Proteja o PostgreSQL

SnapCenter Software 6.0

NetApp
December 19, 2024

Índice

Proteja o PostgreSQL

Plug-in SnapCenter para PostgreSQL

Visão geral do plug-in do SnapCenter para PostgreSQL

O cluster do SnapCenter Plug-in para PostgreSQL é um componente do lado do host do software NetApp SnapCenter que permite o gerenciamento de clusters do PostgreSQL com reconhecimento de aplicativos. O cluster Plug-in para PostgreSQL automatiza o backup, a restauração e a clonagem de clusters PostgreSQL em seu ambiente SnapCenter.

O SnapCenter suporta configurações de cluster único e multi cluster PostgreSQL. Você pode usar o Plug-in para clusters PostgreSQL em ambientes Linux e Windows. Em ambientes Windows, o PostgreSQL será suportado como recurso manual.

Quando o cluster Plug-in para PostgreSQL é instalado, você pode usar o SnapCenter com a tecnologia NetApp SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume. Você também pode usar o plug-in com a tecnologia NetApp SnapVault para executar a replicação de backup disco a disco para conformidade com os padrões.

O plug-in do SnapCenter para PostgreSQL é compatível com NFS e SAN em layouts de storage de arquivos do ONTAP e do Azure NetApp.

O VMDK ou o layout de armazenamento virtual são suportados.

O que você pode fazer usando o plug-in SnapCenter para PostgreSQL

Ao instalar o cluster Plug-in para PostgreSQL em seu ambiente, você pode usar o SnapCenter para fazer backup, restaurar e clonar clusters PostgreSQL e seus recursos. Você também pode executar tarefas de suporte a essas operações.

- Adicionar clusters.
- Criar backups.
- Restauração a partir de backups.
- Backups de clones.
- Agendar operações de backup.
- Monitore operações de backup, restauração e clone.
- Exibir relatórios para operações de backup, restauração e clone.

Plug-in do SnapCenter para recursos PostgreSQL

O SnapCenter se integra à aplicação plug-in e às tecnologias NetApp no sistema de storage. Para trabalhar com o Plug-in para cluster PostgreSQL, use a interface gráfica do usuário do SnapCenter.

- * Interface gráfica unificada do usuário*

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

- * Administração central automatizada*

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

- **Tecnologia de cópia Snapshot NetApp sem interrupções**

  O SnapCenter usa a tecnologia de snapshot do NetApp com o cluster Plug-in para PostgreSQL para fazer backup de recursos.

Usar o Plug-in para PostgreSQL também oferece os seguintes benefícios:

- Suporte a fluxos de trabalho de backup, restauração e clone
- Delegação de funções centralizada e segurança compatível com RBAC

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

- Criação de cópias de recursos com uso eficiente de espaço e pontuais para teste ou extração de dados usando a tecnologia NetApp FlexClone

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

- Suporte para o recurso instantâneo do grupo de consistência (CG) do ONTAP como parte da criação de backups.
- Funcionalidade de executar vários backups simultaneamente em vários hosts de recursos

  Em uma única operação, os snapshots são consolidados quando os recursos em um único host compartilham o mesmo volume.

- Capacidade de criar instantâneos usando comandos externos.
- Suporte para Linux LVM no sistema de arquivos XFS.

Tipos de armazenamento suportados pelo plug-in SnapCenter para PostgreSQL

O SnapCenter oferece suporte a uma ampla variedade de tipos de armazenamento em máquinas físicas e máquinas virtuais (VMs). Você deve verificar o suporte para o seu tipo de armazenamento antes de instalar o plug-in SnapCenter para PostgreSQL.

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

Máquina	Tipo de armazenamento
VMware ESXi	• LUNs RDM conetados por um FC ou iSCSI ESXi HAScanning de adaptadores de barramento de host (HBAs) pode levar muito tempo para ser concluído porque o SnapCenter verifica todos os adaptadores de barramento de host presentes no host. Você pode editar o arquivo **LinuxConfig.pm** localizado em */opt/NetApp/SnapCenter/spl/plugins/scu/scucore/modules/SCU/Config* para definir o valor do parâmetro **SCSI_HOSTS_OPTIMIZED_RESCAN** para 1 para reexaminar somente os HBA listados em HBA_DRIVER_NAMES. • ISCSI LUNs ligados diretamente ao sistema convidado pelo iniciador iSCSI • VMDKs em armazenamentos de dados NFS • VMDKs no VMFS • Volumes NFS conectados diretamente ao sistema convidado • Armazenamentos de dados da VVol em NFS e SAN O armazenamento de dados da VVol só pode ser provisionado com as Ferramentas do ONTAP para o VMware vSphere.

Mínimo de ONTAP Privileges necessário para o plug-in PostgreSQL

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

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

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

    - volume online
    - modificação do volume
    - criar qtree de volume
    - eliminação de qtree de volume
    - modificação de qtree de volume
    - apresentação de qtree de volume
    - restrição de volume
    - apresentação do volume
    - criar instantâneo de volume
    - eliminar instantâneo do volume
    - modificação do instantâneo do volume
    - tempo de expiração do volume snapshot modify-SnapLock
    - mudar o nome do instantâneo do volume
    - restauração de snapshot de volume
    - restauração de arquivo de snapshot de volume
    - apresentação de instantâneo do volume
    - desmontar o volume
    - svm cifs
    - compartilhamento cifs de svm criar
    - exclusão de compartilhamento cifs de svm
    - apresentação do shadowcopy cifs de svm
    - exibição de compartilhamento cifs de svm
    - mostra cifs de svm
    - política de exportação de svm
    - criação de política de exportação de svm
    - exclusão da política de exportação do svm
    - regra de política de exportação de svm criar
    - a regra de política de exportação do svm é exibida
    - exibição da política de exportação do svm
    - svm iscsi
    - apresentação da ligação iscsi de svm
    - mostra o svm
- Comandos somente leitura: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior
    - interface de rede
    - mostra da interface de rede
    - svm

Prepare sistemas de storage para replicação SnapMirror e SnapVault para PostgreSQL

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

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

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

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

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

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

Estratégia de backup para PostgreSQL

Defina uma estratégia de backup para PostgreSQL

Definir uma estratégia de backup antes de criar seus trabalhos de backup ajuda a ter os backups necessários para restaurar ou clonar seus recursos com êxito. Seu contrato de nível de serviço (SLA), objetivo de tempo de recuperação (rto) e objetivo do ponto de restauração (RPO) determinam em grande parte a sua estratégia de backup.

Sobre esta tarefa

Um SLA define o nível de serviço esperado e aborda muitos problemas relacionados ao serviço, incluindo a disponibilidade e o desempenho do serviço. Rto é o momento em que um processo de negócios deve ser restaurado após uma interrupção no serviço. O RPO define a estratégia para a era dos arquivos que precisam ser recuperados do armazenamento de backup para que as operações regulares sejam retomadas após uma falha. SLA, rto e RPO contribuem para a estratégia de proteção de dados.

Passos

1. Determine quando você deve fazer backup de seus recursos.
2. Decida quantos trabalhos de cópia de segurança necessita.
3. Decida como nomear seus backups.
4. Decida se deseja criar uma política baseada em cópia Snapshot para fazer backup de snapshots

consistentes com aplicações do cluster.

5. Decida se você deseja usar a tecnologia NetApp SnapMirror para replicação ou a tecnologia NetApp SnapVault para retenção a longo prazo.
6. Determine o período de retenção dos snapshots no sistema de storage de origem e no destino do SnapMirror.
7. Determine se deseja executar quaisquer comandos antes ou depois da operação de backup e forneça um prescritor ou postscript.

Descoberta automática de recursos no host Linux

Os recursos são clusters e instâncias do PostgreSQL no host Linux que são gerenciados pelo SnapCenter. Depois de instalar o plug-in do SnapCenter para PostgreSQL, os clusters do PostgreSQL de todas as instâncias desse host são automaticamente descobertos e exibidos na página recursos.

Tipos de backups suportados

Tipo de backup especifica o tipo de backup que você deseja criar. O SnapCenter é compatível com o tipo de backup baseado em cópia de snapshot para clusters PostgreSQL.

Backup baseado em cópia snapshot

Os backups baseados em cópias snapshot utilizam a tecnologia NetApp snapshot para criar cópias on-line e somente leitura dos volumes nos quais os clusters PostgreSQL residem.

Como o plug-in do SnapCenter para PostgreSQL usa snapshots de grupo de consistência

Você pode usar o plug-in para criar snapshots de grupo de consistência para grupos de recursos. Um grupo de consistência é um contentor que pode abrigar vários volumes para que você possa gerenciá-los como uma entidade. Um grupo de consistência são snapshots simultâneos de vários volumes, fornecendo cópias consistentes de um grupo de volumes.

Você também pode especificar o tempo de espera para que o controlador de armazenamento agrupe snapshots de forma consistente. As opções de tempo de espera disponíveis são **urgente**, **Médio** e **descontraído**. Você também pode ativar ou desativar a sincronização WAFL (Write Anywhere File Layout) durante uma operação consistente de snapshot em grupo. O WAFL Sync melhora o desempenho de um snapshot de grupo de consistência.

Como o SnapCenter gerencia o gerenciamento de backups de dados

O SnapCenter gerencia o gerenciamento de backups de dados nos níveis do sistema de storage e do sistema de arquivos.

Os instantâneos no armazenamento primário ou secundário e suas entradas correspondentes no catálogo PostgreSQL são excluídos com base nas configurações de retenção.

Considerações para determinar agendas de backup para PostgreSQL

O fator mais crítico na determinação de um agendamento de backup é a taxa de alteração do recurso. Você pode fazer backup de um recurso muito usado a cada hora, enquanto você pode fazer backup de um recurso raramente usado uma vez por dia. Outros fatores incluem a importância do recurso para a sua organização, seu contrato de nível de serviço (SLA) e seu objetivo do ponto de restauração (RPO).

Os programas de backup têm duas partes, como segue:

- Frequência de backup (com que frequência os backups devem ser executados)

  A frequência de backup, também chamada de tipo de programação para alguns plug-ins, faz parte de uma configuração de política. Por exemplo, você pode configurar a frequência de backup como hora, dia, semanal ou mensal.

- Programações de backup (exatamente quando os backups devem ser executados)

  As agendas de backup fazem parte de uma configuração de recurso ou grupo de recursos. Por exemplo, se você tiver um grupo de recursos que tenha uma política configurada para backups semanais, poderá configurar a programação para fazer backup todas as quintas-feiras às 10:00 horas

Número de trabalhos de backup necessários para PostgreSQL

Os fatores que determinam o número de tarefas de backup de que você precisa incluem o tamanho do recurso, o número de volumes usados, a taxa de alteração do recurso e seu Contrato de nível de Serviço (SLA).

Convenções de nomenclatura de backup para clusters Plug-in para PostgreSQL

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

O Snapshot usa a seguinte convenção de nomenclatura padrão:

```
resourcegroupname_hostname_timestamp
```

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

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

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

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

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

Estratégia de restauração e recuperação para PostgreSQL

Defina uma estratégia de restauração e recuperação para os recursos PostgreSQL

Você deve definir uma estratégia antes de restaurar e recuperar o cluster para que possa executar operações de restauração e recuperação com sucesso.

Somente a recuperação manual do cluster é suportada.

Passos

1. Determine as estratégias de restauração suportadas para recursos PostgreSQL adicionados manualmente
2. Determine as estratégias de restauração suportadas para clusters PostgreSQL descobertos automaticamente
3. Decida o tipo de operações de recuperação que você deseja executar.

Tipos de estratégias de restauração suportadas para recursos PostgreSQL adicionados manualmente

Você deve definir uma estratégia antes de executar operações de restauração com êxito usando o SnapCenter.

Você não pode recuperar recursos PostgreSQL adicionados manualmente.

Restauração completa de recursos

- Restaura todos os volumes, qtrees e LUNs de um recurso

Se o recurso contiver volumes ou qtrees, os instantâneos obtidos após o snapshot selecionado para restauração em tais volumes ou qtrees serão excluídos e não poderão ser recuperados. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído.

OBSERVAÇÃO: O plug-in para PostgreSQL cria uma pasta backup_label e tablespace_map na pasta */<OS_temp_folder>/postgresql_SC_recovery*<Restore_JobId>/_ para ajudar a recuperar manualmente .

Tipo de estratégia de restauração suportada para PostgreSQL descoberto automaticamente

Você deve definir uma estratégia antes de executar operações de restauração com êxito usando o SnapCenter.

A restauração completa de recursos é a estratégia de restauração suportada para clusters PostgreSQL descobertos automaticamente. Isso restaura todos os volumes, qtrees e LUNs de um recurso.

Tipos de operações de restauração para PostgreSQL descoberto automaticamente

O plug-in do SnapCenter para PostgreSQL é compatível com SnapRestore de arquivo

único e tipos de restauração de conexão e cópia para clusters PostgreSQL descobertos automaticamente.

O SnapRestore de arquivo único é executado em ambientes NFS para os seguintes cenários:

- Se apenas a opção **Complete Resource** estiver selecionada
- Quando o backup selecionado é de um local secundário SnapMirror ou SnapVault e a opção **recurso completo** está selecionada

O SnapRestore de Arquivo único é executado em ambientes SAN para os seguintes cenários:

- Se apenas a opção **Complete Resource** estiver selecionada
- Quando o backup é selecionado em um local secundário do SnapMirror ou do SnapVault e a opção **recurso completo** está selecionada

Tipos de operações de recuperação compatíveis com clusters PostgreSQL

O SnapCenter permite que você execute diferentes tipos de operações de recuperação para clusters PostgreSQL.

- Recupere o cluster até o estado mais recente
- Recupere o cluster até um ponto específico no tempo

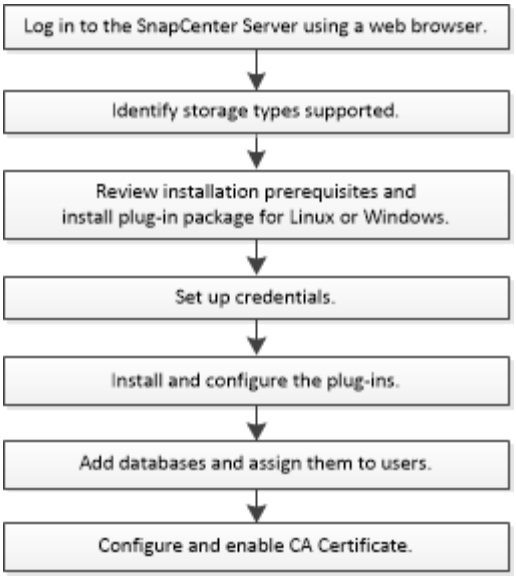
  Você deve especificar a data e a hora para a recuperação.

O SnapCenter também fornece a opção sem recuperação para clusters PostgreSQL.

Prepare-se para instalar o plug-in SnapCenter para PostgreSQL

Fluxo de trabalho de instalação do plug-in SnapCenter para PostgreSQL

Você deve instalar e configurar o plug-in do SnapCenter para PostgreSQL se quiser proteger clusters do PostgreSQL.



Pré-requisitos para adicionar hosts e instalar o plug-in SnapCenter para PostgreSQL

Antes de adicionar um host e instalar os pacotes de plug-in, você deve completar todos os requisitos. O plug-in SnapCenter para PostgreSQL está disponível em ambientes Windows e Linux.

- Você deve ter instalado o Java 11 em seu host.

  O IBM Java não é suportado.

- Para Windows, o Plug-in Creator Service deve ser executado usando o usuário do Windows "'LocalSystem'", que é o comportamento padrão quando o Plug-in para PostgreSQL é instalado como administrador de domínio.
- 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. O plug-in SnapCenter para Microsoft Windows será implantado por padrão com o plug-in PostgreSQL em hosts Windows.
- O servidor SnapCenter deve ter acesso ao 8145 ou à porta personalizada do plug-in para o host PostgreSQL.

Hosts do Windows

- Você deve ter um usuário de domínio com Privileges de administrador local com permissões de login local no host remoto.
- Ao instalar o plug-in para PostgreSQL em um host Windows, o plug-in SnapCenter para Microsoft Windows é instalado automaticamente.
- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.
- Você deve ter instalado o Java 11 em seu host Windows.

  "Downloads Java para todos os sistemas operacionais"

  "Ferramenta de Matriz de interoperabilidade do NetApp"

Hosts Linux

- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.
- Você deve ter instalado o Java 11 em seu host Linux.

  "Downloads Java para todos os sistemas operacionais"

  "Ferramenta de Matriz de interoperabilidade do NetApp"

- Para clusters PostgreSQL que estão sendo executados em um host Linux, ao instalar o plug-in para PostgreSQL, o plug-in SnapCenter para UNIX é instalado automaticamente.
- Você deve ter **bash** como o shell padrão para instalação do plug-in.

Comandos suplementares

Para executar um comando complementar no plug-in do SnapCenter para PostgreSQL, você deve incluí-lo no arquivo *allowed_commands.config*.

- Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
- Localização padrão no host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_Commands.config*

Para permitir comandos suplementares no host do plug-in, abra o arquivo *allowed_Commands.config* em um editor. Digite cada comando em uma linha separada e os comandos não são sensíveis a maiúsculas e minúsculas. Certifique-se de especificar o nome de caminho totalmente qualificado e incluir o nome de caminho entre aspas (") se ele contiver espaços.

Por exemplo:

Comando: Comando de montagem: Comando umount: Comando "C: Arquivos de programas/NetApp comandos do SnapCreator" comando: myscript.bat

Se o arquivo *allowed_commands.config* não estiver presente, os comandos ou a execução de script serão bloqueados e o fluxo de trabalho falhará com o seguinte erro:

"[/mnt/mount -a] execução não permitida. Autorize adicionando o comando no arquivo %s no host do plugin."

Se o comando ou script não estiver presente no *allowed_Commands.config*, a execução do comando ou script será bloqueada e o fluxo de trabalho falhará com o seguinte erro:

"[/mnt/mount -a] execução não permitida. Autorize adicionando o comando no arquivo %s no host do plugin."

Você não deve usar uma entrada curinga (*) para permitir todos os comandos.

Configure sudo Privileges para usuários não-root para host Linux

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

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Se o umask for 0027, certifique-se de que a pasta java e todos os arquivos dentro devem ter permissão de 555. Caso contrário, a instalação do plug-in pode falhar.
- Para o usuário não-root, certifique-se de que o nome do usuário não-root e do grupo do usuário devem ser os mesmos.
- Edite o arquivo */etc/ssh/sshd_config* para configurar os algoritmos de código de autenticação de mensagem: Macs hmac-SHA2-256 e MACs hmac-SHA2-512.

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

  Exemplo:

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

Sobre esta tarefa

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

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

Passos

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

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

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

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

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

Você pode obter o *checksum_value* do arquivo **SC_unix_plugins_checksum.txt**, que está localizado em:

- _C: /ProgramData/NetApp/SnapCenter/Repositório de pacotes/sc_unix_plugins_checksum.txt _ se o servidor SnapCenter estiver instalado no host do Windows.
- _/opt/NetApp/SnapCenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ se o servidor SnapCenter estiver instalado no host Linux.

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

Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Windows

Antes de instalar o pacote de plug-ins do SnapCenter para Windows, você deve estar familiarizado com alguns requisitos básicos de espaço do sistema host e requisitos de dimensionamento.

Item	Requisitos
Sistemas operacionais	Microsoft Windows Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	5 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	• DOTNET Core começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes • PowerShell Core 7.4.2 Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp". Para obter informações específicas de solução de problemas .NET, consulte "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conetividade com a Internet."

Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Linux

Antes de instalar o pacote de plug-ins do SnapCenter para Linux, você deve estar familiarizado com alguns requisitos básicos de espaço e dimensionamento do sistema host.

Item	Requisitos
Sistemas operacionais	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	2 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	Java 11 Oracle Java e OpenJDK Se você atualizou O JAVA para a versão mais recente, você deve garantir que a opção JAVA_HOME localizada em /var/opt/SnapCenter/spl/etc/spl.properties esteja definida para a versão JAVA correta e o caminho correto. Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Configure credenciais para o plug-in SnapCenter para PostgreSQL

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 em clusters ou sistemas de arquivos do Windows.

Sobre esta tarefa

- Hosts Linux

  Você deve configurar credenciais para instalar plug-ins em hosts Linux.

Você deve configurar as credenciais para o usuário raiz ou para um usuário não-root que tenha sudo Privileges para instalar e iniciar o processo de plug-in.

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

- Hosts do Windows

  Você deve configurar as credenciais do Windows antes de instalar os plug-ins.

  Você deve configurar as credenciais com o Privileges de administrador, incluindo direitos de administrador no host remoto.

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

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 informações necessárias para configurar credenciais:

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

Para este campo…	Faça isso…
Nome de utilizador	Introduza o nome de utilizador e a palavra-passe a utilizar para a autenticação. • Administrador de domínio ou qualquer membro do grupo de administradores Especifique o administrador do domínio ou qualquer membro do grupo de administradores no sistema no qual você está instalando o plug-in do SnapCenter. Formatos válidos para o campo Nome de usuário são: ◦ *NetBIOS_username* ◦ *Domain FQDN_username* • Administrador local (apenas para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local incorporado no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host. O formato válido para o campo Nome de usuário é: *Nome de usuário* Não use aspas duplas (") ou backtick (') nas senhas. Você não deve usar os símbolos menos de (>) e exclamação (!) juntos em senhas. Por exemplo, lessthan!10, lessthan10You!, backtick'12.
Palavra-passe	Introduza a palavra-passe utilizada para autenticação.
Modo de autenticação	Selecione o modo de autenticação que pretende utilizar.
Use sudo Privileges	Marque a caixa de seleção **Use sudo Privileges** se estiver criando credenciais para um usuário que não seja root. Aplicável apenas a usuários Linux.

5. Clique em **OK**.

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

Configure o gMSA no Windows Server 2016 ou posterior

O Windows Server 2016 ou posterior permite criar uma conta de serviço gerenciado de grupo (gMSA) que fornece gerenciamento automatizado de senha de conta de serviço a partir de uma conta de domínio gerenciado.

Antes de começar

- Você deve ter um controlador de domínio do Windows Server 2016 ou posterior.
- Você deve ter um host Windows Server 2016 ou posterior, que é um membro do domínio.

Passos

1. Crie uma chave raiz KDS para gerar senhas exclusivas para cada objeto em seu gMSA.
2. Para cada domínio, execute o seguinte comando do controlador de domínio do Windows: Add-KDSRootKey -EffectiveImmediately
3. Crie e configure seu gMSA:
   a. Crie uma conta de grupo de usuários no seguinte formato:

```
 domainName\accountName$
.. Adicione objetos de computador ao grupo.
.. Use o grupo de usuários que você acabou de criar para criar o
gMSA.
```

   Por exemplo,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Execute `Get-ADServiceAccount` o comando para verificar a conta de
serviço.
```

4. Configure o gMSA em seus hosts:
   a. Ative o módulo do ative Directory para Windows PowerShell no host onde você deseja usar a conta gMSA.

   Para fazer isso, execute o seguinte comando do PowerShell:

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                            Name                Install State
------------                            ----                -------------
[ ] Active Directory Domain Services    AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. Reinicie o host.

b. Instale o gMSA em seu host executando o seguinte comando a partir do prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`

5. Atribua o Privileges administrativo ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no servidor SnapCenter.

   O servidor SnapCenter instalará os plug-ins selecionados no host e o gMSA especificado será usado como a conta de logon de serviço durante a instalação do plug-in.

Instale o plug-in SnapCenter para PostgreSQL

Adicione hosts e instale pacotes plug-in em hosts remotos

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. Você pode adicionar o host e instalar pacotes de plug-in para um host individual.

Antes de começar

- Se o sistema operacional do host do servidor SnapCenter for o Windows 2019 e o sistema operacional do host do plug-in for o Windows 2022, você deve executar o seguinte:
  - Atualize para o Windows Server 2019 (versão de SO 17763,5936) ou posterior
  - Atualize para o Windows Server 2022 (versão de SO 20348,2402) ou posterior
- 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.

- Você deve garantir que o serviço de enfileiramento de mensagens esteja em execução.
- A documentação de administração contém informações sobre o gerenciamento de hosts.
- Se você estiver usando a conta de serviço gerenciado de grupo (gMSA), você deve configurar o gMSA com Privileges administrativo.

  "Configurar conta de serviço gerenciado de grupo no Windows Server 2016 ou posterior para PostgreSQL"

Sobre esta tarefa

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

Passos

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

Para este campo…	Faça isso…
Tipo de host	Selecione o tipo de host: • Windows • Linux O Plug-in para PostgreSQL é instalado no host cliente PostgreSQL, e este host pode estar em um sistema Windows ou em um sistema Linux.
Nome do host	Insira o nome do host de comunicação. Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração adequada do DNS. Portanto, a melhor prática é entrar no FQDN.

Para este campo…	Faça isso…
Credenciais	Selecione o nome da credencial que você criou ou crie novas credenciais. A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte as informações sobre como criar credenciais. Você pode exibir detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você forneceu. O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar host.

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

   Ao usar a API REST para instalar o Plug-in para PostgreSQL, você deve passar a versão como 3,0. Por exemplo, PostgreSQL:3,0

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

Para este campo…	Faça isso…
Porta	Guarde o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o servidor SnapCenter tiver sido instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão. Se você instalou manualmente os plug-ins e especificou uma porta personalizada, você deve especificar a mesma porta. Caso contrário, a operação falha.
Caminho de instalação	O Plug-in para PostgreSQL é instalado no host cliente PostgreSQL, e este host pode estar em um sistema Windows ou em um sistema Linux. • Para o pacote de plug-ins do SnapCenter para Windows, o caminho padrão é C: Arquivos de programas/NetApp/SnapCenter. Opcionalmente, você pode personalizar o caminho. • Para o pacote de plug-ins do SnapCenter para Linux, o caminho padrão é /opt/NetApp/SnapCenter. Opcionalmente, você pode personalizar o caminho.

Para este campo…	Faça isso…
Ignorar as verificações de pré-instalação	Marque essa caixa de seleção se você já instalou os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.
Adicione todos os hosts no cluster	Marque esta caixa de seleção para adicionar todos os nós de cluster.
Use a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in	Para o host Windows, marque essa caixa de seleção se desejar usar a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in. Forneça o nome do gMSA no seguinte formato: O gMSA será usado como uma conta de serviço de logon apenas para o serviço SnapCenter Plug-in para Windows.

7. Clique em **Enviar**.

   Se você não tiver selecionado a caixa de seleção Ignorar pré-verificações, o host será validado para verificar se o host atende aos requisitos para a instalação do plug-in. O espaço em disco, a RAM, a versão do PowerShell, a versão do .NET, a localização (para plug-ins do Windows) e a versão Java (para plug-ins do Linux) são validados de acordo com os requisitos mínimos. Se os requisitos mínimos não forem cumpridos, são apresentadas mensagens de erro ou de aviso adequadas.

   Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado no NetApp SnapCenter para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deve corrigir o problema.

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

8. 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.

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

9. Monitorize o progresso da instalação.
   - Para o plug-in do Windows, os logs de instalação e atualização estão localizados em: *C: Plug-in do Windows SnapCenter*<JOBID>_
   - Para o plug-in Linux, os logs de instalação estão localizados em: */var/opt/SnapCenter/logs/SnapCenter_Linux_Host_Plug-in_Install*<JOBID>.log_ e os logs de atualização estão localizados em: */var/opt/SnapCenter/logs/SnapCenter_Linux_Host_Plug-*

in_Upgrade<JOBID>.log_

Instale pacotes de plug-ins do SnapCenter para Linux ou Windows em vários hosts remotos usando cmdlets

Você pode instalar os Pacotes de plug-in do SnapCenter para Linux ou Windows em vários hosts simultaneamente usando o cmdlet Install-SmHostPackage PowerShell.

Antes de começar

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

Passos

1. Inicie o PowerShell.
2. No host do servidor SnapCenter, estabeleça uma sessão usando o cmdlet Open-SmConnection e insira suas credenciais.
3. Instale o plug-in em vários hosts usando o cmdlet Install-SmHostPackage e os parâmetros necessários.

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

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

4. Insira suas credenciais para instalação remota.

Instale o plug-in SnapCenter para PostgreSQL em hosts Linux usando a interface de linha de comando

Você deve instalar o SnapCenter Plug-in para cluster PostgreSQL usando a interface de usuário (UI) do SnapCenter. Se o seu ambiente não permitir a instalação remota do plug-in a partir da IU do SnapCenter, você pode instalar o plug-in para cluster PostgreSQL no modo console ou no modo silencioso usando a interface de linha de comando (CLI).

Antes de começar

- Você deve instalar o cluster Plug-in para PostgreSQL em cada um dos hosts Linux onde o cliente PostgreSQL reside.
- O host Linux no qual você está instalando o SnapCenter Plug-in para PostgreSQL deve atender aos requisitos de software, cluster e sistema operacional dependentes.

  A ferramenta de Matriz de interoperabilidade (IMT) contém as informações mais recentes sobre as configurações suportadas.

  "Ferramenta de Matriz de interoperabilidade do NetApp"

- O cluster do SnapCenter Plug-in para PostgreSQL faz parte do pacote de plug-ins do SnapCenter para Linux. Antes de instalar o pacote de plug-ins do SnapCenter para Linux, você já deve ter instalado o SnapCenter em um host do Windows.

Passos

1. Copie o pacote de plug-ins do SnapCenter SnapCenter para o arquivo de instalação do Linux

(SnapCenter_linux_host_plugin.bin) do NetApp para o host onde você deseja instalar o plug-in para o PostgreSQL.

Você pode acessar esse caminho a partir do host onde o servidor SnapCenter está instalado.

2. No prompt de comando, navegue até o diretório onde você copiou o arquivo de instalação.
3. Instale o plug-in: `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`

   - -DPORT especifica a porta de comunicação HTTPS SMCore.
   - -DSERVER_IP especifica o endereço IP do servidor SnapCenter.
   - -DSERVER_HTTPS_PORT especifica a porta HTTPS do servidor SnapCenter.
   - -DUSER_install_DIR especifica o diretório onde você deseja instalar o pacote de plug-ins do SnapCenter para Linux.
   - DINSTALL_LOG_NAME especifica o nome do arquivo de log.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Edite o arquivo /<installation directory>/NetApp/SnapCenter/scc/etc/SC_SMS_Services.properties e, em seguida, adicione o parâmetro PLUGINS_ENABLED: PostgreSQL:3,0.
5. Adicione o host ao servidor SnapCenter usando o cmdlet Add-Smhost e os parâmetros necessários.

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

Monitore o status da instalação do Plug-in para PostgreSQL

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

Sobre esta tarefa

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

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

Passos

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

Configurar certificado CA

Gerar arquivo CSR do certificado CA

Você pode gerar uma solicitação de assinatura de certificado (CSR) e importar o certificado que pode ser obtido de uma autoridade de certificação (CA) usando a CSR gerada. O certificado terá uma chave privada associada a ele.

CSR é um bloco de texto codificado que é dado a um fornecedor de certificado autorizado para obter o certificado CA assinado.

O comprimento da chave RSA do certificado CA deve ser mínimo de 3072 bits.

Para obter informações sobre como gerar um CSR, "Como gerar o arquivo CSR do certificado CA" consulte .

Se você possui o certificado de CA para o seu domínio (*.domain.company.com) ou para o seu sistema (machine1.domain.company.com), pode ignorar a geração do arquivo CSR de certificado de CA. Você pode implantar o certificado de CA existente com o SnapCenter.

Para configurações de cluster, o nome do cluster (FQDN de cluster virtual) e os respetivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome alternativo (SAN) do assunto antes de adquirir o certificado. Para um certificado Wild card (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados CA

Você deve importar os certificados de CA para o servidor SnapCenter e os plug-ins de host do Windows usando o MMC (console de gerenciamento da Microsoft).

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.

4. Clique em **raiz da consola** > **certificados – computador local** > **autoridades de Certificação raiz fidedignas** > **certificados**.
5. Clique com o botão direito do rato na pasta "autoridades de Certificação de raiz fidedigna" e selecione **todas as tarefas** > **Importar** para iniciar o assistente de importação.
6. Conclua o assistente da seguinte forma:

Nesta janela do assistente…	Faça o seguinte…
Importar chave privada	Selecione a opção **Yes**, importe a chave privada e clique em **Next**.
Importar formato de ficheiro	Não faça alterações; clique em **seguinte**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluir o Assistente de importação de certificados	Revise o resumo e clique em **Finish** para iniciar a importação.

> O certificado de importação deve ser empacotado com a chave privada (os formatos suportados são: *.pfx, *.p12 e *.p7b).

7. Repita o passo 5 para a pasta "Pessoal".

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma cadeia hexadecimal que identifica um certificado. Uma impressão digital é calculada a partir do conteúdo do certificado usando um algoritmo de impressão digital.

Passos

1. Execute o seguinte na GUI:
   a. Clique duas vezes no certificado.
   b. Na caixa de diálogo certificado, clique na guia **Detalhes**.
   c. Percorra a lista de campos e clique em **thumbprint**.
   d. Copie os carateres hexadecimais da caixa.
   e. Remova os espaços entre os números hexadecimais.

      Por exemplo, se a impressão digital for: "A9 09 50 2D D8 2a E4 14 33 E6 F8 38 86 B0 0d 42 77 A3 2a 7b", depois de remover os espaços, será: "A909502d82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:
   a. Execute o seguinte comando para listar a impressão digital do certificado instalado e identificar o certificado instalado recentemente pelo nome do assunto.

      Get-ChildItem -Path Cert: LocalMachine/My

b. Copie a impressão digital.

Configure o certificado CA com os serviços de plug-in do host do Windows

Você deve configurar o certificado CA com os serviços de plug-in host do Windows para ativar o certificado digital instalado.

Execute as etapas a seguir no servidor SnapCenter e em todos os hosts de plug-in em que os certificados de CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão SMCore 8145, executando o seguinte comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Por exemplo:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Vincule o certificado recém-instalado aos serviços de plug-in do host
   do Windows executando os seguintes comandos:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Por exemplo:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

Configure o certificado CA para o serviço de plug-ins SnapCenter PostgreSQL no host Linux

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

Plug-ins personalizados usam o arquivo 'keystore.jks', que está localizado em */opt/NetApp/SnapCenter/scc/etc* tanto como seu armazenamento de confiança e armazenamento de chaves.

Gerenciar senha para armazenamento de chaves plug-in personalizado e alias do par de chaves assinadas CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore do plug-in personalizado do arquivo de propriedade do agente do plug-in personalizado.

   É o valor correspondente à chave 'KEYSTORE_PASS'.

2. Altere a senha do keystore:

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

   ```
   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
   ```

   Atualize o mesmo para a chave KEYSTORE_PASS no arquivo *agent.properties*.

3. Reinicie o serviço depois de alterar a senha.

> A palavra-passe para o armazenamento de chaves plug-in personalizado e para todas as palavras-passe de alias associadas da chave privada deve ser a mesma.

Configure certificados raiz ou intermediários para armazenamento de confiança de plug-in personalizado

Você deve configurar os certificados raiz ou intermediários sem a chave privada para armazenamento de confiança de plug-in personalizado.

Passos

1. Navegue até a pasta que contém o keystore de plug-in personalizado: /Opt/NetApp/SnapCenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.
3. Liste os certificados adicionados no keystore:

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

4. Adicione um certificado raiz ou intermediário:

   ```
    keytool -import -trustcacerts -alias myRootCA -file
   /root/USERTrustRSA_Root.cer -keystore keystore.jks
   . Reinicie o serviço depois de configurar os certificados raiz ou
   intermédios para o armazenamento de confiança de plug-in personalizado.
   ```

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

Configure o par de chaves assinadas da CA para o armazenamento de confiança de plug-in personalizado

Você deve configurar o par de chaves assinadas da CA para o armazenamento de confiança do plug-in personalizado.

Passos

1. Navegue até a pasta que contém o keystore de plug-in personalizado /opt/NetApp/SnapCenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.
3. Liste os certificados adicionados no keystore:

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

4. Adicione o certificado da CA com chave privada e pública.

   ```
   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
   -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
   ```

5. Liste os certificados adicionados no keystore.

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

6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da CA para a senha do keystore.

   A senha padrão do keystore do plug-in personalizado é o valor da chave KEYSTORE_PASS no arquivo agent.properties.

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
   keystore.jks
   . Se o nome do alias no certificado da CA for longo e contiver espaço ou
   carateres especiais ("*",","), altere o nome do alias para um nome
   simples:
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   . Configure o nome do alias do certificado CA no arquivo
   agent.properties.
   ```

   Atualize este valor com a chave SCC_CERTIFICATE_ALIAS.

8. Reinicie o serviço depois de configurar o par de chaves assinadas pela CA para o armazenamento de confiança de plug-in personalizado.

Configurar a lista de revogação de certificados (CRL) para plug-ins personalizados do SnapCenter

Sobre esta tarefa

- Os plug-ins personalizados do SnapCenter pesquisarão os arquivos CRL em um diretório pré-configurado.

- O diretório padrão para os arquivos CRL para plug-ins personalizados do SnapCenter é ' opt/NetApp/SnapCenter/scc/etc/crl'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo agent.properties contra a chave CRL_PATH.

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

Configure o certificado CA para o serviço de plug-ins PostgreSQL do SnapCenter no host Windows

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

Plug-ins personalizados usam o arquivo *keystore.jks*, que está localizado em _C: Arquivos de programas, NetApp, SnapCenter, SnapCenter Plug-in Creator, tanto como seu armazenamento de confiança e armazenamento de chaves.

Gerenciar senha para armazenamento de chaves plug-in personalizado e alias do par de chaves assinadas CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore do plug-in personalizado do arquivo de propriedade do agente do plug-in personalizado.

   É o valor correspondente à chave *KEYSTORE_PASS*.

2. Altere a senha do keystore:

   keytool -storepasswd -keystore keystore.jks

   > Se o comando "keytool" não for reconhecido no prompt de comando do Windows, substitua o comando keytool por seu caminho completo.

   C: Arquivos de programas/<jdk_version>/keytool.exe" -storepasswd -keystore keystore.jks

3. Altere a senha para todos os aliases de entradas de chave privada no keystore para a mesma senha usada para o keystore:

   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks

   Atualize o mesmo para a chave KEYSTORE_PASS no arquivo *agent.properties*.

4. Reinicie o serviço depois de alterar a senha.

   > A palavra-passe para o armazenamento de chaves plug-in personalizado e para todas as palavras-passe de alias associadas da chave privada deve ser a mesma.

Configure certificados raiz ou intermediários para armazenamento de confiança de plug-in personalizado

Você deve configurar os certificados raiz ou intermediários sem a chave privada para armazenamento de confiança de plug-in personalizado.

Passos

1. Navegue até a pasta que contém o armazenamento de chaves de plug-in personalizado *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc*
2. Localize o arquivo 'keystore.jks'.
3. Liste os certificados adicionados no keystore:

   keytool -list -v -keystore keystore.jks

4. Adicione um certificado raiz ou intermediário:

   Keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_root.cer -keystore keystore.jks

5. Reinicie o serviço depois de configurar os certificados raiz ou intermédios para o armazenamento de confiança de plug-in personalizado.

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

Configure o par de chaves assinadas da CA para o armazenamento de confiança de plug-in personalizado

Você deve configurar o par de chaves assinadas da CA para o armazenamento de confiança do plug-in personalizado.

Passos

1. Navegue até a pasta que contém o armazenamento de chaves de plug-in personalizado *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc*
2. Localize o arquivo *keystore.jks*.
3. Liste os certificados adicionados no keystore:

   keytool -list -v -keystore keystore.jks

4. Adicione o certificado da CA com chave privada e pública.

   Keytool -importkeystore -srckeystore /root/SnapCenter.ssl.test.NetApp.com.pfx -srcstoretype PKCS12 -destinkeystore keystore.jks -deststoretype JKS

5. Liste os certificados adicionados no keystore.

   keytool -list -v -keystore keystore.jks

6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da CA para a senha do keystore.

   A senha padrão do keystore do plug-in personalizado é o valor da chave KEYSTORE_PASS no arquivo agent.properties.

   Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore keystore.jks

8. Configure o nome do alias do certificado CA no arquivo *agent.properties*.

   Atualize este valor com a chave SCC_CERTIFICATE_ALIAS.

9. Reinicie o serviço depois de configurar o par de chaves assinadas pela CA para o armazenamento de confiança de plug-in personalizado.

Configurar a lista de revogação de certificados (CRL) para plug-ins personalizados do SnapCenter

Sobre esta tarefa

- Para transferir o ficheiro CRL mais recente para o certificado CA relacionado, "Como atualizar o arquivo de lista de revogação de certificados no certificado da CA do SnapCenter"consulte .
- Os plug-ins personalizados do SnapCenter pesquisarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL para os plug-ins personalizados do SnapCenter é *'C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator etc/crl'*.

Passos

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

   Os certificados recebidos serão verificados em relação a cada CRL.

Ative certificados de CA para plug-ins

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

Antes de começar

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

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

Passos

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

Depois de terminar

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

- * * Indica que o certificado da CA não está habilitado nem atribuído ao host do plug-in.

- * * Indica que o certificado da CA foi validado com êxito.
- * * Indica que o certificado da CA não pôde ser validado.
- * * indica que as informações de conexão não puderam ser recuperadas.

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

Preparar-se para a proteção de dados

Pré-requisitos para usar o plug-in SnapCenter para PostgreSQL

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

- Instalar e configurar o servidor SnapCenter.
- Inicie sessão no servidor SnapCenter.
- Configure o ambiente SnapCenter adicionando conexões do sistema de storage e criando credenciais, se aplicável.
- Instale o Java 11 em seu host Linux ou Windows.

  Você deve definir o caminho Java na variável caminho ambiental da máquina host.

- Configure o SnapMirror e o SnapVault, se quiser replicação de backup.

Como recursos, grupos de recursos e políticas são usados para proteger o PostgreSQL

Antes de usar o SnapCenter, é útil entender conceitos básicos relacionados às operações de backup, clonagem e restauração que você deseja executar. Você interage com recursos, grupos de recursos e políticas para diferentes operações.

- Os recursos geralmente são clusters PostgreSQL que você faz backup ou clonar com o SnapCenter.
- Um grupo de recursos do SnapCenter é uma coleção de recursos em um host.

  Quando você executa uma operação em um grupo de recursos, executa essa operação nos recursos definidos no grupo de recursos de acordo com a programação especificada para o grupo de recursos.

  Você pode fazer backup sob demanda de um único recurso ou de um grupo de recursos. Você também pode executar backups programados para recursos únicos e grupos de recursos.

- As políticas especificam a frequência do backup, a replicação, os scripts e outras caraterísticas das operações de proteção de dados.

  Ao criar um grupo de recursos, você seleciona uma ou mais políticas para esse grupo. Você também pode selecionar uma política quando você executa um backup sob demanda para um único recurso.

Pense em um grupo de recursos como definindo o que você quer proteger e quando você quer protegê-lo em

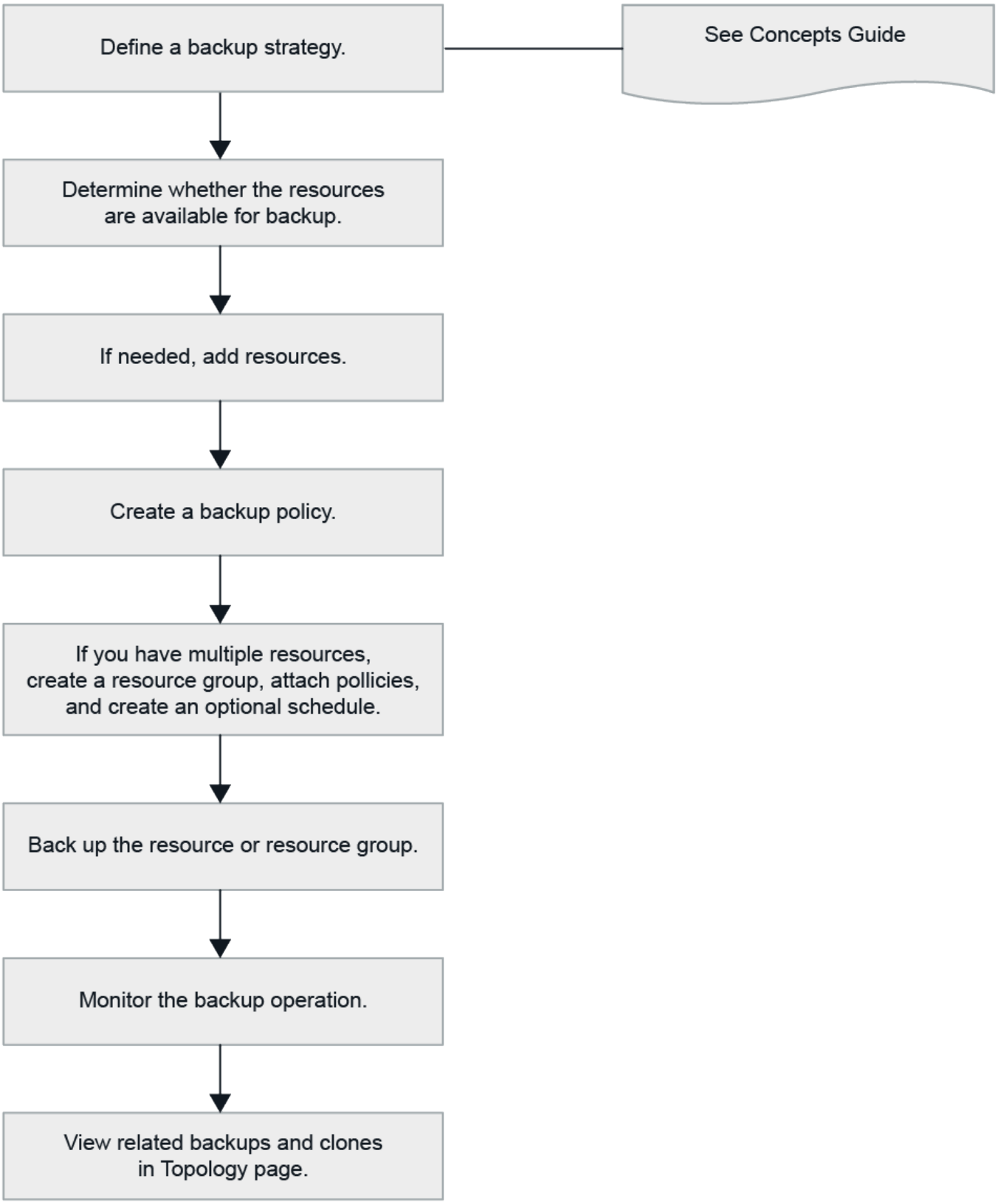
termos de dia e tempo. Pense em uma política como definir como você deseja protegê-la. Se você estiver fazendo backup de todos os clusters, por exemplo, poderá criar um grupo de recursos que inclua todos os clusters no host. Em seguida, você pode anexar duas políticas ao grupo de recursos: Uma política diária e uma política por hora. Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup completo diariamente.

Faça backup dos recursos do PostgreSQL

Faça backup dos recursos do PostgreSQL

Você pode criar um backup de um recurso (cluster) ou grupo de recursos. O fluxo de trabalho de backup inclui Planejamento, identificação dos clusters para backup, gerenciamento de políticas de backup, criação de grupos de recursos e inclusão de políticas, criação de backups e monitoramento das operações.

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



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clone. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm mais informações sobre cmdlets do PowerShell. "Guia de referência de cmdlet do software SnapCenter".

Descobrir os clusters automaticamente

Os recursos são clusters PostgreSQL no host Linux que são gerenciados pelo SnapCenter. Você pode adicionar os recursos a grupos de recursos para executar operações de proteção de dados depois de descobrir os clusters do PostgreSQL disponíveis.

Antes de começar

- Você já deve ter concluído tarefas como instalar o servidor SnapCenter, adicionar hosts e configurar as conexões do sistema de armazenamento.
- O plug-in do SnapCenter para PostgreSQL não oferece suporte à descoberta automática dos recursos residentes em ambientes virtuais RDM/VMDK.

Sobre esta tarefa

- Depois de instalar o plug-in, todos os clusters nesse host Linux são automaticamente descobertos e exibidos na página recursos.
- Somente clusters são auto-descobertos.

Os recursos descobertos automaticamente não podem ser modificados ou excluídos.

Passos

1. No painel de navegação à esquerda, clique em **Resources** e selecione o Plug-in para PostgreSQL na lista.
2. Na página recursos, selecione o tipo de recurso na lista Exibir.
3. (Opcional) clique em e selecione o nome do host.

   Em seguida, pode clicar em* * para fechar o painel do filtro.

4. Clique em **Atualizar recursos** para descobrir os recursos disponíveis no host.

   Os recursos são exibidos juntamente com informações como tipo de recurso, nome do host, grupos de recursos associados, tipo de backup, políticas e status geral.

   - Se o cluster estiver em um armazenamento NetApp e não estiver protegido, então não protegido será exibido na coluna Estado geral.
   - Se o cluster estiver em um sistema de armazenamento NetApp e protegido, e se não houver operação de backup executada, o Backup não executado será exibido na coluna Status geral. O status mudará para Backup failed ou Backup successful com base no último status de backup.

É necessário atualizar os recursos se os clusters forem renomeados fora do SnapCenter.

Adicione recursos manualmente ao host do plug-in

A deteção automática não é suportada no host Windows. Você deve adicionar recursos de cluster PostgreSQL manualmente.

Antes de começar

- Você deve ter concluído tarefas como instalar o servidor SnapCenter, adicionar hosts e configurar conexões do sistema de armazenamento.

Sobre esta tarefa

A deteção automática não é suportada para as seguintes configurações:

- Layouts RDM e VMDK

Passos

1. No painel de navegação à esquerda, selecione o plug-in do SnapCenter para PostgreSQL na lista suspensa e clique em **recursos**.
2. Na página recursos, clique em **Adicionar recursos PostgreSQL**.
3. Na página fornecer detalhes do recurso, execute as seguintes ações:

Para este campo…	Faça isso…
Nome	Especifique o nome do cluster.
Nome do host	Insira o nome do host.
Tipo	Selecione cluster.
Instância	Especifique o nome da instância, que é o pai do cluster.
Credenciais	Selecione as credenciais ou adicione informações para a credencial. Isso é opcional.

4. Na página fornecer espaço físico de armazenamento, selecione um tipo de armazenamento e escolha um ou mais volumes, LUNs e qtrees e clique em **Salvar**.

   Opcional: Você pode clicar no  ícone * para adicionar mais volumes, LUNs e qtrees de outros sistemas de armazenamento.

5. Opcional: Na página Configurações de recursos, para recursos no host do Windows, insira pares de valor de chave personalizados para o plug-in PostgreSQL
6. Revise o resumo e clique em **Finish**.

   Os clusters são exibidos juntamente com informações como o nome do host, grupos e políticas de recursos associados e status geral

Se você quiser fornecer aos usuários acesso a recursos, você deve atribuir os recursos aos usuários. Isso permite que os usuários executem as ações para as quais eles têm permissões nos ativos que são atribuídos a eles.

"Adicione um usuário ou grupo e atribua funções e ativos"

Depois de terminar

- Depois de adicionar os clusters, você pode modificar os detalhes do cluster PostgreSQL.
- Os recursos migrados (tablespace e clusters) do SnapCenter 5,0 serão marcados como tipo de cluster

PostgreSQL no SnapCenter 6,0.

- Quando você modifica os recursos adicionados manualmente que são migrados do SnapCenter 5,0 ou anterior, faça o seguinte na página **Configurações de recurso** para pares de valores de chave personalizados:
  - Especifique o termo "PORT" no campo **Name**.
  - Especifique o número da porta no campo **valor**.

Crie políticas de backup para PostgreSQL

Antes de usar o SnapCenter para fazer backup dos recursos do PostgreSQL, você deve criar uma política de backup para o grupo de recursos ou recursos que deseja fazer backup. Uma política de backup é um conjunto de regras que regem como você gerencia, agenda e retém backups.

Antes de começar

- Você precisa ter definido sua estratégia de backup.

  Para obter detalhes, consulte as informações sobre como definir uma estratégia de proteção de dados para clusters PostgreSQL.

- Você precisa se preparar para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, configurar conexões do sistema de storage e adicionar recursos.
- O administrador do SnapCenter deve ter atribuído os SVMs para os volumes de origem e destino a você se estiver replicando snapshots em um espelho ou cofre.

  Além disso, você pode especificar as configurações de replicação, script e aplicativo na política. Essas opções economizam tempo quando você deseja reutilizar a política para outro grupo de recursos.

Sobre esta tarefa

- SnapLock
  - Se a opção 'reter as cópias de backup para um número específico de dias' estiver selecionada, o período de retenção do SnapLock deve ser menor ou igual aos dias de retenção mencionados.
  - Especificar um período de bloqueio de instantâneos impede a exclusão dos instantâneos até que o período de retenção expire. Isso pode levar a reter um número maior de instantâneos do que a contagem especificada na política.
  - Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

> As configurações do SnapLock primário são gerenciadas na política de backup do SnapCenter e as configurações do SnapLock secundário são gerenciadas pelo ONTAP.

Passos

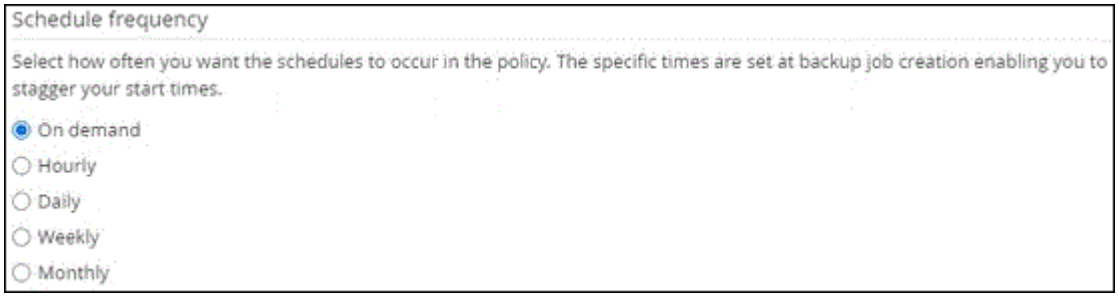
1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **políticas**.
3. Clique em **novo**.
4. Na página Nome, insira o nome e a descrição da política.

5. Na página tipo de política, execute o seguinte:
   a. Selecione o tipo de armazenamento.
   b. Na seção **Configurações personalizadas de backup**, forneça quaisquer configurações específicas de backup que tenham que ser passadas para o formato de valor de chave do plug-in.

      Você pode fornecer vários valores-chave a serem passados para o plug-in.

6. Na página Snapshot, especifique o tipo de agendamento selecionando **On Demand**, **Hourly**, **Daily**, **Weekly** ou **Monthly**.

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



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

7. Na seção Configurações de instantâneos, especifique o número de instantâneos que você deseja manter.
8. Na página retenção, especifique as configurações de retenção para o tipo de backup e o tipo de agendamento selecionado na página tipo de backup:

Se você quiser…	Então…
Mantenha um certo número de instantâneos	Selecione **Copies to keep** e especifique o número de instantâneos que deseja manter. Se o número de instantâneos exceder o número especificado, os instantâneos serão excluídos com as cópias mais antigas excluídas primeiro.

   Para backups baseados em cópias Snapshot, defina a contagem de retenção para 2 ou superior, se quiser habilitar a replicação do SnapVault. Se você definir a contagem de retenção como 1, a operação de retenção pode falhar porque o primeiro snapshot é o snapshot de referência para a relação SnapVault até que um snapshot mais recente seja replicado para o destino.

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

Crie grupos de recursos e anexe políticas

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.

Sobre esta tarefa

- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

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. O nome do grupo de recursos não deve exceder 250 carateres.
Tags	Insira um ou mais rótulos que o ajudarão a pesquisar posteriormente o grupo de recursos. Por exemplo, se você adicionar HR como uma tag a vários grupos de recursos, poderá encontrar mais tarde todos os grupos de recursos associados à tag HR.
Use o formato de nome personalizado para cópia instantânea	Marque essa caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do snapshot. Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.

4. Na página recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Resource Type**.

   Isso ajuda a filtrar informações na tela.

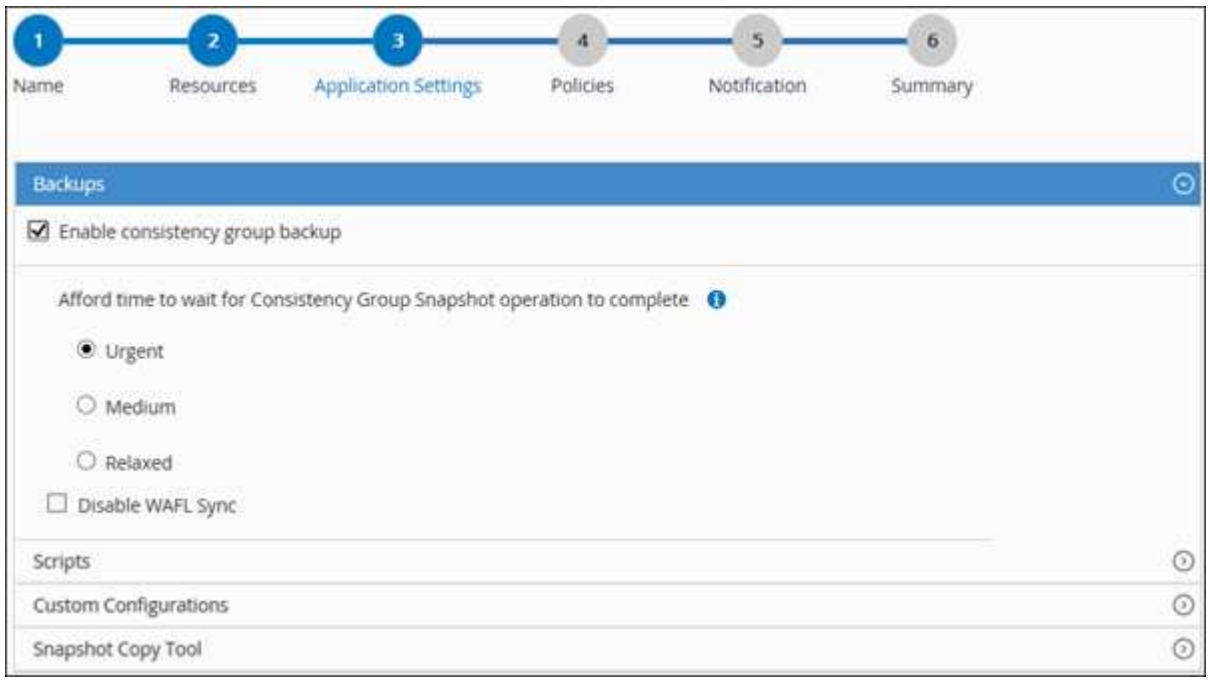
5. Selecione os recursos na seção **recursos disponíveis** e clique na seta para a direita para movê-los para a seção **recursos selecionados**.

6. Na página Configurações do aplicativo, faça o seguinte:

   a. Clique na seta **backups** para definir opções adicionais de backup:

      Ative o backup do grupo de consistência e execute as seguintes tarefas:

Para este campo…	Faça isso…
Tenha tempo para esperar que a operação de snapshot do Grupo de consistência seja concluída	Selecione **urgente**, **Médio** ou **relaxado** para especificar o tempo de espera para que a operação de snapshot seja concluída. Urgente: 5 segundos, Médio: 7 segundos e relaxado: 20 segundos.
Desativar a sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL.

+ 

   a. Clique na seta **Scripts** e insira os comandos pre e POST para operações quiesce, snapshot e unquiesce. Também pode introduzir os pré comandos a serem executados antes de sair em caso de falha.

   b. Clique na seta **Custom Configurations** (Configurações personalizadas) e insira os pares de valor de chave personalizados necessários para todas as operações de proteção de dados usando esse recurso.

Parâmetro	Definição	Descrição
ARCHIVE_LOG_ENABLE	(Y/N)	Permite que a gestão do registo de arquivo elimine os registos de arquivo.

Parâmetro	Definição	Descrição
ARCHIVE_LOG_RETENÇÃO	number_of_days	Especifica o número de dias em que os logs de arquivo são mantidos. Esta definição tem de ser igual ou superior a NTAP_SNAPSHOT_ RETENÇÕES.
ARCHIVE_LOG_DIR	change_info_directory/logs	Especifica o caminho para o diretório que contém os logs do arquivo.
ARCHIVE_LOG_EXT	extensão_ficheiro	Especifica o comprimento da extensão do arquivo de log do arquivo. Por exemplo, se o log de arquivo for log_backup_0_0_0_0,16151855 1942 9 e se o valor file_extension for 5, a extensão do log manterá 5 dígitos, que é 16151.
ARCH ARCHIVE_LOG_RECURSIVE_ SE	(Y/N)	Permite o gerenciamento de logs de arquivo dentro de subdiretórios. Você deve usar este parâmetro se os logs do arquivo estiverem localizados em subdiretórios.

Os pares de chave-valor personalizados são suportados para sistemas de plug-in PostgreSQL Linux e não são suportados para cluster PostgreSQL registrado como um plug-in centralizado do Windows.

c. Clique na seta **Snapshot Copy Tool** para selecionar a ferramenta para criar instantâneos:

Se você quiser…	Então…
SnapCenter para usar o plug-in para Windows e colocar o sistema de arquivos em um estado consistente antes de criar um snapshot. Para recursos do Linux, essa opção não é aplicável.	Selecione **SnapCenter com consistência do sistema de arquivos**.
SnapCenter para criar um instantâneo de nível de storage	Selecione **SnapCenter sem consistência do sistema de arquivos**.

Se você quiser…	Então…
Para inserir o comando a ser executado no host para criar cópias snapshot.	Selecione **Other** e, em seguida, digite o comando a ser executado no host para criar um snapshot.

7. Na página políticas, execute as seguintes etapas:

   a. Selecione uma ou mais políticas na lista suspensa.

      Você também pode criar uma política clicando em + .

      As políticas são listadas na seção Configurar programações para políticas selecionadas.

   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**.

      Onde, policy_name é o nome da política selecionada.

      As programações configuradas são listadas na coluna **programações aplicadas**.

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

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

   Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. O servidor SMTP deve ser configurado em **Configurações** > **Configurações globais**.

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

Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para PostgreSQL

Você deve criar uma conexão de máquina virtual de armazenamento (SVM) e uma credencial antes de usar cmdlets do PowerShell para fazer backup, restaurar ou clonar clusters PostgreSQL.

Antes de começar

- Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.
- Você deve ter as permissões necessárias na função Administrador da infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estão em andamento.

  As instalações de plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento, pois o cache do host pode não ser atualizado e o status dos clusters pode ser exibido na GUI do SnapCenter como "'não disponível para backup'" ou "'não no armazenamento NetApp'".

- Os nomes do sistema de armazenamento devem ser exclusivos.

  O SnapCenter não é compatível com vários sistemas de storage com o mesmo nome em clusters diferentes. Cada sistema de storage com suporte do SnapCenter deve ter um nome exclusivo e um endereço IP de LIF de dados exclusivo.

Passos

1. Inicie uma sessão de conexão do PowerShell Core usando o cmdlet Open-SmConnection.

```
PS C:\> Open-SmConnection
```

2. Crie uma nova conexão com o sistema de armazenamento usando o cmdlet Add-SmStorageConnection.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Crie uma nova credencial usando o cmdlet Add-SmCredential.

   Este exemplo mostra como criar uma nova credencial chamada FinanceAdmin com credenciais do Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. Adicione o host de comunicação PostgreSQL ao servidor SnapCenter.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode PostgreSQL
```

5. Instale o pacote e o plug-in SnapCenter para PostgreSQL no host.

   Para Linux:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
PostgreSQL
```

   Para Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
PostgreSQL -FilesystemCode scw -RunAsName FinanceAdmin
```

6. Defina o caminho para o SQLLIB.

Para Windows, o plug-in PostgreSQL usará o caminho padrão para a pasta SQLLIB:

Se você quiser substituir o caminho padrão, use o seguinte comando.

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
PostgreSQL -configSettings @{“PostgreSQL_SQLLIB_CMD” =
“<custom_path>\IBM\SQLLIB\BIN”}
```

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

Faça backup do PostgreSQL

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 ter criado uma política de backup.
- Se você quiser fazer backup de um recurso que tenha uma relação SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário de armazenamento deve incluir o privilégio "'SnapMirror All'". No entanto, se você estiver usando a função "vsadmin", o privilégio "SnapMirror all" não será necessário.
- Para a operação de backup baseada em cópia Snapshot, verifique se todos os clusters de locatários estão válidos e ativos.
- Para comandos pré e POST para operações quiesce, Snapshot e unquiesce, você deve verificar se os comandos existem na lista de comandos disponível no host plug-in dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
  - Localização padrão no host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_Commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

IU do SnapCenter

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.

   Selecione e, em seguida, selecione o nome do host e o tipo de recurso para filtrar os recursos. Em seguida, pode selecionar para fechar o painel de filtro.
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.

   Por exemplo, *customtext_policy_hostname* ou *resource_hostname*. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.
5. Na página Configurações do aplicativo, faça o seguinte:
   - Selecione a seta **backups** para definir opções adicionais de backup:

     Ative o backup do grupo de consistência, se necessário, e execute as seguintes tarefas:

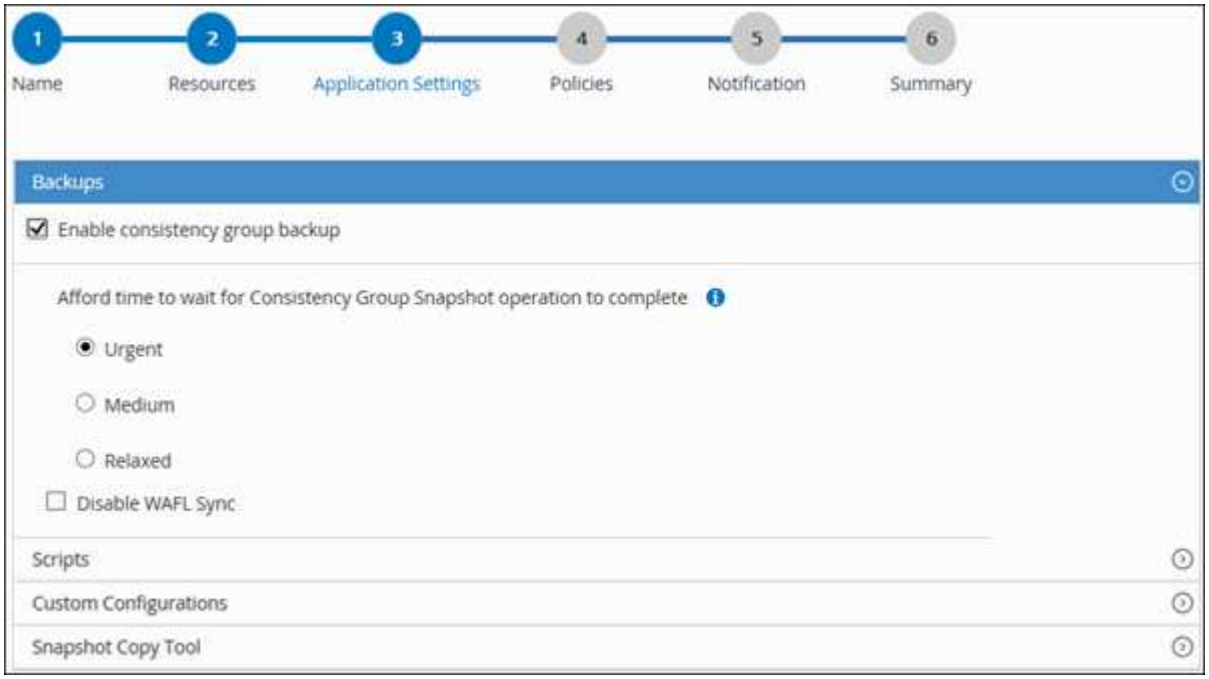
Para este campo…	Faça isso…
Tenha tempo para esperar a conclusão da operação "Consistency Group Snapshot"	Selecione **urgente**, **Médio** ou **relaxado** para especificar o tempo de espera para que a operação Snapshot termine. Urgente: 5 segundos, Médio: 7 segundos e relaxado: 20 segundos.
Desativar a sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL.

   - Selecione a seta **Scripts** para executar comandos pré e POST para operações quiesce, Snapshot e unquiesce.

     Você também pode executar pré-comandos antes de sair da operação de backup. Os Prescripts e postscripts são executados no servidor SnapCenter.
   - Selecione a seta **Custom Configurations (Configurações personalizadas) e, em seguida, insira os pares de valores personalizados necessários para todos os trabalhos que usam esse recurso.
   - Selecione a seta **Snapshot Copy Tool** para selecionar a ferramenta para criar instantâneos:

Se você quiser…	Então…
SnapCenter para criar um Snapshot no nível de storage	Selecione **SnapCenter sem consistência do sistema de arquivos**.

Se você quiser…	Então…
SnapCenter para usar o plug-in para Windows para colocar o sistema de arquivos em um estado consistente e, em seguida, criar um instantâneo	Selecione **SnapCenter com consistência do sistema de arquivos**.
Para inserir o comando para criar uma captura Instantânea	Selecione **Other** e, em seguida, digite o comando para criar uma captura Instantânea.



6. Na página políticas, execute as seguintes etapas:

   a. Selecione uma ou mais políticas na lista suspensa.

      Você também pode criar uma política clicando em + .

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

   b. 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.

   As programações configuradas são listadas na coluna agendas aplicadas.

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

Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. O SMTP também deve ser configurado em **Configurações** > **Configurações globais**.

8. Revise o resumo e selecione **Finish**.

   A página de topologia de recursos é exibida.

9. Selecione **fazer uma cópia de segurança agora**.
10. Na página Backup, execute as seguintes etapas:
    a. Se você aplicou várias políticas ao recurso, na lista suspensa **Política**, selecione a política que deseja usar para backup.

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

    b. Selecione **Backup**.
11. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.
    - Nas configurações do MetroCluster, o SnapCenter pode não ser capaz de detetar uma relação de proteção após um failover.

      Para obter informações, consulte: "Não é possível detetar a relação SnapMirror ou SnapVault após o failover do MetroCluster"

    - Se você estiver fazendo backup de dados de aplicativos em VMDKs e o tamanho de heap Java para o plug-in SnapCenter para VMware vSphere não for grande o suficiente, o backup pode falhar.

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

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado usando o cmdlet Open-SmConnection.

   ```
   PS C:\> Open-SmConnection
   ```

   É apresentado o aviso de nome de utilizador e palavra-passe.

2. Adicione recursos manuais usando o cmdlet Add-SmResources.

   Este exemplo mostra como adicionar uma instância do PostgreSQL:

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode PostgreSQL
-ResourceType Instance -ResourceName postgresqlinst1
-StorageFootPrint
(@{"VolumeName"="winpostgresql01_data01";"LUNName"="winpostgresql01_
data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. Crie uma política de backup usando o cmdlet Add-SmPolicy.
4. Proteja o recurso ou adicione um novo grupo de recursos ao SnapCenter usando o cmdlet Add-SmResourceGroup.
5. Inicie uma nova tarefa de backup usando o cmdlet New-SmBackup.

   Este exemplo mostra como fazer backup de um grupo de recursos:

   ```
   C:\PS> New-SMBackup -ResourceGroupName 'ResourceGroup_wback-up-
   clusters-using-powershell-cmdlets-postgresql.adocith_Resources'
   -Policy postgresql_policy1
   ```

   Este exemplo faz backup de um recurso protegido:

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="postgresql"}
   -Policy postgresql_policy2
   ```

6. Monitore o status da tarefa (em execução, concluída ou com falha) usando o cmdlet Get-smJobSummaryReport.

   ```
   PS C:\> Get-smJobSummaryReport -JobID 123
   ```

7. Monitore os detalhes da tarefa de backup, como ID do backup, nome do backup para executar a operação de restauração ou clone usando o cmdlet Get-SmBackupReport.

```
PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
```

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

Fazer backup de grupos de recursos

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.

Antes de começar

- Você deve ter criado um grupo de recursos com uma política anexada.
- Se você quiser fazer backup de um recurso que tenha uma relação SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário de armazenamento deve incluir o privilégio "'SnapMirror All'". No entanto, se você estiver usando a função "vsadmin", o privilégio "SnapMirror all" não será necessário.

Sobre esta tarefa

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

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**.

   Você pode pesquisar o grupo de recursos inserindo o nome do grupo de recursos na caixa de pesquisa ou selecionando e selecionando a tag. Em seguida, pode selecionar para fechar o painel de filtro.
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 você associou várias políticas ao grupo de recursos, na lista suspensa **Política**, selecione a política que deseja usar para backup.

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

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

Monitore as operações de backup do PostgreSQL

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

Sobre esta tarefa

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

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

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **trabalhos**.
3. Na página trabalhos, execute as seguintes etapas:

a. Clique para filtrar a lista de modo a que apenas as operações de cópia de segurança sejam listadas.
b. Especifique as datas de início e fim.
c. Na lista suspensa **Type**, selecione **Backup**.
d. Na lista suspensa **Status**, selecione o status da cópia de segurança.
e. Clique em **Apply** para ver as operações concluídas com êxito.

4. Selecione um trabalho de cópia de segurança e clique em **Detalhes** para ver os detalhes do trabalho.

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

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

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

Monitore operações de proteção de dados em clusters PostgreSQL no painel atividade

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

O painel atividade exibe informações sobre operações de backup, restauração, clone e backup agendadas.

Passos

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

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

Cancelar operações de backup para PostgreSQL

Você pode cancelar as operações de backup que estão na fila.

O que você vai precisar

- Você deve estar logado como administrador do SnapCenter ou proprietário do trabalho para cancelar as operações.
- Você pode cancelar uma operação de backup na página **Monitor** ou no painel **atividade**.
- Não é possível cancelar uma operação de cópia de segurança em execução.
- Você pode usar os comandos GUI, cmdlets do SnapCenter ou CLI para cancelar as operações de backup.
- O botão **Cancelar trabalho** está desativado para operações que não podem ser canceladas.
- Se você selecionou **todos os membros desta função podem ver e operar em objetos de outros membros** na página usuários/grupos ao criar uma função, você pode cancelar as operações de backup em fila de outros membros enquanto usa essa função.

Passos

1. Execute uma das seguintes ações:

A partir do…	Ação
Página do monitor	a. No painel de navegação esquerdo, clique em **Monitor** > **trabalhos**. b. Selecione a operação e clique em **Cancelar trabalho**.
Painel da atividade	a. Depois de iniciar a operação de backup, clique em no painel atividade para exibir as cinco operações mais recentes. b. Selecione a operação. c. Na página Detalhes da tarefa, clique em **Cancelar tarefa**.

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

Veja backups e clones do PostgreSQL na página topologia

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

Sobre esta tarefa

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

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

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

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

Na página topologia, você pode ver todos os backups e clones disponíveis para o grupo de recursos ou

recursos selecionado. Você pode visualizar os detalhes desses backups e clones e, em seguida, selecioná-los para executar operações de proteção de dados.

Passos

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

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

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

   A seção **cartão de resumo** exibe o número total de backups e clones baseados em cópia Snapshot.

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

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

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

   Após o backup sob demanda, clicando no botão **Refresh** atualiza os detalhes do backup ou clone.

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

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

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

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

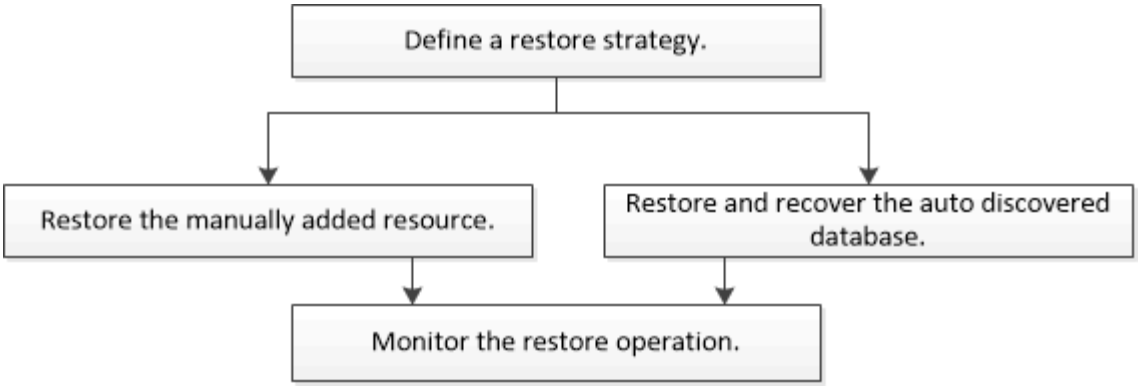
7. Se quiser excluir um clone, selecione-o na tabela e clique em .
8. Se quiser dividir um clone, selecione-o na tabela e clique em .

Restaure o PostgreSQL

Restaure o fluxo de trabalho

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

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



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clone. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre cmdlets do PowerShell.

"Guia de referência de cmdlet do software SnapCenter".

Restaure e recupere um backup de recursos adicionado manualmente

Você pode usar o SnapCenter para restaurar e recuperar dados de um ou mais backups.

Antes de começar

- Você deve ter feito backup dos grupos de recursos ou recursos.
- Você deve ter cancelado qualquer operação de backup que esteja atualmente em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos pré-restauração, pós restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in a partir dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
  - Localização padrão no host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_Commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

Sobre esta tarefa

- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

IU do SnapCenter

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.

   Os recursos são exibidos juntamente com o tipo, host, grupos de recursos e políticas associados e status.

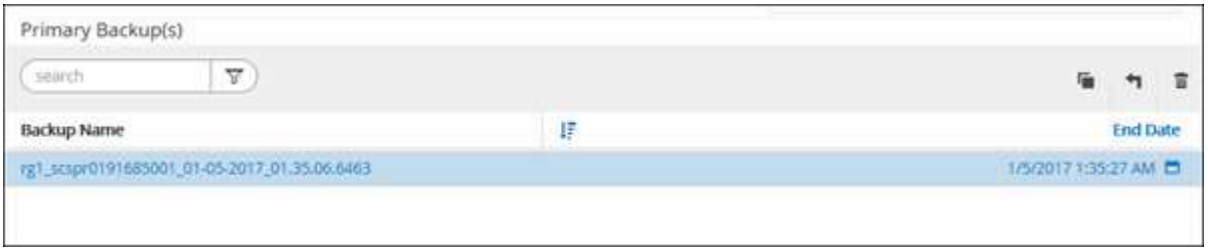
   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

   Se o recurso não estiver protegido, ""não protegido"" é exibido na coluna Estado geral. Isso pode significar que o recurso não está protegido ou que o recurso foi protegido por um usuário diferente.

3. Selecione o recurso ou selecione um grupo de recursos e, em seguida, selecione um recurso nesse grupo.

   A página de topologia do recurso é exibida.

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**.

   a. Se você selecionar **Complete Resource**, todos os volumes de dados configurados do cluster PostgreSQL serão restaurados.

      Se o recurso contiver volumes ou qtrees, os instantâneos obtidos após o instantâneo selecionado para restauração nesses volumes ou qtrees serão excluídos e não poderão ser recuperados. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído.

      Pode selecionar vários LUNs.

      Se você selecionar **All**, todos os arquivos nos volumes, qtrees ou LUNs serão restaurados.

7. Na página operações anteriores, insira pré-restauração e desmonte comandos para serem executados antes de executar um trabalho de restauração.

   Os comandos de desmontagem não estão disponíveis para recursos descobertos automaticamente.

8. Na página Post OPS, insira os comandos mount e POST Restore para serem executados após a execução de um trabalho de restauração.

   Os comandos de montagem não estão disponíveis para recursos descobertos automaticamente.

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

   Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. O SMTP também deve ser configurado na página **Configurações** > **Configurações globais**.

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

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado usando o cmdlet Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Recupere as informações sobre um ou mais backups que você deseja restaurar usando os cmdlets Get-SmBackup e Get-SmBackupReport.

   Este exemplo exibe informações sobre todos os backups disponíveis:

```
PS C:\> Get-SmBackup

BackupId                      BackupName
BackupTime                    BackupType
--------                      ----------
----------                    ----------
  1               Payroll Dataset_vise-f6_08... 8/4/2015    11:02:32
AM                 Full Backup
  2               Payroll Dataset_vise-f6_08... 8/4/2015    11:23:17
AM
```

   Este exemplo exibe informações detalhadas sobre o backup de 29th 2015 de janeiro a 3rd de fevereiro de 2015:

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

   SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

3. Restaure dados do backup usando o cmdlet Restore-SmBackup.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

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

Restaure e recupere um backup de cluster descoberto automaticamente

Você pode usar o SnapCenter para restaurar e recuperar dados de um ou mais backups.

Antes de começar

- Você deve ter feito backup dos grupos de recursos ou recursos.
- Você deve ter cancelado qualquer operação de backup que esteja atualmente em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos pré-restauração, pós restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in a partir dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter*

Plug-in Creator/etc/allowed_commands.config

- Localização padrão no host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_Commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

Sobre esta tarefa

- As cópias de backup baseadas em arquivo não podem ser restauradas a partir do SnapCenter.
- Para recursos descoberta automática, a restauração é suportada com SFSR.
- A recuperação automática não é suportada.
- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

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.

   Os recursos são exibidos juntamente com o tipo, host, grupos de recursos e políticas associados e status.

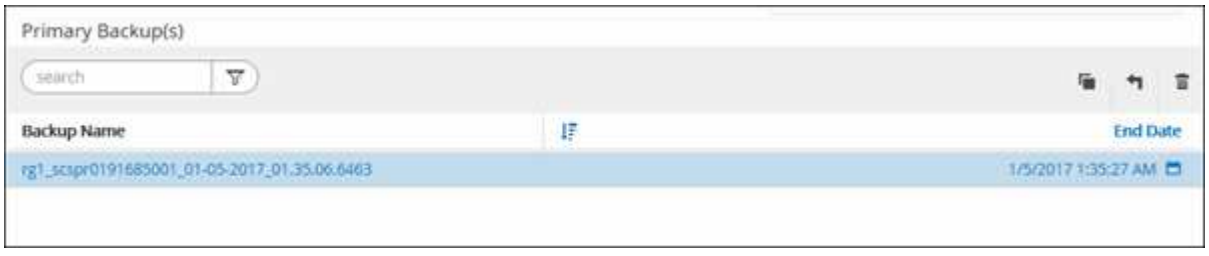
   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

   Se o recurso não estiver protegido, ""não protegido"" é exibido na coluna Estado geral. Isso pode significar que o recurso não está protegido ou que o recurso foi protegido por um usuário diferente.

3. Selecione o recurso ou selecione um grupo de recursos e, em seguida, selecione um recurso nesse grupo.

   A página de topologia do recurso é exibida.

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** para restaurar os volumes de dados configurados do cluster PostgreSQL.
7. Na página âmbito de recuperação, selecione uma das seguintes opções:

Se você…	Faça isso…

Deseja recuperar o mais próximo possível da hora atual	Selecione **Recover to most recent State** (recuperar para o estado mais recente). Para recursos de contentor único, especifique um ou mais locais de backup de log e catálogo.
Deseja recuperar para o ponto especificado no tempo	Selecione **Recover to point in time**. a. Introduza a data e a hora. Introduza a data e a hora. Por exemplo, o host PostgreSQL Linux está localizado em Sunnyvale, CA e o usuário em Raleigh, NC está recuperando os logs no SnapCenter. Se o usuário deseja executar uma recuperação para 5 a.m .Sunnyvale, CA, então o usuário deve definir o fuso horário do navegador para o fuso horário do host PostgreSQL Linux, que é GMT-07:00 e especificar a data e hora como 5:00 a.m.
Não quero recuperar	Selecione **sem recuperação**.

Você não pode recuperar recursos PostgreSQL adicionados manualmente.

O plug-in SnapCenter para PostgreSQL cria uma pasta backup_label e tablespace_map na pasta */<OS_temp_folder>/postgresql_SC_recovery*<Restore_JobId>/_ para ajudar a recuperar manualmente.

1. Na página operações anteriores, insira pré-restauração e desmonte comandos para serem executados antes de executar um trabalho de restauração.

   Os comandos de desmontagem não estão disponíveis para recursos descobertos automaticamente.

2. Na página Post OPS, insira os comandos mount e POST Restore para serem executados após a execução de um trabalho de restauração.

   Os comandos de montagem não estão disponíveis para recursos descobertos automaticamente.

3. 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**.

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

Restaure recursos usando cmdlets do PowerShell

A restauração de um backup de recurso inclui iniciar uma sessão de conexão com o

servidor SnapCenter, listar os backups e recuperar informações de backup e restaurar um backup.

Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado usando o cmdlet Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Recupere as informações sobre um ou mais backups que você deseja restaurar usando os cmdlets Get-SmBackup e Get-SmBackupReport.

   Este exemplo exibe informações sobre todos os backups disponíveis:

```
PS C:\> Get-SmBackup

BackupId                      BackupName                    BackupTime
BackupType
--------                      ----------                    ----------
----------
  1               Payroll Dataset_vise-f6_08... 8/4/2015    11:02:32 AM
Full Backup
  2               Payroll Dataset_vise-f6_08... 8/4/2015    11:23:17 AM
```

   Este exemplo exibe informações detalhadas sobre o backup de 29th 2015 de janeiro a 3rd de fevereiro de 2015:

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

   SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

3. Restaure dados do backup usando o cmdlet Restore-SmBackup.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

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

Monitore as operações de restauração do PostgreSQL

Pode monitorizar o progresso de diferentes operações de restauro do SnapCenter utilizando a página trabalhos. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

os estados pós-restauração descrevem as condições do recurso após uma operação de restauração e quaisquer outras ações de restauração que você possa executar.

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

- Em curso

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

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que apenas as operações de restauração sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Restore**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Apply** para ver as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para exibir os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Visualizar logs**.

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

Clonar backups de recursos do PostgreSQL

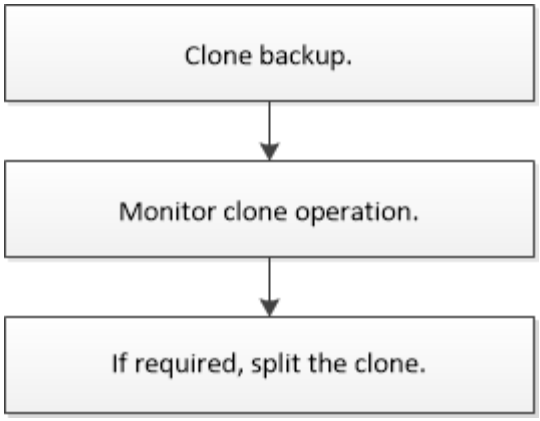
Fluxo de trabalho clone

O fluxo de trabalho do clone inclui a execução da operação de clone e o monitoramento da operação.

Sobre esta tarefa

- Você pode clonar no servidor PostgreSQL de origem.
- Você pode clonar backups de recursos pelos seguintes motivos:
  - Para testar a funcionalidade que deve ser implementada usando a estrutura e o conteúdo atuais dos recursos durante os ciclos de desenvolvimento de aplicativos
  - Para ferramentas de extração e manipulação de dados ao preencher data warehouses
  - Para recuperar dados que foram excluídos ou alterados por engano

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



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clone. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre cmdlets do PowerShell.

Clonar um backup PostgreSQL

Você pode usar o SnapCenter para clonar um backup. Você pode clonar do backup primário ou secundário.

Antes de começar

- Você deve ter feito backup dos recursos ou do grupo de recursos.
- Você deve garantir que os agregados que hospedam os volumes estejam na lista de agregados atribuídos da máquina virtual de storage (SVM).
- Para comandos pré-clone ou pós-clone, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in a partir dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
  - Localização padrão no host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_Commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

Sobre esta tarefa

- Para obter informações sobre limitações de operação de divisão de clones, "Guia de gerenciamento de storage lógico do ONTAP 9" consulte .
- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

IU do SnapCenter

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.

   Os recursos são exibidos juntamente com informações como tipo, host, grupos e políticas de recursos associados e status.

3. Selecione o grupo de recursos ou recursos.

   Você deve selecionar um recurso se selecionar um grupo de recursos.

   A página de topologia do grupo de recursos ou recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).
5. Selecione o backup de dados na tabela e clique em .
6. Na página localização, execute as seguintes ações:

Para este campo…	Faça isso…
Servidor clone	Escolha um host no qual o clone deve ser criado.
Porta-alvo	Insira a porta de destino PostgreSQL para clonar dos backups existentes.
Endereço IP de exportação NFS	Insira endereços IP ou os nomes de host nos quais os volumes clonados serão exportados. Isso é aplicável apenas ao recurso do tipo de storage NFS.
Taxa de transferência máx. Do pool de capacidade (MIB/s)	Insira a taxa de transferência máxima de um pool de capacidade. Isso se aplica apenas ao recurso do tipo de storage do ANF.

7. Na página Scripts, execute as seguintes etapas:

   Os scripts são executados no host do plug-in.

   a. Digite os comandos para pré-clone ou pós-clone que devem ser executados antes ou depois da operação clone, respetivamente.
      - Comando pré-clone: Exclua clusters existentes com o mesmo nome
      - Comando pós-clone: Verifique um cluster ou inicie um cluster.
   b. Digite o comando mount para montar um sistema de arquivos em um host.

Monte o comando para um volume ou qtree em uma máquina Linux:

Exemplo para NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

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

   Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail.

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

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado usando o cmdlet Open-SmConnection.

```
PS C:\> Open-SmConnection
```

2. Recupere os backups para executar a operação de clone usando o cmdlet Get-SmBackup.

   Este exemplo mostra que dois backups estão disponíveis para clonagem:

```
 C:\PS> Get-SmBackup

        BackupId                    BackupName
BackupTime                  BackupType
        --------                    ----------
----------                  ----------
         1                   Payroll Dataset_vise-f6_08...
8/4/2015 11:02:32 AM        Full Backup
         2                   Payroll Dataset_vise-f6_08...
8/4/2015 11:23:17 AM
```

3. Inicie uma operação de clone a partir de um backup existente e especifique os endereços IP de exportação NFS nos quais os volumes clonados são exportados.

   Este exemplo mostra que o backup a ser clonado tem um endereço NFSExportIPs de 10.32.212.14:

   Para o cluster PostgreSQL:

```
PS C:\> New-SmClone -AppPluginCode PostgreSQL -BackupName "
scpostgresql01_ openenglab_netapp_com_PostgreSQL_postgres_5432_06-
26-2024_00_33_41_1570" -Resources @{"Host"="
10.32.212.13";"Uid"="postgres_5432"} -port 2345 -CloneToHost
10.32.212.14
```

Se NFSExportIPs não for especificado, o padrão será exportado para o host de destino clone.

4. Verifique se os backups foram clonados com sucesso usando o cmdlet Get-SmCloneReport para exibir os detalhes da tarefa clone.

   Você pode exibir detalhes como ID do clone, data e hora de início, data e hora de término.

```
PS C:\> Get-SmCloneReport -JobId 186

    SmCloneId           : 1
    SmJobId             : 186
    StartDateTime       : 8/3/2015 2:43:02 PM
    EndDateTime         : 8/3/2015 2:44:08 PM
    Duration            : 00:01:06.6760000
    Status              : Completed
    ProtectionGroupName : Draper
    SmProtectionGroupId : 4
    PolicyName          : OnDemand_Clone
    SmPolicyId          : 4
    BackupPolicyName    : OnDemand_Full_Log
    SmBackupPolicyId    : 1
    CloneHostName       : SCSPR0054212005.mycompany.com
    CloneHostId         : 4
    CloneName           : Draper__clone__08-03-2015_14.43.53
    SourceResources     : {Don, Betty, Bobby, Sally}
    ClonedResources     : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
    SmJobError          :
```

Monitore as operações de clone do PostgreSQL

Você pode monitorar o andamento das operações de clone do SnapCenter usando a página tarefas. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

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

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

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista para que apenas operações de clone sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione a tarefa clone e clique em **Detalhes** para exibir os detalhes da tarefa.
5. Na página Detalhes da tarefa, clique em **Exibir logs**.

Divida um clone

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido torna-se independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clones em um clone intermediário.

  Por exemplo, depois de criar clone1 a partir de um backup de banco de dados, você pode criar um backup de clone1 e clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e não é possível executar a operação de divisão de clones no clone1. No entanto, você pode executar a operação de divisão de clones no clone2.

  Depois de dividir clone2, você pode executar a operação de divisão de clones no clone1 porque clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup e as tarefas de clone do clone são excluídas.
- Para obter informações sobre limitações de operação de divisão de clones, "Guia de gerenciamento de storage lógico do ONTAP 9" consulte .
- Certifique-se de que o volume ou o agregado no sistema de storage esteja on-line.

Passos

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

2. Na página **recursos**, selecione a opção apropriada na lista Exibir:

Opção	Descrição
Para aplicativos de banco de dados	Selecione **Banco de dados** na lista Exibir.
Para sistemas de arquivos	Selecione **caminho** na lista Exibir.

3. Selecione o recurso apropriado na lista.

   A página de topologia do recurso é exibida.

4. No modo de exibição **Gerenciar cópias**, selecione o recurso clonado (por exemplo, o banco de dados ou LUN) e clique em *  .
5. Revise o tamanho estimado do clone que deve ser dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
6. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

   A operação de divisão de clones deixa de responder se o serviço SMCore for reiniciado. Você deve executar o cmdlet Stop-SmJob para interromper a operação de divisão de clones e tentar novamente a operação de divisão de clones.

   Se você quiser um tempo de enquete mais longo ou menor para verificar se o clone está dividido ou não, você pode alterar o valor do parâmetro *CloneSplitStatusCheckPollTime* no arquivo *SMCoreServiceHost.exe.config* para definir o intervalo de tempo para que o SMCore busque o status da operação de divisão de clones. O valor é em milissegundos e o valor padrão é de 5 minutos.

   Por exemplo:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

   A operação de inicialização dividida de clone falhará se o backup, a restauração ou outra divisão de clones estiver em andamento. Você deve reiniciar a operação de divisão de clones somente depois que as operações em execução estiverem concluídas.

Informações relacionadas

"O clone ou a verificação do SnapCenter falha com o agregado não existe"

Exclua ou divida clones do cluster do PostgreSQL após a atualização do SnapCenter

Após a atualização para o SnapCenter 4,3, você não verá mais os clones. Você pode excluir o clone ou dividir os clones da página topologia do recurso a partir do qual os clones foram criados.

Sobre esta tarefa

Se você quiser localizar o espaço físico de armazenamento dos clones ocultos, execute o seguinte comando: `Get-SmClone -ListStorageFootprint`

Passos

1. Exclua os backups dos recursos clonados usando o cmdlet remove-smbackup.
2. Exclua o grupo de recursos dos recursos clonados usando o cmdlet remove-smresourcegroup.
3. Remova a proteção do recurso clonado usando o cmdlet remove-sprotectresource.
4. Selecione o recurso pai na página recursos.

   A página de topologia do recurso é exibida.

5. Na visualização Gerenciar cópias, selecione os clones nos sistemas de storage primário ou secundário (espelhado ou replicado).
6. Selecione os clones e clique  para excluir clones ou clique para  dividir os clones.
7. Clique em **OK**.

Informações sobre direitos autorais

Informações sobre marcas comerciais