Saiba mais sobre o software SnapCenter

SnapCenter software

NetApp
January 09, 2026

Índice

Saiba mais sobre o software SnapCenter

Visão geral do SnapCenter

O SnapCenter software é uma plataforma simples, centralizada e escalável para proteção de dados consistente com aplicativos. Ele protege aplicativos, bancos de dados, sistemas de arquivos host e VMs em sistemas ONTAP na Nuvem Híbrida.

O SnapCenter usa as tecnologias NetApp Snapshot, SnapRestore, FlexClone, SnapMirror e SnapVault para fornecer:

- Backups rápidos, com uso eficiente de espaço, consistentes com aplicações e baseados em disco
- Restauração rápida e detalhada e recuperação consistente com o aplicativo
- Clonagem rápida e com uso eficiente de espaço

O SnapCenter inclui o SnapCenter Server e plug-ins leves. Você pode automatizar a implantação de plug-ins em hosts de aplicativos remotos, agendar operações de backup, verificação e clonagem, além de monitorar operações de proteção de dados.

Você pode instalar o SnapCenter no local ou em uma nuvem pública para proteger dados.

- No local para proteger o seguinte:
  - Dados em sistemas primários ONTAP FAS, AFF ou ASA e replicados para sistemas secundários ONTAP FAS, AFF ou ASA
  - Dados em sistemas primários ONTAP Select
  - Dados em sistemas primários e secundários ONTAP FAS, AFF ou ASA e protegidos no storage de objetos StorageGRID local
  - Dados em sistemas primários e secundários do ONTAP ASA R2
- No local em uma Nuvem Híbrida para proteger o seguinte:
  - Dados em sistemas primários ONTAP FAS, AFF ou ASA e replicados para Cloud Volumes ONTAP
  - Dados que estão em sistemas primários e secundários ONTAP FAS, AFF ou ASA e protegidos para armazenamento de objetos e arquivos na nuvem usando integração de backup e recuperação do NetApp
- Em uma nuvem pública para proteger o seguinte:
  - Dados em sistemas primários Cloud Volumes ONTAP (anteriormente ONTAP Cloud)
  - Dados que estão no Amazon FSX for ONTAP
  - Dados em Azure NetApp Files primário (Oracle, Microsoft SQL e SAP HANA)

Principais recursos

O SnapCenter fornece os seguintes recursos principais:

- Proteção de dados centralizada e consistente com aplicações de diferentes aplicações

  A proteção de dados é compatível com bancos de dados Microsoft Exchange Server, Microsoft SQL Server, Oracle em Linux ou AIX, banco de dados SAP HANA, IBM DB2, PostgreSQL, MySQL e Windows

Host em execução em sistemas ONTAP. O SnapCenter também oferece suporte à proteção de aplicativos como MongoDB, Storage, MaxDB, Sybase ASE, ORASCPM.

- Backups baseados em políticas

  Os backups baseados em políticas aproveitam a tecnologia NetApp Snapshot para criar backups rápidos, com eficiência de espaço e consistentes com aplicativos, baseados em disco. Você também pode configurar a proteção automática desses backups para armazenamento secundário atualizando os relacionamentos de proteção existentes.

- Backups para vários recursos

  Você pode fazer backup de vários recursos (aplicativos, bancos de dados ou sistemas de arquivos host) do mesmo tipo ao mesmo tempo usando grupos de recursos do SnapCenter .

- Restauração e recuperação

  O SnapCenter fornece restaurações granulares e rápidas de backups e recuperação baseada em tempo e consistente com aplicações. Você pode restaurar a partir de qualquer destino na nuvem híbrida.

- Clonagem

  O SnapCenter oferece clonagem rápida, com economia de espaço e consistente com o aplicativo. Você pode clonar em qualquer destino na Nuvem Híbrida.

- Interface gráfica de usuário de gerenciamento de usuário único

  O SnapCenter fornece uma interface única para gerenciar backups e clones em qualquer destino de Nuvem Híbrida.

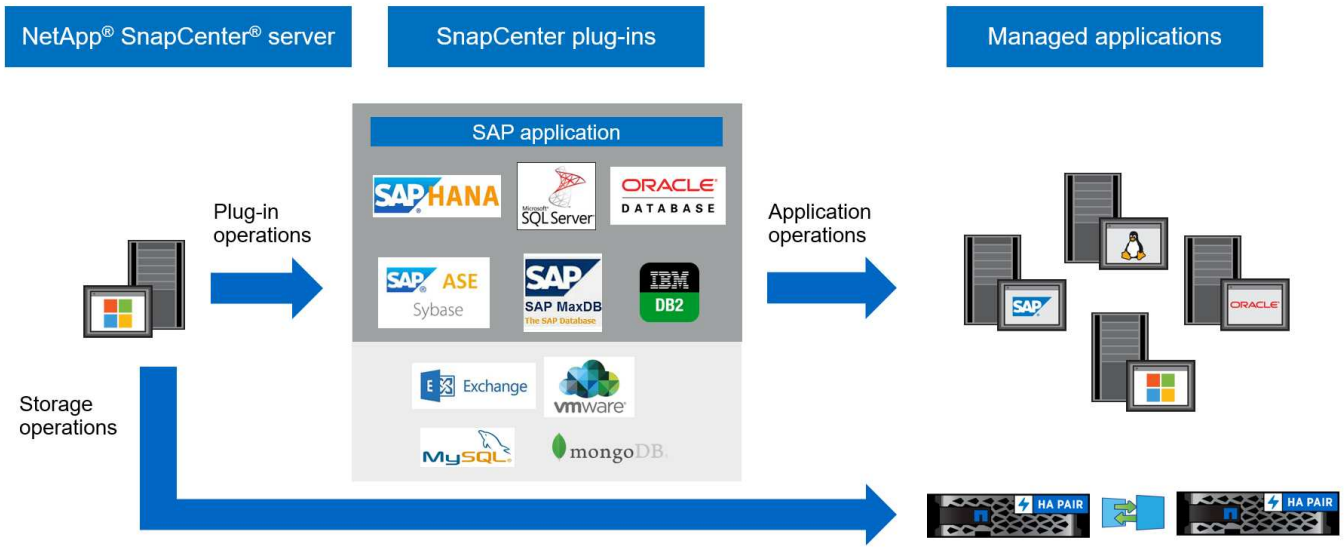
- APIs REST, cmdlets do Windows, comandos UNIX

  O SnapCenter fornece APIS REST para a maioria das funcionalidades para integração com qualquer software de orquestração e uso de cmdlets e interface de linha de comando do Windows PowerShell.

- Painéis e relatórios de proteção de dados centralizados
- Controle de acesso baseado em função (RBAC) para segurança e delegação
- Um banco de dados de repositório incorporado com alta disponibilidade para armazenar todos os metadados de backup
- Instalação automática de plug-ins por push
- Alta disponibilidade
- Recuperação de desastres (DR)
- SnapLock "Saiba mais"
- SnapMirror ative Sync (lançado inicialmente como SnapMirror Business Continuity [SM-BC])
- Espelhamento síncrono "Saiba mais"

Arquitetura e componentes do SnapCenter

O SnapCenter usa um design em camadas com um servidor de gerenciamento central e hosts de plug-in. Os hosts do servidor e do plug-in podem estar em locais diferentes.



O SnapCenter inclui o servidor SnapCenter, o pacote de plug-ins SnapCenter para Windows e o pacote de plug-ins SnapCenter para Linux. Cada pacote contém plug-ins para vários aplicativos e componentes de infraestrutura.

Servidor SnapCenter

O servidor SnapCenter suporta os sistemas operacionais Microsoft Windows e Linux (RHEL 8.x, RHEL 9.x, SLES 15 SP5). O servidor SnapCenter inclui um servidor da Web, uma interface de usuário centralizada baseada em HTML5, cmdlets do PowerShell, APIs REST e o repositório SnapCenter.

O SnapCenter armazena informações sobre suas operações no repositório SnapCenter .

Plug-ins do SnapCenter

Cada plug-in do SnapCenter é compatível com ambientes, bancos de dados e aplicações específicos.

Nome do plug-in	Incluído no pacote de instalação	Requer outros plug-ins	Instalado no host	Plataforma suportada
Plug-in do SnapCenter para Microsoft SQL Server	Pacote de plug-ins para Windows	Plug-in para Windows	Host do SQL Server	Windows
Plug-in SnapCenter para Windows	Pacote de plug-ins para Windows		Host Windows	Windows
Plug-in do SnapCenter para Microsoft Exchange Server	Pacote de plug-ins para Windows	Plug-in para Windows	Host do Exchange Server	Windows
Plug-in SnapCentre para Oracle Database	Pacote de plug-ins para Linux e pacote de plug-ins para AIX	Plug-in para UNIX	Host Oracle	Linux ou AIX

Nome do plug-in	Incluído no pacote de instalação	Requer outros plug-ins	Instalado no host	Plataforma suportada
Plug-in do SnapCenter para banco de dados SAP HANA	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou plug-in para Windows	Host cliente HDBSQL	Linux ou Windows
Plug-in SnapCenter para IBM DB2	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou plug-in para Windows	DB2 host	Linux, AIX ou Windows
Plug-in SnapCenter para PostgreSQL	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou plug-in para Windows	PostgreSQL host	Linux ou Windows
Plug-in SnaoCenter para MySQL	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou Plug-in para Windows	MySQL host	Linux ou Windows
Plug-in do SnapCenter para MongoDB	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou plug-in para Windows	Host MongoDB	Linux ou Windows
Plug-in SnapCenter para ORASCPM (aplicações Oracle)	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou plug-in para Windows	Host Oracle	Linux ou Windows
Plug-in do SnapCenter para SAP ASE	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou plug-in para Windows	Host SAP	Linux ou Windows
Plug-in SnapCenter para SAP MaxDB	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou plug-in para Windows	Host SAP MaxDB	Linux ou Windows
Plug-in SnapCenter para plug-in de storage	Pacote de plug-ins para Linux e pacote Plug-ins para Windows	Plug-in para UNIX ou plug-in para Windows	Host de storage	Linux ou Windows

O SnapCenter Plug-in for VMware vSphere oferece suporte a operações de backup e restauração consistentes em caso de falhas e em VMs para máquinas virtuais (VMs), armazenamentos de dados e discos

de máquina virtual (VMDKs). Ele também oferece suporte a operações de backup e restauração consistentes com aplicativos para bancos de dados virtualizados e sistemas de arquivos.

Para proteger bancos de dados, sistemas de arquivos, VMs ou armazenamentos de dados em VMs, implante o SnapCenter Plug-in for VMware vSphere . Para obter informações, consulte "Plug-in do SnapCenter para documentação do VMware vSphere" .

Repositório SnapCenter

O repositório do SnapCenter, às vezes chamado de banco de dados NSM, armazena informações e metadados para cada operação do SnapCenter.

A instalação do SnapCenter Server instala o banco de dados do repositório do MySQL Server por padrão. Se você já instalou o MySQL Server e deseja executar uma nova instalação do SnapCenter Server, desinstale o MySQL Server.

O SnapCenter suporta o MySQL Server 8.0.37 ou posterior como banco de dados de repositório do SnapCenter . Se você usar uma versão anterior do MySQL Server com uma versão anterior do SnapCenter, o processo de atualização do SnapCenter atualizará o MySQL Server para a versão 8.0.37 ou posterior.

O repositório do SnapCenter armazena as seguintes informações e metadados:

- Metadados de backup, clone, restauração e verificação
- Informações sobre relatórios, trabalhos e eventos
- Informações de host e plug-in
- Detalhes de função, usuário e permissão
- Informações de conexão do sistema de armazenamento

Recursos de segurança no SnapCenter

A SnapCenter emprega recursos rígidos de segurança e autenticação para permitir que você mantenha seus dados seguros.

O SnapCenter inclui os seguintes recursos de segurança:

- Toda a comunicação com o SnapCenter usa HTTP sobre SSL (HTTPS).
- Todas as credenciais no SnapCenter são protegidas usando criptografia AES (Advanced Encryption Standard).
- Suporta algoritmos de segurança compatíveis com o Federal Information Processing Standard (FIPS).
- Suporte ao uso dos certificados de CA autorizados fornecidos pelo cliente.
- Suporta TLS (Transport Layer Security) 1,3 para comunicação com o ONTAP. Você também pode usar o TLS 1,2 para comunicação entre clientes e servidores.
- Suporta um determinado conjunto de pacotes de criptografia SSL para fornecer segurança em toda a comunicação de rede. "Saiba mais".
- O SnapCenter é instalado no firewall da sua empresa para permitir o acesso ao servidor SnapCenter e para permitir a comunicação entre o servidor SnapCenter e os plug-ins.
- O acesso à API e à operação do SnapCenter usa tokens criptografados com criptografia AES, que expiram após 24 horas.

- O SnapCenter é integrado ao Windows active Directory para login e controle de acesso baseado em função (RBAC) que regem as permissões de acesso.
- O IPsec é compatível com o SnapCenter no ONTAP para máquinas host Windows e Linux. "Saiba mais".
- Os cmdlets do SnapCenter PowerShell são protegidos por sessão.
- Após um período padrão de 15 minutos de inatividade, o SnapCenter avisa que você será desconetado em 5 minutos.

  Após 20 minutos de inatividade, o SnapCenter faz o logout e você deve fazer login novamente. Você pode modificar o período de logout.

- O início de sessão está temporariamente desativado após 5 tentativas de início de sessão incorretas.
- Suporta autenticação de certificado CA entre o servidor SnapCenter e o ONTAP. "Saiba mais".
- O verificador de integridade é adicionado ao servidor SnapCenter e aos plug-ins e valida todos os binários enviados durante novas operações de instalação e atualização.

Visão geral do certificado CA

O instalador do servidor SnapCenter permite o suporte centralizado de certificados SSL durante a instalação. Para melhorar a comunicação segura entre o servidor e o plug-in, o SnapCenter suporta o uso dos certificados de CA autorizados fornecidos pelo cliente.

Você deve implantar certificados de CA depois de instalar o servidor SnapCenter e os respetivos plug-ins. Para obter mais informações, "Gerar arquivo CSR do certificado CA"consulte .

Você também pode implantar o certificado CA para o plug-in SnapCenter para VMware vSphere. Para obter mais informações, "Criar e importar certificados"consulte .

Comunicação SSL bidirecional

A comunicação SSL bidirecional protege a comunicação mútua entre o servidor SnapCenter e os plug-ins.

Visão geral da autenticação baseada em certificados

A autenticação baseada em certificado verifica a autenticidade dos respetivos usuários que tentam acessar o host do plug-in do SnapCenter. O usuário deve exportar o certificado do servidor SnapCenter sem chave privada e importá-lo no armazenamento confiável do host do plug-in. A autenticação baseada em certificado só funciona se o recurso SSL bidirecional estiver ativado.

Autenticação multifator (MFA)

O MFA usa um provedor de identidade (IDP) de terceiros por meio da Security Assertion Markup Language (SAML) para gerenciar sessões de usuários. Esta funcionalidade melhora a segurança de autenticação, tendo a opção de utilizar vários fatores, como TOTP, biometria, notificações push, etc., juntamente com o nome de utilizador e palavra-passe existentes. Além disso, ele permite que o cliente use seus próprios provedores de identidade de usuário para obter login de usuário unificado (SSO) em todo o portfólio.

O MFA é aplicável apenas para login na IU do servidor SnapCenter. Os logins são autenticados por meio dos Serviços de Federação do ative Directory (AD FS) do IDP. Você pode configurar vários fatores de autenticação no AD FS. O SnapCenter é o provedor de serviços e você deve configurar o SnapCenter como uma parte confiável no AD FS. Para ativar o MFA no SnapCenter, você precisará dos metadados do AD FS.

Para obter informações sobre como ativar o MFA, "Ativar a autenticação multifator"consulte .

Controles de acesso baseados em função no SnapCenter

O controle de acesso baseado em função (RBAC) do SnapCenter e as permissões ONTAP permitem que os administradores do SnapCenter atribuam acesso a recursos a usuários ou grupos. Esse acesso gerenciado centralmente permite que os administradores de aplicativos trabalhem com segurança em ambientes designados.

Você deve criar ou modificar funções e adicionar acesso a recursos aos usuários. Ao configurar o SnapCenter pela primeira vez, adicione usuários ou grupos do Active Directory às funções e atribua recursos a esses usuários ou grupos.

O SnapCenter não cria contas de usuários ou grupos. Crie contas de usuário ou grupo no Active Directory do sistema operacional ou no banco de dados.

Tipos de RBAC no SnapCenter

O SnapCenter oferece suporte aos seguintes tipos de controle de acesso baseado em função:

- SnapCenter RBAC
- RBAC no nível da aplicação
- Plug-in do SnapCenter para VMware vSphere RBAC
- Permissões da ONTAP

SnapCenter RBAC

O SnapCenter tem funções predefinidas e você pode atribuir usuários ou grupos a essas funções.

- Função de administrador do SnapCenter
- Função de Administrador de cópia de Segurança e Clonagem de aplicações
- Função Visualizador de cópia de Segurança e Clonagem
- Função de administrador de infraestrutura

Quando você atribui uma função a um usuário, o SnapCenter exibe os trabalhos relevantes para esse usuário na página Trabalhos, a menos que o usuário tenha a função SnapCenterAdmin.

Você também pode criar novas funções e gerenciar permissões e usuários. Você pode atribuir permissões a usuários ou grupos para acessar objetos do SnapCenter, como hosts, conexões de storage e grupos de recursos.

É possível atribuir permissões RBAC a usuários e grupos dentro da mesma floresta e a usuários pertencentes a diferentes florestas. Não é possível atribuir permissões RBAC a usuários pertencentes a grupos aninhados entre florestas.

Ao criar uma função personalizada, certifique-se de que ela inclua todas as permissões da função SnapCenterAdmin. Se você copiar apenas algumas permissões, o SnapCenter impedirá que você execute todas as operações.

Os usuários devem se autenticar ao efetuar login por meio da interface do usuário ou dos cmdlets do PowerShell. Se os usuários tiverem várias funções, eles selecionarão uma função após efetuar login. A

autenticação também é necessária para executar APIs.

RBAC no nível da aplicação

O SnapCenter usa credenciais para verificar se os usuários autorizados do SnapCenter também têm permissões no nível do aplicativo.

Por exemplo, para executar operações de proteção de dados em um ambiente SQL Server, defina as credenciais corretas do Windows ou SQL. Se você quiser executar operações de proteção de dados em um ambiente de sistema de arquivos do Windows no armazenamento ONTAP , a função de administrador do SnapCenter deverá ter privilégios de administrador no host do Windows.

Da mesma forma, se você quiser executar operações de proteção de dados em um banco de dados Oracle e se a autenticação do sistema operacional (SO) estiver desabilitada no host do banco de dados, você deverá definir credenciais com as credenciais do banco de dados Oracle ou do Oracle ASM. O SnapCenter Server autentica o conjunto de credenciais usando um destes métodos, dependendo da operação.

Plug-in do SnapCenter para VMware vSphere RBAC

Se você estiver usando o plug-in SnapCenter VMware para proteção de dados consistente com VM, o vCenter Server fornecerá um nível adicional de RBAC. O plug-in SnapCenter VMware é compatível com o vCenter Server RBAC e o ONTAP RBAC. "Saiba mais"

OBSERVAÇÃO: a NetApp recomenda que você crie uma função ONTAP para as operações do SnapCenter Plug-in for VMware vSphere e atribua a ela todos os privilégios necessários.

Permissões da ONTAP

Você deve criar uma conta vsadmin com as permissões necessárias para acessar o sistema de armazenamento."Saiba mais"

Permissões atribuídas às funções SnapCenter predefinidas

Ao adicionar um usuário a uma função, atribua a permissão StorageConnection para habilitar a comunicação da máquina virtual de armazenamento (SVM) ou atribua uma SVM ao usuário para conceder permissão para usar a SVM. A permissão Conexão de armazenamento permite que os usuários criem conexões SVM.

Por exemplo, um administrador do SnapCenter pode criar conexões SVM e atribuí-las a usuários de backup de aplicativo e administrador de clone, que não podem criar ou editar conexões SVM. Sem uma conexão SVM, os usuários não podem executar operações de backup, clonagem ou restauração.

Função de administrador do SnapCenter

A função de administrador do SnapCenter tem todas as permissões ativadas. Não é possível modificar as permissões para esta função. Você pode adicionar usuários e grupos à função ou removê-los.

Função de Administrador de cópia de Segurança e Clonagem de aplicações

A função App Backup and Clone Admin tem as permissões necessárias para executar ações administrativas para backups de aplicativos e tarefas relacionadas a clones. Essa função não tem permissões para gerenciamento de host, provisionamento, gerenciamento de conexão de storage ou instalação remota.

Permissões	Ativado	Criar	Leia	Atualização	Eliminar
Grupo recursos	Não aplicável	Sim	Sim	Sim	Sim
Política	Não aplicável	Sim	Sim	Sim	Sim
Backup	Não aplicável	Sim	Sim	Sim	Sim
Host	Não aplicável	Sim	Sim	Sim	Sim
Ligação de armazenamento	Não aplicável	Não	Sim	Não	Não
Clone	Não aplicável	Sim	Sim	Sim	Sim
Provisionamento	Não aplicável	Não	Sim	Não	Não
Painel de instrumentos	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Relatórios	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Restaurar	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Recurso	Sim	Sim	Sim	Sim	Sim
Instalação/desinstalação do plug-in	Não	Não aplicável		Não aplicável	Não aplicável
Migração	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Montagem	Sim	Sim	Não aplicável	Não aplicável	Não aplicável
Desmontar	Sim	Sim	Não aplicável	Não aplicável	Não aplicável
Restauração completa do volume	Não	Não	Não aplicável	Não aplicável	Não aplicável
Em segundo lugar proteção	Não	Não	Não aplicável	Não aplicável	Não aplicável
Monitor de trabalho	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Função Visualizador de cópia de Segurança e Clonagem

A função Visualizador de Backup e Clone tem a visualização somente leitura de todas as permissões. Essa função também tem permissões habilitadas para descoberta, relatórios e acesso ao Painel.

Permissões	Ativado	Criar	Leia	Atualização	Eliminar
Grupo recursos	Não aplicável	Não	Sim	Não	Não
Política	Não aplicável	Não	Sim	Não	Não
Backup	Não aplicável	Não	Sim	Não	Não
Host	Não aplicável	Não	Sim	Não	Não
Ligação de armazenamento	Não aplicável	Não	Sim	Não	Não
Clone	Não aplicável	Não	Sim	Não	Não
Provisionamento	Não aplicável	Não	Sim	Não	Não
Painel de instrumentos	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Relatórios	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Restaurar	Não	Não	Não aplicável	Não aplicável	Não aplicável
Recurso	Não	Não	Sim	Sim	Não
Instalação/desinstalação do plug-in	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Migração	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Montagem	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Desmontar	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Restauração completa do volume	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Em segundo lugar proteção	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Permissões	Ativado	Criar	Leia	Atualização	Eliminar
Monitor de trabalho	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Função de administrador de infraestrutura

A função Administrador de infraestrutura tem permissões habilitadas para gerenciamento de host, gerenciamento de storage, provisionamento, grupos de recursos, relatórios de instalação remota e acesso ao Dashboard.

Permissões	Ativado	Criar	Leia	Atualização	Eliminar
Grupo recursos	Não aplicável	Sim	Sim	Sim	Sim
Política	Não aplicável	Não	Sim	Sim	Sim
Backup	Não aplicável	Sim	Sim	Sim	Sim
Host	Não aplicável	Sim	Sim	Sim	Sim
Ligação de armazenamento	Não aplicável	Sim	Sim	Sim	Sim
Clone	Não aplicável	Não	Sim	Não	Não
Provisionamento	Não aplicável	Sim	Sim	Sim	Sim
Painel de instrumentos	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Relatórios	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Restaurar	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Recurso	Sim	Sim	Sim	Sim	Sim
Instalação/desinstalação do plug-in	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Migração	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Montagem	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Desmontar	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Permissões	Ativado	Criar	Leia	Atualização	Eliminar
Restauração completa do volume	Não	Não	Não aplicável	Não aplicável	Não aplicável
Em segundo lugar proteção	Não	Não	Não aplicável	Não aplicável	Não aplicável
Monitor de trabalho	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Recuperação de desastres em SnapCenter

O recurso de recuperação de desastres (DR) do SnapCenter permite que você se recupere de desastres como corrupção de recursos ou falhas do servidor. Ele ajuda a restaurar o repositório do SnapCenter, as programações do servidor, os componentes de configuração e o plug-in do SnapCenter para SQL Server e seu armazenamento.

Esta seção explica os dois tipos de DR no SnapCenter:

DR do servidor SnapCenter

- Os dados do servidor SnapCenter são copiados e podem ser recuperados sem nenhum plug-in adicionado ou gerenciado pelo servidor SnapCenter.
- O servidor SnapCenter secundário deve ser instalado no mesmo diretório de instalação e na mesma porta que o servidor SnapCenter primário.
- Para autenticação multifator (MFA), durante a recuperação de desastres do servidor SnapCenter, feche todas as guias do navegador e reabra um navegador para fazer login novamente. Isso apagará os cookies de sessão existentes ou ativos e atualizará os dados de configuração corretos.
- A funcionalidade de recuperação de desastres do SnapCenter usa APIS REST para fazer backup do servidor SnapCenter. "Workflows de API REST para recuperação de desastres do servidor SnapCenter"Consulte .
- O arquivo de configuração relacionado às configurações de auditoria não é feito backup no backup de DR e nem no servidor de DR após a operação de restauração. Deve repetir manualmente as definições do registo de auditoria.

Plug-in do SnapCenter e recuperação de desastres de storage

O DR está disponível apenas para o plug-in SnapCenter para SQL Server. Se o plug-in estiver inativo, mude para outro host SQL e recupere os dados seguindo alguns passos. "Recuperação de desastres do plug-in SnapCenter para SQL Server"Consulte .

O SnapCenter usa o ONTAP SnapMirror para replicar dados, que podem ser usados para a recuperação de desastres mantendo os dados sincronizados em um local secundário. Para iniciar o failover, interrompa a replicação do SnapMirror. Durante o fallback, inverta a sincronização para replicar dados do local de DR de volta para o local principal.

Licenças exigidas pela SnapCenter

O SnapCenter requer várias licenças para habilitar a proteção de dados de aplicativos, bancos de dados, sistemas de arquivos e máquinas virtuais. O tipo de licenças do SnapCenter que você instala depende do ambiente de storage e dos recursos que deseja usar.

Licença	Quando necessário
Baseado em controladora padrão da SnapCenter	Necessário para FAS, AFF, ASA A licença padrão da SnapCenter é uma licença baseada em controlador e está incluída como parte do NetApp ONTAP One. Se você tiver a licença do SnapManager Suite, você também obtém o direito de licença padrão do SnapCenter. Se você quiser instalar o SnapCenter em uma base de avaliação com o storage FAS, AFF ou ASA, poderá obter uma licença de avaliação do NetApp ONTAP One entrando em Contato com o representante de vendas. Para obter informações sobre as licenças incluídas no NetApp ONTAP One, "Licenças incluídas no NetApp ONTAP One" consulte . O SnapCenter também é oferecido como parte do pacote de proteção de dados. Se você comprou o A400 ou posterior, você deve comprar o pacote de proteção de dados.
SnapMirror ou SnapVault	ONTAP A licença SnapMirror ou SnapVault é necessária se a replicação estiver ativada no SnapCenter.
SnapRestore	Necessário para restaurar e verificar backups. Em sistemas de storage primário • Necessário nos sistemas de destino do SnapVault para executar a verificação remota e restaurar a partir de um backup. • Necessário nos sistemas de destino SnapMirror para efetuar a verificação remota.

Licença	Quando necessário
FlexClone	Necessário clonar bancos de dados e operações de verificação. Em sistemas de storage primário e secundário • Necessário nos sistemas de destino do SnapVault para criar clones a partir do backup do Vault secundário. • Necessário nos sistemas de destino do SnapMirror para criar clones do backup secundário do SnapMirror.
Licenças de protocolo	• Licença iSCSI ou FC para LUNs • Licença CIFS para compartilhamentos SMB • Licença NFS para VMDKs do tipo NFS • Licença iSCSI ou FC para VMDKs do tipo VMFS Necessário nos sistemas de destino do SnapMirror para fornecer dados se um volume de origem não estiver disponível.
Licenças padrão da SnapCenter (opcional)	Destinos secundários É recomendado, mas não obrigatório, que você adicione licenças padrão do SnapCenter a destinos secundários. Se as licenças padrão do SnapCenter não estiverem habilitadas em destinos secundários, você não poderá usar o SnapCenter para fazer backup de recursos no destino secundário após executar uma operação de failover. No entanto, é necessária uma licença FlexClone em destinos secundários para executar operações de clonagem e verificação.

Licença	Quando necessário
Licenças SMBR (Single Mailbox Recovery)	Se você estiver usando o plug-in do SnapCenter para gerenciar bancos de dados do Microsoft Exchange Server e a recuperação de caixa de correio única (SMBR), você precisará de licença adicional para SMBR, que precisa ser adquirida separadamente com base na caixa de correio do usuário. A recuperação de caixa de correio única NetApp chegou ao fim da disponibilidade (EOA) em 12 de maio de 2023. Para obter mais informações, "CPC-00507"consulte . A NetApp continuará a oferecer suporte a clientes que adquiriram capacidade, manutenção e suporte da caixa de correio por meio de números de peça de marketing introduzidos em 24 de junho de 2020, durante o período do direito ao suporte. O NetApp Single Mailbox Recovery é um produto parceiro fornecido pela Ontrack. O Ontrack PowerControls oferece recursos semelhantes aos da recuperação de caixa de correio única do NetApp. Os clientes podem adquirir novas licenças de software Ontrack PowerControls e renovações de manutenção e suporte Ontrack PowerControls do Ontrack (até licensingteam@ontrack.com) para recuperação granular da caixa de correio após a data EOA de 12 de maio de 2023.

As licenças do SnapCenter Advanced e do SnapCenter nas File Services estão obsoletas e não estão mais disponíveis. A licença padrão e a licença baseada em capacidade não são mais necessárias para o Amazon FSX for NetApp ONTAP, ONTAP Select, Cloud Volumes ONTAP e Azure NetApp Files.

Você deve instalar uma ou mais licenças do SnapCenter. Para obter informações sobre como adicionar licenças, "Adicione licenças padrão baseadas em controladora SnapCenter"consulte .

Sincronização ativa do SnapMirror no SnapCenter

O SnapMirror active Sync permite que os serviços empresariais continuem operando mesmo em uma falha completa do local, com suporte ao failover de aplicações de forma transparente, usando uma cópia secundária. Nem a intervenção manual nem o script adicional são necessários para acionar um failover com a sincronização ativa do SnapMirror.

Para obter mais informações sobre a sincronização ativa do SnapMirror, "Descrição geral da sincronização ativa do SnapMirror"consulte .

Para a sincronização ativa do SnapMirror, verifique se você atendeu aos vários requisitos de configuração de hardware, software e sistema. Para obter informações, consulte "Pré-requisitos"

Os plug-ins suportados para esse recurso são plug-in SnapCenter para SQL Server, plug-in SnapCenter para Windows, plug-in SnapCenter para banco de dados Oracle, plug-in SnapCenter para banco de dados SAP HANA, plug-in SnapCenter para Microsoft Exchange Server e plug-in SnapCenter para Unix.

Depois de instalar o SnapCenter Server e os plug-ins, você deve habilitar a API REST para o SnapCenter para detectar relacionamentos de sincronização ativos do SnapMirror .

- No host do servidor SnapCenter , edite o arquivo *C:\Program Files\ NetApp\SMCore\SMCoreServiceHost.dll.config* para modificar o valor do parâmetro *IsRestEnabledForStorageConnection* para *true* e reinicie o serviço SnapCenter SMCore.
- Nos hosts de plug-in do Windows:
  - Edite o arquivo *C:\Program Files\ NetApp\ SnapCenter\SMCore\SMCoreServiceHost.dll.config* para modificar o valor do parâmetro *IsRestEnabledForStorageConnection* para *true*.
  - Edite o arquivo *C:\Program Files\ NetApp\ SnapCenter\SMCore\SnapDriveService.dll.config* para modificar o valor do parâmetro *IsRestEnabledForStorageConnection* para *true*.
  - Reinicie o serviço SnapCenter SMCore.

Para suportar a proximidade do iniciador do host no SnapCenter, seu valor, origem ou destino deve ser definido no ONTAP.

Os casos de uso não suportados no SnapCenter:

- Se você converter as cargas de trabalho de sincronização ativa assimétrica do SnapMirror existentes para simétricas alterando a política nas relações de sincronização ativa do SnapMirror de *automatedfailover* para *automatedfailoverduplex* no ONTAP, o mesmo não será suportado no SnapCenter.
- Se houver backups de um grupo de recursos (já protegido no SnapCenter) e a política de armazenamento for alterada nas relações de sincronização ativa do SnapMirror de *automatedfailover* para *automatedfailoverduplex* no ONTAP, o mesmo não é suportado no SnapCenter.

Conceitos-chave de proteção de dados

Antes de usar o SnapCenter, entenda os principais conceitos de backup, clonagem e restauração.

Recursos

Os recursos incluem bancos de dados, sistemas de arquivos do Windows ou compartilhamentos de arquivos copiados ou clonados com o SnapCenter. Dependendo do seu ambiente, os recursos também podem ser instâncias de banco de dados, grupos de disponibilidade do SQL Server, bancos de dados Oracle, bancos de dados RAC ou grupos de aplicativos personalizados.

Grupo de recursos

Um grupo de recursos é um conjunto de recursos em um host ou cluster, potencialmente de vários hosts e clusters. As operações realizadas em um grupo de recursos se aplicam a todos os seus recursos com base no cronograma especificado. É possível executar backups programados ou sob demanda para recursos ou grupos individuais.

Se um host em um grupo de recursos compartilhados entrar no modo de manutenção, todas as operações agendadas para esse grupo serão suspensas em todos os hosts.

Use plug-ins relevantes para fazer backup de recursos específicos: Plug-ins de banco de dados para bancos de dados, plug-ins do sistema de arquivos para sistemas de arquivos e plug-in do SnapCenter para VMware vSphere para VMs e datastores.

Políticas

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

Uma ou mais políticas podem ser selecionadas ao criar um grupo de recursos ou ao executar um backup sob demanda.

Um grupo de recursos define o que precisa ser protegido e quando deve ser protegido em termos de dia e hora. Uma política descreve como a proteção será realizada. Por exemplo, se o backup de todos os bancos de dados ou sistemas de arquivos de um host for necessário, um grupo de recursos incluindo todos os bancos de dados ou sistemas de arquivos no host pode ser criado. Duas políticas poderiam então ser anexadas ao grupo de recursos: Uma política diária e uma política por hora.

Ao criar o grupo de recursos e anexar as políticas, é possível configurá-lo para executar um backup completo diário e outro agendamento para backups de log por hora.

Prescripts e postscripts personalizados podem ser usados em operações de proteção de dados. Esses scripts permitem a automação antes ou depois do trabalho de proteção de dados. Por exemplo, um script pode notificar automaticamente falhas ou avisos de trabalhos de proteção de dados. Entender os requisitos para criar esses scripts é crucial antes de configurar prescripts e postscripts.

Grupo de consistência (GC)

Um grupo de consistência é uma coleção de volumes gerenciados como uma única unidade. Os CGs são sincronizados para consistência de dados em unidades de armazenamento e volumes. No ONTAP, eles fornecem gerenciamento fácil e uma garantia de proteção para uma carga de trabalho de aplicativo abrangendo vários volumes. Saiba mais sobre "grupos de consistência" .

Uso de prescripts e postscripts

Prescripts e postscripts personalizados podem automatizar suas tarefas de proteção de dados antes ou depois do trabalho. Por exemplo, você pode adicionar um script para notificá-lo de falhas ou avisos de trabalhos. Antes de configurá-los, certifique-se de entender os requisitos para esses scripts.

Tipos de script suportados

Os seguintes tipos de scripts são suportados para o Windows:

- Arquivos em lote
- Scripts do PowerShell
- Scripts Perl

Os seguintes tipos de scripts são suportados para UNIX:

- Scripts Perl
- Scripts Python
- Scripts de shell

Junto com shell bash padrão outros shells como sh-shell, k-shell e c-shell também são suportados.

Caminho do script

Todos os prescripts e pós-scripts executados como parte das operações do SnapCenter em sistemas de storage não virtualizados e virtualizados, são executados no host do plug-in.

- Os scripts do Windows devem estar localizados no host do plug-in.

O caminho de prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_path.

- Os scripts UNIX devem estar localizados no host do plug-in.

O caminho do script é validado no momento da execução.

Onde especificar scripts

Os scripts são especificados nas políticas de backup. Quando um trabalho de backup é iniciado, a política associa automaticamente o script aos recursos que estão sendo copiados. Ao criar uma política de backup, você pode especificar os argumentos prescritor e postscript.

Não é possível especificar vários scripts.

Tempos limite de script

O tempo limite é definido para 60 segundos, por padrão. Você pode modificar o valor de tempo limite.

Saída de script

O diretório padrão para os arquivos de saída de prescripts e postscripts do Windows é o Windows System32.

Não há local padrão para as prescripts e postscripts UNIX. Você pode redirecionar o arquivo de saída para qualquer local preferido.

Sistemas e aplicações de storage com suporte da SnapCenter

Você deve conhecer os sistemas de storage, aplicações e bancos de dados compatíveis com o SnapCenter.

Sistemas de storage compatíveis

- NetApp ONTAP 9.12.1 e posterior
- Azure NetApp Files
- Amazon FSX para NetApp ONTAP

O Amazon FSx for NetApp ONTAP oferece suporte à memória expressa não volátil (NVMe) por meio do

Protocolo de Controle de Transporte (TCP).

Para obter informações sobre o Amazon FSX for NetApp ONTAP, "Documentação do Amazon FSX para NetApp ONTAP" consulte .

- Sistemas NetApp ASA r2 que executam o NetApp ONTAP 9.16.1 e posterior

  Você deve usar o ONTAP 9.17.1 se estiver usando o SnapCenter Server 6.2 e os plug-ins do SnapCenter 6.2.

Aplicativos e bancos de dados compatíveis

O SnapCenter oferece suporte à proteção de diferentes aplicativos e bancos de dados.

O SnapCenter é compatível com a proteção de workloads Oracle e Microsoft SQL em ambientes de data center definido por software (SDDC) da Amazon. "Saiba mais".

Métodos de autenticação para credenciais SnapCenter

As credenciais usam diferentes métodos de autenticação, dependendo do aplicativo ou do ambiente. As credenciais autenticam os usuários para que eles possam executar operações do SnapCenter. Você deve criar um conjunto de credenciais para instalar plug-ins e outro para operações de proteção de dados.

Autenticação do Windows

O método de autenticação do Windows é autenticado no ative Directory. Para autenticação do Windows, o ative Directory é configurado fora do SnapCenter. O SnapCenter se autentica sem configuração adicional. Você precisa de uma credencial do Windows para adicionar hosts, instalar pacotes de plug-in e agendar trabalhos.

Autenticação de domínio não confiável

O SnapCenter permite que usuários e grupos pertencentes a domínios não confiáveis criem credenciais do Windows. Para que a autenticação seja bem-sucedida, você deve Registrar os domínios não confiáveis com o SnapCenter.

Autenticação local do grupo de trabalho

O SnapCenter permite a criação de credenciais do Windows com usuários e grupos de trabalho locais. A autenticação do Windows para usuários e grupos de grupos de trabalho locais não acontece durante a criação de credenciais do Windows, mas é adiada até que o Registro do host e outras operações de host sejam executadas.

Autenticação do SQL Server

O método de autenticação SQL é autenticado em uma instância do SQL Server. Isso significa que uma instância do SQL Server deve ser descoberta no SnapCenter. Portanto, antes de adicionar uma credencial SQL, você deve adicionar um host, instalar pacotes de plug-in e atualizar recursos. Você precisa de autenticação do SQL Server para executar operações como agendamento no SQL Server ou descoberta de recursos.

Autenticação Linux

O método de autenticação Linux é autenticado em um host Linux. Você precisa de autenticação Linux durante a etapa inicial de adicionar o host Linux e instalar o pacote de plug-ins do SnapCenter remotamente a partir da GUI do SnapCenter.

Autenticação AIX

O método de autenticação AIX é autenticado em um host AIX. Você precisa de autenticação AIX durante a etapa inicial de adicionar o host AIX e instalar o pacote de plug-ins do SnapCenter para AIX remotamente a partir da GUI do SnapCenter.

Autenticação de banco de dados Oracle

O método de autenticação de banco de dados Oracle é autenticado em um banco de dados Oracle. Você precisa de uma autenticação de banco de dados Oracle para executar operações no banco de dados Oracle se a autenticação do sistema operacional (os) estiver desativada no host do banco de dados. Portanto, antes de adicionar uma credencial de banco de dados Oracle, você deve criar um usuário Oracle no banco de dados Oracle com sysdba Privileges.

Autenticação Oracle ASM

O método de autenticação Oracle ASM é autenticado em uma instância do Oracle Automatic Storage Management (ASM). A autenticação Oracle ASM é necessária se você precisar acessar uma instância do Oracle ASM e a autenticação do SO estiver desativada no host do banco de dados. Antes de adicionar uma credencial Oracle ASM, crie um usuário Oracle com System Privileges na instância ASM.

Autenticação de catálogo RMAN

O método de autenticação de catálogo RMAN é autenticado no banco de dados de catálogo do Oracle Recovery Manager (RMAN). Se você configurou um mecanismo de catálogo externo e registrou seu banco de dados no banco de dados de catálogo, você precisa adicionar autenticação de catálogo RMAN.

Informações sobre direitos autorais

Informações sobre marcas comerciais