Proteja os sistemas de arquivos Unix

SnapCenter software

NetApp
November 06, 2025

Índice

Proteja os sistemas de arquivos Unix

O que você pode fazer com o plug-in SnapCenter para sistemas de arquivos Unix

Quando o Plug-in para sistemas de arquivos Unix estiver instalado em seu ambiente, você poderá usar o SnapCenter para fazer backup, restaurar e clonar sistemas de arquivos Unix. Você também pode executar tarefas de suporte a essas operações.

- Descubra recursos
- Fazer backup de sistemas de arquivos Unix
- Agendar operações de backup
- Restaurar backups do sistema de arquivos
- Backups do sistema de arquivos clone
- Monitore operações de backup, restauração e clonagem

Configurações suportadas

Item	Configuração suportada
Ambientes	• Servidor físico • Servidor virtual Datastores vVol em NFS e SAN. O datastore vVol só pode ser provisionado com o ONTAP Tools para VMware vSphere.
Sistemas operacionais	• Red Hat Enterprise Linux • Oracle Linux • Servidor SUSE Linux Enterprise (SLES)
Sistemas de arquivos	• SAN: ◦ Sistemas de arquivos baseados em LVM e não baseados em LVM ◦ LVM sobre VMDK ext3, ext4 e xfs • NFS: NFS v3, NFS v4.x
Protocolos	• FC • FCoE • iSCSI • NFS

Item	Configuração suportada
Multicaminho	sim

Limitações

- A combinação de RDMs e discos virtuais em um grupo de volumes não é suportada.
- A restauração em nível de arquivo não é suportada.

  No entanto, você pode executar manualmente a restauração no nível do arquivo clonando o backup e depois copiando os arquivos manualmente.

- A mistura de sistemas de arquivos distribuídos entre VMDKs provenientes de armazenamentos de dados NFS e VMFS não é suportada.
- NVMe não é suportado.
- O provisionamento não é suportado.

Características

- Permite que o plug-in para Oracle Database execute operações de proteção de dados em bancos de dados Oracle, manipulando a pilha de armazenamento do host subjacente em sistemas Linux ou AIX
- Suporta protocolos de Network File System (NFS) e de rede de área de armazenamento (SAN) em um sistema de armazenamento que esteja executando o ONTAP.
- Para sistemas Linux, os bancos de dados Oracle em LUNs VMDK e RDM são suportados quando você implanta o SnapCenter Plug-in for VMware vSphere e registra o plug-in com o SnapCenter.
- Suporta Mount Guard para AIX em sistemas de arquivos SAN e layout LVM.
- Suporta Enhanced Journaled File System (JFS2) com registro em linha em sistemas de arquivos SAN e layout LVM somente para sistemas AIX.

  Dispositivos nativos SAN, sistemas de arquivos e layouts LVM criados em dispositivos SAN são suportados.

- Automatiza operações de backup, restauração e clonagem com reconhecimento de aplicativo para sistemas de arquivos UNIX em seu ambiente SnapCenter

Instalar o plug-in SnapCenter para sistemas de arquivos Unix

Pré-requisitos para adicionar hosts e instalar o pacote de plug-ins para Linux

Antes de adicionar um host e instalar o pacote de plug-ins para Linux, você deve atender a todos os requisitos.

- Se você estiver usando iSCSI, o serviço iSCSI deverá estar em execução.
- Você pode usar a autenticação baseada em senha para o usuário root ou não root ou a autenticação baseada em chave SSH.

  O plug-in SnapCenter para sistemas de arquivos Unix pode ser instalado por um usuário não root. No

entanto, você deve configurar os privilégios sudo para que o usuário não root instale e inicie o processo do plug-in. Após instalar o plug-in, os processos serão executados como um usuário não root.

- Crie credenciais com modo de autenticação como Linux para o usuário de instalação.
- Você deve ter instalado o Java 11 no seu host Linux.

  Certifique-se de ter instalado apenas a edição certificada do JAVA 11 no host Linux.

  Para obter informações sobre como baixar o JAVA, consulte: "Downloads Java para todos os sistemas operacionais"

- Você deve ter **bash** como o shell padrão para instalação de plug-ins.

Requisitos do host Linux

Você deve garantir que o host atenda aos requisitos antes de instalar o Pacote de plug-ins do SnapCenter para Linux.

Item	Requisitos
Sistemas operacionais	• Red Hat Enterprise Linux • Oracle Linux • Servidor SUSE Linux Enterprise (SLES)
RAM mínima para o plug-in SnapCenter no host	2 GB
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.

Item	Requisitos
Pacotes de software necessários	Java 11 Oracle Java e OpenJDK Certifique-se de ter instalado apenas a edição certificada do JAVA 11 no host Linux. 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" .

Adicionar hosts e instalar o pacote de plug-ins para Linux usando a GUI

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

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 **Linux** como o tipo de host.
Nome do host	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. Se você estiver adicionando um host usando o SnapCenter e o host fizer parte de um subdomínio, você deverá fornecer 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 que você especificou. 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 **Sistemas de arquivos Unix**.
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 caminho padrão é */opt/ NetApp/snapcenter*. Opcionalmente, você pode personalizar o caminho. Se você usar o caminho personalizado, certifique-se de que o conteúdo padrão dos sudoers seja atualizado com o caminho personalizado.
Ignorar verificações de pré-instalação opcionais	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.

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 instalar o plug-in.

> O script de pré-verificação não valida o status do firewall da porta do plug-in se ele estiver especificado nas regras de rejeição do firewall.

Mensagens de erro ou aviso apropriadas serão exibidas se os requisitos mínimos não forem atendidos. Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado em *C:\Program Files\ 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. Verifique a impressão digital e clique em **Confirmar e Enviar**.

> O SnapCenter não suporta o algoritmo ECDSA.

> 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.

   Os arquivos de log específicos da instalação estão localizados em */custom_location/snapcenter/logs*.

Resultado

Todos os sistemas de arquivos montados no host são descobertos automaticamente e exibidos na Página de Recursos. Se nada for exibido, clique em **Atualizar recursos**.

Monitorar o status da instalação

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 o serviço SnapCenter Plug-in Loader

O serviço SnapCenter Plug-in Loader carrega o pacote de plug-in para Linux interagir com o SnapCenter Server. O serviço SnapCenter Plug-in Loader é instalado quando você instala o SnapCenter Plug-ins Package para Linux.

Sobre esta tarefa

Após instalar o pacote de plug-ins do SnapCenter para Linux, o serviço SnapCenter Plug-in Loader é iniciado automaticamente. Se o serviço SnapCenter Plug-in Loader não iniciar automaticamente, você deve:

- Certifique-se de que o diretório onde o plug-in está operando não seja excluído
- Aumentar o espaço de memória alocado à Máquina Virtual Java

O arquivo spl.properties, localizado em */custom_location/ NetApp/snapcenter/spl/etc/*, contém os seguintes parâmetros. Valores padrão são atribuídos a esses parâmetros.

Nome do parâmetro	Descrição
NÍVEL_LOG	Exibe os níveis de log suportados. Os valores possíveis são TRACE, DEBUG, INFO, WARN, ERROR e FATAL.
PROTOCOLO_SPL	Exibe o protocolo suportado pelo SnapCenter Plug-in Loader. Somente o protocolo HTTPS é suportado. Você pode adicionar o valor se o valor padrão estiver faltando.
PROTOCOLO_DO_SERVIDOR_SNAPCENTER	Exibe o protocolo suportado pelo SnapCenter Server. Somente o protocolo HTTPS é suportado. Você pode adicionar o valor se o valor padrão estiver faltando.

Nome do parâmetro	Descrição
PULAR_ATUALIZAÇÃO_JAVAHOME	Por padrão, o serviço SPL detecta o caminho Java e atualiza o parâmetro JAVA_HOME. Portanto, o valor padrão é definido como FALSE. Você pode definir como TRUE se quiser desabilitar o comportamento padrão e corrigir manualmente o caminho Java.
SPL_KEYSTORE_SENHA	Exibe a senha do arquivo keystore. Você só poderá alterar esse valor se alterar a senha ou criar um novo arquivo de keystore.
PORTA SPL	Exibe o número da porta na qual o serviço SnapCenter Plug-in Loader está em execução. Você pode adicionar o valor se o valor padrão estiver faltando. Você não deve alterar o valor após instalar os plug-ins.
SNAPCENTER_SERVER_HOST	Exibe o endereço IP ou nome do host do SnapCenter Server.
CAMINHO_DE_KEYSTORE_SPL	Exibe o caminho absoluto do arquivo keystore.
PORTA_DO_SERVIDOR_SNAPCENTER	Exibe o número da porta na qual o SnapCenter Server está sendo executado.
CONTAGEM_MÁXIMA_DE_LOGS	Exibe o número de arquivos de log do SnapCenter Plug-in Loader que são retidos na pasta */custom_location/snapcenter/spl/logs*. O valor padrão é definido como 5000. Se a contagem for maior que o valor especificado, os últimos 5000 arquivos modificados serão retidos. A verificação do número de arquivos é feita automaticamente a cada 24 horas a partir do momento em que o serviço SnapCenter Plug-in Loader é iniciado. Se você excluir manualmente o arquivo spl.properties, o número de arquivos a serem retidos será definido como 9999.

Nome do parâmetro	Descrição
JAVA_HOME	Exibe o caminho absoluto do diretório do JAVA_HOME que é usado para iniciar o serviço SPL. Este caminho é determinado durante a instalação e como parte do início do SPL.
TAMANHO_MÁXIMO_DE_LOG	Exibe o tamanho máximo do arquivo de log do trabalho. Quando o tamanho máximo é atingido, o arquivo de log é compactado e os logs são gravados no novo arquivo daquele trabalho.
RETER_REGISTROS_DOS_ÚLTIMOS_DIAS	Exibe o número de dias até os quais os logs são retidos.
HABILITAR_VALIDAÇÃO_DE_CERTIFICADO	Exibe verdadeiro quando a validação do certificado CA está habilitada para o host. Você pode habilitar ou desabilitar esse parâmetro editando o spl.properties ou usando a GUI ou o cmdlet do SnapCenter .

Se algum desses parâmetros não estiver atribuído ao valor padrão ou se você quiser atribuir ou alterar o valor, você poderá modificar o arquivo spl.properties. Você também pode verificar o arquivo spl.properties e editá-lo para solucionar quaisquer problemas relacionados aos valores atribuídos aos parâmetros. Depois de modificar o arquivo spl.properties, você deve reiniciar o serviço SnapCenter Plug-in Loader .

Passos

1. Execute uma das seguintes ações, conforme necessário:
   - Inicie o serviço SnapCenter Plug-in Loader :
     - Como usuário root, execute: `/custom_location/NetApp/snapcenter/spl/bin/spl start`
     - Como usuário não root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
   - Pare o serviço SnapCenter Plug-in Loader :
     - Como usuário root, execute: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
     - Como usuário não root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

     > Você pode usar a opção -force com o comando stop para interromper o serviço SnapCenter Plug-in Loader à força. No entanto, você deve ter cuidado antes de fazer isso, pois isso também encerra as operações existentes.

   - Reinicie o serviço SnapCenter Plug-in Loader :

- Como usuário root, execute: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
- Como usuário não root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`

◦ Encontre o status do serviço SnapCenter Plug-in Loader :

- Como usuário root, execute: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
- Como usuário não root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`

◦ Encontre a alteração no serviço SnapCenter Plug-in Loader :

- Como usuário root, execute: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
- Como usuário não root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Configurar certificado CA com o serviço SnapCenter Plug-in Loader (SPL) no host Linux

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

O SPL usa o arquivo 'keystore.jks', que está localizado em '/var/opt/snapcenter/spl/etc' como seu armazenamento confiável e armazenamento de chaves.

Gerenciar senha para keystore SPL e alias do par de chaves assinadas pela CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore SPL a partir do arquivo de propriedades SPL.

   É o valor correspondente à chave 'SPL_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>" -keystore keystore.jks
```

   Atualize o mesmo para a chave SPL_KEYSTORE_PASS no arquivo spl.properties.

3. Reinicie o serviço após alterar a senha.

A senha para o keystore SPL e para todas as senhas de alias associadas da chave privada deve ser a mesma.

Configurar certificados raiz ou intermediários para armazenamento confiável SPL

Você deve configurar os certificados raiz ou intermediários sem a chave privada para o armazenamento confiável SPL.

Passos

1. Navegue até a pasta que contém o keystore SPL: */var/opt/snapcenter/spl/etc*.
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

```
 keytool -list -v -keystore keystore.jks
. Adicione um certificado raiz ou intermediário:
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Reinicie o serviço após configurar os certificados raiz ou
intermediários para o armazenamento confiável SPL.
```

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

Configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL

Você deve configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL.

Passos

1. Navegue até a pasta que contém o keystore do SPL /var/opt/snapcenter/spl/etc.
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

```
 keytool -list -v -keystore keystore.jks
. Adicione o certificado da CA com chave privada e pública.
```

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Listar os certificados adicionados no keystore.
```

```
 keytool -list -v -keystore keystore.jks
. Verifique se o keystore contém o alias correspondente ao novo
certificado CA, que foi adicionado ao keystore.
. Altere a senha da chave privada adicionada para o certificado CA para
a senha do keystore.
```

A senha padrão do keystore SPL é o valor da chave SPL_KEYSTORE_PASS no arquivo spl.properties.

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -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 "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configure o nome do alias do keystore localizado no arquivo
spl.properties.
```

Atualize este valor em relação à chave SPL_CERTIFICATE_ALIAS.

4. Reinicie o serviço após configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL.

Configurar lista de revogação de certificados (CRL) para SPL

Você deve configurar o CRL para SPL

Sobre esta tarefa

- O SPL procurará os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL do SPL é */var/opt/snapcenter/spl/etc/crl*.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo spl.properties com a chave SPL_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.

Instalar o SnapCenter Plug-in for VMware vSphere

Se seu banco de dados ou sistema de arquivos estiver armazenado em máquinas virtuais (VMs), ou se você quiser proteger VMs e armazenamentos de dados, será necessário implantar o SnapCenter Plug-in for VMware vSphere .

Para obter informações sobre como implantar, consulte "Visão geral da implantação" .

Implantar certificado CA

Para configurar o Certificado CA com o SnapCenter Plug-in for VMware vSphere, consulte "Criar ou importar certificado SSL" .

Configurar o arquivo CRL

O SnapCenter Plug-in for VMware vSphere procura os arquivos CRL em um diretório pré-configurado. O diretório padrão dos arquivos CRL do SnapCenter Plug-in for VMware vSphere é */opt/netapp/config/crl*.

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

Prepare-se para proteger sistemas de arquivos Unix

Antes de executar qualquer operação de proteção de dados, como operações de backup, clonagem ou restauração, você deve configurar seu ambiente. Você também pode configurar o SnapCenter Server para usar a tecnologia SnapMirror e SnapVault .

Para aproveitar a tecnologia SnapVault e SnapMirror , você deve configurar e inicializar um relacionamento de proteção de dados entre os volumes de origem e destino no dispositivo de armazenamento. Você pode usar o NetAppSystem Manager ou usar a linha de comando do console de armazenamento para executar essas tarefas.

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

- Instalar e configurar o SnapCenter Server."Saber mais"
- Configure o ambiente SnapCenter adicionando conexões do sistema de armazenamento."Saber mais"

> O SnapCenter não oferece suporte a várias SVMs com o mesmo nome em clusters diferentes. Cada SVM registrado no SnapCenter usando registro de SVM ou registro de cluster deve ser exclusivo.

- Adicione hosts, instale os plug-ins e descubra os recursos.
- Se você estiver usando o SnapCenter Server para proteger sistemas de arquivos Unix que residem em LUNs ou VMDKs do VMware RDM, será necessário implantar o SnapCenter Plug-in for VMware vSphere e registrar o plug-in no SnapCenter.
- Instale o Java no seu host Linux.
- Configure o SnapMirror e o SnapVault no ONTAP, se desejar replicação de backup.

Fazer backup de sistemas de arquivos Unix

Descubra os sistemas de arquivos UNIX disponíveis para backup

Após instalar o plug-in, todos os sistemas de arquivos naquele host são descobertos automaticamente e exibidos na página Recursos. Você pode adicionar esses sistemas de arquivos a grupos de recursos para executar operações de proteção de dados.

Antes de começar

- Você deve ter concluído tarefas como instalar o SnapCenter Server, adicionar hosts e criar conexões do sistema de armazenamento.
- Se os sistemas de arquivos residirem em um disco de máquina virtual (VMDK) ou mapeamento de dispositivo bruto (RDM), você deverá implantar o SnapCenter Plug-in for VMware vSphere e registrar o

plug-in com o SnapCenter.

Para obter mais informações, consulte "Implantar o SnapCenter Plug-in for VMware vSphere" .

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Caminho** na lista Exibir.
3. Clique em **Atualizar recursos**.

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

Crie políticas de backup para sistemas de arquivos Unix

Antes de usar o SnapCenter para fazer backup de sistemas de arquivos Unix, você deve criar uma política de backup para o recurso ou grupo de recursos do qual deseja fazer backup. Uma política de backup é um conjunto de regras que regem como você gerencia, agenda e mantém backups. Você também pode especificar as configurações de replicação, script e tipo de backup. Criar uma política economiza tempo quando você deseja reutilizá-la em outro recurso ou grupo de recursos.

Antes de começar

- Você deve ter se preparado para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, descobrir os sistemas de arquivos e criar conexões do sistema de armazenamento.
- Se você estiver replicando Snapshots para um espelho ou armazenamento secundário de cofre, o administrador do SnapCenter deverá ter atribuído as SVMs a você para os volumes de origem e destino.
- Revise os pré-requisitos e limitações específicos da sincronização ativa do SnapMirror . Para obter informações, consulte "Limites de objetos para sincronização ativa do SnapMirror" .

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 Snapshot impede a exclusão dos Snapshots até que o período de retenção expire. Isso pode levar à retenção de um número maior de Snapshots do que a contagem especificada na política.

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

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Políticas**.
3. Selecione **Sistemas de arquivos Unix** na lista suspensa.
4. Clique em **Novo**.

5. Na página Nome, insira o nome e os detalhes da política.
6. Na página Backup e Replicação, execute as seguintes ações:

    a. Especifique as configurações de backup.

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

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

Para este campo…	**Faça isso…**
Atualizar 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). Esta opção deve ser habilitada para sincronização ativa do SnapMirror .
Atualizar 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).
Contagem de novas tentativas de erro	Insira o número máximo de tentativas de replicação que podem ser permitidas antes que a operação seja interrompida.

7. Na página Retenção, especifique as configurações de retenção para o tipo de backup e o tipo de agendamento selecionado na página Backup e Replicação:

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. 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 subjacente do ONTAP . 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.
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.
Período de bloqueio de cópia de instantâneo	Selecione **Período de bloqueio de cópia de instantâneo** e especifique a duração em dias, meses ou anos. O período de retenção do Snaplock deve ser inferior a 100 anos.

8. Selecione o rótulo da política.

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

9. Na página Script, insira o caminho e os argumentos do prescript ou postscript que você deseja executar antes ou depois da operação de backup, respectivamente.

   Você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in no caminho _ /opt/ NetApp/snapcenter/scc/etc/allowed_commands.config_.

   Você também pode especificar o valor do tempo limite do script. O valor padrão é 60 segundos.

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

Crie grupos de recursos e anexe políticas para sistemas de arquivos Unix

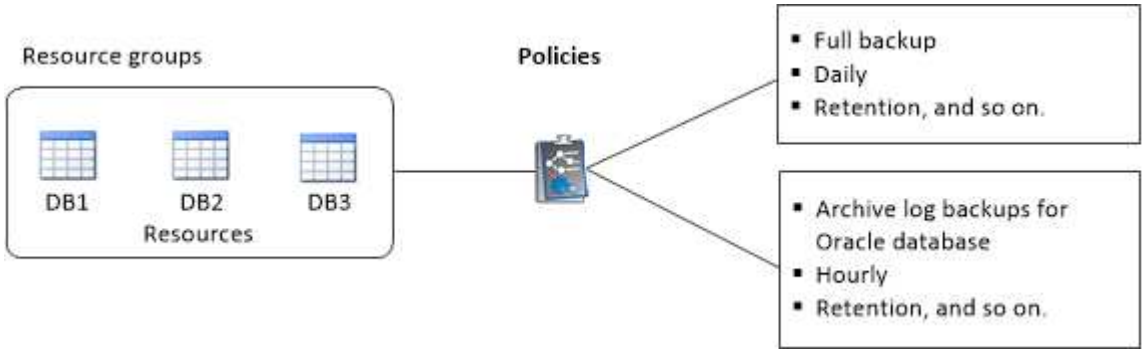
Um grupo de recursos é um contêiner onde você adiciona recursos que deseja fazer backup e proteger. Um grupo de recursos permite que você faça backup de todos os dados associados aos sistemas de arquivos.

Sobre esta tarefa

- Um banco de dados com arquivos em grupos de discos ASM deve estar no estado "MONT" ou "OPEN" para verificar seus backups usando o utilitário Oracle DBVERIFY.

  Anexe uma ou mais políticas ao grupo de recursos para definir o tipo de trabalho de proteção de dados que você deseja executar.

  A imagem a seguir ilustra o relacionamento entre recursos, grupos de recursos e políticas para bancos de dados:



- Para políticas habilitadas para SnapLock , para ONTAP 9.12.1 e versões anteriores, se você especificar um período de bloqueio de Snapshot, os clones criados a partir de Snapshots à prova de violação como parte da restauração herdarão o tempo de expiração do SnapLock . O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .
- Não há suporte para adicionar novos sistemas de arquivos sem sincronização ativa do SnapMirror a um grupo de recursos existente que contém recursos com sincronização ativa do SnapMirror .
- Não há suporte para adicionar novos sistemas de arquivos a um grupo de recursos existente no modo de failover da sincronização ativa do SnapMirror . Você pode adicionar recursos ao grupo de recursos somente no estado regular ou de failback.

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 a 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.

4. Na página Recursos, selecione um nome de host de sistemas de arquivos Unix 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 da seção Recursos Disponíveis e mova-os para a seção Recursos Selecionados.
6. Na página Configurações do aplicativo, faça o seguinte:
   - Selecione a seta Scripts e insira os comandos pre e post para operações de inatividade, instantâneo e ativação/desativação. Você também pode inserir os pré-comandos a serem executados antes de sair em caso de falha.
   - Selecione uma das opções de consistência de backup:
     - Selecione **Consistência do sistema de arquivos** se quiser garantir que os dados armazenados em cache do sistema de arquivos sejam liberados antes de criar o backup e que nenhuma operação de entrada ou saída seja permitida no sistema de arquivos durante a criação do backup.

       Para consistência do sistema de arquivos, serão tirados instantâneos do grupo de consistência para LUNs envolvidos no grupo de volumes.

     - Selecione **Crash Consistent** se quiser garantir que os dados armazenados em cache do sistema de arquivos sejam limpos antes de criar o backup.

       Se você tiver adicionado diferentes sistemas de arquivos no grupo de recursos, todos os volumes de diferentes sistemas de arquivos no grupo de recursos serão colocados em um grupo de Consistência.

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. 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.

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

Crie grupos de recursos e habilite proteção secundária para sistemas de arquivos Unix 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**.

Fazer backup de sistemas de arquivos Unix

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

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e o plug-in apropriado na lista.
2. Na página Recursos, selecione **Caminho** na lista Exibir.
3. Clique e, em seguida, selecione o nome do host e os sistemas de arquivos Unix para filtrar os recursos.
4. Selecione o sistema de arquivos do qual você deseja fazer backup.
5. Na página Recursos, você pode executar as seguintes etapas:
   a. Marque a caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

      Por exemplo, `customtext_policy_hostname` ou `resource_hostname` . Um registro de data e hora é anexado ao nome do Snapshot por padrão.

6. Na página Configurações do aplicativo, faça o seguinte:
   - Selecione a seta Scripts e insira os comandos pre e post para operações de inatividade, instantâneo e ativação/desativação. Você também pode inserir os pré-comandos a serem executados antes de sair em caso de falha.
   - Selecione uma das opções de consistência de backup:
     - Selecione **Consistência do sistema de arquivos** se quiser garantir que os dados armazenados em cache do sistema de arquivos sejam liberados antes de criar o backup e que nenhuma operação seja executada no sistema de arquivos durante a criação do backup.
     - Selecione **Crash Consistent** se quiser garantir que os dados armazenados em cache do sistema de arquivos sejam limpos antes de criar o backup.
7. Na página Políticas, execute as seguintes etapas:
   a. Selecione uma ou mais políticas na lista suspensa.

      Você pode criar uma política clicando em .

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

   b. Clique na coluna Configurar agendamentos para configurar um agendamento para a política desejada.
   c. Na janela 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.

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

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

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

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

   A página de topologia é exibida.

10. Clique em **Fazer backup agora**.
11. 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. Clique em **Backup**.
12. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Fazer backup de grupos de recursos de sistemas de arquivos Unix

Você pode fazer backup dos sistemas de arquivos Unix definidos no grupo de recursos. Você pode fazer backup de um grupo de recursos sob demanda na página Recursos. Se um grupo de recursos tiver uma política anexada e um agendamento configurado, os backups serão criados de acordo com o agendamento.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e o plug-in apropriado na lista.
2. Na página Recursos, selecione **Grupo de recursos** na lista **Exibir**.
3. Digite o nome do grupo de recursos na caixa de pesquisa ou clique em e selecione a tag.

   Clique para fechar o painel de filtro.

4. Na página Grupo de recursos, selecione o grupo de recursos para fazer backup.
5. Na página Backup, execute as seguintes etapas:
    a. Se você tiver várias políticas associadas ao grupo de recursos, selecione a política de backup que deseja usar na lista suspensa **Política**.

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

    b. Selecione **Backup**.
6. Monitore o progresso selecionando **Monitorar > Trabalhos**.

Monitorar backup de sistemas de arquivos Unix

Aprenda a monitorar o progresso das operações de backup e proteção de dados.

Monitorar operações de backup de sistemas de arquivos Unix

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 as operações de proteção de dados 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**.

Exibir sistemas de arquivos Unix protegidos na página Topologia

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

Sobre esta tarefa

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

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.

Se você tiver um relacionamento secundário como sincronização ativa do SnapMirror (inicialmente lançado como SnapMirror Business Continuity [SM-BC]), poderá ver os seguintes ícones adicionais:

-  O site de réplica está no ar.
-  O site de réplicas está fora do ar.
-  O espelho secundário ou o relacionamento do cofre não foram restabelecidos.

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 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 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 sistema de arquivos 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.

   Para sincronização ativa do SnapMirror , clicar no botão **Atualizar** atualiza o inventário de backup do SnapCenter consultando o ONTAP para sites primários e de réplica. Uma programação semanal também executa essa atividade para todos os bancos de dados que contêm o relacionamento de sincronização ativo do SnapMirror .

   - Para sincronização ativa do SnapMirror e somente para o ONTAP 9.14.1, os relacionamentos Async Mirror ou Async MirrorVault com o novo destino primário devem ser configurados manualmente após o failover. A partir do ONTAP 9.15.1, o Async Mirror ou o Async MirrorVault são configurados automaticamente para o novo destino principal.
   - Após o failover, um backup deve ser criado para que o SnapCenter esteja ciente do failover. Você pode clicar em **Atualizar** somente após um backup ter sido criado.
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 .

Exemplo mostrando backups e clones no armazenamento primário

Restaurar e recuperar sistemas de arquivos Unix

Restaurar sistemas de arquivos Unix

Em caso de perda de dados, você pode usar o SnapCenter para restaurar sistemas de arquivos Unix.

Sobre esta tarefa

- Você deve executar os seguintes comandos para estabelecer a conexão com o SnapCenter Server, listar os backups, recuperar suas informações e restaurar o backup.

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

- Para a operação de restauração de sincronização ativa do SnapMirror , você deve selecionar o backup do local principal.

Passos

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

A página de topologia é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou replicado).
5. Selecione o backup da tabela e clique em *  *.
6. Na página Escopo de restauração:
   - Para sistemas de arquivos NFS, por padrão, a restauração **Conectar e Copiar** é selecionada. Você também pode selecionar **Reverter Volume** ou **Restauração Rápida**.
   - Para sistemas de arquivos não NFS, o escopo de restauração é selecionado dependendo do layout.

     Os novos arquivos criados após o backup podem não estar disponíveis após a restauração, dependendo do tipo e do layout do sistema de arquivos.
7. Na página PreOps, insira comandos de pré-restauração a serem executados antes de executar um trabalho de restauração.
8. Na página PostOps, insira comandos de pós-restauração a serem executados após a execução de um trabalho de restauração.

   Você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in no local */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config* path.
9. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar as notificações por e-mail.

   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 de restauração realizada, selecione **Anexar relatório de tarefa**.

   Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.
10. Revise o resumo e clique em **Concluir**.

    Se a operação de restauração falhar, a reversão não será suportada.

    Em caso de restauração de um sistema de arquivos residente em um grupo de volumes, o conteúdo antigo no sistema de arquivos não é excluído. Somente o conteúdo do sistema de arquivos clonado será copiado para o sistema de arquivos de origem. Isso é aplicável quando há vários sistemas de arquivos no grupo de volumes e restaurações do sistema de arquivos NFS padrão.
11. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Monitorar operações de restauração de sistemas de arquivos Unix

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 sistemas de arquivos Unix

Clonar backup do sistema de arquivos Unix

Você pode usar o SnapCenter para clonar o sistema de arquivos Unix usando o backup do sistema de arquivos.

Antes de começar

- Você pode pular a atualização do arquivo fstab definindo o valor de *SKIP_FSTAB_UPDATE* como **true** no arquivo *agent.properties* localizado em */opt/ NetApp/snapcenter/scc/etc*.
- Você pode ter um nome de volume clone estático e um caminho de junção definindo o valor de *USE_CUSTOM_CLONE_VOLUME_NAME_FORMAT* como **true** no arquivo *agent.properties* localizado em */opt/ NetApp/snapcenter/scc/etc*. Após atualizar o arquivo, você deve reiniciar o serviço do criador do plug-in SnapCenter executando o comando: `/opt/NetApp/snapcenter/scc/bin/scc restart` .

  Exemplo: Sem essa propriedade, o nome do volume clone e o caminho da junção serão como <Source_volume_name>_Clone_<Timestamp>, mas agora serão

<Source_volume_name>_Clone_<Clone_Name>

Isso mantém o nome constante para que você possa manter o arquivo fstab atualizado manualmente, caso não prefira atualizar o fstab pelo SnapCenter.

Passos

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

   A página de topologia é exibida.

4. Na exibição Gerenciar cópias, selecione os backups entre Cópias locais (primárias), Cópias espelhadas (secundárias) ou Cópias de cofre (secundárias).
5. Selecione o backup da tabela e clique em *  *.
6. Na página Localização, execute as seguintes ações:

Para este campo…	Faça isso…
Servidor clone	Por padrão, o host de origem é preenchido.
Ponto de montagem do clone	Especifique o caminho onde o sistema de arquivos será montado.

7. Na página Scripts, execute as seguintes etapas:
   a. Insira os comandos para pré-clonagem ou pós-clonagem que devem ser executados antes ou depois da operação de clonagem, respectivamente.

   Você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in no caminho */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*.

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. Se você quiser anexar o relatório da operação de clonagem realizada, 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.

9. Revise o resumo e clique em **Concluir**.
10. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

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"

Monitorar operações de clonagem de sistemas de arquivos Unix

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**.

Informações sobre direitos autorais

Informações sobre marcas comerciais