Criar ou modificar instruções de política de acesso

ONTAP 9

NetApp
January 17, 2025

Índice

Criar ou modificar instruções de política de acesso

Saiba mais sobre as políticas de servidor de armazenamento de objetos e bucket do ONTAP S3

O acesso de usuário e grupo a recursos do S3 é controlado por políticas de servidor de armazenamento de objetos e bucket. Se você tem um pequeno número de usuários ou grupos, controlar o acesso no nível do bucket provavelmente é suficiente, mas se você tiver muitos usuários e grupos, é mais fácil controlar o acesso no nível do servidor do armazenamento de objetos.

Adicione regras de acesso à política de bucket do ONTAP S3 padrão

Você pode adicionar regras de acesso à política de bucket padrão. O escopo de seu controle de acesso é o balde contendo, portanto, é mais apropriado quando há um único balde.

Antes de começar

Uma VM de armazenamento habilitada para S3 contendo um servidor S3 e um bucket já deve existir.

Você já deve ter criado usuários ou grupos antes de conceder permissões.

Sobre esta tarefa

Você pode adicionar novas instruções para novos usuários e grupos ou modificar os atributos de instruções existentes. Para obter mais opções, consulte as `vserver object-store-server bucket policy` páginas de manual.

Permissões de usuário e grupo podem ser concedidas quando o bucket é criado ou conforme necessário mais tarde. Você também pode modificar a capacidade do bucket e a atribuição do grupo de políticas de QoS.

A partir do ONTAP 9.9,1, se você planeja oferecer suporte à funcionalidade de marcação de objetos cliente AWS com o servidor ONTAP S3, as ações `GetObjectTagging` `PutObjectTagging` e `DeleteObjectTagging` precisam ser permitidas usando o bucket ou as políticas de grupo.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Passos

1. Edite o bucket: Clique em **Storage > Buckets**, clique no bucket desejado e clique em **Edit**. Ao adicionar ou modificar permissões, você pode especificar os seguintes parâmetros:
   - **Principal**: O usuário ou grupo a quem o acesso é concedido.
   - **Efeito**: Permite ou nega o acesso a um usuário ou grupo.
   - **Ações**: Ações permitidas no intervalo para um determinado usuário ou grupo.
   - **Recursos**: Caminhos e nomes de objetos dentro do intervalo para o qual o acesso é concedido ou negado.

     Os padrões ***bucketname*** e ***bucketname/**** concedem acesso a todos os objetos no bucket. Você também pode conceder acesso a objetos únicos; por exemplo, ***bucketname/*_readme.txt**.
   - **Condições** (opcional): Expressões que são avaliadas quando o acesso é tentado. Por exemplo, você pode especificar uma lista de endereços IP para os quais o acesso será permitido ou negado.

> A partir do ONTAP 9.14,1, você pode especificar variáveis para a política de bucket no campo **Resources**. Essas variáveis são marcadores de posição que são substituídos por valores contextuais quando a política é avaliada. Por exemplo, se `${aws:username}` for especificado como uma variável para uma política, essa variável será substituída pelo nome de usuário do contexto de solicitação e a ação da política pode ser executada como configurada para esse usuário.

CLI

Passos

1. Adicione uma instrução a uma política de bucket:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

   Os seguintes parâmetros definem permissões de acesso:

`-effect`	A declaração pode permitir ou negar acesso
`-action`	Você pode especificar `*` para indicar todas as ações ou uma lista de uma ou mais das seguintes opções: `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `GetBucketAcl`,`GetObjectAcl`, `ListBucketMultipartUploads`, E `ListMultipartUploadParts`.

`-principal`	Uma lista de um ou mais S3 usuários ou grupos. • Um máximo de 10 usuários ou grupos podem ser especificados. • Se um grupo S3 for especificado, ele deverá estar no formulário `group/group_name`. • `*` pode ser especificado para significar acesso público; ou seja, acesso sem uma chave de acesso e chave secreta. • Se nenhum principal for especificado, todos os usuários do S3 na VM de armazenamento terão acesso.
`-resource`	O balde e qualquer objeto que ele contém. Os carateres curinga `*` e `?` podem ser usados para formar uma expressão regular para especificar um recurso. Para um recurso, você pode especificar variáveis em uma política. Estas são variáveis de política são marcadores de posição que são substituídos pelos valores contextuais quando a política é avaliada.

Opcionalmente, você pode especificar uma cadeia de texto como comentário com a `-sid` opção.

Exemplos

O exemplo a seguir cria uma declaração de política de bucket do servidor de armazenamento de objetos para a VM de armazenamento svm1.example.com e bucket1 que especifica o acesso permitido a uma pasta readme para o usuário do servidor de armazenamento de objetos user1.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

O exemplo a seguir cria uma declaração de política de bucket do servidor de armazenamento de objetos para a VM de armazenamento svm1.example.com e bucket1 que especifica o acesso permitido a todos os objetos para o grupo de servidores de armazenamento de objetos group1.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

A partir do ONTAP 9.14,1, você pode especificar variáveis para uma política de bucket. O exemplo a seguir cria uma declaração de política de bucket do servidor para a VM de armazenamento `svm1` e `bucket1` especifica `${aws:username}` como uma variável para um recurso de diretiva. Quando a política é avaliada, a variável de política é substituída pelo nome de usuário de contexto de solicitação e a ação de política pode ser executada como configurada para esse usuário. Por exemplo, quando a seguinte declaração de política é avaliada, `${aws:username}` é substituída pelo usuário que executa a operação S3. Se um usuário `user1` executar a operação, esse usuário terá acesso ao `bucket1` as `bucket1/user1/*`.

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

Criar ou modificar uma política de servidor de armazenamento de objetos ONTAP S3

Você pode criar políticas que podem ser aplicadas a um ou mais buckets em um armazenamento de objetos. As políticas de servidor de armazenamento de objetos podem ser anexadas a grupos de usuários, simplificando assim o gerenciamento do acesso a recursos em vários buckets.

Antes de começar

Um SVM habilitado para S3 que contenha um servidor S3 e um bucket já deve existir.

Sobre esta tarefa

É possível habilitar políticas de acesso no nível SVM especificando uma política padrão ou personalizada em um grupo de servidores de storage de objetos. As políticas não entram em vigor até que sejam especificadas na definição de grupo.

> Quando você usa políticas de servidor de armazenamento de objetos, você especifica princípios (ou seja, usuários e grupos) na definição de grupo, não na própria política.

Há três políticas padrão somente leitura para acesso aos recursos do ONTAP S3:

- FullAccess
- NoS3Access
- ReadOnlyAccess

Você também pode criar novas políticas personalizadas, adicionar novas instruções para novos usuários e grupos ou modificar os atributos de instruções existentes. Saiba mais sobre `vserver object-store-server policy` o "Referência do comando ONTAP"na .

A partir do ONTAP 9.9,1, se você planeja oferecer suporte à funcionalidade de marcação de objetos cliente AWS com o servidor ONTAP S3, as ações `GetObjectTagging` `PutObjectTagging` e `DeleteObjectTagging` precisam ser permitidas usando o bucket ou as políticas de grupo.

O procedimento a seguir depende da interface que você usa—System Manager ou CLI:

System Manager

Use o System Manager para criar ou modificar uma política de servidor de armazenamento de objetos

Passos

1. Edite a VM de armazenamento: Clique em **armazenamento > VMs de armazenamento**, clique na VM de armazenamento, clique em **Configurações** e, em seguida, clique em S3.
2. Adicionar um usuário: Clique em **políticas** e, em seguida, clique em **Adicionar**.
   a. Introduza um nome de política e selecione a partir de uma lista de grupos.
   b. Selecione uma política padrão existente ou adicione uma nova.

      Ao adicionar ou modificar uma política de grupo, você pode especificar os seguintes parâmetros:

      - Grupo: Os grupos a quem o acesso é concedido.
      - Efeito: Permite ou nega o acesso a um ou mais grupos.
      - Ações: Ações permitidas em um ou mais buckets para um determinado grupo.
      - Recursos: Caminhos e nomes de objetos dentro de um ou mais buckets para os quais o acesso é concedido ou negado. Por exemplo:
        - * Concede acesso a todos os buckets na VM de armazenamento.
        - **bucketname** e **bucketname/*** concedem acesso a todos os objetos em um bucket específico.
        - **bucketname/readme.txt** concede acesso a um objeto em um intervalo específico.
   c. Se desejar, adicione instruções às políticas existentes.

CLI

Use a CLI para criar ou modificar uma política de servidor de armazenamento de objetos

Passos

1. Criar uma política de servidor de armazenamento de objetos:

   ```
   vserver object-store-server policy create -vserver svm_name -policy
   policy_name [-comment text]
   ```

2. Crie uma declaração para a política:

   ```
   vserver object-store-server policy statement create -vserver svm_name
   -policy policy_name -effect {allow|deny} -action object_store_actions
   -resource object_store_resources [-sid text]
   ```

   Os seguintes parâmetros definem permissões de acesso:

`-effect`	A declaração pode permitir ou negar acesso

`-action`	Você pode especificar `*` para indicar todas as ações ou uma lista de uma ou mais das seguintes opções: `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`,`GetBucketAcl`, `GetObjectAcl`, `ListAllMyBuckets`, `ListBucketMultipartUploads`, E `ListMultipartUploadParts`.
`-resource`	O balde e qualquer objeto que ele contém. Os carateres curinga `*` e `?` podem ser usados para formar uma expressão regular para especificar um recurso.

Opcionalmente, você pode especificar uma cadeia de texto como comentário com a `-sid` opção.

Por padrão, novas instruções são adicionadas ao final da lista de instruções, que são processadas em ordem. Quando você adiciona ou modifica instruções mais tarde, você tem a opção de modificar a configuração da instrução `-index` para alterar a ordem de processamento.

Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Configurar serviços de diretório externo para acesso ao ONTAP S3

A partir do ONTAP 9.14,1, os serviços para diretórios externos foram integrados ao armazenamento de objetos ONTAP S3. Essa integração simplifica o gerenciamento de usuários e acessos por meio de serviços de diretório externos.

Você pode fornecer grupos de usuários pertencentes a um serviço de diretório externo com acesso ao ambiente de storage de objetos do ONTAP. O LDAP (Lightweight Directory Access Protocol) é uma interface para comunicação com serviços de diretório, como o ative Directory, que fornece um banco de dados e serviços para gerenciamento de identidade e acesso (IAM). Para fornecer acesso, é necessário configurar grupos LDAP no ambiente do ONTAP S3. Depois de configurar o acesso, os membros do grupo têm permissões para buckets do ONTAP S3. Para obter informações sobre LDAP, "Visão geral do uso do LDAP"consulte .

Você também pode configurar grupos de usuários do ative Directory para o modo de vinculação rápida, para que as credenciais de usuário possam ser validadas e aplicativos S3 de terceiros e de código aberto possam ser autenticados por conexões LDAP.

Antes de começar

Antes de configurar grupos LDAP e ativar o modo de ligação rápida para acesso a grupos, certifique-se de que o seguinte é:

1. Uma VM de armazenamento habilitada para S3 contendo um servidor S3 foi criada. "Criar um SVM para S3"Consulte .
2. Um bucket foi criado nessa VM de storage. "Crie um bucket"Consulte .

3. O DNS está configurado na VM de armazenamento. "Configurar serviços DNS"Consulte .
4. Um certificado de autoridade de certificação raiz (CA) autoassinado do servidor LDAP é instalado na VM de armazenamento. "Instale o certificado de CA raiz autoassinado no SVM"Consulte .
5. Um cliente LDAP é configurado com TLS habilitado no SVM. "Crie uma configuração de cliente LDAP"Consulte e "Associe a configuração do cliente LDAP a SVMs para obter informações".

Configurar o acesso S3 para serviços de diretório externo

1. Especifique LDAP como o banco de dados *name Service* do SVM para o grupo e a senha para LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/vserver-services-name-service-ns-switch-modify.html[`vserver services name-service ns-switch modify` em referência de comando ONTAP.

2. Crie uma declaração de política de bucket do armazenamento de objetos com o `principal` conjunto para o grupo LDAP ao qual você deseja conceder acesso:

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

Exemplo: O exemplo a seguir cria uma declaração de política de bucket para `buck1`. A política permite o acesso do grupo LDAP `group1` ao recurso (bucket e seus objetos `buck1`) .

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. Verifique se um usuário do grupo LDAP `group1` é capaz de executar operações S3 do cliente S3.

Use o modo LDAP fast bind para autenticação

1. Especifique LDAP como o banco de dados *name Service* do SVM para o grupo e a senha para LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/vserver-services-name-service-ns-switch-modify.html[`vserver services name-service ns-switch modify` em referência de comando ONTAP.

2. Certifique-se de que um usuário LDAP acessando o bucket do S3 tenha permissões definidas nas políticas de bucket. Para obter mais informações, "Modificar uma política de bucket"consulte .
3. Verifique se um usuário do grupo LDAP pode executar as seguintes operações:
   a. Configure a chave de acesso no cliente S3 neste formato: `"NTAPFASTBIND" + base64-encode(user-name:password)` Exemplo `"NTAPFASTBIND"`: base64-encode(ldapuser:password), o que resulta em `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`

      O cliente S3 pode pedir uma chave secreta. Na ausência de uma chave secreta, qualquer senha de pelo menos 16 carateres pode ser inserida.

   b. Execute operações S3 básicas do cliente S3 para o qual o usuário tem permissões.

Autenticação de recursos para o ative Directory para usuários sem UID e GID

Se o nasgroup especificado na declaração bucket-policy ou os usuários que fazem parte do nasgroup não tiverem UID e GID definidos, as pesquisas falharão quando esses atributos não forem encontrados.

Para evitar falhas de pesquisa, o NetApp recomenda o uso de domínios confiáveis para autorização de recursos no formato UPN: Nasgroup/group@trusted_domain.com

Para gerar as chaves de acesso do usuário para usuários de domínio confiáveis quando o LDAP fast bind não é usado

Use o `s3/services/<svm_uuid>/users` endpoint com usuários especificados no formato UPN. Exemplo:

```
$curl -siku FQDN\\user:<user_name> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user[@fqdn](https://github.com/fqdn)>,"<key_time_to_live>":"PT6H3M
"}'
```

Habilite os usuários LDAP ou de domínio para gerar suas próprias chaves de acesso ONTAP S3

A partir do ONTAP 9.14,1, como administrador do ONTAP, você pode criar funções personalizadas e concedê-las a grupos locais ou de domínio ou a grupos LDAP

(Lightweight Directory Access Protocol), de modo que os usuários pertencentes a esses grupos possam gerar seu próprio acesso e chaves secretas para acesso ao cliente S3.

Você precisa executar algumas etapas de configuração em sua VM de armazenamento, para que a função personalizada possa ser criada e atribuída ao usuário que invoca a API para geração de chaves de acesso.

Antes de começar

Certifique-se de que:

1. Uma VM de armazenamento habilitada para S3 contendo um servidor S3 foi criada. "Criar um SVM para S3"Consulte .
2. Um bucket foi criado nessa VM de storage. "Crie um bucket"Consulte .
3. O DNS está configurado na VM de armazenamento. "Configurar serviços DNS"Consulte .
4. Um certificado de autoridade de certificação raiz (CA) autoassinado do servidor LDAP é instalado na VM de armazenamento. "Instale o certificado de CA raiz autoassinado no SVM"Consulte .
5. Um cliente LDAP é configurado com TLS ativado na VM de armazenamento. "Crie uma configuração de cliente LDAP"Consulte .
6. Associe a configuração do cliente ao SVM. "Associe a configuração do cliente LDAP a SVMs"Consulte . Saiba mais sobre `vserver services name-service ldap create` o "Referência do comando ONTAP"na .
7. Se você estiver usando uma VM de armazenamento de dados, crie uma interface de rede de gerenciamento (LIF) e na VM e também uma política de serviço para o LIF. Saiba mais sobre os[`network interface create`[`network interface service-policy create` comandos em ONTAP.

Configurar usuários para geração de chaves de acesso

1. Especifique LDAP como o banco de dados *name Service* da VM de armazenamento para o grupo e a senha para LDAP:

   ```
   ns-switch modify -vserver <vserver-name> -database group -sources
   files,ldap
   ns-switch modify -vserver <vserver-name> -database passwd -sources
   files,ldap
   ```

   Saiba mais sobre `vserver services name-service ns-switch modify` o "Referência do comando ONTAP"na .

2. Criar uma função personalizada com acesso ao endpoint da API REST do usuário S3: `security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>` Neste exemplo, a `s3-role` função é gerada para usuários na VM de armazenamento `svm-1` , à qual todos os direitos de acesso, leitura, criação e atualização são concedidos.

   ```
   security login rest-role create -vserver svm-1 -role s3role -api
   "/api/protocols/s3/services/*/users" -access all
   ```

Saiba mais sobre `security login rest-role create` o "Referência do comando ONTAP"na .

3. Crie um grupo de usuários LDAP com o comando de login de segurança e adicione a nova função personalizada para acessar o endpoint da API REST do usuário S3. Saiba mais sobre `security login create` o "Referência do comando ONTAP"na .

```
security login create -user-or-group-name <ldap-group-name> -application
http -authentication-method nsswitch -role <custom-role-name> -is-ns
-switch-group yes
```

Neste exemplo, o grupo LDAP `ldap-group-1` é criado no `svm-1`, e a função personalizada `s3role` é adicionada a ele para acessar o endpoint da API, juntamente com a habilitação do acesso LDAP no modo de vinculação rápida.

```
security login create -user-or-group-name ldap-group-1 -application http
-authentication-method nsswitch -role s3role -is-ns-switch-group yes
-second-authentication-method none -vserver svm-1 -is-ldap-fastbind yes
```

Para obter mais informações, "Use LDAP fast bind para autenticação nsswitch"consulte .

A adição da função personalizada ao domínio ou grupo LDAP permite aos usuários desse grupo um acesso limitado ao endpoint do ONTAP `/api/protocols/s3/services/{svm.uuid}/users`. Ao invocar a API, os usuários do domínio ou grupo LDAP podem gerar seu próprio acesso e chaves secretas para acessar o cliente S3. Eles podem gerar as chaves apenas para si mesmos e não para outros usuários.

Como um usuário S3 ou LDAP, gere suas próprias chaves de acesso

A partir do ONTAP 9.14,1, você pode gerar seu próprio acesso e chaves secretas para acessar clientes S3, se o administrador lhe concedeu a função de gerar suas próprias chaves. Você pode gerar chaves somente para si mesmo usando o seguinte endpoint da API REST do ONTAP.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir. Para obter informações sobre os outros métodos deste endpoint, consulte a "Documentação do API" referência .

Método HTTP	Caminho
POST	/api/protocols/s3/services/(svm.uuid)/users

Curl exemplo

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"_name_"}'
```

Exemplo de saída JSON

```
{
  "records": [
    {
      "access_key":
"Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
"A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "num_records": "1"
}
```

Informações sobre direitos autorais

Informações sobre marcas comerciais