Fazer backup de bancos de dados Oracle

SnapCenter software

NetApp
November 06, 2025

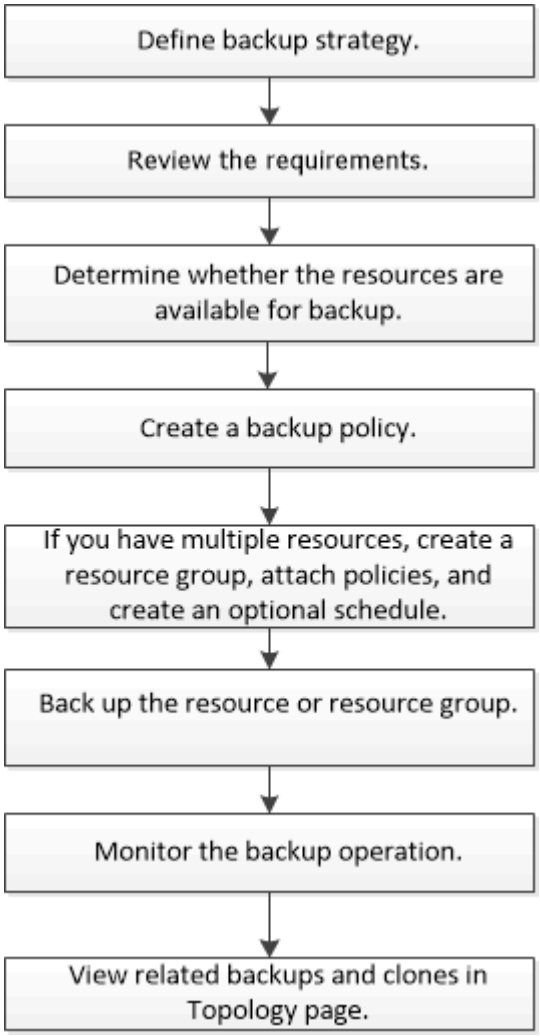
Índice

Fazer 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 anexação 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 do 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.

Entretanto, 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 até */var/opt/snapcenter/sco/lock*.
2. Exclua o bloqueio operacional:`rm -rf .sm_lock_dbsid.`

Informações de configuração de backup

Configurações de banco de dados Oracle suportadas para backups

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

- Oracle autônomo
- Clusters de aplicativos reais Oracle (RAC)
- Oracle Standalone Legacy
- Banco de Dados de Contêineres Autônomos Oracle (CDB)
- Oracle Data Guard em espera

  Você só pode criar backups de montagem offline de bancos de dados standby do Data Guard. Backup com desligamento offline, backup somente de log de arquivo e backup completo não são suportados.

- Oracle Active Data Guard em espera

  Você só pode criar backups on-line de bancos de dados em espera do Active Data Guard. O backup somente do log de arquivo e o backup completo não são suportados.

  Antes de criar um backup do banco de dados Data Guard standby ou Active Data Guard standby, o processo de recuperação gerenciada (MRP) é interrompido e, depois que o backup é criado, o MRP é iniciado.

- Gerenciamento Automático de Armazenamento (ASM)
  - ASM autônomo e ASM RAC em disco de máquina virtual (VMDK)

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

  - ASM autônomo e ASM RAC no mapeamento de dispositivos Raw (RDM) + Você pode executar operações de backup, restauração e clonagem em bancos de dados Oracle no ASM, com ou sem ASMLib.
  - Driver de filtro Oracle ASM (ASMFD)

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

  - Oracle Flex ASM

Para obter as informações mais recentes sobre as versões Oracle suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Tipos de backup suportados para bancos de dados Oracle

O tipo de backup especifica o tipo de backup que você deseja criar. O SnapCenter oferece suporte a tipos de backup online e offline para bancos de dados Oracle.

Backup on-line

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

Como parte do backup online, você pode criar um backup dos seguintes arquivos:

- Somente arquivos de dados e arquivos de controle
- Somente arquivos de log de arquivamento (o banco de dados não é colocado no modo de backup neste cenário)
- Banco de dados completo que inclui arquivos de dados, arquivos de controle e arquivos de log de arquivamento

Backup offline

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

- Ao criar um backup de montagem offline, 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 offline, o banco de dados pode estar em qualquer estado.

  O estado do banco de dados é alterado para o estado necessário para criar um backup. Após criar o backup, o estado do banco 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 11*g* a 12*c*R1

Banco 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 independentes são descobertos apenas com base nas entradas /etc/oratab.

ASM

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

RAC Um Nó

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

O status do banco de dados do RAC One Node será marcado como renomeado ou excluído se o banco de dados já tiver sido descoberto e houver backups 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 realocado no arquivo /etc/oratab no nó RAC com failover.
2. Atualize 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 preferenciais para o nó RAC que atualmente hospeda o banco de dados.
5. Execute as operações do SnapCenter .
6. Se você tiver realocado um banco de dados de um nó para outro 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, 19c ou 21c

Banco 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 independentes são descobertos com base nas entradas no arquivo /etc/oratab e na saída do comando srvctl config.

ASM

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

RAC Um Nó

Os bancos de dados do RAC One Node são descobertos usando somente o comando srvctl config. Os bancos de dados devem estar no estado nomount, mount ou open. O status do banco de dados do RAC One Node será marcado como renomeado ou excluído se o banco de dados já tiver sido descoberto e houver backups associados ao banco de dados.

Você deve executar as seguintes etapas se o banco de dados for realocado: . Atualize 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 preferenciais para o nó RAC que atualmente hospeda o banco de dados. . Execute as operações do SnapCenter .

Se houver entradas de banco de dados Oracle 12*c*R2 e 18*c* no arquivo /etc/oratab e o mesmo banco de dados for registrado com o comando srvctl config, o SnapCenter eliminará as entradas duplicadas do banco de dados. Se houver entradas desatualizadas no banco de dados, o banco de dados será descoberto, mas ficará inacessível e o status será offline.

Nós preferenciais na configuração do RAC

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

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

Exemplo

O banco de dados RAC cdbrac tem três instâncias: cdbrac1 no nó 1, cdbrac2 no nó 2 e cdbrac3 no nó 3.

As instâncias node1 e node2 são configuradas para serem os nós preferenciais, com node2 como a primeira preferência e node1 como a segunda preferência. Quando você executa uma operação de backup, a operação é tentada primeiro no nó2 porque é o primeiro nó preferencial.

Se o node2 não estiver no estado para fazer backup, o que pode ocorrer por vários motivos, como o agente do plug-in não estar em execução no host, a instância do banco de dados no host não estar no estado necessário para o tipo de backup especificado ou a instância do banco de dados no node2 em uma configuração FlexASM não estar sendo atendida pela instância do ASM local; 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 nós Leaf não serão listados como nós preferenciais se a cardinalidade for menor que o número de nós no cluster RAC. Se houver alguma alteração nas funções dos nós do cluster Flex ASM, você deverá descobri-las manualmente para que os nós preferenciais sejam atualizados.

Estado do banco 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 sucesso:

- Uma das instâncias do banco de dados RAC nos nós preferenciais configurados deve estar no estado aberto para criar um backup online.
- 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 inferior para criar um backup de montagem offline.
- As instâncias do banco de dados RAC podem estar em qualquer estado, mas você deve especificar os nós preferenciais para criar um backup de desligamento offline.

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 pontual de tablespace. Quando você não precisar desses backups catalogados, poderá remover as informações do catálogo.

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

Se você quiser catalogar backups de um banco de dados RAC, certifique-se de que nenhuma outra tarefa esteja em execução para esse banco de dados. Se outra tarefa estiver em execução, a operação de catalogação falhará em vez de ser enfileirada.

Banco de dados de catálogo externo

Por padrão, o arquivo de controle do banco de dados de destino é usado para catalogação. Se desejar adicionar um banco de dados de catálogo externo, você poderá configurá-lo especificando a credencial e o nome do Transparent Network Substrate (TNS) do catálogo externo usando o assistente de configurações de banco de dados na interface gráfica do usuário (GUI) do SnapCenter . Você também pode configurar o banco de dados de catálogo externo a partir da CLI executando o comando Configure-SmOracleDatabase com as opções -OracleRmanCatalogCredentialName e -OracleRmanCatalogTnsName.

Comando RMAN

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

Após catalogar os backups, você pode executar o `Get-SmBackupDetails` comando para obter as informações de backup catalogadas, como a tag para arquivos de dados 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 será SC_HASHCODEofDISKGROUP_DBSID_BACKUPID. No entanto, se o nome do grupo de discos tiver menos de 16 caracteres, o formato de nomenclatura usado para o backup será 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 desatualizadas do repositório RMAN sobre backups cujos registros de 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 indicará que os logs estão no disco, quando na verdade não estão.

A operação de verificação cruzada permite que você atualize o arquivo de controle com as informações. Você pode habilitar a verificação cruzada executando o comando Set-SmConfigSettings e atribuindo o valor TRUE ao parâmetro ENABLE_CROSSCHECK. O valor padrão é definido como FALSO.

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings
```

```
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

Remover 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 durante a exclusão do backup ou durante a exclusão do grupo de retenção e recursos associado a esse backup catalogado.

> Quando você força a 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 deverá 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"
```

Após 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. Alternativamente, você pode consultar o "Guia de referência de comandos do software SnapCenter" .

Variáveis de ambiente predefinidas para prescript e postscript específicos de backup

O SnapCenter permite que você use as variáveis de ambiente predefinidas ao executar o prescript e o postscript ao criar políticas de backup. Essa funcionalidade é suportada por todas as configurações do Oracle, exceto VMDK.

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

Variáveis de ambiente predefinidas com suporte para criação de política de backup

- **SC_JOB_ID** especifica o ID do trabalho 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 bancos de dados separados por barra vertical.

  Este 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 será executado.

  Este 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@oracle|NFSB32@oracle

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

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

  Exemplo: NFSB31@install|NFSB32@oinstall

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

  Exemplos:

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

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

  Este 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 do backup.

  Este parâmetro será preenchido para volumes de aplicativos.

  Exemplo: DADOS@203|LOG@205|AV@207

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

  Exemplo: NFSB32@/ora01/app/oracle/product/18.1.0/db_1|NFSB31@/ora01/app/oracle/product/18.1.0/db_1

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

  Exemplos:

  - Para backup completo: De hora em hora|DADOS@DIAS:3|LOG@CONTAGEM:4

    - Para backup de dados somente sob demanda: Ondemand|DATA@COUNT:2
    - Para backup somente de log sob demanda: Ondemand|LOG@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 do aplicativo.

  Exemplo: AV1|AV2

- **SC_PRIMARY_DATA_VOLUME_FULL_PATH** especifica o mapeamento de armazenamento do SVM para o volume do 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 2 bancos de dados no mesmo grupo de recursos: NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA
    - Para um único banco de dados com arquivos de dados distribuídos em vários volumes: buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA,herculus:/vol/scspr2417819002_NFS
- **SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH** especifica o mapeamento de armazenamento do SVM para o volume do diretório de arquivos de logs. Será o nome do volume pai para luns e qtrees.

  Exemplos:

    - Para instância de banco de dados única: buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO
    - Para múltiplas instâncias de banco de dados: NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO|NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO
- **SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG** especifica a lista de Snapshots contendo o nome do sistema de armazenamento e o nome do volume.

  Exemplos:

    - Para instância de banco de dados única: 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@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
    |NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

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

  Exemplos:

  - Para instância de banco de dados única: 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_02.28.26.3973_1|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
  - Para instantâneos de grupo de consistência que envolvem 2 volumes: cg3_R80404CBEF5V1_04-05-2021_03.08.03.4945_0_bfc279cc-28ad-465c-9d60-5487ac17b25d_2021_4_5_3_8_58_350
- **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 sob 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 instância de banco de dados única: /mnt/nfsdb3_data,/mnt/nfsdb3_log,/mnt/nfsdb3_data1
  - Para várias instâncias de banco de dados: NFSB31@/mnt/nfsdb31_data,/mnt/nfsdb31_log,/mnt/nfsdb31_data1|NFSB32@/mnt/nfsdb32_data,/mnt/nfsdb32_log,/mnt/nfsdb32_data1
  - Para ASM: +DATA2DG,+LOG2DG
- **SC_PRIMARY_SNAPSHOTS_AND_MOUNT_POINTS** especifica os nomes dos snapshots criados durante o backup de cada um dos pontos de montagem.

  Exemplos:

  - Para instância de banco de dados única: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_data,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_log
  - Para múltiplas instâncias de banco de dados: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_data,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_log|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb31_data,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb32_log
- **SC_ARCHIVELOGS_LOCATIONS** especifica o local do diretório de logs de arquivamento.

  Os nomes dos diretórios serão os pais imediatos dos arquivos de log de arquivamento. Se os logs de arquivamento forem colocados em mais de um local, todos os locais serão capturados. Isso também inclui os cenários FRA. Se softlinks forem usados para o diretório, o mesmo será preenchido.

  Exemplos:

  - Para banco de dados único no NFS: /mnt/nfsdb2_log

- Para vários bancos de dados no NFS e para os logs de arquivamento do banco de dados NFSB31 que são colocados em dois locais diferentes: NFSB31@/mnt/nfsdb31_log1,/mnt/nfsdb31_log2|NFSB32@/mnt/nfsdb32_log
- Para ASM: +LOG2DG/ASMDB2/ARCHIVELOG/2021_07_15

- **SC_REDO_LOGS_LOCATIONS** especifica o local do diretório de logs de refazer.

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

  Exemplos:

  - Para banco de dados único no NFS: /mnt/nfsdb2_data/newdb1
  - Para vários bancos de dados no NFS: NFSB31@/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/newdb32
  - Para ASM: +LOG2DG/ASMDB2/ONLINELOG

- **SC_CONTROL_FILES_LOCATIONS** especifica o local do diretório dos arquivos de controle.

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

  Exemplos:

  - Para banco de dados único no NFS: /mnt/nfsdb2_data/fra/newdb1,/mnt/nfsdb2_data/newdb1
  - Para vários bancos de dados no NFS: NFSB31@/mnt/nfsdb31_data/fra/newdb31,/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/fra/newdb32,/mnt/nfsdb32_data/newdb32
  - Para ASM: +LOG2DG/ASMDB2/CONTROLFILE

- **SC_DATA_FILES_LOCATIONS"** especifica o local do diretório dos arquivos de dados.

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

  Exemplos:

  - Para banco de dados único no NFS: /mnt/nfsdb3_data1,/mnt/nfsdb3_data/NEWDB3/datafile
  - Para vários bancos de dados no NFS: NFSB31@/mnt/nfsdb31_data1,/mnt/nfsdb31_data/NEWDB31/datafile|NFSB32@/mnt/nfsdb32_data1,/mnt/nfsdb32_data/NEWDB32/datafile
  - Para ASM: +DATA2DG/ASMDB2/DATAFILE,+DATA2DG/ASMDB2/TEMPFILE

- **SC_SNAPSHOT_LABEL** especifica o nome dos rótulos secundários.

  Exemplos: por hora, diariamente, semanalmente, mensalmente ou rótulo personalizado.

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 dados do nome do banco de dados e para separar o valor da sua chave.

  Exemplos:

  - NFSB32@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 |NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
  - NFSB31@oracle|NFSB32@oracle
- **|** 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_RETENTION e SC_BACKUP_NAME.

  Exemplos:

  - DADOS@203|LOG@205
  - Por hora|DADOS@DIAS:3|LOG@CONTAGEM:4
  - DADOS@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 seu Snapshot para os parâmetros SC_PRIMARY_SNAPSHOT_NAMES e SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG.

  Exemplo: NFSB32@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 conjuntos de variáveis para o mesmo banco de dados.

  Exemplo: NFSB32@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 |NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

Opções de retenção de backup

Você pode escolher o número de dias pelos quais deseja manter cópias de backup ou especificar o número de cópias de backup que deseja manter, até um máximo ONTAP de 255 cópias. Por exemplo, sua organização pode exigir que você mantenha 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 foi alterado para o recurso ou grupo de recursos, os backups com o rótulo de tipo de agendamento antigo ainda poderão permanecer no sistema.

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

Agendamentos de backup

A frequência de backup (tipo de agendamento) é especificada nas políticas; um agendamento de backup é especificado na configuração do grupo de recursos. O fator mais crítico na determinação da 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 utilizado a cada hora, enquanto pode fazer backup de um recurso raramente utilizado uma vez por dia. Outros fatores incluem a importância do recurso para sua organização, seu Acordo de Nível de Serviço (SLA) e seu Objetivo de Ponto de Recuperação (RPO).

Um SLA define o nível de serviço esperado e aborda muitas questões relacionadas ao serviço, incluindo a disponibilidade e o desempenho do serviço. Um RPO define a estratégia para a idade dos arquivos que devem ser recuperados do armazenamento 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 utilizado, não há necessidade de executar um backup completo mais de uma ou duas vezes por dia. Por exemplo, backups regulares do log de transações podem ser suficientes para garantir que você tenha os backups necessários. Quanto mais você fizer backup dos seus bancos de dados, menos logs de transações o SnapCenter terá que usar no momento da restauração, o que pode resultar em operações de restauração mais rápidas.

Os agendamentos de backup têm duas partes, conforme a seguir:

- Frequência de backup

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

- Agendamentos de backup

  Os agendamentos 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 com uma política configurada para backups semanais, poderá configurar o agendamento para fazer backup toda quinta-feira às 22h. Você pode acessar as programações dos grupos de recursos clicando em **Recursos** > **Grupos de Recursos**.

Convenções de nomenclatura de backup

Você pode usar a convenção de nomenclatura padrão do Snapshot ou usar uma convenção de nomenclatura personalizada. A convenção de nomenclatura de backup padrão adiciona um registro de data e hora aos nomes de instantâneos que ajuda a

identificar quando as cópias foram criadas.

O 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 registro de data e hora.

Como alternativa, você pode especificar o formato do nome do Snapshot ao proteger recursos ou grupos de recursos selecionando **Usar formato de nome personalizado para cópia do Snapshot**. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, o sufixo do registro de data e hora é adicionado ao nome do Snapshot.

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 atendidos.

- Você deve ter criado um grupo de recursos com uma política anexada.
- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, 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 armazenamento (SVM) usada pelo banco de dados.
- Você deve ter verificado se todos os volumes de dados e volumes de log de arquivamento pertencentes ao banco de dados estão protegidos se a proteção secundária estiver habilitada para esse banco de dados.
- Você deve ter verificado se o banco de dados que contém 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 se 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:\Program Files\ NetApp \SMCore\SMCoreServiceHost.exe.config* no host do SnapCenter Server, se o banco de dados que está sendo feito backup for grande (tamanho em TBs).

  Ao modificar os valores, certifique-se de que não haja trabalhos em execução e reinicie o serviço SnapCenter SMCore após 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.

Antes de começar

- Você deve ter concluído tarefas como instalar o SnapCenter Server, adicionar hosts, criar conexões do sistema de armazenamento 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 SnapCenter Plug-in for VMware vSphere e registrar o plug-in com o SnapCenter.

  Para obter mais informações, consulte "Implantar o SnapCenter Plug-in for VMware vSphere" .
- Se os bancos de dados residirem em um sistema de arquivos VMDK, você deverá ter efetuado login no vCenter e navegado até **Opções da 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.

Etapa 1: impedir que o SnapCenter descubra entradas que não sejam do banco de dados

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

Passos

1. Após instalar o plug-in para Oracle, o usuário root deve criar o arquivo **sc_oratab.config** no diretório */var/opt/snapcenter/sco/etc/*.

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

2. O administrador do banco de dados deve adicionar as entradas que não são do banco de dados no arquivo **sc_oratab.config**.

   É recomendável manter o mesmo formato definido para as entradas não pertencentes ao banco de dados no arquivo */etc/oratab* ou o usuário pode simplesmente adicionar a string de entidade não pertencente ao banco de dados.

   A sequência diferencia maiúsculas de minúsculas. Qualquer texto com # no início é tratado como um comentário. O comentário pode ser anexado após o nome que não seja do 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 pertencentes ao 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 .

Etapa 2: Descubra recursos

Após instalar o plug-in, todos os bancos de dados naquele host são descobertos automaticamente e exibidos na página Recursos.

Os bancos de dados devem estar pelo menos no estado montado ou superior para que a descoberta dos bancos de dados seja bem-sucedida. Em um ambiente Oracle Real Application Clusters (RAC), a instância do banco de dados RAC no host onde a descoberta é realizada deve estar pelo menos no estado montado ou superior para que a descoberta da instância do banco de dados seja bem-sucedida. Somente os bancos de dados descobertos com sucesso podem ser adicionados aos grupos de recursos.

Se você tiver excluído um banco de dados Oracle no host, o SnapCenter Server não saberá 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 **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** na lista **Exibir**.

   Clique ícone do filtro] e selecione o nome do host e o tipo de banco de dados para filtrar os recursos. Você pode então clicar no ícone imagfilter_icon.gif[ícone de filtro]_icon.png[] 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 ele está hospedado atualmente.

Resultados

Os bancos de dados são exibidos junto com informações como tipo de banco de dados, nome do host ou

cluster, grupos de recursos e políticas 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 não 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 armazenamento não 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 protegido na coluna Status 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 de recursos. Você deve configurar as credenciais do banco de dados para poder proteger o banco de dados ou adicioná-lo ao grupo de recursos para executar operações de proteção de dados.

Crie políticas de backup para bancos de dados Oracle

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

Antes de começar

- Você deve ter definido sua estratégia de backup.
- Você deve estar preparado para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, descobrir bancos de dados e criar conexões de sistema de armazenamento.
- Se você estiver replicando Snapshots para um espelho ou armazenamento secundário de cofre, o administrador do SnapCenter deverá ter atribuído as SVMs a você para os volumes de origem e destino.
- Se você instalou o plug-in como um usuário não root, deverá atribuir manualmente as permissões de execução aos diretórios prescript e postscript.
- Revise os pré-requisitos e limitações específicos da sincronização ativa do SnapMirror . Para obter informações, consulte "Limites de objetos para sincronização ativa do SnapMirror" .

Sobre esta tarefa

Se a opção 'Manter as cópias de backup por um número específico de dias' for selecionada, o período de retenção do SnapLock deverá ser menor ou igual aos dias de retenção mencionados.

+ Especificar um período de bloqueio de Snapshot impede a exclusão dos Snapshots até que o período de retenção expire. Isso pode levar à retenção de um número maior de Snapshots do que a contagem especificada na política.

+ Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos Snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

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 os detalhes da política.
6. Na página Tipo de política, execute as seguintes etapas:

    a. Selecione seu tipo de armazenamento.

    b. Selecione o escopo da política:

    - Se você quiser **criar um backup on-line**, selecione **Backup on-line**.

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

    - Se você quiser **criar um backup offline**, selecione **Backup offline** e, em seguida, selecione uma das seguintes opções:
        - Se você quiser criar um backup offline quando o banco de dados estiver no estado montado, selecione **Montar**.
        - Se você quiser criar um backup de desligamento offline alterando o banco de dados para o estado de desligamento, selecione **Desligar**.

          Se você tiver bancos de dados plugáveis (PDBs) e quiser salvar o estado dos PDBs antes de criar o backup, selecione **Salvar estado dos PDBs**. Isso permite que você traga os PDBs ao seu estado original após a criação do backup.

    c. Se você quiser catalogar o backup usando o Oracle Recovery Manager (RMAN), selecione **Catalogar backup com o Oracle Recovery Manager (RMAN)**.

    Você pode executar a catalogação adiada para um backup por vez usando a GUI ou o comando SnapCenter CLI Catalog-SmBackupWithOracleRMAN.

    > Se você quiser catalogar backups de um banco de dados RAC, certifique-se de que nenhuma outra tarefa esteja em execução para esse banco de dados. Se outra tarefa estiver em execução, a operação de catalogação falhará em vez de ser enfileirada.

    d. Se você quiser remover logs de arquivo após o backup, selecione **Remover logs de arquivo após o backup**.

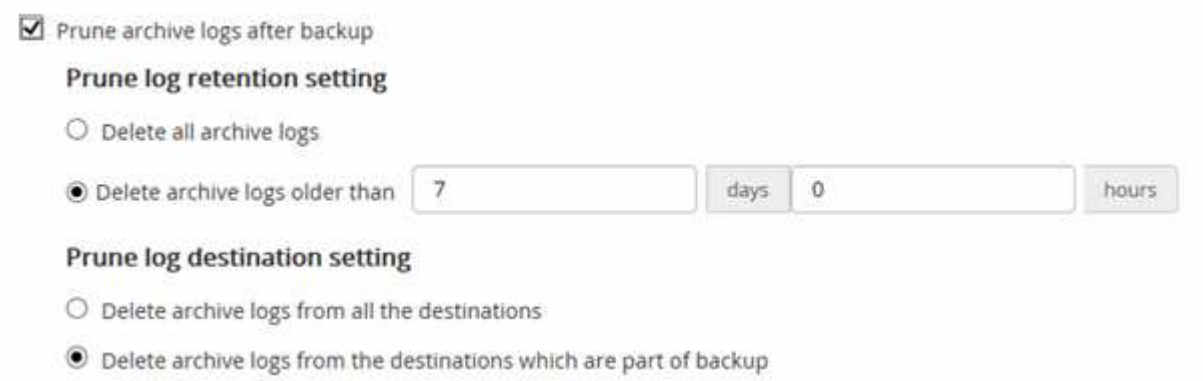
    > A remoção de logs de arquivo do destino de log de arquivo que não está configurado no banco de dados será ignorada.

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

- Você pode excluir logs de arquivamento somente se tiver selecionado os arquivos de log de arquivamento como parte do seu backup.

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…
Excluir todos os logs de arquivo	Selecione **Excluir todos os logs de arquivo**.
Excluir logs de arquivo mais antigos	Selecione **Excluir logs de arquivo mais antigos que** e especifique a idade dos logs de arquivo que devem ser excluídos em dias e horas.
Excluir logs de arquivo de todos os destinos	Selecione **Excluir logs de arquivo de todos os destinos**.
Excluir os logs de arquivamento dos destinos de log que fazem parte do backup	Selecione **Excluir logs de arquivo dos destinos que fazem parte do backup**.



+

7. Na página Snapshot e Replicação, execute as seguintes etapas:

   a. Especifique a frequência da programação selecionando **Sob demanda**, **Por hora**, **Diariamente**, **Semanalmente** ou **Mensalmente**.

Você pode especificar o agendamento (data de início e data de término) para a operação de backup ao criar 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 agendamentos de backup diferentes a cada política.

Se você agendou para 2h00, a programação não será acionada durante o horário de verão (DST).

a. Na seção Configurações de retenção de instantâneo de dados, 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 Snapshots	Selecione **Cópias a serem mantidas** e especifique o número de Snapshots que você deseja manter. Se o número de Snapshots exceder o número especificado, os Snapshots serão excluídos, com as cópias mais antigas sendo excluídas primeiro. O valor máximo de retenção é 1018. Os backups falharão se a retenção for definida como um valor maior do que o suportado pela versão subjacente do ONTAP . Você deve definir a contagem de retenção como 2 ou mais se planeja habilitar a replicação do SnapVault . Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro Snapshot será o Snapshot de referência para o relacionamento SnapVault até que um Snapshot mais recente seja replicado para o destino.
Mantenha os Snapshots por um certo número de dias	Selecione **Manter cópias por** e especifique o número de dias pelos quais você deseja manter os Snapshots antes de excluí-los.
Período de bloqueio de cópia de instantâneo	Selecione o **Período de bloqueio de cópia de instantâneo** e especifique a duração em dias, meses ou anos. O período de retenção do SnapLock deve ser inferior a 100 anos.

b. Na seção Configurações de retenção de instantâneo do Archive Log, 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 Snapshots	Selecione **Cópias a serem mantidas** e especifique o número de Snapshots que você deseja manter. Se o número de Snapshots exceder o número especificado, os Snapshots serão excluídos, com as cópias mais antigas sendo excluídas primeiro. O valor máximo de retenção é 1018. Os backups falharão se a retenção for definida como um valor maior do que o suportado pela versão subjacente do ONTAP . Você deve definir a contagem de retenção como 2 ou mais se planeja habilitar a replicação do SnapVault . Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro Snapshot será o Snapshot de referência para o relacionamento SnapVault até que um Snapshot mais recente seja replicado para o destino.
Mantenha os Snapshots por um certo número de dias	Selecione **Manter cópias por** e especifique o número de dias pelos quais você deseja manter os Snapshots antes de excluí-los.
Período de bloqueio de cópia de instantâneo	Selecione o **Período de bloqueio de cópia de instantâneo** e especifique a duração em dias, meses ou anos. O período de retenção do SnapLock deve ser inferior a 100 anos.

c. Selecione o rótulo da política.

Você pode atribuir rótulos SnapMirror a snapshots primários para replicação remota, permitindo que os snapshots primários descarreguem a operação de replicação de snapshots do SnapCenter para sistemas secundários ONTAP . Isso pode ser feito sem habilitar a opção SnapMirror ou SnapVault na página de política.

8. Na seção Selecionar opções de replicação secundária, selecione uma ou ambas as seguintes opções de replicação secundária:

Você deve selecionar as opções de replicação secundária para que o **Período de bloqueio de cópia de instantâneo secundário** seja efetivo.

Para este campo…	Faça isso…
Atualizar o SnapMirror após criar um Snapshot local	Selecione este campo para criar cópias espelhadas dos conjuntos de backup em outro volume (replicação SnapMirror). Esta opção deve ser habilitada para sincronização ativa do SnapMirror . Durante a replicação secundária, o tempo de expiração do SnapLock carrega o tempo de expiração do SnapLock primário. Clicar no botão **Atualizar** na página Topologia atualiza o tempo de expiração do SnapLock secundário e primário que são recuperados do ONTAP.
Atualizar o SnapVault após criar um Snapshot local	Selecione esta opção para executar a replicação de backup de disco para disco (backups do SnapVault). Quando o SnapLock é configurado somente no secundário do ONTAP conhecido como SnapLock Vault, clicar no botão **Atualizar** na página Topologia atualiza o período de bloqueio no secundário recuperado do ONTAP. Para mais informações sobre o SnapLock Vault, consulte "Enviar cópias do Snapshot para o WORM em um destino de cofre" Ver "Visualize backups e clones do banco de dados Oracle na página Topologia" .
Contagem de novas tentativas de erro	Insira o número máximo de tentativas de replicação que podem ser permitidas antes que a operação seja interrompida.

Você deve configurar a política de retenção do SnapMirror no ONTAP para o armazenamento secundário para evitar atingir o limite máximo de Snapshots no armazenamento secundário.

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

   Você deve armazenar os prescrições e pós-escritos 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 alguma pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.

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

O SnapCenter permite que você use as variáveis de ambiente predefinidas ao executar o prescript e o postscript."Saber 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 prescript ou postscript que você deseja executar antes ou depois da operação de verificação, respectivamente.

       Você deve armazenar os prescrições e pós-escritos 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 alguma pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.

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

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

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

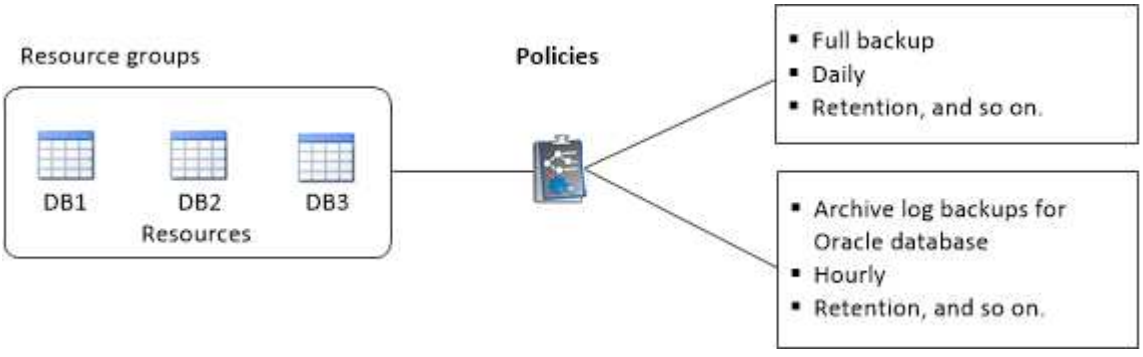
Um grupo de recursos é um contêiner onde você adiciona recursos que deseja fazer backup e proteger. Um grupo de recursos permite que você faça backup de todos os dados associados a um determinado aplicativo simultaneamente.

Sobre esta tarefa

- Um banco de dados com arquivos em grupos de discos ASM deve estar no estado "MONT" 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 trabalho de proteção de dados que você deseja executar.

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



- Para políticas habilitadas para SnapLock , para ONTAP 9.12.1 e versões anteriores, se você especificar um período de bloqueio de Snapshot, os clones criados a partir de Snapshots à prova de violação como parte da restauração herdarão o tempo de expiração do SnapLock . O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .
- Não há suporte para adicionar novos bancos de dados sem sincronização ativa do SnapMirror a um grupo de recursos existente que contém recursos com sincronização ativa do SnapMirror .

- Não há suporte para adicionar novos bancos de dados a um grupo de recursos existente no modo de failover da sincronização ativa do SnapMirror . Você pode adicionar recursos ao grupo de recursos somente no estado regular ou de failback.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** 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. Insira 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 ajudar você a pesquisar o grupo de recursos posteriormente.

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

   c. Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

      Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

   d. Especifique os destinos dos arquivos de log de arquivamento dos quais você não deseja fazer backup.

      Você deve usar exatamente o mesmo destino definido no Oracle, incluindo o prefixo, se necessário.

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

   Os recursos são listados na seção Recursos Disponíveis somente se o recurso for descoberto com sucesso. Se você adicionou recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois que você atualizar sua lista de recursos.

5. Selecione os recursos da 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 Configurações do aplicativo, selecione a opção de backup.
7. 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 agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

b. Clique + na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.

c. Na janela Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

Onde *policy_name* é o nome da política que você selecionou.

Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .

8. Na página Verificação, execute as seguintes etapas:

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

b. Clique + na coluna Configurar agendamentos 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…**
Executar verificação após o backup	Selecione **Executar verificação após backup**.
Agendar uma verificação	Selecione **Executar verificação agendada** e depois selecione o tipo de agendamento na lista suspensa.

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

e. Clique em **OK**.

Os agendamentos de verificação configurados são listados na coluna Agendamentos Aplicados.

9. 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 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 Set-SmSmtpServer do PowerShell.

10. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e habilite proteção secundária para recursos Oracle em sistemas ASA r2

Você deve criar o grupo de recursos para adicionar os recursos que estão nos sistemas ASA r2. Você também pode provisionar a proteção secundária ao criar o grupo de recursos.

Antes de começar

- Você deve garantir que não está adicionando recursos do ONTAP 9.x e recursos do ASA r2 ao mesmo grupo de recursos.
- Você deve garantir que não tenha um banco de dados com recursos ONTAP 9.x e recursos ASA r2.

Sobre esta tarefa

- A proteção secundária estará disponível somente se o usuário conectado estiver atribuído à função que tem o recurso **SecondaryProtection** habilitado.
- Se você habilitar a proteção secundária, o grupo de recursos será colocado no modo de manutenção durante a criação dos grupos de consistência primário e secundário. Depois que os grupos de consistência primário e secundário são criados, o grupo de recursos é retirado do modo de manutenção.
- O SnapCenter não oferece suporte à proteção secundária para um recurso clone.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** 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. Insira 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 ajudar você a pesquisar o grupo de recursos posteriormente.

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

   c. Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

      Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

   d. Especifique os destinos dos arquivos de log de arquivamento dos quais você não deseja fazer backup.

      Você deve usar exatamente o mesmo destino definido no aplicativo, incluindo o prefixo, se necessário.

4. Na página Recursos, selecione o nome do host do banco de dados na lista suspensa **Host**.

Os recursos são listados na seção Recursos Disponíveis somente se o recurso for descoberto com sucesso. Se você adicionou recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois que você atualizar sua lista de recursos.

5. Selecione os recursos do ASA r2 na seção Recursos disponíveis e mova-os para a seção Recursos selecionados.
6. Na página Configurações do aplicativo, selecione a opção de backup.
7. 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 agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique + na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.
   c. Na janela Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

      Onde *policy_name* é o nome da política que você selecionou.

      Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

   Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .
8. Se a proteção secundária estiver habilitada para a política selecionada, a página Proteção Secundária será exibida e você precisará executar as seguintes etapas:
   a. Selecione o tipo de política de replicação.

      A política de replicação síncrona não é suportada.

   b. Especifique o sufixo do grupo de consistência que você deseja usar.
   c. Nos menus suspensos Cluster de destino e SVM de destino, selecione o cluster emparelhado e o SVM que você deseja usar.

      O cluster e o peering de SVM não são suportados pelo SnapCenter. Você deve usar o System Manager ou as CLIs do ONTAP para executar o peering de cluster e SVM.

Se os recursos já estiverem protegidos fora do SnapCenter, eles serão exibidos na seção Recursos Protegidos Secundários.

1. Na página Verificação, execute as seguintes etapas:
   a. Clique em **Carregar localizadores** para carregar os volumes SnapMirror ou SnapVault para realizar a verificação no armazenamento secundário.

b. Clique + na coluna Configurar agendamentos 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…
Executar verificação após o backup	Selecione **Executar verificação após backup**.
Agendar uma verificação	Selecione **Executar verificação agendada** e depois selecione o tipo de agendamento na lista suspensa.

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

e. Clique em **OK**.

Os agendamentos de verificação configurados são listados na coluna Agendamentos Aplicados.

2. 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 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 Set-SmSmtpServer do PowerShell.

3. Revise o resumo e clique em **Concluir**.

Fazer backup de recursos Oracle

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

Passos

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

Você pode então clicar para fechar o painel de filtro.

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

A página Database-Protect é exibida.

5. Na página Recursos, execute as seguintes etapas:

a. Marque a caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

Por exemplo, `customtext_policy_hostname` ou `resource_hostname` . Um registro de data e hora é anexado ao nome do Snapshot por padrão.

b. Especifique os destinos dos arquivos de log de arquivamento dos quais você não deseja fazer backup.

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 agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique + na coluna Configurar agendamentos para configurar um agendamento para a política desejada.

   c. Na janela Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e selecione `OK` .

      policy_name é o nome da política que você selecionou.

   Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

7. Na página Verificação, execute as seguintes etapas:

   a. Clique em **Carregar localizadores** para carregar os volumes SnapMirror ou SnapVault para verificar o armazenamento secundário.

   b. Clique + na coluna Configurar agendamentos para configurar o agendamento de verificação para todos os tipos de agendamento da política. + Na caixa de diálogo Adicionar agendamentos 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, não é possível executar a operação de verificação em nós Leaf se a cardinalidade for menor que o número de nós no cluster RAC.

   e. Selecione **Verificar no local secundário** para verificar seus backups no armazenamento secundário.

   f. Clique em **OK**.

      Os agendamentos de verificação configurados são listados na coluna Agendamentos Aplicados.

8. Na página Notificação, selecione os cenários nos quais você deseja enviar os e-mails na 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 você quiser anexar o relatório da operação de backup realizada no recurso, selecione **Anexar relatório de tarefa**.

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

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

   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 aplicou 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. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Depois que você 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 estava residindo.

  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 ao 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 o comando `Set-SmConfigSettings` cmdlet:

  Após 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 poderá falhar com o código de erro DBV-00100 no arquivo especificado. Você deve modificar os valores dos parâmetros VERIFICATION_DELAY e VERIFICATION_RETRY_COUNT em sco.properties.

  Após 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 conseguir detectar um relacionamento de proteção após um failover.
- Se você estiver fazendo backup de dados do aplicativo em VMDKs e o tamanho do heap Java para o SnapCenter Plug-in for VMware vSphere não for grande o suficiente, o backup poderá falhar.

  Para aumentar o tamanho do heap Java, localize o arquivo de script */opt/netapp/init_scripts/scvservice*. Nesse roteiro, o `do_start method` O 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 o relacionamento SnapMirror ou SnapVault após failover do MetroCluster"
- "O banco de dados Oracle RAC One Node é ignorado para executar operações do SnapCenter"
- "Falha ao alterar o estado de um banco de dados Oracle 12c ASM"

- "Parâmetros personalizáveis para operações de backup, restauração e clonagem em sistemas AIX"(Requer login)

Fazer backup de grupos de recursos do banco de dados Oracle

Um grupo de recursos é uma coleção de recursos em um host ou cluster. A operação de backup é executada 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 um agendamento configurado, os backups serão criados de acordo com o agendamento.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** 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 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 armazenamento não NetApp , a operação de backup será abortada mesmo que o outro banco de dados esteja no armazenamento 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. Monitore o progresso selecionando **Monitorar > Trabalhos**.

Depois que você 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 estava residindo.

  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 ao 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 o comando `Set-SmConfigSettings` cmdlet:

  Após 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 poderá falhar com o código de erro DBV-00100 no arquivo especificado. Você deve modificar os valores dos parâmetros VERIFICATION_DELAY_ e VERIFICATION_RETRY_COUNT em sco.properties.

  Após 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 backup do banco de dados Oracle

Aprenda a monitorar o progresso das operações de backup e proteção de dados.

Monitorar operações de backup do banco de dados Oracle

Você pode monitorar o progresso de diferentes operações de backup usando a página SnapCenterJobs. Talvez você queira verificar o progresso para determinar quando ele foi concluído ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado correspondente das operações:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- 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 que somente as operações de backup sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Backup**.
   d. No menu suspenso **Status**, selecione o status do backup.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.
4. Selecione uma tarefa de backup e clique em **Detalhes** para visualizar os detalhes da tarefa.

   Embora o status do trabalho de backup seja exibido , ao clicar em detalhes do trabalho, você poderá ver que algumas das tarefas filhas da operação de backup ainda estão em andamento ou marcadas com sinais de alerta.

5. Na página Detalhes do trabalho, clique em **Exibir registros**.

O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Monitore as operações de proteção de dados no painel Atividade

O painel Atividade exibe as cinco operações mais recentes realizadas. O painel Atividade também exibe quando a operação foi iniciada e o status da operação.

O painel Atividade exibe informações sobre operações de backup, restauração, clonagem e backup agendado.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** 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 do trabalho**.

Outras operações de backup

Faça backup de bancos de dados Oracle usando comandos UNIX

O fluxo de trabalho de backup inclui planejamento, identificação de recursos para backup, criação de políticas de backup, criação de grupos de recursos e anexação 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 SnapCenter Server usando o comando *Open-SmConnection*.

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

  A sessão de conexão é válida apenas por 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 SnapCenter Server, descobrir as instâncias do banco de dados Oracle, adicionar políticas e grupos 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*. Alternativamente, você também pode consultar o "Guia de referência de comandos do software SnapCenter" .

Passos

1. Iniciar uma sessão de conexão com o SnapCenter Server para um usuário especificado: *Open-SmConnection*
2. Executar operação de descoberta de recursos do host: *Get-SmResources*
3. Configurar credenciais do banco de dados Oracle e nós preferenciais para operação de backup de um banco de dados Real Application Cluster (RAC): *Configure-SmOracleDatabase*
4. Crie uma política de backup: *Add-SmPolicy*
5. Recupere 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 secundárias ao criar um grupo de recursos de backup.
6. Adicionar um grupo de recursos ao SnapCenter: *Add-SmResourceGroup*
7. Criar um backup: *New-SmBackup*

   Você pode pesquisar o trabalho usando a opção WaitForCompletion. Se esta opção for especificada, o comando continuará a pesquisar 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 operações de backup que estejam em execução, na fila ou que não respondam.

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

Sobre esta tarefa

Quando você cancela uma operação de backup, o SnapCenter Server interrompe a operação e remove todos os Snapshots do armazenamento se o backup criado não estiver registrado no SnapCenter Server. Se o backup já estiver registrado no SnapCenter Server, ele não reverterá o Snapshot já criado, mesmo após o cancelamento ser acionado.

- Você pode cancelar somente o log ou a operação de backup completo que estão na fila ou em execução.
- Você não pode cancelar a operação após a verificação ter iniciado.

  Se você cancelar a operação antes da verificação, a operação será cancelada e a operação de verificação não será executada.
- Não é possível cancelar a operação de backup após o início das operações de catálogo.
- Você pode cancelar uma operação de backup na página Monitor ou no painel Atividade.
- Além de usar a GUI do SnapCenter , você pode usar comandos CLI para cancelar operações.
- O botão **Cancelar trabalho** fica desabilitado 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 enfileiradas de outros membros enquanto estiver usando essa função.

Etapa

Execute uma das seguintes ações:

Do…	Ação
Página do monitor	1. No painel de navegação esquerdo, clique em **Monitor** > **Trabalhos**. 2. Selecione a operação e clique em **Cancelar trabalho**.
Painel de atividades	1. Após iniciar o trabalho de backup, clique em no painel Atividade para visualizar as cinco operações mais recentes. 2. Selecione a operação. 3. Na página Detalhes do trabalho, clique em **Cancelar trabalho**.

Resultados

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

Se a operação cancelada não responder no estado de cancelamento ou execução, você deverá executar Cancel-SmJob -JobID <int> -Force para interromper à força a operação de backup.

Visualize backups e clones do banco de dados Oracle na página Topologia

Ao se preparar para fazer backup ou clonar um recurso, pode ser útil visualizar uma representação gráfica de todos os backups e clones no armazenamento primário e secundário.

Sobre esta tarefa

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

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

- exibe o número de backups e clones que estão disponíveis no armazenamento primário.
- exibe o número de backups e clones que são espelhados no armazenamento secundário usando a tecnologia SnapMirror .
- exibe o número de backups e clones que são replicados no armazenamento secundário usando a

tecnologia SnapVault .

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

Clones de um backup de um espelho flexível em termos de versão em um volume do tipo mirror-vault são exibidos na exibição de topologia, mas a contagem de backups de espelho na exibição de topologia não inclui o backup flexível em termos de versão.

Se você tiver um relacionamento secundário como sincronização ativa do SnapMirror (inicialmente lançado como SnapMirror Business Continuity [SM-BC]), poderá ver os seguintes ícones adicionais:

-  O site de réplica está no ar.
-  O site de réplicas está fora do ar.
-  O espelho secundário ou o relacionamento do cofre não foram restabelecidos.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione o recurso ou 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 será exibida.

4. Revise o cartão Resumo para ver um resumo do número de backups e clones disponíveis no armazenamento 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 **Atualizar** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clicar no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Uma programação semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo estiver distribuído em vários volumes, o tempo de expiração do SnapLock para o backup será o maior tempo de expiração do SnapLock definido para um Snapshot em um volume. O maior tempo de expiração do SnapLock é recuperado do ONTAP.

   Para sincronização ativa do SnapMirror , clicar no botão **Atualizar** atualiza o inventário de backup do SnapCenter consultando o ONTAP para sites primários e de réplica. Uma programação semanal também executa essa atividade para todos os bancos de dados que contêm o relacionamento de sincronização ativo do SnapMirror .

   - Para sincronização ativa do SnapMirror e somente para o ONTAP 9.14.1, os relacionamentos Async Mirror ou Async MirrorVault com o novo destino primário devem ser configurados manualmente após o failover. A partir do ONTAP 9.15.1, o Async Mirror ou o Async MirrorVault são configurados automaticamente para o novo destino principal.

- Após o failover, um backup deve ser criado para que o SnapCenter esteja ciente do failover. Você pode clicar em **Atualizar** somente após um backup ter sido criado.

5. Na 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 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, catalogação, descatalogação e exclusão.

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

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

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

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

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

Alternativamente, você também pode consultar o "Guia de referência de comandos do software SnapCenter" ou "Guia de referência do cmdlet do software SnapCenter" .

Informações sobre direitos autorais

Informações sobre marcas comerciais