.

Passos

1. Faça o download do pacote de plug-ins do SnapCenter para AIX a partir do local de instalação do servidor SnapCenter.

O caminho de instalação padrão é *C:/ProgramData/NetApp/SnapCenter/PackageRepository*. Este caminho é acessível a partir do host onde o servidor SnapCenter está instalado.

2. No prompt de comando, navegue até o diretório onde você baixou o arquivo de instalação.
3. Executar

```
./snapcenter_aix_host_plugin.bsx -i silent-DPORT=8145-  
DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-  
DUSER_INSTALL_DIR=/opt/custom_path-  
DINSTALL_LOG_NAME=SnapCenter_AIX_Host_Plug-in_Install_MANUAL.log-
```

DCHOSEN_FEATURE_LIST=CUSTOMDSPL_USER=install_user

4. Edite o arquivo `spl.properties` localizado em `/var/opt/SnapCenter/spl/etc/` para adicionar `SPL_ENABLED_PLUGINS SCO,SCU` e, em seguida, reinicie o serviço SnapCenter Plug-in Loader.



A instalação do pacote plug-ins Registra os plug-ins no host e não no servidor SnapCenter. Você deve Registrar os plug-ins no servidor SnapCenter adicionando o host usando a GUI do SnapCenter ou cmdlet do PowerShell. Ao adicionar o host, selecione "nenhum" como a credencial. Depois que o host é adicionado, os plug-ins instalados são descobertos automaticamente.

Configure o serviço SnapCenter Plug-in Loader

O serviço SnapCenter Plug-in Loader carrega o pacote plug-in para Linux ou AIX para interagir com o servidor SnapCenter. O serviço Plug-in Loader do SnapCenter é instalado quando você instala o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do SnapCenter para AIX.

Sobre esta tarefa

Depois de instalar o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do SnapCenter para AIX, o serviço Loader do plug-in do SnapCenter é iniciado automaticamente. Se o serviço Loader de plug-in do SnapCenter não for iniciado automaticamente, você deve:

- Certifique-se de que o diretório em que o plug-in está a funcionar não é eliminado
- Aumente o espaço de memória atribuído à Máquina Virtual Java

O arquivo `spl.properties`, que está localizado em `/custom_location/NetApp/SnapCenter/spl/etc/`, contém os seguintes parâmetros. Os valores padrão são atribuídos a esses parâmetros.

Nome do parâmetro	Descrição
LOG_LEVEL	Apresenta os níveis de registo suportados. Os valores possíveis são TRACE, DEBUG, INFO, WARN, ERROR e FATAL.
SPL_PROTOCOL (PROTOCOLO SPL)	Apresenta o protocolo suportado pelo Plug-in Loader SnapCenter. Apenas o protocolo HTTPS é suportado. Você pode adicionar o valor se o valor padrão estiver ausente.
SnapCenter_SERVER_PROTOCOL	Apresenta o protocolo suportado pelo servidor SnapCenter. Apenas o protocolo HTTPS é suportado. Você pode adicionar o valor se o valor padrão estiver ausente.

Nome do parâmetro	Descrição
SKIP_JAVAHOME_UPDATE	Por padrão, o serviço SPL deteta o caminho java e atualiza o parâmetro Java_HOME. Portanto, o valor padrão é definido como FALSE. Você pode definir como VERDADEIRO se quiser desativar o comportamento padrão e corrigir manualmente o caminho java.
SPL_KEYSTORE_PASS	Exibe a senha do arquivo keystore. Você pode alterar esse valor somente se você alterar a senha ou criar um novo arquivo de keystore.
SPL_PORT	Exibe o número da porta na qual o serviço Plug-in Loader do SnapCenter está sendo executado. Você pode adicionar o valor se o valor padrão estiver ausente.  Você não deve alterar o valor depois de instalar os plug-ins.
SnapCenter_Server_HOST	Exibe o endereço IP ou o nome do host do servidor SnapCenter.
SPL_KEYSTORE_PATH	Exibe o caminho absoluto do arquivo keystore.
SnapCenter_SERVER_PORT	Exibe o número da porta na qual o servidor SnapCenter está sendo executado.
REGISTOS_MAX_COUNT	Exibe o número de arquivos de log do Loader do plug-in do SnapCenter que são retidos na pasta <i>/custom_location/SnapCenter/spl/logs</i>. O valor padrão é definido como 5000. Se a contagem for superior ao valor especificado, os últimos 5000 arquivos modificados serão retidos. A verificação do número de arquivos é feita automaticamente a cada 24 horas a partir do momento em que o serviço Loader Plug-in SnapCenter é iniciado.  Se você excluir manualmente o arquivo spl.properties, o número de arquivos a serem retidos será definido como 9999.

Nome do parâmetro	Descrição
JAVA_HOME	Exibe o caminho absoluto do diretório do JAVA_HOME que é usado para iniciar o serviço SPL. Este caminho é determinado durante a instalação e como parte da inicialização do SPL.
LOG_MAX_SIZE	Apresenta o tamanho máximo do ficheiro de registo de trabalhos. Assim que o tamanho máximo for atingido, o ficheiro de registo é zipado e os registos são gravados no novo ficheiro desse trabalho.
RETER_LOGS_OF_LAST_DAYS	Exibe o número de dias até os quais os logs são mantidos.
ENABLE_CERTIFICATE_VALIDATION	Exibe verdadeiro quando a validação do certificado CA está ativada para o host. Você pode ativar ou desativar esse parâmetro editando o spl.properties ou usando a GUI ou cmdlet do SnapCenter.

Se algum destes parâmetros não estiver atribuído ao valor predefinido ou se pretender atribuir ou alterar o valor, pode modificar o ficheiro spl.properties. Você também pode verificar o arquivo spl.properties e editar o arquivo para solucionar quaisquer problemas relacionados aos valores atribuídos aos parâmetros. Depois de modificar o arquivo spl.properties, você deve reiniciar o serviço SnapCenter Plug-in Loader.

Passos

1. Execute uma das seguintes ações, conforme necessário:

- Inicie o serviço SnapCenter Plug-in Loader como usuário raiz:

```
`/custom_location/NetApp/snapcenter/spl/bin/spl start`  
** Pare o serviço SnapCenter Plug-in Loader:
```

```
`/custom_location/NetApp/snapcenter/spl/bin/spl stop`
```



Você pode usar a opção -force com o comando stop para parar o serviço SnapCenter Plug-in Loader com força. No entanto, você deve ter cuidado antes de fazê-lo, porque ele também termina as operações existentes.

- Reinicie o serviço SnapCenter Plug-in Loader:

```
`/custom_location/NetApp/snapcenter/spl/bin/spl restart`  
** Encontre o status do serviço SnapCenter Plug-in Loader:
```

```
`/custom_location/NetApp/snapcenter/spl/bin/spl status`  
** Encontre a alteração no serviço SnapCenter Plug-in Loader:
```

```
`/custom_location/NetApp/snapcenter/spl/bin/spl change`
```

Configure o certificado CA com o serviço SnapCenter Plug-in Loader (SPL) no host Linux

Você deve gerenciar a senha do keystore SPL e seu certificado, configurar o certificado CA, configurar certificados raiz ou intermediários para o armazenamento de confiança SPL e configurar o par de chaves assinadas CA para o armazenamento de confiança SPL com o serviço SnapCenter Plug-in Loader para ativar o certificado digital instalado.



O SPL usa o arquivo 'keystore.jks', que está localizado em '/var/opt/SnapCenter/spl/etc', tanto como seu armazenamento de confiança e armazenamento de chaves.

Gerenciar senha para o armazenamento de chaves SPL e alias do par de chaves assinadas CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore SPL do arquivo de propriedade SPL.

É o valor correspondente à chave 'SPL_KEYSTORE_PASS'.

2. Altere a senha do keystore:

```
keytool -storepasswd -keystore keystore.jks  
. Altere a senha para todos os aliases de entradas de chave privada no  
keystore para a mesma senha usada para o keystore:
```

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

Atualize o mesmo para a chave SPL_KEYSTORE_PASS no arquivo spl.properties.

3. Reinicie o serviço depois de alterar a senha.



A senha para o keystore SPL e para todos os alias associados da chave privada deve ser a mesma.

Configure certificados raiz ou intermediários para o armazenamento de confiança SPL

Você deve configurar os certificados raiz ou intermediários sem a chave privada para o armazenamento de confiança SPL.

Passos

1. Navegue até a pasta que contém o keystore SPL: `/var/opt/SnapCenter/spl/etc`.
2. Localize o arquivo 'keystore.jks'.
3. Liste os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
. Adicione um certificado raiz ou intermediário:
```

```
keytool -import -trustcacerts -alias
<AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Reinicie o serviço depois de configurar os certificados raiz ou
intermediários para o armazenamento de confiança SPL.
```



Você deve adicionar o certificado de CA raiz e, em seguida, os certificados de CA intermediários.

Configure o par de chaves assinadas da CA para o armazenamento de confiança SPL

Você deve configurar o par de chaves assinadas da CA para o armazenamento de confiança SPL.

Passos

1. Navegue até a pasta que contém o keystore `/var/opt/SnapCenter/spl/etc` do SPL
2. Localize o arquivo 'keystore.jks'.
3. Liste os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
. Adicione o certificado da CA com chave privada e pública.
```

```
keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Liste os certificados adicionados no keystore.
```

```
keytool -list -v -keystore keystore.jks
```

. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.

. Altere a senha da chave privada adicionada para o certificado da CA para a senha do keystore.

A senha padrão do keystore SPL é o valor da chave SPL_KEYSTORE_PASS no arquivo spl.properties.

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks
```

. Se o nome do alias no certificado da CA for longo e contiver espaço ou caracteres especiais ("*", ",", "), altere o nome do alias para um nome simples:

```
keytool -changealias -alias "<OriginalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks
```

. Configure o nome do alias a partir do keystore localizado no arquivo spl.properties.

Atualize este valor com a chave SPL_CERTIFICATE_ALIAS.

4. Reinicie o serviço depois de configurar o par de chaves assinadas pela CA para o armazenamento de confiança SPL.

Configurar a lista de revogação de certificados (CRL) para SPL

Você deve configurar a CRL para SPL

Sobre esta tarefa

- O SPL procurará os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL para SPL é `/var/opt/SnapCenter/spl/etc/crl`.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo spl.properties contra a chave SPL_CRL_PATH.
2. Você pode colocar mais de um arquivo CRL neste diretório.

Os certificados recebidos serão verificados em relação a cada CRL.

Ative certificados de CA para plug-ins

Você deve configurar os certificados de CA e implantar os certificados de CA no servidor SnapCenter e nos hosts de plug-in correspondentes. Você deve habilitar a validação do

certificado CA para os plug-ins.

Antes de começar

- Você pode ativar ou desativar os certificados de CA usando o cmdlet `Set-SmCertificateSettings`.
- Você pode exibir o status do certificado para os plug-ins usando as `Get-SmCertificateSettings`.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando `get-Help command_name`. Em alternativa, pode também consultar o ["Guia de referência de cmdlet do software SnapCenter"](#).

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **hosts gerenciados**.
3. Selecione um ou vários hosts de plug-in.
4. Clique em **mais opções**.
5. Selecione **Ativar Validação de certificado**.

Depois de terminar

O host de guia hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o servidor SnapCenter e o host do plug-in.

-  ** Indica que o certificado da CA não está habilitado nem atribuído ao host do plug-in.
-  ** Indica que o certificado da CA foi validado com êxito.
-  ** Indica que o certificado da CA não pôde ser validado.
-  ** indica que as informações de conexão não puderam ser recuperadas.



Quando o status é amarelo ou verde, as operações de proteção de dados são concluídas com êxito.

Importar dados do SnapManager para Oracle e SnapManager para SAP para SnapCenter

A importação de dados do SnapManager para Oracle e SnapManager para SAP para SnapCenter permite que você continue usando seus dados de versões anteriores.

Você pode importar dados do SnapManager para Oracle e SnapManager para SAP para SnapCenter executando a ferramenta de importação a partir da interface de linha de comando (CLI de host Linux).

A ferramenta de importação cria políticas e grupos de recursos no SnapCenter. As políticas e os grupos de recursos criados no SnapCenter correspondem aos perfis e operações realizados usando esses perfis no SnapManager para Oracle e no SnapManager para SAP. A ferramenta de importação do SnapCenter interage com os bancos de dados de repositório do SnapManager para Oracle e SnapManager para SAP e o banco de dados que você deseja importar.

- Recupera todos os perfis, programações e operações realizadas usando os perfis.
- Cria uma política de backup do SnapCenter para cada operação exclusiva e cada agendamento anexado a um perfil.

- Cria um grupo de recursos para cada banco de dados de destino.

Você pode executar a ferramenta de importação executando o script SC-migrate localizado em `/opt/NetApp/SnapCenter/spl/bin`. Quando você instala o pacote de plug-ins do SnapCenter para Linux no host de banco de dados que deseja importar, o script SC-Migrate é copiado para `/opt/NetApp/SnapCenter/spl/bin`.



A importação de dados não é suportada pela interface gráfica do usuário (GUI) do SnapCenter.

O SnapCenter não suporta Data ONTAP operando no modo 7D. Você pode usar a ferramenta de transição de 7 modos para migrar dados e configurações que são armazenados em um sistema executando o Data ONTAP operando no modo 7 para um sistema ONTAP.

Configurações suportadas para importação de dados

Antes de importar dados do SnapManager 3,4.x para Oracle e SnapManager 3,4.x para SAP para SnapCenter, você deve estar ciente das configurações que são suportadas com o plug-in SnapCenter para banco de dados Oracle.

As configurações compatíveis com o plug-in SnapCenter para banco de dados Oracle estão listadas na ["Ferramenta de Matriz de interoperabilidade do NetApp"](#).

O que é importado para o SnapCenter

Você pode importar perfis, programações e operações realizadas usando os perfis.

Da SnapManager para Oracle e SnapManager para SAP	Para SnapCenter
Perfis sem quaisquer operações e horários	Uma política é criada com o tipo de backup padrão como Online e escopo de backup como Full.
Perfis com uma ou mais operações	Várias políticas são criadas com base em uma combinação única de um perfil e operações realizadas usando esse perfil. As políticas criadas no SnapCenter contêm os detalhes de eliminação e retenção de Registros de arquivamento recuperados do perfil e das operações correspondentes.
Perfis com configuração do Oracle Recovery Manager (RMAN)	As políticas são criadas com a opção Backup do Catálogo com o Oracle Recovery Manager ativada. Se a catalogação RMAN externa foi usada no SnapManager, você deve configurar as configurações do catálogo RMAN no SnapCenter. Você pode selecionar a credencial existente ou criar uma nova credencial. Se o RMAN foi configurado através do arquivo de controle no SnapManager, então você não precisa configurar o RMAN no SnapCenter.

Da SnapManager para Oracle e SnapManager para SAP	Para SnapCenter
Agendamento anexado a um perfil	Uma política é criada apenas para a programação.
Banco de dados	Um grupo de recursos é criado para cada banco de dados importado. Em uma configuração de Real Application clusters (RAC), o nó no qual você executa a ferramenta de importação se torna o nó preferido após a importação e o grupo de recursos é criado para esse nó.



Quando um perfil é importado, uma política de verificação é criada juntamente com a política de backup.

Quando os perfis SnapManager for Oracle e SnapManager for SAP, os horários e quaisquer operações realizadas usando os perfis são importados para o SnapCenter, os diferentes valores de parâmetros também são importados.

SnapManager para Oracle e SnapManager para SAP parâmetros e valores	Parâmetros e valores do SnapCenter	Notas
Escopo de backup • Cheio • Dados • Registo	Escopo de backup • Cheio • Dados • Registo	
Modo de cópia de segurança • Auto • Online • Offline	Tipo de cópia de segurança • Online • Encerramento offline	Se o modo de cópia de segurança for Auto, a ferramenta de importação verifica o estado da base de dados quando a operação foi executada e define adequadamente o tipo de cópia de segurança como Desligamento Online ou Offline.

SnapManager para Oracle e SnapManager para SAP parâmetros e valores	Parâmetros e valores do SnapCenter	Notas
Retenção • Dias • Conta	Retenção • Dias • Conta	O SnapManager para Oracle e o SnapManager para SAP usam dias e contagens para definir a retenção. Em SnapCenter, há dias <i>OU</i> contagens. Assim, a retenção é definida em relação aos dias, à medida que os dias recebem preferência em relação às contagens no SnapManager para Oracle e no SnapManager para SAP.
Poda para horários • Tudo • Número de mudança do sistema (SCN) • Data • Logs criados antes de horas, dias, semanas e meses especificados	Poda para horários • Tudo • Registos criados antes de horas e dias especificados	A SnapCenter não suporta a poda com base no SCN, Data, semanas e meses.
Notificação • E-mails enviados apenas para operações bem-sucedidas • E-mails enviados apenas para operações com falha • E-mails enviados para operações de sucesso e falha	Notificação • Sempre • Falha ao ligar • Aviso • Erro	As notificações por e-mail são importadas. No entanto, você deve atualizar manualmente o servidor SMTP usando a GUI do SnapCenter. O assunto do e-mail é deixado em branco para você configurar.

O que não é importado para o SnapCenter

A ferramenta de importação não importa tudo para o SnapCenter.

Não é possível importar o seguinte para o SnapCenter:

- Metadados de backup
- Backups parciais
- Backups relacionados ao RDM (Raw Device mapping) e VSC (Virtual Storage Console)
- Funções ou quaisquer credenciais disponíveis no repositório SnapManager para Oracle e SnapManager para SAP

- Dados relacionados a operações de verificação, restauração e clone
- Poda para operações
- Detalhes de replicação especificados no perfil SnapManager para Oracle e SnapManager para SAP

Após a importação, você deve editar manualmente a política correspondente criada no SnapCenter para incluir os detalhes da replicação.

- Informações de backup catalogadas

Prepare-se para importar dados

Antes de importar dados para o SnapCenter, é necessário executar determinadas tarefas para executar a operação de importação com êxito.

Passos

1. Identifique o banco de dados que você deseja importar.
2. Usando o SnapCenter, adicione o host do banco de dados e instale o pacote de plug-ins do SnapCenter para Linux.
3. Usando o SnapCenter, configure as conexões para as máquinas virtuais de armazenamento (SVMs) usadas pelos bancos de dados no host.
4. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
5. Na página recursos, verifique se o banco de dados a ser importado é descoberto e exibido.

Quando você deseja executar a ferramenta de importação, o banco de dados deve estar acessível ou então a criação do grupo de recursos falha.

Se o banco de dados tiver credenciais configuradas, você deverá criar uma credencial correspondente no SnapCenter, atribuir a credencial ao banco de dados e executar novamente a descoberta do banco de dados. Se o banco de dados estiver residindo no Gerenciamento Automático de armazenamento (ASM), você deverá criar credenciais para a instância ASM e atribuir a credencial ao banco de dados.

6. Certifique-se de que o usuário que executa a ferramenta de importação tenha Privileges suficiente para executar os comandos SnapManager para Oracle ou SnapManager para SAP CLI (como o comando para suspender programações) do SnapManager para Oracle ou SnapManager para host SAP.
7. Execute os seguintes comandos no host SnapManager para Oracle ou SnapManager para SAP para suspender as programações:
 - a. Se você quiser suspender as programações no host SnapManager para Oracle, execute:
 - `smo credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
 - `smo profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
 - `smo credential set -profile -name profile_name`



Você deve executar o comando smo Credential set para cada perfil no host.

b. Se você quiser suspender as programações no host SnapManager for SAP, execute:

- `smsap credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
- `smsap profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
- `smsap credential set -profile -name profile_name`



Você deve executar o comando `smsap Credential set` para cada perfil no host.

8. Certifique-se de que o nome de domínio totalmente qualificado (FQDN) do host do banco de dados seja exibido quando você executar `hostname -f`.

Se o FQDN não for exibido, você deverá modificar `/etc/hosts` para especificar o FQDN do host.

Importar dados

Você pode importar dados executando a ferramenta de importação do host do banco de dados.

Sobre esta tarefa

As políticas de backup do SnapCenter criadas após a importação têm diferentes formatos de nomenclatura:

- As políticas criadas para os perfis sem nenhuma operação e programação têm o formato `SM_PROFILENAME_online_full_DEFAULT_MIGRATED`.

Quando nenhuma operação é executada usando um perfil, a política correspondente é criada com o tipo de backup padrão como on-line e o escopo de backup como cheio.

- As políticas criadas para os perfis com uma ou mais operações têm o formato `SM_PROFILENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED`.
- As políticas criadas para as programações anexadas aos perfis têm o formato `SM_PROFILENAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED`.

Passos

1. Faça login no host do banco de dados que você deseja importar.
2. Execute a ferramenta de importação executando o script `SC-migrate` localizado em `/opt/NetApp/SnapCenter/spl/bin`.
3. Introduza o nome de utilizador e a palavra-passe do servidor SnapCenter.

Depois de validar as credenciais, uma conexão é estabelecida com o SnapCenter.

4. Insira os detalhes do banco de dados do repositório SnapManager para Oracle ou SnapManager para SAP.

O banco de dados do repositório lista os bancos de dados que estão disponíveis no host.

5. Introduza os detalhes da base de dados de destino.

Se você quiser importar todos os bancos de dados no host, insira todos.

6. Se você deseja gerar um log do sistema ou enviar mensagens ASUP para operações com falha, você deve ativá-las executando o comando *Add-SmStorageConnection* ou *set-SmStorageConnection*.



Se você quiser cancelar uma operação de importação, seja durante a execução da ferramenta de importação ou após a importação, exclua manualmente as políticas, credenciais e grupos de recursos do SnapCenter que foram criados como parte da operação de importação.

Resultados

As políticas de backup do SnapCenter são criadas para perfis, programações e operações executadas usando os perfis. Os grupos de recursos também são criados para cada banco de dados de destino.

Depois de importar os dados com êxito, as programações associadas ao banco de dados importado são suspensas no SnapManager para Oracle e no SnapManager para SAP.



Após a importação, você deve gerenciar o banco de dados importado ou o sistema de arquivos usando o SnapCenter.

Os logs para cada execução da ferramenta de importação são armazenados no diretório */var/opt/SnapCenter/spl/logs* com o nome *spl_migration_timestamp.log*. Você pode consultar este log para revisar erros de importação e solucioná-los.

Instale o plug-in do SnapCenter para VMware vSphere

Se seu banco de dados estiver armazenado em máquinas virtuais (VMs) ou se você quiser proteger VMs e datastores, será necessário implantar o plug-in do SnapCenter para o dispositivo virtual VMware vSphere.

Para obter informações sobre como implantar, ["Visão geral da implantação"](#) consulte .

Implantar certificado CA

Para configurar o certificado CA com o plug-in SnapCenter para VMware vSphere, ["Criar ou importar certificado SSL"](#) consulte .

Configure o arquivo CRL

O plug-in do SnapCenter para VMware vSphere procura os arquivos CRL em um diretório pré-configurado. O diretório padrão dos arquivos CRL para o plug-in do SnapCenter para VMware vSphere é */opt/NetApp/config/crl*.

Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

Prepare-se para proteger bancos de dados Oracle

Antes de executar qualquer operação de proteção de dados, como operações de backup, clone ou restauração, você precisa definir sua estratégia e configurar o

ambiente. Você também pode configurar o servidor SnapCenter para usar a tecnologia SnapMirror e SnapVault.

Para aproveitar as tecnologias SnapVault e SnapMirror, você deve configurar e inicializar uma relação de proteção de dados entre os volumes de origem e destino no dispositivo de armazenamento. Você pode usar o NetAppSystem Manager ou usar a linha de comando do console de armazenamento para executar essas tarefas.

Antes de usar o plug-in para banco de dados Oracle, o administrador do SnapCenter deve instalar e configurar o servidor SnapCenter e executar as tarefas de pré-requisito.

- Instalar e configurar o servidor SnapCenter. ["Saiba mais"](#)
- Configure o ambiente SnapCenter adicionando conexões do sistema de storage. ["Saiba mais"](#)



O SnapCenter não é compatível com vários SVMs com o mesmo nome em clusters diferentes. Cada SVM registrado no SnapCenter usando o Registro da SVM ou o Registro de cluster precisa ser único.

- Crie credenciais com o modo de autenticação como Linux ou AIX para o usuário de instalação. ["Saiba mais"](#)
- Adicione hosts, instale os plug-ins e descubra os recursos.
- Se você estiver usando o servidor SnapCenter para proteger bancos de dados Oracle que residem em LUNs ou VMDKs do VMware RDM, será necessário implantar o plug-in do SnapCenter para VMware vSphere e Registrar o plug-in com o SnapCenter.
- Instale o Java em seu host Linux ou AIX.

["Requisitos de host do Linux"](#) Consulte ou ["Requisitos do anfitrião de AIX"](#) para obter mais informações.

- Você deve definir o valor de tempo limite do firewall do aplicativo para 3 horas ou mais.
- Se você tiver bancos de dados Oracle em ambientes NFS, configure pelo menos um LIF de dados NFS para storage primário ou secundário para executar operações de montagem, clone, verificação e restauração.
- Se você tiver vários caminhos de dados (LIFs) ou uma configuração DNFS, você pode executar o seguinte usando a CLI do SnapCenter no host do banco de dados:
 - Por padrão, todos os endereços IP do host do banco de dados são adicionados à política de exportação de storage NFS na máquina virtual de armazenamento (SVM) para os volumes clonados. Se você quiser ter um endereço IP específico ou restringir a um subconjunto dos endereços IP, execute a CLI `Set-PreferredHostIPsInStorageExportPolicy`.
 - Se você tiver vários caminhos de dados (LIFs) na SVM, o SnapCenter escolherá o caminho de dados (LIF) apropriado para a montagem do volume clonado NFS. No entanto, se você quiser especificar um caminho de dados específico (LIF), você deve executar a CLI `Set-SvmPreferredDataPath`. O guia de referência do comando tem mais informações.
- Se você tiver bancos de dados Oracle em ambientes SAN, verifique se o ambiente SAN está configurado de acordo com a recomendação mencionada nos guias a seguir:
 - ["Configurações de host recomendadas para utilitários de host unificado do Linux"](#)
 - ["Uso de hosts Linux com storage ONTAP"](#)
 - ["Configurações do host afetadas pelos Utilitários de host AIX"](#)
- Se você tiver bancos de dados Oracle no LVM em sistemas operacionais Oracle Linux ou RHEL, instale a

versão mais recente do Logical volume Management (LVM).

- Se você estiver usando o SnapManager para Oracle e quiser migrar para o plug-in do SnapCenter para o banco de dados Oracle, é possível migrar os perfis para políticas e grupos de recursos do SnapCenter usando o comando `sccli SC-Migrate`.
- Configure o SnapMirror e o SnapVault no ONTAP, se você quiser replicação de backup

Para usuários do SnapCenter 4.1.1, a documentação do plug-in do SnapCenter para VMware vSphere 4.1.1 tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos. Para usuários do SnapCenter 4,2.x, o Agente de dados do NetApp 1,0 e 1,0.1, a documentação tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos usando o plug-in do SnapCenter para VMware vSphere fornecido pelo dispositivo virtual NetApp Data Broker baseado em Linux (formato Open Virtual Appliance). Para usuários do SnapCenter 4,3.x, a documentação do plug-in do SnapCenter para VMware vSphere 4,3 tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos usando o plug-in SnapCenter baseado no Linux para o dispositivo virtual VMware vSphere (formato Open Virtual Appliance).

Encontre mais informações

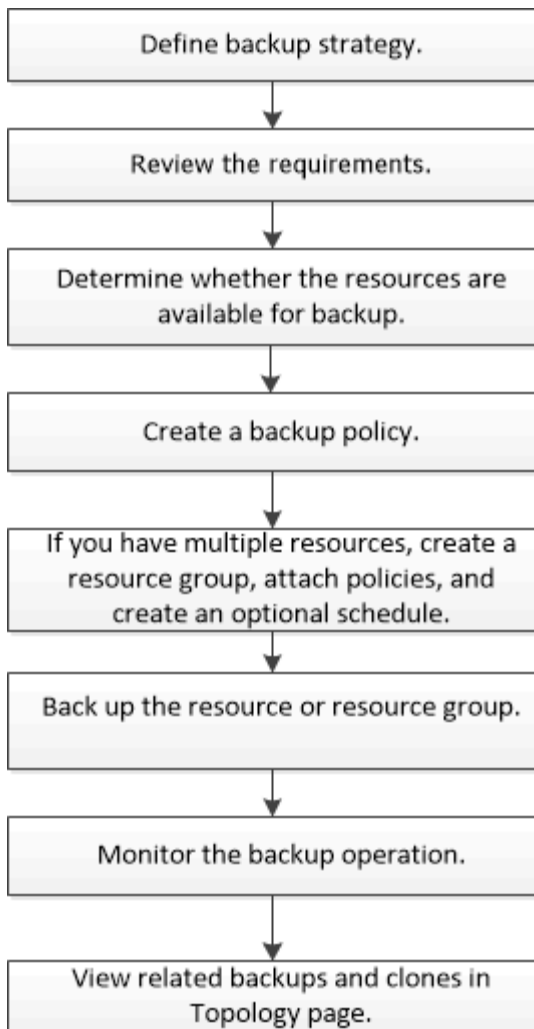
- ["Ferramenta de Matriz de interoperabilidade"](#)
- ["Plug-in do SnapCenter para documentação do VMware vSphere"](#)
- ["Falha na operação de proteção de dados em um ambiente não multipath no RHEL 7 e posterior"](#)

Faça backup de bancos de dados Oracle

Visão geral do procedimento de backup

Você pode criar um backup de um recurso (banco de dados) ou grupo de recursos. O procedimento de backup inclui Planejamento, identificação dos recursos para backup, criação de políticas de backup, criação de grupos de recursos e inclusão de políticas, criação de backups e monitoramento das operações.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de backup:



Ao criar um backup para bancos de dados Oracle, um arquivo de bloqueio operacional (*.SM_lock_dbsid*) é criado no host de banco de dados Oracle no diretório */var/opt/SnapCenter/SCO/lock* para evitar que várias operações sejam executadas no banco de dados. Após o backup do banco de dados, o arquivo de bloqueio operacional é removido automaticamente.

No entanto, se o backup anterior foi concluído com um aviso, o arquivo de bloqueio operacional pode não ser excluído e a próxima operação de backup entra na fila de espera. Ele pode eventualmente ser cancelado se o arquivo *.SM_lock_dbsid* não for excluído. Nesse cenário, você deve excluir manualmente o arquivo de bloqueio operacional executando as seguintes etapas:

1. No prompt de comando, navegue para */var/opt/SnapCenter/SCO/lock*.
2. Eliminar o bloqueio operacional: `rm -rf .sm_lock_dbsid`.

Informações de configuração de backup

Configurações de banco de dados Oracle compatíveis para backups

O SnapCenter suporta backup de diferentes configurações de banco de dados Oracle.

- Oracle Standalone
- Oracle Real Application clusters (RAC)

- Oracle Standalone Legacy
- Oracle Standalone Container Database (CDB)
- Espera do Oracle Data Guard

Você só pode criar backups de montagem offline de bancos de dados em espera do Data Guard. Backup off-line-shutdown, backup somente de log de arquivamento e backup completo não são suportados.

- Espera do Oracle ative Data Guard

Você só pode criar backups online de bancos de dados em espera do ative Data Guard. O backup e o backup completo somente de log de arquivamento não são suportados.

Antes de criar um backup do banco de dados de espera do Data Guard ou do ative Data Guard, o processo de recuperação gerenciado (MRP) é interrompido e, uma vez que o backup é criado, o MRP é iniciado.

- Gerenciamento automático de storage (ASM)
 - ASM autônomo e ASM RAC no Virtual Machine Disk (VMDK)

Entre todos os métodos de restauração suportados para bancos de dados Oracle, você pode executar apenas a restauração de conexão e cópia de bancos de dados ASM RAC no VMDK.

- ASM autônomo e ASM RAC em mapeamento de dispositivo bruto (RDM), você pode executar operações de backup, restauração e clone em bancos de dados Oracle no ASM, com ou sem ASMLib.
- Controlador de filtro Oracle ASM (ASMFD)

As operações de migração PDB e clonagem PDB não são suportadas.

- Oracle Flex ASM

Para obter as informações mais recentes sobre versões Oracle suportadas, consulte o "[Ferramenta de Matriz de interoperabilidade do NetApp](#)".

Tipos de backup suportados para bancos de dados Oracle

Tipo de backup especifica o tipo de backup que você deseja criar. O SnapCenter suporta tipos de backup on-line e off-line para bancos de dados Oracle.

Backup on-line

Um backup que é criado quando o banco de dados está no estado on-line é chamado de backup on-line. Também chamado de hot backup, um backup on-line permite que você crie um backup do banco de dados sem desligá-lo.

Como parte do backup on-line, você pode criar um backup dos seguintes arquivos:

- Arquivos de dados e arquivos de controle somente
- Arquivar apenas ficheiros de registo (a base de dados não é colocada no modo de cópia de segurança neste cenário)
- Banco de dados completo que inclui arquivos de dados, arquivos de controle e arquivos de log de arquivamento

Cópia de segurança offline

Um backup criado quando o banco de dados está em um estado montado ou desligado é chamado de backup off-line. Um backup off-line também é chamado de backup frio. Você pode incluir somente arquivos de dados e arquivos de controle em backups offline. Você pode criar um backup de montagem off-line ou de desligamento off-line.

- Ao criar um backup de montagem off-line, você deve garantir que o banco de dados esteja em um estado montado.

Se o banco de dados estiver em qualquer outro estado, a operação de backup falhará.

- Ao criar um backup de desligamento off-line, o banco de dados pode estar em qualquer estado.

O estado da base de dados é alterado para o estado necessário para criar uma cópia de segurança. Depois de criar a cópia de segurança, o estado da base de dados é revertido para o estado original.

Como o SnapCenter descobre bancos de dados Oracle

Os recursos são bancos de dados Oracle no host que são mantidos pelo SnapCenter. Você pode adicionar esses bancos de dados a grupos de recursos para executar operações de proteção de dados depois de descobrir os bancos de dados disponíveis.

As seções a seguir descrevem o processo que o SnapCenter usa para descobrir diferentes tipos e versões de bancos de dados Oracle.

Para versões Oracle 11g a 12cR1

Base de dados RAC

Os bancos de dados RAC são descobertos apenas com base nas entradas `/etc/oratab`. Você deve ter as entradas do banco de dados no arquivo `/etc/oratab`.

Autônomo

Os bancos de dados autônomos são descobertos apenas com base em entradas `/etc/oratab`.

ASM

A entrada de instância ASM deve estar disponível no arquivo `/etc/oratab`.

Nó RAC um

Os bancos de dados RAC One Node são descobertos apenas com base em entradas `/etc/oratab`. Os bancos de dados devem estar em `nomount`, `mount` ou em estado aberto. Você deve ter as entradas do banco de dados no arquivo `/etc/oratab`.

O status do banco de dados RAC One Node será marcado como renomeado ou excluído se o banco de dados já estiver descoberto e os backups estiverem associados ao banco de dados.

Você deve executar as seguintes etapas se o banco de dados for realocado:

1. Adicione manualmente a entrada do banco de dados realocada no arquivo `/etc/oratab` no nó RAC com falha.
2. Atualizar manualmente os recursos.
3. Selecione o banco de dados RAC One Node na página de recursos e clique em Configurações do banco

de dados.

4. Configure o banco de dados para definir os nós de cluster preferidos para o nó RAC que hospeda o banco de dados atualmente.
5. Execute as operações do SnapCenter.
6. Se você tiver relocado um banco de dados de um nó para outro nó e se a entrada do oratab no nó anterior não for excluída, exclua manualmente a entrada do oratab para evitar que o mesmo banco de dados seja exibido duas vezes.

Para versões Oracle 12cR2 a 18c

Base de dados RAC

Os bancos de dados RAC são descobertos usando o comando `srvctl config`. Você deve ter as entradas do banco de dados no arquivo `/etc/oratab`.

Autônomo

Os bancos de dados autônomos são descobertos com base nas entradas no arquivo `/etc/oratab` e na saída do comando `srvctl config`.

ASM

A entrada de instância ASM não precisa estar no arquivo `/etc/oratab`.

Nó RAC um

Os bancos de dados RAC One Node são descobertos usando apenas o comando `srvctl config`. Os bancos de dados devem estar em `nomount`, `mount` ou em estado aberto. O status do banco de dados RAC One Node será marcado como renomeado ou excluído se o banco de dados já estiver descoberto e os backups estiverem associados ao banco de dados.

Você deve executar as seguintes etapas se o banco de dados for realocado: . Atualizar manualmente os recursos. . Selecione o banco de dados RAC One Node na página de recursos e clique em Configurações do banco de dados. . Configure o banco de dados para definir os nós de cluster preferidos para o nó RAC que hospeda o banco de dados atualmente. . Execute as operações do SnapCenter.



Se houver alguma entrada de banco de dados Oracle 12cR2 e 18c_ no arquivo `/etc/oratab` e o mesmo banco de dados estiver registrado com o comando `srvctl config`, o SnapCenter eliminará as entradas duplicadas do banco de dados. Se houver entradas de banco de dados obsoletas, o banco de dados será descoberto, mas o banco de dados será inacessível e o status será `off-line`.

Nós preferenciais na configuração RAC

Na configuração RAC (Real Application clusters) do Oracle, você pode especificar os nós preferenciais que o SnapCenter usa para executar a operação de backup. Se você não especificar o nó preferido, o SnapCenter atribuirá automaticamente um nó como o nó preferido e o backup será criado nesse nó.

Os nós preferidos podem ser um ou todos os nós de cluster onde as instâncias de banco de dados RAC estão presentes. A operação de backup é acionada somente nesses nós preferenciais na ordem da preferência.

Exemplo

O banco de dados RAC `cdbrac` tem três instâncias: `cdbrac1` em `node1`, `cdbrac2` em `node2` e `cdbrac3` em `node3`.

As instâncias node1 e node2 são configuradas para serem os nós preferidos, com node2 como a primeira preferência e node1 como a segunda preferência. Quando você executa uma operação de backup, a operação é tentada pela primeira vez no node2 porque é o primeiro nó preferido.

Se o node2 não estiver no estado para fazer backup, o que pode ser devido a vários motivos, como o agente plug-in não está sendo executado no host, a instância do banco de dados no host não está no estado necessário para o tipo de backup especificado, ou a instância do banco de dados no node2 em uma configuração FlexASM não está sendo servida pela instância local ASM; então a operação será tentada no node1.

O node3 não será usado para backup porque não está na lista de nós preferenciais.

Configuração do Flex ASM

Em uma configuração do Flex ASM, os Leaf Nodes não serão listados como nós preferenciais se a cardinalidade for menor que os nós numéricos no cluster RAC. Se houver alguma alteração nas funções de nó de cluster do Flex ASM, você deverá descobrir manualmente para que os nós preferidos sejam atualizados.

Estado da base de dados necessário

As instâncias do banco de dados RAC nos nós preferenciais devem estar no estado necessário para que o backup seja concluído com êxito:

- Uma das instâncias do banco de dados RAC nos nós preferenciais configurados deve estar no estado aberto para criar um backup on-line.
- Uma das instâncias do banco de dados RAC nos nós preferenciais configurados deve estar no estado de montagem e todas as outras instâncias, incluindo outros nós preferenciais, devem estar no estado de montagem ou inferiores para criar um backup de montagem off-line.
- As instâncias de banco de dados RAC podem estar em qualquer estado, mas você deve especificar os nós preferenciais para criar um backup de desligamento off-line.

Como catalogar backups com o Oracle Recovery Manager

Você pode catalogar os backups de bancos de dados Oracle usando o Oracle Recovery Manager (RMAN) para armazenar as informações de backup no repositório Oracle RMAN.

Os backups catalogados podem ser usados posteriormente para restauração em nível de bloco ou operações de recuperação de ponto no tempo de tablespace. Quando você não precisa desses backups catalogados, você pode remover as informações do catálogo.

O banco de dados deve estar em estado montado ou superior para catalogação. Você pode fazer catalogação em backups de dados, backups de log de arquivamento e backups completos. Se a catalogação estiver ativada para um backup de um grupo de recursos que tenha vários bancos de dados, a catalogação é realizada para cada banco de dados. Para bancos de dados Oracle RAC, a catalogação será realizada no nó preferido onde o banco de dados está, pelo menos, no estado montado.

Se você quiser catalogar backups de um banco de dados RAC, verifique se nenhum outro trabalho está sendo executado para esse banco de dados. Se outro trabalho estiver em execução, a operação de catalogação falhará em vez de ficar na fila.

Banco de dados de catálogo externo

Por padrão, o arquivo de controle de banco de dados de destino é usado para catalogação. Se você quiser adicionar um banco de dados de catálogo externo, você pode configurá-lo especificando o nome do substrato de rede transparente (TNS) e credencial do catálogo externo usando o assistente Configurações de banco de dados da interface gráfica do usuário (GUI) do SnapCenter. Você também pode configurar o banco de dados de catálogo externo da CLI executando o comando `Configure-SmOracleDatabase` com as opções `-OracleRmanCatalogCredentialName` e `-OracleRmanCatalogTnsName`.

Comando RMAN

Se você ativou a opção catalogação ao criar uma política de backup Oracle a partir da GUI do SnapCenter, os backups serão catalogados usando o Oracle RMAN como parte da operação de backup. Você também pode executar a catalogação diferida de backups executando o `Catalog-SmBackupWithOracleRMAN` comando.

Depois de catalogar os backups, você pode executar o `Get-SmBackupDetails` comando para obter as informações de backup catalogadas, como a tag para datafiles catalogados, o caminho do catálogo do arquivo de controle e os locais de log do arquivo catalogado.

Formato de nomenclatura

Se o nome do grupo de discos ASM for maior ou igual a 16 caracteres, a partir do SnapCenter 3,0, o formato de nomenclatura usado para o backup é `SC_HASHCODEofDISKGROUP_DBSID_BACKUPID`. No entanto, se o nome do grupo de discos for inferior a 16 caracteres, o formato de nomenclatura usado para o backup é `DISKGROUPNAME_DBSID_BACKUPID`, que é o mesmo formato usado no SnapCenter 2,0.

O `HASHCODEofDISKGROUP` é um número gerado automaticamente (2 a 10 dígitos) exclusivo para cada grupo de discos ASM.

Operações de verificação cruzada

Você pode executar verificações cruzadas para atualizar informações do repositório RMAN desatualizadas sobre backups cujos Registros do repositório não correspondem ao seu status físico. Por exemplo, se um usuário remover logs arquivados do disco com um comando do sistema operacional, o arquivo de controle ainda indica que os logs estão no disco, quando na verdade eles não estão.

A operação de verificação cruzada permite-lhe atualizar o ficheiro de controlo com as informações. Você pode ativar a verificação cruzada executando o comando `Set-SmConfigSettings` e atribuindo o valor `TRUE` ao parâmetro `ENABLE_CROSSCHECK`. O valor padrão é definido como `FALSE`.

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings  
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

Remova as informações do catálogo

Você pode remover as informações do catálogo executando o comando `Uncatalog-SmBackupWithOracleRMAN`. Não é possível remover as informações do catálogo usando a GUI do SnapCenter. No entanto, as informações de um backup catalogado são removidas ao excluir o backup ou ao excluir o grupo de retenção e recursos associado ao backup catalogado.



Quando você força uma exclusão do host SnapCenter, as informações dos backups catalogados associados a esse host não são removidas. Você deve remover informações de todos os backups catalogados para esse host antes de forçar a exclusão do host.

Se a catalogação e a descatalogação falharem porque o tempo de operação excedeu o valor de tempo limite

especificado para o parâmetro ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT, você deve modificar o valor do parâmetro executando o seguinte comando:

```
/opt/Netapp/snapcenter/spl/bin/sccli Set-SmConfigSettings-ConfigSettingsType  
Plugin -PluginCode SCO-ConfigSettings  
"KEY=ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT,VALUE=user_defined_value"
```

Depois de modificar o valor do parâmetro, reinicie o serviço SnapCenter Plug-in Loader (SPL) executando o seguinte comando:

```
/opt/NetApp/snapcenter/spl/bin/spl restart
```

As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando get-Help command_name. Em alternativa, pode consultar a ["Guia de Referência de comandos do software SnapCenter"](#).

Variáveis de ambiente predefinidas para prescrição específica de backup e postscript

O SnapCenter permite-lhe utilizar as variáveis de ambiente predefinidas quando executa o prescritor e o postscript ao criar políticas de cópia de segurança. Essa funcionalidade é compatível com todas as configurações Oracle, exceto VMDK.

O SnapCenter predefine os valores dos parâmetros que serão diretamente acessíveis no ambiente onde os scripts shell são executados. Você não precisa especificar manualmente os valores desses parâmetros ao executar os scripts.

Variáveis de ambiente predefinidas suportadas para a criação de política de backup

- **SC_JOB_ID** especifica a ID da tarefa da operação.

Exemplo: 256

- **SC_ORACLE_SID** especifica o identificador do sistema do banco de dados.

Se a operação envolver vários bancos de dados, o parâmetro conterá nomes de banco de dados separados por pipe.

Esse parâmetro será preenchido para volumes de aplicativos.

Exemplo: NFSB32|NFSB31

- **SC_HOST** especifica o nome do host do banco de dados.

Para RAC, o nome do host será o nome do host no qual o backup é executado.

Esse parâmetro será preenchido para volumes de aplicativos.

Exemplo: scsmohost2.gdl.englabe.NetApp.com

- **SC_os_USER** especifica o proprietário do sistema operacional do banco de dados.

Os dados serão formatados como <db1> <osuser1>|<db2> <osuser2>.

Exemplo: NFSB31 em oracle|NFSB32 em oracle

- **SC_os_GROUP** especifica o grupo do sistema operacional do banco de dados.

Os dados serão formatados como <db1> <osgroup1>|<db2> <osgroup2>.

Exemplo: NFSB31 a instalar|NFSB32 a instalar

- **SC_BACKUP_TYPE** especifica o tipo de backup (dados on-line completos, on-line, log on-line, desligamento off-line, montagem off-line)

Exemplos:

- Para backup completo: ONLINEFULL
- Backup apenas de dados: ONLINEDATA
- Para backup somente de log: ONLINELOG

- **SC_BACKUP_NAME** especifica o nome do backup.

Esse parâmetro será preenchido para volumes de aplicativos.

Exemplo: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1|AV@RG2_scspr2417819002_07-20-2021_12.16.48.9267

- **SC_BACKUP_ID** especifica o ID de backup.

Esse parâmetro será preenchido para volumes de aplicativos.

EXEMPLO: DADOS EM 203|LOG EM 205|AV EM 207

- **SC_ORACLE_HOME** especifica o caminho do diretório inicial do Oracle.

Exemplo:

NFSB32/ora01/app/oracle/PRODUCT/18,1.0/dB_1|NFSB31at/ora01/app/oracle/PRODUCT/18,1.0/dB_1

- **SC_BACKUP_RETENSION** especifica o período de retenção definido na política.

Exemplos:

- Para backup completo: Por hora|DADOS em DIA:3|LOG em CONTAGEM:4
- Para backup apenas de dados sob demanda: OnDemand|DATA em CONTAGEM:2
- Para backup somente de log sob demanda: OnDemand|LOG at COUNT:2

- **SC_RESOURCE_GROUP_NAME** especifica o nome do grupo de recursos.

Exemplo: RG1

- **SC_BACKUP_POLICY_NAME** especifica o nome da política de backup.

Exemplo: Backup_policy

- **SC_AV_NAME** especifica os nomes dos volumes da aplicação.

Exemplo: AV1|AV2

- **SC_PRIMARY_DATA_VOLUME_full_PATH** especifica o mapeamento de armazenamento de SVM para o

diretório de arquivos de dados. Será o nome do volume pai para luns e qtrees.

Os dados serão formatados como <db1> <SVM1:volume1>|<db2> <SVM2:volume2>.

Exemplos:

- Para bancos de dados 2 no mesmo grupo de recursos: NFSB32 a
buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA|NFSB31 a
buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA
- Para um único banco de dados com arquivos de dados espalhados por vários volumes:
Buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA,herculus:/vol/scspr2417819002_NFS

- **SC_PRIMARY_ARCHIVELOGS_VOLUME_full_PATH** especifica o mapeamento de armazenamento de SVM para o volume para o diretório de arquivos de logs. Será o nome do volume pai para luns e qtrees.

Exemplos:

- Para uma única instância de banco de dados:
Buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO
- Para várias instâncias de banco de dados: NFSB31 a
buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO|NFSB32 a
buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO

- **SC_PRIMARY_full_SNAPSHOT_NAME_FOR_TAG** especifica a lista de instantâneos contendo nome do sistema de armazenamento e nome do volume.

Exemplos:

- Para uma única instância de banco de dados:
Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- Para várias instâncias de banco de dados: NFSB32 NFSB31 07 02.28.26.3973 NFSB31 07 02.28.26.3973 a buck:/vol/2021 NFSB31 RG2 21 0 RG2 21 1_NFS_CDB_02.28.26.3973 scspr2417819002 scspr2417819002 2021 scspr2417819002 scspr2417819002 2021_DATA/21_scspr2417819002_07-RG2-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/21_scspr2417819002_07_RG2_scspr2417819002_NFSB32_1

- **SC_PRIMARY_SNAPSHOT_NAMES** especifica os nomes dos snapshots primários criados durante o backup.

Exemplos:

- Para instância de banco de dados único: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- Para várias instâncias de banco de dados: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_0_1|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_02.28.26.3973,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- Para instantâneos de grupo de consistência que envolvem volumes: _R80404CBEF5V1_-05-2021_03.08.03.4945_2_cg3-28ad-465c-9d60-5487ac17b25d_2021_04_0_bfc279cc_8_58_350_4_5_3

- **SC_PRIMARY_MOUNT_POINTS** especifica os detalhes do ponto de montagem que fazem parte do backup.

Os detalhes incluem o diretório no qual os volumes são montados e não o pai imediato do arquivo em backup. Para uma configuração ASM, é o nome do grupo de discos.

Os dados serão formatados como <db1> <mountpoint1,mountpoint2>|<db2> <mountpoint1,mountpoint2>.

Exemplos:

- Para uma única instância de banco de dados: /Mnt/nfsdb3_data,/mnt/nfsdb3_log,/mnt/nfsdb3_data1
 - Para várias instâncias de banco de dados:
NFSB31at/mnt/nfsdb31_data,/mnt/nfsdb31_log,/mnt/nfsdb31_data1|NFSB32at/mnt/nfsdb32_data,/mnt/nfsdb32_log,/mnt/nfsdb32_data1
 - PARA ASM: DATA2DG, LOG2DG
- **SC_PRIMARY_SNAPSHOTS_AND_MOUNT_POINTS** especifica os nomes dos instantâneos criados durante o backup de cada um dos pontos de montagem.

Exemplos:

- Para uma única instância de banco de dados: RG2_scspr2417819002_07-2021-2021_02.28.26.3973_0:/mnt/nfsb32_data, RG2_scspr2417819002_07-21-21_02.28.26.3973_1:/mnt/nfsb31_log
 - Para várias instâncias de banco de dados: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_data, RG2_07_07-scspr2417819002-2021_RG2_0:/mnt/nfsb31_log|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_data, 02.28.26.3973_21_scspr2417819002-21-2021_02.28.26.3973_1:/mnt/nfsb32_log
- **SC_ARCHIVELOGS_LOCATIONS** especifica a localização do diretório de logs de arquivo.

Os nomes dos diretórios serão o pai imediato dos arquivos de log do arquivo. Se os registros de arquivo forem colocados em mais de um local, todos os locais serão capturados. Isso também inclui os cenários FRA. Se os softlinks forem usados para o diretório, o mesmo será preenchido.

Exemplos:

- Para um único banco de dados em NFS: /Mnt/nfsdb2_log
 - Para vários bancos de dados em NFS e para os logs de arquivo de banco de dados NFSB31 que são colocados em dois locais diferentes:
NFSB31at/mnt/nfsdb31_log1,/mnt/nfsdb31_log2|NFSB32at/mnt/nfsdb32_log
 - PARA ASM: LOG2DG/ASMDB2/ARCHIVELOG/2021_07_15
- **SC_REDO_LOGS_LOCATIONS** especifica a localização do diretório refazer logs.

Os nomes de diretório serão o pai imediato dos arquivos de log refazer. Se os softlinks forem usados para o diretório, o mesmo será preenchido.

Exemplos:

- Para um único banco de dados em NFS: /Mnt/nfsdb2_data/newdb1
 - Para vários bancos de dados em NFS: NFSB31 a/mnt/nfsdb31_data/newdb31|NFSB32 a/mnt/nfsdb32_data/newdb32
 - PARA ASM: LOG2DG/ASMDB2/ONLINELOG
- **SC_CONTROL_FILES_LOCATIONS** especifica a localização do diretório de arquivos de controle.

Os nomes dos diretórios serão o pai imediato dos arquivos de controle. Se os softlinks forem usados para o diretório, o mesmo será preenchido.

Exemplos:

- Para um único banco de dados em NFS: /Mnt/nfsdb2_data/fra/newdb1,/mnt/nfsdb2_data/newdb1
- Para vários bancos de dados em NFS: NFSB31
a/mnt/nfsdb31_data/fra/newdb31,/mnt/nfsdb31_data/newdb31|NFSB32
a/mnt/nfsdb32_data/fra/newdb32,/mnt/nfsdb32_data/newdb32
- PARA ASM: LOG2DG/ASMDB2/CONTROLFILE
- **SC_DATA_FILES_LOCATIONS** especifica a localização do diretório de arquivos de dados.

Os nomes dos diretórios serão o pai imediato dos arquivos de dados. Se os softlinks forem usados para o diretório, o mesmo será preenchido.

Exemplos:

- Para um único banco de dados em NFS: /Mnt/nfsdb3_data1,/mnt/nfsdb3_data/NEWDB3/datafile
- Para vários bancos de dados em NFS:
NFSB31at/mnt/nfsdb31_data1,/mnt/nfsdb31_data/NEWDB31/datafile|NFSB32at/mnt/nfsdb32_data1,/mnt/nfsdb32_data/NEWDB32/datafile
- PARA ASM: DATA2DG/ASMDB2/ARQUIVO DE DADOS, DATA2DG/ASMDB2/TEMPFILE
- **SC_SNAPSHOT_LABEL** especifica o nome dos rótulos secundários.

Exemplos: Etiqueta horária, diária, semanal, mensal ou personalizada.

Delimitadores suportados

- **:** é usado para separar o nome do SVM e o nome do volume

Exemplo: Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

- ***** é usado para separar os dados do nome do banco de dados e para separar o valor de sua chave.

Exemplos:

- A buck:/vol/_NFS_CDBDATA/
--1__02.28.26.3973,buck:/vol/scspr2417819002_NFS_CDB_2021_REDO/07_RG2_scspr2417819002_NFSB31_0_scspr2417819002_02.28.26.3973_21_07_RG2_2021_NFSB31_NFSB31_scspr2417819002_1_2021_scspr2417819002_02.28.26.3973_21_scspr2417819002_07_RG2_21_NFSB32_0_2021_02.28.26.3973_21_scspr2417819002_07_RG2_NFSB32_NFSB32_scspr2417819002
- NFSB31 de julho de NFSB32
- **|** é usado para separar os dados entre dois bancos de dados diferentes e para separar os dados entre duas entidades diferentes para os parâmetros SC_BACKUP_ID, SC_backup_RETENSION e SC_BACKUP_NAME.

Exemplos:

- DATA 203|LOG EM 205

- HORA|DADOS EM 3|LOG EM 4

- DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1

- / é usado para separar o nome do volume do Snapshot para os parâmetros SC_PRIMARY_SNAPSHOT_NAMES e SC_PRIMARY_full_snapshot_NAME_FOR_TAG.

Exemplo: NFSB32 a buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-20-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/21_scspr2417819002_07-21-2021_02.28.26.3973_1

- , é usado para separar o conjunto de variáveis para o mesmo banco de dados.

Exemplo: A buck:/vol/_NFS_CDBDATA/--
,buck:/vol/_NFS_CDBREDO/_2021_02.28.26.3973_1_scspr2417819002_07|21 buck
a:/vol/scspr2417819002_NFS_CDB_NFSB31_RG2_0_2021_02.28.26.3973_07_21_scspr2417819002_NFSB31_1_RG2_scspr2417819002_NFSB31_02.28.26.3973_07_21_RG2_2021_NFSB32_0_scspr2417819002_02.28.26.3973_21_scspr2417819002_07_RG2_2021_NFSB32_NFSB32_scspr2417819002_scspr2417819002

Opções de retenção de backup

Você pode escolher o número de dias para os quais reter cópias de backup ou especificar o número de cópias de backup que deseja reter, até um máximo de ONTAP de 255 cópias. Por exemplo, sua organização pode exigir que você retenha 10 dias de cópias de backup ou 130 cópias de backup.

Ao criar uma política, você pode especificar as opções de retenção para o tipo de backup e o tipo de agendamento.

Se você configurar a replicação do SnapMirror, a política de retenção será espelhada no volume de destino.

O SnapCenter exclui os backups retidos que têm rótulos de retenção que correspondem ao tipo de agendamento. Se o tipo de agendamento tiver sido alterado para o grupo de recursos ou recursos, os backups com o rótulo de tipo de agendamento antigo ainda poderão permanecer no sistema.



Para retenção de longo prazo de cópias de backup, você deve usar o backup SnapVault.

Fazer backup de programações

A frequência de backup (tipo de agendamento) é especificada em políticas; uma programação de backup é especificada na configuração do grupo de recursos. O fator mais crítico na determinação de uma frequência ou programação de backup é a taxa de alteração do recurso e a importância dos dados. Você pode fazer backup de um recurso muito usado a cada hora, enquanto você pode fazer backup de um recurso raramente usado uma vez por dia. Outros fatores incluem a importância do recurso para a sua organização, seu Contrato de nível de Serviço (SLA) e seu objetivo de ponto de recuperação (RPO).

Um SLA define o nível de serviço esperado e aborda muitos problemas relacionados ao serviço, incluindo a

disponibilidade e o desempenho do serviço. Um RPO define a estratégia para a era dos arquivos que precisam ser recuperados do storage de backup para que as operações regulares sejam retomadas após uma falha. O SLA e o RPO contribuem para a estratégia de proteção de dados.

Mesmo para um recurso muito usado, não é necessário executar um backup completo mais de uma ou duas vezes por dia. Por exemplo, backups regulares de log de transações podem ser suficientes para garantir que você tenha os backups necessários. Quanto mais você fizer backup de seus bancos de dados, menos Registros de transações que o SnapCenter precisa usar no momento da restauração, o que pode resultar em operações de restauração mais rápidas.

Os programas de backup têm duas partes, como segue:

- Frequência de backup

A frequência de backup (com que frequência os backups devem ser executados), chamada *schedule type* para alguns plug-ins, faz parte de uma configuração de política. Você pode selecionar a frequência de backup da política por hora, dia, semanal ou mensal. Se você não selecionar nenhuma dessas frequências, a política criada será uma política somente sob demanda. Você pode acessar políticas clicando em **Configurações > políticas**.

- Fazer backup de programações

As agendas de backup (exatamente quando os backups devem ser executados) fazem parte de uma configuração de grupo de recursos. Por exemplo, se você tiver um grupo de recursos que tenha uma política configurada para backups semanais, poderá configurar a programação para fazer backup todas as quintas-feiras às 10:00 horas. Você pode acessar programações de grupos de recursos clicando em **recursos > grupos de recursos**.

Convenções de nomenclatura de backup

Você pode usar a convenção de nomenclatura de cópia Snapshot padrão ou usar uma convenção de nomenclatura personalizada. A convenção de nomenclatura de backup padrão adiciona um carimbo de data/hora aos nomes de cópia Snapshot que o ajuda a identificar quando as cópias foram criadas.

A cópia Snapshot usa a seguinte convenção de nomenclatura padrão:

```
resourcegroupname_hostname_timestamp
```

Você deve nomear seus grupos de recursos de backup logicamente, como no exemplo a seguir:

```
dts1_mach1x88_03-12-2015_23.17.26
```

Neste exemplo, os elementos de sintaxe têm os seguintes significados:

- *dts1* é o nome do grupo de recursos.
- *mach1x88* é o nome do host.
- *03-12-2015_23.17.26* é a data e o carimbo de data/hora.

Como alternativa, você pode especificar o formato do nome da cópia Snapshot enquanto protege recursos ou grupos de recursos selecionando **usar formato de nome personalizado para cópia Snapshot**. Por exemplo,

customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, o sufixo do carimbo de hora é adicionado ao nome da cópia Instantânea.

Requisitos para fazer backup de um banco de dados Oracle

Antes de fazer backup de um banco de dados Oracle, você deve garantir que os pré-requisitos sejam concluídos.

- Você deve ter criado um grupo de recursos com uma política anexada.
- Se você quiser fazer backup de um recurso que tenha uma relação SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário de armazenamento deve incluir o privilégio "SnapMirror All". No entanto, se você estiver usando a função "vsadmin", o privilégio "SnapMirror all" não será necessário.
- Você deve ter atribuído o agregado que está sendo usado pela operação de backup à máquina virtual de storage (SVM) usada pelo banco de dados.
- Você deve ter verificado que todos os volumes de dados e volumes de log de arquivamento pertencentes ao banco de dados estão protegidos se a proteção secundária estiver ativada para esse banco de dados.
- Você deve ter verificado que o banco de dados que tem arquivos nos grupos de discos ASM deve estar no estado "MOUNT" ou "OPEN" para verificar seus backups usando o utilitário Oracle DBVERIFY.
- Você deve ter verificado que o comprimento do ponto de montagem do volume não excede 240 caracteres.
- Você deve aumentar o valor de RESTTimeout para 86400000 ms no arquivo _C: Arquivos de programas/NetApp no host do servidor SnapCenter, se o banco de dados que está sendo feito backup for grande (tamanho em TBs).

Ao modificar os valores, certifique-se de que não existem trabalhos em execução e reinicie o serviço SnapCenter SMCores depois de aumentar o valor.

Descubra os bancos de dados Oracle disponíveis para backup

Os recursos são bancos de dados Oracle no host que são gerenciados pelo SnapCenter. Você pode adicionar esses bancos de dados a grupos de recursos para executar operações de proteção de dados depois de descobrir os bancos de dados disponíveis.

O que você vai precisar

- Você deve ter concluído tarefas como instalar o servidor SnapCenter, adicionar hosts, criar conexões do sistema de storage e adicionar credenciais.
- Se os bancos de dados residirem em um disco de máquina virtual (VMDK) ou mapeamento de dispositivo bruto (RDM), você deverá implantar o plug-in do SnapCenter para VMware vSphere e Registrar o plug-in com o SnapCenter.

Para obter mais informações, ["Implante o plug-in do SnapCenter para VMware vSphere"](#) consulte .

- Se os bancos de dados residirem em um sistema de arquivos VMDK, você deve ter feito login no vCenter e navegado para **opções de VM > Avançado > Editar configuração** para definir o valor de *disk.enableUUID* como verdadeiro para a VM.
- Você deve ter revisado o processo que o SnapCenter segue para descobrir diferentes tipos e versões de bancos de dados Oracle.

Passo 1: Impedir que o SnapCenter descubra entradas que não sejam do banco de dados

Você pode impedir que o SnapCenter descubra entradas não-banco de dados adicionadas no arquivo `oratab`.

Passos

1. Depois de instalar o plug-in para Oracle, o usuário root deve criar o arquivo **SC_oratab.config** sob o diretório `/var/opt/SnapCenter/SCO/etc/`.

Conceda a permissão de gravação ao proprietário e grupo binários Oracle para que o arquivo possa ser mantido no futuro.

2. O administrador do banco de dados deve adicionar as entradas não-banco de dados no arquivo **SC_oratab.config**.

Recomenda-se manter o mesmo formato definido para as entradas não-banco de dados no arquivo `/etc/oratab` ou o usuário pode simplesmente adicionar a string de entidade não-banco de dados.



A cadeia é sensível a maiúsculas e minúsculas. Qualquer texto com número no início é tratado como um comentário. O comentário pode ser anexado após o nome não-banco de dados.

```
For example:
-----
# Sample entries
# Each line can have only one non-database name
# These are non-database name
oratar # Added by the admin group -1
#Added by the script team
NEWSPT
DBAGNT:/ora01/app/oracle/product/agent:N
-----
```

3. Descubra os recursos.

As entradas não-banco de dados adicionadas no **SC_oratab.config** não serão listadas na página recursos.



É sempre recomendável fazer um backup do arquivo `SC_oratab.config` antes de atualizar o plug-in SnapCenter.

Passo 2: Descubra recursos

Depois de instalar o plug-in, todos os bancos de dados nesse host são automaticamente descobertos e exibidos na página recursos.

Os bancos de dados devem estar pelo menos no estado montado ou acima para que a descoberta dos bancos de dados seja bem-sucedida. Em um ambiente do Oracle Real Application clusters (RAC), a instância do banco de dados RAC no host onde a descoberta é executada deve estar pelo menos no estado montado ou acima para que a descoberta da instância do banco de dados seja bem-sucedida. Somente os bancos de

dados que são descobertos com êxito podem ser adicionados aos grupos de recursos.

Se você tiver excluído um banco de dados Oracle no host, o servidor SnapCenter não estará ciente e listará o banco de dados excluído. Você deve atualizar manualmente os recursos para atualizar a lista de recursos do SnapCenter.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** na lista **Exibir**.

Clique  em e selecione o nome do host e o tipo de banco de dados para filtrar os recursos. Em seguida, clique no  ícone para fechar o painel de filtro.

3. Clique em **Atualizar recursos**.

Em um cenário RAC One Node, o banco de dados é descoberto como o banco de dados RAC no nó onde está hospedado atualmente.

Resultados

Os bancos de dados são exibidos juntamente com informações como tipo de banco de dados, nome de host ou cluster, grupos e políticas de recursos associados e status.



Você deve atualizar os recursos se os bancos de dados forem renomeados fora do SnapCenter.

- Se o banco de dados estiver em um sistema de armazenamento que não seja NetApp, a interface do usuário exibirá uma mensagem não disponível para backup na coluna Status geral.

Você não pode executar operações de proteção de dados no banco de dados que está em um sistema de storage que não é NetApp.

- Se o banco de dados estiver em um sistema de armazenamento NetApp e não estiver protegido, a interface do usuário exibirá uma mensagem não protegida na coluna Estado geral.
- Se o banco de dados estiver em um sistema de armazenamento NetApp e protegido, a interface do usuário exibirá uma mensagem disponível para backup na coluna Status geral.



Se você tiver habilitado uma autenticação de banco de dados Oracle, um ícone de cadeado vermelho será exibido na exibição recursos. Você deve configurar credenciais de banco de dados para poder proteger o banco de dados ou adicioná-lo ao grupo de recursos para executar operações de proteção de dados.

Criar políticas de backup para bancos de dados Oracle

Antes de usar o SnapCenter para fazer backup dos recursos do banco de dados Oracle, você deve criar uma política de backup para o recurso ou para o grupo de recursos que deseja fazer backup. Uma política de backup é um conjunto de regras que regem como você gerencia, agenda e retém backups. Você também pode especificar as configurações de replicação, script e tipo de backup. A criação de uma política economiza tempo quando você deseja reutilizar a política em outro recurso ou grupo de recursos.

Antes de começar

- Você precisa ter definido sua estratégia de backup.
- Você precisa se preparar para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, descobrir bancos de dados e criar conexões do sistema de storage.
- Se você estiver replicando cópias Snapshot em um storage secundário de espelhamento ou cofre, o administrador do SnapCenter precisará atribuir as SVMs a você para os volumes de origem e destino.
- Se tiver instalado o plug-in como um utilizador não root, deve atribuir manualmente as permissões de execução aos diretórios prescriitor e postscript.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **políticas**.
3. Selecione **Oracle Database** na lista suspensa.
4. Clique em **novo**.
5. Na página Nome, insira o nome e a descrição da política.
6. Na página tipo de backup, execute as seguintes etapas:

- Se pretender **criar uma cópia de segurança online**, selecione **cópia de segurança online**.

Você deve especificar se deseja fazer backup de todos os arquivos de dados, arquivos de controle e arquivos de log de arquivamento, somente arquivos de dados e arquivos de controle ou somente arquivos de log de arquivamento.

- Se pretender **criar uma cópia de segurança offline**, selecione **cópia de segurança offline** e, em seguida, selecione uma das seguintes opções:

- Se você quiser criar um backup off-line quando o banco de dados estiver no estado montado, selecione **montar**.
- Se pretender criar uma cópia de segurança de encerramento offline alterando a base de dados para o estado de encerramento, selecione **Encerrar**.

Se você estiver tendo bancos de dados conetáveis (PDBs) e quiser salvar o estado das PDBs antes de criar o backup, selecione **Salvar estado das PDBs**. Isso permite que você traga as PDBs ao seu estado original após a criação do backup.

- Especifique a frequência da programação selecionando **on demand**, **Hourly**, **Daily**, **Weekly** ou **Monthly**.



Você pode especificar a programação (data de início e data de término) para a operação de backup enquanto cria um grupo de recursos. Isso permite que você crie grupos de recursos que compartilham a mesma política e frequência de backup, mas permite que você atribua diferentes programações de backup a cada política.



Se você tiver agendado para as 2:00 da manhã, o horário não será acionado durante o horário de verão (DST).

- Se você quiser catalogar o backup usando o Oracle Recovery Manager (RMAN), selecione **Catálogo de backup com o Oracle Recovery Manager (RMAN)**.

Você pode executar catalogação diferida para um backup de cada vez usando a GUI ou usando o comando SnapCenter CLI `Catalog-SmBackupWithOracleRMAN`.



Se você quiser catalogar backups de um banco de dados RAC, verifique se nenhum outro trabalho está sendo executado para esse banco de dados. Se outro trabalho estiver em execução, a operação de catalogação falhará em vez de ficar na fila.

- Se você quiser podar logs de arquivo após o backup, selecione **Prune archive logs after backup**.



A eliminação dos registros de arquivo do destino do registro de arquivo que não está configurado na base de dados será ignorada.



Se você estiver usando o Oracle Standard Edition, você pode usar os parâmetros `LOG_ARCHIVE_DEST` e `LOG_ARCHIVE_DUPLEX_DEST` ao executar o backup do log de arquivamento.

- Só pode eliminar registros de arquivo se tiver selecionado os ficheiros de registo de arquivo como parte da cópia de segurança.



Você deve garantir que todos os nós em um ambiente RAC possam acessar todos os locais de log de arquivamento para que a operação de exclusão seja bem-sucedida.

Se você quiser...	Então...
Eliminar todos os registros de arquivo	Selecione Eliminar todos os registros de arquivo .
Excluir Registros de arquivamento que são mais antigos	Selecione Eliminar registros de arquivo mais antigos que e, em seguida, especifique a idade dos registros de arquivo a eliminar em dias e horas.
Eliminar registros de arquivo de todos os destinos	Selecione Eliminar registros de arquivo de todos os destinos .
Elimine os registros de arquivo dos destinos de registo que fazem parte da cópia de segurança	Selecione Eliminar registros de arquivo a partir dos destinos que fazem parte da cópia de segurança .

☒ Prune archive logs after backup

Prune log retention setting

☐ Delete all archive logs

☒ Delete archive logs older than

Prune log destination setting

☐ Delete archive logs from all the destinations

+ ☒ Delete archive logs from the destinations which are part of backup

7. Na página retenção, especifique as configurações de retenção para o tipo de backup e o tipo de

agendamento selecionado na página tipo de backup:

Se você quiser...	Então...
Mantenha um certo número de cópias Snapshot	Selecione Total de cópias snapshot a serem mantidas e especifique o número de cópias snapshot que você deseja manter. Se o número de cópias Snapshot exceder o número especificado, as cópias snapshot serão excluídas com as cópias mais antigas excluídas primeiro.  O valor máximo de retenção é 1018 para recursos no ONTAP 9.4 ou posterior e 254 para recursos no ONTAP 9.3 ou anterior. Os backups falharão se a retenção for definida para um valor maior do que o que a versão subjacente do ONTAP suporta.  Você deve definir a contagem de retenção como 2 ou superior, se quiser habilitar a replicação do SnapVault. Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque a primeira cópia Snapshot é a cópia Snapshot de referência para a relação SnapVault até que uma cópia Snapshot mais recente seja replicada para o destino.
Mantenha as cópias Snapshot por um determinado número de dias	Selecione manter cópias Snapshot para e especifique o número de dias para os quais deseja manter as cópias Snapshot antes de excluí-las.



Você pode reter backups de log de arquivamento somente se tiver selecionado os arquivos de log de arquivamento como parte do backup.

8. Na página replicação, especifique as configurações de replicação:

Para este campo...	Faça isso...
Atualize o SnapMirror depois de criar uma cópia Snapshot local	Selecione este campo para criar cópias espelhadas dos conjuntos de backup em outro volume (replicação SnapMirror).
Atualize o SnapVault depois de criar uma cópia Snapshot local	Selecione esta opção para executar a replicação de backup disco a disco (backups SnapVault).

Para este campo...	Faça isso...
Etiqueta de política secundária	Selecione uma etiqueta Snapshot. Dependendo do rótulo da cópia Snapshot selecionado, o ONTAP aplica a política de retenção da cópia snapshot secundária que corresponde ao rótulo.  Se você selecionou Atualizar SnapMirror depois de criar uma cópia Snapshot local, você pode especificar opcionalmente o rótulo de política secundária. No entanto, se você selecionou Atualizar SnapVault depois de criar uma cópia Snapshot local, especifique o rótulo de política secundária.
Contagem de tentativas de erro	Introduza o número máximo de tentativas de replicação que podem ser permitidas antes de a operação parar.



Você deve configurar a política de retenção do SnapMirror no ONTAP para o storage secundário para evitar alcançar o limite máximo de cópias Snapshot no storage secundário.

9. Na página Script, insira o caminho e os argumentos do prescritor ou postscript que você deseja executar antes ou depois da operação de backup, respetivamente.

Você deve armazenar os prescripts e postscripts em `/var/opt/SnapCenter/spl/scripts` ou em qualquer pasta dentro deste caminho. Por padrão, o caminho `/var/opt/SnapCenter/spl/scripts` é preenchido. Se você criou qualquer pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.

Você também pode especificar o valor de tempo limite do script. O valor padrão é de 60 segundos.

O SnapCenter permite-lhe utilizar as variáveis de ambiente predefinidas quando executa o prescritor e o postscript. ["Saiba mais"](#)

10. Na página Verificação, execute as seguintes etapas:

- a. Selecione o agendamento de backup para o qual você deseja executar a operação de verificação.
- b. Na seção comandos do script de verificação, insira o caminho e os argumentos do prescritor ou postscript que você deseja executar antes ou depois da operação de verificação, respetivamente.

Você deve armazenar os prescripts e postscripts em `/var/opt/SnapCenter/spl/scripts` ou em qualquer pasta dentro deste caminho. Por padrão, o caminho `/var/opt/SnapCenter/spl/scripts` é preenchido. Se você criou qualquer pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.

Você também pode especificar o valor de tempo limite do script. O valor padrão é de 60 segundos.

11. Revise o resumo e clique em **Finish**.

Crie grupos de recursos e anexe políticas para bancos de dados Oracle

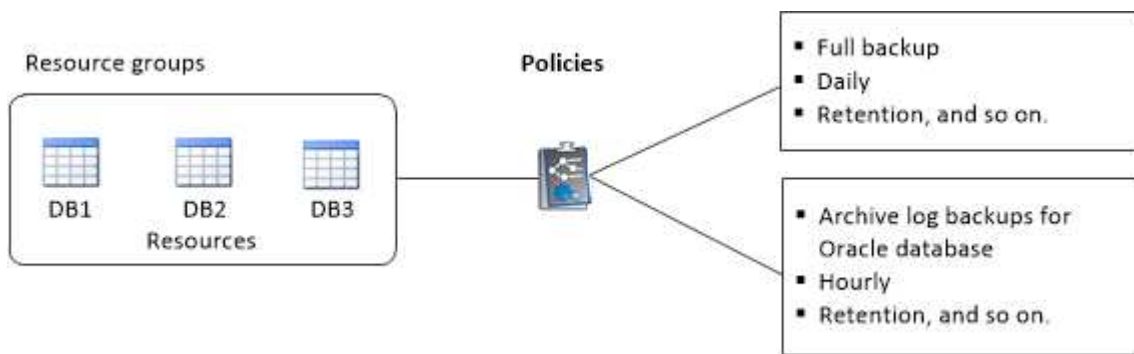
Um grupo de recursos é um contentor onde você adiciona recursos que deseja fazer backup e proteger. Um grupo de recursos permite fazer backup de todos os dados associados a um determinado aplicativo simultaneamente.

Sobre esta tarefa

Um banco de dados com arquivos em grupos de discos ASM deve estar no estado "MOUNT" ou "OPEN" para verificar seus backups usando o utilitário Oracle DBVERIFY.

Anexe uma ou mais políticas ao grupo de recursos para definir o tipo de tarefa de proteção de dados que deseja executar.

A imagem a seguir ilustra a relação entre recursos, grupos de recursos e políticas para bancos de dados:



Passos

1. No painel de navegação esquerdo, selecione **Resources** e o plug-in apropriado na lista.
2. Na página recursos, clique em **novo Grupo de recursos**.
3. Na página Nome, execute as seguintes ações:
 - a. Introduza um nome para o grupo de recursos no campo Nome.



O nome do grupo de recursos não deve exceder 250 caracteres.

- b. Insira um ou mais rótulos no campo Tag para ajudá-lo a pesquisar o grupo de recursos mais tarde.

Por exemplo, se você adicionar HR como uma tag a vários grupos de recursos, poderá encontrar mais tarde todos os grupos de recursos associados à tag HR.

- c. Marque essa caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome da cópia Instantânea.

Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um carimbo de data/hora é anexado ao nome da cópia Snapshot.

- d. Especifique os destinos dos ficheiros de registo de arquivo que não pretende efetuar uma cópia de segurança.

4. Na página recursos, selecione um nome de host de banco de dados Oracle na lista suspensa **Host**.



Os recursos são listados na seção recursos disponíveis somente se o recurso for descoberto com êxito. Se você tiver adicionado recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois de atualizar sua lista de recursos.

5. Selecione os recursos na seção recursos disponíveis e mova-os para a seção recursos selecionados.



Você pode adicionar bancos de dados de hosts Linux e AIX em um único grupo de recursos.

6. Na página políticas, execute as seguintes etapas:

a. Selecione uma ou mais políticas na lista suspensa.



Você também pode criar uma política clicando  em .

Na seção Configurar agendas para políticas selecionadas, as políticas selecionadas são listadas.

b. Clique  na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.

c. Na janela Adicionar programações para a política *policy_name*, configure a programação e clique em **OK**.

Onde, *policy_name* é o nome da política selecionada.

As programações configuradas são listadas na coluna agendas aplicadas.

As agendas de backup de terceiros não são suportadas quando sobrepõem-se às agendas de backup do SnapCenter.

7. Na página Verificação, execute as seguintes etapas:

a. Clique em **carregar localizadores** para carregar os volumes SnapMirror ou SnapVault para executar a verificação no armazenamento secundário.

b. Clique  na coluna Configurar agendas para configurar o agendamento de verificação para todos os tipos de agendamento da política.

c. Na caixa de diálogo Adicionar agendamentos de verificação *policy_name* , execute as seguintes ações:

Se você quiser...	Faça isso...
Execute a verificação após a cópia de segurança	Selecione Executar verificação após backup .
Marque uma verificação	Selecione Executar verificação agendada e, em seguida, selecione o tipo de agendamento na lista suspensa.

d. Selecione **verificar no local secundário** para verificar os backups no sistema de armazenamento secundário.

e. Clique em **OK**.

As programações de verificação configuradas são listadas na coluna agendas aplicadas.

8. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. Se quiser anexar o relatório da operação realizada no grupo de recursos, selecione **Anexar Relatório de trabalho**.



Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando PowerShell SET-SmtpServer.

9. Revise o resumo e clique em **Finish**.

Faça backup dos recursos Oracle

Se um recurso não fizer parte de qualquer grupo de recursos, você poderá fazer backup do recurso na página recursos.

Passos

1. No painel de navegação esquerdo, selecione **Resources** e o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** na lista Exibir.
3. Clique  em e selecione o nome do host e o tipo de banco de dados para filtrar os recursos.

Em seguida, pode clicar  para fechar o painel de filtro.

4. Selecione o banco de dados que deseja fazer backup.

A página Database-Protect (proteção de banco de dados) é exibida.

5. Na página recursos, você pode executar as seguintes etapas:
 - a. Marque a caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome da cópia Instantânea.

Por exemplo, `customtext_policy_hostname` ou `resource_hostname`. Por padrão, um carimbo de data/hora é anexado ao nome da cópia Snapshot.
 - b. Especifique os destinos dos ficheiros de registo de arquivo que não pretende efetuar uma cópia de segurança.
6. Na página políticas, execute as seguintes etapas:
 - a. Selecione uma ou mais políticas na lista suspensa.



Você pode criar uma política clicando  em .

Na seção Configurar agendas para políticas selecionadas, as políticas selecionadas são listadas.

- b. Clique  na coluna Configurar agendas para configurar uma agenda para a política desejada.

- c. Na janela Adicionar agendas para a política *policy_name* , configure a programação e **OK** selecione .

policy_name é o nome da política selecionada.

As programações configuradas são listadas na coluna agendas aplicadas.

7. Na página Verificação, execute as seguintes etapas:

- a. Clique em **Load Locators** para carregar os volumes SnapMirror ou SnapVault para verificar o armazenamento secundário.
- b. Clique  na coluna Configurar agendas para configurar o agendamento de verificação para todos os tipos de agendamento da política. Na caixa de diálogo Adicionar agendas de verificação *policy_name*, você pode executar as seguintes etapas:
- c. Selecione **Executar verificação após backup**.
- d. Selecione **Executar verificação agendada** e selecione o tipo de agendamento na lista suspensa.



Em uma configuração do Flex ASM, você não pode executar a operação de verificação em Leaf Nodes se a cardinalidade for menor que os nós numéricos no cluster RAC.

- e. Selecione **verificar no local secundário** para verificar os backups no armazenamento secundário.
- f. Clique em **OK**.

As programações de verificação configuradas são listadas na coluna agendas aplicadas.

8. Na página notificação, selecione os cenários em que você deseja enviar os e-mails da lista suspensa **preferência de e-mail**.

Você deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. Se quiser anexar o relatório da operação de backup realizada no recurso, selecione **Anexar Relatório de trabalho**.



Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando o comando GUI ou PowerShell `Set-SmSmtServer` .

9. Revise o resumo e clique em **Finish**.

A página de topologia do banco de dados é exibida.

10. Clique em **fazer backup agora**.

11. Na página Backup, execute as seguintes etapas:

- a. Se você tiver aplicado várias políticas ao recurso, na lista suspensa Política, selecione a política que deseja usar para backup.

Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

- b. Clique em **Backup**.

12. Monitorize o progresso da operação clicando em **Monitor > trabalhos**.

Depois de terminar

- Na configuração do AIX, você pode usar o `lkdev` comando para bloquear e o `rendev` comando para renomear os discos nos quais o banco de dados que foi feito backup residia.

Bloquear ou renomear dispositivos não afetará a operação de restauração quando você restaurar usando esse backup.

- Se a operação de backup falhar porque o tempo de execução da consulta do banco de dados excedeu o valor de tempo limite, você deve alterar o valor dos parâmetros `ORACLE_SQL_QUERY_TIMEOUT` e `ORACLE_PLUGIN_SQL_QUERY_TIMEOUT` executando `Set-SmConfigSettings` o `cmdlet`:

Depois de modificar o valor dos parâmetros, reinicie o serviço SnapCenter Plug-in Loader (SPL) executando o seguinte comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Se o arquivo não estiver acessível e o ponto de montagem não estiver disponível durante o processo de verificação, a operação pode falhar com o código de erro DBV-00100 arquivo especificado. Você deve modificar os valores dos parâmetros `VERIFICATION_DELAY` e `VERIFICATION_RETRY_COUNT` em `sco.properties`.

Depois de modificar o valor dos parâmetros, reinicie o serviço SnapCenter Plug-in Loader (SPL) executando o seguinte comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Nas configurações do MetroCluster, o SnapCenter pode não ser capaz de detectar uma relação de proteção após um failover.
- Se você estiver fazendo backup de dados de aplicativos em VMDKs e o tamanho de heap Java para o plug-in SnapCenter para VMware vSphere não for grande o suficiente, o backup pode falhar.

Para aumentar o tamanho do heap Java, localize o arquivo de script `/opt/NetApp/init_scripts/scvservice`. Nesse script, o `do_start method` comando inicia o serviço de plug-in SnapCenter VMware. Atualize esse comando para o seguinte: `Java -jar -Xmx8192M -Xms4096M`.

Encontre mais informações

- ["Não é possível detectar a relação SnapMirror ou SnapVault após o failover do MetroCluster"](#)
- ["O banco de dados Oracle RAC One Node é ignorado para a execução das operações do SnapCenter"](#)
- ["Falha ao alterar o estado de um banco de dados Oracle 12c ASM"](#)
- ["Parâmetros personalizáveis para operações de backup, restauração e clone em sistemas AIX"](#) (Requer login)

Faça backup de grupos de recursos de banco de dados Oracle

Um grupo de recursos é uma coleção de recursos em um host ou cluster. A operação de backup é realizada em todos os recursos definidos no grupo de recursos.

Você pode fazer backup de um grupo de recursos sob demanda na página recursos. Se um grupo de recursos tiver uma política anexada e uma programação configurada, os backups serão criados de acordo com a programação.

Passos

1. No painel de navegação esquerdo, selecione **Resources** e o plug-in apropriado na lista.
2. Na página recursos, selecione **Grupo de recursos** na lista **Exibir**.

3. Digite o nome do grupo de recursos na caixa de pesquisa ou clique  em e selecione a tag.

Clique  em para fechar o painel de filtro.

4. Na página Grupo de recursos, selecione o grupo de recursos para fazer backup.



Se você tiver um grupo de recursos federados com dois bancos de dados e um tiver dados em um storage que não seja NetApp, a operação de backup será abortada mesmo que o outro banco de dados esteja no storage NetApp.

5. Na página Backup, execute as seguintes etapas:

- a. Se você tiver várias políticas associadas ao grupo de recursos, selecione a política de backup que deseja usar na lista suspensa **Política**.

Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

- b. Selecione **Backup**.

6. Monitorize o progresso selecionando **Monitor > trabalhos**.

Depois de terminar

- Na configuração do AIX, você pode usar o `lkdev` comando para bloquear e o `rendev` comando para renomear os discos nos quais o banco de dados que foi feito backup residia.

Bloquear ou renomear dispositivos não afetará a operação de restauração quando você restaurar usando esse backup.

- Se a operação de backup falhar porque o tempo de execução da consulta do banco de dados excedeu o valor de tempo limite, você deve alterar o valor dos parâmetros `ORACLE_SQL_QUERY_TIMEOUT` e `ORACLE_PLUGIN_SQL_QUERY_TIMEOUT` executando `Set-SmConfigSettings` o cmdlet:

Depois de modificar o valor dos parâmetros, reinicie o serviço SnapCenter Plug-in Loader (SPL) executando o seguinte comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Se o arquivo não estiver acessível e o ponto de montagem não estiver disponível durante o processo de verificação, a operação pode falhar com o código de erro DBV-00100 arquivo especificado. Você deve modificar os valores dos parâmetros `VERIFICATION_DELAY_` e `VERIFICATION_RETRY_COUNT` em `sco.properties`.

Depois de modificar o valor dos parâmetros, reinicie o serviço SnapCenter Plug-in Loader (SPL) executando o seguinte comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

Monitorar o backup do banco de dados Oracle

Saiba como monitorar o progresso das operações de backup e operações de proteção de dados.

Monitorar operações de backup de banco de dados Oracle

Você pode monitorar o progresso de diferentes operações de backup usando a página SnapCenterJobs. Você pode querer verificar o progresso para determinar quando ele está concluído ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado correspondente das operações:

-  Em curso
-  Concluído com êxito
-  Falha
-  Preenchido com avisos ou não foi possível iniciar devido a avisos
-  Em fila de espera
-  Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **trabalhos**.
3. Na página trabalhos, execute as seguintes etapas:
 - a. Clique  para filtrar a lista de modo a que apenas as operações de cópia de segurança sejam listadas.
 - b. Especifique as datas de início e fim.
 - c. Na lista suspensa **Type**, selecione **Backup**.
 - d. Na lista suspensa **Status**, selecione o status da cópia de segurança.
 - e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione um trabalho de cópia de segurança e clique em **Detalhes** para ver os detalhes do trabalho.



Embora o status do trabalho de backup seja exibido  , quando você clica nos detalhes do trabalho, você pode ver que algumas das tarefas secundárias da operação de backup ainda estão em andamento ou marcadas com sinais de aviso.

5. Na página Detalhes da tarefa, clique em **Exibir logs**.

O botão **View logs** exibe os logs detalhados para a operação selecionada.

Monitore operações de proteção de dados no painel atividade

O painel atividade exibe as cinco operações mais recentes executadas. O painel atividade também é exibido quando a operação foi iniciada e o status da operação.

O painel atividade exibe informações sobre operações de backup, restauração, clone e backup agendadas. Se você estiver usando Plug-in para SQL Server ou Plug-in para Exchange Server, o painel atividade também exibirá informações sobre a operação de Reseed.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Clique  no painel atividade para visualizar as cinco operações mais recentes.

Quando você clica em uma das operações, os detalhes da operação são listados na página **Detalhes da**

tarefa.

Outras operações de backup

Faça backup de bancos de dados Oracle usando comandos UNIX

O fluxo de trabalho de backup inclui Planejamento, identificação dos recursos para backup, criação de políticas de backup, criação de grupos de recursos e inclusão de políticas, criação de backups e monitoramento das operações.

O que você vai precisar

- Você deve ter adicionado as conexões do sistema de armazenamento e criado a credencial usando os comandos *Add-SmStorageConnection* e *Add-SmCredential*.
- Você deve ter estabelecido a sessão de conexão com o servidor SnapCenter usando o comando *Open-SmConnection*.

Você pode ter apenas uma sessão de login da conta do SnapCenter e o token é armazenado no diretório home do usuário.



A sessão de ligação é válida apenas durante 24 horas. No entanto, você pode criar um token com a opção *TokenNeverExpires* para criar um token que nunca expira e a sessão sempre será válida.

Sobre esta tarefa

Você deve executar os seguintes comandos para estabelecer a conexão com o servidor SnapCenter, descobrir as instâncias de banco de dados Oracle, adicionar política e grupo de recursos, fazer backup e verificar o backup.

As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando *Get-Help command_name*. Em alternativa, pode também consultar o "[Guia de Referência de comandos do software SnapCenter](#)".

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado: *Open-SmConnection*
2. Execute a operação de descoberta de recursos do host: *Get-SmResources*
3. Configurar credenciais de banco de dados Oracle e nós preferenciais para operação de backup de um banco de dados do Real Application Cluster (RAC): *Configure-SmOracleDatabase*
4. Criar uma política de backup: *Add-SmPolicy*
5. Recuperar as informações sobre o local de armazenamento secundário (SnapVault ou SnapMirror) : *Get-SmSecondaryDetails*

Este comando recupera os detalhes do mapeamento de armazenamento primário para secundário de um recurso especificado. Você pode usar os detalhes do mapeamento para configurar as configurações de verificação secundária ao criar um grupo de recursos de backup.

6. Adicionar um grupo de recursos ao SnapCenter: *Adicionar-SmResourceGroup*

7. Criar um backup: *New-SmBackup*

Você pode poll a tarefa usando a opção `WaitForCompletion`. Se essa opção for especificada, o comando continuará a polling o servidor até a conclusão da tarefa de backup.

8. Recuperar os logs do SnapCenter: *Get-SmLogs*

Cancelar operações de backup de bancos de dados Oracle

Você pode cancelar as operações de backup em execução, na fila ou não responsivas.

Você deve estar conectado como administrador do SnapCenter ou proprietário da tarefa para cancelar as operações de backup.

Sobre esta tarefa

Quando você cancela uma operação de backup, o servidor SnapCenter interrompe a operação e remove todas as cópias Snapshot do armazenamento se o backup criado não estiver registrado no servidor SnapCenter. Se o backup já estiver registrado no servidor SnapCenter, ele não reverterá a cópia Snapshot já criada mesmo após o cancelamento ser acionado.

- Pode cancelar apenas a operação de registro ou cópia de segurança completa que está em fila ou em execução.
- Não é possível cancelar a operação após a verificação ter sido iniciada.

Se cancelar a operação antes da verificação, a operação é cancelada e a operação de verificação não será executada.

- Não é possível cancelar a operação de cópia de segurança depois de as operações de catálogo terem sido iniciadas.
- Pode cancelar uma operação de cópia de segurança a partir da página Monitor ou do painel atividade.
- Além de usar a GUI do SnapCenter, você pode usar comandos CLI para cancelar operações.
- O botão **Cancelar trabalho** está desativado para operações que não podem ser canceladas.
- Se você selecionou **todos os membros desta função podem ver e operar em objetos de outros membros** na página usuários/grupos ao criar uma função, você pode cancelar as operações de backup em fila de outros membros enquanto usa essa função.

Passo

Execute uma das seguintes ações:

A partir do...	Ação
Página do monitor	1. No painel de navegação esquerdo, clique em Monitor > trabalhos. 2. Selecione a operação e clique em Cancelar trabalho.

A partir do...	Ação
Painel da atividade	1. Depois de iniciar o trabalho de cópia de segurança, clique  no painel atividade para ver as cinco operações mais recentes. 2. Selecione a operação. 3. Na página Detalhes da tarefa, clique em Cancelar tarefa.

Resultados

A operação é cancelada e o recurso é revertido para o estado original.

Se a operação cancelada não for responsiva no estado de cancelamento ou execução, você deve executar o `Cancelar-SmJob -JobID <int> -forçar` para interromper a operação de backup com força.

Veja os backups e clones do banco de dados Oracle na página topologia

Ao se preparar para fazer backup ou clonar um recurso, talvez seja útil exibir uma representação gráfica de todos os backups e clones no storage primário e secundário.

Sobre esta tarefa

Na página topologia, você pode ver todos os backups e clones disponíveis para o grupo de recursos ou recursos selecionado. Você pode visualizar os detalhes desses backups e clones e, em seguida, selecioná-los para executar operações de proteção de dados.

Você pode revisar os ícones a seguir na exibição Gerenciar cópias para determinar se os backups e clones estão disponíveis no storage primário ou secundário (cópias espelhadas ou cópias do Vault).

-  exibe o número de backups e clones disponíveis no storage primário.
-  Exibe o número de backups e clones espelhados no storage secundário usando a tecnologia SnapMirror.
-  Exibe o número de backups e clones replicados no storage secundário usando a tecnologia SnapVault.

O número de backups exibidos inclui os backups excluídos do armazenamento secundário. Por exemplo, se você criou backups 6 usando uma política para reter apenas 4 backups, o número de backups exibidos é 6.



Os clones de um backup de um espelhamento flexível de versão em um volume do tipo cofre-espelho são exibidos na visualização de topologia, mas a contagem de backup espelhado na visualização de topologia não inclui o backup flexível de versão.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione o recurso ou o grupo de recursos na lista suspensa **Exibir**.
3. Selecione o recurso na exibição de detalhes do recurso ou na exibição de detalhes do grupo de recursos.

Se o recurso estiver protegido, a página topologia do recurso selecionado é exibida.

4. Revise o cartão de resumo para ver um resumo do número de backups e clones disponíveis no storage primário e secundário.

A seção cartão de resumo exibe o número total de backups e clones e o número total de backups de log.

Clicar no botão **Refresh** inicia uma consulta do armazenamento para exibir uma contagem precisa.

5. No modo de exibição Gerenciar cópias, clique em **backups** ou **clones** do armazenamento primário ou secundário para ver detalhes de um backup ou clone.

Os detalhes dos backups e clones são exibidos em um formato de tabela.

6. Selecione o backup na tabela e clique nos ícones de proteção de dados para executar operações de restauração, clonagem, montagem, desmontagem, renomeação, catálogo, descátalo e exclusão.



Não é possível renomear ou excluir backups que estão no armazenamento secundário.

- Se tiver selecionado um backup de log, você só poderá executar operações de renomeação, montagem, desmontagem, catálogo, descátalo e exclusão.
- Se você catalogou o backup usando o Oracle Recovery Manager (RMAN), não será possível renomear esses backups catalogados.

7. Se quiser excluir um clone, selecione-o na tabela e clique  em .

Se o valor atribuído ao `SnapmirrorStatusUpdateWaitTime` for menor, as cópias de backup Mirror e Vault não serão listadas na página de topologia, mesmo que os volumes de dados e log sejam protegidos com êxito. Você deve aumentar o valor atribuído ao `SnapmirrorStatusUpdateWaitTime` usando o cmdlet `Set-SmConfigSettings` PowerShell.

As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando `Get-Help command_name`.

Em alternativa, pode também consultar a ["Guia de Referência de comandos do software SnapCenter"](#) ou ["Guia de referência de cmdlet do software SnapCenter"](#).

Montar e desmontar backups de bancos de dados

Você pode montar um único ou vários dados e Registrar somente backups se quiser acessar os arquivos no backup. Você pode montar o backup no mesmo host em que o backup foi criado ou em um host remoto com o mesmo tipo de configurações Oracle e host. Se você tiver montado manualmente os backups, deverá desmontar manualmente os backups após concluir a operação. Em qualquer instância, um backup de um banco de dados pode ser montado em qualquer um do host. Ao executar uma operação, você pode montar apenas um único backup.



Em uma configuração do Flex ASM, você não pode executar a operação de montagem em Leaf Nodes se a cardinalidade for menor que os nós numéricos no cluster RAC.

Montar um backup de banco de dados

Você deve montar manualmente um backup de banco de dados se quiser acessar os arquivos no backup.

O que você vai precisar

- Se você tiver uma instância de banco de dados de Gerenciamento Automático de armazenamento (ASM) em um ambiente NFS e quiser montar os backups ASM, você deve ter adicionado o caminho de disco ASM `/var/opt/SnapCenter/SCO/backup*/*/` ao caminho existente definido no parâmetro `ASM_diskstring`.
- Se você tiver uma instância de banco de dados ASM em um ambiente NFS e quiser montar os backups de log ASM como parte de uma operação de recuperação, você deve ter adicionado o caminho de disco ASM `/var/opt/SnapCenter/scu/clones*/` ao caminho existente definido no parâmetro `ASM_diskstring`.
- No parâmetro `ASM_diskstring`, você deve configurar `AFD:*` se estiver usando ASMFD ou configurar `ORCL:*` se estiver usando ASMLIB.



Para obter informações sobre como editar o parâmetro `ASM_diskstring`, ["Como adicionar caminhos de disco ao ASM_diskstring"](#) consulte .

- Você deve configurar as credenciais ASM e a porta ASM se for diferente da do host do banco de dados de origem durante a montagem do backup.
- Se você quiser montar em um host alternativo, verifique se o host alternativo atende aos seguintes requisitos:
 - O mesmo UID e GID do host original
 - Mesma versão Oracle que a do host original
 - A mesma distribuição e versão do sistema operacional que a do host original
 - Para NVMe, o NVMe útil deve ser instalado
- Você deve garantir que o LUN não seja mapeado para o host AIX usando o iGroup que consiste em protocolos mistos iSCSI e FC. Para obter mais informações, ["A operação falha com erro não é possível descobrir o dispositivo para LUN"](#) consulte .

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados na exibição de detalhes do banco de dados ou na exibição de detalhes do grupo de recursos.

A página de topologia do banco de dados é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** no sistema de armazenamento primário ou secundário (espelhado ou replicado).
5. Selecione o backup na tabela e clique  em .
6. Na página Monte backups, selecione o host no qual você deseja montar o backup na lista suspensa **escolha o host para montar o backup**.

O caminho de montagem `/var/opt/SnapCenter/SCO/backup_mount/backup_name/database_name` é exibido.

Se você estiver montando o backup de um banco de dados ASM, o caminho de montagem `-diskgroupname_SID_backupid` será exibido.

7. Clique em **montar**.

Depois de terminar

- Você pode executar o seguinte comando para recuperar as informações relacionadas ao backup montado:

```
./sccli Get-SmBackup -BackupName backup_name -ListMountInfo
```

- Se tiver montado uma base de dados ASM, pode executar o seguinte comando para recuperar as informações relacionadas com a cópia de segurança montada:

```
./sccli Get-Smbbackup -BackupNamediskgroupname_SID_backupid-listmountinfo
```

- Para recuperar o ID de backup, execute o seguinte comando:

```
./sccli Get-Smbbackup-BackupNamebackup_name
```

As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando `Get-Help command_name`. Em alternativa, pode também consultar o ["Guia de Referência de comandos do software SnapCenter"](#).

Desmontar um backup de banco de dados

Você pode desmontar manualmente um backup de banco de dados montado quando não quiser mais acessar arquivos no backup.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados na exibição de detalhes do banco de dados ou na exibição de detalhes do grupo de recursos.

A página de topologia do banco de dados é exibida.

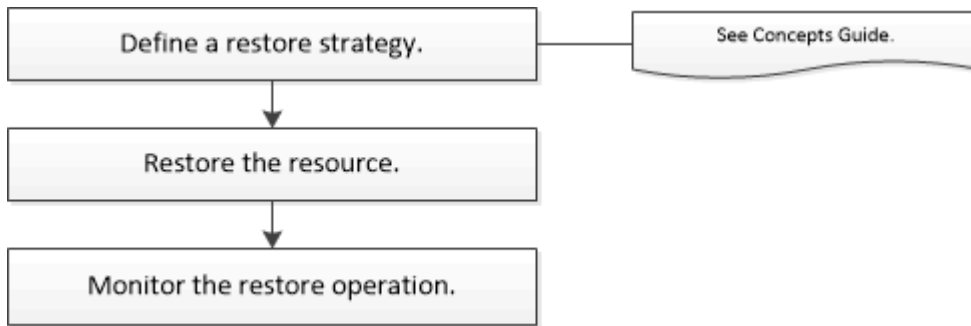
4. Selecione a cópia de segurança montada e, em seguida, clique  em .
5. Clique em **OK**.

Restaurar e recuperar bancos de dados Oracle

Restaure o fluxo de trabalho

O fluxo de trabalho de restauração inclui Planejamento, execução das operações de restauração e monitoramento das operações.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de restauração:



Definir uma estratégia de restauração e recuperação para bancos de dados Oracle

Você deve definir uma estratégia antes de restaurar e recuperar seu banco de dados para que você possa executar operações de restauração e recuperação com sucesso.

Tipos de backups suportados para operações de restauração e recuperação

O SnapCenter dá suporte à restauração e recuperação de diferentes tipos de backups de bancos de dados Oracle.

- Backup de dados on-line
- Backup de dados de desligamento off-line
- Backup de dados de montagem off-line



Se você estiver restaurando um desligamento off-line ou backup de dados de montagem off-line, o SnapCenter deixa o banco de dados no estado off-line. Você deve recuperar manualmente o banco de dados e redefinir os logs.

- Backup completo
- Backups de montagem off-line de bancos de dados em espera do Data Guard
- Backups on-line somente de dados de bancos de dados em espera do ativo Data Guard



Não é possível executar a recuperação de bancos de dados em espera do ativo Data Guard.

- Backups de dados on-line, backups completos on-line, backups de montagem off-line e backups de desligamento off-line em uma configuração RAC (Real Application clusters)
- Backups de dados on-line, backups completos online, backups de montagem off-line e backups de desligamento off-line em uma configuração de gerenciamento de armazenamento automático (ASM)

Tipos de métodos de restauração suportados para bancos de dados Oracle

O SnapCenter é compatível com conexão e cópia ou restauração no local para bancos de dados Oracle. Durante uma operação de restauração, o SnapCenter determina o método de restauração apropriado para que o sistema de arquivos seja usado para restauração sem perda de dados.



O SnapCenter não é compatível com SnapRestore baseado em volume.

Restauração de conexão e cópia

Se o layout do banco de dados for diferente do backup ou se houver novos arquivos após a criação do backup, a restauração de conexão e cópia será executada. No método de restauração de conexão e cópia, as seguintes tarefas são executadas:

Passos

1. O volume é clonado a partir da cópia Snapshot e a pilha do sistema de arquivos é criada no host usando LUNs ou volumes clonados.
2. Os arquivos são copiados dos sistemas de arquivos clonados para os sistemas de arquivos originais.
3. Os sistemas de arquivos clonados são então desmontados do host e os volumes clonados são excluídos do ONTAP.



Para uma configuração do Flex ASM (em que a cardinalidade é menor do que os nós numéricos no cluster RAC) ou bancos de dados do ASM RAC no VMDK ou RDM, somente o método de restauração de conexão e cópia é suportado.

Mesmo que você tenha ativado com força a restauração no local, o SnapCenter executa a restauração de conexão e cópia nos seguintes cenários:

- Faça a restauração a partir do sistema de storage secundário e, se o Data ONTAP for anterior a 8,3
- Restauração de grupos de discos ASM presentes em nós de uma configuração do Oracle RAC em que a instância de banco de dados não está configurada
- Na configuração do Oracle RAC, em qualquer um dos nós pares se a instância ASM ou a instância de cluster não estiver em execução ou se o nó peer estiver inativo
- Restauração de arquivos de controle somente
- Restaure um subconjunto de espaços de tablespaces que residem em um grupo de discos ASM
- O grupo de discos é compartilhado entre ficheiros de dados, ficheiro SP e ficheiro de palavra-passe
- O serviço SnapCenter Plug-in Loader (SPL) não está instalado ou não está em execução no nó remoto em um ambiente RAC
- Novos nós são adicionados ao Oracle RAC e o servidor SnapCenter não está ciente dos nós recém-adicionados

Restauração no local

Se o layout do banco de dados for semelhante ao backup e não tiver sofrido nenhuma alteração de configuração na pilha de armazenamento e banco de dados, a restauração no local é realizada, em que a restauração do arquivo ou LUN é realizada no ONTAP. O SnapCenter suporta apenas o SFSR (Single File SnapRestore) como parte do método de restauração no local.



O Data ONTAP 8.3 ou posterior oferece suporte à restauração no local a partir de um local secundário.

Se você quiser executar a restauração no local no banco de dados, verifique se você tem somente datafiles no grupo de discos ASM. Você deve criar um backup depois que quaisquer alterações forem feitas no grupo de discos ASM ou na estrutura física do banco de dados. Depois de executar a restauração no local, o grupo de discos conterá o mesmo número de arquivos de dados que no momento do backup.

A restauração no local será aplicada automaticamente quando o grupo de discos ou o ponto de montagem

corresponder aos seguintes critérios:

- Não são adicionados dados novos após a cópia de segurança (verificação de ficheiro estrangeiro)
- Sem adição, exclusão ou recriação de disco ASM ou LUN após backup (verificação de alteração estrutural do grupo de discos ASM)
- Sem adição, exclusão ou recriação de LUNs ao grupo de discos LVM (verificação de alteração estrutural do grupo de discos LVM)



Você também pode habilitar a restauração no local com força usando GUI, CLI do SnapCenter ou cmdlet do PowerShell para substituir a verificação de arquivo estrangeiro e a verificação de alteração estrutural do grupo de discos LVM.

Executar a restauração no local no ASM RAC

No SnapCenter, o nó no qual você executa a restauração é denominado como nó principal e todos os outros nós do RAC no qual reside o grupo de discos ASM são chamados de nós de ponto. O SnapCenter altera o estado do grupo de discos ASM para desmontar em todos os nós em que o grupo de discos ASM está no estado de montagem antes de executar a operação de restauração de storage. Após a conclusão da restauração de armazenamento, o SnapCenter altera o estado do grupo de discos ASM como era antes da operação de restauração.

Em ambientes SAN, o SnapCenter remove dispositivos de todos os nós de mesmo nível e executa a operação de desmapear LUN antes da operação de restauração de storage. Após a operação de restauração de storage, o SnapCenter executa operações de mapa LUN e constrói dispositivos em todos os nós de mesmo nível. Em um ambiente SAN, se o layout ASM do Oracle RAC estiver residindo em LUNs, em seguida, durante a restauração do SnapCenter, executa operações de desmapeamento de LUN, restauração de LUN e mapa de LUN em todos os nós do cluster RAC onde reside o grupo de discos ASM. Antes de restaurar, mesmo que todos os iniciadores dos nós RAC não fossem usados para os LUNs, depois de restaurar o SnapCenter, cria um novo iGroup com todos os iniciadores de todos os nós RAC.

- Se houver alguma falha durante a atividade de pré-restauração em nós de pares, o SnapCenter reverte automaticamente o estado do grupo de discos ASM como era antes de executar a restauração em nós de pares nos quais a operação de pré-restauração foi bem-sucedida. A reversão não é suportada para o nó principal e o nó ponto em que a operação falhou. Antes de tentar outra restauração, você deve corrigir manualmente o problema no nó peer e trazer o grupo de discos ASM no nó primário de volta ao estado de montagem.
- Se houver alguma falha durante a atividade de restauração, a operação de restauração falhará e nenhum retorno será executado. Antes de tentar outra restauração, você deve corrigir manualmente o problema de restauração de armazenamento e colocar o grupo de discos ASM no nó principal de volta ao estado de montagem.
- Se houver alguma falha durante a atividade do Postrestore em qualquer um dos nós pares, o SnapCenter continuará com a operação de restauração nos outros nós de mesmo nível. Você deve corrigir manualmente o problema de pós-restauração no nó peer.

Tipos de operações de restauração compatíveis com bancos de dados Oracle

O SnapCenter permite executar diferentes tipos de operações de restauração para bancos de dados Oracle.

Antes de restaurar o banco de dados, os backups são validados para identificar se há arquivos ausentes quando comparados aos arquivos de banco de dados reais.

Restauração completa

- Restaura apenas os arquivos de dados
- Restaura apenas os arquivos de controle
- Restaura os arquivos de dados e controle
- Restaura arquivos de dados, controla arquivos e refaz arquivos de log em bancos de dados de espera do Data Guard e ative Data Guard

Restauração parcial

- Restaura apenas os espaços de tabela selecionados
- Restaura apenas os bancos de dados conectáveis selecionados (PDBs)
- Restaura apenas os espaços de tabela selecionados de um PDB

Tipos de operações de recuperação compatíveis com bancos de dados Oracle

O SnapCenter permite executar diferentes tipos de operações de recuperação para bancos de dados Oracle.

- O banco de dados até a última transação (todos os logs)
- O banco de dados até um número específico de mudança de sistema (SCN)
- A base de dados até uma data e hora específicas

Você deve especificar a data e a hora para recuperação com base no fuso horário do host do banco de dados.

O SnapCenter também fornece a opção sem recuperação para bancos de dados Oracle.



O plug-in para banco de dados Oracle não suporta recuperação se você tiver restaurado usando um backup que foi criado com a função de banco de dados como standby. Você deve sempre executar a recuperação manual para bancos de dados físicos em espera.

Limitações relacionadas à restauração e recuperação de bancos de dados Oracle

Antes de executar operações de restauração e recuperação, você precisa estar ciente das limitações.

Se você estiver usando qualquer versão do Oracle de 11.2.0.4 a 12.1.0.1, a operação de restauração estará no estado suspenso quando você executar o comando *renamedg*. Você pode aplicar o Oracle patch 19544733 para corrigir esse problema.

As seguintes operações de restauração e recuperação não são suportadas:

- Restauração e recuperação de espaços de tablespaces do banco de dados de contentor raiz (CDB)
- Restauração de espaços de tablespaces temporários e espaços de tablespaces temporários associados a PDBs
- Restauração e recuperação de espaços de tablespaces de vários PDBs simultaneamente
- Restauração de backups de log
- Restauração de backups para um local diferente
- Restauração de arquivos de log refazer em qualquer configuração que não seja os bancos de dados de espera do Data Guard ou do ativo Data Guard

- Restauração do arquivo SPFILE e Senha
- Quando você executa uma operação de restauração em um banco de dados que foi recriado usando o nome do banco de dados pré-existente no mesmo host, foi gerenciado pelo SnapCenter e teve backups válidos, a operação de restauração substitui os arquivos de banco de dados recém-criados, mesmo que os DBIDs sejam diferentes.

Isso pode ser evitado executando qualquer uma das seguintes ações:

- Descubra os recursos do SnapCenter depois que o banco de dados for recriado
- Crie uma cópia de segurança da base de dados recriada

Limitações relacionadas à recuperação ponto-em-tempo de tablespaces

- A recuperação pontual (PITR) do SISTEMA, SYSAUX e DESFAZER espaços DE tablespaces não é suportada
- PITR de tablespaces não pode ser executado junto com outros tipos de restauração
- Se um espaço de tabela for renomeado e você quiser recuperá-lo para um ponto antes de ser renomeado, você deve especificar o nome anterior do espaço de tabela
- Se as restrições para as tabelas em um espaço de tabela estiverem contidas em outro espaço de tabela, você deve recuperar ambas as espaço de tabela
- Se uma tabela e seus índices forem armazenados em diferentes espaços de tabela, então os índices devem ser descartados antes de executar o PITR
- O PITR não pode ser usado para recuperar o espaço de tabela padrão atual
- O PITR não pode ser usado para recuperar tablespaces contendo qualquer um dos seguintes objetos:
 - Objetos com objetos subjacentes (como vistas materializadas) ou objetos contidos (como tabelas particionadas), a menos que todos os objetos subjacentes ou contidos estejam no conjunto de recuperação

Além disso, se as partições de uma tabela particionada forem armazenadas em diferentes espaços de tabela, então você deve soltar a tabela antes de executar o PITR ou mover todas as partições para a mesma espaço de tabela antes de executar o PITR.

- Desfazer ou reverter segmentos
- Filas avançadas compatíveis com Oracle 8i com vários destinatários
- Objetos de propriedade do usuário SYS

Exemplos desses tipos de objetos são PL/SQL, classes Java, programas de chamada, visualizações, sinônimos, usuários, Privileges, dimensões, diretórios e sequências.

Fontes e destinos para restaurar bancos de dados Oracle

É possível restaurar um banco de dados Oracle a partir de uma cópia de backup no storage primário ou no storage secundário. Você só pode restaurar bancos de dados para o mesmo local na mesma instância de banco de dados. No entanto, na configuração do Real Application Cluster (RAC), você pode restaurar bancos de dados para outros nós.

Fontes para operações de restauração

É possível restaurar bancos de dados a partir de um backup no storage primário ou no storage secundário. Se

Se você quiser restaurar a partir de um backup no storage secundário em uma configuração de vários espelhos, você pode selecionar o espelho de armazenamento secundário como a origem.

Destinos para operações de restauração

Você só pode restaurar bancos de dados para o mesmo local na mesma instância de banco de dados.

Em uma configuração RAC, você pode restaurar bancos de dados RAC de qualquer nó no cluster.

Variáveis de ambiente predefinidas para restaurar prescrição específica e postscript

O SnapCenter permite-lhe utilizar as variáveis de ambiente predefinidas quando executa o prescriptor e o postscript enquanto restaura uma base de dados.

Variáveis de ambiente predefinidas suportadas para restaurar um banco de dados

- **SC_JOB_ID** especifica a ID da tarefa da operação.

Exemplo: 257

- **SC_ORACLE_SID** especifica o identificador do sistema do banco de dados.

Se a operação envolver vários bancos de dados, isso conterá nomes de banco de dados separados por pipe.

Exemplo: NFSB31

- **SC_HOST** especifica o nome do host do banco de dados.

Esse parâmetro será preenchido para volumes de aplicativos.

Exemplo: scsmohost2.gdl.englobe.NetApp.com

- **SC_os_USER** especifica o proprietário do sistema operacional do banco de dados.

Exemplo: oracle

- **SC_os_GROUP** especifica o grupo do sistema operacional do banco de dados.

Exemplo: Oinstall

- **SC_BACKUP_NAME** especifica o nome do backup.

Esse parâmetro será preenchido para volumes de aplicativos.

Exemplos:

- Se o banco de dados não estiver sendo executado no modo ARCHIVELOG:
DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
- Se o banco de dados estiver sendo executado no modo ARCHIVELOG:
DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1, RG2_22_12.16.48.9267-1-2021_07_21, RG2_scspr2417819002_07-20-2021_12.16.48.9267_1

- **SC_BACKUP_ID** especifica o ID do backup.

Esse parâmetro será preenchido para volumes de aplicativos.

Exemplos:

- Se o banco de dados não estiver sendo executado no modo ARCHIVELOG: DATA 203|LOG 205
- Se o banco de dados estiver sendo executado no modo ARCHIVELOG: DATA 203|LOG at 205.206.207

- **SC_RESOURCE_GROUP_NAME** especifica o nome do grupo de recursos.

Exemplo: RG1

- **SC_ORACLE_HOME** especifica o caminho do diretório inicial do Oracle.

Exemplo: /ora01/app/oracle/product/18,1.0/dB_1

- **SC_RECOVERY_TYPE** especifica os arquivos que são recuperados e também o escopo de recuperação.

Exemplo: RESTORESCOPE:usingBackupControlfile:false|RECOVERYSCOPE:allLogs

Para obter informações sobre delimitadores, "[Delimitadores suportados](#)" consulte .

Requisitos para restaurar um banco de dados Oracle

Antes de restaurar um banco de dados Oracle, você deve garantir que os pré-requisitos sejam concluídos.

- Você deve ter definido sua estratégia de restauração e recuperação.
- O administrador do SnapCenter deve ter atribuído a você as máquinas virtuais de storage (SVMs) para os volumes de origem e de destino se você estiver replicando cópias Snapshot em um espelhamento ou cofre.
- Se os logs de arquivo forem podados como parte do backup, você deve ter montado manualmente os backups de log de arquivamento necessários.
- Se você quiser restaurar bancos de dados Oracle que residem em um VMDK (Virtual Machine Disk), você deve garantir que a máquina convidada tenha o número necessário de slots livres para alocar os VMDKs clonados.
- Você deve garantir que todos os volumes de dados e volumes de log de arquivamento pertencentes ao banco de dados sejam protegidos se a proteção secundária estiver ativada para esse banco de dados.
- Você deve garantir que o banco de dados RAC One Node esteja no estado "nomount" para executar o arquivo de controle ou restauração completa do banco de dados.
- Se você tiver uma instância de banco de dados ASM no ambiente NFS, adicione o caminho de disco ASM `/var/opt/SnapCenter/scu/clones/*/*` ao caminho existente definido no parâmetro `ASM_diskstring` para montar com êxito os backups de log ASM como parte da operação de recuperação.
- No parâmetro `ASM_diskstring`, você deve configurar `AFD:*` se estiver usando ASMFD ou configurar `ORCL:*` se estiver usando ASMLIB.



Para obter informações sobre como editar o parâmetro `ASM_diskstring`, consulte "[Como adicionar caminhos de disco ao ASM_diskstring](#)"

- Você deve configurar o listener estático no arquivo **listener.ora** disponível em `_ORACLE_Home/network/admin` para bancos de dados não ASM e `_GRID_home/network/admin` para bancos de dados ASM se você tiver desabilitado a autenticação do SO e habilitado a autenticação de banco de dados Oracle para um banco de dados Oracle, e desejar restaurar os arquivos de dados e controle desse banco de dados.
- Você deve aumentar o valor do parâmetro `SCORestoreTimeout` executando o comando `Set-SmConfigSettings` se o tamanho do banco de dados estiver em terabytes (TB).
- Você deve garantir que todas as licenças necessárias para o vCenter estejam instaladas e atualizadas.

Se as licenças não estiverem instaladas ou atualizadas, é apresentada uma mensagem de aviso. Se ignorar o aviso e continuar, a restauração a partir do RDM falhará.

- Você deve garantir que o LUN não seja mapeado para o host AIX usando o iGroup que consiste em protocolos mistos iSCSI e FC. Para obter mais informações, ["A operação falha com erro não é possível descobrir o dispositivo para LUN"](#) consulte .

Restaurar e recuperar banco de dados Oracle

Em caso de perda de dados, você pode usar o SnapCenter para restaurar dados de um ou mais backups para o seu sistema de arquivos ativo e, em seguida, recuperar o banco de dados.

Antes de começar

Se tiver instalado o plug-in como um utilizador não root, deve atribuir manualmente as permissões de execução aos diretórios `prescriitor` e `postscript`.

Sobre esta tarefa

A recuperação é efetuada utilizando os registos de arquivo disponíveis no local de registo de arquivo configurado. Se o banco de dados estiver sendo executado no modo `ARCHIVELOG`, o banco de dados Oracle salvará os grupos preenchidos de arquivos de log refazer em um ou mais destinos off-line, conhecidos coletivamente como o log refazer arquivado. O SnapCenter identifica e monta o número ideal de backups de log com base na opção `SCN` especificada, data e hora selecionadas ou todos os logs. Se os logs de arquivo necessários para recuperação não estiverem disponíveis no local configurado, você deverá montar a cópia Snapshot contendo os logs e especificar o caminho como logs de arquivo externo.

Se você migrar o banco de dados ASM do `ASMLIB` para o `ASMFD`, os backups criados com o `ASMLIB` não podem ser usados para restaurar o banco de dados. Você deve criar backups na configuração `ASMFD` e usar esses backups para restaurar. Da mesma forma, se o banco de dados ASM for migrado do `ASMFD` para o `ASMLIB`, você deverá criar backups na configuração `ASMLIB` para restaurar.

Quando você restaura um banco de dados, um arquivo de bloqueio operacional (`.SM_lock_dbsid`) é criado no host de banco de dados Oracle no diretório `/var/opt/SnapCenter/SCO/lock` para evitar que várias operações sejam executadas no banco de dados. Depois que o banco de dados foi restaurado, o arquivo de bloqueio operacional é removido automaticamente.



A restauração do arquivo SPFILE e Senha não é suportada.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.

2. Na página recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados na exibição de detalhes do banco de dados ou na exibição de detalhes do grupo de recursos.

A página de topologia do banco de dados é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou replicado).
5. Selecione a cópia de segurança na tabela e, em seguida, clique em *  .
6. Na página Restaurar escopo, execute as seguintes tarefas:
 - a. Se você tiver selecionado um backup de um banco de dados em um ambiente de Real Application clusters (RAC), selecione o nó RAC.
 - b. Quando você seleciona um dado espelhado ou de cofre:
 - se não houver backup de log no mirror ou vault, nada será selecionado e os localizadores estarão vazios.
 - se existirem cópias de segurança de registro no mirror ou no vault, a cópia de segurança de registro mais recente é selecionada e o localizador correspondente é apresentado.



Se a cópia de segurança de registro selecionada existir na localização do espelho e do cofre, ambos os localizadores são apresentados.

- c. Execute as seguintes ações:

Se você quiser restaurar...	Faça isso...
Todos os arquivos de dados do banco de dados	Selecione todos os dados. Somente os arquivos de dados do banco de dados são restaurados. Os ficheiros de controlo, os registos de arquivo ou os ficheiros de registo de refazer não são restaurados.
Tablespaces	Selecione tablespaces. Você pode especificar os espaços de tablespaces que você deseja restaurar.

Se você quiser restaurar...	Faça isso...
Controlar ficheiros	Selecione Control Files.  Durante a restauração de arquivos de controle, certifique-se de que a estrutura de diretórios existe ou deve ser criada com os proprietários corretos de usuário e grupo, se houver, para permitir que os arquivos sejam copiados para o local de destino pelo processo de restauração. Se o diretório não existir, o trabalho de restauro falhará.
Refazer ficheiros de registo	Selecione Refazer arquivos de log. Esta opção está disponível apenas para bancos de dados em espera do Data Guard ou em espera do ative Data Guard.  Os ficheiros de registo de refazer não são salvaguardados para bases de dados que não sejam do Data Guard. Para bancos de dados que não sejam do Data Guard, a recuperação é realizada usando logs de arquivo.
Bancos de dados conetáveis (PDBs)	Selecione bancos de dados conetáveis e especifique as PDBs que você deseja restaurar.
Espaço de tabela de banco de dados conetável (PDB)	Selecione * espaços de tabela de base de dados Pluggable (PDB)* e especifique o PDB e os espaços de tabela desse PDB que você deseja restaurar. Esta opção só está disponível se tiver selecionado um PDB para restauro.

- d. Selecione **altere o estado do banco de dados, se necessário, para restaurar e recuperar** para alterar o estado do banco de dados para o estado necessário para executar operações de restauração e recuperação.

Os vários estados de um banco de dados de cima para baixo são abertos, montados, iniciados e desligados. Você deve selecionar essa caixa de seleção se o banco de dados estiver em um estado mais alto, mas o estado deve ser alterado para um estado inferior para executar uma operação de restauração. Se o banco de dados estiver em um estado inferior, mas o estado tiver de ser alterado para um estado superior para executar a operação de restauração, o estado do banco de dados será alterado automaticamente, mesmo que você não marque a caixa de seleção.

Se um banco de dados estiver no estado aberto e, para restaurar, o banco de dados precisar estar no estado montado, o estado do banco de dados será alterado somente se você selecionar essa caixa de seleção.

- a. Selecione **forçar restauração no local** se você quiser executar a restauração no local nos cenários em que novos arquivos de dados são adicionados após o backup ou quando LUNs são adicionados, excluídos ou recriados a um grupo de discos LVM.

7. Na página Recovery Scope (Escopo de recuperação), execute as seguintes ações:

Se você...	Faça isso...
Deseja recuperar para a última transação	Selecione todos os registros .
Deseja recuperar para um número específico de mudança de sistema (SCN)	Selecione até SCN (número de mudança do sistema) .
Deseja recuperar dados e tempo específicos	Selecione Data e hora . Você deve especificar a data e a hora do fuso horário do host do banco de dados.
Não quero recuperar	Selecione sem recuperação .
Deseja especificar quaisquer locais de registro de arquivo externo	Se o banco de dados estiver sendo executado no modo ARCHIVELOG, o SnapCenter identifica e monta o número ideal de backups de log com base na opção SCN especificada, data e hora selecionadas ou todos os logs. Se você ainda quiser especificar a localização dos arquivos de log de arquivo externo, selecione especificar locais de log de arquivo externo. Se os logs de arquivo forem podados como parte do backup e você tiver montado manualmente os backups de log de arquivamento necessários, você deve especificar o caminho de backup montado como o local de log de arquivamento externo para recuperação.  Você deve verificar o caminho e o conteúdo do caminho de montagem antes de listá-lo como um local de log externo. • "Proteção de dados Oracle com ONTAP" • "A operação falha com erro ORA-00308"

Não é possível executar a restauração com recuperação de backups secundários se os volumes de log de arquivamento não estiverem protegidos, mas os volumes de dados estiverem protegidos. Você só pode restaurar selecionando **sem recuperação**.

Se você estiver recuperando um banco de dados RAC com a opção abrir banco de dados selecionada, somente a instância RAC em que a operação de recuperação foi iniciada será devolvida ao estado aberto.



A recuperação não é suportada para bancos de dados de espera do Data Guard e ative Data Guard.

8. Na página PreOps, insira o caminho e os argumentos do prescritor que deseja executar antes da operação de restauração.

Você deve armazenar as prescrições no caminho `/var/opt/SnapCenter/spl/scripts` ou em qualquer pasta dentro deste caminho. Por padrão, o caminho `/var/opt/SnapCenter/spl/scripts` é preenchido. Se você criou qualquer pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.

Você também pode especificar o valor de tempo limite do script. O valor padrão é de 60 segundos.

O SnapCenter permite-lhe utilizar as variáveis de ambiente predefinidas quando executa o prescritor e o postscript. ["Saiba mais"](#)

9. Na página PostOps, execute as seguintes etapas:

- a. Insira o caminho e os argumentos do postscript que você deseja executar após a operação de restauração.

Você deve armazenar os postscripts em `/var/opt/SnapCenter/spl/scripts` ou em qualquer pasta dentro deste caminho. Por padrão, o caminho `/var/opt/SnapCenter/spl/scripts` é preenchido. Se você criou qualquer pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.



Se a operação de restauração falhar, os postscripts não serão executados e as atividades de limpeza serão acionadas diretamente.

- b. Marque a caixa de seleção se desejar abrir o banco de dados após a recuperação.

Depois de restaurar um banco de dados de contentor (CDB) com ou sem arquivos de controle, ou depois de restaurar apenas arquivos de controle CDB, se você especificar para abrir o banco de dados após a recuperação, apenas o CDB será aberto e não os bancos de dados conetáveis (PDB) nesse CDB.

Em uma configuração RAC, somente a instância RAC usada para recuperação é aberta após a recuperação.



Depois de restaurar um espaço de tabela do usuário com arquivos de controle, uma espaço de tabela do sistema com ou sem arquivos de controle, ou um PDB com ou sem arquivos de controle, apenas o estado do PDB relacionado à operação de restauração é alterado para o estado original. O estado das outras PDBs que não foram usadas para restauração não é alterado para o estado original porque o estado dessas PDBs não foi salvo. Você deve alterar manualmente o estado das PDBs que não foram usadas para restauração.

10. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários em que deseja enviar as notificações por e-mail.

Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. Se pretender anexar o relatório da operação de restauro efetuada, tem de selecionar **Anexar**

Relatório de trabalho.



Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando PowerShell SET-SmtpServer.

11. Revise o resumo e clique em **Finish**.
12. Monitorize o progresso da operação clicando em **Monitor > trabalhos**.

Para mais informações

- "O banco de dados Oracle RAC One Node é ignorado para a execução das operações do SnapCenter"
- "Falha ao restaurar a partir de um local secundário de SnapMirror ou SnapVault"
- "Falha ao restaurar a partir de um backup de uma encarnação órfã"
- "Parâmetros personalizáveis para operações de backup, restauração e clone em sistemas AIX"

Restaure e recupere espaços de tablespaces usando recuperação ponto no tempo

Você pode restaurar um subconjunto de espaços de tablespaces que foi corrompido ou descartado sem afetar os outros espaços de tablespaces no banco de dados. O SnapCenter usa o RMAN para executar a recuperação pontual (PITR) dos espaços das tabelas.

Antes de começar

- Os backups que são necessários para executar PITR de tablespaces devem ser catalogados e montados.
- Se tiver instalado o plug-in como um utilizador não root, deve atribuir manualmente as permissões de execução aos diretórios prescitor e postscript.

Sobre esta tarefa

Durante a operação PITR, o RMAN cria uma instância auxiliar no destino auxiliar especificado. O destino auxiliar pode ser um ponto de montagem ou um grupo de discos ASM. Se houver espaço suficiente no local montado, você pode reutilizar um dos locais montados em vez de um ponto de montagem dedicado.

Você deve especificar a data e hora ou SCN e o espaço de tabela é restaurado no banco de dados de origem.

Você pode selecionar e restaurar vários espaços de tabela que residem em ambientes ASM, NFS e SAN. Por exemplo, se as tablespaces TS2 e TS3 residem em NFS e TS4 residem em SAN, você pode executar em uma única operação PITR para restaurar todos os espaços de tabela.



Em uma configuração RAC, você pode executar PITR de espaços de tablespaces de qualquer nó do RAC.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados do tipo instância única (multitenant) na exibição de detalhes do banco de dados ou na exibição de detalhes do grupo de recursos.

A página de topologia do banco de dados é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou replicado).

Se o backup não estiver catalogado, selecione o backup e clique em **Catálogo**.

5. Selecione a cópia de segurança catalogada e, em seguida, clique em * .

6. Na página Restaurar escopo, execute as seguintes tarefas:

- a. Se você tiver selecionado um backup de um banco de dados em um ambiente de Real Application clusters (RAC), selecione o nó RAC.
- b. Selecione **tablespaces** e especifique as tablespaces que você deseja restaurar.



Você não pode executar PITR em SYSAUX, SISTEMA e DESFAZER espaços de tablespaces.

- c. Selecione **altere o estado do banco de dados, se necessário, para restaurar e recuperar** para alterar o estado do banco de dados para o estado necessário para executar operações de restauração e recuperação.
7. Na página Recovery Scope (Escopo de recuperação), execute uma das seguintes ações:
 - Se você quiser recuperar para um número específico de mudança de sistema (SCN), selecione **até SCN** e especifique o SCN e o destino auxiliar.
 - Se pretender recuperar para uma data e hora específicas, selecione **Data e hora** e especifique a data e hora e o destino auxiliar.

O SnapCenter identifica e monta e cataloga o número ideal de backups de dados e log necessários para executar o PITR com base no SCN especificado ou na data e hora selecionadas.

8. Na página PreOps, insira o caminho e os argumentos do prescritor que deseja executar antes da operação de restauração.

Você deve armazenar as prescripts no caminho /var/opt/SnapCenter/spl/scripts ou em qualquer pasta dentro deste caminho. Por padrão, o caminho /var/opt/SnapCenter/spl/scripts é preenchido. Se você criou qualquer pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.

Você também pode especificar o valor de tempo limite do script. O valor padrão é de 60 segundos.

O SnapCenter permite-lhe utilizar as variáveis de ambiente predefinidas quando executa o prescritor e o postscript. ["Saiba mais"](#)

9. Na página PostOps, execute as seguintes etapas:

- a. Insira o caminho e os argumentos do postscript que você deseja executar após a operação de restauração.



Se a operação de restauração falhar, os postscripts não serão executados e as atividades de limpeza serão acionadas diretamente.

- b. Marque a caixa de seleção se desejar abrir o banco de dados após a recuperação.

10. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários em que deseja enviar as notificações por e-mail.
11. Revise o resumo e clique em **Finish**.
12. Monitorize o progresso da operação clicando em **Monitor > trabalhos**.

Restaurar e recuperar banco de dados conetável usando recuperação pontual

Você pode restaurar e recuperar um banco de dados conetável (PDB) que foi corrompido ou descartado sem afetar as outras PDBs no banco de dados de contentores (CDB). O SnapCenter usa o RMAN para executar a recuperação pontual (PITR) do PDB.

Antes de começar

- Os backups necessários para executar o PITR de um PDB devem ser catalogados e montados.



Em uma configuração RAC, você deve fechar manualmente o PDB (mudando o estado para MONTADO) em todos os nós da configuração RAC.

- Se tiver instalado o plug-in como um utilizador não root, deve atribuir manualmente as permissões de execução aos diretórios prescitor e postscript.

Sobre esta tarefa

Durante a operação PITR, o RMAN cria uma instância auxiliar no destino auxiliar especificado. O destino auxiliar pode ser um ponto de montagem ou um grupo de discos ASM. Se houver espaço suficiente no local montado, você pode reutilizar um dos locais montados em vez de um ponto de montagem dedicado.

Você deve especificar a data e a hora ou SCN para executar o PITR do PDB. O RMAN pode recuperar PDBs DE LEITURA ESCRITA, LEITURA SOMENTE ou descartados, incluindo datafiles.

Você pode restaurar e recuperar apenas:

- Um PDB de cada vez
- Um espaço de tabela em um PDB
- Várias tablespaces do mesmo PDB



Em uma configuração RAC, você pode executar PITR de espaços de tablespaces de qualquer nó do RAC.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados do tipo instância única (multitenant) na exibição de detalhes do banco de dados ou na exibição de detalhes do grupo de recursos.

A página de topologia do banco de dados é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou replicado).

Se o backup não estiver catalogado, selecione o backup e clique em **Catálogo**.

5. Selecione a cópia de segurança catalogada e, em seguida, clique em * .

6. Na página Restaurar escopo, execute as seguintes tarefas:

- Se você tiver selecionado um backup de um banco de dados em um ambiente de Real Application clusters (RAC), selecione o nó RAC.
- Dependendo se você deseja restaurar o PDB ou espaços de tabela em um PDB, execute uma das ações:

Se você quiser...	Passos...
Restaure um PDB	- Selecione bancos de dados conetáveis (PDBs). - Especifique o PDB que deseja restaurar.  Você não pode executar PITR no banco de dados PDB.
Restaure espaços de tabela em um PDB	- Selecione espaços de tabela de base de dados conetáveis (PDB). - Especifique o PDB. - Especifique um único espaço de tabela ou vários espaços de tabela que você deseja restaurar.  Você não pode executar PITR em SYSAUX, SISTEMA e DESFAZER espaços de tablespaces.

- Selecione **altere o estado do banco de dados, se necessário, para restaurar e recuperar** para alterar o estado do banco de dados para o estado necessário para executar operações de restauração e recuperação.

7. Na página Recovery Scope (Escopo de recuperação), execute uma das seguintes ações:

- Se você quiser recuperar para um número específico de mudança de sistema (SCN), selecione **até SCN** e especifique o SCN e o destino auxiliar.
- Se pretender recuperar para uma data e hora específicas, selecione **Data e hora** e especifique a data e hora e o destino auxiliar.

O SnapCenter identifica e monta e cataloga o número ideal de backups de dados e log necessários para executar o PITR com base no SCN especificado ou na data e hora selecionadas.

8. Na página PreOps, insira o caminho e os argumentos do prescritor que deseja executar antes da operação de restauração.

Você deve armazenar as prescripts no caminho /var/opt/SnapCenter/spl/scripts ou em qualquer pasta

dentro deste caminho. Por padrão, o caminho /var/opt/SnapCenter/spl/scripts é preenchido. Se você criou qualquer pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.

Você também pode especificar o valor de tempo limite do script. O valor padrão é de 60 segundos.

O SnapCenter permite-lhe utilizar as variáveis de ambiente predefinidas quando executa o prescript e o postscript. ["Saiba mais"](#)

9. Na página PostOps, execute as seguintes etapas:

- a. Insira o caminho e os argumentos do postscript que você deseja executar após a operação de restauração.



Se a operação de restauração falhar, os postscripts não serão executados e as atividades de limpeza serão acionadas diretamente.

- b. Marque a caixa de seleção se desejar abrir o banco de dados após a recuperação.

Em uma configuração RAC, o PDB será aberto apenas no nó em que o banco de dados foi recuperado. Você deve abrir manualmente o PDB recuperado em todos os outros nós da configuração RAC.

10. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários em que deseja enviar as notificações por e-mail.
11. Revise o resumo e clique em **Finish**.
12. Monitorize o progresso da operação clicando em **Monitor > trabalhos**.

Restaure e recupere bancos de dados Oracle usando comandos UNIX

O fluxo de trabalho de restauração e recuperação inclui o Planejamento, a execução das operações de restauração e recuperação e o monitoramento das operações.

Sobre esta tarefa

Você deve executar os seguintes comandos para estabelecer a conexão com o servidor SnapCenter, listar os backups e recuperar suas informações e restaurar o backup.

As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando `Get-Help command_name`. Em alternativa, pode também consultar o ["Guia de Referência de comandos do software SnapCenter"](#).

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado: *Open-SmConnection*
2. Recupere as informações sobre os backups que você deseja restaurar: *Get-SmBackup*
3. Recupere as informações detalhadas sobre o backup especificado: *Get-SmBackupDetails*

Este comando recupera as informações detalhadas sobre o backup de um recurso especificado com um determinado ID de backup. As informações incluem nome do banco de dados, versão, home, start e end SCN, tablespaces, bancos de dados conectáveis e suas tablespaces.

Monitorar operações de restauração de banco de dados Oracle

Pode monitorizar o progresso de diferentes operações de restauro do SnapCenter utilizando a página trabalhos. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

os estados pós-restauração descrevem as condições do recurso após uma operação de restauração e quaisquer outras ações de restauração que você possa executar.

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

-  Em curso
-  Concluído com êxito
-  Falha
-  Preenchido com avisos ou não foi possível iniciar devido a avisos
-  Em fila de espera
-  Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
 - a. Clique  para filtrar a lista de modo que apenas as operações de restauração sejam listadas.
 - b. Especifique as datas de início e fim.
 - c. Na lista suspensa **Type**, selecione **Restore**.
 - d. Na lista suspensa **Status**, selecione o status de restauração.
 - e. Clique em **Apply** para ver as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para exibir os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Visualizar logs**.

O botão **View logs** exibe os logs detalhados para a operação selecionada.



Após a operação de restauração baseada em volume, os metadados do backup são excluídos do repositório do SnapCenter, mas as entradas do catálogo de backup permanecem no catálogo do SAP HANA. Embora o status do trabalho de restauração seja exibido  , você deve clicar nos detalhes do trabalho para ver o sinal de aviso de algumas das tarefas secundárias. Clique no sinal de aviso e elimine as entradas do catálogo de cópias de segurança indicadas.

Cancelar operações de restauração de banco de dados Oracle

Você pode cancelar trabalhos de restauração que estão na fila.

Você deve estar logado como administrador do SnapCenter ou proprietário da tarefa para cancelar as operações de restauração.

Sobre esta tarefa

- Você pode cancelar uma operação de restauração em fila na página **Monitor** ou no painel **atividade**.
- Não é possível cancelar uma operação de restauração em execução.
- Você pode usar a GUI do SnapCenter, cmdlets do PowerShell ou os comandos CLI para cancelar as operações de restauração em fila.
- O botão **Cancelar trabalho** está desativado para operações de restauração que não podem ser canceladas.
- Se você selecionou **todos os membros desta função podem ver e operar em outros objetos membros** na página usuários/grupos ao criar uma função, você pode cancelar as operações de restauração em fila de outros membros enquanto usa essa função.

Passo

Execute uma das seguintes ações:

A partir do...	Ação
Página do monitor	1. No painel de navegação esquerdo, clique em Monitor > trabalhos. 2. Selecione o trabalho e clique em Cancelar trabalho.
Painel da atividade	1. Depois de iniciar a operação de restauração, clique  no painel atividade para exibir as cinco operações mais recentes. 2. Selecione a operação. 3. Na página Detalhes da tarefa, clique em Cancelar tarefa.

Clonar banco de dados Oracle

Fluxo de trabalho clone

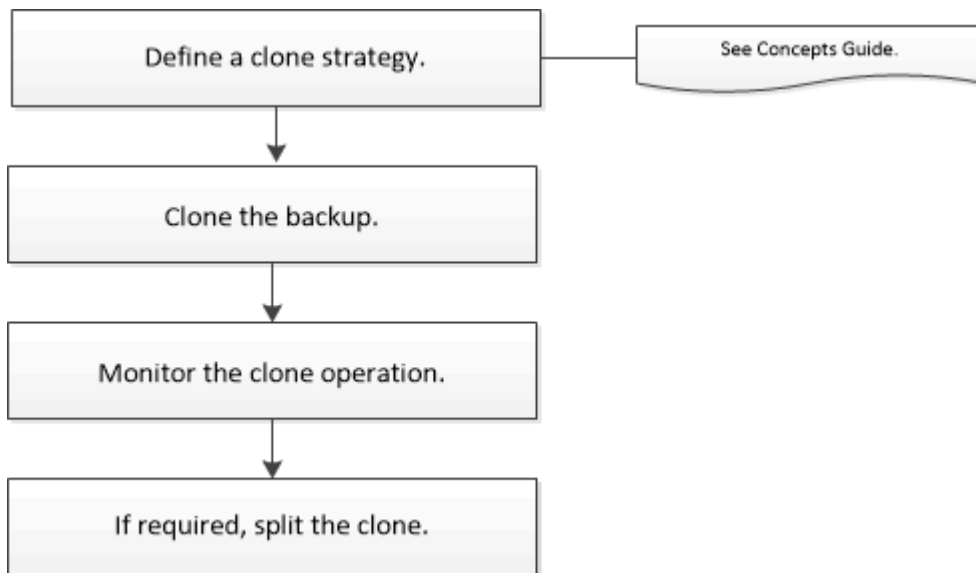
O fluxo de trabalho do clone inclui Planejamento, execução da operação do clone e monitoramento da operação.

Você pode clonar bancos de dados pelos seguintes motivos:

- Para testar a funcionalidade que deve ser implementada usando a estrutura e o conteúdo atuais do banco de dados durante os ciclos de desenvolvimento de aplicativos.
- Para preencher depósitos de dados usando ferramentas de extração e manipulação de dados.

- Para recuperar dados que foram excluídos ou alterados por engano.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação clone:



Definir uma estratégia de clone para bancos de dados Oracle

Definir uma estratégia antes de clonar seu banco de dados garante que a operação de clonagem seja bem-sucedida.

Tipos de backups compatíveis para clonagem

O SnapCenter é compatível com a clonagem de diferentes tipos de backup de bancos de dados Oracle.

- Backup de dados on-line
- Backup completo online
- Backup de montagem off-line
- Backup de desligamento off-line
- Backups de bancos de dados em espera do Data Guard e bancos de dados em espera do ativo Data Guard
- Backups de dados on-line, backups completos on-line, backups de montagem off-line e backups de desligamento off-line em uma configuração RAC (Real Application clusters)
- Backups de dados on-line, backups completos online, backups de montagem off-line e backups de desligamento off-line em uma configuração de gerenciamento de armazenamento automático (ASM)



As configurações SAN não são suportadas se a opção `user_friendly_names` no arquivo de configuração multipath estiver definida como `yes`.



A clonagem de backups de log de arquivamento não é suportada.

Tipos de clonagem compatíveis com bancos de dados Oracle

Em um ambiente de banco de dados Oracle, o SnapCenter é compatível com a clonagem de um backup de banco de dados. Você pode clonar o backup de sistemas de storage primário e secundário.

O servidor SnapCenter usa a tecnologia NetApp FlexClone para clonar backups.

Você pode atualizar um clone executando o comando "Refresh-SmClone". Esse comando cria um backup do banco de dados, exclui o clone existente e cria um clone com o mesmo nome.



A operação de atualização de clone só pode ser executada usando os comandos UNIX.

Convenções de nomenclatura de clones para bancos de dados Oracle

No SnapCenter 3,0, a convenção de nomenclatura usada para clones de sistemas de arquivos é diferente dos clones dos grupos de discos ASM.

- A convenção de nomenclatura para sistemas de arquivos SAN ou NFS é `FileSystemNameofsourcedatabase_CLONESID`.
- A convenção de nomenclatura para grupos de discos ASM é `SC_HASHCODEofDISKGROUP_CLONESID`.

`HASHCODEofDISKGROUP` é um número gerado automaticamente (2 a 10 dígitos) que é exclusivo para cada grupo de discos ASM.

Limitações da clonagem de bancos de dados Oracle

Você deve estar ciente das limitações das operações de clone antes de clonar os bancos de dados.

- Se você estiver usando qualquer versão do Oracle de 11.2.0.4 a 12.1.0.1, a operação clone estará no estado suspenso quando você executar o comando *renamedg*. Você pode aplicar o Oracle patch 19544733 para corrigir esse problema.
- A clonagem de bancos de dados de um LUN que está diretamente conectado a um host (por exemplo, usando o Microsoft iSCSI Initiator em um host Windows) para um VMDK ou um LUN RDM no mesmo host Windows, ou outro host Windows, ou vice-versa, não é suportada.
- O diretório raiz do ponto de montagem do volume não pode ser um diretório compartilhado.
- Se você mover um LUN que contém um clone para um novo volume, o clone não poderá ser excluído.

Variáveis de ambiente predefinidas para o prescritor específico de clone e postscript

O SnapCenter permite-lhe utilizar as variáveis de ambiente predefinidas quando executa o prescritor e o postscript durante a clonagem de uma base de dados.

Variáveis de ambiente predefinidas suportadas para clonar um banco de dados

- **SC_ORIGINAL_SID** especifica o SID do banco de dados de origem.

Esse parâmetro será preenchido para volumes de aplicativos.

Exemplo: NFSB32

- **SC_ORIGINAL_HOST** especifica o nome do host de origem.

Esse parâmetro será preenchido para volumes de aplicativos.

Exemplo: asmrac1.gdl.englab.NetApp.com

- **SC_ORACLE_Home** especifica o caminho do diretório inicial do Oracle do banco de dados de destino.

Exemplo: /ora01/app/oracle/product/18,1.0/dB_1

- **SC_BACKUP_NAME** especifica o nome do backup.

Esse parâmetro será preenchido para volumes de aplicativos.

Exemplos:

- Se o banco de dados não estiver sendo executado no modo ARCHIVELOG:
DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
- Se o banco de dados estiver sendo executado no modo ARCHIVELOG:
DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG:RG2_07_22-20-1_12.16.48.9267_12.16.48.9267, RG2_2021_07-21-scspr2417819002_1_2021, RG2_scspr2417819002_scspr2417819002-07-2021_12.16.48.9267_1

- **SC_AV_NAME** especifica os nomes dos volumes da aplicação.

Exemplo: AV1|AV2

- **SC_ORIGINAL_os_USER** especifica o proprietário do sistema operacional do banco de dados de origem.

Exemplo: oracle

- **SC_ORIGINAL_os_GROUP** especifica o grupo do sistema operacional do banco de dados de origem.

Exemplo: Oinstall

- **SC_TARGET_SID** especifica o SID do banco de dados clonado.

Para o fluxo de trabalho do clone PDB, o valor deste parâmetro não será predefinido.

Esse parâmetro será preenchido para volumes de aplicativos.

Exemplo: Clonedb

- **SC_TARGET_HOST** especifica o nome do host onde o banco de dados será clonado.

Esse parâmetro será preenchido para volumes de aplicativos.

Exemplo: asmrac1.gdl.englab.NetApp.com

- **SC_TARGET_os_USER** especifica o proprietário do sistema operacional do banco de dados clonado.

Para o fluxo de trabalho do clone PDB, o valor deste parâmetro não será predefinido.

Exemplo: oracle

- **SC_TARGET_os_GROUP** especifica o grupo do sistema operacional do banco de dados clonado.

Para o fluxo de trabalho do clone PDB, o valor deste parâmetro não será predefinido.

Exemplo: Oinstall

- **SC_TARGET_DB_port** especifica a porta de banco de dados do banco de dados clonado.

Para o fluxo de trabalho do clone PDB, o valor deste parâmetro não será predefinido.

Exemplo: 1521

Para obter informações sobre delimitadores, ["Delimitadores suportados"](#) consulte .

Requisitos para clonar um banco de dados Oracle

Antes de clonar um banco de dados Oracle, você deve garantir que os pré-requisitos sejam concluídos.

- Você deve ter criado um backup do banco de dados usando o SnapCenter.

Você deve ter criado com êxito os backups de dados on-line e de log ou backups off-line (montagem ou desligamento) para que a operação de clonagem seja bem-sucedida.

- Se você quiser personalizar o arquivo de controle ou refazer caminhos de arquivo de log, você deve ter pré-provisionado o sistema de arquivos necessário ou o grupo de discos de Gerenciamento Automático de armazenamento (ASM).

Por padrão, os arquivos de log refazer e controle do banco de dados clonado são criados no grupo de discos ASM ou no sistema de arquivos provisionado pelo SnapCenter para os arquivos de dados do banco de dados clone.

- Se você estiver usando ASM em NFS, você deve adicionar */var/opt/SnapCenter/scu/clones/*/** ao caminho existente definido no parâmetro **ASM_diskstring**.
- No parâmetro **ASM_diskstring**, você deve configurar *AFD:** se estiver usando ASMFD ou configurar *ORCL:** se estiver usando ASMLIB.

Para obter informações sobre como editar o parâmetro **ASM_diskstring**, ["Como adicionar caminhos de disco ao ASM_diskstring"](#) consulte .

- Se você estiver criando o clone em um host alternativo, o host alternativo deverá atender aos seguintes requisitos:
 - O plug-in do SnapCenter para banco de dados Oracle deve ser instalado no host alternativo.
 - O host clone deve ser capaz de descobrir LUNs de storage primário ou secundário.
 - Se você estiver clonando do storage primário ou do storage secundário (Vault ou Mirror) para um host alternativo, certifique-se de que uma sessão iSCSI seja estabelecida entre o storage secundário e o host alternativo ou zoneada corretamente para FC.
 - Se você estiver clonando do armazenamento do Vault ou Mirror para o mesmo host, certifique-se de que uma sessão iSCSI seja estabelecida entre o armazenamento do Vault ou Mirror e o host, ou zoneada corretamente para o FC.
 - Se você estiver clonando em um ambiente virtualizado, certifique-se de que uma sessão iSCSI

seja estabelecida entre o storage primário ou secundário e o servidor ESX que hospeda o host alternativo ou zoneada corretamente para o FC.

Para obter informações, "[documentação de utilitários do host](#)" consulte .

- Se o banco de dados de origem for um banco de dados ASM:

- A instância ASM deve estar ativa e em execução no host onde o clone será executado.
- O grupo de discos ASM deve ser provisionado antes da operação clone se você quiser colocar arquivos de log de arquivamento do banco de dados clonados em um grupo de discos ASM dedicado.
- O nome do grupo de discos de dados pode ser configurado, mas certifique-se de que o nome não seja usado por nenhum outro grupo de discos ASM no host onde o clone será executado.

Os arquivos de dados que residem no grupo de discos ASM são provisionados como parte do fluxo de trabalho do clone do SnapCenter.

- Para NVMe, o NVMe útil deve ser instalado

- O tipo de proteção para o LUN de dados e o LUN de log, como espelho, cofre ou espelho-Vault, deve ser o mesmo para descobrir localizadores secundários durante a clonagem para um host alternativo usando backups de log.
- Você deve definir o valor de `exclude_seed_cdb_view` como FALSE no arquivo de parâmetro do banco de dados de origem para recuperar informações relacionadas ao PDB de semente para clonar um backup do banco de dados 12_c_.

A PDB de semente é um modelo fornecido pelo sistema que o CDB pode usar para criar PDBs. O PDB de semente é chamado de PDB DE SEMENTE. Para obter informações sobre o PDB, consulte o Oracle Doc ID 1940806,1.



Você deve definir o valor antes de fazer backup do banco de dados 12_c_.

- O SnapCenter suporta backup de sistemas de arquivos gerenciados pelo subsistema autofs. Se você estiver clonando o banco de dados, verifique se os pontos de montagem de dados não estão sob a raiz do ponto de montagem do autofs porque o usuário raiz do host do plug-in não tem permissão para criar diretórios sob a raiz do ponto de montagem do autofs.

Se os arquivos de log de controle e refazer estiverem sob ponto de montagem de dados, você deve modificar o caminho do arquivo de controle e refazer o caminho do arquivo de log de acordo.



Você pode Registrar manualmente os novos pontos de montagem clonados com o subsistema autofs. Os novos pontos de montagem clonados não serão registrados automaticamente.

- Se você tiver um TDE (login automático) e quiser clonar o banco de dados no mesmo host ou alternativo, copie a carteira (arquivos de chave) em `/etc/ORACLE/wallet/ Oracle_SID` do banco de dados de origem para o banco de dados clonado.
- Você deve definir o valor de `use_lvm` em `/etc/lvm/lvm.conf` e parar o serviço `lvm2-lvmetad` para executar a clonagem com sucesso em ambientes de rede de área de armazenamento (SAN) no Oracle Linux 7 ou posterior ou Red Hat Enterprise Linux (RHEL) 7 ou posterior.
- Você deve instalar o patch 13366202 Oracle se estiver usando o banco de dados Oracle 11.2.0.3 ou posterior e o ID do banco de dados para a instância auxiliar for alterado usando um script NID.

- Você deve garantir que os agregados que hospedam os volumes estejam na lista de agregados atribuídos da máquina virtual de storage (SVM).
- Para NVMe, se qualquer porta de destino tiver que ser excluída da conexão, você deve adicionar o nome do nó de destino e o nome da porta no arquivo `/var/opt/SnapCenter/scu/etc/nvme.conf`.

Se o arquivo não existir, você deve criar o arquivo como mostrado no exemplo abaixo:

```
blacklist {
  nn-0x<target_node_name_1>:pn-0x<target_port_name_1>
  nn-0x<target_node_name_2>:pn-0x<target_port_name_2>
}
```

- Você deve garantir que o LUN não seja mapeado para o host AIX usando o iGroup que consiste em protocolos mistos iSCSI e FC. Para obter mais informações, ["A operação falha com erro não é possível descobrir o dispositivo para LUN"](#) consulte .

Clonar um backup de banco de dados Oracle

Você pode usar o SnapCenter para clonar um banco de dados Oracle usando o backup do banco de dados.

Antes de começar

Se tiver instalado o plug-in como um utilizador não root, deve atribuir manualmente as permissões de execução aos diretórios prescriitor e postscript.

Sobre esta tarefa

A operação de clonagem cria uma cópia dos arquivos de dados do banco de dados e cria novos arquivos de log refazer on-line e arquivos de controle. O banco de dados pode ser recuperado opcionalmente para um tempo especificado, com base nas opções de recuperação especificadas.



A clonagem falhará se você tentar clonar um backup criado em um host Linux para um host AIX ou vice-versa.

O SnapCenter cria um banco de dados autônomo quando clonado a partir de um backup de banco de dados do Oracle RAC. O SnapCenter suporta a criação de clone a partir do backup de bancos de dados em espera do Data Guard e do ativo Data Guard.

Durante a clonagem, o SnapCenter monta o número ideal de backups de log com base em SCN ou dat e tempo para operações de recuperação. Após a recuperação, o backup de log é desmontado. Todos esses clones são montados em `/var/opt/SnapCenter/scu/clones/`. Se você estiver usando ASM em NFS, você deve adicionar `/var/opt/SnapCenter/scu/clones/*/*` ao caminho existente definido no parâmetro `ASM_diskstring`.

Ao clonar um backup de um banco de dados ASM em um ambiente SAN, as regras do udev para os dispositivos host clonados são criadas em `/etc/udev/rules.d/999-scu-NetApp.rules`. Essas regras do udev associadas aos dispositivos host clonados são excluídas quando você exclui o clone.



Em uma configuração do Flex ASM, você não pode executar a operação clone em Leaf Nodes se a cardinalidade for menor que os nós numéricos no cluster RAC.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados na exibição de detalhes do banco de dados ou na exibição de detalhes do grupo de recursos.

A página de topologia do banco de dados é exibida.

4. Na exibição Gerenciar cópias, selecione os backups de cópias locais (primárias), cópias espelhadas (secundárias) ou cópias do Vault (secundárias).
5. Selecione a cópia de segurança de dados na tabela e, em seguida, clique em * .
6. Na página Nome, execute uma das seguintes ações:

Se você quiser...	Passos...
Clonar um banco de dados (CDB ou não CDB)	a. Especifique o SID do clone. O SID clone não está disponível por padrão e o tamanho máximo do SID é de 8 caracteres.  Você deve garantir que nenhum banco de dados com o mesmo SID exista no host onde o clone será criado.
Clonar um banco de dados conectável (PDB)	a. Selecione Clonar PDB. b. Especifique o PDB que você deseja clonar. c. Especifique o nome do PDB clonado. Para obter as etapas detalhadas para clonar um PDB, "Clone um banco de dados conectável" consulte .

Quando você seleciona um dado espelhado ou de cofre:

- se não houver backup de log no mirror ou vault, nada será selecionado e os localizadores estarão vazios.
- se existirem cópias de segurança de registro no mirror ou no vault, a cópia de segurança de registro mais recente é selecionada e o localizador correspondente é apresentado.



Se a cópia de segurança de registro selecionada existir na localização do espelho e do cofre, ambos os localizadores são apresentados.

7. Na página locais, execute as seguintes ações:

Para este campo...	Faça isso...
Clone de host	Por padrão, o host do banco de dados de origem é preenchido. Se você quiser criar o clone em um host alternativo, selecione o host com a mesma versão do Oracle e do SO que o host do banco de dados de origem.
Localizações de ficheiros de dados	Por padrão, a localização do arquivo de dados é preenchida. A convenção de nomenclatura padrão do SnapCenter para sistemas de arquivos SAN ou NFS é <code>FileSystemNameofsourcedatabase_CLONESID</code>. A convenção de nomenclatura padrão do SnapCenter para grupos de discos ASM é <code>SC_HASHCODEofDISKGROUP_CLONESID</code>. O <code>HASHCODEofDISKGROUP</code> é um número gerado automaticamente (2 a 10 dígitos) que é exclusivo para cada grupo de discos ASM.  Se você estiver personalizando o nome do grupo de discos ASM, certifique-se de que o comprimento do nome adere ao comprimento máximo suportado pela Oracle. Se você quiser especificar um caminho diferente, insira os pontos de montagem do arquivo de dados ou nomes de grupo de discos ASM para o banco de dados clone. Ao personalizar o caminho do arquivo de dados, você também deve alterar o arquivo de controle e refazer os nomes de grupo de discos ASM do arquivo de log ou sistema de arquivos para o mesmo nome usado para arquivos de dados ou para um grupo de discos ASM existente ou sistema de arquivos.

Para este campo...	Faça isso...
Controlar ficheiros	Por padrão, o caminho do arquivo de controle é preenchido. Os arquivos de controle são colocados no mesmo grupo de discos ASM ou sistema de arquivos que os arquivos de dados. Se você quiser substituir o caminho do arquivo de controle, você pode fornecer um caminho de arquivo de controle diferente.  O sistema de arquivos ou o grupo de discos ASM deve existir no host. Por padrão, o número de arquivos de controle será o mesmo do banco de dados de origem. Você pode modificar o número de arquivos de controle, mas um mínimo de um arquivo de controle é necessário para clonar o banco de dados. Você pode personalizar o caminho do arquivo de controle para um sistema de arquivos diferente (existente) do banco de dados de origem.

Para este campo...	Faça isso...
Refazer registros	Por padrão, o grupo de arquivos de log refazer, o caminho e seus tamanhos são preenchidos. Os logs de refazer são colocados no mesmo grupo de discos ASM ou sistema de arquivos que os arquivos de dados do banco de dados clonado. Se você quiser substituir o caminho do arquivo de log de refazer, você pode personalizar o caminho do arquivo de log de refazer para um sistema de arquivos diferente do banco de dados de origem.  O novo sistema de arquivos ou o grupo de discos ASM deve existir no host. Por padrão, o número de grupos de log refazer, refazer arquivos de log e seus tamanhos serão os mesmos do banco de dados de origem. Você pode modificar os seguintes parâmetros: - Número de grupos de registro refazer  É necessário um mínimo de dois grupos de log de refazer para clonar o banco de dados. - Refaça os arquivos de log em cada grupo e seu caminho Você pode personalizar o caminho do arquivo de log de refazer para um sistema de arquivos diferente (existente) do banco de dados de origem.  Um mínimo de um arquivo de log de refazer é necessário no grupo de log de refazer para clonar o banco de dados. - Tamanhos do ficheiro de registo de refazer

8. Na página credenciais, execute as seguintes ações:

Para este campo...	Faça isso...
Nome da credencial para o usuário do sistema	Selecione a credencial a ser usada para definir a senha do usuário do sistema do banco de dados clone. Se SQLNET.AUTHENTICATION_SERVICES estiver definido como NONE no arquivo sqlnet.ora no host de destino, você não deve selecionar None como credencial na GUI do SnapCenter.
Nome da credencial da instância ASM	Selecione nenhum se a autenticação do sistema operacional estiver ativada para conexão com a instância ASM no host clone. Caso contrário, selecione a credencial Oracle ASM configurada com o usuário "s" ou um usuário com privilégio "sysasm" aplicável ao host clone.

A casa, o nome de usuário e os detalhes do grupo do Oracle são preenchidos automaticamente a partir do banco de dados de origem. Você pode alterar os valores com base no ambiente Oracle do host onde o clone será criado.

9. Na página PreOps, execute as seguintes etapas:

- a. Insira o caminho e os argumentos do prescritor que você deseja executar antes da operação clone.

Você deve armazenar o prescritor em `/var/opt/SnapCenter/spl/scripts` ou em qualquer pasta dentro deste caminho. Por padrão, o caminho `/var/opt/SnapCenter/spl/scripts` é preenchido. Se você colocou o script em qualquer pasta dentro deste caminho, você precisa fornecer o caminho completo até a pasta onde o script é colocado.

O SnapCenter permite-lhe utilizar as variáveis de ambiente predefinidas quando executa o prescritor e o postscript. ["Saiba mais"](#)

- b. Na seção Configurações de parâmetros do banco de dados, modifique os valores dos parâmetros do banco de dados pré-preenchidos que são usados para inicializar o banco de dados.

Você pode adicionar parâmetros adicionais clicando  em .

Se você estiver usando o Oracle Standard Edition e o banco de dados estiver sendo executado no modo de log de arquivamento ou se desejar restaurar um banco de dados do log de reprocessamento de arquivo, adicione os parâmetros e especifique o caminho.

- LOG_ARCHIVE_DEST
- LOG_ARCHIVE_DUPLEX_DEST



A área de recuperação rápida (FRA) não está definida nos parâmetros do banco de dados pré-preenchidos. Você pode configurar FRA adicionando os parâmetros relacionados.



O valor padrão de `log_archive_dest_1` é `ORACLE_Home/clone_sid` e os logs de arquivo do banco de dados clonados serão criados nesse local. Se você tiver excluído o parâmetro `log_archive_dest_1`, o local do log do arquivo será determinado pela Oracle. Você pode definir um novo local para o log de arquivo editando `log_archive_dest_1`, mas certifique-se de que o sistema de arquivos ou o grupo de discos deve estar existente e disponibilizado no host.

a. Clique em **Reset** para obter as configurações padrão de parâmetros do banco de dados.

10. Na página PostOps, **Recover database** e **Until Cancel** são selecionados por padrão para executar a recuperação do banco de dados clonado.

O SnapCenter executa a recuperação montando o backup de log mais recente que tem a sequência ininterrupta de logs de arquivamento após o backup de dados que foi selecionado para clonagem. O backup de log e dados deve estar no storage primário para executar o clone no storage primário e o backup de dados deve estar no storage secundário para executar o clone no storage secundário.

As opções **Recover database** e **Until Cancel** não são selecionadas se o SnapCenter não conseguir encontrar os backups de log apropriados. Você pode fornecer o local de log de arquivamento externo se o backup de log não estiver disponível em **especificar locais de log de arquivamento externo**. Pode especificar vários locais de registro.



Se você quiser clonar um banco de dados de origem configurado para suportar a área de recuperação flash (FRA) e os arquivos gerenciados Oracle (OMF), o destino do log para recuperação também deve aderir à estrutura de diretórios OMF.

A página PostOps não será exibida se o banco de dados de origem for um banco de dados de espera do Data Guard ou um banco de dados de espera do ativo Data Guard. Para o modo de espera do Data Guard ou um banco de dados em espera do ativo Data Guard, o SnapCenter não fornece uma opção para selecionar o tipo de recuperação na GUI do SnapCenter, mas o banco de dados é recuperado usando até Cancelar o tipo de recuperação sem aplicar nenhum log.

Nome do campo	Descrição
Até Cancelar	O SnapCenter executa a recuperação montando o backup de log mais recente com a sequência ininterrupta de logs de arquivamento após esse backup de dados que foi selecionado para clonagem. O banco de dados clonado é recuperado até o arquivo de log ausente ou corrompido.
Data e hora	O SnapCenter recupera o banco de dados até uma data e hora especificadas. O formato aceite é mm/dd/aaaa hh:mm:ss.  A hora pode ser especificada no formato de 24 horas.
Até SCN (número de mudança do sistema)	O SnapCenter recupera o banco de dados até um número de mudança de sistema especificado (SCN).

Nome do campo	Descrição
Especifique locais de registro de arquivo externo	Se o banco de dados estiver sendo executado no modo ARCHIVELOG, o SnapCenter identifica e monta o número ideal de backups de log com base no SCN especificado ou na data e hora selecionadas. Também pode especificar a localização do registro de arquivo externo.  O SnapCenter não identificará e montará automaticamente os backups de log se você tiver selecionado até Cancelar.
Crie um novo DBID	Por padrão Create new DBID caixa de seleção está selecionada para gerar um número único (DBID) para o banco de dados clonado diferenciando-o do banco de dados de origem. Desmarque a caixa de seleção se quiser atribuir o DBID do banco de dados de origem ao banco de dados clonado. Nesse cenário, se você quiser Registrar o banco de dados clonado com o catálogo RMAN externo onde o banco de dados de origem já está registrado, a operação falha.
Crie o tempfile para o espaço de tabela temporário	Marque a caixa de seleção se quiser criar um arquivo tempfile para o espaço de tabela temporário padrão do banco de dados clonado. Se a caixa de seleção não estiver selecionada, o clone do banco de dados será criado sem o tempfile.
Insira entradas sql para aplicar quando o clone for criado	Adicione as entradas sql que você deseja aplicar quando o clone for criado.

Nome do campo	Descrição
Insira scripts para serem executados após a operação clone	Especifique o caminho e os argumentos do postscript que você deseja executar após a operação clone. Você deve armazenar o postscript em <code>/var/opt/SnapCenter/spl/scripts</code> ou em qualquer pasta dentro deste caminho. Por padrão, o caminho <code>/var/opt/SnapCenter/spl/scripts</code> é preenchido. Se você colocou o script em qualquer pasta dentro deste caminho, você precisa fornecer o caminho completo até a pasta onde o script é colocado.  Se a operação de clone falhar, os postscripts não serão executados e as atividades de limpeza serão acionadas diretamente.

11. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. Se quiser anexar o relatório da operação clone executada, selecione **Anexar Relatório de trabalho**.



Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando PowerShell `SET-SmtpServer`.

12. Revise o resumo e clique em **Finish**.



Ao executar a recuperação como parte da operação de criação de clone, mesmo que a recuperação falhe, o clone é criado com um aviso. Você pode executar a recuperação manual neste clone para colocar o banco de dados clone no estado consistente.

13. Monitorize o progresso da operação clicando em **Monitor > trabalhos**.

Resultado

Após a clonagem do banco de dados, você pode atualizar a página recursos para listar o banco de dados clonado como um dos recursos disponíveis para backup. O banco de dados clonado pode ser protegido como qualquer outro banco de dados usando o fluxo de trabalho de backup padrão ou pode ser incluído em um grupo de recursos (recém-criado ou existente). O banco de dados clonado pode ser clonado ainda mais (clone de clones).

Após a clonagem, você nunca deve renomear o banco de dados clonado.



Se você não tiver executado a recuperação durante a clonagem, o backup do banco de dados clonado pode falhar devido a uma recuperação inadequada, e talvez seja necessário executar a recuperação manual. O backup de log também pode falhar se o local padrão que foi preenchido para logs de arquivamento estiver em um armazenamento não NetApp ou se o sistema de armazenamento não estiver configurado com SnapCenter.

Na configuração AIX, você pode usar o comando `lkdev` para bloquear e o comando `rendev` para renomear os discos nos quais o banco de dados clonado residia.

O bloqueio ou a renomeação de dispositivos não afetará a operação de exclusão do clone. Para layouts de LVM AIX criados em dispositivos SAN, a renomeação de dispositivos não será suportada para os dispositivos SAN clonados.

Encontre mais informações

- ["Falha na restauração ou clonagem com a mensagem de erro ORA-00308"](#)
- ["Falha ao recuperar um banco de dados clonado"](#)
- ["Parâmetros personalizáveis para operações de backup, restauração e clone em sistemas AIX"](#)

Clone um banco de dados conetável

Você pode clonar um banco de dados conetável (PDB) para um CDB diferente ou mesmo destino no mesmo host ou host alternativo. Você também pode recuperar o PDB clonado para uma SCN ou data e hora desejadas.

Antes de começar

Se tiver instalado o plug-in como um utilizador não root, deve atribuir manualmente as permissões de execução aos diretórios `prescriitor` e `postscript`.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados do tipo instância única (multitenant) na exibição de detalhes do banco de dados ou na exibição de detalhes do grupo de recursos.

A página de topologia do banco de dados é exibida.

4. Na exibição Gerenciar cópias, selecione os backups de cópias locais (primárias), cópias espelhadas (secundárias) ou cópias do Vault (secundárias).
5. Selecione a cópia de segurança na tabela e, em seguida, clique em * .
6. Na página Nome, execute as seguintes ações:
 - a. Selecione **Clonar PDB**.
 - b. Especifique o PDB que você deseja clonar.



Você pode clonar apenas um PDB de cada vez.

- c. Especifique o nome do clone PDB.

7. Na página locais, execute as seguintes ações:

Para este campo...	Faça isso...
--------------------	--------------

Clone de host	Por padrão, o host do banco de dados de origem é preenchido. Se você quiser criar o clone em um host alternativo, selecione o host com a mesma versão do Oracle e do SO que o host do banco de dados de origem.
CDB alvo	Selecione o CDB onde deseja incluir o PDB clonado. Você deve garantir que o CDB alvo esteja em execução.
Estado da base de dados	Marque a caixa de seleção abrir o PDB clonado no modo DE LEITURA-GRAVAÇÃO se quiser abrir o PDB no modo DE LEITURA-GRAVAÇÃO.
Localizações de ficheiros de dados	Por padrão, a localização do arquivo de dados é preenchida. A convenção de nomenclatura padrão do SnapCenter para sistemas de arquivos SAN ou NFS é <code>FileSystemNameofsourcedatabase_SCJOBID</code>. A convenção de nomenclatura padrão do SnapCenter para grupos de discos ASM é <code>SC_HASHCODEofDISKGROUP_SCJOBID</code>. O <code>HASHCODEofDISKGROUP</code> é um número gerado automaticamente (2 a 10 dígitos) que é exclusivo para cada grupo de discos ASM.  Se você estiver personalizando o nome do grupo de discos ASM, certifique-se de que o comprimento do nome adere ao comprimento máximo suportado pela Oracle. Se você quiser especificar um caminho diferente, insira os pontos de montagem do arquivo de dados ou nomes de grupo de discos ASM para o banco de dados clone.

A casa, o nome de usuário e os detalhes do grupo do Oracle são preenchidos automaticamente a partir do banco de dados de origem. Você pode alterar os valores com base no ambiente Oracle do host onde o clone será criado.

8. Na página PreOps, execute as seguintes etapas:

- a. Insira o caminho e os argumentos do prescritor que você deseja executar antes da operação clone.

Você deve armazenar o prescritor em `/var/opt/SnapCenter/spl/scripts` ou em qualquer pasta dentro

deste caminho. Por padrão, o caminho `/var/opt/SnapCenter/spl/scripts` é preenchido. Se você colocou o script em qualquer pasta dentro deste caminho, você precisa fornecer o caminho completo até a pasta onde o script é colocado.

O SnapCenter permite-lhe utilizar as variáveis de ambiente predefinidas quando executa o prescritor e o postscript. "[Saiba mais](#)"

- a. Na seção Configurações de parâmetros do banco de dados clone CDB auxiliar , modifique os valores dos parâmetros do banco de dados pré-preenchidos que são usados para inicializar o banco de dados.
9. Clique em **Reset** para obter as configurações padrão de parâmetros do banco de dados.
10. Na página PostOps, **Until Cancel** é selecionado por padrão para executar a recuperação do banco de dados clonado.

A opção **Until Cancel** (até Cancelar) não é selecionada se o SnapCenter não conseguir encontrar os backups de log apropriados. Você pode fornecer o local de log de arquivamento externo se o backup de log não estiver disponível em **especificar locais de log de arquivamento externo**. Pode especificar vários locais de registo.



Se você quiser clonar um banco de dados de origem configurado para suportar a área de recuperação flash (FRA) e os arquivos gerenciados Oracle (OMF), o destino do log para recuperação também deve aderir à estrutura de diretórios OMF.

Nome do campo	Descrição
Até Cancelar	O SnapCenter executa a recuperação montando o backup de log mais recente com a sequência ininterrupta de logs de arquivamento após esse backup de dados que foi selecionado para clonagem. O backup de log e dados deve estar no storage primário para executar o clone no storage primário e o backup de dados deve estar no storage secundário para executar o clone no storage secundário. O banco de dados clonado é recuperado até o arquivo de log ausente ou corrompido.
Data e hora	O SnapCenter recupera o banco de dados até uma data e hora especificadas.  A hora pode ser especificada no formato de 24 horas.
Até SCN (número de mudança do sistema)	O SnapCenter recupera o banco de dados até um número de mudança de sistema especificado (SCN).
Especifique locais de registo de arquivo externo	Especifique a localização do log de arquivamento externo.

Nome do campo	Descrição
Crie um novo DBID	Por padrão a caixa de seleção criar novo DBID não está selecionada para o banco de dados de clones auxiliares. Marque a caixa de seleção se desejar gerar um número único (DBID) para o banco de dados clonado auxiliar diferenciando-o do banco de dados de origem.
Crie o tempfile para o espaço de tabela temporário	Marque a caixa de seleção se quiser criar um arquivo tempfile para o espaço de tabela temporário padrão do banco de dados clonado. Se a caixa de seleção não estiver selecionada, o clone do banco de dados será criado sem o tempfile.
Insira entradas sql para aplicar quando o clone for criado	Adicione as entradas sql que você deseja aplicar quando o clone for criado.
Insira scripts para serem executados após a operação clone	Especifique o caminho e os argumentos do postscript que você deseja executar após a operação clone. Você deve armazenar o postscript em <code>/var/opt/SnapCenter/spl/scripts</code> ou em qualquer pasta dentro deste caminho. Por padrão, o caminho <code>/var/opt/SnapCenter/spl/scripts</code> é preenchido. Se você colocou o script em qualquer pasta dentro deste caminho, você precisa fornecer o caminho completo até a pasta onde o script é colocado.  Se a operação de clone falhar, os postscripts não serão executados e as atividades de limpeza serão acionadas diretamente.

11. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. Se quiser anexar o relatório da operação clone executada, selecione **Anexar Relatório de trabalho**.



Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando PowerShell SET-SmtpServer.

12. Revise o resumo e clique em **Finish**.

13. Monitorize o progresso da operação clicando em **Monitor > trabalhos**.

Depois de terminar

Se você quiser criar um backup do PDB clonado, você deve fazer o backup do CDB de destino onde o PDB é clonado porque não é possível fazer backup apenas do PDB clonado. Você deve criar um relacionamento secundário para o CDB de destino se quiser criar o backup com relação secundária.

Em uma configuração RAC, o armazenamento para PDB clonado é anexado apenas ao nó onde o clone PDB foi executado. As PDBs nos outros nós do RAC estão no estado DE MONTAGEM. Se você quiser que o PDB clonado seja acessível a partir dos outros nós, anexe manualmente o storage aos outros nós.

Encontre mais informações

- ["Falha na restauração ou clonagem com a mensagem de erro ORA-00308"](#)
- ["Parâmetros personalizáveis para operações de backup, restauração e clone em sistemas AIX"](#)

Clonar backups de bancos de dados Oracle usando comandos UNIX

O fluxo de trabalho do clone inclui Planejamento, execução da operação do clone e monitoramento da operação.

Sobre esta tarefa

Você deve executar os seguintes comandos para criar o arquivo de especificação de clone de banco de dados Oracle e iniciar a operação de clone.

As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando `Get-Help command_name`. Em alternativa, pode também consultar o ["Guia de Referência de comandos do software SnapCenter"](#).

Passos

1. Crie uma especificação de clone de banco de dados Oracle a partir de um backup especificado: *New-SmOracleCloneSpecification*



Se a política de proteção de dados secundária for unificada mirror-Vault, especifique somente `-IncludeSecondaryDetails`. Você não precisa especificar `-SecondaryStorageType`.

Esse comando cria automaticamente um arquivo de especificação de clone de banco de dados Oracle para o banco de dados de origem especificado e seu backup. Você também deve fornecer um SID de banco de dados clone para que o arquivo de especificação criado tenha os valores gerados automaticamente para o banco de dados clone que você estará criando.



O arquivo de especificação do clone é criado em `/var/opt/SnapCenter/SCO/clone_specs`.

2. Inicie uma operação de clone a partir de um grupo de recursos clone ou de um backup existente: *New-SmClone*

Este comando inicia uma operação clone. Você também precisa fornecer um caminho de arquivo de especificação de clone do Oracle para a operação de clone. Você também pode especificar as opções de recuperação, o host onde a operação de clone a ser executada, as prescrições, os postscripts e outros detalhes.

Por padrão, o arquivo de destino do log de arquivamento para o banco de dados clone é preenchido automaticamente em ORACLE_Home/CLONE_SIDs_.

Divida um clone do banco de dados Oracle

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido torna-se independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clones em um clone intermediário.

Por exemplo, depois de criar clone1 a partir de um backup de banco de dados, você pode criar um backup de clone1 e clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e não é possível executar a operação de divisão de clones no clone1. No entanto, você pode executar a operação de divisão de clones no clone2.

Depois de dividir clone2, você pode executar a operação de divisão de clones no clone1 porque clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup do clone são excluídas.
- Para obter informações sobre limitações de operação de divisão de clones, consulte ["Guia de gerenciamento de storage lógico do ONTAP 9"](#).
- Certifique-se de que o volume ou o agregado no sistema de storage esteja on-line.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** na lista **Exibir**.
3. Selecione o recurso clonado (por exemplo, o banco de dados ou LUN) e clique  em .
4. Revise o tamanho estimado do clone que deve ser dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
5. Monitorize o progresso da operação clicando em **Monitor > trabalhos**.

A operação de divisão de clones deixa de responder se o serviço SMCORE for reiniciado e os bancos de dados nos quais a operação de divisão de clones foi executada são listados como clones na página recursos. Você deve executar o cmdlet *Stop-SmJob* para interromper a operação de divisão de clones e tentar novamente a operação de divisão de clones.

Se você quiser um tempo de enquete mais longo ou menor para verificar se o clone está dividido ou não, você pode alterar o valor do parâmetro CloneSplitStatusCheckPollTime no arquivo SMCOREServiceHost.exe.config para definir o intervalo de tempo para que o SMCORE busque o status da operação de divisão de clones. O valor é em milissegundos e o valor padrão é de 5 minutos.

Por exemplo,

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```



A operação de inicialização dividida do clone falha se o backup, a restauração ou a divisão do clone do outro estiverem em andamento. Você deve reiniciar a operação de divisão de clones somente depois que as operações em execução estiverem concluídas.

Clone dividido de um banco de dados conetável

Você pode usar o SnapCenter para dividir um banco de dados conetável clonado (PDB).

Sobre esta tarefa

Se você criou um backup do CDB de destino onde o PDB é clonado, quando você divide o clone do PDB, o PDB clonado também será removido de todos os backups do CDB de destino que contém o PDB clonado.



Os clones PDB não são exibidos na exibição de inventário ou recursos.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Selecione a base de dados de contentor de origem (CDB) na vista de grupo de recursos ou recursos.
3. Na exibição Gerenciar cópias, selecione **clones** nos sistemas de storage primário ou secundário (espelhado ou replicado).
4. Selecione o clone PDB (targetCDB:PDBClone) e clique  em .
5. Revise o tamanho estimado do clone que deve ser dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
6. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Monitorar operações de clone de banco de dados Oracle

Você pode monitorar o andamento das operações de clone do SnapCenter usando a página tarefas. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

-  Em curso
-  Concluído com êxito
-  Falha
-  Preenchido com avisos ou não foi possível iniciar devido a avisos
-  Em fila de espera
-  Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.

2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
 - a. Clique  para filtrar a lista para que apenas operações de clone sejam listadas.
 - b. Especifique as datas de início e fim.
 - c. Na lista suspensa **Type**, selecione **Clone**.
 - d. Na lista suspensa **Status**, selecione o status do clone.
 - e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione a tarefa clone e clique em **Detalhes** para exibir os detalhes da tarefa.
5. Na página Detalhes da tarefa, clique em **Exibir logs**.

Atualize um clone

Você pode atualizar o clone executando o comando *Refresh-SmClone*. Esse comando cria um backup do banco de dados, exclui o clone existente e cria um clone com o mesmo nome.



Não é possível atualizar um clone PDB.

O que você vai precisar

- Crie um backup completo online ou uma política de backup de dados offline sem backups programados ativados.
- Configure a notificação por e-mail na política apenas para falhas de backup.
- Defina a contagem de retenção para os backups sob demanda adequadamente para garantir que não haja backups indesejados.
- Certifique-se de que apenas um backup completo on-line ou uma política de backup de dados off-line esteja associada ao grupo de recursos identificado para a operação de clone de atualização.
- Crie um grupo de recursos com apenas um banco de dados.
- Se um cron job for criado para o comando clone refresh, certifique-se de que as programações do SnapCenter e as programações do cron não estejam sobrepostas para o grupo de recursos do banco de dados.

Para uma tarefa cron criada para o comando clone refresh, certifique-se de executar o Open-SmConnection a cada 24hrs.

- Certifique-se de que o SID clone seja exclusivo para um host.

Se várias operações de clone de atualização usarem o mesmo arquivo de especificação de clone ou usarem o arquivo de especificação de clone com o mesmo SID de clone, o clone existente com o SID no host será excluído e o clone será criado.

- Certifique-se de que a política de backup esteja habilitada com proteção secundária e que o arquivo de especificação do clone seja criado com `"-IncludeSecondaryDetails"` para criar os clones usando backups secundários.
 - Se o arquivo de especificação do clone primário for especificado, mas a política tiver a opção de atualização secundária selecionada, o backup será criado e a atualização será transferida para o secundário. No entanto, o clone será criado a partir do backup principal.

- Se o arquivo de especificação do clone primário for especificado e a política não tiver a opção de atualização secundária selecionada, o backup será criado no primário e o clone será criado do primário.

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado: *Open-SmConnection*
2. Crie uma especificação de clone de banco de dados Oracle a partir de um backup especificado: *New-SmOracleCloneSpecification*



Se a política de proteção de dados secundária for unificada mirror-Vault, especifique somente `-IncludeSecondaryDetails`. Você não precisa especificar `-SecondaryStorageType`.

Esse comando cria automaticamente um arquivo de especificação de clone de banco de dados Oracle para o banco de dados de origem especificado e seu backup. Você também deve fornecer um SID de banco de dados clone para que o arquivo de especificação criado tenha os valores gerados automaticamente para o banco de dados clone que você estará criando.



O arquivo de especificação do clone é criado em `/var/opt/SnapCenter/SCO/clone_specs`.

3. Execute *Refresh-SmClone*.

Se a operação falhar com as mensagens de erro "PL-SCO-20032: CanExecutar falha com erro: PL-SCO-30031: Refazer arquivo de log -SC_2959770772_clmdb/clmdb/redolog/redo01_01.log exists", especifique um valor mais alto para `-WaitToTriggerClone`.

Para obter informações detalhadas sobre comandos UNIX, consulte ["Guia de Referência de comandos do software SnapCenter"](#).

Excluir clone de um banco de dados conetável

Você pode excluir o clone de um banco de dados conetável (PDB) se não precisar mais.

Se você criou um backup do CDB de destino onde o PDB é clonado, quando você exclui o clone do PDB, o PDB clonado também é removido do backup do CDB de destino.



Os clones PDB não são exibidos na exibição de inventário ou recursos.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Selecione a base de dados de contentor de origem (CDB) na vista de grupo de recursos ou recursos.
3. Na exibição Gerenciar cópias, selecione **clones** nos sistemas de storage primário ou secundário (espelhado ou replicado).
4. Selecione o clone PDB (targetCDB:PDBClone) e clique  em .
5. Clique em **OK**.

Gerenciar volumes de aplicações

Adicionar volumes de aplicações

O SnapCenter é compatível com backup e clonagem de volumes de aplicações de banco de dados Oracle. Você deve adicionar manualmente os volumes de aplicativos. A detecção automática de volumes de aplicações não é suportada.



Os volumes de aplicações são compatíveis apenas com conexões diretas NFS e iSCSI.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in Oracle Database na lista.
2. Clique em **Add Application volume** (Adicionar volume da aplicação).
3. Na página Nome, execute as seguintes ações:
 - No campo Nome , introduza o nome do volume da aplicação.
 - No campo Nome do host , digite o nome do host.
4. Na página espaço físico do armazenamento, insira o nome do sistema de armazenamento, selecione um ou volumes e especifique os LUNs ou Qtrees associados.

Você pode adicionar vários sistemas de storage.

5. Revise o resumo e clique em **Finish**.
6. Na página recursos, selecione **volume do aplicativo** na lista **Exibir** para exibir todos os volumes de aplicativos adicionados.

Modificar o volume da aplicação

Você pode modificar todos os valores especificados ao adicionar o volume do aplicativo, se não forem criados backups. Se o backup for criado, você só poderá modificar os detalhes do sistema de armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in Oracle Database na lista.
2. Na página recursos, selecione **volume do aplicativo** na lista **Exibir**.
3.  Clique  em para modificar os valores.

Eliminar volume da aplicação

Quando você exclui um volume de aplicativo, se houver backups associados ao volume do aplicativo, o volume do aplicativo será colocado em modo de manutenção e nenhum novo backup será criado e nenhum backup anterior será retido. Se não houver backups associados, todos os metadados serão excluídos.

Se necessário, o SnapCenter permite anular a operação de eliminação.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in Oracle Database na lista.

2. Na página recursos, selecione **volume do aplicativo** na lista **Exibir**.
3. Clique  em para modificar os valores.

Volumes de aplicações de backup

Fazer backup do volume do aplicativo

Se o volume do aplicativo não fizer parte de qualquer grupo de recursos, você poderá fazer backup do volume do aplicativo na página recursos.

Sobre esta tarefa

Por padrão, backups do grupo de consistência (CG) são criados. Se você quiser criar backups baseados em volume, defina o valor de **EnableOracleNdvVolumeBasedBackup** como verdadeiro no arquivo *web.config*.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in Oracle Database na lista.
2. Na página recursos, selecione **volume do aplicativo** na lista **Exibir**.
3. Clique em  e selecione o nome do host e o tipo de banco de dados para filtrar os recursos.

Em seguida, pode clicar em  * para fechar o painel do filtro.

4. Selecione o volume da aplicação que pretende efetuar uma cópia de segurança.

É apresentada a página de proteção do volume da aplicação.

5. Na página recurso, execute as seguintes ações:

Para este campo...	Faça isso...
Use o formato de nome personalizado para cópia Snapshot	Marque essa caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome da cópia Instantânea. Por exemplo, customtext__policy_hostname ou resource_hostname. Por padrão, um carimbo de data/hora é anexado ao nome da cópia Snapshot.
Excluir destinos de log de arquivamento do backup	Especifique os destinos dos ficheiros de registo de arquivo que não pretende efetuar uma cópia de segurança.

6. Na página políticas, execute as seguintes etapas:

- a. Selecione uma ou mais políticas na lista suspensa.



Você também pode criar uma política clicando  em .

Na seção Configurar agendas para políticas selecionadas, as políticas selecionadas são listadas.

- b. Clique  na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.
- c. Na janela Adicionar programações para a política *policy_name*, configure a programação e clique em **OK**.

policy_name é o nome da política selecionada.

As programações configuradas são listadas na coluna agendas aplicadas.

- 7. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. Se você quiser anexar o relatório da operação de backup realizada no recurso e selecione **Anexar Relatório de trabalho**.



Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando PowerShell SET-SmtpServer.

- 8. Revise o resumo e clique em **Finish**.

É apresentada a página topologia do volume da aplicação.

- 9. Clique em **fazer backup agora**.

- 10. Na página Backup, execute as seguintes etapas:

- a. Se você tiver aplicado várias políticas ao recurso, na lista suspensa **Política**, selecione a política que deseja usar para backup.
- b. Clique em **Backup**.

- 11. Monitorize o progresso da operação clicando em **Monitor > trabalhos**.

Faça backup do grupo de recursos volumes de aplicativos

É possível fazer backup do grupo de recursos que contém apenas volumes de aplicativos ou uma combinação de volumes de aplicativos e banco de dados. Uma operação de backup no grupo de recursos é executada em todos os recursos definidos no grupo de recursos.

Se o grupo de recursos tiver vários volumes de aplicações, todos os volumes de aplicações deverão ter uma política de replicação do SnapMirror ou do SnapVault.

Sobre esta tarefa

Por padrão, backups do grupo de consistência (CG) são criados. Se você quiser criar backups baseados em volume, defina o valor de **EnableOracleNdvVolumeBasedBackup** como verdadeiro no arquivo *web.config*.

Passos

- 1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in Oracle Database na lista.
- 2. Na página recursos, selecione **Grupo de recursos** na lista **Exibir**.

Você pode pesquisar o grupo de recursos inserindo o nome do grupo de recursos na caixa de pesquisa ou clicando em  e, em seguida, selecionando a tag. Em seguida, pode clicar em  para fechar o painel do filtro.

3. Na página grupos de recursos, selecione o grupo de recursos que deseja fazer backup e clique em **fazer backup agora**.
4. Na página Backup, execute as seguintes etapas:
 - a. Se você associou várias políticas ao grupo de recursos, na lista suspensa **Política**, selecione a política que deseja usar para backup.

Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.
 - b. Clique em **Backup**.
5. Monitorize o progresso da operação clicando em **Monitor > trabalhos**.



A operação de verificação será realizada apenas para os bancos de dados e não para os volumes de aplicativos.

Clone o backup de volume de aplicativo

Você pode usar o SnapCenter para clonar os backups de volume de aplicações.

Antes de começar

Se tiver instalado o plug-in como um utilizador não root, deve atribuir manualmente as permissões de execução aos diretórios prescitor e postscript.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in Oracle Database na lista.
2. Na página recursos, selecione **volume do aplicativo** na lista **Exibir**.
3. Selecione o volume da aplicação na vista de detalhes do volume da aplicação ou na vista de detalhes do grupo de recursos.

É apresentada a página topologia do volume da aplicação.
4. Na exibição Gerenciar cópias, selecione os backups de cópias locais (primárias), cópias espelhadas (secundárias) ou cópias do Vault (secundárias).
5. Selecione a cópia de segurança na tabela e, em seguida, clique em .
6. Na página localização, execute as seguintes ações:

Para este campo...	Faça isso...
Host plug-in	Selecione o host onde você deseja criar o clone.
Nome recurso alvo	Especifique o nome do recurso.

7. Na página Scripts, especifique os nomes dos scripts a serem executados antes da clonagem, comandos para montar um sistema de arquivos e nomes dos scripts a serem executados após a clonagem.
8. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. Se quiser anexar o relatório da operação clone executada, selecione **Anexar Relatório de trabalho**.



Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando PowerShell SET-SmtpServer.

9. Revise o resumo e clique em **Finish**.

Dividir um clone de volume de aplicativo

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido torna-se independente do recurso pai.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in Oracle Database na lista.
2. Na página recursos, selecione **volume do aplicativo** na lista **Exibir**.
3. Selecione o recurso clonado e clique  em .
4. Revise o tamanho estimado do clone que deve ser dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
5. Monitorize o progresso da operação clicando em **Monitor > trabalhos**.

Excluir um clone de volume de aplicativo

Você pode excluir clones se você achar que eles não são mais necessários. Não é possível excluir clones que atuam como fonte para outros clones.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in Oracle Database na lista.
2. Na página recursos, selecione **volume do aplicativo** na lista **Exibir**.
3. Selecione o recurso ou grupo de recursos na lista.

A página de topologia do recurso ou do grupo de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **clones** nos sistemas de storage primário ou secundário (espelhado ou replicado).
5. Selecione o clone e clique  em .
6. Na página Excluir clone, execute as seguintes ações:
 - a. No campo **Pré-clone delete**, insira os nomes dos scripts a serem executados antes de excluir o clone.
 - b. No campo **Desmontar**, digite os comandos para desmontar o clone antes de excluir o clone.
7. Clique em **OK**.

Informações sobre direitos autorais

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

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

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTE; 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.