Proteja aplicativos em execução no Azure NetApp Files

SnapCenter Software 6.0

NetApp
December 19, 2024

Índice

Proteja aplicativos em execução no Azure NetApp Files

Proteja aplicativos em execução no Azure NetApp Files

O SnapCenter é compatível com a proteção de aplicações como Oracle, SQL e SAP HANA que residem no Azure NetApp Files. A partir da versão 6.0.1, o SnapCenter dá suporte ao recurso de backup Azure NetApp Files que expande os recursos de proteção de dados do Azure NetApp Files fornecendo solução de backup totalmente gerenciada para recuperação, arquivamento e conformidade de longo prazo.

O Azure NetApp Files é uma solução de storage premium que pode ser cara para a retenção de backup a longo prazo. Para otimizar custos, você pode migrar os backups do storage Azure NetApp Files para um armazenamento de objetos Azure. A partir do SnapCenter 6,0.1, é possível fazer backup e clonar aplicativos que residem no Azure NetApp Files para o armazenamento de Blobs do Azure (armazenamento de objetos). Você pode manter duas cópias dos seus dados, cópias snapshot de volume no storage Azure NetApp Files para recuperação de curto prazo e outra cópia no armazenamento Blob do Azure para recuperação de longo prazo.

Quando uma política com backup do Azure NetApp Files está habilitada e associada a um recurso, o SnapCenter manipula a criação de snapshots de volume e o backup no armazenamento de Blobs do Azure. O SnapCenter cria o cofre de backup e habilita o backup para o volume. Se você ativou o backup para o volume, o SnapCenter utiliza o cofre existente.

Limitações

- As funcionalidades de armazenamento de objetos para sistemas de armazenamento FAS ou AFF ONTAP e FSxN não são suportadas.
- Workflows de montagem e catálogo no Oracle e SAP HANA não são compatíveis.
- A verificação de backup do storage de objetos, suporte à API REST, gerenciamento do ciclo de vida de clones do storage de objetos e recursos de geração de relatórios para backups de storage de objetos não é compatível.
- A restauração de backups no armazenamento de Blobs do Azure para o Azure NetApp Files não é suportada. Você pode usar a opção clone, alternativamente.
- Divisão de clones não é suportada.

Instale o SnapCenter e crie credenciais

Instale o SnapCenter na Máquina Virtual do Azure

Você pode baixar o software SnapCenter no site de suporte da NetApp e instalar o software na máquina virtual do Azure.

Antes de começar

- Certifique-se de que a máquina virtual do Azure Windows atenda aos requisitos de instalação do servidor SnapCenter. Para obter informações, "Prepare-se para instalar o servidor SnapCenter"consulte .
- Se você é novo no Azure NetApp Files e não tem uma conta NetApp existente, certifique-se de que se

registrou para que você possa acessar o software SnapCenter.

Passos

1. Baixe o pacote de instalação do servidor SnapCenter em "Site de suporte da NetApp".
2. Inicie a instalação do servidor SnapCenter clicando duas vezes no arquivo .exe baixado.

   Depois de iniciar a instalação, todas as pré-verificações são executadas e, se os requisitos mínimos não forem atendidos, as mensagens de erro ou aviso apropriadas serão exibidas. Você pode ignorar as mensagens de aviso e prosseguir com a instalação; no entanto, os erros devem ser corrigidos.

3. Reveja os valores pré-preenchidos necessários para a instalação do servidor SnapCenter e modifique, se necessário.

   Você não precisa especificar a senha para o banco de dados do repositório do MySQL Server. Durante a instalação do servidor SnapCenter, a senha é gerada automaticamente.

   O caractere especial "%" não é suportado no caminho personalizado para o banco de dados do repositório. Se você incluir "%" no caminho, a instalação falhará.

4. Clique em **Instalar agora**.

   Se você tiver especificado quaisquer valores inválidos, as mensagens de erro apropriadas serão exibidas. Deve voltar a introduzir os valores e, em seguida, iniciar a instalação.

   Se você clicar no botão **Cancelar**, a etapa que está sendo executada será concluída e, em seguida, iniciar a operação de reversão. O servidor SnapCenter será completamente removido do host.

   No entanto, se você clicar em **Cancelar** quando as operações "SnapCenter Server site Restart" ou "Waiting for SnapCenter Server to start" estiverem sendo executadas, a instalação continuará sem cancelar a operação.

Registre o produto para habilitar o suporte

Se você é novo no NetApp e não tem uma conta NetApp existente, deve Registrar o produto para habilitar o suporte.

Passos

1. Depois de instalar o SnapCenter, navegue até **Ajuda > sobre**.
2. Na caixa de diálogo *sobre o SnapCenter*, anote a instância do SnapCenter, um número de 20 dígitos que começa com 971.
3. Clique https://register.netapp.comem .
4. Clique em **Eu não sou um Cliente NetApp registrado**.
5. Especifique os seus dados para se registar.
6. Deixe o campo NetApp Reference SN em branco.
7. Selecione **SnapCenter** na lista suspensa linha de produtos.
8. Selecione o fornecedor de faturação.
9. Insira o ID da instância do SnapCenter de 20 dígitos.

10. Clique em **Enviar**.

Crie a credencial do Azure no SnapCenter

Você deve criar a credencial do Azure no SnapCenter para acessar a conta do Azure NetApp.

Antes de criar a credencial do Azure, certifique-se de que criou o principal de serviço no Azure. O ID do locatário, o ID do cliente e a chave secreta associados ao responsável do serviço serão necessários para criar a credencial do Azure.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credential**.
3. Clique em **novo**.
4. Na página Credential (credencial), especifique as seguintes informações necessárias para criar a credencial.

Para este campo…	Faça isso…
Nome da credencial	Introduza um nome para a credencial.
Modo de autenticação	Selecione **credencial do Azure** na lista suspensa.
ID do inquilino	Insira o ID do locatário.
ID do cliente	Introduza a ID do cliente.
Chave secreta do cliente	Introduza a chave secreta do cliente.

5. Clique em **OK**.

Configure a conta de armazenamento do Azure

Você deve configurar a conta de armazenamento do Azure no SnapCenter.

A conta de armazenamento do Azure contém detalhes sobre a ID da subscrição, a credencial do Azure e a conta do Azure NetApp.

As licenças padrão e a licença baseada em capacidade não são necessárias para o Azure NetApp Files.

Passos

1. No painel de navegação esquerdo, clique em **Storage Systems**.
2. Na página sistemas de armazenamento, selecione **Azure NetApp Files** e clique em **novo**.
3. Selecione a credencial, a ID da assinatura e a conta do NetApp nas respetivas listas suspensas.
4. Clique em **Enviar**.

Crie a credencial para adicionar o host do plug-in

O SnapCenter usa credenciais para autenticar usuários para operações do SnapCenter.

Você deve criar credenciais para instalar plug-ins do SnapCenter e credenciais adicionais para executar operações de proteção de dados.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credential**.
3. Clique em **novo**.
4. Na página Credential (credencial), especifique as seguintes informações necessárias para criar a credencial.

Para este campo…	Faça isso…
Nome da credencial	Introduza um nome para a credencial.
Modo de autenticação	Selecione o modo de autenticação na lista pendente.
Tipo de autenticação	Selecione **baseado em senha** ou **baseado em chave SSH** (somente para host Linux).
Nome de utilizador	Especifique o nome de usuário.
Palavra-passe	Se tiver selecionado a autenticação baseada na palavra-passe, especifique a palavra-passe.
Chave privada SSH	Se você selecionou a autenticação baseada em chave SSH, especifique a chave privada.
Use sudo Privileges	Marque a caixa de seleção usar sudo Privileges se estiver criando credenciais para um usuário que não seja root. Isso é aplicável apenas para usuários Linux.

5. Clique em **OK**.

Proteger bancos de dados SAP HANA

Adicione hosts e instale o plug-in do SnapCenter para banco de dados SAP HANA

Você deve usar a página Adicionar host do SnapCenter para adicionar hosts e, em seguida, instalar os pacotes de plug-ins. Os plug-ins são instalados automaticamente

nos hosts remotos.

Antes de começar

- Você deve ser um usuário atribuído a uma função que tenha as permissões de instalação e desinstalação do plug-in, como a função Administrador do SnapCenter.
- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar o UAC no host.
- Se você estiver instalando no host centralizado, verifique se o software cliente SAP HANA está instalado nesse host e abra as portas necessárias no host de banco de dados SAP HANA para executar as consultas SQL do HDB remotamente.

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Verifique se a guia **hosts gerenciados** está selecionada.
3. Clique em **Add**.
4. Na página hosts, execute as seguintes ações:
   a. No campo Host Type (tipo de host), selecione o tipo de host.
   b. No campo Nome do host, insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host.
   c. No campo credenciais, insira a credencial que você criou.
5. Na seção Selecionar plug-ins para instalar, selecione os plug-ins a instalar.
6. (Opcional) clique em **mais Opções** e especifique os detalhes.
7. Clique em **Enviar**.
8. Se o tipo de host for Linux, verifique a impressão digital e clique em **Confirm and Submit**.

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

9. Monitorize o progresso da instalação.

Adicionar banco de dados SAP HANA

Você deve adicionar o banco de dados SAP HANA manualmente.

Sobre esta tarefa

Os recursos precisam ser adicionados manualmente se o plug-in estiver instalado em um servidor centralizado. Se o plug-in SAP HANA estiver instalado no host do banco de dados HANA, o sistema HANA será descoberto automaticamente.

A detecção automática não é compatível com a configuração de vários host HANA, ela precisa ser adicionada somente por meio de plug-in centralizado.

Passos

1. No painel de navegação à esquerda, selecione o plug-in do SnapCenter para banco de dados SAP HANA na lista suspensa e clique em **recursos**.
2. Na página recursos, clique em **Adicionar banco de dados SAP HANA**.

3. Na página fornecer detalhes do recurso, execute as seguintes ações:
    a. Insira o tipo de recurso como contentor único, recipiente de banco de dados multitenant ou volume não-dados.
    b. Introduza o nome do sistema SAP HANA.
    c. Introduza a ID do sistema (SID).
    d. Selecione o host do plug-in.
    e. Digite a chave para se conetar ao sistema SAP HANA.
    f. Introduza o nome de utilizador para o qual a chave de armazenamento de utilizador seguro HDB está configurada.
4. Na página fornecer espaço físico de armazenamento, selecione **Azure NetApp Files** como o tipo de armazenamento.
    a. Selecione a conta do Azure NetApp.
    b. Selecione o pool de capacidade e os volumes associados.
    c. Clique em **Salvar**.
5. Revise o resumo e clique em **Finish**.

Criar políticas de backup para bancos de dados SAP HANA

Antes de usar o SnapCenter para fazer backup dos recursos do banco de dados do SAP HANA, você precisa criar uma política de backup para o recurso ou grupo de recursos que deseja fazer backup.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **políticas**.
3. Clique em **novo**.
4. Na página Nome, insira o nome e a descrição da política.
5. Na página tipo de política, execute as seguintes etapas:
    a. Selecione **Azure NetApp Files** como o tipo de armazenamento.
    b. Selecione **File-based** (baseado em ficheiros) se pretender efetuar uma verificação de integridade da base de dados.
    c. Selecione **Snapshot based** se quiser criar um backup usando a tecnologia Snapshot.
6. Na página Snapshot e backup, execute as seguintes etapas:
    a. Selecione a frequência da cópia de segurança agendada.
    b. Especifique as definições de retenção.
    c. Se você quiser habilitar o backup do Azure NetApp Files, selecione **Ativar backup** e especifique as configurações de retenção.
7. Revise o resumo e clique em **Finish**.

Crie grupos de recursos e anexe políticas de backup do SAP HANA

Um grupo de recursos é o contentor ao qual você deve adicionar recursos que deseja

fazer backup e proteger.

Um grupo de recursos permite fazer backup de todos os dados associados a um determinado aplicativo simultaneamente. Um grupo de recursos é necessário para qualquer trabalho de proteção de dados. Você também deve anexar uma ou mais políticas ao grupo de recursos para definir o tipo de tarefa de proteção de dados que deseja executar.

Passos

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

Para este campo…	Faça isso…
Nome	Introduza um nome para o grupo de recursos.
Tags	Insira um ou mais rótulos que o ajudarão a pesquisar posteriormente o grupo de recursos.
Use o formato de nome personalizado para cópia Snapshot	Marque essa caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.

4. Na página recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Resource Type**.
5. Selecione os recursos na seção **recursos disponíveis** e clique na seta para a direita para movê-los para a seção **recursos selecionados**.
6. Na página políticas, execute as seguintes etapas:
   a. Selecione uma ou mais políticas na lista suspensa.
   b. Na coluna Configurar agendas, clique em + para a política que deseja configurar.
   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e clique em **OK**.
7. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
8. Revise o resumo e clique em **Finish**.

Fazer backup de bancos de dados SAP HANA executados no Azure NetApp Files

Se um recurso ainda 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, em seguida, selecione o plug-in apropriado na lista.
2. Na página recurso, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

3. Selecione o recurso que você deseja fazer backup.
4. Na página recurso, selecione **Use o formato de nome personalizado para cópia Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.
5. Na página Configurações do aplicativo, faça o seguinte:
   a. Selecione a seta **backups** para definir opções de backup adicionais.
   b. Selecione a seta **Scripts** para executar comandos pré e POST para operações quiesce, Snapshot e unquiesce.
   c. Selecione a seta **Custom Configurations** (Configurações personalizadas) e, em seguida, insira os pares de valores personalizados necessários para todos os trabalhos que utilizam este recurso.
   d. Selecione a ferramenta **cópia Snapshot > SnapCenter sem consistência do sistema de arquivos** para criar snapshots.

      A opção **consistência do sistema de arquivos** é aplicável apenas para aplicativos executados em hosts Windows.
6. Na página políticas, execute as seguintes etapas:
   a. Selecione uma ou mais políticas na lista suspensa.
   b. Selecione * * na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.
   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e selecione **OK**.

      policy_name é o nome da política selecionada.
7. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. O SMTP também deve ser configurado em **Configurações** > **Configurações globais**.
8. Revise o resumo e selecione **Finish**.
9. Selecione **fazer uma cópia de segurança agora**.
10. Na página Backup, execute as seguintes etapas:
    a. Se várias políticas estiverem associadas 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.
11. Selecione **Backup**.
12. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Fazer backup de grupos de recursos do SAP HANA

Um grupo de recursos é uma coleção de recursos em um host. Uma operação de backup no grupo de recursos é executada em todos os recursos definidos no grupo de

recursos.

Passos

1. No painel de navegação esquerdo, selecione **Resources** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Grupo de recursos** na lista **Exibir**.
3. Na página grupos de recursos, selecione o grupo de recursos que você deseja fazer backup e selecione **fazer backup agora**.
4. Na página Backup, execute as seguintes etapas:
   a. Se várias políticas estiverem associadas ao grupo de recursos, na lista suspensa **Política**, selecione a política que deseja usar para backup.

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

   b. Selecione **Backup**.
5. Monitorize o progresso da operação selecionando **Monitor** > **trabalhos**.

Restaure e recupere bancos de dados do SAP HANA

Você pode restaurar e recuperar dados dos backups.

Sobre esta tarefa

Para sistemas HANA detetados automaticamente, se a opção **recurso completo** estiver selecionada, a restauração será executada usando a tecnologia de restauração de snapshot de Arquivo único. Se a caixa de seleção **Fast Restore** estiver selecionada, a tecnologia volume Revert será usada.

Para recursos adicionados manualmente, a tecnologia de reversão de volume é sempre usada.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.
3. Selecione o recurso ou selecione um grupo de recursos e, em seguida, selecione um recurso nesse grupo.
4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).
5. Na tabela de backup principal, selecione o backup do qual você deseja restaurar e clique em * *  .
6. Na página Restaurar escopo, selecione **recurso completo**.

   Todos os volumes de dados configurados do banco de dados SAP HANA são restaurados.

7. Para sistemas HANA detetados automaticamente, na página escopo de recuperação, execute as seguintes ações:
   a. Selecione **Recover to most recent State** (recuperar para o estado mais recente) se pretender recuperar o mais próximo possível da hora atual.
   b. Selecione **Recover to Point in Time** se você quiser recuperar para o ponto especificado no tempo.

c. Selecione **Recover to specified data backup** se você quiser recuperar para um backup de dados específico.

d. Selecione **sem recuperação** se não quiser recuperar agora.

e. Especifique as localizações de cópia de segurança do registo.

f. Especifique o local do catálogo de backup.

8. Na página operações anteriores, insira pré-restauração e desmonte comandos para serem executados antes de executar um trabalho de restauração.
9. Na página Post OPS, insira os comandos mount e POST Restore para serem executados após a execução de um trabalho de restauração.
10. 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. O SMTP também deve ser configurado na página **Configurações** > **Configurações globais**.

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

Clone o backup do banco de dados SAP HANA

Você pode usar o SnapCenter para clonar um banco de dados SAP HANA usando o backup do banco de dados. Os clones criados são clones espessos e são criados no pool de capacidade pai.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.
3. Selecione o grupo de recursos ou recursos.
4. Na exibição Gerenciar cópias, selecione **backups** no sistema de armazenamento primário.
5. Selecione o backup de dados na tabela e clique em .
6. Na página localização, execute as seguintes ações:

   a. Selecione o host que tem o plug-in SAP HANA instalado para gerenciar o sistema HANA clonado.

      Ele pode ser um host plug-in centralizado ou um host de sistema HANA.

      Se o plug-in HANA for instalado em um host centralizado que gerencia bancos de DADOS HANA em outros hosts, ao criar ou excluir clones, o SnapCenter descartará intencionalmente as operações do lado do host (montar ou desmontar o sistema de arquivos), pois o servidor de destino é um host centralizado. Você deve usar scripts personalizados pré ou pós-clone para executar operações de montagem e desmontagem.

   a. Insira o SID do SAP HANA para clonar dos backups existentes.

   b. Insira endereços IP ou os nomes de host nos quais os volumes clonados serão exportados.

   c. Se os volumes de ANF do banco de dados SAP HANA estiverem configurados em um pool de CAPACIDADE DE QOS manual, especifique a QOS para os volumes clonados.

Se A QOS para os volumes clonados não for especificada, a QOS do volume de origem será usada. Se o pool de capacidade DE QOS automático for usado, o valor DE QOS especificado será ignorado.

7. Na página Scripts, execute as seguintes etapas:
   a. Digite os comandos para pré-clone ou pós-clone que devem ser executados antes ou depois da operação clone, respetivamente.
   b. Digite o comando mount para montar um sistema de arquivos em um host.

      Se o SISTEMA HANA de origem for descoberto automaticamente e o plug-in de host de destino clone for instalado no host SAP HANA, o SnapCenter removerá automaticamente os volumes de DADOS HANA existentes no host clone de destino e montará os volumes de DADOS HANA recém clonados.
8. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
9. Revise o resumo e clique em **Finish**.
10. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

> O clone Split está desativado para clones do ANF porque o clone do ANF já é um volume independente criado a partir do Snapshot selecionado.

Proteja bancos de dados Microsoft SQL Server

Adicione hosts e instale o plug-in do SnapCenter para o banco de dados SQL Server

O SnapCenter é compatível com a proteção de dados de instâncias SQL em compartilhamentos SMB no Azure NetApp Files. As configurações do grupo de disponibilidade e independente (AG) são suportadas.

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

Antes de começar

- Você deve ser um usuário atribuído a uma função que tenha as permissões de instalação e desinstalação do plug-in, como a função Administrador do SnapCenter.
- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar o UAC no host.

Passos

1. No painel de navegação esquerdo, selecione **hosts**.
2. Verifique se a guia **hosts gerenciados** está selecionada na parte superior.
3. Selecione **Adicionar**.
4. Na página hosts, faça o seguinte:
   a. No campo Host Type (tipo de host), selecione o tipo de host.
   b. No campo Nome do host, insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host.

c. No campo credenciais, insira a credencial que você criou.

5. Na seção **Select Plug-ins to Install**, selecione os plug-ins a instalar.
6. (Opcional) clique em **mais Opções** e especifique os detalhes.
7. Selecione **Enviar**.
8. Selecione **Configure log Directory** e, na página Configurar diretório de log do host, insira o caminho SMB do diretório de log do host e clique em **Save**.
9. Clique em **Submit** e monitore o progresso da instalação.

Criar políticas de backup para bancos de dados do SQL Server

Você pode criar uma política de backup para o recurso ou para o grupo de recursos antes de usar o SnapCenter para fazer backup de recursos do SQL Server ou criar uma política de backup no momento em que criar um grupo de recursos ou fazer backup de um único recurso.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **políticas**.
3. Clique em **novo**.
4. Na página Nome, insira o nome e a descrição da política.
5. Na página tipo de política, execute as seguintes etapas:
   a. Selecione **Azure NetApp Files** como o tipo de armazenamento.
   b. Selecione o tipo de cópia de segurança.
      i. Selecione **Backup completo e Log Backup** se quiser fazer backup de arquivos de banco de dados e logs de transações.
      ii. Selecione **Backup completo** se quiser fazer backup apenas dos arquivos do banco de dados.
      iii. Selecione **Log Backup** se quiser fazer backup apenas dos logs de transação.
      iv. Selecione **Backup somente cópia** se quiser fazer backup de seus recursos usando outro aplicativo.
   c. Na seção Configurações do Grupo de disponibilidade, execute as seguintes ações:
      i. Selecione cópia de segurança na réplica de cópia de segurança preferida se pretender efetuar uma cópia de segurança apenas na réplica.
      ii. Selecione a réplica AG primária ou a réplica AG secundária para o backup.
      iii. Selecione a prioridade da cópia de segurança.
6. Na página Snapshot e backup, execute as seguintes etapas:
   a. Selecione a frequência da cópia de segurança agendada.
   b. Especifique as configurações de retenção dependendo do tipo de backup selecionado.
   c. Se você quiser habilitar o backup do Azure NetApp Files, selecione **Ativar backup** e especifique as configurações de retenção.
7. Na página Verificação, execute as seguintes etapas:
   a. Na seção Executar verificação para as seguintes programações de backup, selecione a frequência de

agendamento.

b. Na seção Opções de verificação consistência de banco de dados, execute as seguintes ações:

   i. Selecione **Limit a estrutura de integridade à estrutura física do banco de dados (PHYSICAL_only)** para limitar a verificação de integridade à estrutura física do banco de dados e para detetar páginas rasgadas, falhas de checksum e falhas comuns de hardware que afetam o banco de dados.

   ii. Selecione **suprimir todas as mensagens de informação (NO_INFOMSGS)** para suprimir todas as mensagens informativas.

   Selecionado por predefinição.

   iii. Selecione **Exibir todas as mensagens de erro relatadas por objeto (ALL_ERRORMSGS)** para exibir todos os erros relatados por objeto.

   iv. Selecione **não verifique índices não agrupados (NOINDEX)** se você não quiser verificar índices não agrupados.

   O banco de dados do SQL Server usa o Microsoft SQL Server Database Consistency Checker (DBCC) para verificar a integridade física e lógica dos objetos no banco de dados.

   v. Selecione **Limit as verificações e obtenha os bloqueios em vez de usar uma cópia Snapshot do banco de dados interno (TABLOCK)** para limitar as verificações e obter bloqueios em vez de usar um instantâneo do banco de dados interno.

c. Na seção **Backup de log**, selecione **verificar backup de log após a conclusão** para verificar o backup de log após a conclusão.

d. Na seção **Configurações do script de verificação**, insira o caminho e os argumentos do prescritor ou postscript que devem ser executados antes ou depois da operação de verificação, respetivamente.

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

Crie grupos de recursos e anexe políticas de backup SQL

Um grupo de recursos é o contentor ao qual você deve adicionar recursos que deseja fazer backup e proteger.

Um grupo de recursos permite fazer backup de todos os dados associados a um determinado aplicativo simultaneamente. Um grupo de recursos é necessário para qualquer trabalho de proteção de dados. Você também deve anexar uma ou mais políticas ao grupo de recursos para definir o tipo de tarefa de proteção de dados que deseja executar.

Passos

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

Para este campo…	Faça isso…
Nome	Introduza um nome para o grupo de recursos.

Para este campo…	Faça isso…
Tags	Insira um ou mais rótulos que o ajudarão a pesquisar posteriormente o grupo de recursos.
Use o formato de nome personalizado para cópia Snapshot	Marque essa caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.

4. Na página recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Resource Type**.
5. Selecione os recursos na seção **recursos disponíveis** e clique na seta para a direita para movê-los para a seção **recursos selecionados**.
6. Na página políticas, execute as seguintes etapas:
   a. Selecione uma ou mais políticas na lista suspensa.
   b. Na coluna Configurar agendas, clique em + para a política que deseja configurar.
   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e clique em **OK**.
   d. Selecione o agendador do Microsoft SQL Server.
7. Na página Verificação, execute as seguintes etapas:
   a. Selecione o servidor de verificação.
   b. Selecione a política para a qual pretende configurar o seu agendamento de verificação e, em seguida, clique em * * + .
   c. Selecione **Executar verificação após cópia de segurança** ou **Executar verificação agendada**.
   d. Clique em **OK**.
8. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
9. Revise o resumo e clique em **Finish**.

Faça backup de bancos de dados do SQL Server em execução no Azure NetApp Files

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

Antes de começar

Você deve criar um balanceador de carga, se o Cluster de failover do Azure Windows não tiver um IP de cluster atribuído ou se não estiver acessível a partir do SnapCenter. O IP do balanceador de carga deve ser configurado e acessível a partir do servidor SnapCenter.

Passos

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

2. Na página recurso, selecione **Banco de dados**, **Instância** ou **Grupo de disponibilidade** na lista suspensa Exibir.
3. Na página recurso, selecione **Use o formato de nome personalizado para cópia Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.
4. Na página políticas, execute as seguintes etapas:
   a. Selecione uma ou mais políticas na lista suspensa.
   b. Selecione * * na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.
   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e selecione **OK**.

      policy_name é o nome da política selecionada.

   d. Selecione **Use o agendador do Microsoft SQL Server** e, em seguida, selecione a instância do agendador na lista suspensa **Instância do Agendador** que está associada à política de agendamento.
5. Na página Verificação, execute as seguintes etapas:
   a. Selecione o servidor de verificação.
   b. Selecione a política para a qual pretende configurar o seu agendamento de verificação e, em seguida, clique em * * .
   c. Selecione **Executar verificação após cópia de segurança** ou **Executar verificação agendada**.
   d. Clique em OK.
6. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
7. Revise o resumo e clique em **Finish**.
8. Selecione **fazer uma cópia de segurança agora**.
9. Na página Backup, execute as seguintes etapas:
   a. Se várias políticas estiverem associadas ao recurso, na lista suspensa **Política**, selecione a política que deseja usar para backup.
   b. Selecione **Verify after backup**.
   c. Selecione **Backup**.
10. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Fazer backup de grupos de recursos do SQL Server

Você pode fazer backup dos grupos de recursos que consistem em vários recursos. Uma operação de backup no grupo de recursos é executada em todos os recursos definidos no grupo de recursos.

Passos

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

3. Na página grupos de recursos, selecione o grupo de recursos que você deseja fazer backup e selecione **fazer backup agora**.
4. Na página Backup, execute as seguintes etapas:
    a. Se várias políticas estiverem associadas ao grupo de recursos, na lista suspensa **Política**, selecione a política que deseja usar para backup.
    b. Após o backup, selecione **Verify** para verificar o backup sob demanda.
    c. Selecione **Backup**.
5. Monitorize o progresso da operação selecionando **Monitor** > **trabalhos**.

Restaurar e recuperar bancos de dados do SQL Server

Você pode usar o SnapCenter para restaurar bancos de dados do SQL Server com backup. Restauração de banco de dados é um processo multifásico que copia todos os dados e páginas de log de um backup especificado do SQL Server para um banco de dados especificado.

Sobre esta tarefa

Você deve garantir que a instância de destino para restauração esteja configurada com um usuário de diretório ativo que pertence ao domínio de diretório ADactive SMB e tenha permissões para definir as permissões de arquivo adequadamente. Você deve configurar as credenciais no SnapCenter no nível da instância.

A autenticação SQL para instância de destino não será suportada para configurações SMB. A instância de destino deve ser configurada no SnapCenter com o usuário do diretório ativo com as permissões necessárias.

Se a conta de serviço de serviços de plug-in do SnapCenter não for um usuário de diretório ativo e, ao executar a restauração para um host alternativo, o usuário que tiver o controle total sobre os volumes de origem será necessário para que ele possa ser representado e executar a operação necessária.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista Exibir.
3. Selecione a base de dados ou o grupo de recursos na lista.
4. Na exibição Gerenciar cópias, selecione **backups** no sistema de armazenamento.
5. Selecione a cópia de segurança na tabela e, em seguida, clique no  ícone.
6. Na página Restaurar escopo, selecione uma das seguintes opções:
    a. Selecione **Restaurar o banco de dados para o mesmo host onde o backup foi criado** se você quiser restaurar o banco de dados para o mesmo servidor SQL onde os backups são feitos.
    b. Selecione **Restaurar o banco de dados para um host alternativo** se você quiser que o banco de dados seja restaurado para um servidor SQL diferente no mesmo ou em um host diferente onde os backups são feitos.
7. Na página âmbito de recuperação, selecione uma das seguintes opções:
    a. Selecione **nenhum** quando precisar restaurar somente o backup completo sem nenhum log.
    b. Selecione **todos os backups de log** operação de restauração de backup atualizada para restaurar todos os backups de log disponíveis após o backup completo.

c. Selecione **por backups de log** para executar uma operação de restauração pontual, que restaura o banco de dados com base em logs de backup até o log de backup com a data selecionada.

d. Selecione **por data específica até** para especificar a data e a hora após as quais os logs de transação não são aplicados ao banco de dados restaurado.

e. Se tiver selecionado **todos os backups de log**, **por backups de log** ou **por data específica até** e os logs estiverem localizados em um local personalizado, selecione **usar diretório de log personalizado** e especifique o local do log.

8. Na página Pré-operações e Pós-operações, especifique os detalhes necessários.
9. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
10. Revise o resumo e clique em **Finish**.
11. Monitorize o processo de restauro utilizando a página **Monitor** > **trabalhos**.

Clone backup do banco de dados SQL Server

Você pode usar o SnapCenter para clonar um banco de dados SQL usando o backup do banco de dados. Os clones criados são clones espessos e são criados no pool de capacidade pai.

Sobre esta tarefa

Você deve garantir que a instância de destino para clone esteja configurada com um usuário de diretório ativo que pertence ao domínio de diretório SMB ADactive e tenha permissões para definir as permissões de arquivo adequadamente. Você deve configurar as credenciais no SnapCenter no nível da instância.

A autenticação SQL para instância de destino não será suportada para configurações SMB. A instância de destino deve ser configurada no SnapCenter com o usuário do diretório ativo com as permissões necessárias.

Se a conta de serviço de serviços de plug-in do SnapCenter não for um usuário de diretório ativo, então, durante a execução do clone, o usuário que tiver controle total sobre os volumes de origem será necessário para que ele possa ser representado e executar a operação necessária.

Passos

1. No painel de navegação esquerdo, selecione **Resources** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados ou o grupo de recursos.
4. Na página de exibição **Gerenciar cópias**, selecione o backup do sistema de armazenamento primário.
5. Selecione a cópia de segurança e, em seguida, selecione  *.
6. Na página **Clone Options**, forneça todos os detalhes necessários.
7. Na página local, selecione um local de armazenamento para criar um clone.

   Se os volumes do ANF do banco de dados do SQL Server estiverem configurados em um pool de CAPACIDADE DE QOS manual, especifique a QOS para os volumes clonados.

   Se A QOS para os volumes clonados não for especificada, a QOS do volume de origem será usada. Se o pool de capacidade DE QOS automático for usado, o valor DE QOS especificado será ignorado.

8. Na página Logs, selecione uma das seguintes opções:
    a. Selecione **nenhum** se você quiser clonar apenas o backup completo sem nenhum log.
    b. Selecione **todos os backups de log** se quiser clonar todos os backups de log disponíveis datados após o backup completo.
    c. Selecione **por backups de log até** se você quiser clonar o banco de dados com base nos logs de backup criados até o log de backup com a data selecionada.
    d. Selecione **por data específica até** se você não quiser aplicar os logs de transação após a data e hora especificadas.
9. Na página **Script**, insira o tempo limite do script, o caminho e os argumentos do prescritor ou postscript que devem ser executados antes ou depois da operação clone, respetivamente.
10. Na página **notificação**, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
11. Revise o resumo e selecione **Finish**.
12. Monitorize o progresso da operação selecionando **Monitor** > **trabalhos**.

Execute o ciclo de vida do clone

Com o SnapCenter, você pode criar clones de um grupo de recursos ou banco de dados. Você pode executar um clone sob demanda ou agendar operações de clone recorrentes de um grupo de recursos ou banco de dados. Se você clonar um backup periodicamente, poderá usar o clone para desenvolver aplicativos, preencher dados ou recuperar dados.

Passos

1. No painel de navegação esquerdo, selecione **Resources** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados ou o grupo de recursos.
4. Na página de exibição **Gerenciar cópias**, selecione o backup do sistema de armazenamento primário.
5. Selecione a cópia de segurança e, em seguida, selecione  *.
6. Na página **Clone Options**, forneça todos os detalhes necessários.
7. Na página local, selecione um local de armazenamento para criar um clone.

    Se os volumes do ANF do banco de dados do SQL Server estiverem configurados em um pool de CAPACIDADE DE QOS manual, especifique a QOS para os volumes clonados.

    Se A QOS para os volumes clonados não for especificada, a QOS do volume de origem será usada. Se o pool de capacidade DE QOS automático for usado, o valor DE QOS especificado será ignorado.

8. Na página **Script**, insira o tempo limite do script, o caminho e os argumentos do prescritor ou postscript que devem ser executados antes ou depois da operação clone, respetivamente.
9. Na página Agendar, execute uma das seguintes ações:
    - Selecione **Executar agora** se quiser executar a tarefa clone imediatamente.
    - Selecione **Configurar agendamento** quando quiser determinar com que frequência a operação de clone deve ocorrer, quando a programação de clones deve ser iniciada, em que dia a operação de clone deve ocorrer, quando a programação deve expirar e se os clones devem ser excluídos após a expiração da programação.

10. Na página **notificação**, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
11. Revise o resumo e selecione **Finish**.
12. Monitorize o progresso da operação selecionando **Monitor** > **trabalhos**.

Proteger bancos de dados Oracle

Adicione hosts e instale o plug-in do SnapCenter para o banco de dados Oracle

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

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

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Verifique se a guia **hosts gerenciados** está selecionada.
3. Clique em **Add**.
4. Na página hosts, execute as seguintes ações:
   a. No campo Host Type (tipo de host), selecione o tipo de host.
   b. No campo Nome do host, insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host.
   c. No campo credenciais, insira a credencial que você criou.
5. Na seção Selecionar plug-ins para instalar, selecione os plug-ins a instalar.
6. (Opcional) clique em **mais Opções** e especifique os detalhes.
7. Clique em **Enviar**.
8. Verifique a impressão digital e clique em **Confirm and Submit**.

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

9. Monitorize o progresso da instalação.

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.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **políticas**.
3. Selecione Oracle Database na lista suspensa.

4. Clique em **novo**.
5. Na página Nome, insira o nome e a descrição da política.
6. Na página tipo de política, execute as seguintes etapas:
   a. Selecione **Azure NetApp Files** como o tipo de armazenamento.
   b. Selecione o tipo de cópia de segurança como cópia de segurança online ou offline.
   c. Se você quiser catalogar o backup usando o Oracle Recovery Manager (RMAN), selecione **Catálogo de backup com o Oracle Recovery Manager (RMAN)**.
   d. Se você quiser podar logs de arquivo após o backup, selecione **Prune archive logs after backup**.
   e. Especifique as definições do registo de eliminação de arquivo.
7. Na página Snapshot e backup, execute as seguintes etapas:
   a. Selecione a frequência da cópia de segurança agendada.
   b. Especifique as definições de retenção.
   c. Se você quiser habilitar o backup do Azure NetApp Files, selecione **Ativar backup** e especifique as configurações de retenção.
8. 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.
9. Na página Verificação, selecione a agenda de backup para a qual deseja executar a operação de verificação e insira o caminho e os argumentos do prescritor ou postscript que deseja executar antes ou depois da operação de verificação, respetivamente.
10. Revise o resumo e clique em **Finish**.

Crie grupos de recursos e anexe políticas de backup Oracle

Um grupo de recursos é o contentor ao qual você deve adicionar recursos que deseja fazer backup e proteger.

Um grupo de recursos permite fazer backup de todos os dados associados a um determinado aplicativo simultaneamente. Um grupo de recursos é necessário para qualquer trabalho de proteção de dados. Você também deve anexar uma ou mais políticas ao grupo de recursos para definir o tipo de tarefa de proteção de dados que deseja executar.

Passos

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

Para este campo…	Faça isso…
Nome	Introduza um nome para o grupo de recursos.
Tags	Insira um ou mais rótulos que o ajudarão a pesquisar posteriormente o grupo de recursos.

Para este campo…	Faça isso…
Use o formato de nome personalizado para cópia Snapshot	Marque essa caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.
Destino do ficheiro de registo de arquivo	Especifique os destinos dos ficheiros de registo de arquivo.

4. Na página recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Resource Type**.
5. Selecione os recursos na seção **recursos disponíveis** e clique na seta para a direita para movê-los para a seção **recursos selecionados**.
6. Na página políticas, execute as seguintes etapas:
   a. Selecione uma ou mais políticas na lista suspensa.
   b. Na coluna Configurar agendas, clique em + para a política que deseja configurar.
   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e clique em **OK**.
7. Na página Verificação, execute as seguintes etapas:
   a. Selecione o servidor de verificação.
   b. Selecione a política para a qual deseja configurar o agendamento de verificação e clique em * + .
   c. Selecione **Executar verificação após cópia de segurança** ou **Executar verificação agendada**.
   d. Clique em **OK**.
8. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
9. Revise o resumo e clique em **Finish**.

Faça backup de bancos de dados Oracle em execução no Azure NetApp Files

Se um recurso ainda 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, em seguida, selecione o plug-in apropriado na lista.
2. Na página recurso, selecione **Banco de dados** na lista suspensa Exibir.
3. Na página recurso, selecione **Use o formato de nome personalizado para cópia Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.
4. Na página políticas, execute as seguintes etapas:
   a. Selecione uma ou mais políticas na lista suspensa.
   b. Selecione + * * na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.

c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e selecione **OK**.

5. Na página Verificação, execute as seguintes etapas:
   a. Selecione o servidor de verificação.
   b. Selecione a política para a qual pretende configurar o seu agendamento de verificação e, em seguida, clique em * * .
   c. Selecione **Executar verificação após cópia de segurança** ou **Executar verificação agendada**.
   d. Clique em OK.
6. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
7. Revise o resumo e clique em **Finish**.
8. Selecione **fazer uma cópia de segurança agora**.
9. Na página Backup, execute as seguintes etapas:
   a. Se várias políticas estiverem associadas ao recurso, na lista suspensa **Política**, selecione a política que deseja usar para backup.
   b. Clique em **Backup**.
10. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Fazer backup de grupos de recursos Oracle

Você pode fazer backup dos grupos de recursos que consistem em vários recursos. Uma operação de backup no grupo de recursos é executada em todos os recursos definidos no grupo de recursos.

Passos

1. No painel de navegação esquerdo, selecione **Resources** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Grupo de recursos** na lista **Exibir**.
3. Na página grupos de recursos, selecione o grupo de recursos que você deseja fazer backup e selecione **fazer backup agora**.
4. Na página Backup, execute as seguintes etapas:
   a. Se várias políticas estiverem associadas ao grupo de recursos, na lista suspensa **Política**, selecione a política que deseja usar para backup.
   b. Selecione **Backup**.
5. Monitorize o progresso da operação selecionando **Monitor** > **trabalhos**.

Restaurar e recuperar bancos de dados Oracle

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

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista Exibir.
3. Selecione a base de dados ou o grupo de recursos na lista.
4. Na exibição Gerenciar cópias, selecione **backups** no sistema de armazenamento primário.
5. Selecione a cópia de segurança na tabela e, em seguida, clique em *  .
6. Na página Restaurar escopo, execute as seguintes tarefas:
   a. Selecione RAC se tiver selecionado um backup de um banco de dados no ambiente RAC.
   b. Execute as seguintes ações:
      i. Selecione **todos os dados** se desejar restaurar apenas os arquivos do banco de dados.
      ii. Selecione **tablespaces** se você quiser restaurar apenas as tablespaces.
      iii. Selecione **Refazer arquivos de log** se quiser restaurar os arquivos de log refazer dos bancos de dados de espera do Data Guard ou do ative Data Guard.
      iv. Selecione **bancos de dados conetáveis** e especifique as PDBs que você deseja restaurar.
      v. Selecione * espaços de tabela de base de dados Pluggable (PDB)* e especifique o PDB e os espaços de tabela desse PDB que você deseja restaurar.
      vi. Selecione **Restaurar o banco de dados para o mesmo host onde o backup foi criado** se você quiser restaurar o banco de dados para o mesmo servidor SQL onde os backups são feitos.
      vii. Selecione **Restaurar o banco de dados para um host alternativo** se você quiser que o banco de dados seja restaurado para um servidor SQL diferente no mesmo ou em um host diferente onde os backups são feitos.
      viii. Selecione **altere o estado do banco de dados, se necessário, para restaurar e recuperar** para alterar o estado do banco de dados para o estado necessário para executar operações de restauração e recuperação.
      ix. Selecione **forçar restauração no local** se você quiser executar a restauração no local nos cenários em que novos arquivos de dados são adicionados após o backup ou quando LUNs são adicionados, excluídos ou recriados a um grupo de discos LVM.
7. Na página âmbito de recuperação, selecione uma das seguintes opções:
   a. Selecione **todos os Logs** se quiser recuperar para a última transação.
   b. Selecione **Until SCN (System Change Number)** se quiser recuperar para um SCN específico.
   c. Selecione **Data e hora** se quiser recuperar para uma data e hora específicas.
   d. Selecione **sem recuperação** se não quiser recuperar.
   e. Selecione **especificar locais de registo de arquivo externo** se pretender especificar a localização dos ficheiros de registo de arquivo externo.
8. Na página Pré-operações e Pós-operações, especifique os detalhes necessários.
9. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
10. Revise o resumo e clique em **Finish**.
11. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Restaure e recupere espaços de tablespaces usando recuperação ponto no tempo

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

Passos

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

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

5. Selecione a cópia de segurança catalogada e, em seguida, clique em *  .
6. Na página Restaurar escopo, execute as seguintes tarefas:
   a. Selecione **RAC** se tiver selecionado um backup de um banco de dados no ambiente RAC.
   b. Selecione **tablespaces** se você quiser restaurar apenas as tablespaces.
   c. Selecione **altere o estado do banco de dados, se necessário, para restaurar e recuperar** para alterar o estado do banco de dados para o estado necessário para executar operações de restauração e recuperação.
7. Na página âmbito de recuperação, selecione uma das seguintes opções:
   a. Selecione **Until SCN (System Change Number)** se quiser recuperar para um SCN específico.
   b. Selecione **Data e hora** se quiser recuperar para uma data e hora específicas.
8. Na página Pré-operações e Pós-operações, especifique os detalhes necessários.
9. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
10. Revise o resumo e clique em **Finish**.
11. Monitorize o processo de restauro utilizando a página **Monitor** > **trabalhos**.

Restaurar e recuperar banco de dados conetável usando recuperação pontual

Você pode restaurar e recuperar um banco de dados conetável (PDB) que foi corrompido ou descartado sem afetar as outras PDBs no banco de dados de contentores (CDB). O SnapCenter usa o RMAN para executar a recuperação pontual (PITR) do PDB.

Passos

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

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

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

6. Na página Restaurar escopo, execute as seguintes tarefas:
   a. Selecione **RAC** se tiver selecionado um backup de um banco de dados no ambiente RAC.
   b. Dependendo se você deseja restaurar o PDB ou espaços de tabela em um PDB, execute uma das ações:
      - Selecione **bancos de dados conetáveis (PDBs)** se você quiser restaurar um PDB.
      - Selecione * espaços de tabela de base de dados Pluggable (PDB)* se quiser restaurar espaços de tabela em um PDB.
7. Na página âmbito de recuperação, selecione uma das seguintes opções:
   a. Selecione **Until SCN (System Change Number)** se quiser recuperar para um SCN específico.
   b. Selecione **Data e hora** se quiser recuperar para uma data e hora específicas.
8. Na página Pré-operações e Pós-operações, especifique os detalhes necessários.
9. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
10. Revise o resumo e clique em **Finish**.
11. Monitorize o processo de restauro utilizando a página **Monitor** > **trabalhos**.

Clone backup de banco de dados Oracle

Você pode usar o SnapCenter para clonar um banco de dados Oracle usando o backup do banco de dados. Os clones criados são clones espessos e são criados no pool de capacidade pai.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista Exibir.
3. Selecione a base de dados.
4. Na página de exibição Gerenciar cópias, selecione o backup no sistema de storage primário.
5. Selecione a cópia de segurança de dados e, em seguida, clique em *  .
6. Na página Nome, selecione se deseja clonar um banco de dados (CDB ou não CDB) ou clonar um banco de dados conetável (PDB).
7. Na página localizações, especifique os detalhes necessários.

   Se os volumes do ANF do banco de dados Oracle estiverem configurados em um pool de CAPACIDADE DE QOS manual, especifique a QOS para os volumes clonados.

   Se A QOS para os volumes clonados não for especificada, a QOS do volume de origem será usada. Se o pool de capacidade DE QOS automático for usado, o valor DE QOS especificado será ignorado.

8. Na página credenciais, execute um dos seguintes procedimentos:
   a. Para o nome da credencial para o usuário do sys, selecione a credencial a ser usada para definir a senha do usuário do sys do banco de dados clone.
   b. Para o nome da credencial da instância ASM, selecione **nenhum** se a autenticação do sistema operacional estiver ativada para conexão com a instância ASM no host clone.

Caso contrário, selecione a credencial Oracle ASM configurada com um usuário "sys" ou um usuário com privilégio "sysasm" aplicável ao host clone.

9. Na página Pre-Ops, especifique o caminho e os argumentos dos prescripts e na seção Configurações de parâmetros de banco de dados, modifique os valores dos parâmetros de banco de dados pré-preenchidos que são usados para inicializar o banco de dados.
10. Na página Pós-operações, **recuperar banco de dados** e **até Cancelar** são selecionados por padrão para executar a recuperação do banco de dados clonado.
    a. Se você selecionar **Until Cancel**, o SnapCenter executa a recuperação montando o backup de log mais recente com a sequência ininterrupta de logs de arquivamento após esse backup de dados que foi selecionado para clonagem.
    b. Se você selecionar **Data e hora**, o SnapCenter recupera o banco de dados até uma data e hora especificadas.
    c. Se você selecionar **até SCN**, o SnapCenter recupera o banco de dados até um SCN especificado.
    d. Se você selecionar **especificar locais de log de arquivo externo**, o SnapCenter identifica e monta o número ideal de backups de log com base na SCN especificada ou na data e hora selecionadas.
    e. Por padrão, a caixa de seleção **Create new DBID** está selecionada para gerar um número único (DBID) para o banco de dados clonado diferenciando-o do banco de dados de origem.

       Desmarque a caixa de seleção se quiser atribuir o DBID do banco de dados de origem ao banco de dados clonado. Nesse cenário, se você quiser Registrar o banco de dados clonado com o catálogo RMAN externo onde o banco de dados de origem já está registrado, a operação falha.

    f. Marque a caixa de seleção **Create tempfile for temporary tablespace** se quiser criar um tempfile para o espaço de tabela temporário padrão do banco de dados clonado.
    g. Em **Digite entradas sql para aplicar quando o clone for criado**, adicione as entradas sql que você deseja aplicar quando o clone for criado.
    h. Em **Digite scripts para serem executados após a operação clone**, especifique o caminho e os argumentos do postscript que você deseja executar após a operação clone.
11. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
12. Revise o resumo e selecione **Finish**.
13. Monitorize o progresso da operação selecionando **Monitor** > **trabalhos**.

Clone um banco de dados conetável

Você pode clonar um banco de dados conetável (PDB) para um CDB diferente ou mesmo destino no mesmo host ou host alternativo. Você também pode recuperar o PDB clonado para uma SCN ou data e hora desejadas.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista Exibir.
3. Selecione o banco de dados do tipo instância única (multitenant).
4. Na página de exibição Gerenciar cópias, selecione o backup no sistema de storage primário.
5. Selecione a cópia de segurança e, em seguida, clique em  *.

6. Na página Nome, selecione **Clonar PDB** e especifique os outros detalhes.
7. Na página localizações, especifique os detalhes necessários.
8. Na página Pre-Ops, especifique o caminho e os argumentos dos prescripts e na seção Configurações de parâmetros de banco de dados, modifique os valores dos parâmetros de banco de dados pré-preenchidos que são usados para inicializar o banco de dados.
9. Na página Pós-operações, **Until Cancel** é selecionado por padrão para executar a recuperação do banco de dados clonado.
    a. Se você selecionar **Until Cancel**, o SnapCenter executa a recuperação montando o backup de log mais recente com a sequência ininterrupta de logs de arquivamento após esse backup de dados que foi selecionado para clonagem.
    b. Se você selecionar **Data e hora**, o SnapCenter recupera o banco de dados até uma data e hora especificadas.
    c. Se você selecionar **especificar locais de log de arquivo externo**, o SnapCenter identifica e monta o número ideal de backups de log com base na SCN especificada ou na data e hora selecionadas.
    d. Por padrão, a caixa de seleção **Create new DBID** está selecionada para gerar um número único (DBID) para o banco de dados clonado diferenciando-o do banco de dados de origem.

       Desmarque a caixa de seleção se quiser atribuir o DBID do banco de dados de origem ao banco de dados clonado. Nesse cenário, se você quiser Registrar o banco de dados clonado com o catálogo RMAN externo onde o banco de dados de origem já está registrado, a operação falha.

    e. Marque a caixa de seleção **Create tempfile for temporary tablespace** se quiser criar um tempfile para o espaço de tabela temporário padrão do banco de dados clonado.
    f. Em **Digite entradas sql para aplicar quando o clone for criado**, adicione as entradas sql que você deseja aplicar quando o clone for criado.
    g. Em **Digite scripts para serem executados após a operação clone**, especifique o caminho e os argumentos do postscript que você deseja executar após a operação clone.
10. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
11. Revise o resumo e selecione **Finish**.
12. Monitorize o progresso da operação selecionando **Monitor** > **trabalhos**.

Informações sobre direitos autorais

Informações sobre marcas comerciais