



Proteja aplicativos usando plug-ins compatíveis com NetApp

SnapCenter software

NetApp
November 06, 2025

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

Índice

Proteja aplicativos usando plug-ins compatíveis com NetApp	1
Plug-ins suportados pela NetApp	1
Visão geral dos plug-ins suportados pela NetApp	1
O que você pode fazer com os plug-ins suportados pela NetApp	1
Recursos de plug-ins suportados pela NetApp	2
Tipos de armazenamento suportados pelos plug-ins suportados pela NetApp	3
Privilégios ONTAP mínimos necessários para plug-in compatível com NetApp	3
Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault para plug-ins compatíveis com NetApp	6
Definir uma estratégia de backup	6
Estratégia de backup para plug-ins suportados pela NetApp	7
Tipos de estratégias de restauração suportadas para recursos de plug-in suportados pela NetApp adicionados manualmente	8
Prepare-se para instalar plug-ins compatíveis com NetApp	8
Fluxo de trabalho de instalação de plug-ins compatíveis com SnapCenter NetApp	8
Pré-requisitos para adicionar hosts e instalar o pacote de plug-ins para Windows, Linux ou AIX	9
Requisitos de host para instalar o pacote de plug-ins SnapCenter para Windows	13
Requisitos de host para instalar o pacote de plug-ins SnapCenter para Linux e AIX	14
Configurar credenciais para plug-ins compatíveis com NetApp	15
Configurar o gMSA no Windows Server 2016 ou posterior	18
Instalar os plug-ins suportados pela NetApp	19
Configurar certificado CA	25
Prepare-se para a proteção de dados	33
Pré-requisitos para usar os plug-ins suportados pela NetApp	33
Como recursos, grupos de recursos e políticas são usados para proteger recursos de plug-in com suporte da NetApp	34
Faça backup dos recursos de plug-ins suportados pela NetApp	34
Faça backup dos recursos de plug-ins suportados pela NetApp	34
Adicionar recursos aos plug-ins suportados pela NetApp	35
Criar políticas para recursos de plug-in suportados NetApp	39
Crie grupos de recursos e anexe políticas	43
Crie grupos de recursos e habilite proteção secundária para recursos em sistemas ASA r2	47
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell	49
Faça backup de recursos individuais de plug-ins suportados pela NetApp	50
Fazer backup de grupos de recursos de plug-ins suportados NetApp	56
Monitorar operações de backup de recursos de plug-in com suporte da NetApp	57
Cancelar operações de backup para plug-ins compatíveis com NetApp	58
Exibir backups e clones relacionados a recursos de plug-ins suportados pela NetApp na página Topologia	59
Restaurar recursos de plug-ins suportados pela NetApp	60
Restaurar recursos de plug-in suportados pelo NetApp	60
Restaurar um backup de recurso	61
Monitorar operações de restauração de recursos de plug-in suportados NetApp	65

Clonar backups de recursos de plug-ins suportados pelo NetApp	66
Clonar backups de recursos de plug-ins suportados pelo NetApp	66
Clonar de um backup	67
Monitorar operações de clonagem de recursos de plug-in com suporte do NetApp	73

Proteja aplicativos usando plug-ins compatíveis com NetApp

Plug-ins suportados pela NetApp

Visão geral dos plug-ins suportados pela NetApp

Você pode usar os plug-ins suportados NetApp , como MongoDB, ORASCPM (Oracle Applications), SAP ASE, SAP MaxDB e plug-in de armazenamento para os aplicativos que você usa e, em seguida, usar o SnapCenter para fazer backup, restaurar ou clonar esses aplicativos. Os plug-ins suportados NetApp atuam como componentes do lado do host do NetApp SnapCenter Software, permitindo a proteção de dados com reconhecimento de aplicativo e o gerenciamento de recursos.

Quando os plug-ins suportados NetApp estiverem instalados, você poderá usar o SnapCenter com a tecnologia NetApp SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e usar a tecnologia NetApp SnapVault para executar a replicação de backup de disco para disco. Os plug-ins suportados pela NetApp podem ser usados em ambientes Windows e Linux.



O SnapCenterCLI não oferece suporte a comandos de plug-ins suportados NetApp .

A NetApp fornece o plug-in de armazenamento para executar operações de proteção de dados do volume de dados no armazenamento ONTAP usando a estrutura de plug-in integrada ao SnapCenter.

Você pode instalar os plug-ins suportados pela NetApp na página Adicionar Host.

["Adicione hosts e instale pacotes de plug-ins em hosts remotos."](#)



A política de suporte do SnapCenter cobrirá o suporte para a estrutura do plug-in, o mecanismo principal e as APIs associadas. O suporte não cobrirá o código-fonte do plug-in e os scripts associados criados na estrutura do plug-in.

O que você pode fazer com os plug-ins suportados pela NetApp

Você pode usar os plug-ins suportados pela NetApp , como MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB e plug-in de armazenamento para operações de proteção de dados.

- Adicione recursos como bancos de dados, instâncias, documentos ou tablespaces.
- Crie backups.
- Restaurar a partir de backups.
- Clonar backups.
- Agende operações de backup.
- Monitore operações de backup, restauração e clonagem.
- Visualize relatórios de operações de backup, restauração e clonagem.

Você pode usar os plug-ins suportados pela NetApp para operações de proteção de dados.

- Faça snapshots do grupo de consistência dos volumes de armazenamento em clusters ONTAP .
- Faça backup de aplicativos personalizados usando a estrutura de pré e pós-script integrada

Você pode fazer backup de um volume ONTAP , LUN ou Qtree.

- Atualizar instantâneos tirados do primário para um secundário ONTAP , aproveitando o relacionamento de replicação existente (SnapVault/ SnapMirror/replicação unificada) usando a política do SnapCenter

ONTAP primário e secundário podem ser ONTAP FAS, AFF, ASA, ONTAP Select ou Cloud Volumes ONTAP.

- Recupere volumes ONTAP , LUN ou arquivos completos.

Você deve fornecer o caminho do arquivo respectivo manualmente, pois os recursos de navegação ou indexação não estão incorporados ao produto.

A restauração de Qtree ou diretório não é suportada, mas você pode clonar e exportar somente o Qtree se o escopo de backup estiver definido no nível do Qtree.

Recursos de plug-ins suportados pela NetApp

O SnapCenter integra-se ao aplicativo plug-in e às tecnologias NetApp no sistema de armazenamento. Para trabalhar com plug-ins compatíveis com NetApp , como MongoDB, ORASCPM (Oracle Applications), SAP ASE, SAP MaxDB e plug-in de armazenamento, use a interface gráfica do usuário do SnapCenter .

- **Interface gráfica de usuário unificada**

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

- **Administração central automatizada**

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

- **Tecnologia NetApp Snapshot não disruptiva**

O SnapCenter usa a tecnologia NetApp Snapshot com os plug-ins suportados pela NetApp para fazer backup de recursos. Os instantâneos consomem espaço de armazenamento mínimo.

Os plug-ins suportados pela NetApp também oferecem os seguintes benefícios:

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

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

- Criação de cópias de recursos com eficiência de espaço e em um determinado momento para testes ou extração de dados usando a tecnologia NetApp FlexClone

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

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

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

- Capacidade de criar Snapshot usando comandos externos.
- Capacidade de criar instantâneos consistentes do sistema de arquivos em ambientes Windows.

Tipos de armazenamento suportados pelos plug-ins suportados pela NetApp

O SnapCenter oferece suporte a uma ampla variedade de tipos de armazenamento em máquinas físicas e virtuais. Você deve verificar o suporte para seu tipo de armazenamento antes de instalar plug-ins compatíveis com o NetApp .

Máquina	Tipo de armazenamento
Montagens físicas e diretas NFS nos hosts de VM (VMDKs e RDM LUNs não são suportados).	LUNs conectados por FC
Montagens físicas e diretas NFS nos hosts de VM (VMDKs e RDM LUNs não são suportados).	LUNs conectados por iSCSI
Montagens físicas e diretas NFS nos hosts de VM (VMDKs e RDM LUNs não são suportados).	Volumes conectados ao NFS
VMware ESXi	Armazenamentos de dados vVol em NFS e SAN O armazenamento de dados vVol só pode ser provisionado com o ONTAP Tools para VMware vSphere.

Privilégios ONTAP mínimos necessários para plug-in compatível com NetApp

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

- Comandos de acesso total: privilégios mínimos necessários para ONTAP 9.12.1 e posterior
 - evento generate-autosupport-log
 - histórico de trabalho mostrar
 - parada de trabalho
 - mostrar atributo lun

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

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

Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault para plug-ins compatíveis com NetApp

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

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



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

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



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

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

Definir uma estratégia de backup

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

Sobre esta tarefa

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

Passos

1. Determine quando você deve fazer backup dos seus recursos.
2. Decida quantos trabalhos de backup você precisa.
3. Decida como nomear seus backups.
4. Decida se você deseja Snapshots do Grupo de Consistência e decida sobre as opções apropriadas para excluir Snapshots do Grupo de Consistência.

5. Decida se você deseja usar a tecnologia NetApp SnapMirror para replicação ou a tecnologia NetApp SnapVault para retenção de longo prazo.
6. Determine o período de retenção dos Snapshots no sistema de armazenamento de origem e no destino do SnapMirror .
7. Determine se você deseja executar algum comando antes ou depois da operação de backup e forneça uma prescrição ou pós-escrito.

Estratégia de backup para plug-ins suportados pela NetApp

Cronogramas de backup de recursos de plug-in suportados NetApp

O fator mais crítico na determinação de um cronograma de backup é a taxa de alteração do recurso. Quanto mais você fizer backup dos seus recursos, menos logs de arquivamento o SnapCenter terá que usar para restauração, o que pode resultar em operações de restauração mais rápidas.

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

O SLA define o nível de serviço esperado e aborda muitas questões relacionadas ao serviço, incluindo a disponibilidade e o desempenho do serviço. O RPO define a estratégia para a idade dos arquivos que devem ser recuperados do armazenamento de backup para que as operações regulares sejam retomadas após uma falha. SLA e RPO contribuem para a estratégia de proteção de dados.

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

- Frequência de backup

A frequência de backup (com que frequência os backups devem ser realizados), também chamada de tipo de agendamento para alguns plug-ins, faz parte de uma configuração de política. Por exemplo, você pode configurar a frequência de backup como horária, diária, semanal ou mensal. Você pode acessar políticas na GUI do SnapCenter clicando em **Configurações > Políticas**.

- Agendamentos de backup

Os agendamentos de backup (exatamente quando os backups devem ser executados) fazem parte de uma configuração de recurso ou grupo de recursos. Por exemplo, se você tiver um grupo de recursos com uma política configurada para backups semanais, poderá configurar o agendamento para fazer backup toda quinta-feira às 22h. Você pode acessar os agendamentos do grupo de recursos na GUI do SnapCenter clicando em **Recursos**, selecionando o plug-in apropriado e clicando em **Exibir > Grupo de recursos**.

Número de trabalhos de backup necessários

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

O número de tarefas de backup que você escolhe normalmente depende do número de volumes nos quais você colocou seus recursos. Por exemplo, se você colocar um grupo de recursos pequenos em um volume e um recurso grande em outro volume, você poderá criar uma tarefa de backup para os recursos pequenos e

uma tarefa de backup para o recurso grande.

Tipos de estratégias de restauração suportadas para recursos de plug-in suportados pela NetApp adicionados manualmente

Você deve definir uma estratégia antes de poder executar com sucesso operações de restauração usando o SnapCenter. Há dois tipos de estratégias de restauração para recursos de plug-in suportados NetApp adicionados manualmente.



Não é possível recuperar recursos de plug-in suportados NetApp adicionados manualmente.

Restauração completa de recursos

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



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

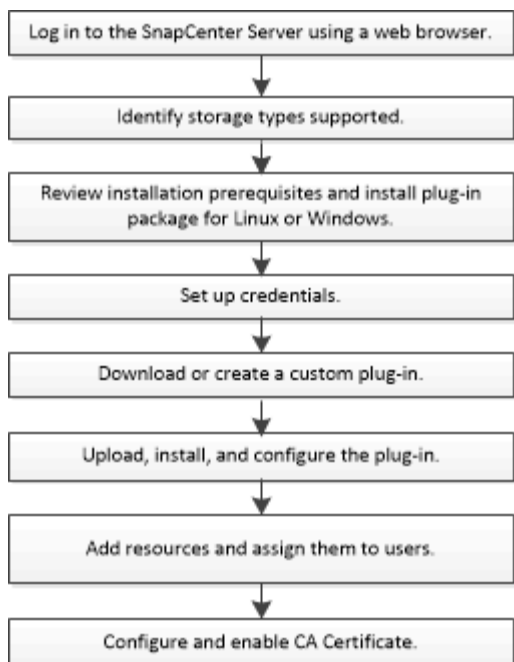
Restauração em nível de arquivo

- Restaura arquivos de volumes, qtrees ou diretórios
- Restaura apenas os LUNs selecionados

Prepare-se para instalar plug-ins compatíveis com NetApp

Fluxo de trabalho de instalação de plug-ins compatíveis com SnapCenter NetApp

Você deve instalar e configurar plug-ins compatíveis com o SnapCenter NetApp se quiser proteger os recursos de plug-ins compatíveis com o NetApp .



Pré-requisitos para adicionar hosts e instalar o pacote de plug-ins para Windows, Linux ou AIX

Antes de adicionar um host e instalar os pacotes de plug-ins, você deve atender a todos os requisitos. Os plug-ins suportados pela NetApp são suportados em ambientes Windows, Linux e AIX.



Aplicativos de armazenamento e Oracle são suportados no AIX.

- Você deve ter instalado o Java 11 no seu host Linux, Windows ou AIX.



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

- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.
- Os plug-ins suportados NetApp, como MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB e plug-in de armazenamento, devem estar disponíveis no host do cliente de onde a operação de adição de host é realizada.

Em geral

Se você estiver usando iSCSI, o serviço iSCSI deverá estar em execução.

Hosts do Windows

- Você deve ter um usuário de domínio com privilégios de administrador local e permissões de login local no host remoto.
- Se você gerenciar nós de cluster no SnapCenter, deverá ter um usuário com privilégios administrativos para todos os nós do cluster.

- Você deve escolher manualmente o SnapCenter Plug-in para Microsoft Windows.

["Baixe JAVA para Windows"](#)

Hosts Linux e AIX



Aplicativos de armazenamento e Oracle são suportados no AIX.

- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.
- Você deve ter instalado o Java 11 no seu host Linux.

Se estiver usando o Windows Server 2019 ou o Windows Server 2016 para o host do SnapCenter Server, você deverá instalar o Java 11. A Ferramenta de Matriz de Interoperabilidade (IMT) contém as informações mais recentes sobre requisitos.

["Baixe JAVA para Linux"](#)

["Baixe JAVA para AIX"](#)

["Ferramenta de Matriz de Interoperabilidade da NetApp"](#)

- Você deve configurar privilégios sudo para que o usuário não root forneça acesso a vários caminhos. Adicione as seguintes linhas ao arquivo `/etc/sudoers` usando o utilitário visudo Linux.



Certifique-se de estar usando o Sudo versão 1.8.7 ou posterior.

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

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

Você pode obter o *checksum_value* do arquivo **sc_unix_plugins_checksum.txt**, localizado em:

- *C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* se o SnapCenter Server estiver instalado no host Windows.
- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* se o SnapCenter Server estiver instalado no host Linux.



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

Requisitos do host AIX


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



Aplicativos de armazenamento e Oracle são suportados no AIX.



O SnapCenter Plug-in para UNIX, que faz parte do Pacote de Plug-ins SnapCenter para AIX, não oferece suporte a grupos de volumes simultâneos.

Item	Requisitos
Sistemas operacionais	AIX 7.1 ou posterior
RAM mínima para o plug-in SnapCenter no host	4 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.
Pacotes de software necessários	Java 11 IBM Java Se você atualizou o JAVA para a versão mais recente, certifique-se de que a opção JAVA_HOME localizada em <i>/var/opt/snapcenter/spl/etc/spl.properties</i> esteja definida para a versão correta do JAVA e o caminho correto.

Para obter as informações mais recentes sobre as versões suportadas, consulte o ["Ferramenta de Matriz de Interoperabilidade da NetApp"](#).

Configurar privilégios sudo para usuários não root para host AIX

O SnapCenter 4.4 e versões posteriores permitem que um usuário não root instale o Pacote de plug-ins do SnapCenter para AIX e inicie o processo de plug-in. Os processos do plug-in serão executados como um usuário não root efetivo. Você deve configurar privilégios sudo para que o usuário não root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Edite o arquivo `/etc/ssh/sshd_config` para configurar os algoritmos do código de autenticação de mensagens: MACs hmac-sha2-256 e MACs hmac-sha2-512.

Reinicie o serviço sshd após atualizar o arquivo de configuração.

Exemplo:

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

Sobre esta tarefa

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

- `/home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx`
- `/localização_personalizada/ NetApp/snapcenter/spl/instalação/plugins/desinstalação`
- `/localização_personalizada/ NetApp/snapcenter/spl/bin/spl`

Passos

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

```

Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty

```



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

Você pode obter o valor de `crs_home` do arquivo `/etc/oracle/olr.loc`.

`AIX_USER` é o nome do usuário não root que você criou.

Você pode obter o `checksum_value` do arquivo `sc_unix_plugins_checksum.txt`, localizado em:


- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` se o SnapCenter Server estiver instalado no host Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` se o SnapCenter Server estiver instalado no host Linux.



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

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

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

Item	Requisitos
Sistemas Operacionais	<p>Microsoft Windows</p> <p>Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .</p>
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	<p>5 GB</p> <div>  <p>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.</p> </div>
Pacotes de software necessários	<ul style="list-style-type: none"> • Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) • PowerShell Core 7.4.2 • Java 11 Oracle Java e OpenJDK <p>O Java 11 Oracle Java e OpenJDK são necessários apenas para SAP HANA, IBM Db2, PostgreSQL, MySQL, plug-ins compatíveis com NetApp e outros aplicativos personalizados que podem ser instalados no host Windows.</p> <p>Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .</p> <p>Para obter informações específicas sobre solução de problemas do .NET, consulte "A atualização ou instalação do SnapCenter falha em sistemas legados que não têm conectividade com a Internet."</p>

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

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



Aplicativos de armazenamento e Oracle são suportados no AIX.

Item	Requisitos
Sistemas operacionais	<ul style="list-style-type: none">• Red Hat Enterprise Linux• Oracle Linux• Servidor SUSE Linux Enterprise (SLES)
RAM mínima para o plug-in SnapCenter no host	1 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.
Pacotes de software necessários	Java 11 Oracle Java ou OpenJDK Se você atualizou o JAVA para a versão mais recente, certifique-se de que a opção JAVA_HOME localizada em <code>/var/opt/snapcenter/spl/etc/spl.properties</code> esteja definida para a versão correta do JAVA e o caminho correto.

Para obter as informações mais recentes sobre as versões suportadas, consulte o ["Ferramenta de Matriz de Interoperabilidade da NetApp"](#)

Configurar credenciais para plug-ins compatíveis com NetApp

O SnapCenter usa credenciais para autenticar usuários para operações do SnapCenter . Você deve criar credenciais para instalar plug-ins do SnapCenter e credenciais adicionais para executar operações de proteção de dados em bancos de dados ou sistemas de arquivos do Windows.

Antes de começar

- Hosts Linux ou AIX

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

Você deve configurar as credenciais para o usuário root ou para um usuário não root que tenha privilégios

sudo para instalar e iniciar o processo do plug-in.

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

- Hosts do Windows

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

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

- Aplicativos de plug-ins suportados pela NetApp

O plug-in usa as credenciais selecionadas ou criadas ao adicionar um recurso. Se um recurso não exigir credenciais durante operações de proteção de dados, você poderá definir as credenciais como **Nenhum**.


Sobre esta tarefa

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

Passos

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

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

Para este campo...	Faça isso...
Nome de usuário	<p>Digite o nome de usuário e a senha que serão usados para autenticação.</p> <ul style="list-style-type: none"> Administrador de domínio ou qualquer membro do grupo de administradores <p>Especifique o administrador do domínio ou qualquer membro do grupo de administradores no sistema em que você está instalando o plug-in SnapCenter . Os formatos válidos para o campo Nome de usuário são:</p> <ul style="list-style-type: none"> <i>NetBIOS\Nome do Usuário</i> <i>FQDN do domínio\Nome do usuário</i> <ul style="list-style-type: none"> Administrador local (somente para grupos de trabalho) <p>Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local integrado no sistema em que você está instalando o plug-in SnapCenter . Você pode especificar uma conta de usuário local que pertença ao grupo de administradores locais se a conta de usuário tiver privilégios elevados ou se o recurso de Controle de Acesso do Usuário estiver desabilitado no sistema host. O formato válido para o campo Nome de usuário é: <i>UserName</i></p>
Senha	Digite a senha usada para autenticação.
Tipo de autenticação	Selecione o tipo de autenticação que você deseja usar.
Use privilégios sudo	<p>Marque a caixa de seleção Usar privilégios sudo se estiver criando credenciais para um usuário não root.</p> <div>  <p>Aplicável somente a usuários de Linux e AIX.</p> </div>

5. Clique em **OK**.

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

Configurar o gMSA no Windows Server 2016 ou posterior

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

Antes de começar

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

Passos

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

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

Por exemplo,

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

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

Para fazer isso, execute o seguinte comando no PowerShell:

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

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

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

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- Reinicie seu host.
 - Instale o gMSA no seu host executando o seguinte comando no prompt de comando do PowerShell:
`Install-AdServiceAccount <gMSA>`
 - Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`
- Atribua privilégios administrativos ao gMSA configurado no host.
 - Adicione o host do Windows especificando a conta gMSA configurada no SnapCenter Server.

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

Instalar os plug-ins suportados pela NetApp

Adicionar hosts e instalar pacotes de plug-ins em hosts remotos

Você deve usar a página Adicionar Host do SnapCenter para adicionar hosts e, em seguida, instalar os pacotes de plug-in. Os plug-ins são instalados automaticamente nos hosts remotos. Você pode adicionar um host e instalar os pacotes de plug-in para um host individual ou para um cluster.

Antes de começar

- Você deve ser um usuário atribuído a uma função que tenha permissões de instalação e desinstalação de plug-ins, como a função de administrador do SnapCenter .
- Você deve garantir que o serviço de enfileiramento de mensagens esteja em execução.
- Se estiver usando uma conta de serviço gerenciada em grupo (gMSA), você deverá configurar a gMSA com privilégios administrativos.

["Configurar conta de serviço gerenciada de grupo no Windows Server 2016 ou posterior para aplicativos personalizados"](#)



- Para o host Windows, você deve garantir que selecionou o SnapCenter Plug-in para Windows.


Sobre esta tarefa

- Não é possível adicionar um SnapCenter Server como um host de plug-in a outro SnapCenter Server.
- Se você instalar plug-ins em um cluster (WSFC), os plug-ins serão instalados em todos os nós do cluster.

Passos

1. No painel de navegação esquerdo, selecione **Hosts**.
2. Verifique se a aba **Hosts Gerenciados** está selecionada na parte superior.
3. Selecione **Adicionar**.
4. Na página Hosts, execute as seguintes ações:

Para este campo...	Faça isso...
Tipo de host	<p>Selecione o tipo de host:</p> <ul style="list-style-type: none"> • Windows • Linux • AIX <div>  Os plug-ins suportados pela NetApp podem ser usados em ambientes Windows, Linux e AIX. </div> <div>  Aplicativos de armazenamento e Oracle são suportados no AIX. </div>
Nome do host	<p>Digite o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host.</p> <p>O SnapCenter depende da configuração correta do DNS. Portanto, a melhor prática é inserir o FQDN.</p> <p>Para ambientes Windows, o endereço IP é suportado para hosts de domínio não confiáveis somente se for resolvido para o FQDN.</p> <p>Você pode inserir os endereços IP ou FQDN de um host autônomo.</p> <p>Se você estiver adicionando um host usando o SnapCenter e o host fizer parte de um subdomínio, você deverá fornecer o FQDN.</p>


Para este campo...	Faça isso...
Credenciais	<p>Selecione o nome da credencial que você criou ou crie novas credenciais.</p> <p>As credenciais devem ter direitos administrativos no host remoto. Para obter detalhes, consulte as informações sobre como criar credenciais.</p> <p>Você pode visualizar detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você especificou.</p> <div>  <p>O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar Host.</p> </div>



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

Você pode instalar os seguintes plug-ins da lista:

- MongoDB
- ORASCPM (exibido como Aplicativos Oracle)
- SAP ASE
- SAP MaxDB
- Armazenar

6. (Opcional) Selecione **Mais opções** para instalar os outros plug-ins.

Para este campo...	Faça isso...
Porta	<p>Mantenha o número da porta padrão ou especifique o número da porta.</p> <p>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.</p> <div>  <p>Se você instalou manualmente os plug-ins e especificou uma porta personalizada, deverá especificar a mesma porta. Caso contrário, a operação falhará.</p> </div>

Para este campo...	Faça isso...
Caminho de instalação	<p>Os plug-ins suportados pela NetApp podem ser instalados em um sistema Windows ou Linux.</p> <ul style="list-style-type: none"> Para o pacote de plug-ins SnapCenter para Windows, o caminho padrão é C:\Arquivos de Programas\ NetApp\ SnapCenter. <p>Opcionalmente, você pode personalizar o caminho.</p> <ul style="list-style-type: none"> Para o pacote de plug-ins SnapCenter para Linux e o pacote de plug-ins SnapCenter para AIX, o caminho padrão é /opt/NetApp/snapcenter . <p>Opcionalmente, você pode personalizar o caminho.</p>
Ignorar verificações de pré-instalação	<p>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.</p>
Use a conta de serviço gerenciada em grupo (gMSA) para executar os serviços do plug-in	<p>Para o host Windows, marque esta caixa de seleção se desejar usar a Conta de Serviço Gerenciada em Grupo (gMSA) para executar os serviços do plug-in.</p> <div>  <p>Forneça o nome do gMSA no seguinte formato: domainName\accountName\$.</p> </div> <div>  <p>O gMSA será usado como uma conta de serviço de logon somente para o serviço SnapCenter Plug-in para Windows.</p> </div>

7. Selecione **Enviar**.

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

Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado em C:\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 SnapManager.Web.UI.dll.config, deverá atualizar o arquivo em ambos os nós e reiniciar o SnapCenter App Pool.

O caminho padrão do Windows é `C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config`

O caminho padrão do Linux é

`/opt/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config`

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



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/registros`.

Instalar pacotes de plug-in SnapCenter para Linux, Windows ou AIX em vários hosts remotos usando cmdlets

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

Antes de começar

O usuário que adiciona um host deve ter direitos administrativos no host.



Aplicativos de armazenamento e Oracle são suportados no AIX.

Passos

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

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando `Get-Help command_name`. Alternativamente, você também pode consultar o ["Guia de referência do cmdlet do software SnapCenter"](#).

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

4. Insira suas credenciais para instalação remota.

Instale os plug-ins suportados pela NetApp em hosts Linux usando a interface de linha de comando

Você deve instalar os plug-ins suportados NetApp usando a interface de usuário (IU) do SnapCenter. Se o seu ambiente não permitir a instalação remota do plug-in pela interface do usuário do SnapCenter, você poderá instalar os plug-ins suportados NetApp

no modo de console ou no modo silencioso usando a interface de linha de comando (CLI).

Passos

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

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

2. No prompt de comando, navegue até o diretório onde você copiou o arquivo de instalação.
3. Instale o plug-in: `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`
 - -DPORT especifica a porta de comunicação HTTPS do SMCORE.
 - -DSERVER_IP especifica o endereço IP do SnapCenter Server.
 - -DSERVER_HTTPS_PORT especifica a porta HTTPS do SnapCenter Server.
 - -DUSER_INSTALL_DIR especifica o diretório onde você deseja instalar o pacote de plug-ins do SnapCenter para Linux.
 - _DINSTALL_LOG_NAME especifica o nome do arquivo de log.

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

4. Adicione o host ao SnapCenter Server usando o cmdlet Add-Smhost e os parâmetros necessários.

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

5. Efetue login no SnapCenter e carregue o plug-in compatível com NetApp a partir da interface do usuário ou usando cmdlets do PowerShell.

Você pode carregar o plug-in compatível com NetApp a partir da IU consultando "[Adicionar hosts e instalar pacotes de plug-ins em hosts remotos](#)" seção.

A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm mais informações sobre cmdlets do PowerShell.

"[Guia de referência do cmdlet do software SnapCenter](#)".






Monitore o status da instalação de plug-ins compatíveis com a NetApp

Você pode monitorar o progresso da instalação do pacote de plug-in SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento da instalação para determinar

quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

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

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

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Trabalhos**, para filtrar a lista de modo que apenas as operações de instalação de plug-ins sejam listadas, faça o seguinte:
 - a. Clique em **Filtrar**.
 - b. Opcional: especifique a data de início e término.
 - c. No menu suspenso Tipo, selecione **Instalação de plug-in**.
 - d. No menu suspenso Status, selecione o status da instalação.
 - e. Clique em **Aplicar**.
4. Selecione o trabalho de instalação e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

Configurar certificado CA

Gerar arquivo CSR de certificado CA

Você pode gerar uma Solicitação de Assinatura de Certificado (CSR) e importar o certificado que pode ser obtido de uma Autoridade de Certificação (CA) usando o CSR gerado. O certificado terá uma chave privada associada a ele.

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



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

Para obter informações sobre como gerar um CSR, consulte ["Como gerar um arquivo CSR de certificado CA"](#).



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

Para configurações de cluster, o nome do cluster (FQDN do cluster virtual) e os respectivos nomes de host

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

Importar certificados de CA

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

Passos

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo > Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
4. Clique em **Console Root > Certificados – Computador local > Autoridades de certificação raiz confiáveis > Certificados**.
5. Clique com o botão direito do mouse na pasta “Autoridades de Certificação Raiz Confiáveis” e selecione **Todas as Tarefas > Importar** para iniciar o assistente de importação.
6. Conclua o assistente da seguinte forma:

Nesta janela do assistente...	Faça o seguinte...
Importar chave privada	Selecione a opção Sim , importe a chave privada e clique em Avançar .
Formato de arquivo de importação	Não faça alterações; clique em Avançar .
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em Avançar .
Concluindo o Assistente de Importação de Certificados	Revise o resumo e clique em Concluir para iniciar a importação.



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

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

Obtenha a impressão digital do certificado CA

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

Passos

1. Execute o seguinte na GUI:
 - a. Clique duas vezes no certificado.

- b. Na caixa de diálogo Certificado, clique na guia **Detalhes**.
- c. Percorra a lista de campos e clique em **Impressão digital**.
- d. Copie os caracteres hexadecimais da caixa.
- e. Remova os espaços entre os números hexadecimais.

Por exemplo, se a impressão digital for: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", após remover os espaços, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:

- a. Execute o seguinte comando para listar a impressão digital do certificado instalado e identificar o certificado instalado recentemente pelo nome do assunto.

```
Get-ChildItem -Path Cert:\LocalMachine\My
```

- b. Copie a impressão digital.

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

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

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

Passos

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

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

Por exemplo:

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

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

Por exemplo:

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

Configurar o certificado CA para o serviço de plug-ins suportados pela NetApp no host Linux

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

Os plug-ins usam o arquivo 'keystore.jks', que está localizado em `/opt/NetApp/snapcenter/scc/etc` como seu armazenamento confiável e armazenamento de chaves.

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

Passos

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

É o valor correspondente à chave 'KEYSTORE_PASS'.

2. Alterar a senha do keystore:

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

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

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

3. Reinicie o serviço após alterar a senha.



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

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

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

Passos

1. Navegue até a pasta que contém o keystore do plug-in: `/opt/NetApp/snapcenter/scc/etc`.
2. Localize o arquivo 'keystore.jks'.

3. Listar os certificados adicionados no keystore:

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

4. Adicione um certificado raiz ou intermediário:

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks  
. Reinicie o serviço após configurar os certificados raiz ou  
intermediários para conectar o trust-store.
```



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

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

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

Passos

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

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

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

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

5. Listar os certificados adicionados no keystore.

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

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

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

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



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

Atualize este valor em relação à chave SCC_CERTIFICATE_ALIAS.

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

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

Sobre esta tarefa

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

Passos

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

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

Configurar o certificado CA para o serviço de plug-ins suportados pela NetApp no host Windows

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

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

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

Passos

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

É o valor correspondente à chave *KEYSTORE_PASS*.

2. Alterar a senha do keystore:

```
keytool -storepasswd -keystore keystore.jks
```



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

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

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

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

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

4. Reinicie o serviço após alterar a senha.



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

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

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

Passos

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

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

4. Adicione um certificado raiz ou intermediário:

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. Reinicie o serviço após configurar os certificados raiz ou intermediários para conectar o trust-store.



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

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

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

Passos

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

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

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

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

5. Listar os certificados adicionados no keystore.

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

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

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

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

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

Atualize este valor em relação à chave `SCC_CERTIFICATE_ALIAS`.

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

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

Sobre esta tarefa

- Para baixar o arquivo CRL mais recente para o certificado CA relacionado, consulte ["Como atualizar o arquivo de lista de revogação de certificados no SnapCenter CA Certificate"](#).
- Os plug-ins do SnapCenter procurarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL dos plug-ins do SnapCenter é `'C:\Arquivos de Programas\NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl'`.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo `agent.properties` em relação à chave `CRL_PATH`.
2. Você pode colocar mais de um arquivo CRL neste diretório.

Os certificados recebidos serão verificados em relação a cada CRL.

Habilitar certificados CA para plug-ins

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

Antes de começar

- Você pode habilitar ou desabilitar os certificados da CA usando o cmdlet run `Set-SmCertificateSettings`.
- Você pode exibir o status do certificado para os plug-ins usando `Get-SmCertificateSettings`.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando `Get-Help command_name`. Alternativamente, você também pode consultar o ["Guia de referência do cmdlet do software SnapCenter"](#).





Passos

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

5. Selecione **Ativar validação de certificado**.

Depois que você terminar

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

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



Quando o status é amarelo ou verde, as operações de proteção de dados foram concluídas com sucesso.

Prepare-se para a proteção de dados

Pré-requisitos para usar os plug-ins suportados pela NetApp

Antes de usar os plug-ins suportados SnapCenter NetApp , o administrador do SnapCenter deve instalar e configurar o SnapCenter Server e executar as tarefas de pré-requisito.

- Instalar e configurar o SnapCenter Server.
- Efetue login no SnapCenter Server.
- Configure o ambiente SnapCenter adicionando conexões do sistema de armazenamento e criando credenciais, se aplicável.
- Adicione hosts, instale e carregue os plug-ins.
- Se aplicável, instale o Java 11 no host do plug-in.
- Se você tiver vários caminhos de dados (LIFs) ou uma configuração dNFS, poderá executar o seguinte usando a CLI do SnapCenter no host do banco de dados:
 - Por padrão, todos os endereços IP do host do banco de dados são adicionados à política de exportação de armazenamento NFS na máquina virtual de armazenamento (SVM) para os volumes clonados. Se você quiser ter um endereço IP específico ou restringir a um subconjunto de endereços IP, execute a CLI `Set-PreferredHostIPsInStorageExportPolicy`.
 - Se você tiver vários caminhos de dados (LIFs) em SVMs, o SnapCenter escolherá o caminho de dados (LIF) apropriado para montar o volume clonado NFS. No entanto, se você quiser especificar um caminho de dados específico (LIF), deverá executar a CLI `Set-SvmPreferredDataPath`. 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"](#) .
- Configure o SnapMirror e o SnapVault se desejar replicação de backup.
- Certifique-se de que a porta 9090 não esteja sendo usada por nenhum outro aplicativo no host.

A porta 9090 deve ser reservada para uso por plug-ins suportados NetApp , além das outras portas exigidas pelo SnapCenter.

Como recursos, grupos de recursos e políticas são usados para proteger recursos de plug-in com suporte da NetApp

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

- Os recursos geralmente são bancos de dados, sistemas de arquivos do Windows ou VMs que você faz backup ou clona com o SnapCenter.
- Um grupo de recursos do SnapCenter é uma coleção de recursos em um host ou cluster.

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

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

- As políticas especificam a frequência de backup, retenção de cópias, replicação, scripts e outras características das operações de proteção de dados.

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

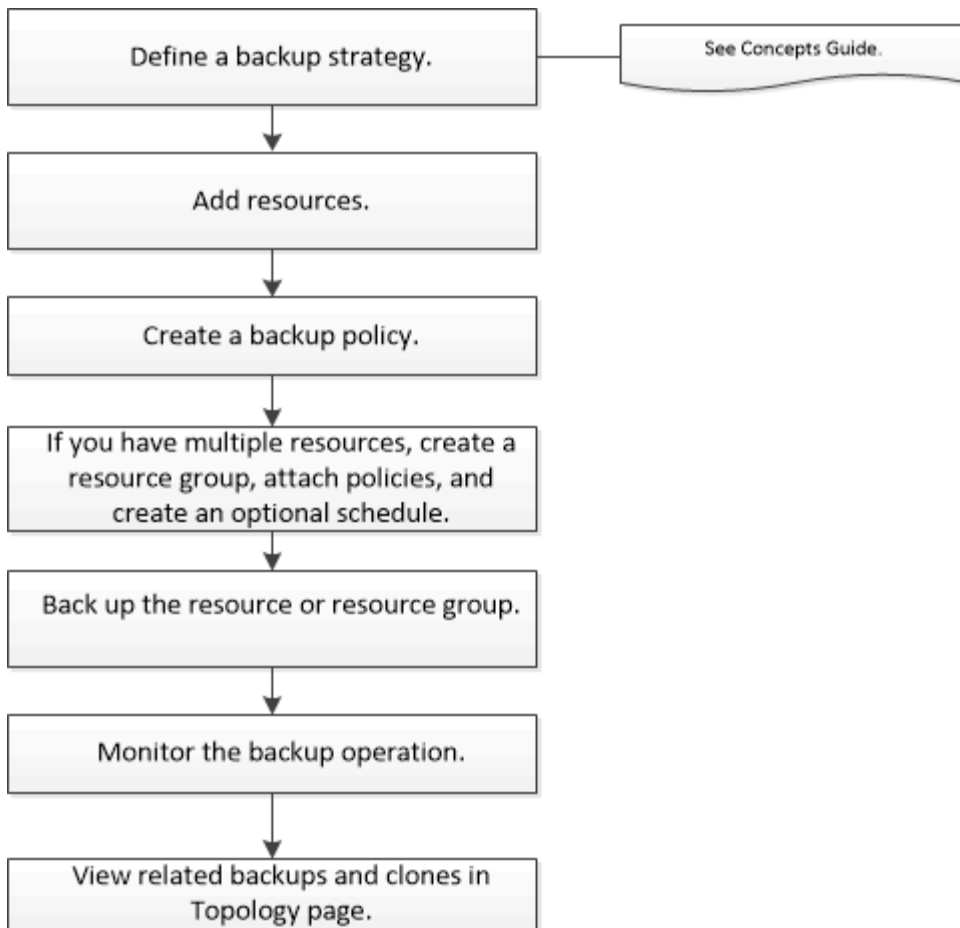
Pense em um grupo de recursos como definidor de *o que* você quer proteger e quando quer proteger em termos de dia e hora. Pense em uma política como a definição de *como* você quer protegê-la. Se você estiver fazendo backup de todos os bancos de dados ou de todos os sistemas de arquivos de um host, por exemplo, poderá criar um grupo de recursos que inclua todos os bancos de dados ou todos os sistemas de arquivos no host. Você pode então anexar duas políticas ao grupo de recursos: uma política diária e uma política horária. Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup baseado em arquivo diariamente e outra programação que executa um backup baseado em instantâneo a cada hora.

Faça backup dos recursos de plug-ins suportados pela NetApp

Faça backup dos recursos de plug-ins suportados pela NetApp

O fluxo de trabalho de backup inclui planejamento, identificação de recursos para backup, gerenciamento de políticas de backup, criação de grupos de recursos e anexação de políticas, criação de backups e monitoramento das operações.

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



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. Para obter informações detalhadas sobre cmdlets do PowerShell, use a ajuda do cmdlet do SnapCenter ou consulte o ["Guia de referência do cmdlet do software SnapCenter"](#)

Adicionar recursos aos plug-ins suportados pela NetApp

Você deve adicionar os recursos que deseja fazer backup ou clonar. Dependendo do seu ambiente, os recursos podem ser instâncias de banco de dados ou coleções que você deseja fazer backup ou clonar.

Antes de começar


- Você deve ter concluído tarefas como instalar o SnapCenter Server, adicionar hosts, criar conexões do sistema de armazenamento e adicionar credenciais.
- Você deve ter carregado os plug-ins no SnapCenter Server.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Adicionar Recurso**.
3. Na página Fornecer detalhes do recurso, execute as seguintes ações:

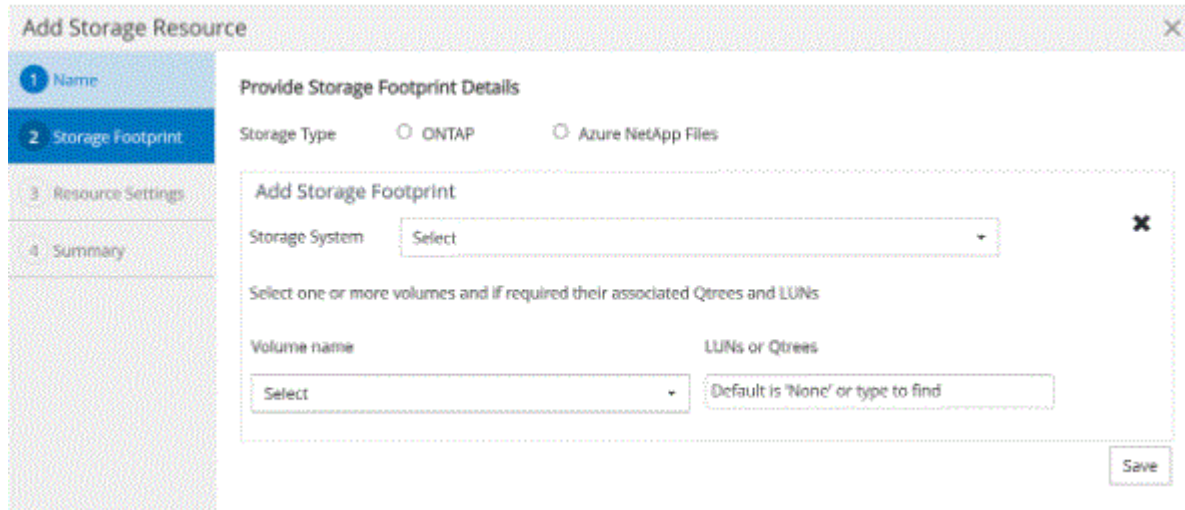
Para este campo...	Faça isso...
Nome	Digite o nome do recurso.
Nome do host	Selecione o host.
Tipo	<p>Selecione o tipo. O tipo é definido pelo usuário conforme o arquivo de descrição do plug-in. Por exemplo, banco de dados e instância.</p> <p>Caso o tipo selecionado tenha um pai, insira os detalhes do pai. Por exemplo, se o tipo for Banco de Dados e o pai for Instância, insira os detalhes da Instância.</p>
Nome da credencial	Selecione Credencial ou crie uma nova credencial.
Caminhos do Monte	Insira os caminhos de montagem onde o recurso está montado. Isso é aplicável somente para um host Windows.

4. Na página Fornecer espaço de armazenamento, selecione um sistema de armazenamento e escolha um ou mais volumes, LUNs e qtrees e, em seguida, selecione **Salvar**.

Opcional: Selecione o  ícone para adicionar mais volumes, LUNs e qtrees de outros sistemas de armazenamento.



Os plug-ins suportados pela NetApp não oferecem suporte à descoberta automática de recursos. Os detalhes de armazenamento de ambientes físicos e virtuais também não são descobertos automaticamente. Você deve fornecer as informações de armazenamento para ambientes físicos e virtuais ao criar os recursos.



5. Na página Configurações de recursos, forneça pares de chave-valor personalizados para o recurso.



Certifique-se de que o nome das chaves personalizadas esteja em letras maiúsculas.

Resource settings ⓘ

Para os respectivos parâmetros do plug-in, consulte "[Parâmetros para configurar o recurso](#)"

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

Resultado

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



Você deve atualizar os recursos se os bancos de dados forem renomeados fora do SnapCenter.

Depois que você terminar

Se você quiser fornecer acesso aos ativos a outros usuários, o administrador do SnapCenter deverá atribuir ativos a esses usuários. Isso permite que os usuários executem as ações para as quais têm permissão nos ativos atribuídos a eles.

Depois de adicionar os recursos, você pode modificar os detalhes dos recursos. Se um recurso de plug-ins suportado NetApp tiver backups associados a ele, os seguintes campos não poderão ser modificados: nome do recurso, tipo de recurso e nome do host.

Parâmetros para configurar o recurso

Se estiver adicionando os plug-ins manualmente, você poderá usar os seguintes parâmetros para configurar o recurso na página Configurações do recurso.

Plug-in para MongoDB

Configurações de recursos:

- MONGODB_APP_SERVER=(para tipo de recurso como cluster fragmentado) ou MONGODB_REPLICASET_SERVER=(para tipo de recurso como replicaset)
- OPLOG_PATH=(Parâmetro opcional caso seja fornecido pelo MongoDB.propertiesfile)
- MONGODB_AUTHENTICATION_TYPE= (PLAIN para autenticação LDAP e None para outros)

Você deve fornecer os seguintes parâmetros que precisam ser fornecidos no arquivo MongoDB.properties:

- DESATIVAR_INICIAR_PARAR_SERVIÇOS=
 - N se os serviços de início/parada forem executados pelo plug-in.
 - Y se os serviços de início/parada forem executados pelo usuário.

- O parâmetro opcional como valor padrão é definido como N.
- OPLOG_PATH_ = (Parâmetro opcional caso já seja fornecido como par chave-valor personalizado no SnapCenter).

Plug-in para MaxDB

Configurações de recursos:

- XUSER_ENABLE (S|N) habilita ou desabilita o uso de um xuser para MaxDB para que uma senha não seja necessária para o usuário do banco de dados.
- HANDLE_LOGWRITER (S|N) executa operações de suspensão do logwriter (N) ou retomada do logwriter (S).
- DBMCLICMD (path_to_dbmcli_cmd) especifica o caminho para o comando MaxDB dbmcli. Se não for definido, dbmcli será usado no caminho de pesquisa.



Para o ambiente Windows, o caminho deve estar entre aspas duplas ("...").

- SQLCLICMD (path_to_sqlcli_cmd) especifica o caminho para o comando sqlcli do MaxDB. Se o caminho não estiver definido, sqlcli será usado no caminho de pesquisa.
- MAXDB_UPDATE_HIST_LOG (S|N) instrui o programa de backup do MaxDB sobre se ele deve atualizar o log de histórico do MaxDB.
- MAXDB_CHECK_SNAPSHOT_DIR: Exemplo, SID1:directory[,directory...]; [SID2:directoary[,directory...]] verifica se uma operação de cópia do Snap Creator Snapshot foi bem-sucedida e garante que o snapshot seja criado.

Isso se aplica somente ao NFS. O diretório deve apontar para o local que contém o diretório .snapshot. Vários diretórios podem ser incluídos em uma lista separada por vírgulas.

No MaxDB 7.8 e versões posteriores, a solicitação de backup do banco de dados é marcada como Falha no histórico de backup.

- MAXDB_BACKUP_TEMPLATES: Especifica um modelo de backup para cada banco de dados.

O modelo deve existir e ser um tipo externo de modelo de backup. Para habilitar a integração de snapshots para o MaxDB 7.8 e versões posteriores, você deve ter a funcionalidade do servidor em segundo plano do MaxDB e o modelo de backup do MaxDB já configurado do tipo EXTERNAL.

- MAXDB_BG_SERVER_PREFIX: Especifica o prefixo para o nome do servidor em segundo plano.

Se o parâmetro MAXDB_BACKUP_TEMPLATES estiver definido, você também deverá definir o parâmetro MAXDB_BG_SERVER_PREFIX. Se você não definir o prefixo, o valor padrão na_bg_ será usado.

Plug-in para SAP ASE

Configurações de recursos:

- SYBASE_SERVER (data_server_name) especifica o nome do servidor de dados Sybase (opção -S no comando isql). Por exemplo, p_test.
- SYBASE_DATABASES_EXCLUDE (db_name) permite que bancos de dados sejam excluídos se a construção "ALL" for usada.

Você pode especificar vários bancos de dados usando uma lista separada por ponto e vírgula. Por exemplo: pubs2;test_db1.

- SYBASE_USER: user_name especifica o usuário do sistema operacional que pode executar o comando isql.

Obrigatório para UNIX. Este parâmetro é necessário se o usuário que executa os comandos iniciar e parar do Snap Creator Agent (geralmente o usuário root) e o usuário que executa o comando isql forem diferentes.

- SYBASE_TRAN_DUMP db_name:directory_path permite que você execute um dump de transação do Sybase após criar um snapshot. Por exemplo, pubs2:/sybasedumps/ pubs2

Você deve especificar cada banco de dados que requer um despejo de transação.

- SYBASE_TRAN_DUMP_COMPRESS (S|N) habilita ou desabilita a compactação de despejo de transações nativas do Sybase.
- SYBASE_ISQL_CMD (por exemplo, /opt/sybase/OCS-15_0/bin/isql) define o caminho para o comando isql.
- SYBASE_EXCLUDE_TEMPDB (S|N) permite que você exclua automaticamente bancos de dados temporários criados pelo usuário.

Plug-in para aplicativos Oracle (ORASCPM)

Configurações de recursos:

- SQLPLUS_CMD especifica o caminho para SQLplus.
- ORACLE_DATABASES lista os bancos de dados Oracle a serem copiados e o usuário correspondente (banco de dados:usuário).
- CNTL_FILE_BACKUP_DIR especifica o diretório para backup do arquivo de controle.
- ORA_TEMP especifica o diretório para arquivos temporários.
- ORACLE_HOME especifica o diretório onde o software Oracle está instalado.
- ARCHIVE_LOG_ONLY especifica se os logs de arquivamento devem ser feitos ou não.
- ORACLE_BACKUPMODE especifica se o backup deve ser executado online ou offline.
- ORACLE_EXPORT_PARAMETERS especifica se as variáveis de ambiente definidas acima devem ser reexportadas durante a execução de `/bin/su <usuário executando sqlplus> -c sqlplus /nolog <cmd>`. Este é normalmente o caso quando o usuário que está executando o sqlplus não definiu todas as variáveis de ambiente necessárias para se conectar ao banco de dados usando `connect / as sysdba`.

Criar políticas para recursos de plug-in suportados NetApp

Antes de usar o SnapCenter para fazer backup de recursos específicos do plug-in suportados NetApp , você deve criar uma política de backup para o recurso ou grupo de recursos do qual deseja fazer backup.

Antes de começar

- Você deve ter definido sua estratégia de backup.

Para obter detalhes, consulte as informações sobre como definir uma estratégia de proteção de dados para plug-ins compatíveis com NetApp .

- Você deveria estar preparado para a proteção de dados.

A preparação para a proteção de dados inclui tarefas como instalar o SnapCenter, adicionar hosts, criar conexões de sistema de armazenamento e adicionar recursos.

- As máquinas virtuais de armazenamento (SVMs) devem ser atribuídas a você para operações de espelhamento ou cofre.

O administrador do SnapCenter deve ter atribuído as SVMs para os volumes de origem e destino a você se estiver replicando Snapshots para um espelho ou cofre.

- Você deve ter adicionado manualmente os recursos que deseja proteger.

Sobre esta tarefa

- Uma política de backup é um conjunto de regras que regem como você gerencia, agenda e mantém backups. Além disso, você pode especificar configurações de replicação, script e aplicativo.
- Especificar opções em uma política economiza tempo quando você deseja reutilizar a política para outro grupo de recursos.
- 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 .



As configurações primárias do SnapLock são gerenciadas na política de backup do SnapCenter e as configurações secundárias do SnapLock são gerenciadas pelo ONTAP.

Passos

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

Você pode fornecer vários valores-chave a serem passados ao plug-in.
6. Na página Snapshot e Replicação, execute as seguintes etapas:
 - a. Especifique o tipo de programação selecionando **Sob demanda**, **Por hora**, **Diário**, **Semanal** ou **Mensal**.





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



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

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

Se você quiser...	Então...
Mantenha um certo número de Snapshots	<p>Selecione Cópias a serem mantidas e especifique o número de Snapshots que você deseja manter.</p> <p>Se o número de Snapshots exceder o número especificado, os Snapshots serão excluídos, com as cópias mais antigas sendo excluídas primeiro.</p> <div>  <p>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.</p> </div> <div>  <p>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 .</p> </div>
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	<p>Selecione Período de bloqueio de cópia de instantâneo e especifique dias, meses ou anos.</p> <p>O período de retenção do SnapLock deve ser inferior a 100 anos.</p>

b. Selecione um rótulo de política.



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

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

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

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



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

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

Crie grupos de recursos e anexe políticas

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

Passos

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

Para este campo...	Faça isso...
Nome	<p>Insira um nome para o grupo de recursos.</p> <p>Observação: o nome do grupo de recursos não deve exceder 250 caracteres.</p>
Etiquetas	<p>Insira um ou mais rótulos que ajudarão você a pesquisar posteriormente o grupo de recursos.</p> <p>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.</p>
Use formato de nome personalizado para cópia do Snapshot	<p>Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.</p> <p>Por exemplo, <i>customtext_resource group_policy_hostname</i> ou <i>resource group_hostname</i>. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.</p>

4. Opcional: Na página Recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Tipo de recurso**.

Isso ajuda a filtrar informações na tela.

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

- a. Selecione a seta Backups para definir opções adicionais de backup:

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

Para este campo...	Faça isso...
Permitir tempo de espera para que a operação do Consistency Group Snapshot seja concluída	<p>Selecione Urgente, Médio ou Relaxado para especificar o tempo de espera para a conclusão da operação de Snapshot.</p> <p>Urgente = 5 segundos, Médio = 7 segundos e Relaxado = 20 segundos.</p>
Desativar sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL .

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

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

Parâmetro	Contexto	Descrição
EXT_DE_LOG_DE_ARQUIVO	extensão_de_arquivo	<p>Especifica o comprimento da extensão do arquivo de log de arquivamento.</p> <p>Por exemplo, se o log de arquivamento for log_backup_0_0_0_0.161518551942 9 e se o valor file_extension for 5, a extensão do log manterá 5 dígitos, que é 16151.</p>
ARQUIVO_LOG_RECURSIVO_SE ARQUIVO	(S/N)	<p>Permite o gerenciamento de logs de arquivo dentro de subdiretórios.</p> <p>Você deve usar este parâmetro se os logs de arquivamento estiverem localizados em subdiretórios.</p>

- c. Selecione a seta **Ferramenta de Cópia de Instantâneo** para selecionar a ferramenta para criar Instantâneos:

Se você quiser...	Então...
SnapCenter para usar o plug-in para Windows e colocar o sistema de arquivos em um estado consistente antes de criar um Snapshot. Para recursos do Linux, esta opção não é aplicável.	<p>Selecione * SnapCenter com consistência do sistema de arquivos*.</p> <p>Esta opção não é aplicável ao SnapCenter Plug-in para banco de dados SAP HANA.</p>
SnapCenter para criar um instantâneo de nível de armazenamento	Selecione * SnapCenter sem consistência do sistema de arquivos*.
Para inserir o comando a ser executado no host para criar Snapshots.	Selecione Outro e insira o comando a ser executado no host para criar um Snapshot.

7. Na página Políticas, execute as seguintes etapas:

- a. Selecione uma ou mais políticas na lista suspensa.



Você também pode criar uma política selecionando *  *.

As políticas estão listadas na seção **Configurar agendamentos para políticas selecionadas**.

- b. Na coluna **Configurar agendamentos**, selecione *  * para a política que você deseja configurar.

- c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e selecione 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 lista suspensa **Preferências de e-mail** na página **Notificação**, selecione os cenários nos quais você deseja enviar os e-mails.

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

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

Crie grupos de recursos e habilite proteção secundária para recursos 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:

- Clique em **Carregar localizadores** para carregar os volumes SnapMirror ou SnapVault para realizar a verificação no armazenamento secundário.
- Clique  na coluna Configurar agendamentos para configurar o agendamento de verificação para todos os tipos de agendamento da política.
- 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.

- Selecione **Verificar no local secundário** para verificar seus backups no sistema de armazenamento secundário.
- 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-SmSmtServer do PowerShell.

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

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

Você deve criar uma conexão de máquina virtual de armazenamento (SVM) e uma credencial antes de usar cmdlets do PowerShell para executar operações de proteção de dados.

Antes de começar

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

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

- Os nomes dos sistemas de armazenamento devem ser exclusivos.

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

Passos

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

Este exemplo abre uma sessão do PowerShell:

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

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

Este exemplo cria uma nova conexão de sistema de armazenamento:

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

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

Este exemplo cria uma nova credencial chamada FinanceAdmin com credenciais do Windows:

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

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"](#).

Faça backup de recursos individuais de plug-ins suportados pela NetApp

Se um recurso de plug-in individual compatível com NetApp não fizer parte de nenhum grupo de recursos, você poderá fazer backup do recurso na página Recursos. Você pode

fazer backup do recurso sob demanda ou, se o recurso tiver uma política anexada e um agendamento configurado, os backups ocorrerão automaticamente de acordo com o agendamento.

Antes de começar

- Você deve ter criado uma política de backup.
- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.

Interface do usuário do SnapCenter

Passos

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

Clique  e selecione o nome do host e o tipo de recurso para filtrar os recursos. Você pode então clicar  para fechar o painel de filtro.

3. Clique no recurso que você deseja fazer backup.
4. Na página Recurso, se desejar usar um nome personalizado, marque a caixa de seleção **Usar formato de nome personalizado para cópia do Snapshot** e insira um formato de nome personalizado para o nome do Snapshot.

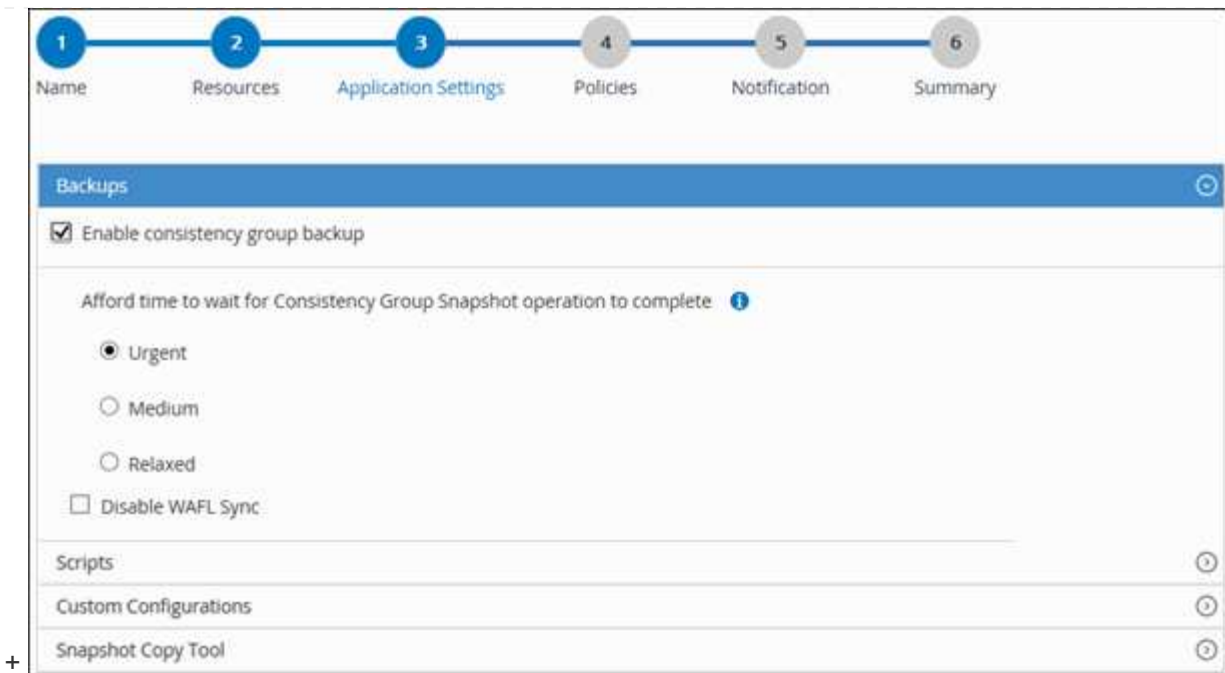
Por exemplo, *customtext_policy_hostname* ou *resource_hostname*. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

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

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

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

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



- a. Clique na seta **Scripts** para executar comandos pré e pós para operações de inatividade, instantâneo e ativação/desativação. Você também pode executar pré-comandos antes de sair da operação de backup.

Prescrições e pós-escritos são executados no SnapCenter Server.

- b. Clique na seta **Configurações personalizadas** e insira os pares de valores personalizados necessários para todos os trabalhos que usam este recurso.
- c. Clique na seta **Ferramenta de Cópia de Instantâneo** para selecionar a ferramenta para criar Instantâneos:

Se você quiser...	Então...
SnapCenter para tirar um instantâneo de nível de armazenamento	Selecione * SnapCenter sem consistência do sistema de arquivos*.
SnapCenter para usar o plug-in para Windows para colocar o sistema de arquivos em um estado consistente e, em seguida, tirar um instantâneo	Selecione * SnapCenter com consistência do sistema de arquivos*.
Para inserir o comando para criar um Snapshot	Selecione Outro e insira o comando para criar um Snapshot.

6. Na página Políticas, execute as seguintes etapas:


- a. Selecione uma ou mais políticas na lista suspensa.



Você também pode criar uma política clicando em  .

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

listadas.

- b. Clique  na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.
- c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

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

Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

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

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

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

A página de topologia de recursos é exibida.

9. Clique em **Fazer backup agora**.

10. Na página Backup, execute as seguintes etapas:

- a. Se você aplicou várias políticas ao recurso, na lista suspensa **Política**, selecione a política que deseja usar para backup.

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

- b. Clique em **Backup**.

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

Cmdlets do PowerShell

Passos

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

```
Open-smconnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146\
```

O prompt de nome de usuário e senha é exibido.

2. Adicione recursos usando o cmdlet Add-SmResources.

Este exemplo adiciona recursos:

```
Add-SmResource -HostName 'scc55.sscore.test.com' -PluginCode
'DummyPlugin' -ResourceName QDBVOL1 -ResourceType Database
-StorageFootPrint (
@{"VolumeName"="qtree_voll_scc55_sscore_test_com";"QTREENAME"="qtree
Voll";"StorageSystem"="vserver_scauto_primary"}) -Instance QTREE1
```

3. Crie uma política de backup usando o cmdlet Add-SmPolicy.

Este exemplo cria uma nova política de backup:

```
Add-SMPolicy -PolicyName 'test2' -PolicyType 'Backup'
-PluginPolicyType DummyPlugin -description 'testPolicy'
```

4. Adicione um novo grupo de recursos ao SnapCenter usando o cmdlet Add-SmResourceGroup.

Este exemplo cria um novo grupo de recursos com a política e os recursos especificados:

```
Add-SmResourceGroup -ResourceGroupName
'Verify_Backup_on_Multiple_Qtree_different_vserver_windows'
-Resources
@(@{"Host"="scc55.sscore.test.com";"Uid"="QTREE2";"PluginName"="Dummm
yPlugin"},@{"Host"="scc55.sscore.test.com";"Uid"="QTREE";"PluginName"
"="DummyPlugin"}) -Policies test2 -plugincode 'DummyPlugin'
-usesnapcenterwithoutfilesystemconsistency
```

5. Inicie uma nova tarefa de backup usando o cmdlet New-SmBackup.

```
New-SMBackup -DatasetName
Verify_Backup_on_Multiple_Qtree_different_vserver_windows -Policy
test2
```

6. Visualize o status do trabalho de backup usando o cmdlet Get-SmBackupReport.

Este exemplo exibe um relatório de resumo de todos os trabalhos que foram executados na data especificada:

```
Get-SmBackupReport -JobId 149
```

```
BackedUpObjects      : {QTREE2, QTREE}
FailedObjects        : {}
IsScheduled          : False
HasMetadata          : False
SmBackupId           : 1
SmJobId              : 149
StartDateTime        : 1/15/2024 1:35:17 AM
EndDateTime          : 1/15/2024 1:36:19 AM
Duration             : 00:01:02.4265750
CreatedDateTime      : 1/15/2024 1:35:51 AM
Status               : Completed
ProtectionGroupName  :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows
SmProtectionGroupId  : 1
PolicyName           : test2
SmPolicyId           : 4
BackupName           :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows_scc55_01-
15-2024_01.35.17.4467
VerificationStatus    : NotApplicable
VerificationStatuses  :
SmJobError            :
BackupType            : SCC_BACKUP
CatalogingStatus      : NotApplicable
CatalogingStatuses    :
ReportDataCreatedDateTime :
PluginCode            : SCC
PluginName            : DummyPlugin
PluginDisplayName     : DummyPlugin
JobTypeId             :
JobHost               : scc55.sscore.test.com
```

Fazer backup de grupos de recursos de plug-ins suportados NetApp

Você pode fazer backup de um grupo de recursos sob demanda na página Recursos. Se um grupo de recursos tiver uma política anexada e um agendamento configurado, os backups ocorrerão automaticamente de acordo com o agendamento.



Antes de começar

- Você deve ter criado um grupo de recursos com uma política anexada.
- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com o armazenamento secundário, a função ONTAP atribuída ao usuário do armazenamento deve incluir o

privilegio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilegio “snapmirror all” não será necessário.

Passos

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

Você pode pesquisar o grupo de recursos inserindo o nome do grupo de recursos na caixa de pesquisa ou clicando em  e selecionando a tag. Você pode então clicar  para fechar o painel de filtro.

3. Na página Grupos de recursos, selecione o grupo de recursos que você deseja fazer backup e clique em **Fazer backup agora**.
4. Na página Backup, execute as seguintes etapas:
 - a. Se você tiver associado várias políticas ao grupo de recursos, na lista suspensa **Política**, selecione a política que deseja usar para backup.

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

- b. Clique em **Backup**.
5. Monitore o progresso da operação clicando em **Monitorar > Trabalhos**.
 - Nas configurações do MetroCluster, o SnapCenter pode não conseguir detectar um relacionamento de proteção após um failover.

["Não é possível detectar o relacionamento SnapMirror ou SnapVault após failover do MetroCluster"](#)






- Se você estiver fazendo backup de dados do aplicativo em VMDKs e o tamanho do heap Java para o SnapCenter Plug-in for VMware vSphere não for grande o suficiente, o backup poderá falhar. Para aumentar o tamanho do heap Java, localize o arquivo de script `/opt/netapp/init_scripts/scvservice`. Nesse roteiro, o `do_start method` O comando inicia o serviço de plug-in SnapCenter VMware. Atualize esse comando para o seguinte: `Java -jar -Xmx8192M -Xms4096M`.

Monitorar operações de backup de recursos de plug-in com suporte da NetApp

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.

Cancelar operações de backup para plug-ins compatíveis com NetApp


Você pode cancelar operações de backup que estão na fila.

O que você vai precisar

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

Passos

1. Execute uma das seguintes ações:

Do...	Ação
Página do monitor	<ol style="list-style-type: none"> No painel de navegação esquerdo, clique em Monitor > Trabalhos. Selecione a operação e clique em Cancelar trabalho.
Painel de atividades	<ol style="list-style-type: none"> Após iniciar a operação de backup, clique em  no painel Atividade para visualizar as cinco operações mais recentes. Selecione a operação. Na página Detalhes do trabalho, clique em Cancelar trabalho.





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

Exibir backups e clones relacionados a recursos de plug-ins suportados pela NetApp na página Topologia

Ao se preparar para fazer backup ou clonar um recurso, pode ser útil visualizar uma representação gráfica de todos os backups e clones no armazenamento primário e secundário. Na página Topologia, você pode ver todos os backups e clones disponíveis para o recurso ou grupo de recursos selecionado. Você pode visualizar os detalhes desses backups e clones e selecioná-los para executar operações de proteção de dados.

Sobre esta tarefa

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

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

Passos

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

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

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

A seção Cartão de Resumo exibe o número total de backups e clones.

Clicar no botão de atualização inicia uma consulta ao armazenamento para exibir uma contagem precisa.

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

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

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

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

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

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



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



Não é possível renomear os backups que estão no sistema de armazenamento primário.

7. Se você quiser excluir um clone, selecione o clone da tabela e clique em  para excluir o clone.

Restaurar recursos de plug-ins suportados pela NetApp

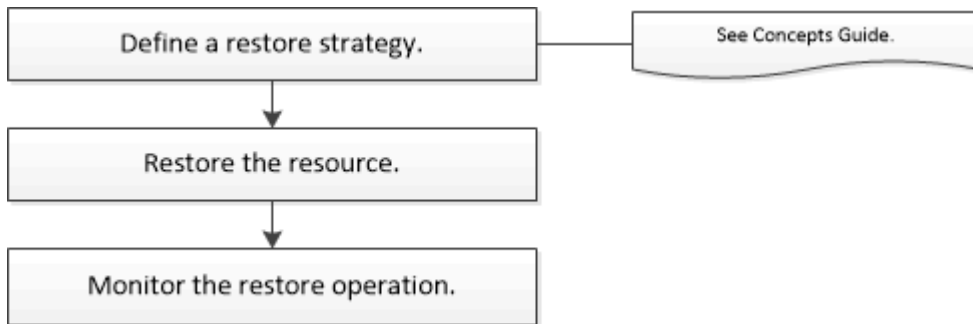
Restaurar recursos de plug-in suportados pelo NetApp

O fluxo de trabalho de restauração e recuperação inclui planejamento, execução de

operações de restauração e monitoramento das operações.

Sobre esta tarefa

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



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. Para obter informações sobre cmdlets do PowerShell, use a ajuda do cmdlet SnapCenter ou consulte o ["Guia de referência do cmdlet do software SnapCenter"](#).

Restaurar um backup de recurso

Você pode usar o SnapCenter para restaurar recursos. Os recursos das operações de restauração dependem do plug-in que você usa.

Antes de começar

- Você deve ter feito backup do recurso ou dos grupos de recursos.
- O administrador do SnapCenter deve ter atribuído a você as máquinas virtuais de armazenamento (SVMs) para os volumes de origem e de destino se você estiver replicando Snapshots para um espelho ou cofre.
- Você deve ter cancelado qualquer operação de backup que esteja em andamento para o recurso ou grupo de recursos que deseja restaurar.

Sobre esta tarefa

- A operação de restauração padrão restaura apenas objetos de armazenamento. As operações de restauração no nível do aplicativo só poderão ser executadas se o plug-in compatível com NetApp fornecer esse recurso.
- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock.

Interface do usuário do SnapCenter

Passos

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

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



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


Se o recurso não estiver protegido, *Não protegido* será exibido na coluna **Status geral**.

O status *Não protegido* na coluna **Status geral** pode significar que o recurso não está protegido ou que o recurso foi feito backup por um usuário diferente.

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

A página de topologia de recursos é exibida.

4. Na exibição **Gerenciar cópias**, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).

5. Na tabela de backup(s) primário(s), selecione o backup que deseja restaurar e clique em .



Backup Name	End Date
rg1_scspr0191683001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

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

- a. Se você selecionou **Recurso Completo**, o backup do recurso será restaurado.

Se o recurso contiver volumes ou qtrees como Storage Footprint, os Snapshots mais recentes nesses volumes ou qtrees serão excluídos e não poderão ser recuperados. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído.

- b. Se você selecionou **Nível de arquivo**, poderá selecionar **Todos** ou selecionar volumes ou qtrees e, em seguida, inserir o caminho relacionado aos volumes ou qtrees selecionados, separados por vírgulas.
 - Você pode selecionar vários volumes e qtrees.
 - Se o tipo de recurso for LUN, o LUN inteiro será restaurado. Você pode selecionar vários LUNs. + NOTA: Se você selecionar **Todos**, todos os arquivos nos volumes, qtrees ou LUNs serão restaurados.

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

realizar um trabalho de restauração.

8. Na página **Post ops**, insira os comandos mount e post restore para serem executados após realizar um trabalho de restauração.
9. Na página **Notificação**, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais deseja enviar os e-mails.

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

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

Cmdlets do PowerShell

Passos

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

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

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

Este exemplo exibe informações sobre todos os backups disponíveis:

```
PS C:\> Get-SmBackup
```

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

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

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

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

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

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

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

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







Monitorar operações de restauração de recursos de plug-in suportados NetApp

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


Sobre esta tarefa

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

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

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

Passos

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

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

Clonar backups de recursos de plug-ins suportados pelo NetApp

Clonar backups de recursos de plug-ins suportados pelo NetApp

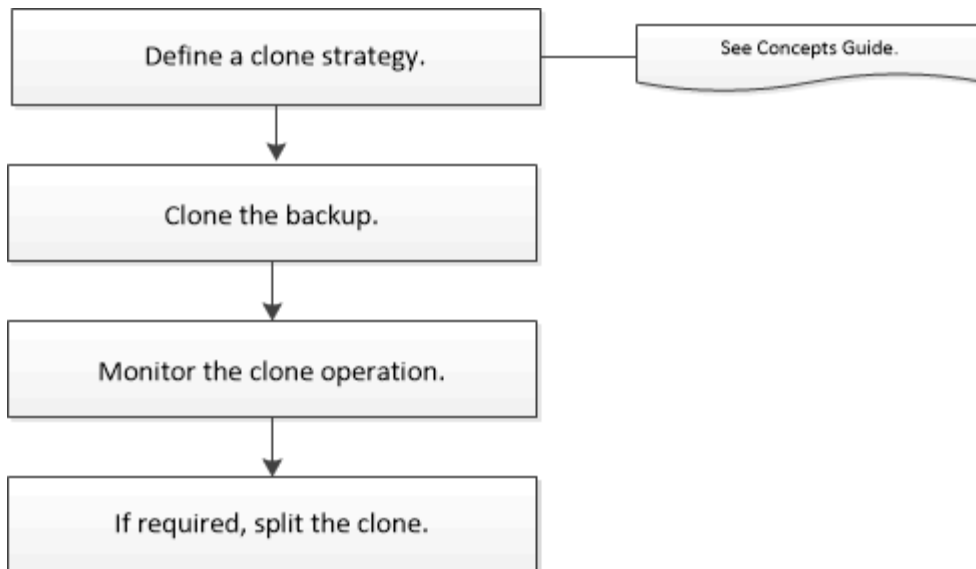
O fluxo de trabalho de clonagem inclui executar a operação de clonagem e monitorar a operação.

Sobre esta tarefa

Você pode clonar backups de recursos pelos seguintes motivos:

- Para testar a funcionalidade que deve ser implementada usando a estrutura e o conteúdo atuais dos recursos durante os ciclos de desenvolvimento do aplicativo
- Para ferramentas de extração e manipulação de dados ao preencher data warehouses
- Para recuperar dados que foram excluídos ou alterados por engano

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



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. Para obter informações detalhadas sobre cmdlets do PowerShell, use a ajuda do cmdlet do SnapCenter ou consulte o ["Guia de referência do cmdlet do software SnapCenter"](#) .

Clonar de um backup

Você pode usar o SnapCenter para clonar um backup. Você pode clonar a partir do backup primário ou secundário. Os recursos das operações de clonagem dependem do plug-in que você usa.

Antes de começar

- Você deve ter feito backup dos recursos ou do grupo de recursos.
- A operação de clonagem padrão clona apenas objetos de armazenamento. As operações de clonagem no nível do aplicativo só podem ser executadas se o plug-in compatível com o NetApp fornecer esse recurso.
- Você deve garantir que os agregados que hospedam os volumes estejam na lista de agregados atribuídos da máquina virtual de armazenamento (SVM).

Sobre esta tarefa

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

Interface do usuário do SnapCenter

Passos


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

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

3. Selecione o recurso ou grupo de recursos.

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

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

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Selecione o backup de dados da tabela e clique em .
6. Na página Locais, faça o seguinte:

Para este campo...	Faça isso...
Servidor clone	<p>Por padrão, o host de origem é preenchido.</p> <p>Se você quiser especificar um host diferente, selecione o host no qual o clone deve ser montado e o plug-in será instalado.</p>
Sufixo clone	<p>Isso é obrigatório quando o destino do clone é o mesmo que a origem.</p> <p>Insira um sufixo que será anexado ao nome do recurso recém-clonado. O sufixo garante que o recurso clonado seja exclusivo no host.</p> <p>Por exemplo, rs1_clone. Se você estiver clonando para o mesmo host do recurso original, deverá fornecer um sufixo para diferenciar o recurso clonado do recurso original; caso contrário, a operação falhará.</p>

Se o recurso selecionado for um LUN e você estiver clonando de um backup secundário, os volumes de destino serão listados. Uma única origem pode ter vários volumes de destino.

7. Na página **Configurações**, faça o seguinte:

Para este campo...	Faça isso...
Nome do iniciador	Digite o nome do iniciador do host, que pode ser um IQDN ou WWPN.

Para este campo...	Faça isso...
Protocolo Igroup	Selecione o protocolo Igroup.



A página de configurações será exibida somente se o tipo de armazenamento for LUN.

- Na página Scripts, insira os comandos para pré-clonagem ou pós-clonagem que devem ser executados antes ou depois da operação de clonagem, respectivamente. Digite o comando mount para montar um sistema de arquivos em um host.

Por exemplo:

- Comando pré-clone: exclui bancos de dados existentes com o mesmo nome
- Comando post clone: verifica um banco de dados ou inicia um banco de dados.

Comando de montagem para um volume ou qtree em uma máquina Linux:
`mount<VSERVER_NAME>:%<VOLUME_NAME_Clone /mnt>`

- Na página **Notificação**, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais 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.

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

Cmdlets do PowerShell

Passos

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

```
Open-SmConnection -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

- Liste os backups que podem ser clonados usando o cmdlet Get-SmBackup ou Get-SmResourceGroup.

Este exemplo exibe informações sobre todos os backups disponíveis:


```
C:\PS>PS C:\> Get-SmBackup
```

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

Este exemplo exibe informações sobre um grupo de recursos especificado:

```
PS C:\> Get-SmResourceGroup
```

```
Description :
CreationTime : 10/10/2016 4:45:53 PM
ModificationTime : 10/10/2016 4:45:53 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {}
HostResourceMaping : {}
Configuration :
SMCoreContracts.SmCloneConfiguration
LastBackupStatus : Completed
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo :
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Tag :
IsInternal : False
```

```

EnableEmailAttachment      : False
VerificationSettings       : {}
Name                       : NFS_DB
Type                       : Group
Id                         : 2
Host                       :
UserName                   :
Passphrase                 :
Deleted                    : False
Auth                      : SMCoreContracts.SmAuth
IsClone                    : False
CloneLevel                 : 0
Hosts                      :
StorageName                :
ResourceGroupNames        :
PolicyNames                :

Description                :
CreationTime               : 10/10/2016 4:51:36 PM
ModificationTime           : 10/10/2016 5:27:57 PM
EnableEmail                : False
EmailSMTPServer            :
EmailFrom                  :
EmailTo                    :
EmailSubject               :
EnableSysLog               : False
ProtectionGroupType        : Backup
EnableAsupOnFailure        : False
Policies                   : {}
HostResourceMapping        : {}
Configuration              :

SMCoreContracts.SmCloneConfiguration
LastBackupStatus           : Failed
VerificationServer         :
EmailBody                  :
EmailNotificationPreference : Never
VerificationServerInfo     :
SchedulerSQLInstance       :
CustomText                 :
CustomSnapshotFormat       :
SearchResources            : False
ByPassRunAs                : False
IsCustomSnapshot           :
MaintenanceStatus          : Production
PluginProtectionGroupTypes : {SMSQL}
Tag                        :

```

```

IsInternal           : False
EnableEmailAttachment : False
VerificationSettings : {}
Name                 : Test
Type                 : Group
Id                   : 3
Host                 :
UserName             :
Passphrase           :
Deleted              : False
Auth                 : SMCoreContracts.SmAuth
IsClone              : False
CloneLevel           : 0
Hosts                :
StorageName          :
ResourceGroupNames   :
PolicyNames          :

```

3. Inicie uma operação de clonagem de um grupo de recursos de clonagem ou de um backup existente usando o cmdlet `New-SmClone`.

Este exemplo cria um clone de um backup especificado com todos os logs:

```

New-SmClone -BackupName
Verify_delete_clone_on_qtree_windows_scc54_10-04-2016_19.05.48.0886
-Resources @{"Host"="scc54.sccore.test.com";"Uid"="QTREE1"} -
CloneToInstance scc54.sccore.test.com -Suffix '_QtreeCloneWin9'
-AutoAssignMountPoint -AppPluginCode 'DummyPlugin' -initiatorname
'iqn.1991-
05.com.microsoft:scc54.sccore.test.com' -igroupprotocol 'mixed'

```

4. Visualize o status do trabalho de clonagem usando o cmdlet `Get-SmCloneReport`.

Este exemplo exibe um relatório de clone para o ID do trabalho especificado:

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







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

Monitorar operações de clonagem de recursos de plug-in com suporte do NetApp

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

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

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

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

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

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

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

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

Informações sobre marcas comerciais

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