Faça backup de bancos de dados Oracle

SnapCenter software

NetApp
February 20, 2026

Índice

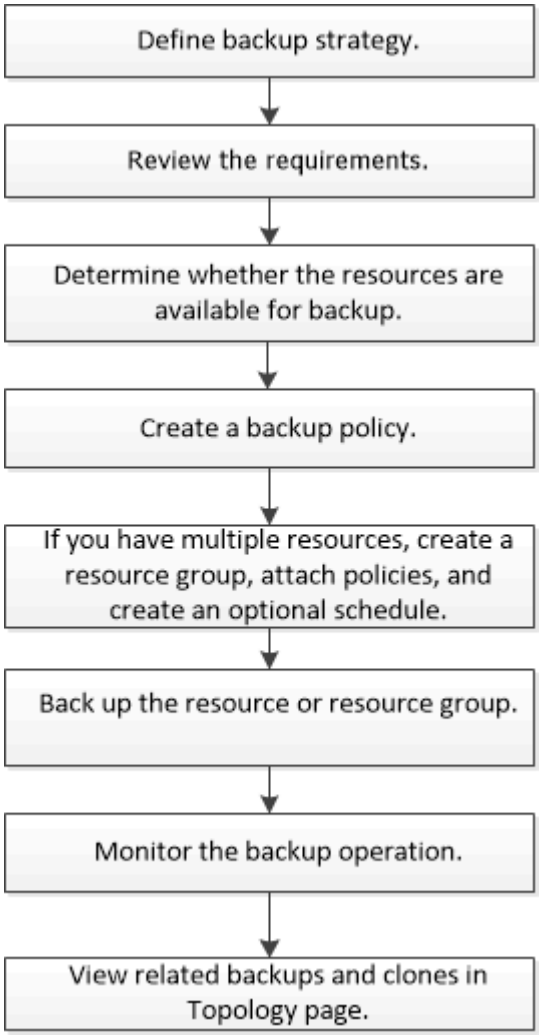
Faça backup de bancos de dados Oracle . . . 1
- Visão geral do procedimento de backup . . . 1
- Informações de configuração de backup . . . 2
  - Configurações de banco de dados Oracle compatíveis para backups . . . 2
  - Tipos de backup suportados para bancos de dados Oracle . . . 2
  - Como o SnapCenter descobre bancos de dados Oracle . . . 3
  - Nós preferenciais na configuração RAC . . . 5
  - Como catalogar backups com o Oracle Recovery Manager . . . 5
  - Variáveis de ambiente predefinidas para prescrição específica de backup e postscript . . . 7
  - Opções de retenção de backup . . . 12
  - Fazer backup de programações . . . 13
  - Convenções de nomenclatura de backup . . . 13
- Requisitos para fazer backup de um banco de dados Oracle . . . 14
- Descubra os bancos de dados Oracle disponíveis para backup . . . 15
  - Passo 1: Impedir que o SnapCenter descubra entradas que não sejam do banco de dados . . . 15
  - Passo 2: Descubra recursos . . . 16
- Criar políticas de backup para bancos de dados Oracle . . . 17
- Crie grupos de recursos e anexe políticas para bancos de dados Oracle . . . 23
- Crie grupos de recursos e habilite a proteção secundária para recursos Oracle em sistemas ASA R2 . . . 25
- Faça backup dos recursos Oracle . . . 28
- Faça backup de grupos de recursos de banco de dados Oracle . . . 30
- Monitorar o backup do banco de dados Oracle . . . 32
  - Monitorar operações de backup de banco de dados Oracle . . . 32
  - Monitore operações de proteção de dados no painel atividade . . . 32
- Outras operações de backup . . . 33
  - Faça backup de bancos de dados Oracle usando comandos UNIX . . . 33
  - Cancelar operações de backup de bancos de dados Oracle . . . 34
  - Veja os backups e clones do banco de dados Oracle na página topologia . . . 35

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 as versões do Oracle compatíveis, 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 11*g* a 12*c*R1

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 do Oracle 12cR2 a 18c, 19C ou 21c

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 12*c*R2 e 18*c*_ 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 carateres, 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 carateres, 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. Alternativamente, você pode consultar o "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 registos 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_CDB*DATA/*--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-RG2-2021_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_CDB*DATA/*--*,buck:/vol/_NFS_CDB*REDO/__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 padrão de nomenclatura Snapshot ou usar uma convenção de nomenclatura personalizada. A convenção de nomenclatura de backup padrão adiciona um carimbo de data/hora aos nomes de Snapshot 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 carimbo de data/hora.

Como alternativa, você pode especificar o formato do nome da captura Instantânea enquanto protege recursos ou grupos de recursos selecionando **usar formato de nome personalizado para cópia Instantânea**. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, o sufixo do carimbo de hora é adicionado ao nome do instantâneo.

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 carateres.
- 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 SMCore 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.

Antes de começar

- 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 ícone ilter] e, em seguida, selecione o nome do host e o tipo de banco de dados para filtrar os recursos. Você pode clicar no ícone imagfilter_icon.gif[filter icon]_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 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 snapshots em um storage secundário de espelhamento ou cofre, o administrador do SnapCenter deverá ter atribuído 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 prescritor e postscript.
- Reveja os pré-requisitos e limitações específicos da sincronização ativa do SnapMirror. Para obter informações, "Limites de objetos para sincronização ativa do SnapMirror" consulte .

Sobre esta tarefa

Se a opção 'reter as cópias de backup para um número específico de dias' estiver selecionada, o período de retenção do SnapLock deve ser menor ou igual aos dias de retenção mencionados.

Especificar um período de bloqueio instantâneo impede a exclusão dos instantâneos até que o período de retenção expire. Isso pode levar a reter um número maior de instantâneos do que a contagem especificada na

política.

Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots 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 o tipo de armazenamento.

   b. Selecionar escopo da política:

      - 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.

   c. 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.

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

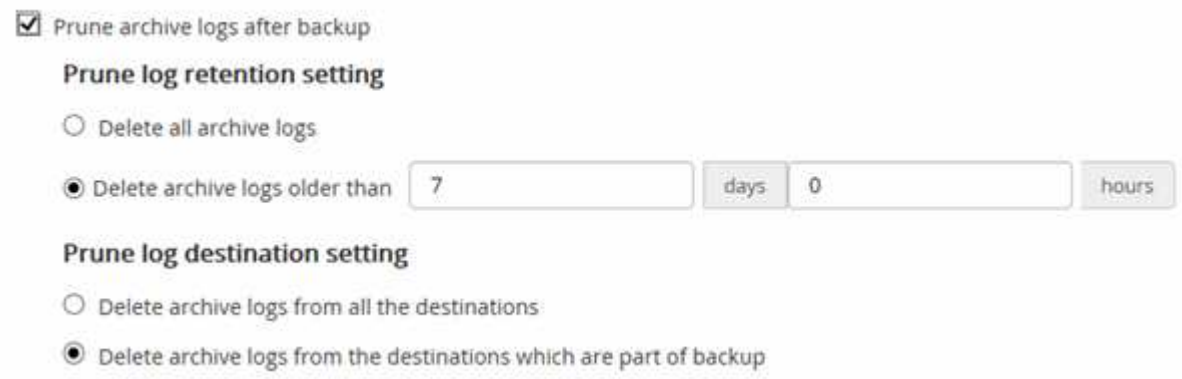
      > A eliminação dos registos de arquivo do destino do registo de arquivo que não está configurado na base de dados será ignorada.

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



+

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

   a. 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).

a. Na seção Configurações de retenção de instantâneos 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 instantâneos	Selecione **Copies to keep** e especifique o número de instantâneos que deseja manter. Se o número de instantâneos exceder o número especificado, os instantâneos serão excluídos com as cópias mais antigas excluídas primeiro. O valor máximo de retenção é 1018. 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 o primeiro snapshot é o snapshot de referência para a relação SnapVault até que um snapshot mais recente seja replicado para o destino.
Mantenha as capturas instantâneas por um determinado número de dias	Selecione **reter cópias para** e especifique o número de dias para os quais deseja manter as capturas instantâneas antes de excluí-las.
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 instantâneos do Registro de arquivamento, 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 instantâneos	Selecione **Copies to keep** e especifique o número de instantâneos que deseja manter. Se o número de instantâneos exceder o número especificado, os instantâneos serão excluídos com as cópias mais antigas excluídas primeiro. O valor máximo de retenção é 1018. 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 o primeiro snapshot é o snapshot de referência para a relação SnapVault até que um snapshot mais recente seja replicado para o destino.
Mantenha as capturas instantâneas por um determinado número de dias	Selecione **reter cópias para** e especifique o número de dias para os quais deseja manter as capturas instantâneas antes de excluí-las.
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 a etiqueta 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 **período de bloqueio de cópia snapshot secundário** para entrar em vigor.

Para este campo…	Faça isso…
Atualize o SnapMirror depois de criar um instantâneo local	Selecione este campo para criar cópias espelhadas dos conjuntos de backup em outro volume (replicação SnapMirror). Esta opção deve estar ativada para a 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.
Atualize o SnapVault depois de criar um instantâneo local	Selecione esta opção para executar a replicação de backup disco a disco (backups SnapVault). Quando o SnapLock é configurado apenas no secundário do ONTAP conhecido como SnapLock Vault, clicar no botão **Atualizar** na página topologia atualiza o período de bloqueio no secundário que é recuperado do ONTAP. Para obter mais informações sobre o SnapLock Vault, consulte "Armazene cópias Snapshot em WORM em um destino de cofre" "Veja os backups e clones do banco de dados Oracle na página topologia"Consulte .
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 atingir o limite máximo de snapshots 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

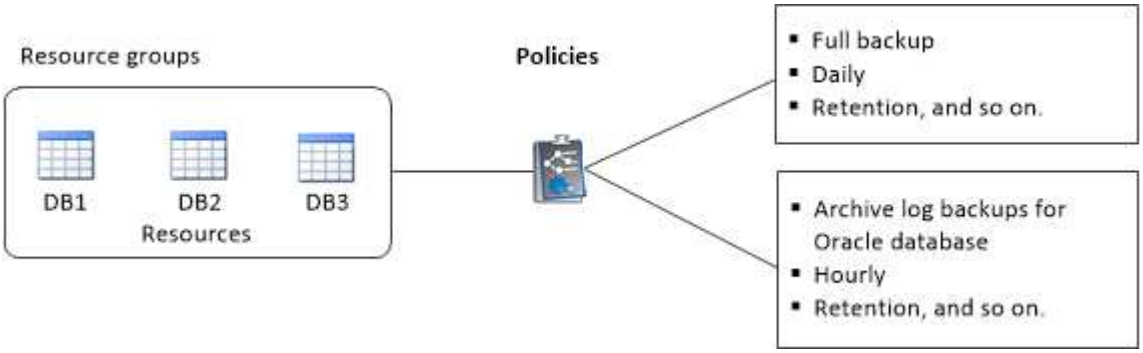
Um grupo de recursos é um contentor onde você adiciona recursos que deseja fazer backup e proteger. Um grupo de recursos permite fazer backup de todos os dados associados a um determinado aplicativo simultaneamente.

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:



- Para políticas habilitadas para o SnapLock, para ONTAP 9.12,1 e versões abaixo, se você especificar um período de bloqueio do Snapshot, os clones criados a partir dos snapshots à prova de violação como parte da restauração herdarão o tempo de expiração do SnapLock. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.
- A adição de novos bancos de dados sem a sincronização ativa do SnapMirror a um grupo de recursos existente que contenha recursos com a sincronização ativa do SnapMirror não é suportada.
- A adição de novos bancos de dados a um grupo de recursos existente no modo failover da sincronização ativa do SnapMirror não é suportada. Você pode adicionar recursos ao grupo de recursos apenas no estado regular ou de failback.

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 carateres.

   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 captura Instantânea.

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

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

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

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 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 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.

8. 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.

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 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.

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

Crie grupos de recursos e habilite a proteção secundária para recursos Oracle em sistemas ASA R2

Você deve criar o grupo de recursos para adicionar os recursos que estão em sistemas ASA R2. Você também pode provisionar a proteção secundária enquanto cria o grupo de recursos.

Antes de começar

- Você deve garantir que não esteja adicionando recursos do ONTAP 9.x e do ASA R2 ao mesmo grupo de recursos.
- Você deve garantir que não tenha um banco de dados com recursos do ONTAP 9.x e do ASA R2.

Sobre esta tarefa

- A proteção secundária só está disponível se o usuário conetado for atribuído à função que tem a capacidade **SecondaryProtection** ativada.
- Se você ativou a proteção secundária, o grupo de recursos será colocado no modo de manutenção ao criar os grupos de consistência primária e secundária. Depois que os grupos de consistência primária e secundária são criados, o grupo de recursos é colocado fora do modo de manutenção.
- O SnapCenter não é compatível com proteção secundária para um recurso clone.

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 carateres.

   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 captura Instantânea.

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

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

      Você deve usar exatamente o mesmo destino que foi 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 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 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 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.

8. Se a proteção secundária estiver ativada para a política selecionada, a página proteção secundária será exibida e você precisará executar as seguintes etapas:

a. Selecione o tipo da 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 drop-down Cluster de destino e SVM de destino, selecione o cluster com peering e SVM que você deseja usar.

O peering de cluster e SVM não é compatível com o SnapCenter. Você deve usar o Gerenciador de sistema ou os CLIs ONTAP para executar peering de cluster e SVM.

Se os recursos já estiverem protegidos fora do SnapCenter, esses recursos 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 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**.

Se você quiser…	Faça isso…
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.

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 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.

3. 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, execute as seguintes etapas:

a. Marque a caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.

Por exemplo, `customtext_policy_hostname` ou `resource_hostname`. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.

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-SmSmtpServer` .

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 detetar 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 detetar 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.

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*. Alternativamente, você também pode 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 conetado 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 todos os snapshots do armazenamento se o backup criado não estiver registrado no servidor SnapCenter. Se o backup já estiver registrado no servidor SnapCenter, ele não reverterá o instantâneo já criado mesmo após o cancelamento ser acionado.

- Pode cancelar apenas a operação de registo 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**.
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.

Se você tiver uma relação secundária como sincronização ativa do SnapMirror (lançada inicialmente como SnapMirror Business Continuity [SM-BC]), você poderá ver os seguintes ícones adicionais:

-  O site da réplica está em cima.
-  O site da réplica está inativo.
-  A relação do espelho secundário ou do cofre não foi restabelecida.

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.

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

   Quando o recurso do aplicativo é espalhado por vários volumes, o tempo de expiração do SnapLock para o backup será o tempo de expiração do SnapLock mais longo definido para um snapshot em um volume. O tempo de expiração mais longo do SnapLock é recuperado do ONTAP.

   Para a 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 a relação de sincronização ativa do SnapMirror.

   - Para a sincronização ativa do SnapMirror e somente para o ONTAP 9.14,1, as relações de espelhamento do Async ou EspelrorVault do Async com o novo destino primário devem ser configuradas manualmente após o failover. A partir do ONTAP 9.15,1 em diante, o espelho do Async ou o MirrorVault do Async 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 **Refresh** somente depois que um backup tiver sido criado.

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, descatálogo 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, descatálogo 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*.

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

Informações sobre direitos autorais

Informações sobre marcas comerciais