Saiba mais sobre o SnapCenter software

SnapCenter software

NetApp
November 06, 2025

Índice

Saiba mais sobre o SnapCenter software

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 eficiência de espaço, consistentes com o aplicativo e baseados em disco
- Restauração rápida e detalhada e recuperação consistente com o aplicativo
- Clonagem rápida e com economia 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 que estão nos sistemas primários ONTAP FAS, AFF ou ASA e replicados para os sistemas secundários ONTAP FAS, AFF ou ASA
  - Dados que estão nos sistemas primários ONTAP Select
  - Dados que estão nos sistemas primários e secundários ONTAP FAS, AFF ou ASA e protegidos no armazenamento de objetos StorageGRID local
  - Dados que estão nos sistemas primário e secundário ONTAP ASA r2
- No local em uma Nuvem Híbrida para proteger o seguinte:
  - Dados que estão nos sistemas primários ONTAP FAS, AFF ou ASA e replicados para o 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 que estão nos sistemas primários do Cloud Volumes ONTAP (anteriormente ONTAP Cloud)
  - Dados que estão no Amazon FSX para ONTAP
  - Dados que estão nos Azure NetApp Files (Oracle, Microsoft SQL e SAP HANA)

Principais características

O SnapCenter oferece os seguintes recursos principais:

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

  A proteção de dados é suportada pelo Microsoft Exchange Server, Microsoft SQL Server, Oracle

Databases no Linux ou AIX, banco de dados SAP HANA, IBM Db2, PostgreSQL, MySQL e Windows Host Filesystems executados 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 rápidas e granulares de backups e recuperação consistente com o aplicativo e baseada em tempo. Você pode restaurar 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.

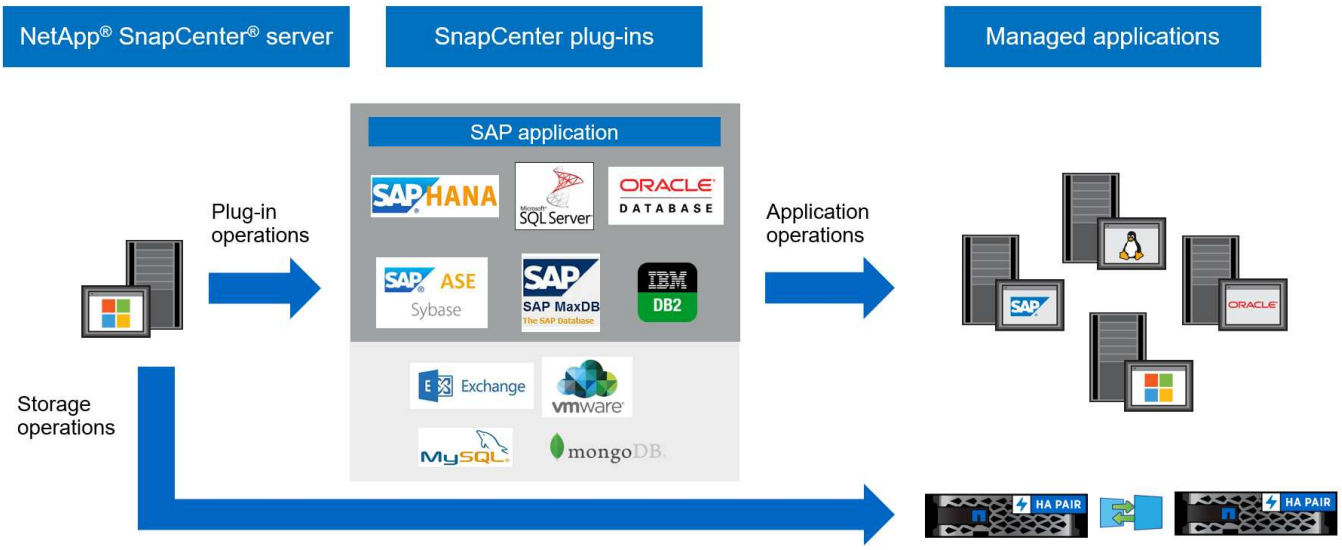
- APIs REST, cmdlets do Windows, comandos UNIX

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

- Painel e relatórios centralizados de proteção de dados
- Controle de acesso baseado em função (RBAC) para segurança e delegação
- Um banco de dados de repositório integrado com alta disponibilidade para armazenar todos os metadados de backup
- Instalação automática de plug-ins
- Alta disponibilidade
- Recuperação de Desastres (DR)
- SnapLock "Saber mais"
- Sincronização ativa do SnapMirror (inicialmente lançado como SnapMirror Business Continuity [SM-BC])
- Espelhamento síncrono "Saber 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 SnapCenter Server, o pacote SnapCenter Plug-in para Windows e o pacote SnapCenter Plug-In para Linux. Cada pacote contém plug-ins para vários aplicativos e componentes de infraestrutura.

Servidor SnapCenter

O SnapCenter Server oferece suporte aos sistemas operacionais Microsoft Windows e Linux (RHEL 8.x, RHEL 9.x, SLES 15 SP5). O servidor SnapCenter inclui um servidor 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 oferece suporte a ambientes, bancos de dados e aplicativos específicos.

Nome do plug-in	Incluído no pacote de instalação	Requer outros plug-ins	Instalado no host	Plataforma suportada
Plug-in 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 do Windows	Windows
Plug-in 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 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 do 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	Host Db2	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	Host PostgreSQL	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	Host MySQL	Linux ou Windows
Plug-in 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 (Aplicativos 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 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 armazenamento	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou plug-in para Windows	Host de armazenamento	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 "Documentação do SnapCenter Plug-in for VMware vSphere" .

Repositório SnapCenter

O repositório 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 SnapCenter armazena as seguintes informações e metadados:

- Backup, clonagem, restauração e verificação de metadados
- Relatórios, informações sobre empregos 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

O SnapCenter emprega recursos rigorosos 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 Advanced Encryption Standard (AES).
- Suporta algoritmos de segurança compatíveis com o Padrão Federal de Processamento de Informações (FIPS).
- Suporta o uso de certificados de CA autorizados fornecidos pelo cliente.
- Suporta Transport Layer Security (TLS) 1.3 para comunicação com ONTAP. Você também pode usar o TLS 1.2 para comunicação entre clientes e servidores.
- Oferece suporte a um determinado conjunto de conjuntos de cifras SSL para fornecer segurança na comunicação de rede. "Saber mais" .
- O SnapCenter é instalado dentro do firewall da sua empresa para permitir o acesso ao SnapCenter Server e permitir a comunicação entre o SnapCenter Server 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 integra-se ao Windows Active Directory para login e controle de acesso baseado em função (RBAC) que controlam as permissões de acesso.
- O IPsec é compatível com o SnapCenter no ONTAP para máquinas host Windows e Linux. "Saber 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 desconectado em 5 minutos.

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

- O login é temporariamente desativado após 5 tentativas incorretas de login.
- Suporta autenticação de certificado CA entre SnapCenter Server e ONTAP. "Saber mais" .
- O Integrity Verifier é adicionado ao SnapCenter Server 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 SnapCenter Server habilita o suporte ao certificado SSL centralizado durante a instalação. Para melhorar a comunicação segura entre o servidor e o plug-in, o SnapCenter oferece suporte ao uso de certificados de CA autorizados fornecidos pelo cliente.

Você deve implantar certificados de CA após instalar o SnapCenter Server e os respectivos plug-ins. Para obter mais informações, consulte "Gerar arquivo CSR de certificado CA" .

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

Comunicação SSL bidirecional

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

Visão geral da autenticação baseada em certificado

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

Autenticação multifator (MFA)

O MFA usa um Provedor de Identidade (IdP) de terceiros por meio da Linguagem de Marcação de Asserção de Segurança (SAML) para gerenciar sessões de usuários. Essa funcionalidade aumenta a segurança da autenticação ao oferecer a opção de usar vários fatores, como TOTP, biometria, notificações push etc., juntamente com o nome de usuário e a senha 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 seu portfólio.

O MFA é aplicável somente ao login da interface de usuário do SnapCenter Server. Os logins são autenticados por meio do IdP Active Directory Federation Services (AD FS). 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 habilitar o MFA no SnapCenter, você precisará dos

metadados do AD FS.

Para obter informações sobre como habilitar o MFA, consulte"Habilitar autenticação multifator" .

Controle de acesso baseado em função no SnapCenter

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

Você pode criar e modificar funções e adicionar acesso a recursos aos usuários a qualquer momento. No entanto, ao configurar o SnapCenter pela primeira vez, você deve pelo menos adicionar usuários ou grupos do Active Directory às funções e, em seguida, adicionar acesso a recursos a esses usuários ou grupos.

Você não pode usar o SnapCenter para criar contas de usuário ou grupo. Você deve criar contas de usuário ou grupo no Active Directory do sistema operacional ou banco de dados.

Tipos de RBAC no SnapCenter

O SnapCenter usa os seguintes tipos de controle de acesso baseado em função:

- SnapCenter RBAC
- RBAC de nível de aplicação
- Plug-in SnapCenter para VMware vSphere RBAC
- Permissões da ONTAP

SnapCenter RBAC

O SnapCenter tem funções predefinidas e você pode atribuir usuários ou grupos de usuários a essas funções. As funções predefinidas são:

- Função de administrador do SnapCenter
- Função de administrador de backup e clonagem de aplicativos
- Função de Visualizador de Backup e Clone
- Função de administrador de infraestrutura

Quando você atribui uma função a um usuário, somente os trabalhos relevantes para esse usuário ficam visíveis na página Trabalhos, a menos que você tenha atribuído 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 armazenamento e grupos de recursos.

Você pode atribuir permissões RBAC a usuários e grupos dentro da mesma floresta e a usuários pertencentes a florestas diferentes. Não é possível atribuir permissões RBAC a usuários pertencentes a grupos aninhados em florestas.

Se você criar uma função personalizada, ela deverá conter todas as permissões da função SnapCenterAdmin. Se você copiar apenas algumas das permissões, por exemplo, Adicionar Host ou Remover Host, não poderá executar essas operações.

Os usuários precisam fornecer autenticação durante o login, por meio da interface gráfica do usuário (GUI) ou usando cmdlets do PowerShell. Se os usuários forem membros de mais de uma função, após inserir as credenciais de login, eles serão solicitados a especificar a função que desejam usar. Os usuários também precisam fornecer autenticação para executar as APIs.

RBAC de nível de aplicação

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

Por exemplo, se você quiser executar operações de proteção de dados em um ambiente SQL Server, deverá definir credenciais com as credenciais adequadas do Windows ou SQL. O SnapCenter Server autentica o conjunto de credenciais usando qualquer um dos métodos. 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.

SnapCenter Plug-in for 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 oferece suporte ao vCenter Server RBAC e ao ONTAP RBAC. "Saber mais"

Melhores práticas: 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."Saber mais"

Permissões atribuídas às funções predefinidas do SnapCenter

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

Por exemplo, um usuário com a função de administrador do SnapCenter pode criar conexões SVM e atribuí-las a um usuário com a função de administrador de backup e clonagem de aplicativos, que por padrão não tem permissão para criar ou editar conexões SVM. Sem uma conexão SVM, os usuários não podem concluir nenhuma operação de backup, clonagem ou restauração.

Função de administrador do SnapCenter

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

Função de administrador de backup e clonagem de aplicativos

A função de administrador de backup e clonagem de aplicativos tem as permissões necessárias para executar ações administrativas para backups de aplicativos e tarefas relacionadas à clonagem. Esta função não tem permissões para gerenciamento de host, provisionamento, gerenciamento de conexão de armazenamento ou instalação remota.

Permissões	Habilitado	Criar	Ler	Atualizar	Excluir
Grupo de Recursos	Não aplicável	Sim	Sim	Sim	Sim
Política	Não aplicável	Sim	Sim	Sim	Sim
Backup	Não aplicável	Sim	Sim	Sim	Sim
Hospedar	Não aplicável	Sim	Sim	Sim	Sim
Conexão de armazenamento	Não aplicável	Não	Sim	Não	Não
Clone	Não aplicável	Sim	Sim	Sim	Sim
Provisão	Não aplicável	Não	Sim	Não	Não
Painel	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 de Plug-in	Não	Não aplicável		Não aplicável	Não aplicável
Migração	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Monte	Sim	Sim	Não aplicável	Não aplicável	Não aplicável
Desmontar	Sim	Sim	Não aplicável	Não aplicável	Não aplicável

Permissões	Habilitado	Criar	Ler	Atualizar	Excluir
Restauração de volume total	Não	Não	Não aplicável	Não aplicável	Não aplicável
Proteção Secundária	Não	Não	Não aplicável	Não aplicável	Não aplicável
Monitor de tarefas	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Função de Visualizador de Backup e Clone

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

Permissões	Habilitado	Criar	Ler	Atualizar	Excluir
Grupo de Recursos	Não aplicável	Não	Sim	Não	Não
Política	Não aplicável	Não	Sim	Não	Não
Backup	Não aplicável	Não	Sim	Não	Não
Hospedar	Não aplicável	Não	Sim	Não	Não
Conexão de armazenamento	Não aplicável	Não	Sim	Não	Não
Clone	Não aplicável	Não	Sim	Não	Não
Provisão	Não aplicável	Não	Sim	Não	Não
Painel	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 de Plug-in	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Migração	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Permissões	Habilitado	Criar	Ler	Atualizar	Excluir
Monte	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Desmontar	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Restauração de volume total	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Proteção Secundária	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Monitor de tarefas	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 armazenamento, provisionamento, grupos de recursos, relatórios de instalação remota e acesso ao Painel.

Permissões	Habilitado	Criar	Ler	Atualizar	Excluir
Grupo de Recursos	Não aplicável	Sim	Sim	Sim	Sim
Política	Não aplicável	Não	Sim	Sim	Sim
Backup	Não aplicável	Sim	Sim	Sim	Sim
Hospedar	Não aplicável	Sim	Sim	Sim	Sim
Conexão de armazenamento	Não aplicável	Sim	Sim	Sim	Sim
Clone	Não aplicável	Não	Sim	Não	Não
Provisão	Não aplicável	Sim	Sim	Sim	Sim
Painel	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

Permissões	Habilitado	Criar	Ler	Atualizar	Excluir
Instalação/Desinstalação de Plug-in	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Migração	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Monte	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Desmontar	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Restauração de volume total	Não	Não	Não aplicável	Não aplicável	Não aplicável
Proteção Secundária	Não	Não	Não aplicável	Não aplicável	Não aplicável
Monitor de tarefas	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Recuperação de desastres no SnapCenter

O recurso de recuperação de desastres (DR) do SnapCenter permite que você se recupere de desastres como corrupção de recursos ou falhas no servidor. Ele ajuda a restaurar o repositório SnapCenter , agendamentos do servidor, componentes de configuração e o plug-in SnapCenter para SQL Server e seu armazenamento.

Esta seção explica os dois tipos de DR no SnapCenter:

SnapCenter Server DR

- Os dados do SnapCenter Server são copiados e podem ser recuperados sem nenhum plug-in adicionado ou gerenciado pelo SnapCenter Server.
- O SnapCenter Server secundário deve ser instalado no mesmo diretório de instalação e na mesma porta que o SnapCenter Server primário.
- Para autenticação multifator (MFA), durante o SnapCenter Server DR, feche todas as guias do navegador e reabra um navegador para efetuar login novamente. Isso limpará 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 SnapCenter Server. Ver "Fluxos de trabalho da API REST para recuperação de desastres do SnapCenter Server" .
- 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. Você deve repetir manualmente as configurações do log de auditoria.

Plug-in SnapCenter e DR de armazenamento

O DR está disponível somente para o SnapCenter Plug-in para SQL Server. Se o plug-in estiver inativo, mude para outro host SQL e recupere os dados seguindo algumas etapas. Ver "Recuperação de desastres do plug-in SnapCenter para SQL Server" .

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

Licenças exigidas pelo 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 licença do SnapCenter que você instala depende do seu ambiente de armazenamento e dos recursos que você deseja usar.

Licença	Onde necessário
Controlador SnapCenter Standard baseado em	Obrigatório para FAS, AFF, ASA A licença SnapCenter Standard é uma licença baseada em controlador e está incluída como parte do NetApp ONTAP One. Se você tiver a licença do SnapManager Suite, também receberá o direito à licença do SnapCenter Standard. Se você quiser instalar o SnapCenter em caráter de teste com armazenamento 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 licenças incluídas no NetApp ONTAP One, consulte "Licenças incluídas no NetApp ONTAP One" . O SnapCenter também é oferecido como parte do pacote de proteção de dados. Se você adquiriu o A400 ou posterior, deverá adquirir o pacote de proteção de dados.
SnapMirror ou SnapVault	ONTAP A licença SnapMirror ou SnapVault é necessária se a replicação estiver habilitada no SnapCenter.

Licença	Onde necessário
SnapRestore	Necessário para restaurar e verificar backups. Em sistemas de armazenamento primário • Necessário em sistemas de destino SnapVault para executar verificação remota e restaurar a partir de um backup. • Obrigatório em sistemas de destino SnapMirror para executar verificação remota.
FlexClone	Necessário para clonar bancos de dados e operações de verificação. Em sistemas de armazenamento primário e secundário • Obrigatório em sistemas de destino SnapVault para criar clones do backup do vault secundário. • Necessário em sistemas de destino SnapMirror para criar clones do backup secundário do SnapMirror .
Licenças de protocolo	• Licença iSCSI ou FC para LUNs • Licença CIFS para ações SMB • Licença NFS para VMDKs do tipo NFS • Licença iSCSI ou FC para VMDKs do tipo VMFS Obrigatório em sistemas de destino SnapMirror para fornecer dados se um volume de origem não estiver disponível.
Licenças SnapCenter Standard (opcional)	Destinos secundários ⓘ É recomendado, mas não obrigatório, que você adicione licenças do SnapCenter Standard a destinos secundários. Se as licenças do SnapCenter Standard 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, uma licença FlexClone é necessária em destinos secundários para executar operações de clonagem e verificação.

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

As licenças SnapCenter Advanced e 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 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, consulte"Adicionar licenças baseadas no controlador SnapCenter Standard" .

Sincronização ativa do SnapMirror no SnapCenter

A sincronização ativa do SnapMirror permite que os serviços empresariais continuem operando mesmo durante uma falha completa do site, permitindo que os aplicativos façam failover de forma transparente usando uma cópia secundária. Não é necessária intervenção manual nem script adicional para acionar um failover com a sincronização ativa do SnapMirror .

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

Para sincronização ativa do SnapMirror , certifique-se de ter atendido aos diversos requisitos de hardware, software e configuração do sistema. Para obter informações, consulte "Pré-requisitos"

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

Para oferecer suporte à 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 assimétricas existentes do SnapMirror em simétricas alterando a política nos relacionamentos 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 nos relacionamentos de sincronização ativos do SnapMirror de *automatedfailover* para *automatedfailoverduplex* no ONTAP, o mesmo não será 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 uma coleção de recursos em um host ou cluster, potencialmente de vários hosts e clusters. As operações executadas em um grupo de recursos se aplicam a todos os seus recursos com base no cronograma especificado. Você pode executar backups sob demanda ou agendados para recursos individuais ou grupos.

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 de sistema de arquivos para sistemas de arquivos e SnapCenter Plug-in for VMware vSphere para VMs e datastores.

Políticas

As políticas especificam a frequência de backup, retenção de cópias, replicação, 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 for necessário fazer backup de todos os bancos de dados ou sistemas de arquivos de um host, um grupo de recursos incluindo todos os bancos de dados ou sistemas de arquivos no host poderá ser criado. Duas políticas podem então ser anexadas ao grupo de recursos: uma política diária e uma política horária.

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

Prescrições e pós-escritos 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 sobre falhas ou avisos de tarefas de proteção de dados. Entender os requisitos para criar esses scripts é crucial antes de configurar prescrições e pós-escritos.

Uso de prescrições e posfácios

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

Tipos de script suportados

Os seguintes tipos de scripts são suportados pelo Windows:

- Arquivos em lote
- Scripts do PowerShell
- Scripts Perl

Os seguintes tipos de scripts são suportados pelo UNIX:

- Scripts Perl
- Scripts Python
- Scripts de shell

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

Caminho do script

Todos os prescrições e pós-escritos executados como parte das operações do SnapCenter em sistemas de armazenamento virtualizados e não virtualizados são executados no host do plug-in.

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

> O caminho de prescrições ou pós-escritos não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPTS_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 em políticas de backup. Quando uma tarefa de backup é iniciada, a política associa automaticamente o script aos recursos que estão sendo copiados. Ao criar uma política de backup, você pode especificar os argumentos prescript e postscript.

Você não pode especificar vários scripts.

Tempo limite de script

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

Saída do script

O diretório padrão para os arquivos de saída de prescrições e postscripts do Windows é Windows\System32.

Não há um local padrão para os prescrições e pós-escritos do UNIX. Você pode redirecionar o arquivo de saída para qualquer local preferido.

Sistemas de armazenamento e aplicativos suportados pelo SnapCenter

Você deve conhecer os sistemas de armazenamento, aplicativos e bancos de dados suportados pelo SnapCenter.

Sistemas de armazenamento suportados

- NetApp ONTAP 9.12.1 e posterior
- Azure NetApp Files
- Amazon FSx for NetApp ONTAP

  Suporta memória não volátil expressa (NVMe) via Protocolo de Controle de Transporte (TCP).

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

- Sistemas NetApp ASA r2 que executam o NetApp ONTAP 9.16.1.

Aplicativos e bancos de dados suportados

O SnapCenter oferece suporte à proteção de diferentes aplicativos e bancos de dados. Para obter informações detalhadas sobre os aplicativos e bancos de dados suportados, consulte "Ferramenta de Matriz de Interoperabilidade da NetApp" .

O SnapCenter oferece suporte à proteção de cargas de trabalho Oracle e Microsoft SQL em ambientes de Software-Defined Data Center (SDDC) do VMware Cloud on Amazon Web Services (AWS). "Saber mais" .

Métodos de autenticação para credenciais do SnapCenter

As credenciais usam métodos de autenticação diferentes dependendo do aplicativo ou

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 autentica no Active Directory. Para autenticação do Windows, o Active Directory é configurado fora do SnapCenter. O SnapCenter autentica sem nenhuma configuração adicional. Você precisa de uma credencial do Windows para adicionar hosts, instalar pacotes de plug-ins e agendar tarefas.

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 no SnapCenter.

Autenticação de grupo de trabalho local

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

Autenticação do SQL Server

O método de autenticação SQL autentica 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 os recursos. Você precisa da autenticação do SQL Server para executar operações como agendamento no SQL Server ou descobrir recursos.

Autenticação Linux

O método de autenticação do Linux autentica em um host Linux. Você precisa de autenticação do Linux durante a etapa inicial de adição do host Linux e instalação remota do Pacote de plug-ins do SnapCenter para Linux a partir da GUI do SnapCenter .

Autenticação AIX

O método de autenticação AIX autentica em um host AIX. Você precisa da autenticação do AIX durante a etapa inicial de adição do host do AIX e instalação remota do Pacote de plug-ins do SnapCenter para AIX a partir da GUI do SnapCenter .

Autenticação de banco de dados Oracle

O método de autenticação do banco de dados Oracle autentica 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 (SO) estiver desabilitada 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 privilégios sysdba.

Autenticação Oracle ASM

O método de autenticação Oracle ASM autentica em uma instância do Oracle Automatic Storage Management (ASM). A autenticação do Oracle ASM será necessária se você precisar acessar uma instância do Oracle ASM e a autenticação do sistema operacional estiver desabilitada no host do banco de dados. Antes de adicionar uma credencial do Oracle ASM, crie um usuário Oracle com privilégios de sistema na instância do ASM.

Autenticação de catálogo RMAN

O método de autenticação do catálogo RMAN autentica no banco de dados do catálogo Oracle Recovery Manager (RMAN). Se você configurou um mecanismo de catálogo externo e registrou seu banco de dados no banco de dados de catálogo, será necessário adicionar a autenticação de catálogo do RMAN.

Informações sobre direitos autorais

Informações sobre marcas comerciais