Proteger PostgreSQL

SnapCenter software

NetApp
November 06, 2025

Índice

Proteger PostgreSQL

Plug-in SnapCenter para PostgreSQL

Visão geral do plug-in SnapCenter para PostgreSQL

O plug-in SnapCenter para cluster PostgreSQL é um componente do lado do host do software NetApp SnapCenter software que permite o gerenciamento de proteção de dados com reconhecimento de aplicativo de clusters PostgreSQL. O plug-in para cluster PostgreSQL automatiza o backup, a restauração e a clonagem de clusters PostgreSQL no seu ambiente SnapCenter .

O SnapCenter oferece suporte a configurações de cluster único e multicluster do 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 estiver instalado, você poderá 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 de disco para disco para conformidade com os padrões.

O plug-in SnapCenter para PostgreSQL oferece suporte a NFS e SAN em layouts de armazenamento de arquivos ONTAP e Azure NetApp .

O layout de armazenamento virtual VMDK, vVol e RDM é suportado.

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

Ao instalar o plug-in para cluster 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.
- Crie backups.
- Restaurar a partir de backups.
- Clonar backups.
- Agende operações de backup.
- Monitore operações de backup, restauração e clonagem.
- Visualize relatórios de operações de backup, restauração e clonagem.

Recursos do plug-in SnapCenter para PostgreSQL

O SnapCenter integra-se ao aplicativo plug-in e às tecnologias NetApp no sistema de armazenamento. Para trabalhar com o Plug-in para o Cluster PostgreSQL, use a interface gráfica do usuário do SnapCenter .

- **Interface gráfica de usuário unificada**

A interface do SnapCenter fornece padronização e consistência entre plug-ins e ambientes. A interface do SnapCenter permite que você conclua operações consistentes de backup, restauração e clonagem em plug-ins, use relatórios centralizados, use visualizações de painel rápidas, configure o controle de acesso baseado em função (RBAC) e monitore trabalhos em todos os plug-ins.

- **Administração central automatizada**

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

- *Tecnologia de cópia instantânea não disruptiva da NetApp *

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

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

- Suporte para fluxos de trabalho de backup, restauração e clonagem
- Segurança com suporte RBAC e delegação centralizada de funções

  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 eficiência de espaço e em um determinado momento para testes ou extração de dados usando a tecnologia NetApp FlexClone

  Uma licença FlexClone é necessária no sistema de armazenamento onde você deseja criar o clone.

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

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

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

Tipos de armazenamento suportados pelo SnapCenter Plug-in para PostgreSQL

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

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

Máquina	Tipo de armazenamento
VMware ESXi	• LUNs RDM conectados por um FC ou iSCSI ESXi HBAA varredura de adaptadores de barramento de host (HBAs) pode levar muito tempo para ser concluída 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** como 1 para verificar novamente apenas os HBAs listados em HBA_DRIVER_NAMES. • LUNs iSCSI conectados 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 vVol em NFS e SAN O armazenamento de dados vVol só pode ser provisionado com o ONTAP Tools para VMware vSphere.

Privilégios ONTAP mínimos necessários para o plug-in PostgreSQL

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

- Comandos de acesso total: privilégios mínimos necessários para ONTAP 9.12.1 e posterior
  - evento generate-autosupport-log
  - histórico de trabalho mostrar
  - parada de trabalho
  - lua
  - lun criar
  - lun criar
  - lun criar
  - lun delete
  - lun igroup adicionar
  - lun igroup criar

- lun igroup excluir
- renomear lun igroup
- renomear lun igroup
- show do lun igroup
- mapeamento lun add-reporting-nodes
- criação de mapeamento lun
- exclusão de mapeamento lun
- mapeamento lun remove-reporting-nodes
- show de mapeamento lunar
- lun modificar
- volume de entrada lun
- lua offline
- lua online
- lun persistente-reserva clara
- redimensionamento de lun
- série lun
- show de lua
- política de adição de regra do snapmirror
- regra de modificação de política do snapmirror
- política de remoção do snapmirror
- política do snapmirror mostrar
- restauração do snapmirror
- show de espelhos instantâneos
- histórico de exibição do snapmirror
- atualização do snapmirror
- atualização do snapmirror-ls-set
- lista-destinos do snapmirror
- versão
- criação de clone de volume
- show de clones de volume
- volume clone split start
- volume clone divisão parada
- volume criar
- destruição de volume
- clone de arquivo de volume criar
- arquivo de volume mostrar-uso-do-disco
- volume offline

    - volume on-line
    - modificação de volume
    - volume qtree criar
    - volume qtree delete
    - volume qtree modificar
    - volume qtree mostrar
    - restrição de volume
    - show de volume
    - criação de instantâneo de volume
    - exclusão de instantâneo de volume
    - modificação de instantâneo de volume
    - instantâneo de volume modificar-tempo-de-expiração-do-snaplock
    - renomeação de instantâneo de volume
    - restauração de instantâneo de volume
    - arquivo de restauração de instantâneo de volume
    - exibição de instantâneo de volume
    - desmontagem de volume
    - cifs do vserver
    - vserver cifs compartilhar criar
    - vserver cifs compartilhar excluir
    - vserver cifs shadowcopy mostrar
    - vserver cifs compartilhar mostrar
    - vserver cifs mostrar
    - política de exportação do vserver
    - criação de política de exportação do vserver
    - exclusão da política de exportação do vserver
    - criação de regra de política de exportação do vserver
    - mostrar regra de política de exportação do vserver
    - mostrar política de exportação do vserver
    - vserver iscsi
    - mostrar conexão iscsi do vserver
    - vserver mostrar
- Comandos somente leitura: privilégios mínimos necessários para ONTAP 8.3.0 e posterior
    - interface de rede
    - exibição de interface de rede
    - vserver

Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault para PostgreSQL

Você pode usar um plug-in 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 de disco para disco para conformidade com padrões e outros propósitos relacionados à governança. Antes de executar essas tarefas, você deve configurar um relacionamento de proteção de dados entre os volumes de origem e destino e inicializar o relacionamento.

O SnapCenter executa as atualizações no SnapMirror e no SnapVault após concluir a operação Snapshot. As atualizações do SnapMirror e do SnapVault são executadas como parte do trabalho do SnapCenter ; não crie uma programação ONTAP separada.

Se você estiver acessando o SnapCenter a partir de um produto NetApp SnapManager e estiver satisfeito com os relacionamentos de proteção de dados configurados, pode pular esta seção.

Um relacionamento de proteção de dados replica dados do armazenamento primário (o volume de origem) para o armazenamento secundário (o volume de destino). Quando você inicializa o relacionamento, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

O SnapCenter não oferece suporte a relacionamentos em cascata entre volumes SnapMirror e SnapVault (**Primário** > **Espelho** > **Cofre**). Você deve usar relacionamentos fanout.

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

Estratégia de backup para PostgreSQL

Definir uma estratégia de backup para PostgreSQL

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

Sobre esta tarefa

Um SLA define o nível de serviço esperado e aborda muitas questões relacionadas ao serviço, incluindo a disponibilidade e o desempenho do serviço. RTO é o tempo em que um processo de negócios deve ser restaurado após uma interrupção no serviço. O RPO define a estratégia para a idade dos arquivos que devem ser recuperados do armazenamento de backup para que as operações regulares sejam retomadas após uma falha. SLA, RTO e RPO contribuem para a estratégia de proteção de dados.

Passos

1. Determine quando você deve fazer backup dos seus recursos.
2. Decida quantos trabalhos de backup você precisa.
3. Decida como nomear seus backups.

4. Decida se você deseja criar uma política baseada em cópia de instantâneo para fazer backup de instantâneos consistentes com o aplicativo do cluster.
5. Decida se você deseja usar a tecnologia NetApp SnapMirror para replicação ou a tecnologia NetApp SnapVault para retenção de longo prazo.
6. Determine o período de retenção dos snapshots no sistema de armazenamento de origem e no destino do SnapMirror .
7. Determine se você deseja executar algum comando antes ou depois da operação de backup e forneça uma prescrição ou pós-escrito.

Descoberta automática de recursos no host Linux

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

Tipo de backups suportados

O tipo de backup especifica o tipo de backup que você deseja criar. O SnapCenter oferece suporte ao tipo de backup baseado em cópia de snapshot para clusters PostgreSQL.

Backup baseado em cópia instantânea

Os backups baseados em cópias de instantâneo aproveitam a tecnologia de instantâneo da NetApp para criar cópias on-line somente leitura dos volumes nos quais os clusters PostgreSQL residem.

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

Você pode usar o plug-in para criar instantâneos de grupos de consistência para grupos de recursos. Um grupo de consistência é um contêiner que pode abrigar vários volumes para que você possa gerenciá-los como uma única entidade. Um grupo de consistência é composto por instantâneos 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 **Relaxado**. Você também pode habilitar ou desabilitar a sincronização do Write Anywhere File Layout (WAFL) durante a operação consistente de snapshot de grupo. A sincronização do WAFL melhora o desempenho de um instantâneo de grupo de consistência.

Como o SnapCenter gerencia a manutenção de backups de dados

O SnapCenter gerencia a manutenção de backups de dados nos níveis do sistema de armazenamento e do sistema de arquivos.

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

Considerações para determinar agendamentos de backup para PostgreSQL

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

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

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

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

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

  Os agendamentos de backup fazem parte de uma configuração de recurso ou grupo de recursos. Por exemplo, se você tiver um grupo de recursos com uma política configurada para backups semanais, poderá configurar o agendamento para fazer backup todas as quintas-feiras às 22h.

Número de trabalhos de backup necessários para PostgreSQL

Os fatores que determinam o número de tarefas de backup necessárias 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 do Plug-in para PostgreSQL

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

O Snapshot usa a seguinte convenção de nomenclatura padrão:

```
resourcegroupname_hostname_timestamp
```

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

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

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

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

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

Estratégia de restauração e recuperação para PostgreSQL

Definir uma estratégia de restauração e recuperação para recursos do PostgreSQL

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

Somente a recuperação manual do cluster é suportada.

Passos

1. Determinar as estratégias de restauração suportadas para recursos PostgreSQL adicionados manualmente
2. Determinar 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 poder executar com sucesso operações de restauração usando o SnapCenter.

Não é possível recuperar recursos do 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 tirados 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.

OBSERVAÇÃO: O plug-in para PostgreSQL cria um backup_label e um tablespace_map na pasta */<OS_temp_folder>/postgresql_sc_recovery*<Restore_JobId>/_ para ajudar na recuperação manual.

Tipo de estratégia de restauração suportada para PostgreSQL descoberto automaticamente

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

A restauração completa de recursos é a estratégia de restauração suportada por 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 SnapCenter para PostgreSQL oferece suporte a Single File SnapRestore e tipos de restauração de conexão e cópia para clusters PostgreSQL descobertos automaticamente.

O Single File SnapRestore é executado em ambientes NFS para os seguintes cenários:

- Se apenas a opção **Recurso Completo** for selecionada
- Quando o backup selecionado for de um local secundário do SnapMirror ou SnapVault e a opção **Recurso Completo** for selecionada

O Single File SnapRestore é executado em ambientes SAN para os seguintes cenários:

- Se apenas a opção **Recurso Completo** for selecionada
- Quando o backup é selecionado de um local secundário do SnapMirror ou SnapVault e a opção **Recurso Completo** é selecionada

Tipos de operações de recuperação suportadas para clusters PostgreSQL

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

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

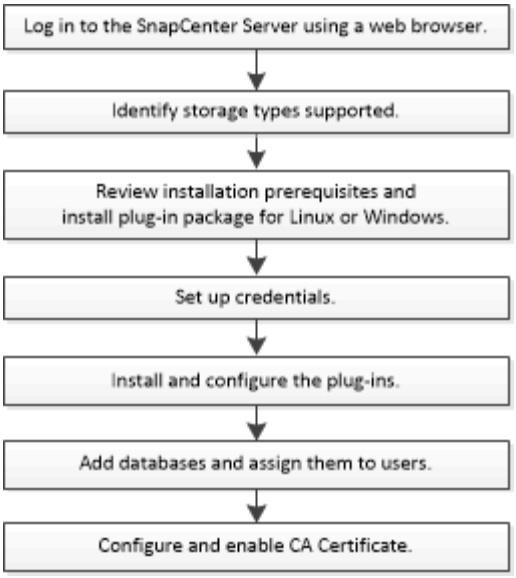
  Você deve especificar a data e a hora da recuperação.

O SnapCenter também oferece 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 SnapCenter Plug-in para PostgreSQL se quiser proteger clusters 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 concluir todos os requisitos. O plug-in SnapCenter para PostgreSQL está disponível em ambientes Windows e Linux.

- Você deve ter instalado o Java 11 no seu host.

  O IBM Java não é suportado em hosts Windows e Linux.

- No 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 Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host. O plug-in SnapCenter para Microsoft Windows será implantado por padrão com o plug-in PostgreSQL em hosts Windows.
- O SnapCenter Server deve ter acesso à porta 8145 ou personalizada do host Plug-in para PostgreSQL.

Hosts do Windows

- Você deve ter um usuário de domínio com privilégios de administrador local e permissões de login local no host remoto.
- Ao instalar o Plug-in para PostgreSQL em um host Windows, o SnapCenter Plug-in 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 no seu host Windows.

  "Baixe JAVA para todos os sistemas operacionais"

  "Ferramenta de Matriz de Interoperabilidade da 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 no seu host Linux.

  "Baixe JAVA para todos os sistemas operacionais"

  "Ferramenta de Matriz de Interoperabilidade da NetApp"

- Para clusters PostgreSQL em execução em um host Linux, ao instalar o Plug-in para PostgreSQL, o SnapCenter Plug-in para UNIX é instalado automaticamente.
- Você deve ter **bash** como o shell padrão para instalação de plug-ins.

Comandos suplementares

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

- Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Local 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 diferenciam maiúsculas de minúsculas. Certifique-se de especificar o caminho totalmente qualificado e coloque-o entre aspas (") se ele contiver espaços.

Por exemplo:

comando: mount comando: umount comando: "C:\Arquivos de Programas\ NetApp\SnapCreator commands\sdcli.exe" comando: myscript.bat

Se o arquivo *allowed_commands.config* não estiver presente, os comandos ou a execução do 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.

Configurar privilégios sudo para usuários não root para host Linux

O SnapCenter permite que um usuário não root instale o pacote de plug-ins do SnapCenter para Linux e inicie o processo de plug-in. Os processos do plug-in serão executados como um usuário não root efetivo. Você deve configurar privilégios sudo para que o usuário não root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.

- Se a umask for 0027, certifique-se de que a pasta java e todos os arquivos dentro dela tenham permissão de 555. Caso contrário, a instalação do plug-in poderá falhar.
- Para o usuário não root, certifique-se de que o nome do usuário não root e o nome do grupo do usuário sejam os mesmos.
- Edite o arquivo */etc/ssh/sshd_config* para configurar os algoritmos do código de autenticação de mensagens: MACs hmac-sha2-256 e MACs hmac-sha2-512.

  Reinicie o serviço sshd após 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 privilégios sudo para que o usuário não root forneça acesso aos seguintes caminhos:

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /localização_personalizada/ NetApp/snapcenter/spl/instalação/plugins/desinstalação
- /localização_personalizada/ NetApp/snapcenter/spl/bin/spl

Passos

1. Efetue 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 env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

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**, localizado em:

- _C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt _ se o SnapCenter Server estiver instalado no host Windows.
- _/opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ se o SnapCenter Server 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 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 e dimensionamento do sistema host.

Item	Requisitos
Sistemas Operacionais	Microsoft Windows Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .
RAM mínima para o plug-in SnapCenter no host	1 GB

Item	Requisitos
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	5 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	• Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) • PowerShell Core 7.4.2 Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" . Para obter informações específicas sobre solução de problemas do .NET, consulte "A atualização ou instalação do SnapCenter falha em sistemas legados que não têm conectividade com a Internet."

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

Antes de instalar o pacote de plug-ins 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 • Servidor SUSE Linux Enterprise (SLES) Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .
RAM mínima para o plug-in SnapCenter no host	1 GB

Item	Requisitos
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	2 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção 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, certifique-se de que a opção JAVA_HOME localizada em /var/opt/snapcenter/spl/etc/spl.properties esteja definida para a versão correta do JAVA e o caminho correto. Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Configurar 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 root ou para um usuário não root que tenha privilégios sudo para instalar e iniciar o processo do plug-in.

  Melhores práticas: embora você tenha permissão para criar credenciais para o Linux após implantar hosts e instalar plug-ins, a melhor prática é criar credenciais depois de adicionar SVMs, antes de implantar hosts e instalar plug-ins.

- Hosts do Windows

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

Você deve configurar as credenciais com privilégios 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 privilégios de administrador completos, será necessário atribuir pelo menos os privilégios de grupo de recursos e backup ao nome de usuário.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credencial**.
3. Clique em **Novo**.
4. Na página Credencial, especifique as informações necessárias para configurar as credenciais:

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

Para este campo…	Faça isso…
Nome de usuário	Digite o nome de usuário e a senha que serão usados para 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 em que você está instalando o plug-in SnapCenter . Os formatos válidos para o campo Nome de usuário são: ◦ *NetBIOS\Nome do Usuário* ◦ *FQDN do domínio\Nome do usuário* • Administrador local (somente para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local integrado no sistema em que você está instalando o plug-in SnapCenter . Você pode especificar uma conta de usuário local que pertença ao grupo de administradores locais se a conta de usuário tiver privilégios elevados ou se o recurso de Controle de Acesso do Usuário estiver desabilitado no sistema host. O formato válido para o campo Nome de usuário é: *UserName* Não use aspas duplas (") ou acento grave (`) nas senhas. Você não deve usar os símbolos de menor que (<) e exclamação (!) juntos em senhas. Por exemplo, menor que <! 10, menor que 10 <!, acento grave `12.
Senha	Digite a senha usada para autenticação.
Modo de autenticação	Selecione o modo de autenticação que você deseja usar.
Use privilégios sudo	Marque a caixa de seleção **Usar privilégios sudo** se estiver criando credenciais para um usuário não root. Aplicável somente a usuários do 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.

Configurar o gMSA no Windows Server 2016 ou posterior

O Windows Server 2016 ou posterior permite que você crie uma Conta de Serviço Gerenciada de grupo (gMSA) que fornece gerenciamento automatizado de senhas de contas de serviço a partir de uma conta de domínio gerenciada.

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 seja membro do domínio.

Passos

1. Crie uma chave raiz do KDS para gerar senhas exclusivas para cada objeto no seu gMSA.
2. Para cada domínio, execute o seguinte comando no 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,…>
.. Correr `Get-ADServiceAccount` comando para verificar a conta de
serviço.
```

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

   Para fazer isso, execute o seguinte comando no 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 seu host.

b. Instale o gMSA no seu host executando o seguinte comando no prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`

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

5. Atribua privilégios administrativos ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no SnapCenter Server.

   O SnapCenter Server 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.

Instalar o plug-in SnapCenter para PostgreSQL

Adicionar hosts e instalar pacotes de plug-ins 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 SnapCenter Server for o Windows 2019 e o sistema operacional do host do plug-in for o Windows 2022, você deverá executar o seguinte:
  - Atualize para o Windows Server 2019 (versão do sistema operacional 17763.5936) ou posterior
  - Atualize para o Windows Server 2022 (versão do sistema operacional 20348.2402) ou posterior
- Você deve ser um usuário atribuído a uma função que tenha permissões de instalação e desinstalação de plug-ins, como a função de administrador do SnapCenter .
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada

ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.

- 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 estiver usando uma conta de serviço gerenciada em grupo (gMSA), você deverá configurar a gMSA com privilégios administrativos.

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

Sobre esta tarefa

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

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Verifique se a aba **Hosts Gerenciados** está selecionada na parte superior.
3. Clique em **Adicionar**.
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 do cliente PostgreSQL, e esse host pode estar em um sistema Windows ou Linux.
Nome do host	Digite o nome do host de comunicação. Digite o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração correta do DNS. Portanto, a melhor prática é inserir o 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 visualizar detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial fornecida. 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 serem instalados.

   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	Mantenha o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o SnapCenter Server foi 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, deverá especificar a mesma porta. Caso contrário, a operação falhará.
Caminho de instalação	O plug-in para PostgreSQL é instalado no host do cliente PostgreSQL, e esse host pode estar em um sistema Windows ou Linux. • Para o pacote de plug-ins 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 SnapCenter para Linux, o caminho padrão é /opt/ NetApp/snapcenter. Opcionalmente, você pode personalizar o caminho.

Para este campo…	Faça isso…
Ignorar verificações de pré-instalação	Marque esta caixa de seleção se você já instalou os plug-ins manualmente e não deseja validar se o host atende aos requisitos para instalar o plug-in.
Adicionar todos os hosts no cluster	Marque esta caixa de seleção para adicionar todos os nós do cluster.
Use a conta de serviço gerenciada em grupo (gMSA) para executar os serviços do plug-in	Para o host Windows, marque esta caixa de seleção se desejar usar a Conta de Serviço Gerenciada em Grupo (gMSA) para executar os serviços do plug-in. Forneça o nome do gMSA no seguinte formato: domainName\accountName$. O gMSA será usado como uma conta de serviço de logon somente para o serviço SnapCenter Plug-in para Windows.

7. Clique em **Enviar**.

   Se você não tiver marcado a caixa de seleção Ignorar pré-verificações, o host será validado para verificar se ele 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 do Java (para plug-ins do Linux) são validados em relação aos requisitos mínimos. Se os requisitos mínimos não forem atendidos, mensagens de erro ou aviso apropriadas serão exibidas.

   Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado em C:\Arquivos de Programas\ NetApp\ SnapCenter WebApp para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deverá corrigir o problema.

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

8. Se o tipo de host for Linux, verifique a impressão digital e clique em **Confirmar e Enviar**.

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

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

9. Monitore o progresso da instalação.
   - Para o plug-in do Windows, os logs de instalação e atualização estão localizados em: *C:\Windows\ SnapCenter plugin\Install*<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_

Instalar pacotes de plug-in 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 do PowerShell.

Antes de começar

Você deve ter efetuado 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 SnapCenter Server, 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*. Alternativamente, você também pode consultar o "Guia de referência do 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 plug-in SnapCenter para cluster PostgreSQL usando a interface de usuário (IU) do SnapCenter . Se o seu ambiente não permitir a instalação remota do plug-in pela interface do usuário do SnapCenter , você poderá instalar o cluster do Plug-in para PostgreSQL no modo de 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 host Linux onde o cliente PostgreSQL reside.
- O host Linux no qual você está instalando o plug-in SnapCenter para cluster 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 da NetApp"

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

Passos

1. Copie o arquivo de instalação do pacote de plug-ins do SnapCenter para Linux (snapcenter_linux_host_plugin.bin) de C:\ProgramData\ NetApp\ SnapCenter\Package Repository para o host onde você deseja instalar o plug-in para PostgreSQL.

   Você pode acessar esse caminho a partir do host onde o SnapCenter Server 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 do SMCore.
   - -DSERVER_IP especifica o endereço IP do SnapCenter Server.
   - -DSERVER_HTTPS_PORT especifica a porta HTTPS do SnapCenter Server.
   - -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 /<diretório de instalação>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties e adicione o parâmetro PLUGINS_ENABLED = PostgreSQL:3.0.
5. Adicione o host ao SnapCenter Server 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*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Monitore o status da instalação do Plug-in para PostgreSQL

Você pode monitorar o progresso da instalação do pacote de plug-in SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento da instalação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos

- Na fila

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Trabalhos**, para filtrar a lista de modo que apenas as operações de instalação de plug-ins sejam listadas, faça o seguinte:
   a. Clique em **Filtrar**.
   b. Opcional: especifique a data de início e término.
   c. No menu suspenso Tipo, selecione **Instalação de 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 **Exibir registros**.

Configurar certificado CA

Gerar arquivo CSR de 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 o CSR gerado. O certificado terá uma chave privada associada a ele.

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

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

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

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

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

Importar certificados de CA

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

Passos

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover**

Snapin.

2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados – Computador local** > **Autoridades de certificação raiz confiáveis** > **Certificados**.
5. Clique com o botão direito do mouse na pasta “Autoridades de Certificação Raiz Confiáveis” 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 **Sim**, importe a chave privada e clique em **Avançar**.
Formato de arquivo de importação	Não faça alterações; clique em **Avançar**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluindo o Assistente de Importação de Certificados	Revise o resumo e clique em **Concluir** para iniciar a importação.

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

7. Repita a Etapa 5 para a pasta “Pessoal”.

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma sequência 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 **Impressão digital**.
   d. Copie os caracteres 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", após remover os espaços, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

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.

Configurar certificado CA com serviços de plug-in de host do Windows

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

Execute as seguintes etapas no SnapCenter Server e em todos os hosts de plug-in onde os certificados CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão 8145 do SMCore, 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"
   ```

Configurar o certificado CA para o serviço SnapCenter PostgreSQL Plug-ins no host Linux

Você deve gerenciar a senha do keystore do plug-in e seu certificado, configurar o certificado da CA, configurar certificados raiz ou intermediários para o trust-store do plug-in e configurar o par de chaves assinadas pela CA para o trust-store do plug-in com o serviço de plug-ins do SnapCenter para ativar o certificado digital instalado.

Os plug-ins usam o arquivo 'keystore.jks', que está localizado em */opt/ NetApp/snapcenter/scc/etc* como seu

armazenamento confiável e armazenamento de chaves.

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

Passos

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

   É o valor correspondente à chave 'KEYSTORE_PASS'.

2. Alterar a senha do keystore:

   ```
    keytool -storepasswd -keystore keystore.jks
   . Altere a senha de 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 após alterar a senha.

> A senha para o keystore do plug-in e para todas as senhas de alias associadas da chave privada deve ser a mesma.

Configurar certificados raiz ou intermediários para plug-in trust-store

Você deve configurar os certificados raiz ou intermediários sem a chave privada para conectar o trust-store.

Passos

1. Navegue até a pasta que contém o keystore do plug-in: /opt/ NetApp/snapcenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.
3. Listar 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 após configurar os certificados raiz ou
   intermediários para conectar o trust-store.
   ```

> Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

Configurar o par de chaves assinadas pela CA para plug-in trust-store

Você deve configurar o par de chaves assinadas pela CA para o trust-store do plug-in.

Passos

1. Navegue até a pasta que contém o keystore do plug-in /opt/ NetApp/snapcenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.
3. Listar 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. Listar os certificados adicionados no keystore.

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

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

   A senha padrão do keystore do plug-in 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 espaços
   ou caracteres 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 em relação à chave SCC_CERTIFICATE_ALIAS.

8. Reinicie o serviço após configurar o par de chaves assinadas pela CA para plug-in trust-store.

Configurar lista de revogação de certificados (CRL) para plug-ins

Sobre esta tarefa

- Os plug-ins do SnapCenter procurarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL dos plug-ins do SnapCenter é ' opt/ NetApp/snapcenter/scc/etc/crl'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo agent.properties em relação à chave CRL_PATH.

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

Configurar o certificado CA para o serviço SnapCenter PostgreSQL Plug-ins no host Windows

Você deve gerenciar a senha do keystore do plug-in e seu certificado, configurar o certificado da CA, configurar certificados raiz ou intermediários para o trust-store do plug-in e configurar o par de chaves assinadas pela CA para o trust-store do plug-in com o serviço de plug-ins do SnapCenter para ativar o certificado digital instalado.

Os plug-ins usam o arquivo *keystore.jks*, que está localizado em *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* como seu armazenamento confiável e armazenamento de chaves.

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

Passos

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

   É o valor correspondente à chave *KEYSTORE_PASS*.

2. Alterar 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 pelo seu caminho completo.

   C:\Arquivos de Programas\Java\<versão_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks

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

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

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

4. Reinicie o serviço após alterar a senha.

   > A senha para o keystore do plug-in e para todas as senhas de alias associadas da chave privada deve ser a mesma.

Configurar certificados raiz ou intermediários para plug-in trust-store

Você deve configurar os certificados raiz ou intermediários sem a chave privada para conectar o trust-store.

Passos

1. Navegue até a pasta que contém o keystore do plug-in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localize o arquivo 'keystore.jks'.
3. Listar 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 após configurar os certificados raiz ou intermediários para conectar o trust-store.

Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

Configurar o par de chaves assinadas pela CA para plug-in trust-store

Você deve configurar o par de chaves assinadas pela CA para o trust-store do plug-in.

Passos

1. Navegue até a pasta que contém o keystore do plug-in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localize o arquivo *keystore.jks*.
3. Listar 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. Listar os certificados adicionados no keystore.

   keytool -list -v -keystore keystore.jks

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

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

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

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

   Atualize este valor em relação à chave SCC_CERTIFICATE_ALIAS.

9. Reinicie o serviço após configurar o par de chaves assinadas pela CA para plug-in trust-store.

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

Sobre esta tarefa

- Para baixar o arquivo CRL mais recente para o certificado CA relacionado, consulte "Como atualizar o arquivo de lista de revogação de certificados no SnapCenter CA Certificate" .
- Os plug-ins do SnapCenter procurarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL dos plug-ins 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* em relação à chave CRL_PATH.
2. Você pode colocar mais de um arquivo CRL neste diretório.

   Os certificados recebidos serão verificados em relação a cada CRL.

Habilitar certificados CA para plug-ins

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

Antes de começar

- Você pode habilitar ou desabilitar os certificados da CA usando o cmdlet run *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando *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*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.
3. Selecione hosts de plug-in únicos ou múltiplos.
4. Clique em **Mais opções**.
5. Selecione **Ativar validação de certificado**.

Depois que você terminar

A guia Hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o SnapCenter Server e o host do plug-in.

- *  * indica que o certificado CA não está habilitado nem atribuído ao host do plug-in.
- *  * indica que o certificado CA foi validado com sucesso.
- *  * indica que o certificado 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 foram concluídas com sucesso.

Prepare-se para a proteção de dados

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

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

- Instalar e configurar o SnapCenter Server.
- Efetue login no SnapCenter Server.
- Configure o ambiente SnapCenter adicionando conexões do sistema de armazenamento e criando credenciais, se aplicável.
- Instale o Java 11 no seu host Linux ou Windows.

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

- Configure o SnapMirror e o SnapVault se desejar replicação de backup.

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

Antes de usar o SnapCenter, é útil entender os 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 dos quais você faz backup ou clona com o SnapCenter.
- Um grupo de recursos do SnapCenter é uma coleção de recursos em um host.

  Ao executar uma operação em um grupo de recursos, você executa essa operação nos recursos definidos no grupo de recursos de acordo com o cronograma especificado 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 agendados para recursos individuais e grupos de recursos.

- As políticas especificam a frequência de backup, replicação, scripts e outras características 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 ao executar um backup sob demanda para um único recurso.

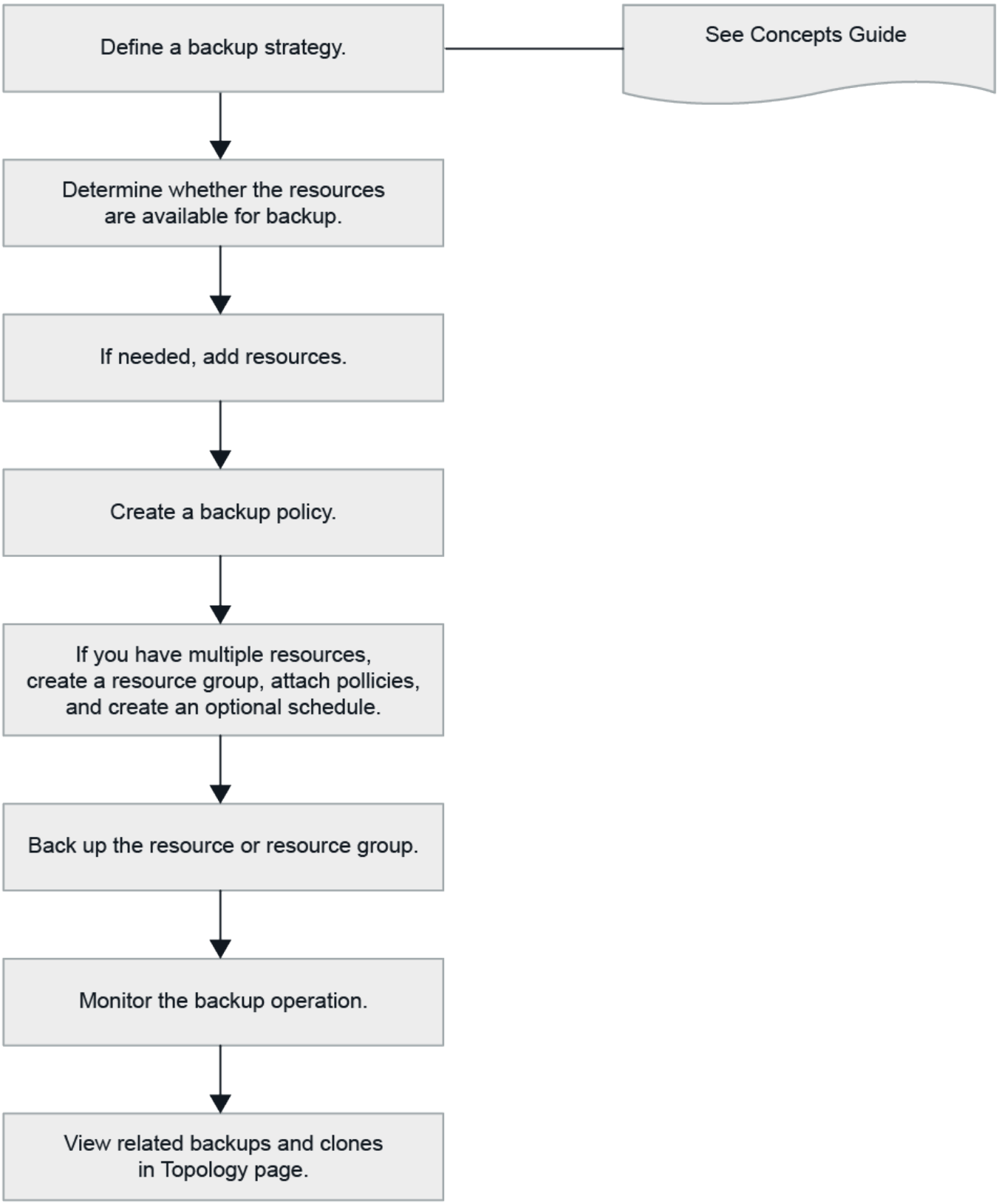
Pense em um grupo de recursos como algo que define o que você quer proteger e quando quer proteger em termos de dia e hora. Pense em uma política como a definição de como você deseja protegê-la. Se você estiver fazendo backup de todos os clusters, por exemplo, poderá criar um grupo de recursos que inclua todos os clusters no host. Você pode então anexar duas políticas ao grupo de recursos: uma política diária e uma política horária. Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup completo diariamente.

Fazer backup dos recursos do PostgreSQL

Fazer 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 de clusters para backup, gerenciamento de políticas de backup, criação de grupos de recursos e anexação de políticas, criação de backups e monitoramento das operações.

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



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

Descubra os clusters automaticamente

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

Antes de começar

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

Sobre esta tarefa

- Após instalar o plug-in, todos os clusters naquele host Linux são descobertos automaticamente e exibidos na página Recursos.
- Somente clusters são descobertos automaticamente.

Os recursos descobertos automaticamente não podem ser modificados ou excluídos.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** 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, em seguida, selecione o nome do host.

   Você pode então clicar em * * para fechar o painel de filtro.

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

   Os recursos são exibidos junto 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, Não protegido será exibido na coluna Status geral.
   - Se o cluster estiver em um sistema de armazenamento NetApp e protegido, e se nenhuma operação de backup for realizada, Backup não executado será exibido na coluna Status geral. Caso contrário, o status mudará para Falha no backup ou Backup bem-sucedido com base no último status do backup.

Você deve atualizar os recursos se os clusters forem renomeados fora do SnapCenter.

Adicionar recursos manualmente ao host do plug-in

A descoberta 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 SnapCenter Server, adicionar hosts e configurar conexões do sistema de armazenamento.

Sobre esta tarefa

A descoberta automática não é suportada para as seguintes configurações:

- Layouts RDM e VMDK

Passos

1. No painel de navegação esquerdo, selecione o SnapCenter Plug-in para Postgresql na lista suspensa e clique em **Recursos**.
2. Na página Recursos, clique em **Adicionar recursos do 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	Digite o nome do host.
Tipo	Selecione o cluster.
Exemplo	Especifique o nome da instância, que é o pai do cluster.
Credenciais	Selecione as credenciais ou adicione informações para a credencial. Isto é opcional.

4. Na página Fornecer espaço 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 chave-valor personalizados para o plug-in PostgreSQL
6. Revise o resumo e clique em **Concluir**.

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

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

"Adicionar um usuário ou grupo e atribuir função e ativos"

Depois que você 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.

- Ao modificar os recursos adicionados manualmente que são migrados do SnapCenter 5.0 ou anterior, faça o seguinte na página **Configurações de recursos** para pares de valores-chave personalizados:
  - Especifique o termo "PORT" no campo **Nome**.
  - Especifique o número da porta no campo **Valor**.

Criar políticas de backup para PostgreSQL

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

Antes de começar

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

  Além disso, você pode especificar 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 'Manter as cópias de backup por um número específico de dias' for selecionada, o período de retenção do SnapLock deverá ser menor ou igual aos dias de retenção mencionados.
  - Especificar um período de bloqueio de instantâneo impede a exclusão dos instantâneos até que o período de retenção expire. Isso pode levar à retenção de um número maior de instantâneos do que a contagem especificada na política.
  - Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Políticas**.
3. Clique em **Novo**.
4. Na página Nome, insira o nome e os detalhes da política.
5. Na página Tipo de política, faça o seguinte:
   a. Selecione o tipo de armazenamento.
   b. Na seção **Configurações de backup personalizadas**, forneça quaisquer configurações de backup específicas que devem ser passadas ao plug-in no formato chave-valor.

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

6. Na página Backup e Replicação, execute as seguintes ações:

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

      Você pode especificar o agendamento (data de início, data de término e frequência) para a operação de backup ao criar um grupo de recursos. Isso permite que você crie grupos de recursos que compartilham a mesma política e frequência de backup, mas também permite que você atribua diferentes agendamentos de backup a cada política.

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

   a. Na seção Configurações de instantâneo, especifique as configurações de retenção para o tipo de backup e o tipo de agendamento selecionado na página **Tipo de backup**:

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

Se você quiser…	Então…
Período de bloqueio de cópia de instantâneo	Selecione **Período de bloqueio de cópia de instantâneo** e especifique dias, meses ou anos. O período de retenção do SnapLock deve ser inferior a 100 anos.

7. Selecione um rótulo de política.

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

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

Para este campo…	Faça isso…
Atualize o SnapMirror após criar uma cópia local do Snapshot	Selecione este campo para criar cópias espelhadas dos conjuntos de backup em outro volume (replicação SnapMirror). Se o relacionamento de proteção no ONTAP for do tipo Mirror and Vault e se você selecionar apenas esta opção, o Snapshot criado no primário não será transferido para o destino, mas será listado no destino. Se este Snapshot for selecionado no destino para executar uma operação de restauração, a seguinte mensagem de erro será exibida: O local secundário não está disponível para o backup em cofre/espelho selecionado. Durante a replicação secundária, o tempo de expiração do SnapLock carrega o tempo de expiração do SnapLock primário. Clicar no botão **Atualizar** na página Topologia atualiza o tempo de expiração do SnapLock secundário e primário que são recuperados do ONTAP. Ver "Visualize backups e clones relacionados a recursos do PostgreSQL na página Topologia" .

Para este campo…	Faça isso…
Atualize o SnapVault após criar uma cópia local do Snapshot	Selecione esta opção para executar a replicação de backup de disco para disco (backups do SnapVault). Durante a replicação secundária, o tempo de expiração do SnapLock carrega o tempo de expiração do SnapLock primário. Clicar no botão **Atualizar** na página Topologia atualiza o tempo de expiração do SnapLock secundário e primário que são recuperados do ONTAP. Quando o SnapLock é configurado somente no secundário do ONTAP conhecido como SnapLock Vault, clicar no botão **Atualizar** na página Topologia atualiza o período de bloqueio no secundário recuperado do ONTAP. Para obter mais informações sobre o SnapLock Vault, consulte Confirmar instantâneos para WORM em um destino de cofre Ver "Visualize backups e clones relacionados a recursos do PostgreSQL na página Topologia" .
Erro na contagem de novas tentativas	Insira o número máximo de tentativas de replicação que podem ser permitidas antes que a operação seja interrompida.

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

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

Crie grupos de recursos e anexe políticas

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

Sobre esta tarefa

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

Passos

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

Para este campo…	Faça isso…
Nome	Insira um nome para o grupo de recursos.  O nome do grupo de recursos não deve exceder 250 caracteres.
Etiquetas	Insira um ou mais rótulos que ajudarão você a pesquisar posteriormente o grupo de recursos. Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.
Use formato de nome personalizado para cópia de instantâneo	Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do instantâneo. Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um registro de data e 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 **Tipo de recurso**.

   Isso ajuda a filtrar informações na tela.

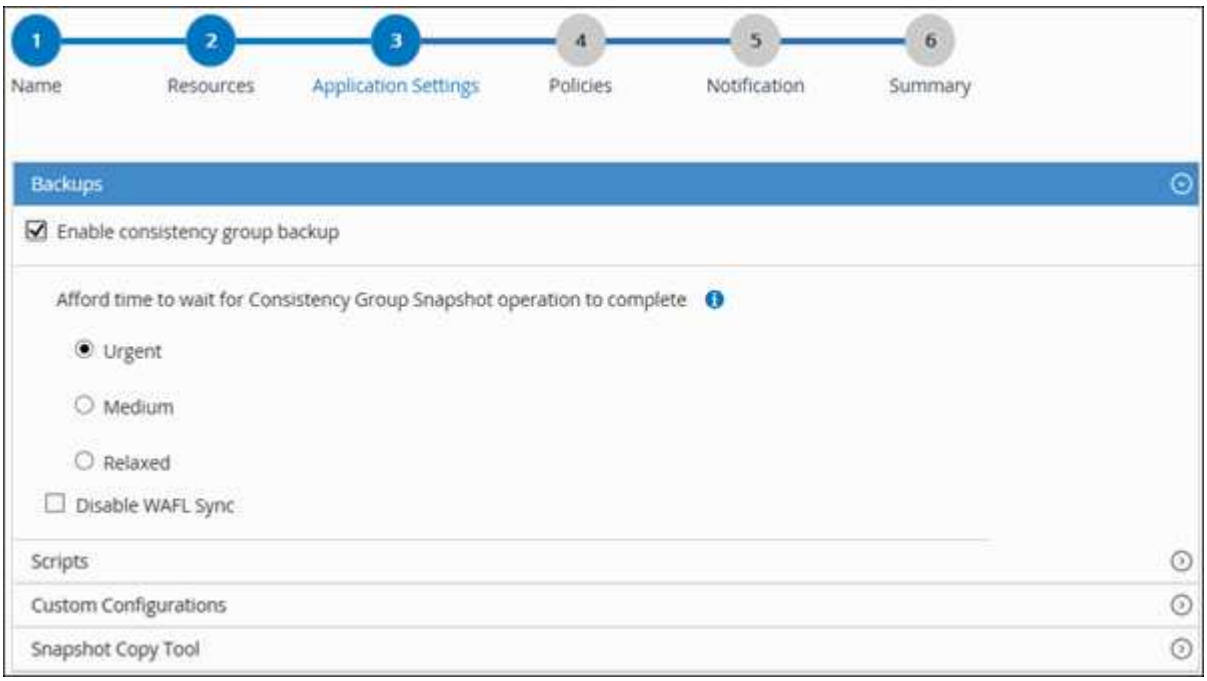
5. Selecione os recursos na seção **Recursos disponíveis** e clique na seta para a direita para movê-los para a seção **Recursos selecionados**.
6. Na página Configurações do aplicativo, faça o seguinte:

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

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

Para este campo…	Faça isso…
Permitir tempo para esperar a conclusão da operação de instantâneo do Consistency Group	Selecione **Urgente**, **Médio** ou **Relaxado** para especificar o tempo de espera para a conclusão da operação de instantâneo. Urgente = 5 segundos, Médio = 7 segundos e Relaxado = 20 segundos.

Para este campo…	Faça isso…
Desativar 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 de inatividade, snapshot e unquiesce. Você também pode inserir os pré-comandos a serem executados antes de sair em caso de falha.

b. Clique na seta **Configurações personalizadas** e insira os pares de chave-valor personalizados necessários para todas as operações de proteção de dados que usam este recurso.

Parâmetro	Contexto	Descrição
HABILITAR_REGISTRO_DE_ARQUIVO	(S/N)	Permite que o gerenciamento de log de arquivamento exclua os logs de arquivamento.
RETENÇÃO_DE_REGISTRO_DE_ARQUIVO	número_de_dias	Especifica o número de dias que os logs de arquivamento são retidos. Esta configuração deve ser igual ou maior que NTAP_SNAPSHOT_RETENTIONS.
DIRETÓRIO_DE_LOG_DE_ARQUIVO	change_info_directory/logs	Especifica o caminho para o diretório que contém os logs de arquivamento.

Parâmetro	Contexto	Descrição
EXT_DE_LOG_DE_ARQUIVO	extensão_de_arquivo	Especifica o comprimento da extensão do arquivo de log de arquivamento. Por exemplo, se o log de arquivamento 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.
ARQUIVO_LOG_RECURSIVO_ SE ARQUIVO	(S/N)	Permite o gerenciamento de logs de arquivo dentro de subdiretórios. Você deve usar este parâmetro se os logs de arquivamento estiverem localizados em subdiretórios.

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

c. Clique na seta **Ferramenta de Cópia de Instantâneo** 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, esta opção não é aplicável.	Selecione * SnapCenter com consistência do sistema de arquivos*.
SnapCenter para criar um instantâneo de nível de armazenamento	Selecione * SnapCenter sem consistência do sistema de arquivos*.
Para inserir o comando a ser executado no host para criar cópias de instantâneos.	Selecione **Outro** e insira o comando a ser executado no host para criar um instantâneo.

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 agendamentos para políticas selecionadas.

b. Na coluna Configurar agendamentos, clique em * + * para a política que você deseja configurar.

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

   Onde policy_name é o nome da política que você selecionou.

   Os agendamentos configurados são listados na coluna **Agendamentos Aplicados**.

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

8. Na página 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 **Concluir**.

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

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

Antes de começar

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

Sobre esta tarefa

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

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:
   a. Insira um nome para o grupo de recursos no campo Nome.

      O nome do grupo de recursos não deve exceder 250 caracteres.

   b. Insira um ou mais rótulos no campo Tag para ajudar você a pesquisar o grupo de recursos posteriormente.

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

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

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

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

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

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

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

5. Selecione os recursos do ASA r2 na seção Recursos disponíveis e mova-os para a seção Recursos selecionados.
6. Na página Configurações do aplicativo, selecione a opção de backup.
7. Na página Políticas, execute as seguintes etapas:

a. Selecione uma ou mais políticas na lista suspensa.

Você também pode criar uma política clicando em + .

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

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

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

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

Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

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

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

a. Selecione o tipo de política de replicação.

A política de replicação síncrona não é suportada.

b. Especifique o sufixo do grupo de consistência que você deseja usar.

c. Nos menus suspensos Cluster de destino e SVM de destino, selecione o cluster emparelhado e o SVM que você deseja usar.

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

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

1. Na página Verificação, execute as seguintes etapas:

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

   b. Clique + na coluna Configurar agendamentos para configurar o agendamento de verificação para todos os tipos de agendamento da política.

   c. Na caixa de diálogo Adicionar agendamentos de verificação policy_name, execute as seguintes ações:

Se você quiser…	Faça isso…
Executar verificação após o backup	Selecione **Executar verificação após backup**.
Agendar uma verificação	Selecione **Executar verificação agendada** e depois selecione o tipo de agendamento na lista suspensa.

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

   e. Clique em **OK**.

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

2. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação realizada no grupo de recursos, selecione **Anexar relatório de trabalho**.

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

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

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 de administrador de infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estejam em andamento.

  As instalações do plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento porque 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 dos sistemas de armazenamento devem ser exclusivos.

  O SnapCenter não oferece suporte a vários sistemas de armazenamento com o mesmo nome em clusters diferentes. Cada sistema de armazenamento suportado pelo SnapCenter deve ter um nome exclusivo e um endereço IP 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 SnapCenter Server.

```
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: “C:\Arquivos de Programas\IBM\SQLLIB\BIN”

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

Fazer backup do PostgreSQL

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

Antes de começar

- Você deve ter criado uma política de backup.
- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.
- Para a operação de backup baseada em cópia de instantâneo, certifique-se de que todos os clusters de locatários sejam válidos e ativos.
- Para comandos pré e pós para operações de inatividade, instantâneo e retomada de atividade, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

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

Interface do usuário do SnapCenter

Passos

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

   Selecione * * e selecione o nome do host e o tipo de recurso para filtrar os recursos. Você pode então selecionar para fechar o painel de filtro.
3. Selecione o recurso que você deseja fazer backup.
4. Na página Recurso, selecione **Usar formato de nome personalizado para cópia do Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

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

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

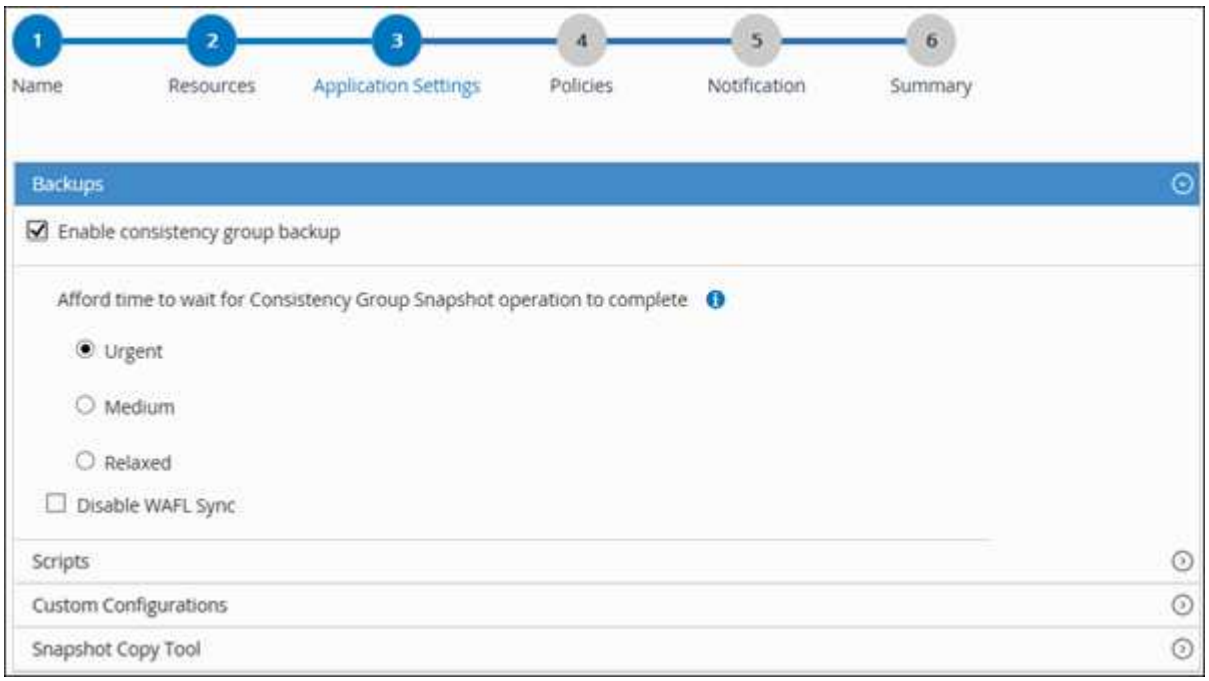
Para este campo…	Faça isso…
Permitir tempo para esperar a conclusão da operação "Consistency Group Snapshot"	Selecione **Urgente**, ou **Médio**, ou **Relaxado** para especificar o tempo de espera para a operação de Snapshot terminar. Urgente = 5 segundos, Médio = 7 segundos e Relaxado = 20 segundos.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

   - Selecione a seta **Scripts** para executar comandos pré e pós para operações de inatividade, instantâneo e ativação/desativação.

     Você também pode executar pré-comandos antes de sair da operação de backup. Prescrições e pós-escritos são executados no SnapCenter Server.
   - Selecione a seta **Configurações personalizadas** e insira os pares de valores personalizados necessários para todos os trabalhos que usam este recurso.
   - Selecione a seta **Ferramenta de Cópia de Instantâneo** para selecionar a ferramenta para criar Instantâneos:

Se você quiser…	Então…
SnapCenter para criar um Snapshot de nível de armazenamento	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 Snapshot	Selecione * SnapCenter com consistência do sistema de arquivos*.
Para inserir o comando para criar um Snapshot	Selecione **Outro** e insira o comando para criar um Snapshot.



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 agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

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

   c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e selecione **OK**.

      policy_name é o nome da política que você selecionou.

   Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

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

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

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

   A página de topologia de recursos é exibida.

9. Selecione **Fazer backup 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. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.
    - Nas configurações do MetroCluster , o SnapCenter pode não conseguir detectar um relacionamento de proteção após um failover.

      Para mais informações, consulte: "Não é possível detectar o relacionamento SnapMirror ou SnapVault após failover do MetroCluster"

    - Se você estiver fazendo backup de dados do aplicativo em VMDKs e o tamanho do heap Java para o SnapCenter Plug-in for VMware vSphere não for grande o suficiente, o backup poderá falhar.

      Para aumentar o tamanho do heap Java, localize o arquivo de script */opt/netapp/init_scripts/scvservice*. Nesse 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 SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

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

   O prompt de nome de usuário e senha é exibido.

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 do trabalho (em execução, concluído ou com falha) usando o cmdlet Get-smJobSummaryReport.

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

7. Monitore os detalhes do trabalho de backup, como ID do backup, nome do backup para executar a operação de restauração ou clonagem 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*. Alternativamente, você também pode consultar o "Guia de referência do 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 um relacionamento SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.

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 um agendamento configurado, os backups ocorrerão automaticamente de acordo com o agendamento.

Passos

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

   Você pode pesquisar o grupo de recursos inserindo o nome do grupo de recursos na caixa de pesquisa ou selecionando e, em seguida, selecionando a tag. Você pode então 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. Monitore o progresso da operação selecionando **Monitor** > **Trabalhos**.

Monitorar operações de backup do PostgreSQL

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

Sobre esta tarefa

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

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

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

a. Clique para filtrar a lista de modo que somente as operações de backup sejam listadas.
b. Especifique as datas de início e término.
c. Na lista suspensa **Tipo**, selecione **Backup**.
d. No menu suspenso **Status**, selecione o status do backup.
e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.

4. Selecione uma tarefa de backup e clique em **Detalhes** para visualizar os detalhes da tarefa.

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

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

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

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

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

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

Passos

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

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

Cancelar operações de backup para PostgreSQL

Você pode cancelar operações de backup que estão na fila.

O que você vai precisar

- Você deve estar conectado como administrador do SnapCenter ou proprietário do trabalho para cancelar operações.
- Você pode cancelar uma operação de backup na página **Monitor** ou no painel **Atividade**.
- Não é possível cancelar uma operação de backup em execução.
- Você pode usar a GUI do SnapCenter , os cmdlets do PowerShell ou os comandos da CLI para cancelar as operações de backup.
- O botão **Cancelar trabalho** fica desabilitado para operações que não podem ser canceladas.
- Se você selecionou **Todos os membros desta função podem ver e operar em objetos de outros membros** na página Usuários\Grupos ao criar uma função, você pode cancelar as operações de backup enfileiradas de outros membros enquanto estiver usando essa função.

Passos

1. Execute uma das seguintes ações:

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 de atividades	a. Após iniciar a operação de backup, clique em * * no painel Atividade para visualizar as cinco operações mais recentes. b. Selecione a operação. c. Na página Detalhes do trabalho, clique em **Cancelar trabalho**.

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

Visualizar backups e clones do PostgreSQL na página Topologia

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

Sobre esta tarefa

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

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

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

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

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

Passos

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

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

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

   A seção **Cartão de resumo** exibe o número total de backups baseados em cópias de instantâneo e clones.

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

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

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

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

5. Na exibição Gerenciar cópias, clique em **Backups** ou **Clones** do armazenamento primário ou secundário para ver detalhes de um backup ou clone.

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

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

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

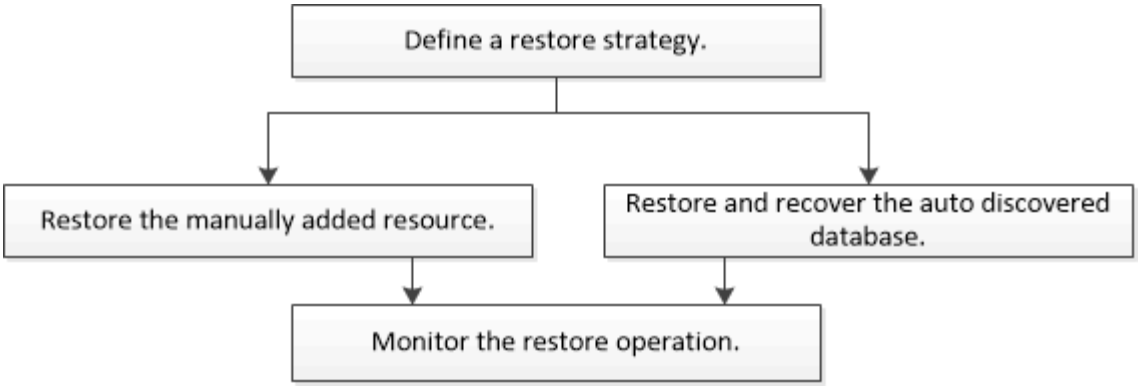
7. Se você quiser excluir um clone, selecione o clone na tabela e clique em .
8. Se você quiser dividir um clone, selecione o clone na tabela e clique em .

Restaurar PostgreSQL

Fluxo de trabalho de restauração

O fluxo de trabalho de restauração e recuperação inclui planejamento, execução de 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 clonagem. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre os cmdlets do PowerShell.

"Guia de referência do cmdlet do software SnapCenter" .

Restaurar e recuperar um backup de recurso 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 do recurso ou dos grupos de recursos.
- Você deve ter cancelado qualquer operação de backup que esteja em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos de pré-restauração, pós-restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Local 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 o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Interface do usuário do SnapCenter

Passos

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

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

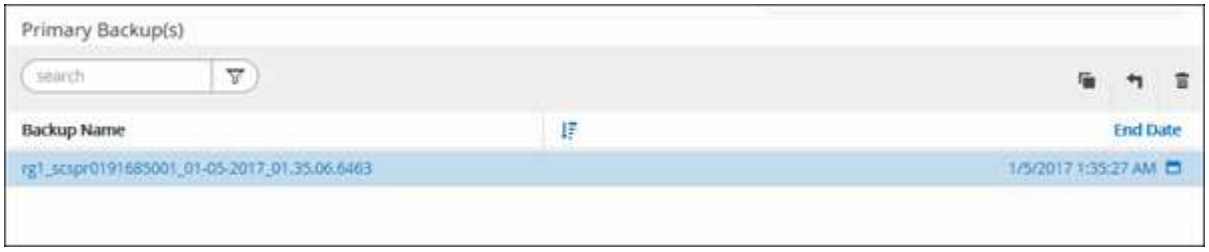
   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

   Se o recurso não estiver protegido, “Não protegido” será exibido na coluna Status geral. Isso pode significar que o recurso não está protegido ou que o backup do recurso foi feito por um usuário diferente.

3. Selecione o recurso ou selecione um grupo de recursos e depois selecione um recurso nesse grupo.

   A página de topologia de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Na tabela Backup(s) primário(s), selecione o backup que deseja restaurar e clique em * * .



6. Na página Escopo de restauração, selecione **Recurso completo**.

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

      Se o recurso contiver volumes ou qtrees, os Snapshots tirados após o Snapshot 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.

      Você pode selecionar vários LUNs.

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

7. Na página Pré-operações, insira os comandos pre restore e unmount para executar antes de realizar 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 realizar

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

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server 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 29 de janeiro de 2015 a 3 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 os 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*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Restaurar e recuperar 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 do recurso ou dos grupos de recursos.
- Você deve ter cancelado qualquer operação de backup que esteja em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos de pré-restauração, pós-restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-*

in Creator\etc\allowed_commands.config

- Local 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

- Cópias de backup baseadas em arquivo não podem ser restauradas do SnapCenter.
- Para recursos descobertos automaticamente, a restauração é suportada com SFSR.
- A recuperação automática não é suportada.
- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

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

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

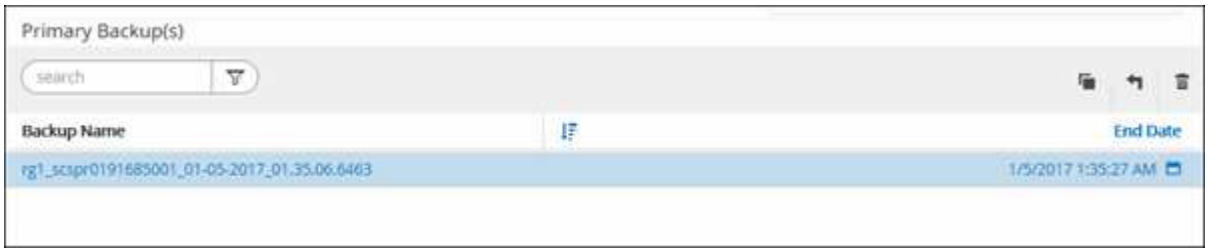
   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

   Se o recurso não estiver protegido, “Não protegido” será exibido na coluna Status geral. Isso pode significar que o recurso não está protegido ou que o backup do recurso foi feito por um usuário diferente.

3. Selecione o recurso ou selecione um grupo de recursos e depois selecione um recurso nesse grupo.

   A página de topologia de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Na tabela Backup(s) primário(s), selecione o backup que deseja restaurar e clique em * * .



6. Na página Escopo de restauração, selecione **Recurso completo** para restaurar os volumes de dados configurados do cluster PostgreSQL.
7. Na página Escopo de recuperação, selecione uma das seguintes opções:

Se você…	Faça isso…

Quer recuperar o mais próximo possível do tempo atual	Selecione **Recuperar para o estado mais recente**. Para recursos de contêiner único, especifique um ou mais locais de backup de log e catálogo.
Deseja recuperar até o ponto especificado no tempo	Selecione **Recuperar para um ponto no tempo**. a. Insira a data e a hora. Insira 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 quiser executar uma recuperação para 5h da manhã em Sunnyvale, CA, o usuário deverá definir o fuso horário do navegador para o fuso horário do host Linux PostgreSQL, que é GMT-07:00 e especificar a data e a hora como 5h da manhã.
Não quero recuperar	Selecione **Sem recuperação**.

Não é possível recuperar recursos do PostgreSQL adicionados manualmente.

O plug-in SnapCenter para PostgreSQL cria um backup_label e um tablespace_map na pasta */<OS_temp_folder>/postgresql_sc_recovery*<Restore_JobId>/_ para ajudar na recuperação manual.

1. Na página Pré-operações, insira os comandos pre restore e unmount para executar antes de realizar 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 realizar 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 **Concluir**.
5. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Restaurar recursos usando cmdlets do PowerShell

Restaurar um backup de recursos inclui iniciar uma sessão de conexão com o SnapCenter Server, listar os backups e recuperar informações de backup, além de

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 SnapCenter Server 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 29 de janeiro de 2015 a 3 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 os 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*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Monitorar operações de restauração do PostgreSQL

Você pode monitorar o progresso de diferentes operações de restauração do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum 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 tomar.

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento

- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de restauração sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Restaurar**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Aplicar** para visualizar as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

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

Clonar backups de recursos do PostgreSQL

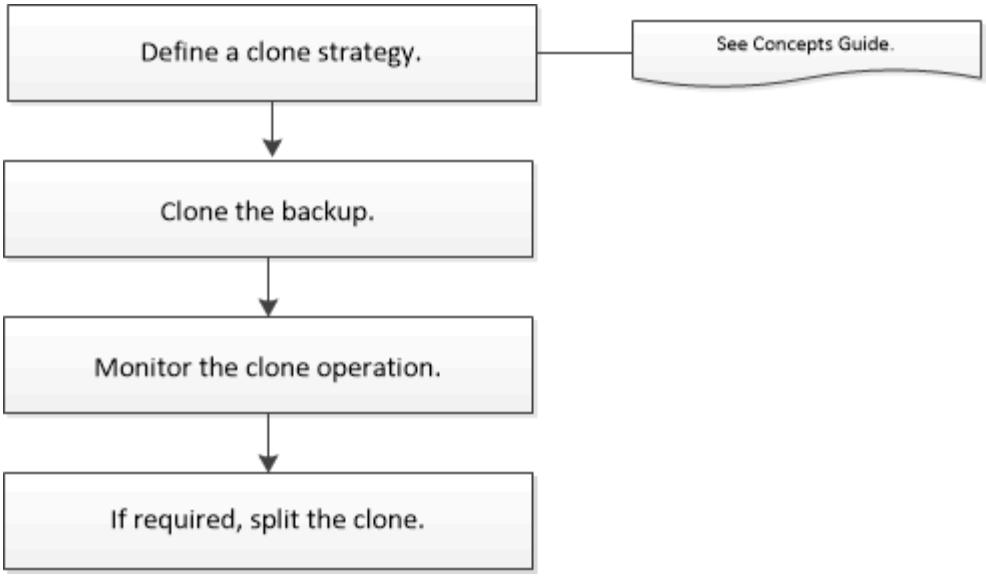
Fluxo de trabalho de clonagem

O fluxo de trabalho de clonagem inclui executar a operação de clonagem e monitorar a 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 do aplicativo
  - 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 de clonagem:



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

Clonar um backup do PostgreSQL

Você pode usar o SnapCenter para clonar um backup. Você pode clonar a partir 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 armazenamento (SVM).
- Para comandos de pré-clonagem ou pós-clonagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Local 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 as operações de divisão de volume do FlexClone , consultehttps://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html["Dividir um volume FlexClone de seu volume pai"] .
- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Interface do usuário do SnapCenter

Passos

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

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

3. Selecione o recurso ou grupo de recursos.

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

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

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Selecione o backup de dados da 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.
Porto de destino	Insira a porta de destino do PostgreSQL a ser clonada a partir dos backups existentes.
Endereço IP de exportação NFS	Insira os endereços IP ou os nomes de host nos quais os volumes clonados serão exportados. Isso é aplicável somente ao recurso do tipo de armazenamento NFS.
Pool de Capacidade Máxima Taxa de Transferência (MiB/s)	Insira a taxa de transferência máxima de um pool de capacidade. Isso é aplicável somente ao recurso do tipo de armazenamento ANF.

7. Na página Scripts, execute as seguintes etapas:

   Os scripts são executados no host do plug-in.

   a. Insira os comandos para pré-clonagem ou pós-clonagem que devem ser executados antes ou depois da operação de clonagem, respectivamente.
      - Comando pré-clone: exclui clusters existentes com o mesmo nome
      - Comando pós-clone: verificar um cluster ou iniciar um cluster.
   b. Digite o comando mount para montar um sistema de arquivos em um host.

Comando de montagem 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 **Concluir**.
10. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Cmdlets do PowerShell

Passos

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

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

2. Recupere os backups para executar a operação de clonagem 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 clonagem a partir de um backup existente e especifique os endereços IP de exportação do NFS nos quais os volumes clonados serão exportados.

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

   Para 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 do clone.

4. Verifique se os backups foram clonados com sucesso usando o cmdlet Get-SmCloneReport para visualizar os detalhes do trabalho de clonagem.

   Você pode visualizar 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          :
```

Monitorar operações de clonagem do PostgreSQL

Você pode monitorar o progresso das operações de clonagem do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente operações de clonagem sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.
4. Selecione o trabalho de clonagem e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página Detalhes do trabalho, clique em **Exibir registros**.

Dividir um clone

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

Sobre esta tarefa

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

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

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

- Quando você divide um clone, as cópias de backup e os trabalhos de clonagem do clone são excluídos.
- Para obter informações sobre as operações de divisão de volume do FlexClone , consulte "Dividir um volume FlexClone de seu volume pai" .
- Certifique-se de que o volume ou agregado no sistema de armazenamento esteja online.

Passos

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

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

Opção	Descrição
Para aplicações 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 de recursos é exibida.

4. Na 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 será dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
6. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

   A operação de divisão do clone para de responder se o serviço SMCore for reiniciado. Você deve executar o cmdlet Stop-SmJob para interromper a operação de divisão de clone e, em seguida, tentar novamente a operação de divisão de clone.

   Se você quiser um tempo de pesquisa maior 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 o SMCore pesquisar o status da operação de divisão do clone. O valor está em milissegundos e o valor padrão é 5 minutos.

   Por exemplo:

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

   A operação de início da divisão do clone falha se um backup, uma restauração ou outra divisão do clone estiver em andamento. Você deve reiniciar a operação de divisão do clone somente após a conclusão das operações em execução.

Informações relacionadas

"O clone ou a verificação do SnapCenter falham com o agregado inexistente"

Excluir ou dividir clones de cluster do PostgreSQL após atualizar o SnapCenter

Após atualizar para o SnapCenter 4.3, você não verá mais os clones. Você pode excluir o clone ou dividir os clones na página Topologia do recurso a partir do qual os clones foram criados.

Sobre esta tarefa

Se você quiser localizar a pegada 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-smprotectresource.
4. Selecione o recurso pai na página Recursos.

   A página de topologia de recursos é exibida.

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

Informações sobre direitos autorais

Informações sobre marcas comerciais