Começar

NetApp Backup and Recovery

NetApp
February 13, 2026

Índice

Começar

Saiba mais sobre o NetApp Backup and Recovery

O NetApp Backup and Recovery é um serviço de dados que fornece proteção de dados eficiente, segura e econômica para todas as suas cargas de trabalho ONTAP , incluindo volumes, bancos de dados, máquinas virtuais e cargas de trabalho do Kubernetes.

O suporte para backup e recuperação já está integrado em todos os sistemas ONTAP , portanto não há necessidade de hardware adicional, licenças de software ou gateways de mídia. Isso torna as operações de backup simples e econômicas. O NetApp Console simplifica a implementação de qualquer estratégia de backup, incluindo todo o espectro de variantes de backup 3-2-1, sem a necessidade de vários gerentes de recursos ou pessoal especializado.

> A documentação sobre a proteção de cargas de trabalho VMware, KVM, Hyper-V e Kubernetes é fornecida como uma prévia da tecnologia. Com esta oferta de visualização, a NetApp reserva-se o direito de modificar os detalhes, o conteúdo e o cronograma da oferta antes da disponibilidade geral.

O que você pode fazer com o NetApp Backup and Recovery

Use o NetApp Backup and Recovery para atingir os seguintes objetivos:

- * Cargas de trabalho de volume ONTAP *:
  - Crie snapshots locais, replique para armazenamento secundário e faça backup de volumes ONTAP de sistemas ONTAP locais ou Cloud Volumes ONTAP para armazenamento de objetos em sua conta de nuvem pública ou privada.
  - Crie backups incrementais permanentes em nível de bloco que são armazenados em outro cluster ONTAP e no armazenamento de objetos na nuvem.
  - Use o NetApp Backup and Recovery junto com o SnapCenter.
  - Consulte"Proteger volumes ONTAP" .
- **Cargas de trabalho do Microsoft SQL Server**:
  - Faça backup de instâncias e bancos de dados do Microsoft SQL Server do ONTAP local, Cloud Volumes ONTAP ou Amazon FSx for NetApp ONTAP.
  - Restaurar bancos de dados do Microsoft SQL Server.
  - Clonar bancos de dados do Microsoft SQL Server.
  - Use o NetApp Backup and Recovery sem o SnapCenter.
  - Consulte"Proteja as cargas de trabalho do Microsoft SQL Server" .
- **Cargas de trabalho VMware (visualização com nova interface de usuário sem o SnapCenter Plug-in for VMware vSphere)**:
  - Proteja suas VMs e armazenamentos de dados VMware com o NetApp Backup and Recovery.
  - Faça backup de cargas de trabalho do VMware no Amazon Web Services S3 ou StorageGRID (para visualização).
  - Restaure dados do VMware da nuvem para o vCenter local.

    - Você pode restaurar a VM exatamente no mesmo local de onde o backup foi feito ou em um local alternativo.
    - Use o NetApp Backup and Recovery sem o SnapCenter Plug-in for VMware vSphere.
    - Consulte"Proteja as cargas de trabalho do VMware" .
- **Cargas de trabalho VMware (com SnapCenter Plug-in for VMware vSphere)**:
    - Faça backup de VMs e armazenamentos de dados no Amazon Web Services S3, Microsoft Azure Blob, Google Cloud Platform e StorageGRID e restaure as VMs de volta para o host SnapCenter Plug-in for VMware vSphere local.
    - Restaure dados de VM da nuvem de volta para o vCenter local com o NetApp Backup and Recovery. Você pode restaurar a VM exatamente no mesmo local de onde o backup foi feito ou em um local alternativo.
    - Use o NetApp Backup and Recovery junto com o SnapCenter Plug-in for VMware vSphere.
    - Consulte"Proteja as cargas de trabalho do VMware" .
- **Cargas de trabalho KVM (visualização)**:
    - Fazer backup e restaurar máquinas virtuais
    - Fazer backup de pools de armazenamento KVM
    - Use grupos de proteção para gerenciar tarefas de backup
    - Consulte"Proteja cargas de trabalho KVM" .
- **Cargas de trabalho do Hyper-V (visualização)**:
    - Fazer backup e restaurar máquinas virtuais
    - Use grupos de proteção para gerenciar tarefas de backup
    - Consulte"Proteja as cargas de trabalho do Hyper-V" .
- **Cargas de trabalho do Oracle Database (Prévia)**:
    - Fazer backup e restaurar bancos de dados e logs
    - Use grupos de proteção para gerenciar tarefas de backup
    - Crie políticas para gerenciar backups de banco de dados e logs
    - Protegendo um banco de dados com uma arquitetura de backup 3-2-1
    - Configurar retenção de backup
    - Montar e desmontar backups do ARCHIVELOG
    - Consulte "Proteger cargas de trabalho do Oracle Database".
- **Cargas de trabalho do Kubernetes (visualização)**:
    - Gerencie e proteja seus aplicativos e recursos do Kubernetes em um só lugar.
    - Use políticas de proteção para estruturar seus backups incrementais.
    - Restaure aplicativos e recursos para os mesmos clusters e namespaces ou para clusters diferentes.
    - Use o NetApp Backup and Recovery sem o SnapCenter.
    - Consulte"Proteja as cargas de trabalho do Kubernetes" .

Benefícios de usar o NetApp Backup and Recovery

O NetApp Backup and Recovery oferece os seguintes benefícios:

- **Eficiente**: o NetApp Backup and Recovery executa replicação incremental contínua em nível de bloco, o que reduz significativamente a quantidade de dados replicados e armazenados. Isso ajuda a minimizar o tráfego de rede e os custos de armazenamento.
- **Seguro**: o NetApp Backup and Recovery criptografa dados em trânsito e em repouso e usa protocolos de comunicação seguros para proteger seus dados.
- **Custo-benefício**: o NetApp Backup and Recovery usa os níveis de armazenamento de menor custo disponíveis na sua conta na nuvem, o que ajuda a reduzir custos.
- **Automatizado**: o NetApp Backup and Recovery gera backups automaticamente com base em uma programação predefinida, o que ajuda a garantir que seus dados estejam protegidos.
- **Flexível**: o NetApp Backup and Recovery permite que você restaure dados no mesmo sistema ou em sistemas diferentes, o que proporciona flexibilidade na recuperação de dados.

Custo

A NetApp não cobra pelo uso da versão de teste. No entanto, você é responsável pelos custos associados aos recursos de nuvem que utiliza, como custos de armazenamento e transferência de dados.

Há dois tipos de custos associados ao uso do recurso de backup para objeto do NetApp Backup and Recovery com sistemas ONTAP :

- Taxas de recursos
- Taxas de serviço

A criação de snapshots ou volumes replicados é gratuita, exceto pelo espaço em disco necessário para armazená-los.

Custos de recursos

As taxas de recursos são pagas ao provedor de nuvem pela capacidade de armazenamento de objetos e pela gravação e leitura de arquivos de backup na nuvem.

- Para fazer backup em armazenamento de objetos, você paga ao seu provedor de nuvem pelos custos de armazenamento de objetos.

  Como o NetApp Backup and Recovery preserva a eficiência de armazenamento do volume de origem, você paga os custos de armazenamento de objetos do provedor de nuvem pelos dados *após* as eficiências do ONTAP (para a menor quantidade de dados após a aplicação da desduplicação e da compactação).

- Para restaurar dados usando o Search & Restore, certos recursos são provisionados pelo seu provedor de nuvem, e há um custo por TiB associado à quantidade de dados verificados pelas suas solicitações de pesquisa. (Esses recursos não são necessários para Navegar e Restaurar.)
  - Na AWS, "Amazona Atena" e "Cola AWS" os recursos são implantados em um novo bucket S3.
  - No Azure, um "Espaço de trabalho do Azure Synapse" e "Armazenamento do Azure Data Lake" são provisionados em sua conta de armazenamento para armazenar e analisar seus dados.
  - No Google, um novo bucket é implantado e o "Serviços do Google Cloud BigQuery" são provisionados em nível de conta/projeto.
- Se você planeja restaurar dados de volume de um arquivo de backup que foi movido para um armazenamento de objetos de arquivamento, haverá uma taxa adicional de recuperação por GiB e uma taxa por solicitação do provedor de nuvem.

- Se você planeja verificar se há ransomware em um arquivo de backup durante o processo de restauração de dados de volume (se você habilitou o DataLock e o Ransomware Resilience para seus backups na nuvem), você também incorrerá em custos extras de saída do seu provedor de nuvem.

Taxas de serviço

Para cargas de trabalho de volume ONTAP , você só paga pelos volumes protegidos em armazenamento de objetos. As cobranças são baseadas na capacidade lógica utilizada dos volumes ONTAP de origem antes da aplicação de otimizações de eficiência, também conhecida como Front-End Terabytes (FETB).

Para cargas de trabalho do Kubernetes, você é cobrado com base no tamanho combinado de todos os volumes persistentes.

Para todas as outras cargas de trabalho, você será cobrado pelos recursos protegidos em pelo menos um destino de armazenamento secundário ou de objetos. As cobranças são calculadas com base no tamanho lógico da carga de trabalho de origem. Para bancos de dados, isso significa o tamanho do banco de dados; para máquinas virtuais, o tamanho da máquina virtual.

Existem três formas de pagar pelo serviço de Backup e Recuperação:

- A primeira opção é assinar com seu provedor de nuvem, o que permite que você pague por mês.
- A segunda opção é adquirir um contrato anual.
- A terceira opção é comprar licenças diretamente da NetApp. Consulte o Licenciamento Para mais detalhes, consulte a seção abaixo.

Licenciamento

O NetApp Backup and Recovery oferece um período de avaliação gratuito, permitindo que você o utilize sem uma chave de licença por um tempo limitado.

Uma licença de backup só é necessária para operações de backup e restauração que envolvam armazenamento de objetos. A criação de snapshots e volumes replicados não requer licença.

Você pode escolher entre três opções de licenciamento:

- **Traga sua própria licença (BYOL)**: Compre uma licença com prazo determinado (1, 2 ou 3 anos) e baseada em capacidade (em incrementos de 1 TiB) da NetApp. Insira o número de série fornecido no NetApp Console para ativar. A licença abrange todos os sistemas de origem da sua organização. A renovação é obrigatória quando o prazo ou o limite de capacidade for atingido.
- **Pagamento conforme o uso (PAYGO)**: Assine através do marketplace do seu provedor de nuvem e pague por GiB de dados armazenados em backup, com cobrança mensal. Não é necessário nenhum pagamento antecipado. Um período de teste gratuito de 30 dias está disponível após a sua inscrição. Para mais informações, consulte "utilize uma assinatura pré-paga do NetApp Backup and Recovery." .
- **Contrato anual**: Disponível nos marketplaces da AWS e do Azure por 1, 2 ou 3 anos. Estão disponíveis dois contratos anuais:
  - **Backup na Nuvem**: Faz backup de dados do Cloud Volumes ONTAP e do ONTAP local.
  - **CVO Professional**: Inclui Cloud Volumes ONTAP e NetApp Backup and Recovery, com backups ilimitados para volumes do Cloud Volumes ONTAP (a capacidade de backup não é contabilizada na licença).
    - No plano CVO Professional, existem dois tipos de cobranças:
      - **Custos de recursos**: Baseados no uso de armazenamento. Para mais informações, consulte

"Licenciamento para Cloud Volumes ONTAP" .

- **Taxas de serviço**: Tarifas para NetApp Backup and Recovery. No entanto, se o volume de origem estiver em um sistema de armazenamento que utilize o plano CVO Professional, o NetApp Backup and Recovery será fornecido gratuitamente.

Ao usar o Google Cloud Platform, solicite uma oferta privada da NetApp e selecione seu plano durante a ativação no Google Cloud Marketplace.

"Aprenda a configurar licenças".

Cargas de trabalho, sistemas e destinos de backup suportados

Cargas de trabalho suportadas

O NetApp Backup and Recovery protege os seguintes tipos de cargas de trabalho:

- Volumes ONTAP
- Instâncias e bancos de dados do Microsoft SQL Server armazenados em disco físico e em Disco de Máquina Virtual VMware (VMDK) sobre VMFS ou NFS.
- VMs e datastores VMware
- Cargas de trabalho KVM (visualização)
- Cargas de trabalho do Hyper-V (visualização)
- Cargas de trabalho do Oracle Database (Prévia)
- Cargas de trabalho do Kubernetes (visualização)

Sistemas suportados

- SAN ONTAP local (protocolo iSCSI) e NAS (usando protocolos NFS e CIFS) com ONTAP versão 9.8 ou superior.
- Cloud Volumes ONTAP 9.8 ou superior para AWS (usando SAN e NAS)
- Cloud Volumes ONTAP 9.8 ou superior para Google Cloud Platform (usando os protocolos NFS e CIFS)
- Cloud Volumes ONTAP 9.8 ou superior para Microsoft Azure (usando SAN e NAS)
- Amazon FSx for NetApp ONTAP (somente para cargas de trabalho do Microsoft SQL Server)

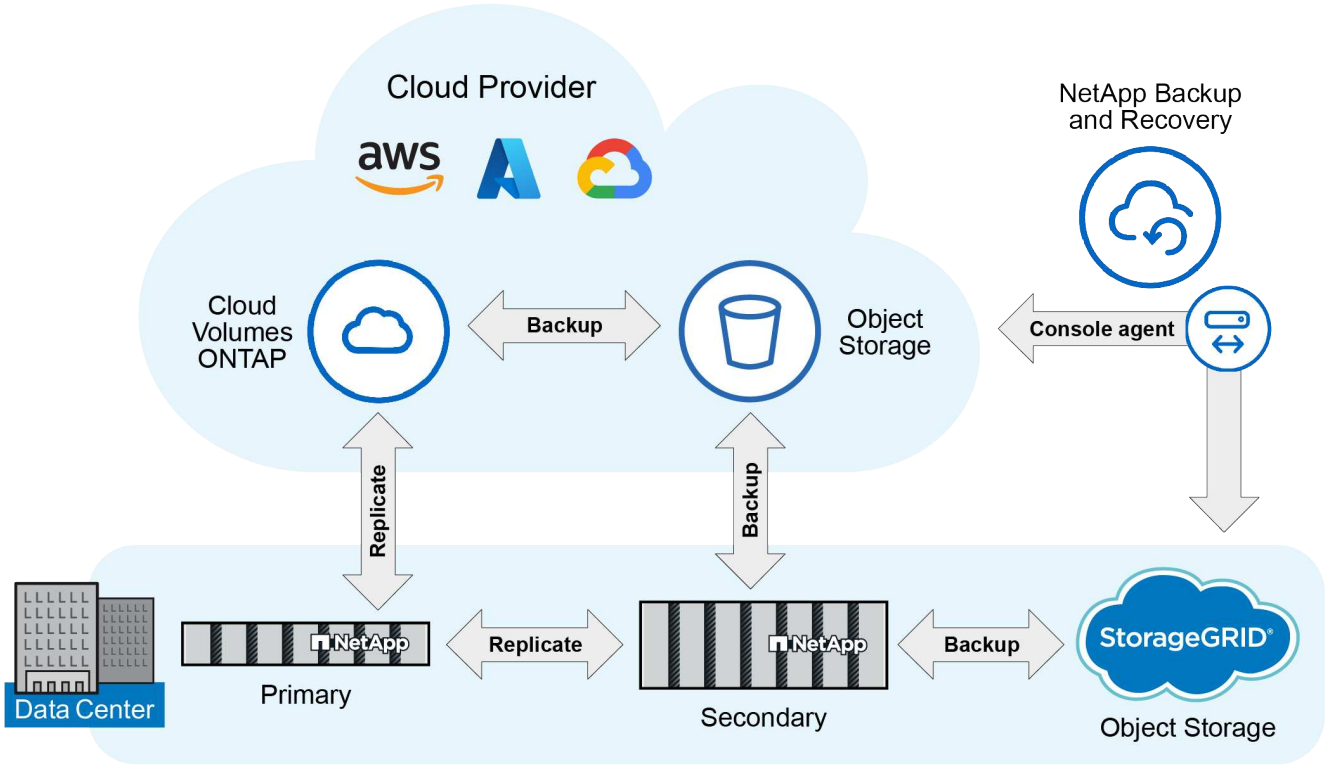
Destinos de backup suportados

- Amazon Web Services (AWS) S3
- Armazenamento em nuvem do Google
- Microsoft Azure Blob (não disponível para cargas de trabalho VMware na versão de visualização)
- StorageGRID
- ONTAP S3 (não disponível para cargas de trabalho VMware na versão de visualização)

Como funciona o NetApp Backup and Recovery

Quando você ativa o NetApp Backup and Recovery, o serviço executa um backup completo dos seus dados. Após o backup inicial, todos os backups adicionais são incrementais. Isso mantém o tráfego de rede no mínimo.

A imagem a seguir mostra o relacionamento entre os componentes.



O armazenamento primário para o objeto também é suportado, não apenas do armazenamento secundário para o armazenamento de objetos.

Onde os backups residem em locais de armazenamento de objetos

As cópias de backup são armazenadas em um armazenamento de objetos que o NetApp Console cria na sua conta na nuvem. Há um armazenamento de objetos por cluster ou sistema, e o Console nomeia o armazenamento de objetos da seguinte forma: `netapp-backup-clusteruuid` . Certifique-se de não excluir este armazenamento de objetos.

- Na AWS, o NetApp Console permite o "Recurso de bloqueio de acesso público do Amazon S3" no bucket S3.
- No Azure, o NetApp Console usa um grupo de recursos novo ou existente com uma conta de armazenamento para o contêiner de Blobs. "bloqueia o acesso público aos seus dados de blob" Por padrão.
- No StorageGRID, o Console usa uma conta de armazenamento existente para o bucket de armazenamento de objetos.
- No ONTAP S3, o Console usa uma conta de usuário existente para o bucket S3.

As cópias de backup estão associadas à sua organização do NetApp Console

As cópias de backup são associadas à organização do NetApp Console na qual o agente do Console reside. "Saiba mais sobre identidade e acesso do NetApp Console" .

Se você tiver vários agentes do Console na mesma organização do NetApp Console , cada agente do Console exibirá a mesma lista de backups.

Termos que podem ajudar você com o NetApp Backup and Recovery

Você pode se beneficiar ao entender alguma terminologia relacionada à proteção.

- **Proteção**: Proteção no NetApp Backup and Recovery significa garantir que snapshots e backups imutáveis ocorram regularmente em um domínio de segurança diferente usando políticas de proteção.
- **Carga de trabalho**: uma carga de trabalho no NetApp Backup and Recovery pode incluir volumes ONTAP , instâncias e bancos de dados do Microsoft SQL Server; VMs e datastores do VMware; ou clusters e aplicativos do Kubernetes.

Pré-requisitos do NetApp Backup and Recovery

Comece a usar o NetApp Backup and Recovery verificando a prontidão do seu ambiente operacional, do agente do NetApp Console e da conta do NetApp Console . Para usar o NetApp Backup and Recovery, você precisará destes pré-requisitos.

Pré-requisito para ONTAP 9.8 e posterior

Uma licença ONTAP One deve ser habilitada na instância ONTAP local.

Pré-requisitos para backups no armazenamento de objetos

Para usar o armazenamento de objetos como destinos de backup, você precisa de uma conta no AWS S3, Microsoft Azure Blob, StorageGRID ou ONTAP e as permissões de acesso apropriadas configuradas.

- "Proteja seus dados de volume ONTAP"

Requisitos para proteger cargas de trabalho do Microsoft SQL Server

Para usar o NetApp Backup and Recovery para cargas de trabalho do Microsoft SQL Server, você precisa dos seguintes pré-requisitos de sistema host, espaço e dimensionamento.

Item	Requisitos
Sistemas operacionais	Microsoft Windows Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .
Versões do Microsoft SQL Server	A versão 2012 e posteriores são suportadas pelo VMware Virtual Machine File System (VMFS) e pelo VMware Virtual Machine Disk (VMDK) NFS.
Versão do SnapCenter Server	O SnapCenter Server versão 5.0 ou superior é necessário se você for importar seus dados existentes do SnapCenter para o NetApp Backup and Recovery. Se você já tem o SnapCenter, primeiro verifique se atendeu aos pré-requisitos antes de importar do SnapCenter. Ver"Pré-requisitos para importar recursos do SnapCenter" .

Item	Requisitos
RAM mínima para o plug-in no host do SQL Server	1 GB
Espaço mínimo de instalação e log para o plug-in no host do SQL Server	5 GB Aloque espaço em disco suficiente e monitore o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de backups realizados e da frequência das operações de proteção de dados. Se não houver espaço suficiente, os logs não serão criados para as operações.
Pacotes de software necessários	• Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) • PowerShell 7.4.2 Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Requisitos para proteger cargas de trabalho do VMware

Você precisa de requisitos específicos para descobrir e proteger suas cargas de trabalho do VMware.

Suporte de software

- São suportados armazenamentos de dados NFS e VMFS.
- Versões NFS suportadas: NFS 3 e NFS 4.1
- Versões do VMware ESXi Server suportadas: 7.0U1 e superior
- Versões do VMware vCenter vSphere suportadas: 7.0U1 e superior
- Endereços IP: IPv4 e IPv6
- VMware TLS: 1.2, 1.3
- Armazenamento conectado compatível: ONTAP 9.13 ou posterior

Requisitos de conexão e porta para proteger cargas de trabalho do VMware

Tipo de porta	Porta pré-configurada
Porta do servidor VMware ESXi	443 (HTTPS), bidirecional. O recurso Restauração de arquivo convidado usa esta porta.
Cluster de armazenamento ou porta de VM de armazenamento	443 (HTTPS), bidirecional. 80 (HTTP), bidirecional. Esta porta é usada para comunicação entre o dispositivo virtual e a VM de armazenamento ou o cluster que contém a VM de armazenamento.

Requisitos de controle de acesso baseado em função (RBAC) para proteger cargas de trabalho do VMware

A conta de administrador do vCenter deve ter os privilégios necessários do vCenter.

Para obter uma lista de privilégios do vCenter necessários, consulte "Privilégios necessários do SnapCenter Plug-in for VMware vSphere vCenter" .

Requisitos para proteger cargas de trabalho KVM

Você precisa de requisitos específicos para descobrir e proteger máquinas virtuais KVM.

- Uma distribuição Linux moderna executando a versão do kernel 5.14.0-503.22.1.el9_5.x86_64 (longo prazo) ou posterior
- Seus hosts KVM e máquinas virtuais devem ser gerenciados por uma plataforma de gerenciamento. O NetApp Backup and Recovery é compatível com as seguintes plataformas de gerenciamento:
  - Apache CloudStack 4.22.0.0
- Certifique-se de que o tráfego de rede de entrada para a porta 22 seja permitido do agente do console para o host KVM.
- QEMU Guest Agent versão 9.0.0 ou posterior
- libvirt versão 10.5.0 ou posterior

Para garantir que a restauração da carga de trabalho KVM seja concluída com sucesso, certifique-se de que a configuração **Habilitar snapshot consistente com a VM** esteja ativa na política de proteção usada para backups do KVM.

Para habilitar a proteção de VMs KVM administradas por usuários não root, siga os passos abaixo:

1. Monte o volume como tipo NFS3 para evitar o uso do `nobody` usuário e grupo.
2. Use o seguinte comando para adicionar um usuário não root ao grupo. `qemu` grupo preservando seus grupos existentes:

```
usermod -aG qemu <non-root-user>
```

3. Use o seguinte comando para conceder a propriedade do caminho de montagem ao `qemu` Usuário e grupo, e alterar permissões para o caminho de montagem:

```
chown -R qemu:qemu <kvm_vm_mount_path> & chmod 771
<kvm_vm_mount_path>
```

4. Exclua o diretório NetApp_SnapCenter_Backups existente, caso esteja presente.

Requisitos para proteger cargas de trabalho do Oracle Database

Garanta que seu ambiente atenda aos requisitos específicos para descobrir e proteger recursos Oracle.

- Banco de dados Oracle:
  - O Oracle 19C e 21C são suportados em uma implantação autônoma.
  - O Oracle Database deve ser implantado no armazenamento NetApp ONTAP primário ou secundário.

    - Suporte ao sistema operacional host: Red Hat Enterprise Linux 8 e 9
- Suporte de armazenamento de objetos:
    - Armazenamento de Objetos do Azure
    - Amazon AWS
    - NetApp StorageGRID
    - ONTAP S3

Requisitos para proteger aplicativos Kubernetes

Você precisa de requisitos específicos para descobrir recursos do Kubernetes e proteger seus aplicativos Kubernetes.

Para requisitos do NetApp Console , consulteNo NetApp Console .

- Um sistema ONTAP primário (ONTAP 9.16.1 ou posterior)
- Um cluster do Kubernetes - As distribuições e versões do Kubernetes suportadas incluem:
    - Anthos On-Prem (VMware) e Anthos em bare metal 1.16
    - Kubernetes 1.27 - 1.33
    - OpenShift 4.10 - 4.18
    - Rancher Kubernetes Engine 2 (RKE2) v1.26.7+rke2r1, v1.28.5+rke2r1
    - Suse Rancher
- NetApp Trident 24.10 ou posterior
- NetApp Trident Protect 25.07 ou posterior (instalado durante a descoberta de workload do Kubernetes)
- NetApp Trident Protect Connector 25.07 ou posterior (instalado durante a descoberta de cargas de trabalho do Kubernetes)
    - Certifique-se de que a porta TCP 443 esteja desbloqueada na direção de saída entre o cluster Kubernetes, o Trident Protect Connector e o proxy Trident Protect.

Requisitos para proteger cargas de trabalho do Hyper-V

Certifique-se de que sua instância do Hyper-V atenda aos requisitos específicos para descobrir e proteger máquinas virtuais.

- Requisitos de software para o host do Hyper-V Windows Server:
    - Edições do Microsoft Hyper-V 2019, 2022 e 2025
    - Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes)
    - PowerShell 7.4.2 ou posterior
    - Se usuários que não fazem parte de um domínio de administrador forem proteger máquinas virtuais Hyper-V, certifique-se de que eles tenham as seguintes permissões:
        - Certifique-se de que o usuário seja membro do grupo de administradores locais.
        - Certifique-se de que o usuário faça parte da política de segurança local "Fazer logon como serviço".
    - Certifique-se de que o tráfego HTTPS bidirecional seja permitido para as seguintes portas nas configurações do Firewall do Windows:

        - 8144 (Plug-in NetApp para Hyper-V)
        - 8145 (Plug-in NetApp para Windows)
- Requisitos de hardware para o host Hyper-V:
    - Hosts autônomos e agrupados pela FCI são suportados
    - Mínimo de 1 GB de RAM para o plug-in NetApp Hyper-V no host Hyper-V
    - 5 GB de espaço mínimo para instalação e log do plug-in no host Hyper-V

> Certifique-se de alocar espaço em disco suficiente no host Hyper-V para a pasta de logs e monitore regularmente seu uso. O espaço necessário depende da frequência com que ocorrem backups e operações de proteção de dados. Se não houver espaço suficiente, os logs não serão gerados.

- Requisitos de configuração do NetApp ONTAP :
    - Um sistema ONTAP primário (ONTAP 9.14.1 ou posterior)
    - Para implantações do Hyper-V usando compartilhamentos CIFS para armazenar dados de máquina virtual, certifique-se de que a propriedade de compartilhamento de disponibilidade contínua esteja habilitada no sistema ONTAP . Consulte o "Documentação do ONTAP" para obter instruções.

No NetApp Console

Certifique-se de que o NetApp Console atenda aos seguintes requisitos.

- Um usuário do Console deve ter a função e os privilégios necessários para executar operações em cargas de trabalho do Microsoft SQL Server e do Kubernetes. Para descobrir os recursos, você precisa ter a função de Superadministrador do NetApp Backup and Recovery . Ver"Acesso baseado em função do NetApp Backup and Recovery aos recursos" para obter detalhes sobre as funções e permissões necessárias para executar operações no NetApp Backup and Recovery.
- Uma organização do Console com pelo menos um agente do Console ativo que se conecta a clusters ONTAP locais ou ao Cloud Volumes ONTAP.
- Pelo menos um sistema de console com um cluster NetApp ONTAP local ou Cloud Volumes ONTAP .
- Um agente de console

  Consulte "Aprenda a configurar um agente de console" e "requisitos padrão do NetApp Console" .

    - A versão de visualização requer o sistema operacional Ubuntu 22.04 LTS para o agente do Console.

Configurar o NetApp Console

A próxima etapa é configurar o Console e o NetApp Backup and Recovery.

Análise "requisitos padrão do NetApp Console" .

Criar um agente de console

Você deve entrar em contato com sua equipe de produtos da NetApp para testar o Backup e a recuperação. Então, quando você usar o agente do Console, ele incluirá os recursos apropriados para o serviço.

Para criar um agente do Console no NetApp Console antes de usar o serviço, consulte a documentação do Console que descreve "como criar um agente de console" .

Onde instalar o agente do Console

Para concluir uma operação de restauração, o agente do Console pode ser instalado nos seguintes locais:

- Para o Amazon S3, o agente do Console pode ser implantado em suas instalações.
- Para o Azure Blob, o agente do Console pode ser implantado em suas instalações.
- Para o StorageGRID, o agente do Console deve ser implantado em suas instalações; com ou sem acesso à Internet.
- Para o ONTAP S3, o agente do Console pode ser implantado em suas instalações (com ou sem acesso à Internet) ou em um ambiente de provedor de nuvem

Referências a "sistemas ONTAP locais" incluem sistemas FAS e AFF .

Configurar licenciamento para NetApp Backup and Recovery

Você pode licenciar o NetApp Backup and Recovery comprando uma assinatura de pagamento conforme o uso (PAYGO) ou anual do mercado para * NetApp Intelligent Services* do seu provedor de nuvem ou comprando uma licença "traga sua própria licença" (BYOL) da NetApp. Uma licença válida é necessária para ativar o NetApp Backup and Recovery em um sistema, criar backups dos seus dados de produção e restaurar dados de backup em um sistema de produção.

Algumas notas antes de continuar lendo:

- Se você já assinou a assinatura pré-paga (PAYGO) no marketplace do seu provedor de nuvem para um sistema Cloud Volumes ONTAP , você também estará automaticamente inscrito no NetApp Backup and Recovery . Você não precisará assinar novamente.
- A licença BYOL (Bring Your Own License) do NetApp Backup and Recovery é uma licença flutuante que você pode usar em todos os sistemas associados à sua organização ou conta do NetApp Console . Portanto, se você tiver capacidade de backup suficiente disponível em uma licença BYOL existente, não precisará comprar outra licença BYOL.
- Se você estiver usando uma licença BYOL, é recomendável que você assine também uma assinatura PAYGO. Se você fizer backup de mais dados do que o permitido pela sua licença BYOL, ou se o prazo da sua licença expirar, o backup continuará por meio da sua assinatura paga conforme o uso - não haverá interrupção do serviço.
- Ao fazer backup de dados ONTAP locais no StorageGRID, você precisa de uma licença BYOL, mas não há custo para espaço de armazenamento do provedor de nuvem.

"Saiba mais sobre os custos relacionados ao uso do NetApp Backup and Recovery."

Teste gratuito de 30 dias

Um teste gratuito de 30 dias do NetApp Backup and Recovery está disponível se você assinar uma assinatura paga conforme o uso no marketplace do seu provedor de nuvem para * NetApp Intelligent Services*. O teste gratuito começa no momento em que você assina a listagem do mercado. Observe que se você pagar pela assinatura do marketplace ao implantar um sistema Cloud Volumes ONTAP e iniciar seu teste gratuito do NetApp Backup and Recovery 10 dias depois, você terá 20 dias restantes para usar o teste gratuito.

Quando o teste gratuito terminar, você será transferido automaticamente para a assinatura PAYGO sem interrupção. Se você decidir não continuar usando o NetApp Backup and Recovery, basta"cancelar o registro do NetApp Backup and Recovery do sistema" antes do término do teste e você não será cobrado.

Encerrar o teste gratuito

Se quiser continuar usando o NetApp Backup and Recovery após o término do teste gratuito, você deverá configurar uma assinatura paga. Você pode fazer isso na interface do NetApp Console navegando até a seção de cobrança e selecionando um plano de assinatura que atenda às suas necessidades. Se não quiser continuar usando o NetApp Backup and Recovery, você pode encerrar o teste gratuito.

Quando você encerra o teste gratuito sem assinar um plano pago, seus dados são excluídos automaticamente 60 dias após o término do teste gratuito. Opcionalmente, você pode fazer com que o sistema exclua seus dados imediatamente.

Passos

1. Na página inicial do NetApp Backup and Recovery , selecione **Ver avaliação gratuita**.
2. Selecione **Encerrar teste gratuito**.
3. Selecione **Excluir dados imediatamente após encerrar meu teste gratuito** para excluir seus dados imediatamente.
4. Digite **fim do teste** na caixa.
5. Selecione **Fim** para confirmar.

Use uma assinatura PAYGO do NetApp Backup and Recovery

No pagamento conforme o uso, você pagará ao seu provedor de nuvem pelos custos de armazenamento de objetos e pelos custos de licenciamento de backup da NetApp por hora em uma única assinatura. Você deve assinar o * NetApp Intelligent Services* no Marketplace mesmo se tiver uma avaliação gratuita ou se trouxer sua própria licença (BYOL):

- A assinatura garante que não haverá interrupção do serviço após o término do teste gratuito. Quando o período de teste terminar, você será cobrado por hora, de acordo com a quantidade de dados dos quais fizer backup.
- Se você fizer backup de mais dados do que o permitido pela sua licença BYOL, as operações de backup e restauração de dados continuarão por meio da sua assinatura paga conforme o uso. Por exemplo, se você tiver uma licença BYOL de 10 TiB, toda a capacidade além de 10 TiB será cobrada por meio da assinatura PAYGO.

Você não será cobrado pela sua assinatura pré-paga durante o período de teste gratuito ou se não tiver excedido sua licença BYOL.

Existem alguns planos PAYGO para NetApp Backup and Recovery:

- Um pacote "Cloud Backup" que permite fazer backup de dados Cloud Volumes ONTAP e de dados ONTAP locais.
- Um pacote "CVO Professional" que permite agrupar o Cloud Volumes ONTAP e o NetApp Backup and Recovery. Isso inclui backups ilimitados para o sistema Cloud Volumes ONTAP usando a licença (a capacidade de backup não é contabilizada na capacidade licenciada). Esta opção não permite que você faça backup de dados ONTAP locais.

  Observe que esta opção também requer uma assinatura PAYGO de backup e recuperação, mas nenhuma cobrança será cobrada para sistemas Cloud Volumes ONTAP qualificados.

"Saiba mais sobre esses pacotes de licença baseados em capacidade".

Use estes links para assinar o NetApp Backup and Recovery no marketplace do seu provedor de nuvem:

- AWS: "Acesse a oferta do Marketplace para NetApp Intelligent Services para obter detalhes sobre preços" .
- Azure: "Acesse a oferta do Marketplace para NetApp Intelligent Services para obter detalhes sobre preços" .
- Google Cloud: "Acesse a oferta do Marketplace para NetApp Intelligent Services para obter detalhes sobre preços" .

Use um contrato anual

Pague pelo NetApp Backup and Recovery anualmente adquirindo um contrato anual. Eles estão disponíveis em prazos de 1, 2 ou 3 anos.

Se você tiver um contrato anual de um marketplace, todo o consumo do NetApp Backup and Recovery será cobrado desse contrato. Você não pode misturar e combinar um contrato de mercado anual com um BYOL.

Ao usar a AWS, há dois contratos anuais disponíveis na "Página do AWS Marketplace" para sistemas Cloud Volumes ONTAP e ONTAP locais:

- Um plano "Cloud Backup" que permite fazer backup de dados Cloud Volumes ONTAP e de dados ONTAP locais.

  Se você quiser usar esta opção, configure sua assinatura na página do Marketplace e então "associe a assinatura às suas credenciais da AWS" . Observe que você também precisará pagar pelos seus sistemas Cloud Volumes ONTAP usando esta assinatura de contrato anual, pois você pode atribuir apenas uma assinatura ativa às suas credenciais da AWS no Console.

- Um plano "CVO Professional" que permite combinar o Cloud Volumes ONTAP e o NetApp Backup and Recovery. Isso inclui backups ilimitados para o sistema Cloud Volumes ONTAP usando a licença (a capacidade de backup não é contabilizada na capacidade licenciada). Esta opção não permite que você faça backup de dados ONTAP locais.

  Veja o "Tópico de licenciamento do Cloud Volumes ONTAP" para saber mais sobre esta opção de licenciamento.

  Se você deseja usar essa opção, pode configurar o contrato anual ao criar um sistema Cloud Volumes ONTAP e o Console solicitar que você se inscreva no AWS Marketplace.

Ao usar o Azure, há dois contratos anuais disponíveis no "Página do Azure Marketplace" para sistemas Cloud Volumes ONTAP e ONTAP locais:

- Um plano "Cloud Backup" que permite fazer backup de dados Cloud Volumes ONTAP e de dados ONTAP locais.

  Se você quiser usar esta opção, configure sua assinatura na página do Marketplace e então "associar a assinatura às suas credenciais do Azure" . Observe que você também precisará pagar pelos seus sistemas Cloud Volumes ONTAP usando esta assinatura de contrato anual, pois você pode atribuir apenas uma assinatura ativa às suas credenciais do Azure no Console.

- Um plano "CVO Professional" que permite combinar o Cloud Volumes ONTAP e o NetApp Backup and Recovery. Isso inclui backups ilimitados para o sistema Cloud Volumes ONTAP usando a licença (a

capacidade de backup não é contabilizada na capacidade licenciada). Esta opção não permite que você faça backup de dados ONTAP locais.

Veja o "Tópico de licenciamento do Cloud Volumes ONTAP" para saber mais sobre esta opção de licenciamento.

Se você deseja usar essa opção, pode configurar o contrato anual ao criar um sistema Cloud Volumes ONTAP e o Console solicitar que você se inscreva no Azure Marketplace.

Ao usar o GCP, entre em contato com seu representante de vendas da NetApp para adquirir um contrato anual. O contrato está disponível como uma oferta privada no Google Cloud Marketplace.

Após a NetApp compartilhar a oferta privada com você, você poderá selecionar o plano anual ao se inscrever no Google Cloud Marketplace durante a ativação do NetApp Backup and Recovery .

Use uma licença BYOL do NetApp Backup and Recovery

As licenças "traga sua própria" da NetApp oferecem prazos de 1, 2 ou 3 anos. Você paga somente pelos dados que protege, calculados pela capacidade lógica utilizada (*antes* de quaisquer eficiências) dos volumes ONTAP de origem que estão sendo copiados. Essa capacidade também é conhecida como Terabytes Front-End (FETB).

A licença BYOL NetApp Backup and Recovery é uma licença flutuante em que a capacidade total é compartilhada entre todos os sistemas associados à sua organização ou conta do NetApp Console . Para sistemas ONTAP , você pode obter uma estimativa aproximada da capacidade necessária executando o comando CLI `volume show -fields logical-used-by-afs` para os volumes que você planeja fazer backup.

Se você não tiver uma licença BYOL do NetApp Backup and Recovery , clique no ícone de bate-papo no canto inferior direito do Console para adquirir uma.

Opcionalmente, se você tiver uma licença baseada em nó não atribuída para o Cloud Volumes ONTAP que não será usada, você poderá convertê-la em uma licença do NetApp Backup and Recovery com a mesma equivalência em dólares e a mesma data de expiração. "Clique aqui para mais detalhes" .

Use o NetApp Console para gerenciar licenças BYOL. Você pode adicionar novas licenças, atualizar licenças existentes e visualizar o status da licença no Console.

"Saiba mais sobre como adicionar licenças".

Excedendo a capacidade da licença

Exceder a capacidade da sua licença aciona as tarifas PAYGO; sem uma assinatura PAYGO, você não pode criar novos backups, embora os backups existentes possam ser restaurados sem garantia de serviço. Certifique-se de renovar sua licença antes que ela expire; uma licença expirada impede novos backups e interrompe o serviço.

Configurar certificados de segurança para StorageGRID e ONTAP no NetApp Backup and Recovery

Crie um certificado de segurança para permitir a comunicação entre o NetApp Backup and Recovery e o StorageGRID ou ONTAP.

Crie um certificado de segurança para StorageGRID

Se a comunicação entre os contêineres do NetApp Backup and Recovery e o StorageGRID verificar o certificado do StorageGRID , conclua as etapas a seguir.

O certificado gerado deve ter CN e Nome Alternativo do Assunto como o nome fornecido no NetApp Backup and Recovery quando você ativou o backup.

Passos

1. Siga as etapas na documentação do StorageGRID para criar o certificado do StorageGRID .

   "Informações do StorageGRID sobre a configuração de certificados"

2. Atualize o StorageGRID com o certificado, caso ainda não tenha feito isso.
3. Efetue login no agente do Console como usuário root. Correr:

   ```
   sudo su
   ```

4. Obtenha o volume do Docker do NetApp Backup and Recovery (Cloud Backup Service). Correr:

   ```
   docker volume ls | grep cbs
   ```

   Exemplo de saída:

   ```
   local service-manager-2_cloudmanager_cbs_volume"
   ```

   O nome do volume difere entre os modos de implantação Padrão, Privado e Restrito. Este exemplo usa o modo Padrão. Consulte "Modos de implantação do NetApp Console" .

5. Localize o ponto de montagem do volume do NetApp Backup and Recovery . Correr:

   ```
   docker volume inspect service-manager-2_cloudmanager_cbs_volume | grep
   Mountpoint
   ```

   Exemplo de saída:

   ```
   "Mountpoint": "/var/lib/docker/volumes/service-manager-
   2_cloudmanager_cbs_volume/_data"
   ```

   O ponto de montagem difere entre os modos de implantação Padrão, Privado e Restrito. Este exemplo mostra uma implantação de nuvem padrão. Consulte "Modos de implantação do NetApp Console" .

6. Mude para o diretório MountPoint. Correr:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

7. Se o certificado do StorageGRID for assinado pela CA raiz e uma CA intermediária, anexe o `pem` arquivos de ambos em um arquivo chamado `sgws.crt` no local atual. Não adicione o certificado de folha a este arquivo.

Etapas para o contêiner cloudmanager_cbs

Você precisará habilitar a verificação do certificado do StorageGRID Server no NetApp Backup and Recovery (Cloud Backup Service).

1. Altere os diretórios para o volume do Docker obtido nas etapas anteriores.

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Altere os diretórios para o diretório config.

```
cd cbs_config
```

3. Crie e salve um arquivo de configuração conforme mostrado abaixo com um dos seguintes nomes com base no seu ambiente de implantação:

   - `production-customer.json`Usado para implantações de modo Padrão e modo Restrito.
   - `darksite-customer.json`Usado para implantações em modo privado.

   Consulte "Modos de implantação do NetApp Console" .

   Arquivo de configuração

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  }
}
```

4. Saia do contêiner. Correr:

```
exit
```

5. Reiniciar `cloudmanager_cbs` . Correr:

```
docker restart cloudmanager_cbs
```

Etapas para o contêiner cloudmanager_cbs_catalog

Em seguida, você precisará habilitar a verificação do certificado do StorageGRID Server para o Cataloging Service.

1. Alterar diretórios para o volume do Docker:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Configurar o catálogo. Correr:

```
cd cbs_catalog_config
```

3. Crie um arquivo de configuração conforme mostrado abaixo com um dos seguintes nomes com base no seu ambiente de implantação:

   - `production-customer.json`Usado para implantações de modo Padrão e modo Restrito.
   - `darksite-customer.json`Usado para implantações em modo privado.

   Consulte "Modos de implantação do NetApp Console" .

   Arquivo de configuração do catálogo

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  }
}
```

4. Reinicie o catálogo. Correr:

```
docker restart cloudmanager_cbs_catalog
```

Atualizar o certificado do agente do Console com o certificado StorageGRID com base no sistema operacional do agente

Ubuntu

1. Copie o certificado SGWS para `/usr/local/share/ca-certificates` . Aqui está um exemplo:

```
cp /config/sgws.crt /usr/local/share/ca-certificates/
```

onde `sgws.crt` é o certificado da CA raiz.

2. Atualize os certificados do host com o certificado StorageGRID . Correr

```
sudo update-ca-certificates
```

Red Hat Enterprise Linux

1. Copie o certificado SGWS para `/etc/pki/ca-trust/source/anchors/` .

```
cp /config/sgws.crt /etc/pki/ca-trust/source/anchors/
```

onde `sgws.crt` é o certificado da CA raiz.

2. Atualize os certificados do host com o certificado StorageGRID .

```
update-ca-trust extract
```

3. Atualizar o `ca-bundle.crt`

```
cd /etc/pki/tls/certs/
openssl x509 -in ca-bundle.crt -text -noout
```

4. Para verificar se os certificados estão presentes, execute o seguinte comando:

```
openssl crl2pkcs7 -nocrl -certfile /etc/pki/tls/certs/ca-bundle.crt |
openssl pkcs7 -print_certs | grep subject | head
```

Crie um certificado de segurança para o ONTAP

Se a comunicação entre os contêineres do NetApp Backup and Recovery e o ONTAP validar o certificado ONTAP , conclua as etapas a seguir.

O NetApp Backup and Recovery usa o IP de gerenciamento de cluster para se conectar ao ONTAP. Insira o endereço IP do cluster em Assunto Nomes alternativos do certificado. Especifique esta etapa ao gerar o CSR usando a interface do usuário do System Manager.

Use a documentação do System Manager para criar um novo certificado CA para o ONTAP.

- "Gerenciar certificados com o Gerenciador de Sistemas"
- "Como gerenciar certificados SSL ONTAP com o System Manager"

Passos

1. Efetue login no agente do Console como root. Correr:

```
sudo su
```

2. Obtenha o volume do Docker do NetApp Backup and Recovery . Correr:

```
docker volume ls | grep cbs
```

Exemplo de saída:

```
local service-manager-2_cloudmanager_cbs_volume
```

> O nome do volume difere entre os modos de implantação Padrão, Privado e Restrito. Este exemplo mostra uma implantação de nuvem padrão. Consulte "Modos de implantação do NetApp Console" .

3. Obtenha a montagem para o volume. Correr:

```
docker volume inspect service-manager-2_cloudmanager_cbs_volume | grep
Mountpoint
```

Exemplo de saída:

```
"Mountpoint": "/var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

> O ponto de montagem difere entre os modos de implantação Padrão, Privado e Restrito. Este exemplo mostra uma implantação de nuvem padrão. Consulte "Modos de implantação do NetApp Console" .

4. Mude para o diretório do ponto de montagem. Correr:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

5. Conclua uma das seguintes etapas:
   - Se o certificado ONTAP for assinado pela CA raiz e uma CA intermediária, anexe o `pem` arquivos de ambos em um arquivo chamado `ontap.crt` no local atual.
   - Se o certificado ONTAP for assinado por uma única CA, renomeie o `pem` arquivar como `ontap.crt` e copie-o no local atual. Não adicione o certificado de folha a este arquivo.

Etapas para o contêiner cloudmanager_cbs

Em seguida, ative a verificação do certificado do servidor ONTAP no NetApp Backup and Recovery (Cloud Backup Service).

1. Altere os diretórios para o volume do Docker obtido nas etapas anteriores.

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Mude para o diretório de configuração. Correr:

```
cd cbs_config
```

3. Crie um arquivo de configuração conforme mostrado abaixo com um dos seguintes nomes com base no seu ambiente de implantação:
   - `production-customer.json`Usado para implantações de modo Padrão e modo Restrito.
   - `darksite-customer.json`Usado para implantações em modo privado.

     Consulte "Modos de implantação do NetApp Console" .

     Arquivo de configuração

```
{
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

4. Saia do contêiner. Correr:

```
exit
```

5. Reinicie o NetApp Backup and Recovery. Correr:

```
docker restart cloudmanager_cbs
```

Etapas para o contêiner cloudmanager_cbs_catalog

Habilite a verificação do certificado do servidor ONTAP para o Serviço de Catalogação.

1. Altere os diretórios para o volume do Docker. Correr:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Correr:

```
cd cbs_catalog_config
```

3. Crie um arquivo de configuração conforme mostrado abaixo com um dos seguintes nomes com base no seu ambiente de implantação:

   - `production-customer.json`Usado para implantações de modo Padrão e modo Restrito.
   - `darksite-customer.json`Usado para implantações em modo privado.

   Consulte "Modos de implantação do NetApp Console" .

   Arquivo de configuração

```
{
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

4. Reinicie o NetApp Backup and Recovery. Correr:

```
docker restart cloudmanager_cbs_catalog
```

Crie um certificado para ONTAP e StorageGRID

Se você precisar habilitar o certificado para ONTAP e StorageGRID, o arquivo de configuração ficará assim:

Arquivo de configuração para ONTAP e StorageGRID

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  },
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

Configure destinos de backup antes de usar o NetApp Backup and Recovery

Antes de usar o NetApp Backup and Recovery, execute algumas etapas para configurar destinos de backup.

Antes de começar, revise"pré-requisitos" para garantir que seu ambiente esteja pronto.

Preparar o destino do backup

Prepare um ou mais dos seguintes destinos de backup:

- NetApp StorageGRID.

  Consulte "Descubra o StorageGRID" .

  Consulte "Documentação do StorageGRID" para obter detalhes sobre StorageGRID.

- Serviços Web da Amazon. Consulte "Documentação do Amazon S3" .

  Faça o seguinte para preparar a AWS como um destino de backup:

    - Crie uma conta na AWS.
    - Configure as permissões do S3 na AWS, listadas na próxima seção.
    - Para obter detalhes sobre como gerenciar seu armazenamento AWS no Console, consulte "Gerencie seus buckets do Amazon S3" .
- Microsoft Azure.
    - Consulte "Documentação do Azure NetApp Files" .
    - Crie uma conta no Azure.
    - Configurar "Permissões do Azure" no Azure.
    - Para obter detalhes sobre como gerenciar seu armazenamento do Azure no Console, consulte "Gerencie suas contas de armazenamento do Azure" .

Depois de configurar as opções no próprio destino de backup, você o configurará posteriormente como um destino de backup no NetApp Backup and Recovery. Para obter detalhes sobre como configurar o destino de backup no NetApp Backup and Recovery, consulte"Descubra alvos de backup" .

Configurar permissões S3

Você precisará configurar dois conjuntos de permissões do AWS S3:

- Permissões para o agente do Console criar e gerenciar o bucket do S3.
- Permissões para o cluster ONTAP local para que ele possa ler e gravar dados no bucket S3.

Passos

1. Certifique-se de que o agente do Console tenha as permissões necessárias. Para mais detalhes, veja "Permissões de política do NetApp Console" .

    Ao criar backups nas regiões da AWS China, você precisa alterar o nome do recurso da AWS "arn" em todas as seções *Resource* nas políticas do IAM de "aws" para "aws-cn"; por exemplo `arn:aws-cn:s3:::netapp-backup-*` .

2. Ao ativar o serviço, o assistente de backup solicitará que você insira uma chave de acesso e uma chave secreta. Essas credenciais são passadas ao cluster ONTAP para que o ONTAP possa fazer backup e restaurar dados no bucket S3. Para isso, você precisará criar um usuário do IAM com as seguintes permissões.

    Consulte o "Documentação da AWS: Criando uma função para delegar permissões a um usuário do IAM" .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "arn:aws:s3:::netapp-backup-*",
      "Effect": "Allow",
      "Sid": "backupPolicy"
    },
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*/*",
      "Effect": "Allow"
    }
  ]
}
```

Efetue login no NetApp Backup and Recovery

Use o NetApp Console para efetuar login no NetApp Backup and Recovery.

O NetApp Backup and Recovery usa gerenciamento de identidade e acesso para controlar o que cada usuário pode fazer.

Para obter detalhes sobre as ações que cada função pode executar, consulte"Funções de usuário do NetApp Backup and Recovery" .

Para efetuar login no NetApp Console, você pode usar suas credenciais do site de suporte da NetApp ou pode se inscrever para um login no NetApp Console usando seu e-mail e uma senha. "Saiba mais sobre como fazer login" .

*Função necessária do NetApp Console * Superadministrador de backup e recuperação ou função de administrador de restauração de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Para adicionar um agente do Console, você precisa ter a função de superadministrador do Backup and Recovery.

Passos

1. Abra um navegador da web e vá para o "NetApp Console" .

   A página de login do NetApp Console é exibida.

2. Efetue login no Console.
3. Na navegação à esquerda do Console, selecione **Proteção** > **Backup e Recuperação**.
   - Se esta for a sua primeira vez a iniciar sessão no Backup and Recovery e ainda não tiver adicionado um sistema à página **Sistemas**, o Backup and Recovery apresenta a página inicial "Bem-vindo ao novo NetApp Backup and Recovery" com uma opção para adicionar um sistema. Para obter detalhes sobre como adicionar um sistema à página **Sistemas**, consulte "Introdução ao modo padrão do NetApp Console".
   - Se você estiver acessando o Backup and Recovery pela primeira vez e tiver um sistema no Console, mas nenhum recurso descoberto, a página *Bem-vindo ao novo NetApp Backup and Recovery* será exibida com uma opção para **Descobrir recursos**.
4. Se você ainda não fez isso, selecione a opção **Descobrir e gerenciar**.
   - Para cargas de trabalho do Microsoft SQL Server, consulte"Descubra as cargas de trabalho do Microsoft SQL Server" .
   - Para cargas de trabalho VMware, consulte"Descubra as cargas de trabalho da VMware" .
   - Para cargas de trabalho KVM, consulte"Descubra cargas de trabalho KVM" .
   - Para cargas de trabalho do Oracle Database, consulte "Descubra cargas de trabalho do Oracle Database".
   - Para cargas de trabalho do Hyper-V, consulte"Descubra as cargas de trabalho do Hyper-V" .
   - Para cargas de trabalho do Kubernetes, consulte"Descubra as cargas de trabalho do Kubernetes" .

Descubra alvos de backup externos no NetApp Backup and Recovery

Conclua algumas etapas para descobrir ou adicionar manualmente destinos de backup externos no NetApp Backup and Recovery.

Descubra um alvo de backup

Configure seus destinos de backup (Amazon Web Services (AWS) S3, Microsoft Azure Blob Storage, Google Cloud Storage ou StorageGRID) antes de usar o NetApp Backup and Recovery.

Você pode descobrir esses alvos automaticamente ou adicioná-los manualmente.

Forneça credenciais para acessar a conta de armazenamento. O NetApp Backup and Recovery usa essas credenciais para descobrir as cargas de trabalho das quais você deseja fazer backup.

Antes de começar

Você precisa descobrir pelo menos uma carga de trabalho antes de poder adicionar um destino de backup externo.

Passos

1. No menu NetApp Backup and Recovery , selecione **Inventário**.
2. Selecione a aba **Destinos de backup externo**.
3. Selecione **Descobrir destino de backup**.
4. Selecione um dos tipos de destino de backup: **Amazon Web Services (AWS) S3**, **Microsoft Azure Blob Storage**, * StorageGRID* ou * ONTAP S3*.
5. Na seção **Escolher local das credenciais**, escolha o local onde as credenciais residem e, em seguida, escolha como associá-las.
6. Selecione **Avançar**.
7. Insira as informações de credenciais. As informações variam dependendo do tipo de destino de backup selecionado e do local das credenciais escolhido.
   - Para AWS:
     - **Nome da credencial**: insira o nome da credencial da AWS.
     - **Chave de acesso**: Digite o segredo da AWS.
     - **Chave secreta**: Insira a chave secreta da AWS.
   - Para o Azure:
     - **Nome da credencial**: insira o nome da credencial do Armazenamento de Blobs do Azure.
     - **Segredo do cliente**: insira o segredo do cliente do Armazenamento de Blobs do Azure.
     - **ID do aplicativo (cliente)**: selecione o ID do aplicativo do Armazenamento de Blobs do Azure.
     - **ID do locatário do diretório**: insira o ID do locatário do Armazenamento de Blobs do Azure.
   - Para StorageGRID:
     - **Nome da credencial**: insira o nome da credencial do StorageGRID .
     - **FQDN do nó de gateway**: insira um nome de FQDN para StorageGRID.

- **Porta**: Insira o número da porta para StorageGRID.
- **Chave de acesso**: Insira a chave de acesso do StorageGRID S3.
- **Chave secreta**: Insira a chave secreta do StorageGRID S3.

◦ Para ONTAP S3:

- **Nome da credencial**: insira o nome da credencial do ONTAP S3.
- **FQDN do nó do gateway**: insira um nome FQDN para o ONTAP S3.
- **Porta**: Digite o número da porta para o ONTAP S3.
- **Chave de acesso**: Digite a chave de acesso do ONTAP S3.
- **Chave secreta**: Digite a chave secreta do ONTAP S3.

8. Selecione **Descobrir**.

Adicionar um bucket para um destino de backup

Em vez de o NetApp Backup and Recovery descobrir buckets automaticamente, você pode adicionar manualmente um bucket a um destino de backup externo.

Passos

1. No menu NetApp Backup and Recovery , selecione **Inventário**.
2. Selecione **Destinos de backup externos**.
3. Selecione o alvo e à direita, selecione **Ações*** ••• **ícone e selecione *Adicionar bucket**.
4. Insira as informações do bucket. As informações variam dependendo do tipo de destino de backup selecionado.

◦ Para AWS:

- **Nome do bucket**: insira o nome do bucket S3. O prefixo "netapp-backup" é um prefixo obrigatório e é adicionado automaticamente ao nome fornecido.
- **Conta AWS**: Insira o nome da conta AWS.
- **Região do bucket**: insira a região da AWS para o bucket.
- **Habilitar bloqueio de objeto S3**: selecione esta opção para habilitar o bloqueio de objeto S3 para o bucket. O S3 Object Lock impede que objetos sejam excluídos ou substituídos por um período de retenção especificado, fornecendo uma camada adicional de proteção de dados. Você pode habilitar isso somente quando estiver criando um bucket e não poderá desativá-lo mais tarde.
  - **Modo de governança**: selecione esta opção para habilitar o modo de governança para o bucket de bloqueio de objeto do S3. O modo de governança permite que você proteja objetos de serem excluídos ou substituídos pela maioria dos usuários, mas permite que certos usuários alterem as configurações de retenção.
  - **Modo de conformidade**: selecione esta opção para habilitar o modo de conformidade para o bucket de bloqueio de objeto do S3. O modo de conformidade impede que qualquer usuário, incluindo o usuário root, altere as configurações de retenção ou exclua objetos até que o período de retenção expire.
- **Controle de versão**: selecione esta opção para habilitar o controle de versão para o bucket S3. O controle de versão permite que você mantenha várias versões de objetos no bucket, o que pode ser útil para fins de backup e recuperação.
- **Tags**: Selecione tags para o bucket S3. Tags são pares de chave-valor que podem ser usados para organizar e gerenciar seus recursos do S3.

- **Criptografia**: Selecione o tipo de criptografia para o bucket S3. As opções são chaves gerenciadas pelo AWS S3 ou chaves do AWS Key Management Service. Se você selecionar chaves do AWS Key Management Service, deverá fornecer o ID da chave.

◦ Para o Azure:

- **Assinatura**: Selecione o nome do contêiner do Azure Blob Storage.
- **Grupo de recursos**: selecione o nome do grupo de recursos do Azure.
- **Detalhes da instância**:
  - **Nome da conta de armazenamento**: insira o nome do contêiner do Armazenamento de Blobs do Azure.
  - **Região do Azure**: insira a região do Azure para o contêiner.
  - **Tipo de desempenho**: selecione o tipo de desempenho padrão ou premium para o contêiner do Azure Blob Storage, indicando o nível de desempenho necessário.
  - **Criptografia**: Selecione o tipo de criptografia para o contêiner do Azure Blob Storage. As opções são chaves gerenciadas pela Microsoft ou chaves gerenciadas pelo cliente. Se você selecionar chaves gerenciadas pelo cliente, deverá fornecer o nome do cofre de chaves e o nome da chave.

◦ Para StorageGRID:

- **Nome do destino do backup**: Selecione o nome do bucket do StorageGRID .
- **Nome do bucket**: insira o nome do bucket do StorageGRID .
- **Região**: insira a região StorageGRID para o bucket.
- **Habilitar controle de versão**: selecione esta opção para habilitar o controle de versão para o bucket StorageGRID . O controle de versão permite que você mantenha várias versões de objetos no bucket, o que pode ser útil para fins de backup e recuperação.
- **Bloqueio de objeto**: selecione esta opção para habilitar o bloqueio de objeto para o bucket StorageGRID . O bloqueio de objetos impede que objetos sejam excluídos ou substituídos por um período de retenção especificado, fornecendo uma camada adicional de proteção de dados. Você pode habilitar isso somente quando estiver criando um bucket e não poderá desativá-lo mais tarde.
- **Capacidade**: insira a capacidade do bucket StorageGRID . Esta é a quantidade máxima de dados que podem ser armazenados no bucket.

◦ Para ONTAP S3:

- **Nome do destino do backup**: Selecione o nome do bucket ONTAP S3.
- **Nome de destino do bucket**: insira o nome do bucket ONTAP S3.
- **Capacidade**: insira a capacidade do bucket ONTAP S3. Esta é a quantidade máxima de dados que podem ser armazenados no bucket.
- **Habilitar controle de versão**: selecione esta opção para habilitar o controle de versão para o bucket ONTAP S3. O controle de versão permite que você mantenha várias versões de objetos no bucket, o que pode ser útil para fins de backup e recuperação.
- **Bloqueio de objeto**: selecione esta opção para habilitar o bloqueio de objeto para o bucket ONTAP S3. O bloqueio de objetos impede que objetos sejam excluídos ou substituídos por um período de retenção especificado, fornecendo uma camada adicional de proteção de dados. Você pode habilitar isso somente quando estiver criando um bucket e não poderá desativá-lo mais tarde.

5. Selecione **Adicionar**.

Alterar credenciais para um destino de backup

Insira as credenciais necessárias para acessar o destino de backup.

Passos

1. No menu NetApp Backup and Recovery , selecione **Inventário**.
2. Selecione **Destinos de backup externos**.
3. Selecione o alvo e à direita, selecione **Ações*** ••• **ícone e selecione *Alterar credenciais**.
4. Insira as novas credenciais para o destino de backup. As informações variam dependendo do tipo de destino de backup selecionado.
5. Selecione **Concluído**.

Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery

Você pode alternar entre as diferentes cargas de trabalho do NetApp Backup and Recovery .

Mudar para uma carga de trabalho diferente

Você pode alternar para uma carga de trabalho diferente na interface do usuário do NetApp Backup and Recovery .

Passos

1. Na navegação à esquerda do Console, selecione **Proteção** > **Backup e Recuperação**.
2. No canto superior direito da página, selecione a lista suspensa **Alternar carga de trabalho**.
3. Selecione a carga de trabalho para a qual você deseja alternar.

   A página é atualizada e mostra a carga de trabalho selecionada.

Configurar as configurações de NetApp Backup and Recovery

Depois de configurar o NetApp Console, defina as configurações de backup e recuperação. Adicione credenciais para recursos de host, importe recursos do SnapCenter , configure diretórios de log e defina configurações do VMware vCenter. Conclua estas etapas antes de fazer backup ou recuperar dados.

- Adicionar credenciais para recursos do host para quaisquer hosts Windows, Microsoft SQL Server, Oracle Database ou Linux com os quais o NetApp Backup and Recovery precise se autenticar. Isso inclui as credenciais do sistema operacional convidado Windows usadas ao restaurar arquivos ou pastas do sistema convidado.
- Manter as configurações do VMware vCenter.
- Importar e gerenciar recursos do host SnapCenter. (Somente cargas de trabalho do Microsoft SQL Server)
- Adicione uma plataforma de gerenciamento KVM. (Apenas cargas de trabalho KVM)

- Configurar diretórios de log em instantâneos para hosts Windows.
- Crie um modelo de gancho de execução para executar scripts antes e depois dos trabalhos de backup. (Apenas cargas de trabalho do Kubernetes)

*Função necessária do NetApp Console * Superadministrador de backup e recuperação, administrador de backup de backup e recuperação, administrador de restauração de backup e recuperação. Aprenda sobre"Funções e privilégios de backup e recuperação" . "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Adicionar credenciais para recursos do host

Adicione credenciais para recursos do host. O NetApp Backup and Recovery usa essas credenciais para descobrir cargas de trabalho e aplicar políticas de backup.

Se você não tiver credenciais, crie-as com permissões para acessar e gerenciar cargas de trabalho do host.

Você precisa configurar os seguintes tipos de credenciais:

- Credenciais do Microsoft SQL Server
- Credenciais do host do SnapCenter Windows
- Credenciais do sistema operacional convidado Windows usadas ao restaurar arquivos ou pastas do sistema operacional convidado.
- Credenciais do banco de dados Oracle
- credenciais do host Linux

Passos

1. No menu NetApp Backup and Recovery , selecione **Configurações**.
2. Selecione a seta para baixo para **Credenciais**.
3. Selecione **Adicionar novas credenciais**.
4. Insira as informações de credenciais. Os campos exibidos variam dependendo do modo de autenticação selecionado. Passe o cursor sobre o ícone de Informação **i** para obter mais informações sobre os campos.
    - **Nome das credenciais**: Insira um nome para as credenciais.
    - **Modo de autenticação**: Selecione **Windows**, **Microsoft SQL**, **Banco de Dados Oracle** ou **Linux**.

Para cargas de trabalho do Microsoft SQL Server, você precisa inserir credenciais tanto para o Windows quanto para o Microsoft SQL Server, portanto, será necessário adicionar dois conjuntos de credenciais.

Windows

i. Se você selecionou **Windows**:

- **Agentes**: Selecione um agente do Console na lista.
- **Domínio e nome de usuário**: insira o NetBIOS ou o FQDN do domínio e o nome de usuário para as credenciais.
- **Senha**: Digite a senha para as credenciais.

Servidor Microsoft SQL

i. Se você selecionou **Microsoft SQL Server**:

- **Domínio e nome de usuário**: insira o NetBIOS ou o FQDN do domínio e o nome de usuário para as credenciais.
- **Senha**: Digite a senha para as credenciais.
- **Hosts**: Selecione um endereço de host do SQL Server já descoberto.
- **Instância do SQL Server**: Selecione uma instância do SQL Server descoberta.

Banco de Dados Oracle

i. Se você selecionou **Banco de Dados Oracle**:

- **Agentes**: Selecione um agente do Console na lista.
- **Nome de usuário**: Digite o nome de usuário para as credenciais.
- **Senha**: Digite a senha para as credenciais.

Linux

i. Se você selecionou **Linux**:

- **Agentes**: Selecione um agente do Console na lista.
- **Nome de usuário**: Digite o nome de usuário para as credenciais.
- **Senha**: Digite a senha para as credenciais.

5. Selecione **Adicionar**.

Editar credenciais para recursos do host

Você poderá editar posteriormente a senha de quaisquer credenciais que tenha criado.

Passos

1. No menu NetApp Backup and Recovery , selecione **Configurações**.
2. Selecione a seta para baixo para expandir a seção **Credenciais**.
3. Selecione o ícone Ações ••• > **Editar credenciais**.
   - **Senha**: Digite a senha para as credenciais.
4. Selecione **Salvar**.

Manter as configurações do VMware vCenter

Forneça credenciais do VMware vCenter para descobrir cargas de trabalho para backup. Se você não tiver

credenciais, crie-as com permissões para acessar e gerenciar as cargas de trabalho do VMware vCenter Server.

Passos

1. No menu NetApp Backup and Recovery , selecione **Configurações**.
2. Selecione a seta para baixo para expandir a seção **VMware vCenter**.
3. Selecione **Adicionar vCenter**.
4. Insira as informações do VMware vCenter Server.
   - **FQDN ou endereço IP do vCenter**: insira um nome FQDN ou o endereço IP do VMware vCenter Server.
   - **Nome de usuário** e **Senha**: Digite o nome de usuário e a senha do VMware vCenter Server.
   - **Porta**: Digite o número da porta para o VMware vCenter Server.
   - **Protocolo**: Selecione **HTTP** ou **HTTPS**.
5. Selecione **Adicionar**.

Importar e gerenciar recursos do host SnapCenter

Se você usou anteriormente o SnapCenter para fazer backup de seus recursos, poderá importar e gerenciar esses recursos no NetApp Backup and Recovery. Esta opção permite importar informações do servidor SnapCenter para registrar vários servidores SnapCenter e descobrir cargas de trabalho do banco de dados.

Este é um processo de duas partes:

- Importar recursos do aplicativo e do host do SnapCenter Server
- Gerenciar recursos selecionados do host SnapCenter

Importar recursos do aplicativo e do host do SnapCenter Server

Esta primeira etapa importa recursos de host do SnapCenter e exibe esses recursos na página Inventário de NetApp Backup and Recovery . Nesse ponto, os recursos ainda não são gerenciados pelo NetApp Backup and Recovery.

Após importar os recursos do host do SnapCenter , o NetApp Backup and Recovery não assume o gerenciamento de proteção. Para fazer isso, você deve selecionar explicitamente gerenciar esses recursos no NetApp Backup and Recovery.

Passos

1. No menu NetApp Backup and Recovery , selecione **Configurações**.
2. Selecione a seta para baixo para expandir a seção **Importar do SnapCenter**.
3. Selecione **Importar do SnapCenter** para importar os recursos do SnapCenter .
4. Insira * Credenciais do aplicativo SnapCenter *:
   a. * FQDN ou endereço IP do SnapCenter *: insira o FQDN ou endereço IP do próprio aplicativo SnapCenter .
   b. **Porta**: insira o número da porta para o SnapCenter Server.
   c. **Nome de usuário** e **Senha**: Digite o nome de usuário e a senha do SnapCenter Server.
   d. **Agente de console**: Selecione o agente de console para o SnapCenter.

5. Insira * Credenciais do host do servidor SnapCenter *:
   a. **Credenciais existentes**: Se você selecionar esta opção, poderá usar as credenciais existentes que você já adicionou. Digite o nome das credenciais.
   b. **Adicionar novas credenciais**: Se você não tiver credenciais de host do SnapCenter existentes, poderá adicionar novas credenciais. Digite o nome das credenciais, o modo de autenticação, o nome de usuário e a senha.
6. Selecione **Importar** para validar suas entradas e registrar o SnapCenter Server.

> Se o SnapCenter Server já estiver registrado, você poderá atualizar os detalhes de registro existentes.

Resultado

A página Inventário mostra os recursos importados do SnapCenter .

Gerenciar recursos do host SnapCenter

Depois de importar os recursos do SnapCenter , gerencie esses recursos de host no NetApp Backup and Recovery. Depois de selecionar o gerenciamento desses recursos importados, o NetApp Backup and Recovery pode fazer backup e recuperar os recursos que você está importando do SnapCenter. Você não precisa mais gerenciar esses recursos no SnapCenter Server.

Passos

1. Depois de importar os recursos do SnapCenter , na página Inventário exibida, selecione os recursos do SnapCenter que você importou e que deseja que o NetApp Backup and Recovery gerencie a partir de agora.
2. Selecione o ícone Ações ••• > **Gerenciar** para gerenciar os recursos.
3. Selecione **Gerenciar no NetApp Console**.

   A página Inventário mostra **Gerenciado** sob o nome do host para indicar que os recursos do host selecionados agora são gerenciados pelo NetApp Backup and Recovery.

Editar recursos importados do SnapCenter

Mais tarde, você pode reimportar os recursos do SnapCenter ou editar os recursos importados do SnapCenter para atualizar os detalhes de registro.

Você pode alterar apenas os detalhes da porta e da senha do SnapCenter Server.

Passos

1. No menu NetApp Backup and Recovery , selecione **Configurações**.
2. Selecione a seta para baixo para **Importar do SnapCenter**.

   A página Importar do SnapCenter mostra todas as importações anteriores.

3. Selecione o ícone Ações ••• > **Editar** para atualizar os recursos.
4. Atualize a senha e os detalhes da porta do SnapCenter , conforme necessário.
5. Selecione **Importar**.

Adicione uma plataforma de gerenciamento KVM

Se você utiliza a plataforma de gerenciamento Apache CloudStack para gerenciar recursos KVM, é necessário integrá-la ao NetApp Backup and Recovery para que este possa detectar e proteger os hosts KVM e as VMs gerenciadas.

Passos

1. No menu NetApp Backup and Recovery , selecione **Configurações**.
2. Selecione a seta para baixo para expandir a seção **Plataforma de gerenciamento**.
3. Selecione **Adicionar credencial da plataforma de gerenciamento**.
4. Insira as seguintes informações:
   - **Endereço IP ou FQDN da plataforma de gerenciamento**: Insira o endereço IP ou o nome de domínio totalmente qualificado da plataforma de gerenciamento.
   - **Chave de API**: Insira a chave de API a ser usada para autenticar as solicitações de API.
   - **Chave secreta**: Insira a chave secreta a ser usada para autenticar as solicitações da API.
   - **Porta**: Insira a porta a ser usada para comunicação entre o Backup e Recuperação e a plataforma de gerenciamento.
   - **Agentes**: Selecione um agente de console para facilitar a comunicação entre o Backup e Recuperação e a plataforma de gerenciamento.
5. Ao terminar, selecione **Adicionar**.

Configurar diretórios de log em instantâneos para hosts Windows

Antes de criar políticas para hosts Windows, você deve configurar diretórios de log em instantâneos para hosts Windows. Os diretórios de log são usados para armazenar os logs gerados durante o processo de backup.

Passos

1. No menu NetApp Backup and Recovery , selecione **Inventário**.
2. Na página Inventário, selecione uma carga de trabalho e, em seguida, selecione o ícone Ações ••• > **Ver detalhes** para exibir os detalhes da carga de trabalho.
3. Na página Detalhes do inventário que mostra o Microsoft SQL Server, selecione a guia Hosts.
4. Na página de detalhes do inventário, selecione um host e selecione o ícone Ações ••• > **Configurar diretório de log**.
5. Navegue ou insira o caminho para o diretório de log.
6. Selecione **Salvar**.

Crie um modelo de gancho de execução

Você pode criar um modelo de gancho de execução personalizado que pode ser usado para executar ações antes ou depois de uma operação de proteção de dados em um aplicativo.

Os modelos que você cria aqui só podem ser usados ao proteger cargas de trabalho do Kubernetes.

Passos

1. No Console, vá para **Proteção** > **Backup e recuperação**.
2. Selecione a aba **Configurações**.
3. Expanda a seção **Modelo de gancho de execução**.
4. Selecione **Criar modelo de gancho de execução**.
5. Digite um nome para o gancho de execução.
6. Opcionalmente, escolha um tipo de gancho. Por exemplo, um gancho pós-restauração é executado após a conclusão da operação de restauração.
7. Na caixa de texto **Script**, insira o script de shell executável que você deseja executar como parte do modelo de gancho de execução. Opcionalmente, você pode selecionar **Carregar script** para carregar um arquivo de script.
8. Selecione **Criar**.

   Depois de criar o modelo, ele aparece na lista de modelos na seção **Modelo de gancho de execução**.

Configurar controle de acesso baseado em funções no NetApp Backup e Restauração

Para aumentar a segurança e controlar o acesso aos recursos, configure o controle de acesso baseado em funções para NetApp Backup e Recovery. O NetApp Console oferece suporte ao controle de acesso baseado em funções (RBAC) para algumas cargas de trabalho de backup e restauração. Você pode atribuir funções administrativas ou de visualizador específicas para essas cargas de trabalho. Outras cargas de trabalho que ainda não oferecem suporte ao controle de acesso baseado em funções permanecem acessíveis a todos os usuários com funções de backup e restauração até que a associação em nível de projeto seja suportada.

Siga estes passos para controlar o acesso aos recursos da sua organização. Faça as alterações na página **Administração > Identidade e acesso** no menu NetApp Console.

Esses passos pressupõem que você tenha a função Organization Admin atribuída no Console.

Passos

1. Crie a estrutura do projeto de identidade e acesso.

   Como administrador da organização, configure a pasta Identidade e acesso e a estrutura de projetos onde as cargas de trabalho residirão.

2. Atribuir funções de usuário.
   a. Opção principal:

      Adicione usuários a cada projeto designado para cargas de trabalho e atribua a eles a função apropriada. Por exemplo:

      - **Administrador da organização** e **Backup and Recovery super admin**: Um usuário com essas funções pode visualizar todos os recursos em todas as organizações, e descobrir Backup and Recovery workloads e atribuí-los a projetos (por exemplo, US East ou US West).

- **Administrador de pasta ou projeto** e **Backup and Recovery super admin**: Um usuário com essas funções pode ver apenas os recursos na pasta ou projeto para o qual possui permissões, mas pode descobrir Backup and Recovery workloads e atribuí-las a esse projeto.

b. Opção alternativa:

   Em vez de conceder a um usuário acesso administrativo completo ao Backup and Recovery, você pode atribuir a si mesmo a função de superadministrador de Backup and Recovery e descobrir as workloads diretamente.

3. Descubra cargas de trabalho em Backup and Recovery.

   Os administradores da organização ou administradores de pasta ou projeto descobrem as cargas de trabalho disponíveis e selecionam o projeto apropriado (como US East ou US West). Cada carga de trabalho é automaticamente associada ao projeto selecionado.

4. Adicionar usuários aos projetos.

   Os administradores da organização ou os administradores de pastas/projetos adicionam usuários do Console a projetos com cargas de trabalho. Atribua aos usuários a função de visualizador da organização e uma função de Backup and Recovery com base em suas necessidades de acesso. Os usuários com a função de Backup and Recovery adequada obterão acesso automaticamente a novas cargas de trabalho nesses projetos.

Informações relacionadas

- "Saiba mais sobre o gerenciamento de identidade e acesso do NetApp Console".
- "Funções de NetApp Backup and Recovery no NetApp Console".

Informações sobre direitos autorais

Informações sobre marcas comerciais