



Proteja aplicativos em execução no Azure NetApp Files

SnapCenter software

NetApp
November 06, 2025

This PDF was generated from <https://docs.netapp.com/pt-br/snapcenter-61/protect-azure/protect-applications-azure-netapp-files.html> on November 06, 2025. Always check docs.netapp.com for the latest.

Índice

Proteja aplicativos em execução no Azure NetApp Files	1
Proteja aplicativos em execução no Azure NetApp Files	1
Limitações	1
Instale o SnapCenter e crie credenciais	1
Instalar o SnapCenter na Máquina Virtual do Azure	1
Crie a credencial do Azure no SnapCenter	3
Configurar a conta de armazenamento do Azure	4
Crie a credencial para adicionar o host do plug-in	4
Proteja bancos de dados SAP HANA	5
Adicionar hosts e instalar o plug-in SnapCenter para o banco de dados SAP HANA	5
Adicionar banco de dados SAP HANA	6
Crie políticas de backup para bancos de dados SAP HANA	6
Crie grupos de recursos e anexe políticas de backup do SAP HANA	7
Fazer backup de bancos de dados SAP HANA em execução no Azure NetApp Files	8
Fazer backup de grupos de recursos do SAP HANA	9
Restaurar e recuperar bancos de dados SAP HANA	9
Clonar backup de banco de dados SAP HANA	10
Proteja bancos de dados do Microsoft SQL Server	11
Adicionar hosts e instalar o plug-in SnapCenter para banco de dados SQL Server	11
Crie políticas de backup para bancos de dados SQL Server	12
Crie grupos de recursos e anexe políticas de backup SQL	14
Fazer backup de bancos de dados do SQL Server em execução no Azure NetApp Files	15
Fazer backup de grupos de recursos do SQL Server	16
Restaurar e recuperar bancos de dados SQL Server	16
Clonar backup do banco de dados SQL Server	17
Proteja bancos de dados Oracle	19
Adicionar hosts e instalar o plug-in SnapCenter para banco de dados Oracle	19
Crie políticas de backup para bancos de dados Oracle	20
Crie grupos de recursos e anexe políticas de backup do Oracle	20
Fazer backup de bancos de dados Oracle em execução no Azure NetApp Files	22
Fazer backup de grupos de recursos Oracle	22
Restaurar e recuperar bancos de dados Oracle	23
Clonar backup do banco de dados Oracle	25

Proteja aplicativos em execução no Azure NetApp Files

Proteja aplicativos em execução no Azure NetApp Files

O SnapCenter oferece suporte à proteção de seus aplicativos, como Oracle, SQL e SAP HANA, que residem no Azure NetApp Files. A partir da versão 6.0.1, o SnapCenter oferece suporte ao recurso de backup do Azure NetApp Files, que expande os recursos de proteção de dados do Azure NetApp Files ao fornecer uma solução de backup totalmente gerenciada para recuperação, arquivamento e conformidade de longo prazo.

O Azure NetApp Files é uma solução de armazenamento premium que pode ser cara para retenção de backup de longo prazo. Para otimizar custos, você pode mover os backups do armazenamento do Azure NetApp Files para um armazenamento de objetos do Azure. A partir do SnapCenter 6.0.1, você pode fazer backup e clonar aplicativos que residem no Azure NetApp Files para o Azure Blob Storage (armazenamento de objetos). Você pode manter duas cópias dos seus dados, cópias de instantâneos de volume no armazenamento do Azure NetApp Files para recuperação de curto prazo e outra cópia no Armazenamento de Blobs do Azure para recuperação de longo prazo.

Quando uma política com backup do Azure NetApp Files é habilitada e associada a um recurso, o SnapCenter lida com a criação de instantâneos de volume e o backup deles no Armazenamento de Blobs do Azure. O SnapCenter cria o Backup Vault e habilita o backup para o volume. Se você tiver habilitado o backup para o volume, o SnapCenter utilizará o cofre existente.

Limitações

- As funcionalidades de armazenamento de objetos para sistemas de armazenamento FAS, ASA ou AFF ONTAP e Amazon FSx for NetApp ONTAP não são suportadas.
- Os fluxos de trabalho de montagem e catálogo do Oracle e SAP HANA não são suportados para backups de armazenamento de objetos, mas são suportados para snapshots.
- Os clones do Oracle PDB não são suportados para backups de armazenamento de objetos, mas são suportados para snapshots.
- A verificação de backup do armazenamento de objetos, o suporte à API REST, o gerenciamento do ciclo de vida do clone do armazenamento de objetos e os recursos de relatório para backups de armazenamento de objetos não são suportados.
- Não há suporte para restauração de backups no Armazenamento de Blobs do Azure para o Azure NetApp Files. Você pode usar a opção clone como alternativa.
- A divisão de clones não é suportada.

Instale o SnapCenter e crie credenciais

Instalar o SnapCenter na Máquina Virtual do Azure

Você pode baixar o SnapCenter software 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 para instalação do SnapCenter Server. Para obter informações, consulte "["Requisitos para instalar o SnapCenter Server"](#)" .
- Se você é novo no Azure NetApp Files e não tem uma conta NetApp existente, certifique-se de ter se registrado para poder acessar o SnapCenter Software. Para obter informações, consulte "["Registre-se para acessar o SnapCenter software"](#)" .

Passos

1. Baixe o pacote de instalação do SnapCenter Server em "["Site de suporte da NetApp"](#)" .
2. Inicie a instalação do SnapCenter Server clicando duas vezes no arquivo .exe baixado.

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

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

Você não precisa especificar a senha para o banco de dados do repositório do MySQL Server. Durante a instalação do SnapCenter Server, 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 algum valor inválido, mensagens de erro apropriadas serão exibidas. Você deve inserir os valores novamente e então iniciar a instalação.



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

Entretanto, se você clicar em **Cancelar** quando as operações "Reinicialização do site do SnapCenter Server" ou "Aguardando o início do SnapCenter Server" estiverem sendo executadas, a instalação prosseguirá sem cancelar a operação.

Registre o produto para habilitar o suporte

Se você é novo na NetApp e não tem uma conta NetApp existente, registre o produto para habilitar o suporte.

Passos

1. Após 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.com> .
4. Clique em *Não sou um cliente registrado da NetApp * .
5. Especifique seus dados para se registrar.
6. Deixe o campo SN de referência da NetApp em branco.
7. Selecione * SnapCenter* no menu suspenso Linha de produtos.

8. Selecione o provedor de cobrança.
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 começar

- Certifique-se de ter criado a entidade de serviço no Azure.
- Certifique-se de ter o ID do locatário, o ID do cliente e a chave secreta associados à entidade de serviço disponíveis.
 - O ID do locatário pode ser encontrado no Portal do Azure, na página Visão geral do ID de entrada.
 - O ID do cliente também é conhecido como ID do aplicativo para o aplicativo/serviço principal corporativo. Isso pode ser encontrado no Portal do Azure, na página Visão geral do aplicativo empresarial que você criou para atuar como a entidade de serviço do SnapCenter.
 - A Chave Secreta do Cliente também é conhecida como Valor Secreto. Você pode criar esse segredo do cliente no Portal do Azure navegando até **Registros de aplicativo** em ID de entrada. Depois de selecionar o aplicativo corporativo que você criou, navegue até **Certificados e segredos** e depois **Novo segredo do cliente**.



O valor secreto só pode ser acessado quando criado. Você não poderá acessá-lo mais tarde.

- O Principal de Serviço precisa receber permissões. A função de Colaborador permitirá que a entidade de serviço execute as ações necessárias no Azure. Isso pode ser concedido na página Controle de Acesso (IAM) na página Assinatura.

Passos

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

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

5. Clique em **OK**.

Configurar 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 o ID da assinatura, a credencial do Azure e a conta do Azure NetApp .



As licenças padrão e baseadas em capacidade não são necessárias para o Azure NetApp Files.

Passos

1. No painel de navegação esquerdo, clique em **Sistemas de armazenamento**.
2. Na página Sistemas de Armazenamento, selecione * Azure NetApp Files* e clique em **Novo**.
3. Selecione a credencial, o ID da assinatura e a conta NetApp nas respectivas 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 **Credencial**.
3. Clique em **Novo**.
4. Na página Credencial, especifique as seguintes informações necessárias para criar a credencial.

Para este campo...	Faça isso...
Nome da credencial	Digite um nome para a credencial.
Modo de autenticação	Selecione o modo de autenticação na lista suspensa.
Tipo de autenticação	Selecione Baseado em senha ou Baseado em chave SSH (somente para host Linux).
Nome de usuário	Especifique o nome de usuário.
Senha	Se você selecionou Autenticação baseada em senha, especifique a senha.

Para este campo...	Faça isso...
Chave privada SSH	Se você selecionou a autenticação baseada em chave SSH, especifique a chave privada.
Use privilégios sudo	Marque a caixa de seleção Usar privilégios sudo se estiver criando credenciais para um usuário não root.  Isso é aplicável somente para usuários do Linux.

5. Clique em **OK**.

Proteja bancos de dados SAP HANA

Adicionar hosts e instalar o plug-in SnapCenter para o 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 permissões de instalação e desinstalação de plug-ins, como a função de administrador do SnapCenter .
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.
- Se você estiver instalando no host centralizado, certifique-se de que o software cliente SAP HANA esteja instalado nesse host e abra as portas necessárias no host do 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 **Adicionar**.
4. Na página Hosts, execute as seguintes ações:
 - a. No campo 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 serem instalados.
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 **Confirmar e Enviar**.

Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós do cluster.

9. Monitore 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 descoberta automática não é suportada para configuração de vários hosts do HANA; eles devem ser adicionados somente por meio de plug-in centralizado.

Passos

1. No painel de navegação esquerdo, selecione o plug-in 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 Contêiner Único, Contêiner de Banco de Dados Multilocatário ou Volume sem dados.
 - b. Digite o nome do sistema SAP HANA.
 - c. Digite o ID do sistema (SID).
 - d. Selecione o host do plug-in.
 - e. Insira a chave para conectar ao sistema SAP HANA.
 - f. Digite o nome de usuário para o qual a chave de armazenamento de usuário seguro do HDB está configurada.
4. Na página Fornecer espaço 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 **Concluir**.

Crie políticas de backup para bancos de dados SAP HANA

Antes de usar o SnapCenter para fazer backup de recursos do banco de dados SAP HANA, você deve 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 **Baseado em arquivo** se quiser executar uma verificação de integridade do banco de dados.
 - c. Selecione **Baseado em instantâneo** se quiser criar um backup usando a tecnologia Snapshot.
6. Na página Snapshot e backup, execute as seguintes etapas:
 - a. Selecione a frequência do backup agendado.
 - b. Especifique as configurações de retenção.
 - c. Se você quiser habilitar o backup do Azure NetApp Files , selecione **Habilitar backup** e especifique as configurações de retenção.
7. Revise o resumo e clique em **Concluir**.

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

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

Um grupo de recursos permite que você faça backup de todos os dados associados a um determinado aplicativo simultaneamente. 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 trabalho de proteção de dados que deseja executar.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** 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	Insira um nome para o grupo de recursos.
Etiquetas	Insira um ou mais rótulos que ajudarão você a pesquisar posteriormente o grupo de recursos.
Use formato de nome personalizado para cópia do Snapshot	Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

4. Na página Recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Tipo de recurso**.
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 agendamentos, clique em  * para a política que você deseja configurar.
 - c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento 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 **Concluir**.

Fazer backup de bancos de dados SAP HANA em execução no Azure NetApp Files

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

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, 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 **Usar formato de nome personalizado para cópia do Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.
5. Na página Configurações do aplicativo, faça o seguinte:
 - a. Selecione a seta **Backups** para definir opções adicionais de backup.
 - b. Selecione a seta **Scripts** para executar comandos pré e pós para operações de inatividade, instantâneo e ativação/desativação.
 - c. Selecione a seta **Configurações personalizadas** e insira os pares de valores personalizados necessários para todos os trabalhos que usam este recurso.
 - d. Selecione a **Ferramenta de cópia de instantâneo > SnapCenter sem consistência do sistema de arquivos** para criar instantâneos.

A opção **Consistência do sistema de arquivos** é aplicável somente 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 agendamentos da política para a qual você deseja configurar um agendamento.
 - c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e selecione **OK**.

policy_name é o nome da política que você selecionou.
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 **Concluir**.
9. Selecione **Fazer backup 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 você 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. Monitore o progresso da operação clicando em **Monitorar > 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 **Recursos** 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 você 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. Monitore o progresso da operação selecionando **Monitor > Trabalhos**.

Restaurar e recuperar bancos de dados SAP HANA

Você pode restaurar e recuperar dados dos backups.

Sobre esta tarefa

Para sistemas HANA descobertos automaticamente, se a opção **Recurso Completo** for selecionada, a restauração será realizada usando a tecnologia de restauração de instantâneo de arquivo único. Se a caixa de seleção **Restauração rápida** estiver selecionada, a tecnologia de reversão de volume será usada.

Para recursos adicionados manualmente, a tecnologia Volume Revert é sempre usada.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, filtre os 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** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Na tabela Backup(s) primário(s), selecione o backup que deseja restaurar e clique em  *.
6. Na página Escopo de restauração, selecione **Recurso completo**.

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

7. Para sistemas HANA descobertos automaticamente, na página Escopo de recuperação, execute as seguintes ações:
 - a. Selecione **Recuperar para o estado mais recente** se quiser recuperar o mais próximo possível do momento atual.
 - b. Selecione **Recuperar para um ponto no tempo** se quiser recuperar para o ponto no tempo especificado.
 - c. Selecione **Recuperar para backup de dados especificado** se quiser recuperar para um backup de dados específico.
 - d. Selecione **Sem recuperação** se não quiser recuperar agora.
 - e. Especifique os locais de backup do log.
 - f. Especifique o local do catálogo de backup.
8. Na página Pré-operações, insira os comandos pre restore e unmount para executar antes de realizar um trabalho de restauração.
9. Na página Post ops, insira os comandos mount e post restore para serem executados após realizar 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 **Concluir**.
12. Monitore o progresso da operação clicando em **Monitorar > Trabalhos**.

Clonar backup de 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 grossos e são criados no pool de capacidade pai.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

3. Selecione o recurso ou grupo de recursos.
4. Na exibição Gerenciar cópias, selecione **Backups** do sistema de armazenamento primário.
5. Selecione o backup de dados da 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.

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



Se o plug-in HANA estiver instalado em um host centralizado que gerencia bancos de dados HANA em outros hosts, ao criar ou excluir clones, o SnapCenter intencionalmente ignorará 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 de pré ou pós-clonagem para executar operações de montagem e desmontagem.

- a. Insira o SID do SAP HANA para clonar dos backups existentes.
- b. Insira os endereços IP ou os nomes de host nos quais os volumes clonados serão exportados.
- c. Se os volumes ANF do banco de dados SAP HANA estiverem configurados em um pool de capacidade de QOS manual, especifique o QOS para os volumes clonados.

Se o QOS para os volumes clonados não for especificado, o QOS do volume de origem será usado. 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. Insira os comandos para pré-clonagem ou pós-clonagem que devem ser executados antes ou depois da operação de clonagem, respectivamente.
- 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 do host de destino do clone estiver instalado no host SAP HANA, o SnapCenter desmontará automaticamente os volumes de dados HANA existentes no host de destino do clone 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 **Concluir**.
10. Monitore o progresso da operação clicando em **Monitorar > Trabalhos**.



A divisão de clones está desabilitada para clones ANF porque o clone ANF já é um volume independente criado a partir do Snapshot selecionado.

Proteja bancos de dados do Microsoft SQL Server

Adicionar hosts e instalar o plug-in SnapCenter para banco de dados SQL Server

O SnapCenter oferece suporte à proteção de dados de instâncias SQL em compartilhamentos SMB no Azure NetApp Files. As configurações autônomas e de

grupo de disponibilidade (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 permissões de instalação e desinstalação de plug-ins, como a função de administrador do SnapCenter .
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.

Passos

1. No painel de navegação esquerdo, selecione **Hosts**.
2. Verifique se a aba **Hosts Gerenciados** está selecionada na parte superior.
3. Selecione **Adicionar**.
4. Na página Hosts, faça o seguinte:
 - a. No campo 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 serem instalados.
6. (Opcional) Clique em **Mais opções** e especifique os detalhes.
7. Selecione **Enviar**.
8. Selecione **Configurar diretório de log** e na página Configurar diretório de log do host, insira o caminho SMB do diretório de log do host e clique em **Salvar**.
9. Clique em **Enviar** e monitore o progresso da instalação.

Crie políticas de backup para bancos de dados SQL Server

Você pode criar uma política de backup para o recurso ou grupo de recursos antes de usar o SnapCenter para fazer backup de recursos do SQL Server ou pode criar uma política de backup no momento em que cria um grupo de recursos ou faz 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 backup.
 - i. Selecione **Backup completo e backup de log** 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 **Backup de Log** se quiser fazer backup apenas dos logs de transações.
 - iv. Selecione **Copiar somente backup** se quiser fazer backup de seus recursos usando outro aplicativo.
- c. Na seção Configurações do grupo de disponibilidade, execute as seguintes ações:
- i. Selecione Fazer backup na réplica de backup preferida se quiser fazer backup somente na réplica.
 - ii. Selecione a réplica do AG primário ou a réplica do AG secundário para o backup.
 - iii. Selecione a prioridade do backup.
6. Na página Snapshot e backup, execute as seguintes etapas:
- a. Selecione a frequência do backup agendado.
 - b. Especifique as configurações de retenção dependendo do tipo de backup selecionado.
 - c. Se você quiser habilitar o backup do Azure NetApp Files , selecione **Habilitar backup** e especifique as configurações de retenção.
7. Na página Verificação, execute as seguintes etapas:
- a. Na seção Executar verificação para os seguintes agendamentos de backup, selecione a frequência do agendamento.
 - b. Na seção Opções de verificação de consistência do banco de dados, execute as seguintes ações:
 - i. Selecione **Limitar 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 detectar páginas quebradas, falhas de soma de verificação e falhas comuns de hardware que afetam o banco de dados.
 - ii. Selecione **Suprimir todas as mensagens informativas (NO_INFOMSGS)** para suprimir todas as mensagens informativas.
- Selecionado por padrão.
- iii. Selecione **Exibir todas as mensagens de erro relatadas por objeto (ALL_ERRORMSG)** para exibir todos os erros relatados por objeto.
 - iv. Selecione **Não verificar índices não agrupados (NOINDEX)** se não quiser verificar índices não agrupados.
- O banco de dados SQL Server usa o Microsoft SQL Server Database Consistency Checker (DBCC) para verificar a integridade lógica e física dos objetos no banco de dados.
- v. Selecione **Limitar as verificações e obter os bloqueios em vez de usar uma cópia de instantâneo do banco de dados interno (TABLOCK)** para limitar as verificações e obter os 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 prescript ou postscript que devem ser executados antes ou depois da operação de verificação, respectivamente.
8. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e anexe políticas de backup SQL

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

Um grupo de recursos permite que você faça backup de todos os dados associados a um determinado aplicativo simultaneamente. 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 trabalho de proteção de dados que deseja executar.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** 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	Insira um nome para o grupo de recursos.
Etiquetas	Insira um ou mais rótulos que ajudarão você a pesquisar posteriormente o grupo de recursos.
Use formato de nome personalizado para cópia do Snapshot	Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

4. Na página Recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Tipo de recurso**.
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 agendamentos, clique em  * para a política que você deseja configurar.
 - c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento 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 deseja configurar seu cronograma de verificação e clique em  *.
 - c. Selecione **Executar verificação após backup** 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 **Concluir**.

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

Se um recurso ainda não fizer parte de nenhum 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 Windows do Azure não tiver um IP de cluster atribuído ou se não puder ser acessado pelo SnapCenter. O IP do balanceador de carga deve ser configurado e acessível a partir do SnapCenter Server.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** 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 **Usar formato de nome personalizado para cópia do Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.
4. Na página Políticas, execute as seguintes etapas:
 - a. Selecione uma ou mais políticas na lista suspensa.
 - b. Selecione *  * na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.
 - c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e selecione **OK**.

policy_name é o nome da política que você selecionou.
 - d. Selecione **Usar o agendador do Microsoft SQL Server** e, em seguida, selecione a instância do agendador na lista suspensa **Instância do agendador** 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 deseja configurar seu cronograma de verificação e clique em *  *.
 - c. Selecione **Executar verificação após backup** 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 **Concluir**.
8. Selecione **Fazer backup 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 você deseja usar para backup.

- b. Selecione **Verificar após backup**.
 - c. Selecione **Backup**.
10. Monitore o progresso da operação clicando em **Monitorar > 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 **Recursos** 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 você deseja usar para backup.
 - b. Após o backup, selecione **Verificar** para verificar o backup sob demanda.
 - c. Selecione **Backup**.
5. Monitore o progresso da operação selecionando **Monitor > Trabalhos**.

Restaurar e recuperar bancos de dados SQL Server

Você pode usar o SnapCenter para restaurar bancos de dados SQL Server com backup. A restauração do 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 do Active Directory que pertença ao domínio do Active Directory do SMB AD 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 Active Directory tendo as permissões necessárias.

Se a conta de serviço do SnapCenter Plug-in não for um usuário do Active Directory, ao executar a restauração no host alternativo, será necessário o usuário que tem controle total sobre os volumes de origem para que ele possa ser representado e executar a operação necessária.

Passos

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

3. Selecione o banco de dados ou o grupo de recursos na lista.
4. Na exibição Gerenciar cópias, selecione **Backups** do sistema de armazenamento.
5. Selecione o backup da tabela e clique em  ícone.
6. Na página Escopo de restauração, selecione uma das seguintes opções:
 - a. Selecione **Restaurar o banco de dados para o mesmo host onde o backup foi criado** se quiser restaurar o banco de dados para o mesmo servidor SQL onde os backups foram feitos.
 - b. Selecione **Restaurar o banco de dados em um host alternativo** se desejar que o banco de dados seja restaurado em um servidor SQL diferente no mesmo host ou em um host diferente onde os backups são feitos.
7. Na página Escopo de Recuperação, selecione uma das seguintes opções:
 - a. Selecione **Nenhum** quando precisar restaurar apenas o backup completo, sem nenhum log.
 - b. Selecione a operação de restauração de backup atualizada **Todos os backups de log** 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 nos 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 transações não serão aplicados ao banco de dados restaurado.
 - e. Se você selecionou **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-operatório e Pós-operatório, 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 **Concluir**.
11. Monitore o processo de restauração usando a página **Monitor > Tarefas**.

Clonar 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 grossos e são criados no pool de capacidade pai.

Sobre esta tarefa

Você deve garantir que a instância de destino para clonagem esteja configurada com um usuário do Active Directory que pertença ao domínio do Active Directory do SMB AD 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 Active Directory tendo as permissões necessárias.

Se a conta de serviço do SnapCenter Plug-in não for um usuário do Active Directory, ao executar a clonagem, será necessário o usuário que tem controle total sobre os volumes de origem para que ele possa ser representado e executar a operação necessária.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** 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 grupo de recursos.
4. Na página de exibição **Gerenciar cópias**, selecione o backup do sistema de armazenamento primário.
5. Selecione o backup e, em seguida, selecione  *.
6. Na página **Opções de Clone**, forneça todos os detalhes necessários.
7. Na página Localização, selecione um local de armazenamento para criar um clone.

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

Se o QOS para os volumes clonados não for especificado, o QOS do volume de origem será usado. 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 quiser clonar apenas o backup completo, sem nenhum registro.
 - 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 quiser clonar o banco de dados com base nos logs de backup que foram criados até o log de backup com a data selecionada.
 - d. Selecione **Por data específica até** se não quiser aplicar os logs de transações após a data e hora especificadas.
9. Na página **Script**, insira o tempo limite do script, o caminho e os argumentos do prescript ou postscript que devem ser executados antes ou depois da operação de clonagem, respectivamente.
10. Na página **Notificação**, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais deseja enviar os e-mails.
11. Revise o resumo e selecione **Concluir**.
12. Monitore o progresso da operação selecionando **Monitor > Trabalhos**.

Executar ciclo de vida do clone

Usando o SnapCenter, você pode criar clones de um grupo de recursos ou banco de dados. Você pode executar uma clonagem sob demanda ou agendar operações de clonagem 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 **Recursos** 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 grupo de recursos.
4. Na página de exibição **Gerenciar cópias**, selecione o backup do sistema de armazenamento primário.
- 5.

Selecione o backup e, em seguida, selecione *  *.

6. Na página **Opções de Clone**, forneça todos os detalhes necessários.
7. Na página Localização, selecione um local de armazenamento para criar um clone.

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

Se o QOS para os volumes clonados não for especificado, o QOS do volume de origem será usado. 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 prescript ou postscript que devem ser executados antes ou depois da operação de clonagem, respectivamente.
9. Na página Agendar, execute uma das seguintes ações:
 - Selecione **Executar agora** se quiser executar o trabalho de clonagem imediatamente.
 - Selecione **Configurar agendamento** quando quiser determinar com que frequência a operação de clonagem deve ocorrer, quando o agendamento de clonagem deve começar, em que dia a operação de clonagem deve ocorrer, quando o agendamento deve expirar e se os clones devem ser excluídos após o agendamento expirar.
10. Na página **Notificação**, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais deseja enviar os e-mails.
11. Revise o resumo e selecione **Concluir**.
12. Monitore o progresso da operação selecionando **Monitor > Trabalhos**.

Proteja bancos de dados Oracle

Adicionar hosts e instalar o plug-in SnapCenter para banco de dados Oracle

Você pode usar a página Adicionar Host para adicionar hosts e, em seguida, instalar o Pacote de Plug-ins SnapCenter para Linux ou o Pacote de Plug-ins 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 o Oracle RAC One Node, você deve instalar o plug-in nos 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 **Adicionar**.
4. Na página Hosts, execute as seguintes ações:
 - a. No campo 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 serem instalados.

6. (Opcional) Clique em **Mais opções** e especifique os detalhes.
7. Clique em **Enviar**.
8. Verifique a impressão digital e clique em **Confirmar e Enviar**.

Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós do cluster.

9. Monitore o progresso da instalação.

Crie políticas de backup para bancos de dados Oracle

Antes de usar o SnapCenter para fazer backup de recursos do banco de dados Oracle, você deve criar uma política de backup para o recurso ou grupo de recursos do qual deseja fazer backup.

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 backup como backup online ou offline.
 - c. Se você quiser catalogar o backup usando o Oracle Recovery Manager (RMAN), selecione **Catalogar backup com o Oracle Recovery Manager (RMAN)**.
 - d. Se você quiser remover logs de arquivo após o backup, selecione **Remover logs de arquivo após o backup**.
 - e. Especifique as configurações de log de arquivo de exclusão.
7. Na página Snapshot e backup, execute as seguintes etapas:
 - a. Selecione a frequência do backup agendado.
 - b. Especifique as configurações de retenção.
 - c. Se você quiser habilitar o backup do Azure NetApp Files , selecione **Habilitar backup** e especifique as configurações de retenção.
8. Na página Script, insira o caminho e os argumentos do prescript ou postscript que você deseja executar antes ou depois da operação de backup, respectivamente.
9. Na página Verificação, selecione o agendamento de backup para o qual você deseja executar a operação de verificação e insira o caminho e os argumentos do prescript ou postscript que você deseja executar antes ou depois da operação de verificação, respectivamente.
10. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e anexe políticas de backup do Oracle

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

Um grupo de recursos permite que você faça backup de todos os dados associados a um determinado aplicativo simultaneamente. 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 trabalho de proteção de dados que deseja executar.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** 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	Insira um nome para o grupo de recursos.
Etiquetas	Insira um ou mais rótulos que ajudarão você a pesquisar posteriormente o grupo de recursos.
Use formato de nome personalizado para cópia do Snapshot	Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.
Destino do arquivo de log de arquivamento	Especifique os destinos dos arquivos de log de arquivamento.

4. Na página Recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Tipo de recurso**.
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 agendamentos, clique em  * para a política que você deseja configurar.
 - c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento 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 seu cronograma de verificação e clique em  .
 - c. Selecione **Executar verificação após backup** 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 **Concluir**.

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

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

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, 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 **Usar formato de nome personalizado para cópia do Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.
4. Na página Políticas, execute as seguintes etapas:
 - a. Selecione uma ou mais políticas na lista suspensa.
 - b. Selecione *  * na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.
 - c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e selecione **OK**.
5. Na página Verificação, execute as seguintes etapas:
 - a. Selecione o servidor de verificação.
 - b. Selecione a política para a qual deseja configurar seu cronograma de verificação e clique em *  *.
 - c. Selecione **Executar verificação após backup** 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 **Concluir**.
8. Selecione **Fazer backup 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 você deseja usar para backup.
 - b. Clique em **Backup**.
10. Monitore o progresso da operação clicando em **Monitorar > 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 **Recursos** 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 você deseja usar para backup.
 - b. Selecione **Backup**.
5. Monitore 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 seu sistema de arquivos ativo e, em seguida, recuperar o banco de dados.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista Exibir.
3. Selecione o banco de dados ou o grupo de recursos na lista.
4. Na exibição Gerenciar cópias, selecione **Backups** do sistema de armazenamento primário.
5. Selecione o backup da tabela e clique em *  *.
6. Na página Escopo de restauração, execute as seguintes tarefas:
 - a. Selecione RAC se você selecionou um backup de um banco de dados no ambiente RAC.
 - b. Execute as seguintes ações:
 - i. Selecione **Todos os arquivos de dados** se quiser restaurar apenas os arquivos do banco de dados.
 - ii. Selecione **Tablespaces** se quiser restaurar apenas os tablespaces.
 - iii. Selecione **Refazer arquivos de log** se quiser restaurar os arquivos de log de refazer dos bancos de dados de espera do Data Guard ou do Active Data Guard.
 - iv. Selecione **Bancos de dados conectáveis** e especifique os PDBs que deseja restaurar.
 - v. Selecione **Tablespaces de banco de dados conectáveis (PDB)** e especifique o PDB e os tablespaces desse PDB que você deseja restaurar.
 - vi. Selecione **Restaurar o banco de dados para o mesmo host onde o backup foi criado** se quiser restaurar o banco de dados para o mesmo servidor SQL onde os backups foram feitos.
 - vii. Selecione **Restaurar o banco de dados em um host alternativo** se desejar que o banco de dados seja restaurado em um servidor SQL diferente no mesmo host ou em um host diferente onde os backups são feitos.
 - viii. Selecione **Alterar estado do banco de dados, se necessário, para restauração e recuperação** 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 desejar executar a restauração no local em cenários onde novos arquivos de dados são adicionados após o backup ou quando LUNs são adicionados, excluídos ou recriados em um grupo de discos LVM.

7. Na página Escopo de Recuperação, selecione uma das seguintes opções:
 - a. Selecione **Todos os registros** se quiser recuperar a última transação.
 - b. Selecione **Até SCN (Número de alteração do sistema)** 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 log de arquivamento externo** se desejar especificar o local dos arquivos de log de arquivamento externo.
8. Na página Pré-operatório e Pós-operatório, 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 **Concluir**.
11. Monitore o progresso da operação clicando em **Monitorar > Trabalhos**.

Restaurar e recuperar tablespaces usando recuperação de ponto no tempo

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

Passos

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

Se o backup não estiver catalogado, você deve selecioná-lo e clicar em **Catálogo**.

5. Selecione o backup catalogado e clique em  *.
6. Na página Escopo de restauração, execute as seguintes tarefas:
 - a. Selecione **RAC** se você selecionou um backup de um banco de dados no ambiente RAC.
 - b. Selecione **Tablespaces** se quiser restaurar apenas os tablespaces.
 - c. Selecione **Alterar estado do banco de dados, se necessário, para restauração e recuperação** para alterar o estado do banco de dados para o estado necessário para executar operações de restauração e recuperação.
7. Na página Escopo de Recuperação, selecione uma das seguintes opções:
 - a. Selecione **Até SCN (Número de alteração do sistema)** 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-operatório e Pós-operatório, 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 **Concluir**.
11. Monitore o processo de restauração usando a página **Monitor > Tarefas**.

Restaurar e recuperar banco de dados plugável usando recuperação de ponto no tempo

Você pode restaurar e recuperar um banco de dados conectável (PDB) que foi corrompido ou descartado sem afetar os outros PDBs no banco de dados do contêiner (CDB). O SnapCenter usa o RMAN para executar a recuperação de ponto no tempo (PITR) do PDB.

Passos

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

Se o backup não estiver catalogado, você deve selecioná-lo e clicar em **Catálogo**.

5. Selecione o backup catalogado e clique em  *.
6. Na página Escopo de restauração, execute as seguintes tarefas:
 - a. Selecione **RAC** se você selecionou um backup de um banco de dados no ambiente RAC.
 - b. Dependendo se você deseja restaurar o PDB ou os tablespaces em um PDB, execute uma das ações:
 - Selecione **Bancos de dados conectáveis (PDBs)** se quiser restaurar um PDB.
 - Selecione **Tablespaces de banco de dados conectáveis (PDB)** se desejar restaurar tablespaces em um PDB.
7. Na página Escopo de Recuperação, selecione uma das seguintes opções:
 - a. Selecione **Até SCN (Número de alteração do sistema)** 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-operatório e Pós-operatório, 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 **Concluir**.
11. Monitore o processo de restauração usando a página **Monitor > Tarefas**.

Clonar backup do 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 grossos e são criados no pool de capacidade pai.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista Exibir.
3. Selecione o banco de dados.
4. Na página de exibição Gerenciar cópias, selecione o backup do sistema de armazenamento primário.
5. Selecione o backup de dados e clique em  *.

6. Na página Nome, selecione se deseja clonar um banco de dados (CDB ou não CDB) ou clonar um banco de dados conectável (PDB).
7. Na página Locais, especifique os detalhes necessários.

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

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

8. Na página Credenciais, execute uma das seguintes ações:
 - a. Para Nome da credencial para o usuário sys, selecione a credencial a ser usada para definir a senha do usuário sys do banco de dados clone.
 - b. Para Nome da credencial da instância ASM, selecione **Nenhum** se a autenticação do sistema operacional estiver habilitada para conexão com a instância ASM no host clone.

Caso contrário, selecione a credencial do Oracle ASM configurada com o usuário “sys” ou um usuário com privilégio “sysasm” aplicável ao host clone.
9. Na página Pré-operações, especifique o caminho e os argumentos das prescrições e, na seção Configurações dos parâmetros do banco de dados, modifique os valores dos parâmetros do banco de dados pré-preenchidos que são usados para inicializar o banco de dados.
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 **Até Cancelar**, o SnapCenter executará a recuperação montando o backup de log mais recente com a sequência ininterrupta de logs de arquivamento após o backup de dados que foi selecionado para clonagem.
 - b. Se você selecionar **Data e hora**, o SnapCenter recuperará o banco de dados até uma data e hora especificadas.
 - c. Se você selecionar **Até SCN**, o SnapCenter recuperará o banco de dados até um SCN especificado.
 - d. Se você selecionar **Especificar locais de log de arquivamento externo**, o SnapCenter identificará e montará o número ideal de backups de log com base no SCN especificado ou na data e hora selecionadas.
 - e. Por padrão, a caixa de seleção **Criar novo DBID** é selecionada para gerar um número exclusivo (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 no catálogo RMAN externo onde o banco de dados de origem já está registrado, a operação falhará.

 - f. Marque a caixa de seleção **Criar arquivo temporário para espaço de tabela temporário** se desejar criar um arquivo temporário para o espaço de tabela temporário padrão do banco de dados clonado.
 - g. Em **Inserir entradas SQL a serem aplicadas quando o clone for criado**, adicione as entradas SQL que você deseja aplicar quando o clone for criado.
 - h. Em **Inserir scripts a serem executados após a operação de clonagem**, especifique o caminho e os argumentos do postscript que você deseja executar após a operação de clonagem.
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 **Concluir**.

13. Monitore o progresso da operação selecionando **Monitor > Trabalhos**.

Clonar um banco de dados plugável

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

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** 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 do sistema de armazenamento primário.
5. Selecione o backup e clique em  *.
6. Na página Nome, selecione **PDB Clone** e especifique os outros detalhes.
7. Na página Locais, especifique os detalhes necessários.
8. Na página Pré-operações, especifique o caminho e os argumentos das prescrições e, na seção Configurações dos parâmetros do banco de dados, modifique os valores dos parâmetros do banco de dados pré-preenchidos que são usados para inicializar o banco de dados.
9. Na página Pós-Operações, **Até Cancelar** é selecionado por padrão para executar a recuperação do banco de dados clonado.
 - a. Se você selecionar **Até Cancelar**, o SnapCenter executará a recuperação montando o backup de log mais recente com a sequência ininterrupta de logs de arquivamento após o backup de dados que foi selecionado para clonagem.
 - b. Se você selecionar **Data e hora**, o SnapCenter recuperará o banco de dados até uma data e hora especificadas.
 - c. Se você selecionar **Especificar locais de log de arquivamento externo**, o SnapCenter identificará e montará o número ideal de backups de log com base no SCN especificado ou na data e hora selecionadas.
 - d. Por padrão, a caixa de seleção **Criar novo DBID** é selecionada para gerar um número exclusivo (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 no catálogo RMAN externo onde o banco de dados de origem já está registrado, a operação falhará.
- e. Marque a caixa de seleção **Criar arquivo temporário para espaço de tabela temporário** se desejar criar um arquivo temporário para o espaço de tabela temporário padrão do banco de dados clonado.
- f. Em **Inserir entradas SQL a serem aplicadas quando o clone for criado**, adicione as entradas SQL que você deseja aplicar quando o clone for criado.
- g. Em **Inserir scripts a serem executados após a operação de clonagem**, especifique o caminho e os argumentos do postscript que você deseja executar após a operação de clonagem.
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 **Concluir**.

12. Monitore o progresso da operação selecionando **Monitor > Trabalhos**.

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

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

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

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.