Fornecer acesso de cliente S3 aos dados nas

ONTAP 9

NetApp
January 17, 2025

Índice

Fornecer acesso de cliente S3 aos dados nas

Suporte multiprotocolo S3 no ONTAP

A partir do ONTAP 9.12,1, é possível permitir que os clientes que executam o protocolo S3 acessem os mesmos dados que estão sendo atendidos aos clientes que usam os protocolos NFS e SMB sem reformatação. Esse recurso permite que os dados nas continuem sendo servidos a clientes nas, enquanto apresentam dados de objetos a clientes S3 que executam aplicações S3 (como data mining e inteligência artificial).

A funcionalidade multiprotocolo S3 aborda dois casos de uso:

1. Acesso a dados nas existentes usando clientes S3

   Se os dados existentes tiverem sido criados usando clientes nas tradicionais (NFS ou SMB) e estiverem localizados em volumes nas (volumes FlexVol ou FlexGroup), agora você poderá usar ferramentas de análise em clientes do S3 para acessar esses dados.

2. Storage de back-end para clientes modernos com capacidade para executar e/S usando protocolos nas e S3

   Agora você pode fornecer acesso integrado para aplicativos como Spark e Kafka que podem ler e gravar os mesmos dados usando protocolos nas e S3.

Como funciona o suporte multiprotocolo S3

O suporte multiprotocolo ONTAP permite que você apresente o mesmo conjunto de dados que uma hierarquia de arquivos ou objetos em um bucket. Para fazer isso, o ONTAP cria "S3 buckets nas" que permitem que os clientes do S3 criem, leiam, excluam e enumerem arquivos no storage nas usando solicitações de objetos do S3. Este mapeamento está em conformidade com a configuração de segurança nas, observando permissões de acesso a arquivos e diretórios, bem como gravar na trilha de auditoria de segurança, conforme necessário.

Esse mapeamento é realizado apresentando uma hierarquia de diretórios nas especificada como um bucket S3. Cada arquivo na hierarquia de diretórios é representado como um objeto S3 cujo nome é relativo do diretório mapeado para baixo, com limites de diretório representados pelo caractere de barra ('/').

Os usuários do S3 definidos pela ONTAP podem acessar esse storage, conforme governado pelas políticas de bucket definidas para o bucket que é mapeado para o diretório nas. Para que isso seja possível, mapeamentos devem ser definidos entre os usuários S3 e os usuários SMB/NFS. As credenciais do usuário SMB/NFS serão usadas para a verificação de permissões nas e incluídas em todos os Registros de auditoria resultantes desses acessos.

Quando criado por clientes SMB ou NFS, um arquivo é colocado imediatamente em um diretório e, portanto, visível para clientes, antes que qualquer dado seja gravado nele. Os clientes S3 esperam semântica diferente, na qual o novo objeto não é visível no namespace até que todos os seus dados tenham sido escritos. Esse mapeamento do S3 para o armazenamento nas cria arquivos usando semântica S3, mantendo os arquivos invisíveis externamente até que o comando de criação S3 seja concluído.

Proteção de dados para buckets do nas S3

S3 "buckets" nas são simplesmente mapeamentos de dados nas para clientes S3, e não são buckets do S3

padrão. Portanto, não há necessidade de proteger buckets do nas S3 usando a funcionalidade do NetApp SnapMirror S3. Em vez disso, você pode proteger volumes que contêm S3 buckets do nas usando a replicação de volume assíncrona do SnapMirror. A recuperação de desastres síncrona SnapMirror e SVM não é compatível.

A partir do ONTAP 9.14,1, os buckets nas de S3 GB são compatíveis com agregados espelhados e sem espelhamento para configurações MetroCluster IP e FC.

Saiba mais "Assíncrono com SnapMirror"sobre .

Auditoria para buckets do nas S3

Como os buckets do nas S3 não são buckets do S3 convencionais, a auditoria do S3 não pode ser configurada para auditar o acesso neles. Saiba mais "Auditoria S3"sobre o .

No entanto, os arquivos e diretórios nas mapeados em buckets do nas S3 podem ser auditados para eventos de acesso usando procedimentos de auditoria convencionais do ONTAP. As operações S3 podem, portanto, acionar eventos de auditoria nas, com as seguintes exceções:

- Se o acesso de cliente S3 for negado pela configuração de diretiva S3 (política de grupo ou bucket), a auditoria nas para o evento não será iniciada. Isso ocorre porque as permissões do S3 são verificadas antes que as verificações de auditoria SVM possam ser feitas.
- Se o arquivo de destino de uma solicitação de S3 GET for de tamanho 0, o conteúdo 0 será retornado à solicitação de GET e o acesso de leitura não será registrado.
- Se o arquivo de destino de uma solicitação de S3 GET estiver em uma pasta para a qual o usuário não tenha permissão de avanço, a tentativa de acesso falhará e o evento não será registrado.

Saiba mais "Auditoria de eventos nas em SVMs"sobre .

Upload multipart de objeto

A partir do ONTAP 9.16,1, o upload de várias partes de objetos é suportado quando "balanceamento de capacidade avançado" o FlexGroup volumes está ativado.

O upload multipart de objeto no armazenamento de arquivos nas permite que um cliente de protocolo S3 carregue um objeto grande como partes menores. O upload de várias partes do objeto tem os seguintes benefícios:

- Ele permite que objetos sejam carregados em paralelo.
- Em caso de falha ou pausa no upload, apenas as partes que ainda não foram carregadas precisarão ser carregadas. O upload de todo o objeto não precisa ser reiniciado.
- Se o tamanho do objeto não for conhecido antecipadamente (por exemplo, quando um objeto grande ainda está sendo escrito), os clientes podem começar a carregar partes do objeto imediatamente e concluir o upload após o objeto inteiro ter sido criado.

O upload multipart suporta as seguintes ações S3:

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- ListMultipartUpload

Interoperabilidade do S3 e nas

Os buckets do ONTAP S3 nas suportam a funcionalidade nas e S3 padrão, exceto conforme listado aqui.

Funcionalidade nas atualmente não suportada por buckets do nas S3

Camada de capacidade do FabricPool

Os buckets do nas S3 não podem ser configurados como uma camada de capacidade para o FabricPool.

S3 ações e funcionalidade não compatíveis atualmente com buckets do nas S3

Ações

- ByPassGovernanceRetention
- CopyObject
- GetBucketObjectLockConfiguration
- GetBucketControle de versão
- GetObjectRetention
- PutBucketControle de versão
- PutObjectLockConfiguration
- Retenção PutObjectRetention
- ListBucketControle de versão
- ListObjectVersions

Essas S3 ações não são especificamente suportadas ao usar o S3 em buckets do nas S3. Ao usar buckets nativos do S3, essas ações são "suportado como normal".

Metadados de usuários da AWS

- Os pares de valores-chave recebidos como parte dos metadados de usuário do S3 não são armazenados no disco juntamente com os dados de objeto na versão atual.
- Cabeçalhos de solicitação com o prefixo "x-amz-meta" são ignorados.

Tags da AWS

- Em pedidos PUT object e Multipart Initiate, cabeçalhos com o prefixo "x-amz-tagging" são ignorados.
- As solicitações para atualizar tags em um arquivo existente (ou seja, um put, get e Delete Requests com a string de consulta ?tagging) são rejeitadas com um erro.

Controle de versão

Não é possível especificar o controle de versão na configuração de mapeamento de bucket.

- Solicitações que incluem especificações de versão não null (a query-string) recebem respostas de erro.
- As solicitações para afetar o estado de controle de versão de um bucket são rejeitadas com erros.

Requisitos de dados nas para acesso ao cliente S3

É importante entender que existem algumas incompatibilidades inerentes ao mapeamento de arquivos e diretórios nas para acesso S3. Pode ser necessário ajustar

hierarquias de arquivos nas antes de servi-los usando buckets do nas S3.

Um bucket do S3 nas fornece acesso S3 a um diretório nas mapeando esse diretório usando a sintaxe do bucket do S3, e os arquivos na árvore de diretórios são vistos como objetos. Os nomes de objeto são os nomes de caminho delimitados por barra dos arquivos em relação ao diretório especificado na configuração de bucket S3.

Esse mapeamento impõe alguns requisitos quando arquivos e diretórios são servidos usando buckets do nas S3:

- Os nomes S3 são limitados a 1024 bytes, portanto os arquivos com pathnames mais longos não são acessíveis usando S3.
- Os nomes de arquivo e diretório estão limitados a 255 carateres, portanto, um nome de objeto não pode ter mais de 255 carateres consecutivos sem barra ('/')
- Um nome de caminho SMB delimitado por carateres de barra invertida ('") aparecerá em S3 como um nome de objeto contendo carateres de barra direta ('/') em vez disso.
- Alguns pares de nomes de objetos S3 legais não podem coexistir na árvore de diretórios nas mapeada. Por exemplo, os nomes de objetos S3 legais "part1/part2" e "part1/part2/part3" mapeiam para arquivos que não podem existir simultaneamente na árvore de diretórios nas, pois "part1/part2" é um arquivo no primeiro nome e um diretório no outro.
  - Se "part1/part2" for um arquivo existente, uma criação S3 de "part1/part2/part3" falhará.
  - Se "part1/part2/part3" for um arquivo existente, uma criação ou exclusão S3 de "part1/part2" falhará.
  - Uma criação de objeto S3 que corresponde ao nome de um objeto existente substitui o objeto pré-existente (em buckets não versionados); que se mantém no nas, mas requer uma correspondência exata. Os exemplos acima não causarão a remoção do objeto existente porque enquanto os nomes colidem, eles não coincidem.

Embora um armazenamento de objetos seja projetado para suportar um número muito grande de nomes arbitrários, uma estrutura de diretório nas pode experimentar problemas de desempenho se um número muito grande de nomes for colocado em um diretório. Em particular, nomes sem carateres de barra ('/') serão todos colocados no diretório raiz do mapeamento nas. As aplicações que fazem uso extensivo de nomes que não são "amigáveis ao nas" seriam mais bem hospedadas em um bucket de armazenamento de objetos real em vez de um mapeamento nas.

Habilite o acesso de protocolo S3 a dados nas

A habilitação do acesso ao protocolo S3 consiste em garantir que um SVM habilitado para nas atenda aos mesmos requisitos que um servidor habilitado para S3, incluindo a adição de um servidor de armazenamento de objetos e a verificação dos requisitos de rede e autenticação.

Para novas instalações do ONTAP, é recomendável habilitar o acesso de protocolo S3 a um SVM depois de configurá-lo para fornecer dados nas aos clientes. Para saber mais sobre a configuração do protocolo nas, consulte:

- "Configuração NFS"
- "Configuração SMB"

Antes de começar

É necessário configurar o seguinte antes de ativar o protocolo S3:

- O protocolo S3 e os protocolos nas desejados - NFS, SMB ou ambos - são licenciados.
- Um SVM é configurado para os protocolos nas desejados.
- Existem servidores NFS e/ou SMB.
- DNS e quaisquer outros serviços necessários estão configurados.
- Os dados nas estão sendo exportados ou compartilhados para sistemas cliente.

Sobre esta tarefa

Um certificado de autoridade de certificação (CA) é necessário para habilitar o tráfego HTTPS de clientes S3 para o SVM habilitado para S3. Os certificados CA de três fontes podem ser usados:

- Um novo certificado auto-assinado da ONTAP no SVM.
- Certificado auto-assinado existente do ONTAP no SVM.
- Um certificado de terceiros.

Você pode usar os mesmos LIFs de dados para o bucket do S3/nas que você usa para fornecer dados nas. Se forem necessários endereços IP específicos, "Crie LIFs de dados"consulte . Uma política de dados de serviço do S3 é necessária para habilitar o tráfego de dados do S3 nos LIFs. Você pode modificar a política de serviços existente da SVM para incluir o S3.

Quando você cria o servidor de objetos S3, você deve estar preparado para inserir o nome do servidor S3 como um nome de domínio totalmente qualificado (FQDN), que os clientes usarão para o acesso S3. O FQDN do servidor S3 não deve começar com um nome de bucket.

System Manager

1. Habilite o S3 em uma VM de storage com protocolos nas configurados.
   a. Clique em **armazenamento > armazenamento VMs**, selecione uma VM de armazenamento pronta para nas, clique em Configurações e, em seguida, clique em S3.
   b. Selecione o tipo de certificado. Se você selecionar um certificado gerado pelo sistema ou um de seu, ele será necessário para acesso ao cliente.
   c. Introduza as interfaces de rede.
2. Se você selecionou o certificado gerado pelo sistema, as informações do certificado serão exibidas quando a nova criação da VM de armazenamento for confirmada. Clique em **Download** e salve-o para acesso ao cliente.
   - A chave secreta não será exibida novamente.
   - Se você precisar das informações do certificado novamente: Clique em **armazenamento > armazenamento de VMs**, selecione a VM de armazenamento e clique em **Configurações**.

CLI

1. Verifique se o protocolo S3 é permitido no SVM `vserver show -fields allowed-protocols`
2. Registre o certificado de chave pública deste SVM. Se for necessário um novo certificado auto-assinado do ONTAP, "Crie e instale um certificado de CA no SVM"consulte .
3. Atualize a política de dados de serviço
   a. Exibir a política de dados de serviço do SVM `network interface service-policy show -vserver svm_name`
   b. Adicione o `data-core` e `data-s3-server services` se não estiverem presentes. E `network interface service-policy add-service -vserver svm_name -policy policy_name -service data-core,data-s3-server`
4. Verifique se as LIFs de dados no SVM atendem aos seus requisitos `network interface show -vserver svm_name`
5. Crie o servidor S3 `vserver object-store-server create -vserver svm_name -object -store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

Você pode especificar opções adicionais ao criar o servidor S3 ou a qualquer momento mais tarde.

- O HTTPS é ativado por padrão na porta 443. Você pode alterar o número da porta com a opção -secure-listener-port. Quando o HTTPS está ativado, os certificados de CA são necessários para uma integração adequada com SSL/TLS. A partir do ONTAP 9.15,1, o TLS 1,3 é compatível com armazenamento de objetos S3.
- O HTTP está desativado por padrão; quando ativado, o servidor escuta na porta 80. Você pode ativá-lo com a opção -is-http-enabled ou alterar o número da porta com a opção -listener-port. Quando o HTTP está ativado, todas as solicitações e respostas são enviadas pela rede em texto não criptografado.
  1. Verifique se S3 está configurado como desejado `vserver object-store-server show`

O seguinte comando verifica os valores de configuração de todos os servidores de armazenamento de objetos `cluster1::> vserver object-store-server show`

```
Vserver: vs1

                        Object Store Server Name: s3.example.com
                            Administrative State: up
                          Listener Port For HTTP: 80
                  Secure Listener Port For HTTPS: 443
                                    HTTP Enabled: false
                                   HTTPS Enabled: true
              Certificate for HTTPS Connections: svm1_ca
                                         Comment: Server comment
```

Crie um bucket do nas S3

Um buckets do nas S3 é um mapeamento entre um nome de bucket do S3 e um caminho nas. Os buckets nas do S3 permitem que você forneça acesso S3 a qualquer parte do namespace SVM com volumes e estrutura de diretórios existentes.

Antes de começar

- Um servidor de objetos S3 é configurado em uma SVM que contém dados nas.
- Os dados nas estão em conformidade com a "Requisitos para acesso ao cliente S3".

Sobre esta tarefa

Você pode configurar buckets do S3 nas para especificar qualquer conjunto de arquivos e diretórios no diretório raiz do SVM.

Você também pode definir políticas de bucket que permitem ou não permitem o acesso aos dados do nas com base em qualquer combinação desses parâmetros:

- Arquivos e diretórios
- Permissões de usuário e grupo
- S3 operações

Por exemplo, você pode querer políticas de bucket separadas que concedem acesso somente leitura a um grande grupo de usuários e outra que permita que um grupo limitado execute operações em um subconjunto desses dados.

Como os "buckets" do nas S3 são mapeamentos e não buckets do S3, as seguintes propriedades dos buckets do S3 padrão não se aplicam aos buckets do nas S3.

- * aggr-list-multiplicador / storage-Service-level / volume / exclude-aggr-list / qos-policy-group * não são criados volumes ou qtree ao configurar buckets do S3 nas.
- **A função é -protegida/está -protegida/está -protegida-na-ONTAP** mais de S3 buckets nas não são protegidos ou espelhados usando o SnapMirror S3, mas em vez disso estarão usando a proteção SnapMirror regular disponível na granularidade do volume.
- **Os volumes nas de estado de versionamento** geralmente têm a tecnologia Snapshot disponível para salvar versões diferentes. No entanto, o controle de versão não está disponível atualmente em buckets do

nas S3.

- *As estatísticas equivalentes usadas em lógica estão disponíveis para volumes nas através dos comandos de volume.

System Manager

Adicione um novo bucket do S3 nas em uma VM de storage habilitada para nas.

1. Clique em **armazenamento > baldes** e, em seguida, clique em **Adicionar**.
2. Insira um nome para o bucket do nas S3 e selecione a VM de armazenamento, não insira um tamanho e clique em **mais Opções**.
3. Introduza um nome de caminho válido ou clique em Procurar para selecionar a partir de uma lista de nomes de caminho válidos. Quando você insere um pathname válido, as opções que não são relevantes para a configuração do nas S3 são ocultadas.
4. Se você já mapeou usuários do S3 para usuários do nas e grupos criados, você pode configurar suas permissões e clique em **Salvar**. Você já deve ter mapeado S3 usuários para usuários nas antes de configurar permissões nesta etapa.

Caso contrário, clique em **Save** para concluir a configuração do bucket do nas do S3.

CLI

Crie um bucket do nas S3 em um SVM que contenha sistemas de arquivos nas. E `vserver object-store-server bucket create -vserver` *`svm_name`* `-bucket` *`bucket_name`* `-type nas -nas-path` *`junction_path`* `[-comment` *`text`*`]`

Exemplo `cluster1::> vserver object-store-server bucket create -bucket testbucket -type nas -path /vol1`

Ative S3 usuários de cliente

Para permitir que os usuários de cliente S3 acessem dados nas, você deve mapear nomes de usuário S3 para os usuários nas correspondentes e conceder permissão para acessar os dados nas usando políticas de serviço de bucket.

Antes de começar

Os nomes de usuário para acesso ao cliente – usuários clientes LINUX/UNIX, Windows e S3 – já devem existir.

Você deve estar ciente de que alguma funcionalidade do S3 é "Não compatível com buckets do nas S3".

Sobre esta tarefa

Mapear um nome de usuário S3 para um USUÁRIO LINUX/UNIX ou Windows correspondente permite que verificações de autorização nos arquivos nas sejam honradas quando esses arquivos são acessados por clientes S3. Os mapeamentos S3 para nas são especificados fornecendo um nome de usuário S3 *pattern*, que pode ser expresso como um único nome ou uma expressão regular POSIX, e um nome de usuário LINUX/UNIX ou Windows *Replacement*.

Caso não haja nenhum mapeamento de nomes presente, será usado o mapeamento de nomes padrão, onde o próprio nome de usuário S3 será usado como o nome de usuário UNIX e o nome de usuário do Windows. Você pode modificar os mapeamentos de nome de usuário padrão UNIX e Windows com o `vserver`

`object-store-server modify` comando.

Apenas a configuração de mapeamento de nomes local é suportada; o LDAP não é suportado.

Depois que os usuários do S3 são mapeados para usuários nas, você pode conceder permissões aos usuários especificando os recursos (diretórios e arquivos) aos quais eles têm acesso e as ações que eles têm permissão ou não podem executar lá.

System Manager

1. Crie mapeamentos de nomes locais para clientes UNIX ou Windows (ou ambos).
   a. Clique em **Storage > Buckets** (armazenamento > baldes*) e selecione a VM de armazenamento habilitada para S3/nas.
   b. Selecione **Configurações** e clique → em **Mapeamento de nomes** (em **usuários e grupos de hosts**).
   c. Nos blocos **S3 para Windows** ou **S3 para UNIX** (ou ambos), clique em **Add** e, em seguida, insira os nomes de usuário **Pattern** (S3) e **Replacement** (nas) desejados.
2. Crie uma política de bucket para fornecer acesso ao cliente.
   a. Clique em **armazenamento > baldes**, clique ⋮ em junto ao balde S3 pretendido e, em seguida, clique em **Editar**.
   b. Clique em **Add** e forneça os valores desejados.
      - **Principal** - forneça S3 nomes de usuário ou use o padrão (todos os usuários).
      - **Efeito** - Selecione **permitir** ou **Negar**.
      - **Ações** - Digite as ações para esses usuários e recursos. O conjunto de operações de recursos que o servidor de armazenamento de objetos suporta atualmente para buckets do nas S3 são: GetObject, PutObject, DeletObject, ListBucketAcl, GetObjectTagging, PutObjectTagging, DeletObjectTagging, GetBucketLocation, GetBucketVerketversioning, PutBucketVerketverversions e ListBucketsions. Wildcards são aceitos para este parâmetro.
      - **Resources** - Insira caminhos de pasta ou arquivo nos quais as ações são permitidas ou negadas, ou use os padrões (diretório raiz do bucket).

CLI

1. Crie mapeamentos de nomes locais para clientes UNIX ou Windows (ou ambos). E `vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position` *`integer`* `-pattern` *`s3_user_name`* `-replacement` *`nas_user_name`*
   - `-position` - número de prioridade para a avaliação do mapeamento; introduza 1 ou 2.
   - `-pattern` - Um nome de usuário S3 ou uma expressão regular
   - `-replacement` - um nome de usuário do windows ou unix

Exemplos `vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1 -replacement win_user_1 vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1 -replacement unix_user_1`

1. Crie uma política de bucket para fornecer acesso ao cliente. E `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]`
   - `-effect {deny|allow}` - especifica se o acesso é permitido ou negado quando um usuário solicita uma ação.
   - `-action <Action>, …` - especifica operações de recursos que são permitidas ou negadas. O conjunto de operações de recursos que o servidor de armazenamento de objetos suporta atualmente para buckets do nas S3 são: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl e GetBucketLocation. Wildcards são aceitos para este parâmetro.

- `-principal <Objectstore Principal>, …` - valida o usuário que solicita acesso aos usuários ou grupos de servidores de armazenamento de objetos especificados neste parâmetro.
  - Um grupo de servidores de armazenamento de objetos é especificado adicionando um grupo de prefixo/ ao nome do grupo.
  - `-principal` - (o caractere hífen) concede acesso a todos os usuários.
- `-resource <text>, …` - especifica o bucket, pasta ou objeto para o qual permissões de permissão/negação são definidas. Wildcards são aceitos para este parâmetro.
- `[-sid <SID>]` - especifica um comentário de texto opcional para a declaração de política de bucket do servidor de armazenamento de objetos.

Exemplos
```
cluster1::> vserver object-store-server bucket policy add-statement
-bucket testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

Informações sobre direitos autorais

Informações sobre marcas comerciais