Referência

NetApp Backup and Recovery

NetApp
February 10, 2026

Índice

Referência

Políticas no SnapCenter comparadas com aquelas no NetApp Backup and Recovery

Há algumas diferenças entre as políticas usadas no SnapCenter e aquelas usadas no NetApp Backup and Recovery que podem afetar o que você vê após importar recursos e políticas do SnapCenter.

Níveis de programação

O SnapCenter usa os seguintes níveis de agendamento:

- **Por hora**: Várias horas e minutos com quaisquer horas (0-23) e quaisquer minutos (0-60).
- **Diariamente**: Opção de repetir a cada número definido de dias, por exemplo, a cada 3 dias.
- **Semanal**: de domingo a segunda-feira, com a opção de realizar um snapshot no primeiro dia da semana ou em vários dias da semana.
- **Mensal**: de janeiro a dezembro, com opção de apresentação em dias específicos ou em vários dias de cada mês, por exemplo, no dia 7.

O NetApp Backup and Recovery usa os seguintes níveis de agendamento, que são ligeiramente diferentes:

- **Por hora**: executa instantâneos somente em intervalos de 15 minutos, por exemplo, intervalos de 1 hora ou 15 minutos menores que 60.
- **Diariamente**: Horas do dia (0-23) com horário de início, por exemplo, às 10:00, com opção de execução a cada tantas horas.
- **Semanal**: Dia da semana (domingo a segunda-feira) com opção de apresentação em 1 dia ou em vários dias. Isso é o mesmo que o SnapCenter.
- **Mensal**: Datas do mês (0-30) com hora de início em várias datas do mês.
- **Anual**: Mensal. Isso corresponde ao mensal do SnapCenter.

Várias políticas no SnapCenter com o mesmo nível de agendamento

Você pode atribuir várias políticas com o mesmo nível de agendamento a um recurso no SnapCenter. No entanto, o NetApp Backup and Recovery não oferece suporte a várias políticas em um recurso que usa a mesma camada de agendamento.

Exemplo: Se você usar três políticas (para Dados, Log e Log de snapshots) no SnapCenter, após a migração do SnapCenter, o NetApp Backup and Recovery usará uma única política em vez de todas as três.

Agendas diárias importadas do SnapCenter

O NetApp Backup and Recovery ajusta os agendamentos do SnapCenter da seguinte forma:

- Se o agendamento do SnapCenter for definido como menor ou igual a 7 dias, o NetApp Backup and Recovery definirá o agendamento como semanal. Alguns instantâneos são pulados durante a semana.

  Exemplo: Se você tiver uma política diária do SnapCenter com um intervalo de repetição de 3 dias a partir

de segunda-feira, o NetApp Backup and Recovery definirá o agendamento para semanalmente às segundas, quintas e domingos. Alguns dias serão pulados porque não são exatamente a cada 3 dias.

- Se o agendamento do SnapCenter for definido para mais de 7 dias, o NetApp Backup and Recovery definirá o agendamento como mensal. Alguns instantâneos serão ignorados durante o mês.

  Exemplo: Se você tiver uma política diária do SnapCenter com um intervalo de repetição de 10 dias a partir do dia 2 do mês, o NetApp Backup and Recovery, após a migração, definirá o agendamento como mensal nos dias 2, 12 e 22 do mês. O NetApp Backup and Recovery pulará alguns dias no mês seguinte.

Cronogramas horários importados do SnapCenter

As políticas horárias do SnapCenter com intervalos de repetição maiores que uma hora são convertidas em uma política diária no NetApp Backup and Recovery.

Qualquer política horária com intervalos repetidos que não sejam um fator de 24 (por exemplo, 5, 7, etc.) pulará alguns instantâneos em um dia.

Exemplo: Se você tiver uma política horária do SnapCenter com um intervalo de repetição a cada 5 horas, começando à 1h, o NetApp Backup and Recovery (após a migração) definirá a programação como diária com intervalos de 5 horas à 1h, 6h, 11h, 16h e 21h. Algumas horas serão ignoradas, depois das 21:00 deve ser 2:00 da manhã para repetir a cada 5 horas, mas será sempre 1:00 da manhã.

Retenção de logs de políticas do SnapCenter

Se você tiver um recurso no SnapCenter com várias políticas, o NetApp Backup and Recovery usará a seguinte ordem de prioridade para atribuir o valor de retenção de log:

- Para "Backup completo com política de backup de log" mais políticas "somente log" no SnapCenter, o NetApp Backup and Recovery usa o valor de retenção da política somente log.
- Para as políticas "Backup completo somente com log" e "Completo e log" no SnapCenter, o NetApp Backup and Recovery usa o valor de retenção somente log.
- Para "Backup completo e log" mais "Backup completo" no SnapCenter, o NetApp Backup and Recovery usa o valor de retenção "Backup completo e log".
- Se você tiver apenas um backup completo no SnapCenter, o NetApp Backup and Recovery não habilitará o backup de log.

Retenção de backup de log

O SnapCenter oferece suporte a vários valores de retenção para políticas em um recurso. O NetApp Backup and Recovery suporta apenas um valor de retenção por recurso.

Contagem de retenção de políticas do SnapCenter

Se você tiver um recurso com proteção secundária habilitada no SnapCenter com vários volumes de origem, vários volumes de destino e vários relacionamentos SnapMirror , o NetApp Backup and Recovery usará apenas a contagem de retenção da primeira política.

Exemplo: Se você tiver uma política do SnapCenter com uma contagem de retenção de 5 e outra política com uma contagem de retenção de 10, o NetApp Backup and Recovery usará a contagem de retenção de 5.

Rótulos SnapMirror de políticas SnapCenter

O SnapCenter mantém os rótulos do SnapMirror para cada política após a migração, mesmo que o nível seja alterado.

Exemplo: Uma política horária do SnapCenter pode mudar para diária no NetApp Backup and Recovery. No entanto, os rótulos do SnapMirror permanecem os mesmos após a migração.

Funções de gerenciamento de identidade e acesso (IAM) do NetApp Backup and Recovery

O NetApp Backup and Recovery emprega o Identity and Access Management (IAM) para controlar o acesso que cada usuário tem a recursos e ações específicos.

Para saber mais sobre as funções do IAM específicas do NetApp Backup and Recovery, consulte "Funções de NetApp Backup and Recovery no NetApp Console" .

Restaurar dados de configuração do NetApp Backup and Recovery em um site escuro

Ao usar o NetApp Backup and Recovery em um site sem acesso à Internet, conhecido como *modo privado*, os dados de configuração do NetApp Backup and Recovery são copiados para o bucket StorageGRID ou ONTAP S3 onde seus backups estão sendo armazenados. Se você tiver um problema com o sistema host do agente do Console, poderá implantar um novo agente do Console e restaurar os dados críticos do NetApp Backup and Recovery .

Este procedimento se aplica somente aos dados de volume ONTAP .

Quando você usa o NetApp Backup and Recovery em um ambiente SaaS com o agente do Console implantado no seu provedor de nuvem ou no seu próprio host conectado à Internet, o sistema faz backup e protege todos os dados de configuração importantes na nuvem. Se você tiver um problema com o agente do Console, crie um novo agente do Console e adicione seus sistemas. Os detalhes do backup são restaurados automaticamente.

Existem dois tipos de dados que são copiados:

- Banco de dados de NetApp Backup and Recovery - contém uma listagem de todos os volumes, arquivos de backup, políticas de backup e informações de configuração.
- Arquivos de catálogo indexados - contêm índices detalhados usados para a funcionalidade de pesquisa e restauração, tornando suas pesquisas muito rápidas e eficientes ao procurar dados de volume que você deseja restaurar.

É feito backup desses dados uma vez por dia à meia-noite, e no máximo 7 cópias de cada arquivo são retidas. Se o agente do Console estiver gerenciando vários sistemas ONTAP locais, os arquivos de NetApp Backup and Recovery serão armazenados no bucket do sistema que foi ativado primeiro.

Nenhum dado de volume é incluído no banco de dados do NetApp Backup and Recovery ou nos arquivos do Catálogo Indexado.

Restaurar dados de NetApp Backup and Recovery para um novo agente do Console

Se o seu agente do Console local parar de funcionar, você precisará instalar um novo agente do Console e restaurar os dados do NetApp Backup and Recovery para o novo agente do Console.

Você precisará executar as seguintes tarefas para retornar seu sistema NetApp Backup and Recovery a um estado de funcionamento:

- Instalar um novo agente do Console
- Restaurar o banco de dados de NetApp Backup and Recovery
- Restaurar os arquivos do catálogo indexado
- Redescubra todos os seus sistemas ONTAP locais e sistemas StorageGRID na interface de usuário do NetApp Console

Depois de verificar se o sistema está funcionando, crie novos arquivos de backup.

O que você vai precisar

Você precisará acessar os backups de banco de dados e índice mais recentes do bucket StorageGRID ou ONTAP S3 onde seus arquivos de backup estão sendo armazenados:

- Arquivo de banco de dados MySQL do NetApp Backup and Recovery

  Este arquivo está localizado no seguinte local no bucket `netapp-backup-<GUID>/mysql_backup/` , e é chamado `CBS_DB_Backup_<day>_<month>_<year>.sql` .

- Arquivo zip de backup do catálogo indexado

  Este arquivo está localizado no seguinte local no bucket `netapp-backup-<GUID>/catalog_backup/` , e é chamado `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip` .

Instalar um novo agente de console em um novo host Linux local

Ao instalar um novo agente do Console, baixe a mesma versão de software do agente original. Alterações no banco de dados do NetApp Backup and Recovery podem fazer com que versões mais recentes do software não funcionem com backups de bancos de dados antigos. Você pode "atualize o software do agente do Console para a versão mais atual após restaurar o banco de dados de backup" .

1. "Instale o agente do Console em um novo host Linux local"
2. Efetue login no Console usando as credenciais de usuário administrador que você acabou de criar.

Restaurar o banco de dados de NetApp Backup and Recovery

1. Copie o backup do MySQL do local de backup para o novo host do agente do Console. Usaremos o nome de arquivo de exemplo "CBS_DB_Backup_23_05_2023.sql" abaixo.
2. Copie o backup para o contêiner Docker do MySQL usando um dos seguintes comandos, dependendo se você estiver usando um contêiner Docker ou Podman:

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

```
podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. Entre no shell do contêiner MySQL usando um dos seguintes comandos, dependendo se você estiver usando um contêiner Docker ou Podman:

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. No shell do contêiner, implante o "env".
5. Você precisará da senha do banco de dados MySQL, então copie o valor da chave "MYSQL_ROOT_PASSWORD".
6. Restaure o banco de dados MySQL do NetApp Backup and Recovery usando o seguinte comando:

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Verifique se o NetApp Backup and Recovery MySQL DB foi restaurado corretamente usando os seguintes comandos SQL:

```
mysql -u root -p cloud_backup
```

8. Digite a senha.

```
mysql> show tables;
mysql> select * from volume;
```

9. Certifique-se de que os volumes exibidos sejam os mesmos que existiam em seu ambiente original.

Restaurar os arquivos do catálogo indexado

1. Copie o arquivo zip de backup do Catálogo Indexado (usaremos o nome de arquivo de exemplo "Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip") do local de backup para o novo host do agente do Console na pasta "/opt/application/netapp/cbs".
2. Descompacte o arquivo "Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip" usando o seguinte comando:

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. Execute o comando **ls** para garantir que a pasta "catalogdb1" foi criada com as subpastas "changes" e "snapshots" abaixo.

Descubra seus clusters ONTAP e sistemas StorageGRID

1. "Descubra todos os sistemas ONTAP on-prem"que estavam disponíveis no seu ambiente anterior. Isso inclui o sistema ONTAP que você usou como servidor S3.
2. "Descubra seus sistemas StorageGRID".

Configurar os detalhes do ambiente StorageGRID

Adicione os detalhes do sistema StorageGRID associado aos seus sistemas ONTAP conforme eles foram configurados na configuração original do agente do Console usando o "APIs do NetApp Console" .

As informações a seguir se aplicam a instalações em modo privado a partir do NetApp Console 3.9.xx. Para versões mais antigas, use o seguinte procedimento: "DarkSite Cloud Backup: backup e restauração de MySQL e catálogo indexado" .

Você precisará executar essas etapas para cada sistema que estiver fazendo backup de dados no StorageGRID.

1. Extraia o token de autorização usando a seguinte API oauth/token.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept:
application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-
Encoding: gzip, deflate' -H 'Content-Type: application/json' -d '
{"username":"admin@netapp.com","password":"Netapp@123","grant_type":"pas
sword"}
> '
```

   Embora o endereço IP, o nome de usuário e as senhas sejam valores personalizados, o nome da conta não é. O nome da conta é sempre "account-DARKSITE1". Além disso, o nome de usuário deve usar um nome no formato de e-mail.

   Esta API retornará uma resposta como a seguinte. Você pode recuperar o token de autorização conforme mostrado abaixo.

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```

2. Extraia o ID do sistema e o X-Agent-Id usando a API tenancy/external/resource.

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

Esta API retornará uma resposta como a seguinte. O valor em "resourceIdentifier" denota o *WorkingEnvironment Id* e o valor em "agentId" denota *x-agent-id*.

```
[{"resourceIdentifier":"OnPremWorkingEnvironment-
pMtZND0M","resourceType":"ON_PREM","agentId":"vB_1xShPpBtUosjD7wfBlLIhqD
gIPA0wclients","resourceClass":"ON_PREM","name":"CBSFAS8300-01-
02","metadata":"{\"clusterUuid\": \"2cb6cb4b-dc07-11ec-9114-
d039ea931e09\"}","workspaceIds":["workspace2wKYjTy9"],"agentIds":["vB_1x
ShPpBtUosjD7wfBlLIhqDgIPA0wclients"]}]
```

3. Atualize o banco de dados do NetApp Backup and Recovery com os detalhes do sistema StorageGRID associado aos sistemas. Certifique-se de inserir o Nome de Domínio Totalmente Qualificado do StorageGRID, bem como a Chave de Acesso e a Chave de Armazenamento, conforme mostrado abaixo:

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

Verifique as configurações de NetApp Backup and Recovery

1. Selecione cada sistema ONTAP e clique em **Exibir backups** ao lado do serviço de backup e recuperação no painel direito.

   Você deverá ver todos os backups criados para seus volumes.

2. No Painel de restauração, na seção Pesquisar e restaurar, clique em **Configurações de indexação**.

   Certifique-se de que os sistemas que tinham a Catalogação Indexada habilitada anteriormente permaneçam habilitados.

3. Na página Pesquisar e restaurar, execute algumas pesquisas de catálogo para confirmar se a restauração do catálogo indexado foi concluída com sucesso.

Camadas de armazenamento de arquivo AWS compatíveis com o NetApp Backup and Recovery

O NetApp Backup and Recovery oferece suporte a duas classes de armazenamento de arquivamento S3 e à maioria das regiões.

Para alternar entre as versões da interface de usuário do NetApp Backup and Recovery , consulte"Mudar para a interface de usuário anterior do NetApp Backup and Recovery" .

Classes de armazenamento de arquivamento S3 com suporte para NetApp Backup and Recovery

Quando os arquivos de backup são criados inicialmente, eles são armazenados no armazenamento S3 *Standard*. Esta camada é otimizada para armazenar dados acessados com pouca frequência; mas isso também permite que você os acesse imediatamente. Após 30 dias, os backups passam para a classe de armazenamento S3 *Standard-Infrequent Access* para economizar custos.

Se seus clusters de origem estiverem executando o ONTAP 9.10.1 ou superior, você poderá optar por dividir os backups em camadas no armazenamento *S3 Glacier* ou *S3 Glacier Deep Archive* após um determinado número de dias (normalmente mais de 30 dias) para otimizar ainda mais os custos. Você pode definir isso como "0" ou de 1 a 999 dias. Se você definir como "0" dias, não poderá alterá-lo posteriormente para 1-999 dias.

Os dados nessas camadas não podem ser acessados imediatamente quando necessário e exigirão um custo de recuperação mais alto, então você precisa considerar com que frequência precisará restaurar dados desses arquivos de backup arquivados. Consulte a seção nesta página sobre restauração de dados do armazenamento de arquivo.

- Se você não selecionar nenhuma camada de arquivamento em sua primeira política de backup ao ativar o NetApp Backup and Recovery, o *S3 Glacier* será sua única opção de arquivamento para políticas futuras.
- Se você selecionar *S3 Glacier* na sua primeira política de backup, poderá mudar para a camada *S3 Glacier Deep Archive* para futuras políticas de backup para esse cluster.
- Se você selecionar *S3 Glacier Deep Archive* na sua primeira política de backup, essa camada será a única camada de arquivamento disponível para futuras políticas de backup para esse cluster.

Observe que, ao configurar o NetApp Backup and Recovery com esse tipo de regra de ciclo de vida, você não deve configurar nenhuma regra de ciclo de vida ao configurar o bucket na sua conta da AWS.

"Saiba mais sobre as classes de armazenamento S3".

Restaurar dados do armazenamento de arquivo

Embora armazenar arquivos de backup mais antigos em armazenamento de arquivo seja muito mais barato do que o armazenamento Standard ou Standard-IA, acessar dados de um arquivo de backup em armazenamento de arquivo para operações de restauração levará mais tempo e custará mais dinheiro.

Quanto custa restaurar dados do Amazon S3 Glacier e do Amazon S3 Glacier Deep Archive?

Há 3 prioridades de restauração que você pode escolher ao recuperar dados do Amazon S3 Glacier e 2 prioridades de restauração ao recuperar dados do Amazon S3 Glacier Deep Archive. O S3 Glacier Deep Archive custa menos que o S3 Glacier:

Camada de arquivo	Restaurar Prioridade e Custo		
	Alto	**Padrão**	**Baixo**
Geleira S3	Recuperação mais rápida, custo mais alto	Recuperação mais lenta, menor custo	Recuperação mais lenta, menor custo
Arquivo S3 Glacier Deep		Recuperação mais rápida, custo mais alto	Recuperação mais lenta, menor custo

Cada método tem uma taxa diferente de recuperação por GB e por solicitação. Para obter preços detalhados do S3 Glacier por região da AWS, visite o "Página de preços do Amazon S3" .

Quanto tempo levará para restaurar meus objetos arquivados no Amazon S3 Glacier?

Há 2 partes que compõem o tempo total de restauração:

- **Tempo de recuperação**: O tempo para recuperar o arquivo de backup do arquivo morto e colocá-lo no armazenamento padrão. Às vezes, isso é chamado de período de "reidratação". O tempo de recuperação é diferente dependendo da prioridade de restauração escolhida.

Camada de arquivo	Restaurar prioridade e tempo de recuperação		
	Alto	**Padrão**	**Baixo**
Geleira S3	3-5 minutos	3-5 horas	5-12 horas
Arquivo S3 Glacier Deep		12 horas	48 horas

- **Tempo de restauração**: O tempo para restaurar os dados do arquivo de backup no armazenamento padrão. Desta vez não é diferente da operação típica de restauração diretamente do armazenamento padrão, quando não se usa uma camada de arquivamento.

Para obter mais informações sobre as opções de recuperação do Amazon S3 Glacier e do S3 Glacier Deep Archive, consulte "Perguntas frequentes da Amazon sobre essas classes de armazenamento" .

Camadas de acesso ao arquivo do Azure com suporte ao NetApp Backup and Recovery

O NetApp Backup and Recovery oferece suporte a uma camada de acesso de arquivamento do Azure e à maioria das regiões.

Para alternar entre as versões da interface de usuário do NetApp Backup and Recovery , consulte"Mudar para a interface de usuário anterior do NetApp Backup and Recovery" .

Camadas de acesso do Azure Blob com suporte para NetApp Backup and Recovery

Quando os arquivos de backup são criados inicialmente, eles são armazenados na camada de acesso *Cool*. Esta camada é otimizada para armazenar dados que são acessados com pouca frequência, mas que podem ser acessados imediatamente quando necessário.

Se seus clusters de origem estiverem executando o ONTAP 9.10.1 ou superior, você poderá optar por dividir os backups em camadas do armazenamento *Cool* para o *Azure Archive* após um determinado número de dias (normalmente mais de 30 dias) para otimizar ainda mais os custos. Os dados nesta camada não podem ser acessados imediatamente quando necessário e exigirão um custo de recuperação mais alto, então você precisa considerar com que frequência pode precisar restaurar dados desses arquivos de backup arquivados. Consulte a seção nesta página sobre restauração de dados do armazenamento de arquivo.

Observe que, ao configurar o NetApp Backup and Recovery com esse tipo de regra de ciclo de vida, você não deve configurar nenhuma regra de ciclo de vida ao configurar o contêiner na sua conta do Azure.

"Saiba mais sobre as camadas de acesso do Azure Blob".

Restaurar dados do armazenamento de arquivo

Embora armazenar arquivos de backup mais antigos no armazenamento de arquivo seja muito mais barato do que no armazenamento frio, acessar dados de um arquivo de backup no Azure Archive para operações de restauração levará mais tempo e custará mais dinheiro.

Quanto custa restaurar dados do Arquivo do Azure?

Há duas prioridades de restauração que você pode escolher ao recuperar dados do Arquivo do Azure:

- **Alto**: Recuperação mais rápida, custo mais alto
- **Padrão**: Recuperação mais lenta, menor custo

Cada método tem uma taxa diferente de recuperação por GB e por solicitação. Para obter preços detalhados do Azure Archive por região do Azure, visite o "Página de preços do Azure" .

A alta prioridade não é suportada ao restaurar dados do Azure para sistemas StorageGRID .

Quanto tempo levará para restaurar meus dados arquivados no Arquivo do Azure?

Existem 2 partes que compõem o tempo de restauração:

- **Tempo de recuperação**: o tempo para recuperar o arquivo de backup arquivado do Azure Archive e colocá-lo no armazenamento frio. Às vezes, isso é chamado de período de "reidratação". O tempo de recuperação é diferente dependendo da prioridade de restauração escolhida:
  - **Alto**: < 1 hora
  - **Padrão**: < 15 horas
- **Tempo de restauração**: O tempo para restaurar os dados do arquivo de backup no armazenamento Cool. Desta vez não é diferente da operação típica de restauração diretamente do armazenamento Cool, quando não se usa uma camada de arquivamento.

Para obter mais informações sobre as opções de recuperação do Azure Archive, consulte "estas perguntas frequentes do Azure" .

Camadas de armazenamento de arquivo do Google compatíveis com o NetApp Backup and Recovery

O NetApp Backup and Recovery oferece suporte a uma classe de armazenamento de arquivamento do Google e à maioria das regiões.

Para alternar entre as versões da interface de usuário do NetApp Backup and Recovery , consulte"Mudar para a interface de usuário anterior do NetApp Backup and Recovery" .

Classes de armazenamento de arquivamento do Google com suporte para NetApp Backup and Recovery

Quando os arquivos de backup são criados inicialmente, eles são armazenados no armazenamento *Padrão*. Esta camada é otimizada para armazenar dados acessados com pouca frequência; mas isso também permite que você os acesse imediatamente.

Se o seu cluster local estiver usando o ONTAP 9.12.1 ou superior, você poderá optar por colocar backups mais antigos em camadas no armazenamento *Archive* na interface do NetApp Backup and Recovery após um determinado número de dias (normalmente mais de 30 dias) para otimizar ainda mais os custos. Os dados nessa camada exigirão um custo de recuperação mais alto, então você precisa considerar com que frequência precisará restaurar dados desses arquivos de backup arquivados. Consulte a seção nesta página sobre restauração de dados do armazenamento de arquivo.

Observe que, ao configurar o NetApp Backup and Recovery com esse tipo de regra de ciclo de vida, você não deve configurar nenhuma regra de ciclo de vida ao configurar o bucket na sua conta do Google.

"Saiba mais sobre as classes de armazenamento do Google".

Restaurar dados do armazenamento de arquivo

Embora armazenar arquivos de backup mais antigos no armazenamento de arquivo seja muito mais barato do que o armazenamento padrão, acessar dados de um arquivo de backup no armazenamento de arquivo para operações de restauração levará um pouco mais de tempo e custará mais dinheiro.

Quanto custa restaurar dados do Google Archive?

Para obter preços detalhados do Google Cloud Storage por região, visite o "Página de preços do Google Cloud Storage" .

Quanto tempo levará para restaurar meus objetos arquivados no Google Archive?

Há 2 partes que compõem o tempo total de restauração:

- **Tempo de recuperação**: O tempo para recuperar o arquivo de backup do Archive e colocá-lo no armazenamento padrão. Às vezes, isso é chamado de período de "reidratação". Ao contrário das soluções de armazenamento "mais frias" fornecidas por outros provedores de nuvem, seus dados ficam acessíveis em milissegundos.
- **Tempo de restauração**: O tempo para restaurar os dados do arquivo de backup no armazenamento padrão. Desta vez não é diferente da operação típica de restauração diretamente do armazenamento padrão, quando não se usa uma camada de arquivamento.

Informações sobre direitos autorais

Informações sobre marcas comerciais