



Conceitos

SnapCenter Software 4.7

NetApp
April 02, 2025

Índice

Conceitos	1
Visão geral do SnapCenter	1
Arquitetura da SnapCenter	3
Componentes do SnapCenter	3
Servidor SnapCenter	4
Plug-ins do SnapCenter	5
Repositório SnapCenter	7
Recursos de segurança	7
Visão geral do certificado CA	8
Autenticação multifator (MFA)	8
Controles de acesso baseados em função do SnapCenter (RBAC)	9
Tipos de RBAC	9
Permissões e funções do RBAC	10
Funções e permissões do SnapCenter predefinidas	12
Recuperação de desastres	16
Recursos, grupos de recursos e políticas	16
Prescripts e postscripts	18
Tipos de script suportados	18
Caminho do script	18
Onde especificar scripts	19
Tempos limite de script	19
Saída de script	19
Automação da SnapCenter usando APIS REST	19

Conceitos

Visão geral do SnapCenter

O software SnapCenter é uma plataforma simples, centralizada e dimensionável que fornece proteção de dados consistente com aplicações para aplicações, bancos de dados, sistemas de arquivos host e VMs em execução nos sistemas ONTAP em qualquer lugar na nuvem híbrida.

O SnapCenter utiliza as tecnologias NetApp Snapshot, SnapRestore, FlexClone, SnapMirror e SnapVault para oferecer o seguinte:

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

O SnapCenter inclui o servidor SnapCenter e plug-ins leves individuais. É possível automatizar a implantação de plug-ins para hosts remotos de aplicações, agendar operações de backup, verificação e clone e monitorar todas as operações de proteção de dados.

O SnapCenter pode ser implantado das seguintes maneiras:

- No local para proteger o seguinte:
 - Dados em sistemas primários ONTAP FAS ou AFF e replicados para sistemas secundários ONTAP FAS ou AFF
 - Dados em sistemas primários ONTAP Select
- No local em uma nuvem híbrida para proteger o seguinte:
 - Dados em sistemas primários ONTAP FAS ou AFF e replicados para sistemas secundários Cloud Volumes ONTAP ou NetApp Private Storage
- Em uma nuvem pública para proteger o seguinte:
 - Dados em sistemas primários Cloud Volumes ONTAP (anteriormente ONTAP Cloud)

O SnapCenter inclui os seguintes recursos principais:

- Proteção de dados centralizada e consistente com 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 e sistemas de arquivos do Windows Host executados em sistemas ONTAP.

A proteção de dados também é compatível com outros aplicativos e bancos de dados padrão ou personalizados, fornecendo uma estrutura para criar plug-ins do SnapCenter definidos pelo usuário. Isso permite a proteção de dados para outros aplicativos e bancos de dados a partir do mesmo painel único. Ao aproveitar essa estrutura, a NetApp lançou plug-ins personalizados do SnapCenter para IBM DB2, MongoDB e MySQL.

- Backups baseados em políticas

Os backups baseados em políticas utilizam a tecnologia de cópia Snapshot do NetApp para criar backups

rápidos, com uso eficiente de espaço, consistentes com aplicações e baseados em disco. Como opção, você pode automatizar a proteção desses backups para um storage secundário por meio de atualizações dos relacionamentos de proteção existentes.

- Backups para vários recursos

É possível fazer backup de vários recursos (aplicações, 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 fornece clonagem rápida, com uso eficiente de espaço e consistente com aplicações, o que possibilita o desenvolvimento acelerado de software. Você pode clonar em qualquer destino na nuvem híbrida.

- Interface gráfica do usuário (GUI) de gerenciamento de usuário único

A GUI do SnapCenter fornece uma interface única e única para gerenciar backups e clones de um recurso em qualquer destino na nuvem híbrida.

- APIs REST, cmdlets do Windows, comandos UNIX

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

Para obter mais informações sobre APIs REST, "[Visão geral da API REST](#)" consulte .

Para obter mais informações sobre cmdlets do Windows, "[Guia de referência de cmdlet do software SnapCenter](#)" consulte .

Para obter mais informações sobre comandos UNIX, "[Guia de Referência de comandos do software SnapCenter](#)" consulte .

- Dashboard e relatórios centralizados de proteção de dados

- Controle de acesso baseado em função (RBAC) para segurança e delegação.

- Banco de dados de repositório com alta disponibilidade

O SnapCenter fornece um banco de dados de repositório integrado com alta disponibilidade para armazenar todos os metadados de backup.

- Instalação automática de plug-ins por push

Você pode automatizar um envio remoto de plug-ins do SnapCenter do host do servidor SnapCenter para os hosts de aplicativos.

- Alta disponibilidade

A alta disponibilidade para SnapCenter é configurada usando o balanceador de carga externo (F5). Até dois nós são suportados no mesmo data center.

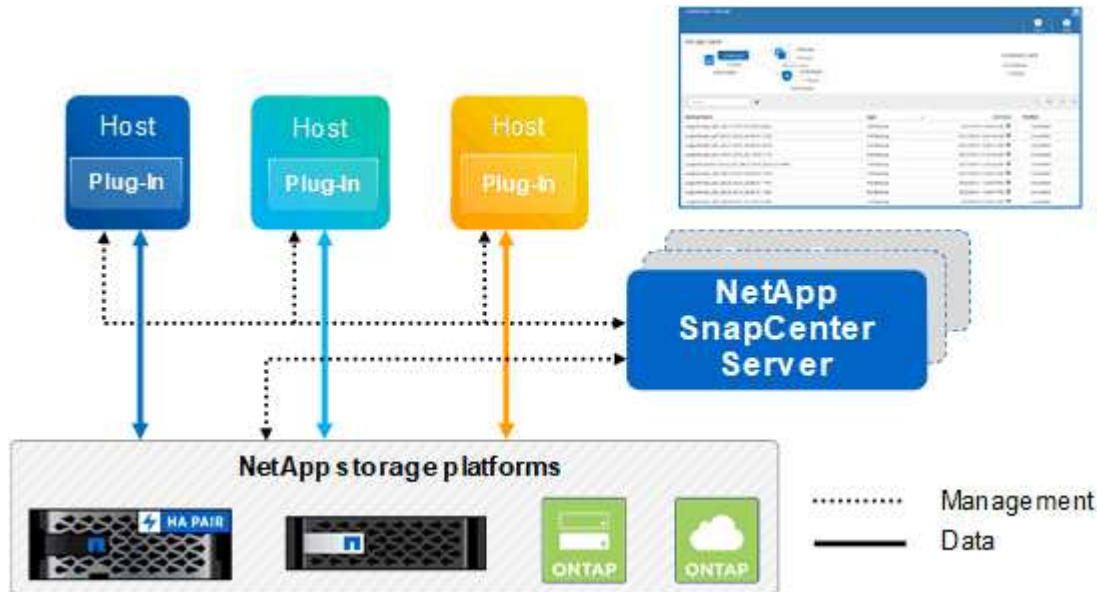
- Recuperação de desastres (DR)

Você pode recuperar o servidor SnapCenter em caso de desastres como corrupção de recursos ou falha do servidor.

Arquitetura da SnapCenter

A plataforma SnapCenter é baseada em uma arquitetura de vários níveis que inclui um servidor de gerenciamento centralizado (servidor SnapCenter) e um host de plug-in SnapCenter.

O SnapCenter é compatível com data center multisite. O servidor SnapCenter e o host do plug-in podem estar em diferentes locais geográficos.



Componentes do SnapCenter

O SnapCenter consiste nos plug-ins do servidor SnapCenter e do SnapCenter. Você deve instalar apenas os plug-ins apropriados para os dados que deseja proteger.

- Servidor SnapCenter
- Pacote de plug-ins do SnapCenter para Windows, que inclui os seguintes plug-ins:
 - Plug-in do SnapCenter para Microsoft SQL Server
 - Plug-in do SnapCenter para Microsoft Windows
 - Plug-in do SnapCenter para Microsoft Exchange Server
 - Plug-in do SnapCenter para banco de dados SAP HANA
- Pacote de plug-ins do SnapCenter para Linux, que inclui os seguintes plug-ins:
 - Plug-in SnapCenter para banco de dados Oracle
 - Plug-in do SnapCenter para banco de dados SAP HANA
 - Plug-in do SnapCenter para UNIX



O plug-in SnapCenter para UNIX não é um plug-in autônomo e não pode ser instalado de forma independente. Esse plug-in é instalado automaticamente quando você instala o plug-in do SnapCenter para banco de dados Oracle ou o plug-in do SnapCenter para banco de dados SAP HANA.

- Pacote de plug-ins do SnapCenter para AIX, que inclui os seguintes plug-ins:

- Plug-in SnapCenter para banco de dados Oracle
- Plug-in do SnapCenter para UNIX



O plug-in SnapCenter para UNIX não é um plug-in autônomo e não pode ser instalado de forma independente. Esse plug-in é instalado automaticamente quando você instala o plug-in do SnapCenter para o banco de dados Oracle.

- Plug-ins personalizados do SnapCenter

Plug-ins personalizados são compatíveis com a comunidade.

O plug-in do SnapCenter para VMware vSphere, antigo agente de dados da NetApp, é um dispositivo virtual autônomo que suporta operações de proteção de dados da SnapCenter em bancos de dados virtualizados e sistemas de arquivos.

Servidor SnapCenter

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 permite alta disponibilidade e dimensionamento horizontal em vários servidores SnapCenter em uma única interface de usuário. Você pode obter alta disponibilidade usando o balanceador de carga externo (F5). Para ambientes maiores com milhares de hosts, adicionar vários servidores SnapCenter pode ajudar a equilibrar a carga.

- Se você estiver usando o pacote de plug-ins do SnapCenter para Windows, o agente host será executado no host de plug-ins do SnapCenter Server e do Windows. O agente host executa as programações nativamente no host remoto do Windows ou, para Microsoft SQL Servers, a programação é executada na instância SQL local.

O servidor SnapCenter se comunica com os plug-ins do Windows por meio do agente host.

- Se você estiver usando o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do SnapCenter para AIX, as programações serão executadas no servidor SnapCenter como programações de tarefas do Windows.
 - Para o plug-in do SnapCenter para banco de dados Oracle, o agente host que é executado no host do servidor SnapCenter se comunica com o SnapCenter Plug-in Loader (SPL) que é executado no host Linux ou AIX para executar diferentes operações de proteção de dados.
 - Para plug-in do SnapCenter para banco de dados SAP HANA e plug-ins personalizados do SnapCenter, o servidor SnapCenter se comunica com esses plug-ins por meio do agente SCCore que é executado no host.

O servidor SnapCenter e os plug-ins se comunicam com o agente host usando HTTPS.

As informações sobre as operações do SnapCenter são armazenadas no repositório do 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 para SQL Server	Pacote de plug-ins para Windows	Plug-in para Windows	Host do SQL Server	Windows
Plug-in para Windows	Pacote de plug-ins para Windows		Host Windows	Windows
Plug-in para Exchange	Pacote de plug-ins para Windows	Plug-in para Windows	Host do Exchange Server	Windows
Plug-in 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
Plug-in 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-ins personalizados		Para backups do sistema de arquivos, Plug-in para Windows	Host de aplicativo personalizado	Linux ou Windows



O plug-in do SnapCenter para VMware vSphere é compatível com operações de backup e restauração consistentes com VM e falhas para máquinas virtuais (VMs), armazenamentos de dados e discos de máquinas virtuais (VMDKs), além de oferecer suporte aos plug-ins específicos da aplicação SnapCenter para proteger operações de backup e restauração consistentes com aplicações para bancos de dados e sistemas de arquivos virtualizados.

Para usuários do SnapCenter 4.1.1, a documentação do plug-in do SnapCenter para VMware vSphere 4.1.1 tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos. Para usuários do SnapCenter 4,2.x, o Agente de dados do NetApp 1,0 e 1,0.1, a documentação tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos usando o plug-in do SnapCenter para VMware vSphere fornecido pelo dispositivo virtual NetApp Data Broker baseado em Linux (formato Open Virtual Appliance). Para usuários que usam o SnapCenter 4,3 ou posterior, o "[Plug-in do SnapCenter para documentação do VMware vSphere](#)" tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos usando o plug-in SnapCenter baseado em Linux para o dispositivo virtual VMware vSphere (formato Open Virtual Appliance).

Plug-in do SnapCenter para recursos do Microsoft SQL Server

- Automatiza operações de backup, restauração e clone com reconhecimento de aplicações para bancos de dados Microsoft SQL Server em seu ambiente SnapCenter.

- Suporta bancos de dados Microsoft SQL Server em VMDK e LUNs de mapeamento de dispositivo bruto (RDM) quando você implementa o plug-in SnapCenter para VMware vSphere e Registra o plug-in com o SnapCenter
- É compatível apenas com o provisionamento de compartilhamentos SMB. Não é fornecido suporte para fazer backup de bancos de dados SQL Server em compartilhamentos SMB.
- Suporta a importação de backups do SnapManager para Microsoft SQL Server para SnapCenter.

Plug-in do SnapCenter para recursos do Microsoft Windows

- Habilita a proteção de dados com reconhecimento de aplicativos para outros plug-ins que estão sendo executados em hosts do Windows em seu ambiente SnapCenter
- Automatiza operações de backup, restauração e clone com reconhecimento de aplicações para sistemas de arquivos da Microsoft em seu ambiente SnapCenter
- É compatível com o provisionamento de storage, a consistência da cópia Snapshot e a exigência de espaço para hosts do Windows



O Plug-in para Windows provisiona compartilhamentos SMB e sistemas de arquivos do Windows em LUNs físicos e RDM, mas não suporta operações de backup para sistemas de arquivos do Windows em compartilhamentos SMB.

Plug-in do SnapCenter para recursos do Microsoft Exchange Server

- Automatiza as operações de backup e restauração com reconhecimento de aplicativos para bancos de dados do Microsoft Exchange Server e grupos de disponibilidade de banco de dados (DAGs) em seu ambiente SnapCenter
- Suporta servidores Exchange virtualizados em LUNs RDM quando você implementa o plug-in SnapCenter para VMware vSphere e Registra o plug-in com o SnapCenter

Plug-in do SnapCenter para recursos de banco de dados Oracle

- Automatiza operações de backup, restauração, recuperação, verificação, montagem, desmontagem e clone com reconhecimento de aplicações para bancos de dados Oracle em seu ambiente SnapCenter
- Suporta bancos de dados Oracle para SAP, no entanto, a integração SAP BR*Tools não é fornecida

Plug-in do SnapCenter para recursos UNIX

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

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

Plug-in do SnapCenter para recursos de banco de dados SAP HANA

- Automatiza o backup, a restauração e a clonagem com reconhecimento de aplicações de bancos de dados SAP HANA em seu ambiente SnapCenter

Recursos de plug-ins personalizados do SnapCenter

- Oferece suporte a plug-ins personalizados para gerenciar aplicativos ou bancos de dados que não são compatíveis com outros plug-ins do SnapCenter. Plug-ins personalizados não são fornecidos como parte da instalação do SnapCenter.
- Suporta a criação de cópias espelhadas de conjuntos de backup em outro volume e a execução de replicação de backup disco para disco.
- Suporta ambientes Windows e Linux. Em ambientes Windows, aplicativos personalizados por meio de plug-ins personalizados podem, opcionalmente, utilizar o plug-in SnapCenter para Microsoft Windows para fazer backups consistentes com o sistema de arquivos.



Os plug-ins personalizados MySQL, DB2 e MongoDB são compatíveis apenas com as comunidades NetApp.

O NetApp suporta a capacidade de criar e usar plug-ins personalizados; no entanto, os plug-ins personalizados criados não são suportados pelo NetApp.

Para obter mais informações, consulte ["Desenvolva um plug-in para sua aplicação"](#)

Repositório SnapCenter

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

O banco de dados do repositório do servidor MySQL é instalado por padrão quando você instala o servidor SnapCenter. Se o servidor MySQL já estiver instalado e você estiver fazendo uma nova instalação do servidor SnapCenter, você deve desinstalar o servidor MySQL.

O SnapCenter suporta o MySQL Server 5.7.25 ou posterior como o banco de dados de repositório do SnapCenter. Se você estava usando uma versão anterior do servidor MySQL com uma versão anterior do SnapCenter, durante a atualização do SnapCenter, o servidor MySQL é atualizado para 5.7.25 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

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).
- O SnapCenter usa algoritmos de segurança compatíveis com o padrão Federal de processamento de informações (FIPS).
- O SnapCenter suporta o uso dos certificados de CA autorizados fornecidos pelo cliente.
- O SnapCenter 4.1.1 ou posterior suporta a comunicação TLS (Transport Layer Security) 1,2 com o ONTAP. Você também pode usar a comunicação TLS 1,2 entre clientes e servidores.
- O SnapCenter suporta um determinado conjunto de pacotes de criptografia SSL para fornecer segurança em toda a comunicação de rede.

Para obter mais informações, ["Como configurar o SSL Cipher Suite suportado"](#) consulte .

- 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.
- 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 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 ou mais tentativas de início de sessão incorretas.

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 respectivos 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 .

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 active 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 do SnapCenter (RBAC)

Tipos de RBAC

As permissões de controle de acesso baseado em função (RBAC) e ONTAP do SnapCenter permitem que os administradores do SnapCenter delegem o controle de recursos do SnapCenter a diferentes usuários ou grupos de usuários. Esse acesso gerenciado centralmente capacita os administradores de aplicativos a trabalhar com segurança em ambientes delegados.

Você pode criar e modificar funções e adicionar acesso a recursos aos usuários a qualquer momento, mas quando você estiver configurando o SnapCenter pela primeira vez, você deve pelo menos adicionar usuários ou grupo do ative Directory a 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 ative Directory do sistema operacional ou banco de dados.

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

- SnapCenter RBAC
- Plug-in RBAC do SnapCenter (para alguns plug-ins)
- RBAC no nível da aplicação
- Permissões da ONTAP

SnapCenter RBAC

Funções e permissões

O SnapCenter é fornecido com funções predefinidas com permissões já atribuídas. Você pode atribuir usuários ou grupos de usuários a essas funções. Você também pode criar novas funções e gerenciar permissões e usuários.

Atribuindo permissões a usuários ou grupos

Você pode atribuir permissões a usuários ou grupos para acessar objetos do SnapCenter, como hosts, conexões de storage e grupos de recursos. Não é possível alterar as permissões da função SnapCenterAdmin.

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.



Se você criar uma função personalizada, ela deverá conter todas as permissões da função de administrador do SnapCenter. Se você copiar apenas algumas das permissões, por exemplo, Host add ou Host remove, não será possível executar essas operações.

Autenticação

Os usuários são obrigados a 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, depois de inserir credenciais de login, eles serão solicitados a especificar a função que desejam usar. Os usuários também são obrigados a fornecer autenticação para executar as 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, se você deseja executar operações de cópia Snapshot e proteção de dados em um ambiente SQL Server, você deve definir credenciais com as credenciais Windows ou SQL adequadas. O servidor SnapCenter autentica o conjunto de credenciais usando qualquer um dos métodos. Se você quiser executar operações de proteção de dados e cópia Snapshot em um ambiente de sistema de arquivos do Windows no storage ONTAP, a função de administração do SnapCenter deve ter admin Privileges no host do Windows.

Da mesma forma, se você deseja executar operações de proteção de dados em um banco de dados Oracle e se a autenticação do sistema operacional (os) estiver desativada no host do banco de dados, você deve definir credenciais com o banco de dados Oracle ou as credenciais Oracle ASM. O servidor SnapCenter autentica as credenciais definidas usando um desses 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 Data ONTAP RBAC.

Para obter informações, consulte ["Plug-in do SnapCenter para VMware vSphere RBAC"](#)

Permissões da ONTAP

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

Para obter informações sobre como criar a conta e atribuir permissões, consulte ["Crie uma função de cluster do ONTAP com Privileges mínimo"](#)

Permissões e funções do RBAC

O controle de acesso baseado em função (RBAC) do SnapCenter permite criar funções e atribuir permissões a essas funções e, em seguida, atribuir usuários ou grupos de usuários às funções. Isso permite que os administradores do SnapCenter criem um ambiente gerenciado centralmente, enquanto os administradores de aplicativos podem gerenciar tarefas de proteção de dados. O SnapCenter é fornecido com algumas funções e permissões predefinidas.

Funções do SnapCenter

O SnapCenter é fornecido com as seguintes funções predefinidas. Você pode atribuir usuários e grupos a essas funções ou criar novas funções.

Quando você atribui uma função a um usuário, somente os trabalhos relevantes a esse usuário são visíveis na página trabalhos, a menos que você tenha atribuído a função Administrador do SnapCenter.

- App Backup e Clone Admin
- Visualizador de cópias de segurança e clones
- Administrador de infraestrutura
- SnapCenterAdmin

Plug-in do SnapCenter para funções do VMware vSphere

Para gerenciar a proteção de dados consistente com VM de VMs, VMDKs e armazenamentos de dados, as funções a seguir são criadas no vCenter pelo plug-in do SnapCenter para VMware vSphere:

- Administrador do SCV
- Vista SCV
- Backup da VCR
- Restauração da VCR
- Restauração do arquivo convidado SCV

Para obter mais informações, consulte ["Tipos de plug-in RBAC para SnapCenter para usuários do VMware vSphere"](#)

Prática recomendada: a NetApp recomenda que você crie uma função do ONTAP para o plug-in do SnapCenter para operações do VMware vSphere e atribua a ele todos os Privileges necessários.

Permissões do SnapCenter

O SnapCenter fornece as seguintes permissões:

- Grupo recursos
- Política
- Backup
- Host
- Ligação de armazenamento
- Clone
- Provisionamento (apenas para banco de dados Microsoft SQL)
- Painel de instrumentos
- Relatórios
- Restaurar
 - Restauração completa de volume (somente para plug-ins personalizados)
- Recurso

Os plug-in Privileges são necessários do administrador para que não administradores realizem operações de descoberta de recursos.

- Instalação ou desinstalação do plug-in



Quando você ativa permissões de instalação de plug-in, você também deve modificar a permissão de host para habilitar leituras e atualizações.

- Migração
- Montar (apenas para banco de dados Oracle)
- Desmontar (apenas para banco de dados Oracle)
- Monitor de trabalho

A permissão Monitor de tarefas permite que membros de diferentes funções vejam as operações em todos os objetos aos quais são atribuídos.

Funções e permissões do SnapCenter predefinidas

O SnapCenter é fornecido com funções predefinidas, cada uma com um conjunto de permissões já ativadas. Ao configurar e administrar o controle de acesso baseado em funções (RBAC), você pode usar essas funções predefinidas ou criar novas.

O SnapCenter inclui as seguintes funções predefinidas:

- 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

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

Por exemplo, um usuário com a função Administrador do SnapCenter pode criar conexões SVM e atribuí-las a um usuário com a função Administrador de Backup e Clonagem de aplicativos, que por padrão não tem permissão para criar ou editar conexões SVM. Sem uma conexão com o SVM, os usuários não podem concluir 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
Monitor de trabalho	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Função Visualizador de cópia de Segurança e Clonagem

A função Visualizador de cópia de Segurança e Clonagem tem uma vista só de leitura de todas as permissões. Essa função também tem permissões habilitadas para descoberta, geração de relatórios e

acesso ao Dashboard.

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
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
Restauração completa do volume	Não	Não	Não aplicável	Não aplicável	Não aplicável

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

Recuperação de desastres

Você pode recuperar o servidor SnapCenter em caso de desastres como corrupção de recursos ou falha do servidor usando o recurso de recuperação de desastres do SnapCenter. Você pode recuperar o repositório do SnapCenter, as programações do servidor e os componentes de configuração do servidor.

Você também pode recuperar o plug-in do SnapCenter para SQL Server e o plug-in do SnapCenter para armazenamento de dados SQL Server.

A seguir estão os tipos de recuperação de desastres (DR) :

- **DR do servidor SnapCenter**

Os dados do servidor SnapCenter serão copiados e recuperados independentemente de qualquer plug-in ter sido 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), quando a restauração de DR é executada para o servidor SnapCenter, feche todas as guias do navegador e reabra um navegador para fazer login novamente. Isso eliminará os cookies de sessão existentes ou ativos e garante que os dados de configuração corretos sejam atualizados.

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"](#)

- **SnapCenter Plug-in e Storage DR**

O DR é compatível apenas com o plug-in SnapCenter para SQL Server. Quando o plug-in do SnapCenter estiver inativo, mude para um host SQL diferente e recupere os dados executando algumas etapas.

["Recuperação de desastres do plug-in SnapCenter para SQL Server"](#)

A SnapCenter usa a tecnologia ONTAP SnapMirror para replicar dados. Ele pode ser usado para replicar dados para um local secundário para recuperação de desastres e mantê-los sincronizados. Um failover pode ser iniciado quebrando a relação de replicação no SnapMirror. Durante o failback, a sincronização pode ser revertida e os dados do local de DR podem ser replicados de volta para o local principal.

Recursos, grupos de recursos e políticas

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** são normalmente bancos de dados, sistemas de arquivos do Windows ou compartilhamentos de arquivos que você faz backup ou clone com o SnapCenter.

No entanto, dependendo do seu ambiente, os recursos podem ser instâncias de banco de dados, grupos de disponibilidade do Microsoft SQL Server, bancos de dados Oracle RAC, sistemas de arquivos do Windows ou um grupo de aplicativos personalizados.

- Um **grupo de recursos** é uma coleção de recursos em um host ou cluster. O grupo de recursos também pode conter recursos de vários hosts e vários clusters.

Quando você executa uma operação em um grupo de recursos, executa essa operação em todos os 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 configurar backups programados para recursos únicos e grupos de recursos.



Se você colocar um host de um grupo de recursos compartilhados no modo de manutenção e se houver programações associadas ao mesmo grupo de recursos compartilhados, todas as operações agendadas serão suspensas para todos os outros hosts do grupo de recursos compartilhados.

Você deve usar um plug-in de banco de dados para fazer backup de bancos de dados, um plug-in de sistema de arquivos para fazer backup de sistemas de arquivos e o plug-in SnapCenter para VMware vSphere para fazer backup de VMs e datastores.

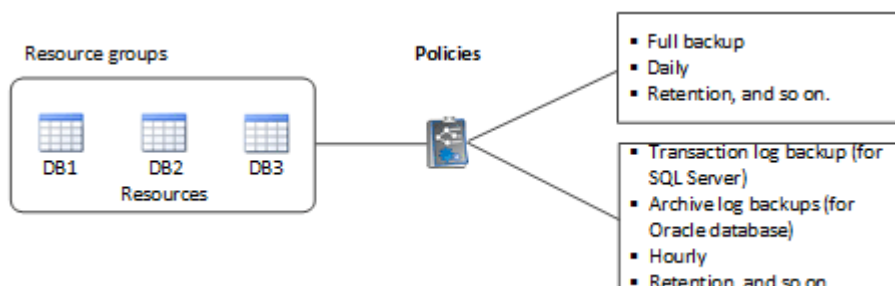
- **Políticas** especificam a frequência de backup, retenção de cópia, replicação, scripts e outras características das operações de proteção de dados.

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

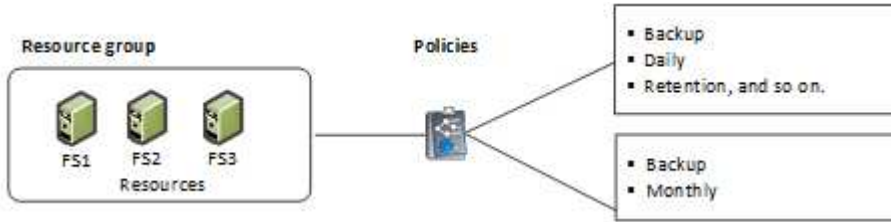
Pense em um grupo de recursos como definindo *o que* você quer proteger e quando você quer protegê-lo em termos de dia e tempo. Pense em uma política como definindo *como* você quer protegê-la. Se você estiver fazendo backup de todos os bancos de dados ou fazendo backup de todos os sistemas de arquivos 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 completo diário e outro agendamento que executa backups de log por hora.

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



A imagem a seguir ilustra a relação entre recursos, grupos de recursos e políticas para sistemas de arquivos do Windows:



Prescripts e postscripts

Você pode usar prescripts e postscripts personalizados como parte de suas operações de proteção de dados. Esses scripts habilitam a automação antes do trabalho de proteção de dados ou depois. Por exemplo, você pode incluir um script que o notifica automaticamente sobre falhas ou avisos de trabalhos de proteção de dados. Antes de configurar suas prescriptas e pós-scripts, você deve entender alguns dos requisitos para criar 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 diretiva associa automaticamente o script aos recursos que estão sendo copiados. Ao criar uma política de backup, você pode especificar os argumentos prescriitor e postscript.

Somente para Windows, você pode especificar vários scripts. Você deve pressionar **Enter** após cada caminho de script para listar cada script em uma linha separada. Ponto e vírgula (;) não são permitidos. Você pode especificar várias prescripts e vários postscripts. Um único script pode ser codificado como um prescriitor e um postscript e pode chamar outros scripts.



Para UNIX, não é possível especificar vários scripts.

Tempos limite de script

Para o Windows, o tempo limite é definido para 15 minutos e não pode ser modificado.

Para UNIX, 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.

Automação da SnapCenter usando APIS REST

Você pode usar APIS REST para executar várias operações de gerenciamento do SnapCenter. As APIs REST são expostas por meio da página da Web do Swagger. Você pode acessar a página da Web do Swagger para exibir a documentação da API REST, bem como emitir manualmente uma chamada de API. Você pode usar APIS REST para ajudar a gerenciar seu servidor SnapCenter ou seu host do SnapCenter vSphere.

As APIs REST para...	Este hotel fica bem perto...
Servidor SnapCenter	Https:// cliente SnapCenter_IP_address_or_name>: Cliente SnapCenter_port>/swagger/
Plug-in do SnapCenter para VMware vSphere	/<OVA_IP_address_or_host_name>:<scv_plugin_port >/api/swagger-ui.html

Para obter informações sobre APIS REST do SnapCenter, consulte "[Visão geral das APIs REST](#)"

Para obter informações sobre o plug-in do SnapCenter para APIs REST do VMware vSphere, consulte "[Plug-in do SnapCenter para APIs REST do VMware vSphere](#)"

Informações sobre direitos autorais

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

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

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS 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.