



Proteja aplicativos usando plug-ins compatíveis com NetApp

SnapCenter software

NetApp
February 20, 2026

Índice

Proteja aplicativos usando plug-ins compatíveis com NetApp	1
Plug-ins compatíveis com NetApp	1
Visão geral dos plug-ins compatíveis com NetApp	1
O que você pode fazer com os plug-ins compatíveis com o NetApp	1
Recursos de plug-ins compatíveis com NetApp	2
Tipos de storage compatíveis com plug-ins compatíveis com NetApp	3
Mínimo de ONTAP Privileges necessário para o plug-in compatível com NetApp	3
Preparar sistemas de storage para a replicação do SnapMirror e do SnapVault para plug-ins compatíveis com NetApp	6
Defina uma estratégia de backup	6
Estratégia de backup para plug-ins compatíveis com NetApp	7
Tipos de estratégias de restauração compatíveis com recursos de plug-in compatíveis com 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 Plug-ins para Windows, Linux ou AIX	9
Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Windows	13
Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Linux e AIX	14
Configurar credenciais para plug-ins compatíveis com NetApp	15
Configure o gMSA no Windows Server 2016 ou posterior	18
Instale os plug-ins suportados pelo NetApp	19
Configurar certificado CA	25
Preparar-se para a proteção de dados	33
Pré-requisitos para usar os plug-ins suportados pelo NetApp	33
Como os recursos, grupos de recursos e políticas são usados para proteger os recursos de plug-in compatíveis com o NetApp	33
Fazer backup de recursos de plug-ins compatíveis com NetApp	34
Fazer backup de recursos de plug-ins compatíveis com NetApp	34
Adicione recursos aos plug-ins compatíveis com NetApp	35
Criar políticas para recursos de plug-in compatíveis com o NetApp	39
Crie grupos de recursos e anexe políticas	43
Crie grupos de recursos e habilite a proteção secundária para recursos em sistemas ASA R2	47
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell	49
Fazer backup de recursos de plug-ins compatíveis com NetApp individuais	50
Fazer backup de grupos de recursos de plug-in compatíveis com o NetApp	56
Monitorar as operações de backup de recursos de plug-in compatíveis com NetApp	57
Cancelar operações de backup para plug-ins compatíveis com NetApp	58
Veja os backups e clones relacionados a recursos de plug-ins compatíveis com o NetApp na página topologia	59
Restaure os recursos de plug-ins compatíveis com o NetApp	60
Restaure os recursos de plug-in compatíveis com o NetApp	60
Restaurar um backup de recursos	61
Monitorar as operações de restauração de recursos de plug-in compatíveis com o NetApp	65

Clone NetApp compatível com backups de recursos de plug-ins	66
Clone NetApp compatível com backups de recursos de plug-ins	66
Clone de um backup	67
Monitorar as operações de clone de recurso de plug-in compatíveis com o NetApp	73

Proteja aplicativos usando plug-ins compatíveis com NetApp

Plug-ins compatíveis com NetApp

Visão geral dos plug-ins compatíveis com NetApp

Você pode usar os plug-ins compatíveis com o NetApp, como MongoDB, ORASCPM (aplicações Oracle), SAP ASE, SAP MaxDB e plug-in de storage para aplicativos que você usa e depois usa o SnapCenter para fazer backup, restauração ou clonagem desses aplicativos. Seus plug-ins compatíveis com NetApp atuam como componentes do lado do host do software NetApp SnapCenter, permitindo a proteção de dados com reconhecimento de aplicações e o gerenciamento de recursos.

Quando os plug-ins compatíveis com NetApp estão instalados, você pode usar a tecnologia SnapCenter com 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 disco para disco. Os plug-ins compatíveis com NetApp podem ser usados em ambientes Windows e Linux.



SnapCenterCLI não suporta comandos de plug-ins suportados pelo 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 incorporada ao SnapCenter.

Você pode instalar os plug-ins compatíveis com o NetApp na página Adicionar host.

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



A política de suporte do SnapCenter abrangerá o suporte à estrutura do plug-in, ao mecanismo principal e às APIs associadas. O suporte não abrangerá 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 compatíveis com o NetApp

Você pode usar os plug-ins compatíveis com NetApp, como MongoDB, ORASCPM, aplicações Oracle, SAP ASE, SAP MaxDB e plug-in de storage para operações de proteção de dados.

- Adicione recursos como bancos de dados, instâncias, documentos ou espaços de tabela.
- Criar backups.
- Restauração a partir de backups.
- Backups de clones.
- Agendar operações de backup.
- Monitore operações de backup, restauração e clone.
- Exibir relatórios para operações de backup, restauração e clone.

Você pode usar os plug-ins compatíveis com NetApp para operações de proteção de dados.

- Tire snapshots de grupos de consistência dos volumes de storage nos clusters do ONTAP.
- Faça backup de aplicativos personalizados usando a estrutura de script pré e pós integrada

Você pode fazer backup do volume ONTAP, LUN ou Qtree.

- Atualize os snapshots feitos no primário para um secundário ONTAP, aproveitando a relação de replicação existente (SnapVault/SnapMirror/replicação unificada) usando a política SnapCenter

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

- Recupere o volume, LUN ou arquivos completos do ONTAP.

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

A restauração de Qtree ou diretório não é suportada, mas você pode clonar e exportar apenas o Qtree se o escopo de backup estiver definido em um nível Qtree.

Recursos de plug-ins compatíveis com NetApp

O SnapCenter se integra à aplicação plug-in e às tecnologias NetApp no sistema de storage. Para trabalhar com plug-ins compatíveis com NetApp, como MongoDB, ORASCPM (aplicações Oracle), SAP ASE, SAP MaxDB e plug-in de storage, você usa a interface gráfica de usuário do SnapCenter.

- * Interface gráfica unificada do usuário*

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

- * Administração central automatizada*

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

- **Tecnologia NetApp Snapshot sem interrupções**

O SnapCenter usa a tecnologia Snapshot do NetApp com os plug-ins compatíveis com o NetApp para fazer backup de recursos. Os snapshots consomem espaço mínimo de storage.

Os plug-ins compatíveis com NetApp também oferecem os seguintes benefícios:

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

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

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

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

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

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

- Capacidade de criar Snapshot usando comandos externos.
- Capacidade de criar snapshots consistentes no sistema de arquivos em ambientes Windows.

Tipos de storage compatíveis com plug-ins compatíveis com 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 storage antes de instalar os plug-ins compatíveis com NetApp.

Máquina	Tipo de armazenamento
Montagens físicas e diretas NFS nos hosts de VM (VMDKs e RDM LUNs não são compatíveis.)	LUNs conectados a FC
Montagens físicas e diretas NFS nos hosts de VM (VMDKs e RDM LUNs não são compatíveis.)	LUNs ligados ao iSCSI
Montagens físicas e diretas NFS nos hosts de VM (VMDKs e RDM LUNs não são compatíveis.)	Volumes conectados a NFS
VMware ESXi	Armazenamentos de dados da VVol em NFS e SAN O armazenamento de dados da VVol só pode ser provisionado com as Ferramentas do ONTAP para o VMware vSphere.

Mínimo de ONTAP Privileges necessário para o plug-in compatível com NetApp

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

- Comandos All-Access: Privileges mínimo necessário para o ONTAP 9.12.1 e posterior
 - event generate-AutoSupport-log
 - mostra o histórico de trabalhos
 - paragem do trabalho
 - show de atributo lun

- lun criar
- eliminação lun
- geometria lun
- lun igrop add
- lun igrop criar
- eliminação do agrupamento lun
- mudar o nome do grupo lun
- show de grupos de lun
- nós complementares de mapeamento de lun
- mapeamento lun criar
- eliminação do mapeamento lun
- mapeamento lun remove-reporting-nonos
- mostra de mapeamento lun
- modificação de lun
- movimentação de lun no volume
- lun offline
- lun online
- redimensionar lun
- série lun
- mostra lun
- interface de rede
- regra adicional de política do SnapMirror
- regra de modificação de política do SnapMirror
- regra de remoção da política do SnapMirror
- SnapMirror policy show
- restauração de SnapMirror
- SnapMirror show
- SnapMirror show-history
- atualização do SnapMirror
- SnapMirror update-ls-set
- SnapMirror lista-destinos
- versão
- clone de volume criar
- show de clone de volume
- início da divisão do clone de volume
- paragem dividida clone volume
- criar volume

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

Preparar sistemas de storage para a replicação do SnapMirror e do SnapVault para plug-ins compatíveis com NetApp

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

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



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

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



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

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

Defina uma estratégia de backup

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

Sobre esta tarefa

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

Passos

1. Determine quando você deve fazer backup de seus recursos.
2. Decida quantos trabalhos de cópia de segurança necessita.
3. Decida como nomear seus backups.
4. Decida se você deseja Snapshots de Grupo de consistência e decida as opções apropriadas para excluir Snapshots de Grupo de consistência.

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

Estratégia de backup para plug-ins compatíveis com NetApp

Programações de backup de recursos de plug-in compatíveis com NetApp

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

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

O SLA define o nível de serviço esperado e aborda muitos problemas relacionados ao serviço, incluindo a disponibilidade e o desempenho do serviço. O RPO define a estratégia para a era dos arquivos que precisam ser recuperados do armazenamento de backup para que as operações regulares sejam retomadas após uma falha. O SLA e o RPO contribuem para a estratégia de proteção de dados.

Os programas de backup têm duas partes, como segue:

- Frequência de backup

A frequência de backup (com que frequência os backups devem ser executados), 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 hora, dia, semanal ou mensal. Você pode acessar políticas na GUI do SnapCenter clicando em **Configurações > políticas**.

- Fazer backup de programações

As programações 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 que tenha uma política configurada para backups semanais, poderá configurar a programação para fazer backup todas as quintas-feiras às 10:00 horas. Você poderá acessar programações de grupos de recursos na GUI do SnapCenter clicando em **Resources**, selecionando o plug-in apropriado e clicando em **Exibir > Grupo de recursos**.

Número de trabalhos de cópia de segurança necessários

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

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

de backup para o recurso grande.

Tipos de estratégias de restauração compatíveis com recursos de plug-in compatíveis com NetApp adicionados manualmente

Você deve definir uma estratégia antes de executar operações de restauração com êxito usando o SnapCenter. Existem dois tipos de estratégias de restauração para recursos de plug-in compatíveis com NetApp adicionados manualmente.



Não é possível recuperar recursos de plug-in suportados pelo 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 instantâneos obtidos após o instantâneo selecionado para restauração nesses volumes ou qtrees serão excluídos e não poderão ser recuperados. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído.

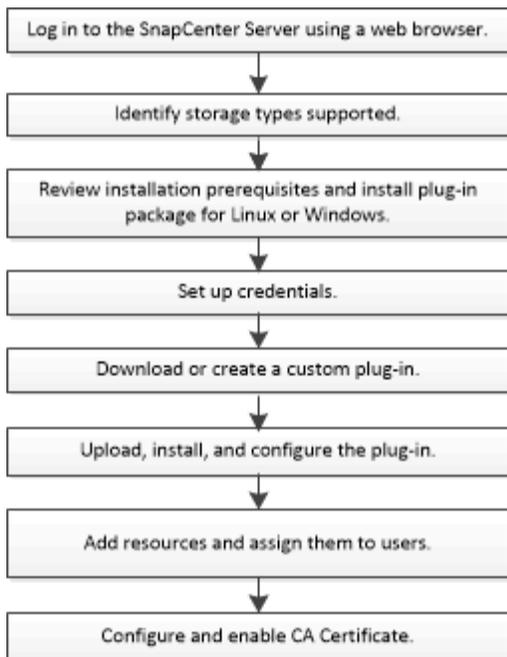
Restauração no nível do arquivo

- 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-in compatíveis com o NetApp.



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

Antes de adicionar um host e instalar os pacotes de plug-ins, você deve completar todos os requisitos. Os plug-ins compatíveis com NetApp são compatíveis com ambientes Windows, Linux e AIX.



Os aplicativos de armazenamento e Oracle são compatíveis com AIX.

- Você deve ter instalado o Java 11 em 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 do Windows, se você especificar uma credencial que não está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar o UAC no host.
- Os plug-ins compatíveis com o NetApp, como MongoDB, ORASCPM, aplicativos Oracle, 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 executada.

Geral

Se estiver a utilizar iSCSI, o serviço iSCSI deverá estar em execução.

Hosts do Windows

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

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

["Baixe JAVA para Windows"](#)

Hosts Linux e AIX



Os aplicativos de armazenamento e Oracle são compatíveis com 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 em 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.

["Baixe JAVA para Linux"](#)

["Baixe JAVA para AIX"](#)

- Você deve configurar o sudo Privileges 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 que está a utilizar 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`, que está localizado em:

- Se o servidor SnapCenter estiver instalado no host do Windows, o SnapCenter NetApp não será

instalado no sistema operacional Windows.

- `/opt/NetApp/SnapCenter/SnapManagerWeb/Repository/SC_UNIX_plugins_checksum.txt` se o servidor SnapCenter estiver instalado no host Linux.



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

Requisitos de anfitrião do AIX

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



Os aplicativos de armazenamento e Oracle são compatíveis com AIX.



O plug-in do SnapCenter para UNIX, que faz parte do pacote de plug-ins do SnapCenter para AIX, não suporta grupos de volume 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 log para o plug-in SnapCenter no host	2 GB  Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registros. O espaço de registro necessário varia consoante o número de entidades a proteger e a 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, você deve garantir que a opção <code>JAVA_HOME</code> localizada em <code>/var/opt/SnapCenter/spl/etc/spl.properties</code> esteja definida para a versão JAVA correta e o caminho correto.

Configure sudo Privileges para usuários não-root para host AIX

O SnapCenter 4,4 e posterior permite que um usuário não root instale o pacote de plug-ins do SnapCenter para AIX e inicie o processo de plug-in. Os processos de plug-in serão executados como um usuário não-root

eficaz. Você deve configurar o sudo Privileges para que o usuário não-root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Edite o arquivo `/etc/ssh/sshd_config` para configurar os algoritmos de código de autenticação de mensagem: Macs hmac-SHA2-256 e MACs hmac-SHA2-512.

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

Exemplo:

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

Sobre esta tarefa

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

- `/Home/AIX_USER/.SC_NetApp/SnapCenter_aix_host_plugin.bsx`
- `/Custom_location/NetApp/SnapCenter/spl/installation/plugins/uninstall`
- `/Custom_location/NetApp/SnapCenter/spl/bin/spl`

Passos

1. Faça 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 estiver tendo uma configuração RAC, juntamente com os outros comandos permitidos, você deve adicionar o seguinte ao arquivo `/etc/sudoers`:

```
'/<crs_home>/bin/olsnodes'
```

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

`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**, que está localizado em:

- Se o servidor SnapCenter estiver instalado no host do Windows, o SnapCenter NetApp não será instalado no sistema operacional Windows.
- `/opt/NetApp/SnapCenter/SnapManagerWeb/Repository/SC_UNIX_plugins_checksum.txt` se o servidor SnapCenter estiver instalado no host Linux.



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

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

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

Item	Requisitos
Sistemas operacionais	Microsoft Windows Para obter as informações mais recentes sobre as versões compatíveis, consulte "Ferramenta de Matriz de interoperabilidade do NetApp" .
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	5 GB <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente. </div>
Pacotes de software necessários	<ul style="list-style-type: none"> • Pacote de Hospedagem 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>Para obter informações específicas de solução de problemas .NET, consulte "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conectividade com a Internet."</p>

Requisitos de host para instalar o pacote de plug-ins do 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.



Os aplicativos de armazenamento e Oracle são compatíveis com AIX.

Item	Requisitos
Sistemas operacionais	<ul style="list-style-type: none"> • Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)

Item	Requisitos
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	2 GB <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;">  Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente. </div>
Pacotes de software necessários	Java 11 Oracle Java ou OpenJDK Se você atualizou O JAVA para a versão mais recente, você deve garantir que a opção JAVA_HOME localizada em /var/opt/SnapCenter/spl/etc/spl.properties esteja definida para a versão JAVA correta e o caminho correto.

Para obter as informações mais recentes sobre versões suportadas, consulte a. ["Ferramenta de Matriz de interoperabilidade do 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 raiz ou para um usuário não-root que tenha sudo Privileges para instalar e iniciar o processo de plug-in.

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

- Hosts do Windows

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

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

- Aplicações de plug-ins compatíveis com 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 pode definir as credenciais como **Nenhuma**.

Sobre esta tarefa

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

Passos

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

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

Para este campo...	Faça isso...
Nome de utilizador	<p>Introduza o nome de utilizador e a palavra-passe a utilizar para a 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 no qual você está instalando o plug-in do SnapCenter. Formatos válidos para o campo Nome de usuário são:</p> <ul style="list-style-type: none"> ◦ <i>NetBIOS_username</i> ◦ <i>Domain FQDN_username</i> <ul style="list-style-type: none"> • Administrador local (apenas para grupos de trabalho) <p>Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local incorporado no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host. O formato válido para o campo Nome de usuário é: <i>Nome de usuário</i></p>
Palavra-passe	Introduza a palavra-passe utilizada para autenticação.
Tipo de autenticação	Selecione o tipo de autenticação que pretende utilizar.
Use sudo Privileges	<p>Marque a caixa de seleção Use sudo Privileges se estiver criando credenciais para um usuário que não seja root.</p> <div style="display: flex; align-items: center;">  <p>Aplicável apenas a usuários 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.

Configure o gMSA no Windows Server 2016 ou posterior

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

Antes de começar

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

Passos

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

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

Por exemplo,

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

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

Para fazer isso, execute o seguinte comando do PowerShell:

```

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

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

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

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

```

- a. Reinicie o host.
 - b. Instale o gMSA em seu host executando o seguinte comando a partir do prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`
 - c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`
5. Atribua o Privileges administrativo ao gMSA configurado no host.
 6. Adicione o host do Windows especificando a conta gMSA configurada no servidor SnapCenter.

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

Instale os plug-ins suportados pelo NetApp

Adicione hosts e instale pacotes plug-in em hosts remotos

Você deve usar a página SnapCenter Adicionar host 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 as permissões de instalação e desinstalação do plug-in, como a função Administrador do SnapCenter.
- Você deve garantir que o serviço de enfileiramento de mensagens esteja em execução.
- Se você estiver usando a conta de serviço gerenciado de grupo (gMSA), você deve configurar o gMSA com Privileges administrativo.

["Configure a conta de serviço gerenciado de grupo no Windows Server 2016 ou posterior para aplicativos personalizados"](#)

- Para o host do Windows, você deve garantir que você selecione o plug-in do SnapCenter para Windows.

Sobre esta tarefa

- Não é possível adicionar um servidor SnapCenter como um host plug-in a outro servidor SnapCenter.
- 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 guia **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 <p> Os plug-ins compatíveis com NetApp podem ser usados em ambientes Windows, Linux e AIX.</p> <p> Os aplicativos de armazenamento e Oracle são compatíveis com AIX.</p>
Nome do host	<p>Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host.</p> <p>O SnapCenter depende da configuração adequada do DNS. Portanto, a melhor prática é entrar no 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 exibir detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você especificou.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar host.</p> </div>

5. Na seção **Select Plug-ins to Install**, selecione os plug-ins a instalar.

Você pode instalar os seguintes plug-ins na lista:

- MongoDB
- ORASCPM (exibido como aplicativos Oracle)
- SAP ASE
- SAP MaxDB
- Armazenamento

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

Para este campo...	Faça isso...
Porta	<p>Guarde o número da porta padrão ou especifique o número da porta.</p> <p>O número da porta padrão é 8145. Se o servidor SnapCenter tiver sido instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Se você instalou manualmente os plug-ins e especificou uma porta personalizada, você deve especificar a mesma porta. Caso contrário, a operação falha.</p> </div>

Para este campo...	Faça isso...
Caminho de instalação	<p>Os plug-ins compatíveis com NetApp podem ser instalados em um sistema Windows ou em um sistema Linux.</p> <ul style="list-style-type: none"> • Para o pacote de plug-ins do 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 do SnapCenter para Linux e o pacote de plug-ins do SnapCenter para AIX, o caminho padrão é /opt/NetApp/snapcenter. <p>Opcionalmente, você pode personalizar o caminho.</p>
Ignorar as verificações de pré-instalação	<p>Marque essa caixa de seleção se você já instalou os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.</p>
Use a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in	<p>Para o host Windows, marque essa caixa de seleção se desejar usar a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> Forneça o nome do gMSA no seguinte formato:</p> <p> O gMSA será usado como uma conta de serviço de logon apenas para o serviço SnapCenter Plug-in para Windows.</p> </div>

7. Selecione **Enviar**.

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

Se o erro estiver relacionado ao espaço em disco ou à RAM, você poderá 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 deve corrigir o problema.



Em uma configuração de HA, se você estiver atualizando o SnapManager.Web.UI.dll.config, será necessário atualizar o arquivo em ambos os nós e reiniciar o pool de aplicativos do SnapCenter.

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 **Confirm and Submit**.



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

9. Monitorize o progresso da instalação.

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

Instale pacotes de plug-in do 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` PowerShell.

Antes de começar

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



Os aplicativos de armazenamento e Oracle são compatíveis com AIX.

Passos

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

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

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

4. Insira suas credenciais para instalação remota.

Instale os plug-ins compatíveis com NetApp em hosts Linux usando a interface de linha de comando

Você deve instalar os plug-ins compatíveis com o NetApp usando a interface de usuário (UI) do SnapCenter. Se o seu ambiente não permitir a instalação remota do plug-in a

partir da IU do SnapCenter, você poderá instalar os plug-ins compatíveis com NetApp no modo console ou no modo silencioso usando a interface de linha de comando (CLI).

Passos

1. Copie o pacote de plug-ins do SnapCenter para o arquivo de instalação do Linux (SnapCenter_linux_host_plugin.bin) de C:/NetApp/SnapCenter para o host onde você deseja instalar os plug-ins suportados pelo NetApp.

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

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

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

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

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

5. Faça login no SnapCenter e faça o upload do plug-in compatível com o NetApp a partir da IU ou usando cmdlets do PowerShell.

Pode carregar o plug-in suportado pelo NetApp a partir da IU consultando ["Adicione hosts e instale pacotes plug-in em hosts remotos"](#) a secção.

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

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

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

Pode monitorizar o progresso da instalação do pacote de plug-ins do SnapCenter utilizando a página trabalhos. Você pode querer verificar o andamento da instalação para

determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

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

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

Passos

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

Configurar certificado CA

Gerar arquivo CSR do certificado CA

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

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



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

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



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

Para configurações de cluster, o nome do cluster (FQDN de cluster virtual) e os respectivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome

alternativo (SAN) do assunto antes de adquirir o certificado. Para um certificado Wild card (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados CA

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

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File > Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola > certificados – computador local > autoridades de Certificação raiz fidedignas > certificados**.
5. Clique com o botão direito do rato na pasta "autoridades de Certificação de raiz fidedigna" e selecione **todas as tarefas > Importar** para iniciar o assistente de importação.
6. Conclua o assistente da seguinte forma:

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



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

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

Obtenha a impressão digital do certificado CA

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

Passos

1. Execute o seguinte na GUI:
 - a. Clique duas vezes no certificado.
 - b. Na caixa de diálogo certificado, clique na guia **Detalhes**.

- c. Percorra a lista de campos e clique em **thumbprint**.
- d. Copie os 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", depois de remover os espaços, será: "A909502d82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:

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

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

- b. Copie a impressão digital.

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

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

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

Passos

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

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

Por exemplo:

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

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

Por exemplo:

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

Configure o certificado CA para o serviço de plug-ins compatíveis com 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. Altere a senha do keystore:

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

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

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

3. Reinicie o serviço depois de alterar a senha.



A 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. Liste os certificados adicionados no keystore:

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

4. Adicione um certificado raiz ou intermediário:

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



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

Configurar o par de chaves assinadas pela CA para plug-in de armazenamento confiável

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. Liste os certificados adicionados no keystore:

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

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

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

5. Liste os certificados adicionados no keystore.

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

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

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

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
. Se o nome do alias no certificado da CA for longo e contiver espaço ou
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 com a chave `SCC_CERTIFICATE_ALIAS`.

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

Configurar a 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 SnapCenter é 'opt/NetApp/snapcenter/scc/etc/crl'.

Passos

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

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

Configure o certificado CA para o serviço de plug-ins compatíveis com o 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. Altere a senha do keystore:

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



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

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

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

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

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

4. Reinicie o serviço depois de alterar a senha.



A 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. Liste os certificados adicionados no keystore:

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

4. Adicione um certificado raiz ou intermediário:

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

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



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

Configurar o par de chaves assinadas pela CA para plug-in de armazenamento confiável

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. Liste os certificados adicionados no keystore:

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

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

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

5. Liste os certificados adicionados no keystore.

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

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

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

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

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

Atualize este valor com a chave SCC_CERTIFICATE_ALIAS.

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

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

Sobre esta tarefa

- Para transferir o ficheiro CRL mais recente para o certificado CA relacionado, "[Como atualizar o arquivo de lista de revogação de certificados no certificado da CA do SnapCenter](#)" consulte .
- Os plug-ins 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* contra a chave CRL_PATH.
2. Você pode colocar mais de um arquivo CRL neste diretório.

Os certificados recebidos serão verificados em relação a cada CRL.

Ative certificados de CA para plug-ins

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

Antes de começar

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

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

Passos

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

Depois de terminar

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

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

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



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

Preparar-se para a proteção de dados

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

Antes de usar plug-ins compatíveis com o SnapCenter NetApp, o administrador do SnapCenter deve instalar e configurar o servidor SnapCenter e executar as tarefas de pré-requisito.

- Instalar e configurar o servidor SnapCenter.
- Inicie sessão no servidor SnapCenter.
- Configure o ambiente SnapCenter adicionando conexões do sistema de storage e criando credenciais, se aplicável.
- Adicione hosts e 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, você pode 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 storage NFS na máquina virtual de armazenamento (SVM) para os volumes clonados. Se você quiser ter um endereço IP específico ou restringir a um subconjunto dos 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 quiser replicação de backup.
- Certifique-se de que a porta 9090 não seja usada por nenhum outro aplicativo no host.

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

Como os recursos, grupos de recursos e políticas são usados para proteger os recursos de plug-in compatíveis com o NetApp

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

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

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

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

- As políticas especificam a frequência de backup, retenção de cópia, 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 quando você executa um backup sob demanda para um único recurso.

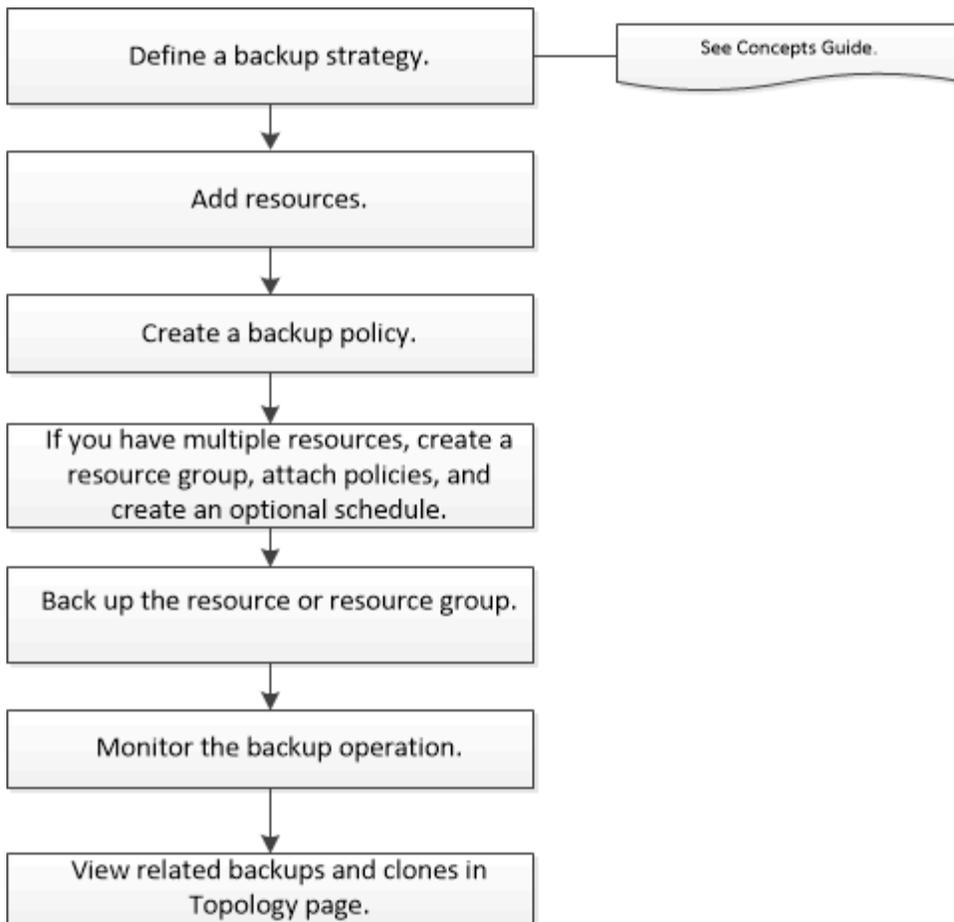
Pense em um grupo de recursos como definindo *o que* você quer proteger e quando você quer protegê-lo em termos de dia e tempo. Pense em uma política como definindo *como* você quer protegê-la. Se você estiver fazendo backup de todos os bancos de dados ou fazendo backup de todos os sistemas de arquivos de um host, por exemplo, você pode criar um grupo de recursos que inclua todos os bancos de dados ou todos os sistemas de arquivos no host. Em seguida, você pode anexar duas políticas ao grupo de recursos: Uma política diária e uma política por hora. Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup baseado em arquivo diariamente e outro agendamento que executa backup baseado em Snapshot por hora.

Fazer backup de recursos de plug-ins compatíveis com NetApp

Fazer backup de recursos de plug-ins compatíveis com NetApp

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

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



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

Adicione recursos aos plug-ins compatíveis com 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 servidor SnapCenter, adicionar hosts, criar conexões do sistema de storage e adicionar credenciais.
- Você deve ter carregado os plug-ins para o servidor SnapCenter.

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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	Introduza o nome do recurso.
Nome do host	Selecione o host.
Tipo	<p>Selecione o tipo. Tipo é definido pelo usuário de acordo com 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.
Monte caminhos	Introduza os caminhos de montagem onde o recurso está montado. Isso é aplicável apenas para um host Windows.

4. Na página fornecer espaço físico 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 compatíveis com NetApp não oferecem suporte à descoberta automática dos recursos. Os detalhes de armazenamento de ambientes físicos e virtuais também não são descobertos automaticamente. Você precisa fornecer as informações de storage para ambientes físicos e virtuais ao criar os recursos.

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



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

Resource settings

Name	Value	
HOST	localhost	x
PORT	3306	x
MASTER_SLAVE	NO	+ x

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

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

Resultado

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



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

Depois de terminar

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

Depois de adicionar os recursos, você pode modificar os detalhes do recurso. Se um recurso de plug-ins compatível com 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 você estiver adicionando os plug-ins manualmente, poderá usar os seguintes parâmetros para configurar o recurso na página Configurações de recursos.

Plug-in para MongoDB

Definições de recursos:

- MONGODB_APP_SERVER(para tipo de recurso como cluster sharded) ou MONGODB_REPLICASE_SERVER(para tipo de recurso como replicaset)
- OPLOG_PATH (parâmetro opcional no caso de ser fornecido a partir de MongoDB.propertiesfile)
- MONGODB_AUTHENTICATION_TYPE (SIMPLES para autenticação LDAP e nenhum para outros)

Você deve fornecer os seguintes parâmetros precisam ser fornecidos n arquivo MongoDB.properties:

- DISABLE_STARTING_STARTING_SERVICES
 - N se os serviços de arranque/paragem forem executados pelo plug-in.
 - Y se iniciar/**parar serviços são executados pelo usuário.

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

Plug-in para MaxDB

Definições de recursos:

- XUSER_ENABLE (Y|N) ativa ou desativa o uso de um xuser para MaxDB para que uma senha não seja necessária para o usuário do banco de dados.
- HANDLE_LOGWRITER (Y|N) executa as operações de suspender o gravador de log (N) ou retomar logwriter (Y).
- DBMCLICMD (path_to_dbmcli_cmd) especifica o caminho para o comando MaxDB dbmcli. Se não estiver definido, dbmcli no caminho de pesquisa será usado.



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

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

Isso se aplica somente a 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 tem de existir e ser um tipo externo de modelo de cópia de segurança. Para habilitar a integração de snapshot para o MaxDB 7,8 e posterior, você deve ter a funcionalidade de servidor em segundo plano do MaxDB e modelo de backup do MaxDB já configurado do tipo EXTERNO.

- 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 deve 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

Definições de recursos:

- SYBASE_SERVER (data_Server_NAME) especifica o nome do servidor de dados Sybase (-S opção 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.

Necessário para UNIX. Esse parâmetro é necessário se o usuário executando os comandos de início e parada do Snap Creator Agent (geralmente o usuário raiz) e o usuário executando o comando isql forem diferentes.

- SYBASE_TRAN_DUMP dB_name:Directory_path permite que você execute um despejo de transação Sybase depois de 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 (Y|N) ativa ou desativa a compressão de despejo de transação Sybase nativa.
- SYBASE_ISQL_CMD (por exemplo, /opt/sybase/OCS-15_0/bin/isql) define o caminho para o comando isql.
- SYBASE_EXCLUDE_TEMPDB (Y|N) permite excluir automaticamente bancos de dados temporários criados pelo usuário.

Plug-in para aplicativos Oracle (ORASCPM)

Definições 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 o 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 você deve fazer o backup dos logs do arquivo ou não.
- ORACLE_BACKUPMODE especifica se o backup deve ser realizado 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>`. Isso normalmente ocorre 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 compatíveis com o NetApp

Antes de usar o SnapCenter para fazer backup de recursos específicos de plug-in compatíveis com o NetApp, você deve criar uma política de backup para o recurso ou grupo de recursos que 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 deve ter se preparado para a proteção de dados.

A preparação para a proteção de dados inclui tarefas como a instalação do SnapCenter, a adição de hosts, a criação de conexões do sistema de storage e a adição de 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 os SVMs para os volumes de origem e destino a você se estiver replicando snapshots em 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 retém backups. Além disso, você pode especificar as 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 'reter as cópias de backup para um número específico de dias' estiver selecionada, o período de retenção do SnapLock deve ser menor ou igual aos dias de retenção mencionados.
 - Especificar um período de bloqueio instantâneo impede a exclusão dos instantâneos até que o período de retenção expire. Isso pode levar a reter um número maior de instantâneos do que a contagem especificada na política.
 - Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.



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

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **políticas**.
3. Clique em **novo**.
4. Na página Nome, insira o nome e os detalhes da política.
5. Na página tipo de política, execute o seguinte:
 - a. Selecione o tipo de armazenamento.
 - b. Na seção Configurações personalizadas de backup, forneça quaisquer configurações específicas de backup que tenham que ser passadas para o formato de valor de chave do plug-in.

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

6. Na página Snapshot e replicação, execute as seguintes etapas:
 - a. Especifique o tipo de agendamento selecionando **on demand**, **Hourly**, **Daily**, **Weekly** ou **Monthly**.



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



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

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

Se você quiser...	Então...
Mantenha um certo número de instantâneos	<p>Selecione Copies to keep e especifique o número de instantâneos que deseja manter.</p> <p>Se o número de instantâneos exceder o número especificado, os instantâneos serão excluídos com as cópias mais antigas excluídas primeiro.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> Você deve definir a contagem de retenção como 2 ou superior, se quiser habilitar a replicação do SnapVault. Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro snapshot é o snapshot de referência para a relação SnapVault até que um snapshot mais recente seja replicado para o destino.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> O valor máximo de retenção é 1018. Os backups falharão se a retenção for definida para um valor maior do que o que a versão subjacente do ONTAP suporta.</p> </div>
Mantenha as capturas instantâneas por um determinado número de dias	Selecione reter cópias para e especifique o número de dias para os quais deseja manter as capturas instantâneas antes de excluí-las.
Período de bloqueio de cópia de instantâneo	<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 uma etiqueta 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...
Atualizar SnapMirror depois de criar uma cópia Snapshot local	<p>Selecione este campo para criar cópias espelhadas dos conjuntos de backup em outro volume (replicação SnapMirror).</p> <p>Se a relação de proteção no ONTAP for do tipo espelho e Cofre e se você selecionar somente essa opção, instantâneo criado no primário não será transferido para o destino, mas será listado no destino. Se este instantâneo for selecionado no destino para executar uma operação de restauração, a seguinte mensagem de erro será exibida: Local secundário não está disponível para o backup abobadado/espelhado 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>"Veja os backups e clones relacionados a recursos de plug-ins compatíveis com o NetApp na página topologia"Consulte .</p>

Para este campo...	Faça isso...
Atualizar SnapVault depois de criar uma cópia Snapshot local	<p>Selecione esta opção para executar a replicação de backup disco a disco (backups 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 apenas no secundário do ONTAP conhecido como SnapLock Vault, clicar no botão Atualizar na página topologia atualiza o período de bloqueio no secundário que é recuperado do ONTAP.</p> <p>Para obter mais informações sobre o SnapLock Vault, consulte confirmar snapshots para WORM em um destino de cofre.</p> <p>"Veja os backups e clones relacionados a recursos de plug-ins compatíveis com o NetApp na página topologia"Consulte .</p>
Contagem de tentativas de erro	Introduza o número máximo de tentativas de replicação que podem ser permitidas antes de a operação parar.



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

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

Crie grupos de recursos e anexe políticas

Um grupo de recursos é o contendor ao qual você deve adicionar recursos que deseja fazer backup e proteger. Ele permite fazer backup de todos os dados associados a uma determinada aplicação simultaneamente. Você também deve anexar uma ou mais políticas ao grupo de recursos para definir o tipo de tarefa de proteção de dados que deseja executar.

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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>Introduza um nome para o grupo de recursos.</p> <p>Observação: O nome do grupo de recursos não deve exceder 250 caracteres.</p>
Tags	<p>Insira um ou mais rótulos que o ajudarão a pesquisar posteriormente o grupo de recursos.</p> <p>Por exemplo, se você adicionar HR como uma tag a vários grupos de recursos, poderá encontrar mais tarde todos os grupos de recursos associados à tag HR.</p>
Use o formato de nome personalizado para cópia Snapshot	<p>Marque essa caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.</p> <p>Por exemplo, <i>customtext_resource_group_policy_hostname</i> ou <i>resource_group_hostname</i>. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.</p>

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

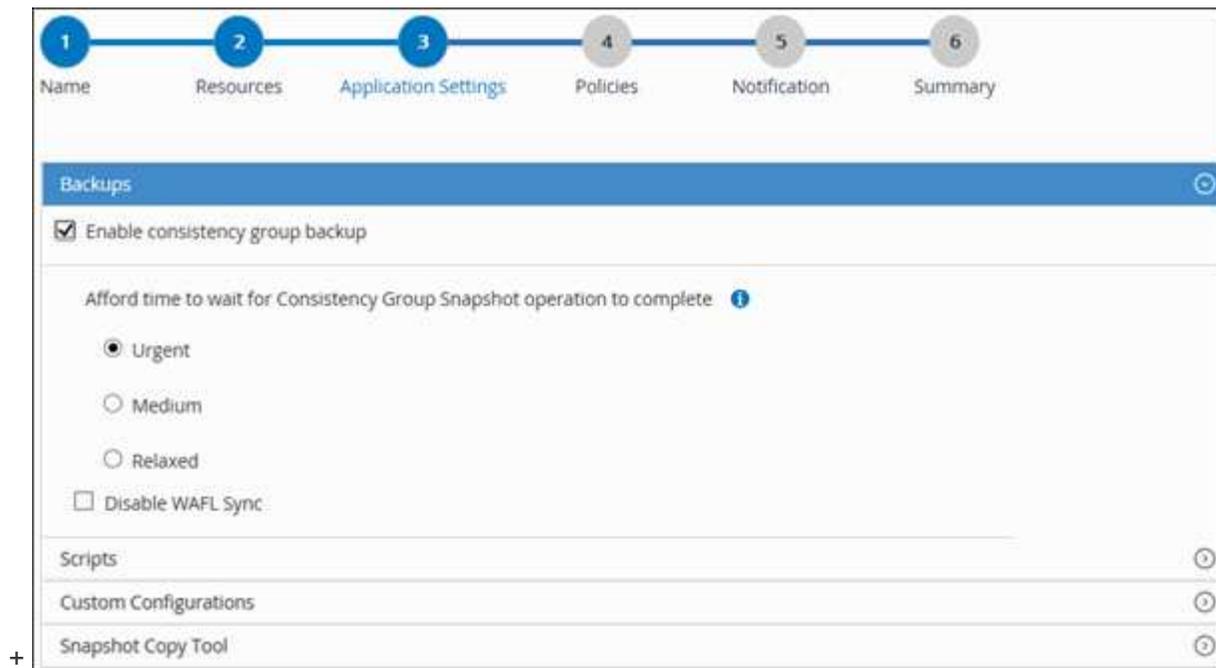
Isso ajuda a filtrar informações na tela.

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

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

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

Para este campo...	Faça isso...
Tenha tempo para esperar que a operação de snapshot do grupo de consistência seja concluída	<p>Selecione urgente, Médio ou relaxado para especificar o tempo de espera para que a operação Snapshot seja concluída.</p> <p>Urgente: 5 segundos, Médio: 7 segundos e relaxado: 20 segundos.</p>
Desativar a 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 quiesce, Snapshot e unquiesce. Também pode introduzir os pré comandos a serem executados antes de sair em caso de falha.
- b. Selecione a seta Configurações personalizadas e insira os pares de valor de chave personalizados necessários para todas as operações de proteção de dados usando esse recurso.

Parâmetro	Definição	Descrição
ARCHIVE_LOG_ENABLE	(Y/N)	Permite que a gestão do registo de arquivo elimine os registos de arquivo.
ARCHIVE_LOG_RETENÇÃO	number_of_days	<p>Especifica o número de dias em que os logs de arquivo são mantidos.</p> <p>Esta definição tem de ser igual ou superior a NTAP_SNAPSHOT_RETENÇÕES.</p>
ARCHIVE_LOG_DIR	change_info_directory/logs	Especifica o caminho para o diretório que contém os logs do arquivo.

Parâmetro	Definição	Descrição
ARCHIVE_LOG_EXT	extensão_ficheiro	Especifica o comprimento da extensão do arquivo de log do arquivo. Por exemplo, se o log de arquivo for log_backup_0_0_0_0,1615185519429 e se o valor file_extension for 5, a extensão do log manterá 5 dígitos, que é 16151.
ARCH ARCHIVE_LOG_RECURSIVE_ SE	(Y/N)	Permite o gerenciamento de logs de arquivo dentro de subdiretórios. Você deve usar este parâmetro se os logs do arquivo estiverem localizados em subdiretórios.

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

Se você quiser...	Então...
SnapCenter para usar o plug-in para Windows e colocar o sistema de arquivos em um estado consistente antes de criar um instantâneo. Para recursos do Linux, essa opção não é aplicável.	Selecione SnapCenter com consistência do sistema de arquivos . Esta opção não é aplicável ao plug-in SnapCenter para banco de dados SAP HANA.
SnapCenter para criar um instantâneo no nível de storage	Selecione SnapCenter sem consistência do sistema de arquivos .
Para inserir o comando a ser executado no host para criar Snapshots.	Selecione Other e digite o comando a ser executado no host para criar uma captura Instantânea.

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

b. Na coluna **Configurar agendas**, selecione para a política que deseja configurar.

c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e

selecione OK.

Onde `policy_name` é o nome da política selecionada.

As programações configuradas são listadas na coluna agendas aplicadas. As agendas de backup de terceiros não são suportadas quando sobrepõem-se às agendas de backup do SnapCenter.

8. Na lista suspensa **preferência de e-mail** na página **notificação**, 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 servidor SMTP deve ser configurado em **Configurações > Configurações globais**.

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

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

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

Antes de começar

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

Sobre esta tarefa

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

Passos

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



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

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

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

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

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

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



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

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



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

5. Selecione os recursos do ASA R2 na seção recursos disponíveis e mova-os para a seção recursos selecionados.
6. Na página Configurações do aplicativo, selecione a opção de backup.
7. Na página políticas, execute as seguintes etapas:

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



Você também pode criar uma política clicando  em .

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

- b. Clique  na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.
- c. Na janela Adicionar programações para a política *policy_name*, configure a programação e clique em **OK**.

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

As programações configuradas são listadas na coluna agendas aplicadas.

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

8. Se a proteção secundária estiver ativada para a política selecionada, a página proteção secundária será exibida e você precisará executar as seguintes etapas:
 - a. Selecione o tipo da política de replicação.



A política de replicação síncrona não é suportada.

- b. Especifique o sufixo do grupo de consistência que você deseja usar.
- c. Nos drop-down Cluster de destino e SVM de destino, selecione o cluster com peering e SVM que você deseja usar.



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



Se os recursos já estiverem protegidos fora do SnapCenter, esses recursos serão exibidos na seção recursos protegidos secundários.

1. Na página Verificação, execute as seguintes etapas:
 - a. Clique em **carregar localizadores** para carregar os volumes SnapMirror ou SnapVault para executar a verificação no armazenamento secundário.
 - b.
 - Clique  na coluna Configurar agendas para configurar o agendamento de verificação para todos os tipos de agendamento da política.
 - c. Na caixa de diálogo Adicionar agendamentos de verificação policy_name , execute as seguintes ações:

Se você quiser...	Faça isso...
Execute a verificação após a cópia de segurança	Selecione Executar verificação após backup .
Marque uma verificação	Selecione Executar verificação agendada e, em seguida, selecione o tipo de agendamento na lista suspensa.

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

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

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

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



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

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

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

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

- Os nomes do sistema de armazenamento devem ser exclusivos.

O SnapCenter não é compatível com vários sistemas de storage com o mesmo nome em clusters diferentes. Cada sistema de storage com suporte do SnapCenter deve ter um nome exclusivo e um endereço IP de LIF de 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_vs1 -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`. Em alternativa, pode também consultar o ["Guia de referência de cmdlet do software SnapCenter"](#).

Fazer backup de recursos de plug-ins compatíveis com NetApp individuais

Se um recurso de plug-ins com suporte do NetApp individual não fizer parte de qualquer grupo de recursos, você poderá fazer o backup do recurso na página recursos. Você pode fazer backup do recurso sob demanda ou, se o recurso tiver uma política anexada

e uma programação configurada, os backups ocorrem automaticamente de acordo com a programação.

Antes de começar

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

IU do SnapCenter

Passos

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

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

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

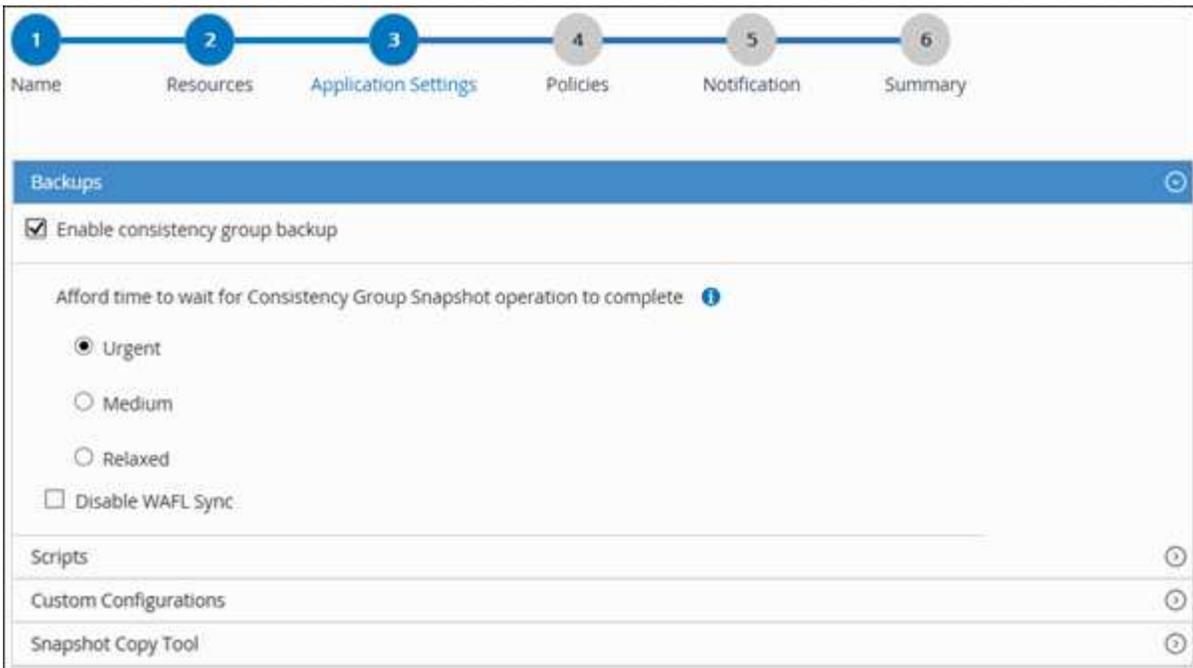
Por exemplo, *customtext_policy_hostname* ou *resource_hostname*. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.

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

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

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

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



- a. Clique na seta **Scripts** para executar comandos pré e POST para operações quiesce, Snapshot e unquiesce. Você também pode executar pré-comandos antes de sair da operação de backup.

Os Prescripts e postscripts são executados no servidor SnapCenter.

- b. Clique na seta **Custom Configurations** (Configurações personalizadas) e insira os pares de valores personalizados necessários para todos os trabalhos que usam esse recurso.
- c. Clique na seta **Snapshot Copy Tool** para selecionar a ferramenta para criar instantâneos:

Se você quiser...	Então...
SnapCenter para tirar uma Snapshot no nível de storage	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 depois tirar uma Snapshot	Selecione SnapCenter com consistência do sistema de arquivos .
Para inserir o comando para criar uma captura Instantânea	Selecione Other e, em seguida, digite o comando para criar uma captura Instantânea.

6. Na página políticas, execute as seguintes etapas:

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



Você também pode criar uma política clicando  em .

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

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

agendamento.

- c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e clique em **OK**.

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

As programações configuradas são listadas na coluna agendas aplicadas.

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

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

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

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 tiver aplicado várias políticas ao recurso, na lista suspensa **Política**, selecione a política que deseja usar para backup.

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

- b. Clique em **Backup**.

11. Monitorize o progresso da operação clicando em **Monitor > trabalhos**.

Cmdlets do PowerShell

Passos

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

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

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

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_vol1_scc55_sscore_test_com";"QTREENAME"="qtree  
Vol1";"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"="Dumm  
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. Exiba o status da tarefa de backup usando o cmdlet Get-SmBackupReport.

Este exemplo exibe um relatório de resumo de todos os trabalhos 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-in compatíveis com o 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 uma programação configurada, os backups ocorrerão automaticamente de acordo com a programação.

Antes de começar

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

All". No entanto, se você estiver usando a função "vsadmin", o privilégio "SnapMirror all" não será necessário.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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  e selecionando a tag. Em seguida, pode clicar  para fechar o painel de filtro.

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

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

- b. Clique em **Backup**.

5. Monitorize o progresso da operação clicando em **Monitor > trabalhos**.

- Nas configurações do MetroCluster, o SnapCenter pode não ser capaz de detectar uma relação de proteção após um failover.

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

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

Monitorar as operações de backup de recursos de plug-in compatíveis com NetApp

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

Sobre esta tarefa

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

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

- 🔄 Em fila de espera
- 🚫 Cancelado

Passos

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



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

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

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

Cancelar operações de backup para plug-ins compatíveis com NetApp

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

O que você vai precisar

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

Passos

1. Execute uma das seguintes ações:

A partir do...	Ação
Página do monitor	<ol style="list-style-type: none"> No painel de navegação esquerdo, clique em Monitor > trabalhos. Selecione a operação e clique em Cancelar trabalho.
Painel da atividade	<ol style="list-style-type: none"> Depois de iniciar a operação de backup, clique em  no painel atividade para exibir as cinco operações mais recentes. Selecione a operação. Na página Detalhes da tarefa, clique em Cancelar tarefa.

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

Veja os backups e clones relacionados a recursos de plug-ins compatíveis com o NetApp na página topologia

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

Sobre esta tarefa

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

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



Os clones de um backup de um espelhamento flexível de versão em um volume do tipo cofre-espelho são exibidos na visualização de topologia, mas a contagem de backup espelhado na visualização de topologia não inclui o backup flexível de versão.
- 
 Exibe o número de backups e clones replicados no storage secundário usando a tecnologia SnapVault.

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



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

Passos

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

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

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

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

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

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

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

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

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

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

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



Não é possível renomear ou excluir backups que estão 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  para excluir o clone.

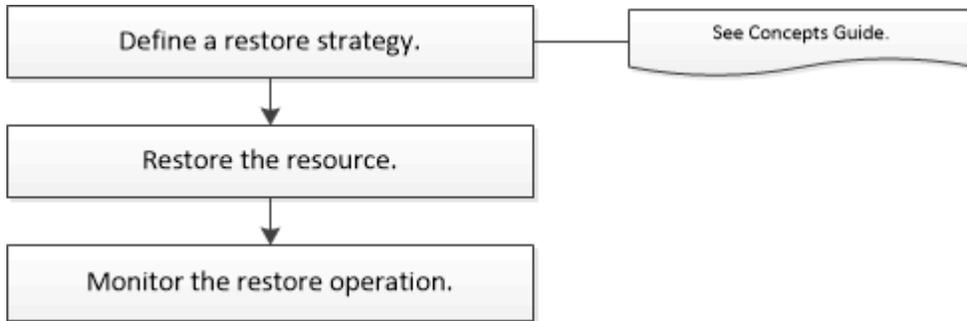
Restaure os recursos de plug-ins compatíveis com o NetApp

Restaure os recursos de plug-in compatíveis com o NetApp

O fluxo de trabalho de restauração e recuperação inclui Planejamento, execução das 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 clone. Para obter informações sobre cmdlets do PowerShell, use a ajuda do cmdlet SnapCenter ou consulte "[Guia de referência de cmdlet do software SnapCenter](#)".

Restaurar um backup de recursos

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

Sobre esta tarefa

- A operação de restauração padrão somente restaura objetos de armazenamento. As operações de restauração no nível da aplicação só podem ser executadas se o plug-in suportado pela NetApp fornecer essa capacidade.
- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

IU do SnapCenter

Passos

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

Os recursos são exibidos juntamente com informações como tipo, nome do host ou cluster, grupos e políticas de recursos 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 **Estado geral**.

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

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

A página de topologia do recurso é exibida.

4. Na exibição **Gerenciar cópias**, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).

5. Na tabela backup(s) primário(s), selecione o backup do qual você deseja restaurar e clique  em .



6. Na página Restaurar escopo, selecione **recurso completo** ou **nível de arquivo**.

- a. Se você selecionou **Complete Resource**, 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 **File Level**, então você pode selecionar **All** ou selecionar volumes ou qtrees e, em seguida, inserir o caminho relacionado aos volumes ou qtrees que são selecionados separados por vírgulas.

- Você pode selecionar vários volumes e qtrees.
- Se o tipo de recurso for LUN, todo o LUN será restaurado. Pode selecionar vários LUNs. Observação: Se você selecionar **All**, todos os arquivos nos volumes, qtrees ou LUNs serão restaurados.

7. Na página **Pré-operações**, insira pré-restaurar e desmontar comandos para serem executados antes

de executar um trabalho de restauração.

8. Na página **Post OPS**, insira os comandos mount e POST Restore para serem executados após a execução de um trabalho de restauração.
9. Na página **notificação**, na lista suspensa **preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

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

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

Cmdlets do PowerShell

Passos

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

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

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

Este exemplo exibe informações sobre todos os backups disponíveis:

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

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

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

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

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

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

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

```

Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.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*. Em alternativa, pode também consultar o ["Guia de referência de cmdlet do software SnapCenter"](#).

Monitorar as operações de restauração de recursos de plug-in compatíveis com o NetApp

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

Sobre esta tarefa

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

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

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

Passos

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

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

Clone NetApp compatível com backups de recursos de plug-ins

Clone NetApp compatível com backups de recursos de plug-ins

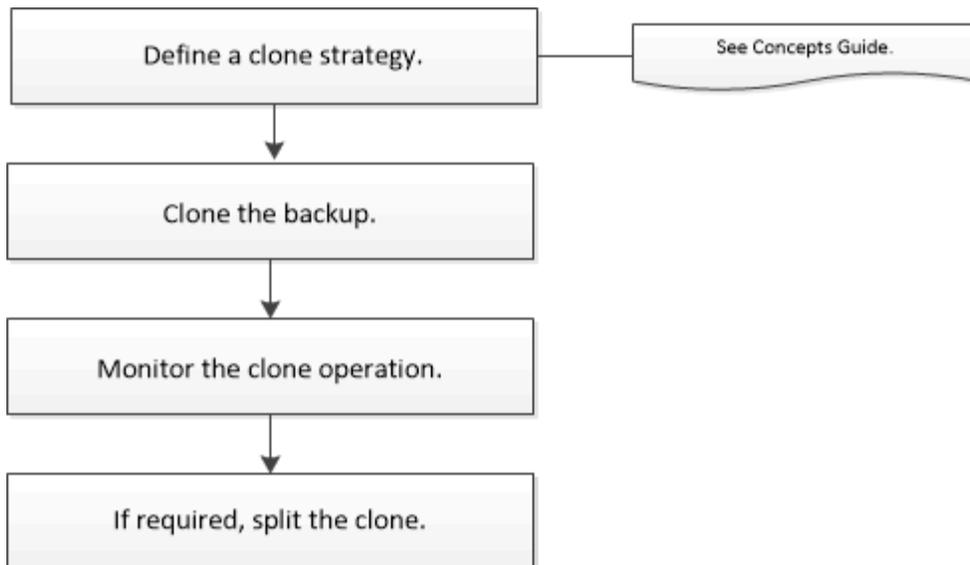
O fluxo de trabalho do clone inclui a execução da operação de clone e o monitoramento da operação.

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 de aplicativos
- Para ferramentas de extração e manipulação de dados ao preencher data warehouses
- Para recuperar dados que foram excluídos ou alterados por engano

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



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

Clone de um backup

Você pode usar o SnapCenter para clonar um backup. Você pode clonar do backup primário ou secundário. As funcionalidades das operações de clone 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 clone padrão somente clona objetos de storage. As operações de clone no nível da aplicação só podem ser executadas se o plug-in compatível com NetApp fornecer essa funcionalidade.
- Você deve garantir que os agregados que hospedam os volumes estejam na lista de agregados atribuídos da máquina virtual de storage (SVM).

Sobre esta tarefa

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

IU do SnapCenter

Passos

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

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

3. Selecione o grupo de recursos ou recursos.

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

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

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

Para este campo...	Faça isso...
Servidor clone	Por padrão, o host de origem é preenchido. Se você quiser especificar um host diferente, selecione o host no qual o clone deve ser montado e o plug-in está instalado.
Sufixo clone	Isso é obrigatório quando o destino do clone é o mesmo que a origem. Digite um sufixo que será anexado ao nome do recurso recém-clonado. O sufixo garante que o recurso clonado seja exclusivo no host. Por exemplo, RS1_clone. Se você estiver clonando para o mesmo host que o recurso original, forneça um sufixo para diferenciar o recurso clonado do recurso original; caso contrário, a operação falha.

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

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

Para este campo...	Faça isso...
Nome do iniciador	Insira o nome do iniciador do host, que é IQDN ou WWPN.

Para este campo...	Faça isso...
Protocolo Igroup	Selecione Igroup Protocol (Protocolo de grupo).



A página de definições é apresentada apenas se o tipo de armazenamento for LUN.

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

Por exemplo:

- Comando pre clone: Exclua bancos de dados existentes com o mesmo nome
- Comando Post clone: Verifique um banco de dados ou inicie um banco de dados.

Montar comando 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 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.

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

- Monitorize o progresso da operação clicando em **Monitor > trabalhos**.

Cmdlets do PowerShell

Passos

- Inicie uma sessão de conexão com o servidor SnapCenter 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 : {}  
HostResourceMapping : {}  
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 clone a partir de um grupo de recursos de clone ou de um backup existente usando o cmdlet `New-SmClone`.

Este exemplo cria um clone a partir 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. Exiba o status da tarefa clone usando o cmdlet `Get-SmCloneReport`.

Este exemplo exibe um relatório de clone para a ID de tarefa especificada:

```
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 as operações de clone de recurso de plug-in compatíveis com o NetApp

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

Sobre esta tarefa

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

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

Passos

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

3. Na página **trabalhos**, execute as seguintes etapas:
 - a. Clique  para filtrar a lista para que apenas operações de clone sejam listadas.
 - b. Especifique as datas de início e fim.
 - c. Na lista suspensa **Type**, selecione **Clone**.
 - d. Na lista suspensa **Status**, selecione o status do clone.
 - e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione a tarefa clone e clique em **Detalhes** para exibir os detalhes da tarefa.
5. Na página Detalhes da tarefa, clique em **Exibir logs**.

Informações sobre direitos autorais

Copyright © 2026 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 SOBRESSALIENTES; 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.