# Proteja sistemas de arquivos Unix

## SnapCenter software

NetApp
February 20, 2026

# Índice

# Proteja 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 é instalado em seu ambiente, você pode 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
- Faça backup de sistemas de arquivos Unix
- Agendar operações de backup
- Restaure backups do sistema de arquivos
- Clonar backups do sistema de arquivos
- Monitore operações de backup, restauração e clone

### Configurações compatíveis

| Item | Configuração suportada |
| --- | --- |
| Ambientes | • Servidor físico<br>• Servidor virtual<br><br>Armazenamentos de dados da Vevolve em NFS e SAN. O armazenamento de dados da Vevolve só pode ser provisionado com as ferramentas do ONTAP para VMware vSphere. |
| Sistemas operacionais | • Red Hat Enterprise Linux<br>• Oracle Linux<br>• SUSE Linux Enterprise Server (SLES) |
| Sistemas de arquivos | • SAN:<br>◦ Sistemas de arquivos baseados em LVM e não em LVM<br>◦ LVM sobre VMDK ext3, ext4 e xfs<br>• NFS: NFS v3, NFS v4.x |
| Protocolos | • FC<br>• FCoE<br>• ISCSI<br>• NFS |

| Item | Configuração suportada |
| --- | --- |
| Multipath | sim |

## Limitações

- A combinação de RDMs e discos virtuais em um grupo de volumes não é suportada.
- A restauração no nível do arquivo não é suportada.

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

- A combinação de sistemas de arquivos espalhados por VMDKs provenientes do armazenamento de dados NFS e VMFS não é compatível.
- NVMe não é compatível.
- O provisionamento não é compatível.

## Caraterísticas

- Permite que o Plug-in para Oracle Database execute operações de proteção de dados em bancos de dados Oracle, manipulando a pilha de armazenamento de host subjacente em sistemas Linux ou AIX
- Dá suporte aos protocolos NFS (Network File System) e SAN (Storage Area Network) em um sistema de storage que esteja executando o ONTAP.
- Para sistemas Linux, os bancos de dados Oracle em VMDK e LUNs RDM são suportados quando você implementa o plug-in SnapCenter para VMware vSphere e Registra o plug-in com o SnapCenter.
- Suporta Mount Guard para AIX em sistemas de arquivos SAN e layout LVM.
- Suporta o Enhanced Journaled File System (JFS2) com Registro em linha em sistemas de arquivos SAN e layout LVM apenas para sistemas AIX.

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

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

# Instale o plug-in SnapCenter para sistemas de arquivos Unix

## Pré-requisitos para adicionar hosts e instalar o pacote Plug-ins para Linux

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

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

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

entanto, você deve configurar o sudo Privileges para que o usuário não-root instale e inicie o processo de plug-in. Depois de instalar o plug-in, os processos serão executados como um usuário não-root eficaz.

- Crie credenciais com o modo de autenticação como Linux para o usuário de instalação.
- Você deve ter instalado o Java 11 em seu host Linux.

  Certifique-se de ter instalado apenas a edição certificada DO Java 11 no host Linux.

  Para obter informações sobre O download DO JAVA, consulte: "Downloads Java para todos os sistemas operacionais"

- Você deve ter **bash** como o shell padrão para instalação do plug-in.

### Requisitos de 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<br>• Oracle Linux<br>• SUSE Linux Enterprise Server (SLES) |
| RAM mínima para o plug-in SnapCenter no host | 2 GB |
| Espaço mínimo de instalação e log para o plug-in SnapCenter no host | 2 GB<br>Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente. |

| Item | Requisitos |
| --- | --- |
| Pacotes de software necessários | Java 11 Oracle Java e OpenJDK<br><br>Certifique-se de ter instalado apenas a edição certificada DO Java 11 no host Linux.<br><br>Se você atualizou O JAVA para a versão mais recente, você deve garantir que a opção JAVA_HOME localizada em /var/opt/SnapCenter/spl/etc/spl.properties esteja definida para a versão JAVA correta e o caminho correto. |

Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp" .

## Adicione hosts e instale o pacote Plug-ins para Linux usando 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 guia **hosts gerenciados** está selecionada na parte superior.
3. Clique em **Add**.
4. Na página hosts, execute as seguintes ações:

| Para este campo… | Faça isso… |
| --- | --- |
| Tipo de host | Selecione **Linux** como o tipo de host. |
| Nome do host | Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host.<br><br>O SnapCenter depende da configuração adequada do DNS. Portanto, a melhor prática é entrar no FQDN.<br><br>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.<br><br>A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte as informações sobre como criar credenciais.<br><br>Você pode exibir detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você especificou.<br><br>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 | Guarde o número da porta padrão ou especifique o número da porta.<br><br>O número da porta padrão é 8145. Se o servidor SnapCenter tiver sido instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão.<br><br>Se você instalou manualmente os plug-ins e especificou uma porta personalizada, você deve especificar a mesma porta. Caso contrário, a operação falha. |
| Caminho de instalação | O caminho padrão é */opt/NetApp/SnapCenter*.<br><br>Opcionalmente, você pode personalizar o caminho. Se você usar o caminho personalizado, verifique se o conteúdo padrão dos sudoers é atualizado com o caminho personalizado. |
| Ignorar verificações de pré-instalação opcionais | Marque essa 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 selecionado a caixa de seleção Ignorar pré-verificações, o host será validado para

verificar se o host 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 for especificado nas regras de rejeição do firewall.

Mensagens de erro ou aviso apropriadas são 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: SnapCenter NetApp para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deve corrigir o problema.

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

8. Verifique a impressão digital e clique em **Confirm and Submit**.

> O SnapCenter não suporta o algoritmo ECDSA.

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

9. Monitorize o progresso da instalação.

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

**Resultado**

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

**Monitorar o status da instalação**

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

**Sobre esta tarefa**

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

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

**Passos**

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.

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

## Configure o serviço SnapCenter Plug-in Loader

O serviço SnapCenter Plug-in Loader carrega o pacote plug-in para que o Linux interaja com o servidor SnapCenter. O serviço SnapCenter Plug-in Loader é instalado quando você instala o pacote de plug-ins do SnapCenter para Linux.

### Sobre esta tarefa

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

- Certifique-se de que o diretório em que o plug-in está a funcionar não é eliminado
- Aumente o espaço de memória atribuído à Máquina Virtual Java

O arquivo spl.properties, que está localizado em */custom_location/NetApp/SnapCenter/spl/etc/*, contém os seguintes parâmetros. Os valores padrão são atribuídos a esses parâmetros.

| Nome do parâmetro | Descrição |
|---|---|
| LOG_LEVEL | Apresenta os níveis de registo suportados.<br><br>Os valores possíveis são TRACE, DEBUG, INFO, WARN, ERROR e FATAL. |
| SPL_PROTOCOL (PROTOCOLO SPL) | Apresenta o protocolo suportado pelo Plug-in Loader SnapCenter.<br><br>Apenas o protocolo HTTPS é suportado. Você pode adicionar o valor se o valor padrão estiver ausente. |
| SnapCenter_SERVER_PROTOCOL | Apresenta o protocolo suportado pelo servidor SnapCenter.<br><br>Apenas o protocolo HTTPS é suportado. Você pode adicionar o valor se o valor padrão estiver ausente. |

| Nome do parâmetro | Descrição |
| --- | --- |
| SKIP_JAVAHOME_UPDATE | Por padrão, o serviço SPL deteta o caminho java e atualiza o parâmetro Java_HOME.<br><br>Portanto, o valor padrão é definido como FALSE. Você pode definir como VERDADEIRO se quiser desativar o comportamento padrão e corrigir manualmente o caminho java. |
| SPL_KEYSTORE_PASS | Exibe a senha do arquivo keystore.<br><br>Você pode alterar esse valor somente se você alterar a senha ou criar um novo arquivo de keystore. |
| SPL_PORT | Exibe o número da porta na qual o serviço Plug-in Loader do SnapCenter está sendo executado.<br><br>Você pode adicionar o valor se o valor padrão estiver ausente.<br><br>Você não deve alterar o valor depois de instalar os plug-ins. |
| SnapCenter_Server_HOST | Exibe o endereço IP ou o nome do host do servidor SnapCenter. |
| SPL_KEYSTORE_PATH | Exibe o caminho absoluto do arquivo keystore. |
| SnapCenter_SERVER_PORT | Exibe o número da porta na qual o servidor SnapCenter está sendo executado. |
| REGISTOS_MAX_COUNT | Exibe o número de arquivos de log do Loader do plug-in do SnapCenter que são retidos na pasta */custom_location/SnapCenter/spl/logs*.<br><br>O valor padrão é definido como 5000. Se a contagem for superior ao 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 Loader Plug-in SnapCenter é iniciado.<br><br>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.<br><br>Este caminho é determinado durante a instalação e como parte da inicialização do SPL. |
| LOG_MAX_SIZE | Apresenta o tamanho máximo do ficheiro de registo de trabalhos.<br><br>Assim que o tamanho máximo for atingido, o ficheiro de registo é zipado e os registos são gravados no novo ficheiro desse trabalho. |
| RETER_LOGS_OF_LAST_DAYS | Exibe o número de dias até os quais os logs são mantidos. |
| ENABLE_CERTIFICATE_VALIDATION | Exibe verdadeiro quando a validação do certificado CA está ativada para o host.<br><br>Você pode ativar ou desativar esse parâmetro editando o spl.properties ou usando a GUI ou cmdlet do SnapCenter. |

Se algum destes parâmetros não estiver atribuído ao valor predefinido ou se pretender atribuir ou alterar o valor, pode modificar o ficheiro spl.properties. Você também pode verificar o arquivo spl.properties e editar o arquivo 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 um 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 um usuário não-root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

     Você pode usar a opção -force com o comando stop para parar o serviço SnapCenter Plug-in Loader com força. No entanto, você deve ter cuidado antes de fazê-lo, porque ele também termina as operações existentes.

   - Reinicie o serviço SnapCenter Plug-in Loader:

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

## Configure o 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 armazenamento de confiança SPL e configurar o par de chaves assinadas CA para o armazenamento de confiança 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', tanto como seu armazenamento de confiança e armazenamento de chaves.

**Gerenciar senha para o armazenamento de chaves SPL e alias do par de chaves assinadas CA em uso**

**Passos**

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

   É o valor correspondente à chave 'SPL_KEYSTORE_PASS'.

2. Altere a senha do keystore:

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

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

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

3. Reinicie o serviço depois de alterar a senha.

A senha para o keystore SPL e para todos os alias associados da chave privada deve ser a mesma.

**Configure certificados raiz ou intermediários para o armazenamento de confiança SPL**

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

**Passos**

1. Navegue até a pasta que contém o keystore SPL: */var/opt/SnapCenter/spl/etc*.
2. Localize o arquivo 'keystore.jks'.
3. Liste 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 depois de configurar os certificados raiz ou
intermédios para o armazenamento de confiança SPL.
```

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

**Configure o par de chaves assinadas da CA para o armazenamento de confiança SPL**

Você deve configurar o par de chaves assinadas da CA para o armazenamento de confiança SPL.

**Passos**

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

```
 keytool -list -v -keystore keystore.jks
. Verifique se o keystore contém o alias correspondente ao novo
certificado da CA, que foi adicionado ao keystore.
. Altere a senha da chave privada adicionada para o certificado da 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 espaço ou
carateres especiais ("*",","), altere o nome do alias para um nome
simples:
```

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

Atualize este valor com a chave SPL_CERTIFICATE_ALIAS.

4. Reinicie o serviço depois de configurar o par de chaves assinadas pela CA para o armazenamento de confiança SPL.

**Configurar a lista de revogação de certificados (CRL) para SPL**

Você deve configurar a CRL para SPL

**Sobre esta tarefa**

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

**Passos**

1. Você pode modificar e atualizar o diretório padrão no arquivo spl.properties contra 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.

## Ative certificados de CA para plug-ins

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

**Antes de começar**

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

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

**Passos**

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

**Depois de terminar**

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

- * * Indica que o certificado da CA não está habilitado nem atribuído ao host do plug-in.
- * * Indica que o certificado da CA foi validado com êxito.
- * * Indica que o certificado da CA não pôde ser validado.
- * * indica que as informações de conexão não puderam ser recuperadas.

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

# Instale o plug-in do SnapCenter para VMware vSphere

Se seu banco de dados ou sistema de arquivos estiver armazenado em máquinas virtuais (VMs) ou se você quiser proteger VMs e datastores, você deverá implantar o plug-in do SnapCenter para o dispositivo virtual VMware vSphere.

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

## Implantar certificado CA

Para configurar o certificado CA com o plug-in SnapCenter para VMware vSphere, "Criar ou importar certificado SSL" consulte .

### Configure o arquivo CRL

O plug-in do SnapCenter para VMware vSphere procura os arquivos CRL em um diretório pré-configurado. O diretório padrão dos arquivos CRL para o plug-in do SnapCenter para 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, clone ou restauração, você deve configurar o ambiente. Você também pode configurar o servidor SnapCenter para usar a tecnologia SnapMirror e SnapVault.

Para aproveitar as tecnologias SnapVault e SnapMirror, você deve configurar e inicializar uma relação 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 servidor SnapCenter e executar as tarefas de pré-requisito.

- Instalar e configurar o servidor SnapCenter. "Saiba mais"
- Configure o ambiente SnapCenter adicionando conexões do sistema de storage. "Saiba mais"

> O SnapCenter não é compatível com vários SVMs com o mesmo nome em clusters diferentes. Cada SVM registrado no SnapCenter usando o Registro da SVM ou o Registro de cluster precisa ser único.

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

# Faça backup de sistemas de arquivos Unix

### Descubra os sistemas de arquivos UNIX disponíveis para backup

Depois de instalar o plug-in, todos os sistemas de arquivos nesse host são automaticamente descobertos 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 servidor SnapCenter, 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 plug-in do SnapCenter para VMware vSphere e Registrar o plug-in com o SnapCenter.

  Para obter mais informações, "Implante o plug-in do SnapCenter para VMware vSphere"consulte .

**Passos**

1. No painel de navegação esquerdo, clique em **Resources** 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 juntamente com informações como tipo, nome do host, grupos e políticas de recursos 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 o grupo de recursos que deseja fazer backup. Uma política de backup é um conjunto de regras que regem como você gerencia, agenda e retém backups. Você também pode especificar as configurações de replicação, script e tipo de backup. A criação de uma política economiza tempo quando você deseja reutilizar a política em outro recurso ou grupo de recursos.

**Antes de começar**

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

**Sobre esta tarefa**

- SnapLock
  - Se a opção 'reter as cópias de backup para um número específico de dias' estiver selecionada, o período de retenção do SnapLock deve ser menor ou igual aos dias de retenção mencionados.

    Especificar um período de bloqueio instantâneo impede a exclusão dos instantâneos até que o período de retenção expire. Isso pode levar a reter um número maior de instantâneos do que a contagem especificada na política.

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

**Passos**

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **políticas**.

3. Selecione **Unix File Systems** 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 definições de cópia de segurança.

    b. Especifique a frequência da programação selecionando **on demand**, **Hourly**, **Daily**, **Weekly** ou **Monthly**.

    c. 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 depois de criar uma cópia Snapshot local | Selecione este campo para criar cópias espelhadas dos conjuntos de backup em outro volume (replicação SnapMirror).<br><br>Esta opção deve estar ativada para a sincronização ativa do SnapMirror. |
| Atualize o SnapVault depois de criar uma cópia Snapshot local | Selecione esta opção para executar a replicação de backup disco a disco (backups SnapVault). |
| Contagem de tentativas de erro | Introduza o número máximo de tentativas de replicação que podem ser permitidas antes de a operação parar. |

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 instantâneos | Selecione **Copies to keep** e especifique o número de instantâneos que deseja manter.<br><br>Se o número de instantâneos exceder o número especificado, os instantâneos serão excluídos com as cópias mais antigas excluídas primeiro.<br><br>O valor máximo de retenção é 1018. Os backups falharão se a retenção for definida para um valor maior do que o que a versão subjacente do ONTAP suporta.<br><br>Você deve definir a contagem de retenção como 2 ou superior, se quiser habilitar a replicação do SnapVault. Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro snapshot é o snapshot de referência para a relação SnapVault até que um snapshot mais recente seja replicado para o destino. |
| Mantenha as capturas instantâneas por um determinado número de dias | Selecione **reter cópias para** e especifique o número de dias para os quais deseja manter as capturas instantâneas antes de excluí-las. |
| Período de bloqueio de cópia de instantâneo | Selecione **Período de bloqueio de cópia de instantâneo** e especifique a duração em dias, meses ou anos.<br><br>O período de retenção do SnapLock deve ser inferior a 100 anos. |

8. Selecione a etiqueta 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 prescritor ou postscript que você deseja executar antes ou depois da operação de backup, respetivamente.

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

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

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

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

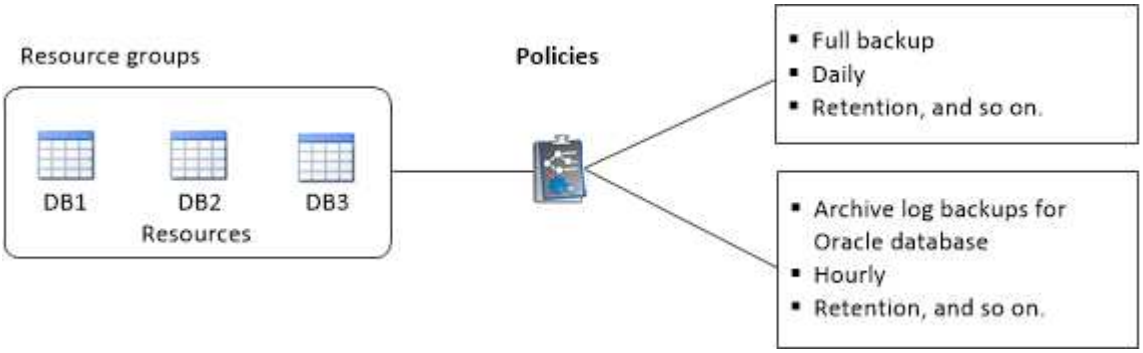
Um grupo de recursos é um contentor onde você adiciona recursos que deseja fazer backup e proteger. Um grupo de recursos permite fazer backup de todos os dados associados aos sistemas de arquivos.

**Sobre esta tarefa**

- Um banco de dados com arquivos em grupos de discos ASM deve estar no estado "MOUNT" 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 tarefa de proteção de dados que deseja executar.

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




- Para políticas habilitadas para o SnapLock, para ONTAP 9.12,1 e versões abaixo, se você especificar um período de bloqueio do Snapshot, os clones criados a partir dos snapshots à prova de violação como parte da restauração herdarão o tempo de expiração do SnapLock. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.
- A adição de novos sistemas de arquivos sem a sincronização ativa do SnapMirror a um grupo de recursos existente que contenha recursos com a sincronização ativa do SnapMirror não é suportada.
- A adição de novos sistemas de arquivos a um grupo de recursos existente no modo failover da sincronização ativa do SnapMirror não é suportada. Você pode adicionar recursos ao grupo de recursos apenas no estado regular ou de failback.

**Passos**

1. No painel de navegação esquerdo, selecione **Resources** 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. Introduza um nome para o grupo de recursos no campo Nome.

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

   b. Insira um ou mais rótulos no campo Tag para ajudá-lo a pesquisar o grupo de recursos mais tarde.

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

c. Marque a caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.

   Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.

4. Na página recursos, selecione um nome de host de sistemas de arquivos Unix na lista suspensa **Host**.

   Os recursos são listados na seção recursos disponíveis somente se o recurso for descoberto com êxito. Se você tiver adicionado recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois de atualizar sua lista de recursos.

5. Selecione os recursos na seção recursos disponíveis e mova-os para a seção recursos selecionados.
6. Na página Configurações do aplicativo, execute o seguinte:
   - Selecione a seta Scripts e insira os comandos pre e POST para operações quiesce, Snapshot e unquiesce. Também pode introduzir os pré comandos a serem executados antes de sair em caso de falha.
   - Selecione uma das opções de consistência de backup:
     - Selecione **sistema de arquivos consistente** se você quiser garantir que os dados em cache dos sistemas de arquivos sejam limpos antes de criar o backup e nenhuma operação de entrada ou saída seja permitida no sistema de arquivos durante a criação do backup.

       Para o sistema de arquivos consistente, instantâneos de grupo de consistência serão feitos para LUNs envolvidos no grupo volume.

     - Selecione **Crash consistente** se quiser garantir que os dados em cache dos sistemas de arquivos sejam limpos antes de criar o backup.

       Se você adicionou 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 agendas para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.

   c. Na janela Adicionar programações para a política *policy_name*, configure a programação e clique em **OK**.

      Onde, *policy_name* é o nome da política selecionada.

      As programações configuradas são listadas na coluna agendas aplicadas.

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

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

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

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

## Crie grupos de recursos e habilite a proteção secundária para sistemas de arquivos Unix em sistemas ASA R2

Você deve criar o grupo de recursos para adicionar os recursos que estão em sistemas ASA R2. Você também pode provisionar a proteção secundária enquanto cria o grupo de recursos.

**Antes de começar**

- Você deve garantir que não esteja adicionando recursos do ONTAP 9.x e do ASA R2 ao mesmo grupo de recursos.
- Você deve garantir que não tenha um banco de dados com recursos do ONTAP 9.x e do ASA R2.

**Sobre esta tarefa**

- A proteção secundária só está disponível se o usuário conetado for atribuído à função que tem a capacidade **SecondaryProtection** ativada.
- Se você ativou a proteção secundária, o grupo de recursos será colocado no modo de manutenção ao criar os grupos de consistência primária e secundária. Depois que os grupos de consistência primária e secundária são criados, o grupo de recursos é colocado fora do modo de manutenção.
- O SnapCenter não é compatível com proteção secundária para um recurso clone.

**Passos**

1. No painel de navegação esquerdo, selecione **Resources** 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. Introduza um nome para o grupo de recursos no campo Nome.

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

   b. Insira um ou mais rótulos no campo Tag para ajudá-lo a pesquisar o grupo de recursos mais tarde.

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

   c. Marque essa caixa de seleção e insira um formato de nome personalizado que você deseja usar para

o nome da captura Instantânea.

Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.

d. Especifique os destinos dos ficheiros de registo de arquivo que não pretende efetuar uma cópia de segurança.

> Você deve usar exatamente o mesmo destino que foi 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 êxito. Se você tiver adicionado recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois de 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 agendas para políticas selecionadas, as políticas selecionadas são listadas.

b. Clique na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.

c. Na janela Adicionar programações para a política *policy_name*, configure a programação e clique em **OK**.

Onde, *policy_name* é o nome da política selecionada.

As programações configuradas são listadas na coluna agendas aplicadas.

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

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

a. Selecione o tipo da 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 drop-down Cluster de destino e SVM de destino, selecione o cluster com peering e SVM que você deseja usar.

O peering de cluster e SVM não é compatível com o SnapCenter. Você deve usar o Gerenciador de sistema ou os CLIs ONTAP para executar peering de cluster e SVM.

Se os recursos já estiverem protegidos fora do SnapCenter, esses recursos 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 executar a verificação no armazenamento secundário.
   b. Clique + na coluna Configurar agendas 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… |
|---|---|
| Execute a verificação após a cópia de segurança | Selecione **Executar verificação após backup**. |
| Marque uma verificação | Selecione **Executar verificação agendada** e, em seguida, selecione o tipo de agendamento na lista suspensa. |

   d. Selecione **verificar no local secundário** para verificar os backups no sistema de armazenamento secundário.
   e. Clique em **OK**.

   As programações de verificação configuradas são listadas na coluna agendas aplicadas.

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 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 PowerShell SET-SmtpServer.

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

## Faça backup de sistemas de arquivos Unix

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

**Passos**

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

2. Na página recursos, selecione **caminho** na lista Exibir.
3. Clique em e selecione o nome do host e os sistemas de arquivos Unix para filtrar os recursos.
4. Selecione o sistema de ficheiros que pretende efetuar uma cópia de segurança.
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 da captura Instantânea.

      Por exemplo, `customtext_policy_hostname` ou `resource_hostname`. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.

6. Na página Configurações do aplicativo, execute o seguinte:
   - Selecione a seta Scripts e insira os comandos pre e POST para operações quiesce, Snapshot e unquiesce. Também pode introduzir os pré comandos a serem executados antes de sair em caso de falha.
   - Selecione uma das opções de consistência de backup:
     - Selecione **File System consistent** se quiser garantir que os dados em cache dos sistemas de arquivos sejam limpos antes de criar o backup e nenhuma operação seja executada no sistema de arquivos enquanto cria o backup.
     - Selecione **Crash consistente** se quiser garantir que os dados em cache dos sistemas 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 agendas para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique na coluna Configurar agendas para configurar uma agenda para a política desejada.
   c. Na janela Adicionar agendas para a política *policy_name* , configure a programação e `OK` selecione .

      *policy_name* é o nome da política selecionada.

   As programações configuradas são listadas na coluna agendas aplicadas.

8. Na página notificação, selecione os cenários em que você deseja enviar os e-mails da 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 quiser anexar o relatório da operação de backup realizada no recurso, selecione **Anexar Relatório de trabalho**.

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

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

A página de topologia é exibida.

10. Clique em **fazer backup agora**.
11. Na página Backup, execute as seguintes etapas:
    a. Se você tiver aplicado 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. Monitorize o progresso da operação clicando em **Monitor** > **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 uma programação configurada, os backups serão criados de acordo com a programação.

**Passos**

1. No painel de navegação esquerdo, selecione **Resources** 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 em 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. Monitorize o progresso selecionando **Monitor > trabalhos**.

## Monitorar backup de sistemas de arquivos Unix

Saiba como monitorar o progresso das operações de backup e operações de 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. Você pode querer verificar o progresso para determinar quando ele está concluído ou se há um problema.

**Sobre esta tarefa**

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

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

**Passos**

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

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

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

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

### Monitore operações de proteção de dados no painel atividade

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

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

**Passos**

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

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

## Veja sistemas de arquivos Unix protegidos na página topologia

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

### Sobre esta tarefa

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

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

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

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

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

Se você tiver uma relação secundária como sincronização ativa do SnapMirror (lançada inicialmente como SnapMirror Business Continuity [SM-BC]), você poderá ver os seguintes ícones adicionais:

-  O site da réplica está em cima.
-  O site da réplica está inativo.
-  A relação do espelho secundário ou do cofre não foi restabelecida.

### Passos

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

3. Selecione o recurso na exibição de detalhes do recurso ou na exibição de detalhes do grupo de recursos.

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

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

   A seção cartão de resumo exibe o número total de backups e clones.

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

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

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

   Para a 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 a relação de sincronização ativa do SnapMirror.

   - Para a sincronização ativa do SnapMirror e somente para o ONTAP 9.14,1, as relações de espelhamento do Async ou EspelrorVault do Async com o novo destino primário devem ser configuradas manualmente após o failover. A partir do ONTAP 9.15,1 em diante, o espelho do Async ou o MirrorVault do Async 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 **Refresh** somente depois que um backup tiver sido criado.

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

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

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

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

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

**Exemplo mostrando backups e clones no storage primário**


# Restaurar e recuperar sistemas de arquivos Unix

## Restaure 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 servidor SnapCenter, listar os backups e 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 no local principal.

### Passos

1. No painel de navegação esquerdo, clique em **Resources** 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** nos sistemas de armazenamento primário ou secundário (espelhado ou replicado).
5. Selecione a cópia de segurança na tabela e, em seguida, clique em *  .
6. Na página Restaurar escopo:
   - Para sistemas de arquivos NFS, por padrão, a opção **Connect and Copy** Restore está selecionada. Você também pode selecionar **Reverter volume** ou **Restauração rápida**.
   - Para sistemas de arquivos que não sejam NFS, o escopo de restauração é selecionado dependendo do layout.

     Os novos ficheiros criados após a cópia de segurança poderão não estar disponíveis após a restauração, dependendo do tipo de sistema de ficheiros e do esquema.
7. Na página PreOps, insira os comandos de pré-restauração a serem executados antes de executar uma tarefa de restauração.
8. Na página PostOps, insira os comandos pós-restauração para 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 caminho */opt/NetApp/SnapCenter/scc/etc/allowed_Commands.config*.
9. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários em que 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 pretender anexar o relatório da operação de restauro efetuada, tem de selecionar **Anexar Relatório de trabalho**.

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

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

    Em caso de restauração de um sistema de arquivos residente no 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 padrão do sistema de arquivos NFS.
11. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

## Monitorar operações de restauração de sistemas de arquivos Unix

Pode monitorizar o progresso de diferentes operações de restauro do SnapCenter utilizando a página trabalhos. Você pode querer verificar o progresso de uma operação

para determinar quando ela está concluída ou se há um problema.

**Sobre esta tarefa**

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

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

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

**Passos**

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

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

# Clonar sistemas de arquivos Unix

## Clone 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 ignorar a atualização do arquivo fstab definindo o valor de *SKIP_FSTAB_UPDATE* para **true** no arquivo *agent.properties* localizado em */opt/NetApp/SnapCenter/scc/etc*.
- Você pode ter um nome de volume de clone estático e caminho de junção definindo o valor de *USE_CUSTOM_CLONE_VOLUME_NAME_FORMAT* para **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 esta propriedade o nome do volume do clone e o caminho de junção serão como <Source_volume_name>_Clone_<Timestamp>, mas agora será <Source_volume_name>_Clone_<Clone_Name>

Isso mantém o nome constante para que você possa manter manualmente o arquivo fstab atualizado se você não preferir atualizar o fstab pelo SnapCenter.

**Passos**

1. No painel de navegação esquerdo, clique em **Resources** 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 de cópias locais (primárias), cópias espelhadas (secundárias) ou cópias do Vault (secundárias).
5. Selecione a cópia de segurança na tabela e, em seguida, 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 clone | Especifique o caminho onde o sistema de arquivos será montado. |

7. Na página Scripts, execute as seguintes etapas:
   a. Digite os comandos para pré-clone ou pós-clone que devem ser executados antes ou depois da operação clone, respetivamente.

   > Você deve verificar se os comandos existem na lista de comandos disponível no host plug-in do 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 quiser anexar o relatório da operação clone executada, 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 PowerShell SET-SmtpServer.

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

## Divida um clone

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone

que é dividido torna-se independente do recurso pai.

**Sobre esta tarefa**

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

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

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

- Quando você divide um clone, as cópias de backup e as tarefas de clone do clone são excluídas.
- Para obter informações sobre operações de divisão de volume do FlexClone, consulte, "Divida um volume FlexClone do volume pai".
- Certifique-se de que o volume ou o agregado no sistema de storage esteja on-line.

**Passos**

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página **recursos**, selecione a opção apropriada na lista Exibir:

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

3. Selecione o recurso apropriado na lista.

   A página de topologia do recurso é exibida.

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

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

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

   Por exemplo:

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

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

**Informações relacionadas**

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

## Monitorar operações de clones de sistemas de arquivos Unix

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

**Sobre esta tarefa**

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

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

**Passos**

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

## Informações sobre direitos autorais



## Informações sobre marcas comerciais