



Create or modify access policy statements

ONTAP 9

NetApp
May 12, 2022

Table of Contents

- Create or modify access policy statements 1
 - About bucket and object store server policies 1
 - Modify a bucket policy 1
 - Create or modify an object store server policy 2

Create or modify access policy statements

About bucket and object store server policies

User and group access to S3 resources is controlled by bucket and object store server policies. If you have a small number of users or groups, controlling access at the bucket level is probably sufficient, but if you have many users and groups, it is easier to control access at the object store server level.

Modify a bucket policy

You can add access rules to the default bucket policy. The scope of its access control is the containing bucket, so it is most appropriate when there is a single bucket.

What you'll need

An S3-enabled SVM containing an S3 server and a bucket must already exist.

About this task

You can add new statements for new users and groups, or you can modify the attributes of existing statements. For more options, see the `vserver object-store-server bucket policy` man pages.

Steps

1. Add a statement to a bucket policy:

```
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]
```

The following parameters define access permissions:

| | |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -effect | The statement may allow or deny access |
| -action | You can specify * to mean all actions, or a list of one or more of the following: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, and ListMultipartUploadParts. |

| | |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-principal</code> | <p>A list of one or more S3 users or groups.</p> <ul style="list-style-type: none"> • A maximum of 10 users or groups can be specified. • If an S3 group is specified, it must be in the form <code>group/group_name</code>. • <code>*</code> can be specified to mean public access; that is, access without an access-key and secret-key. • If no principal is specified, all S3 users in the SVM are granted access. |
| <code>-resource</code> | <p>The bucket and any object it contains. The wildcard characters <code>*</code> and <code>?</code> can be used to form a regular expression for specifying a resource.</p> |

You can optionally specify a text string as comment with the `-sid` option.

Examples

The following example creates an object store server bucket policy statement for the SVM `svm1.example.com` and `bucket1` which specifies allowed access to a `readme` folder for object store server user `user1`.

```
cluster1::> vservers 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"
```

The following example creates an object store server bucket policy statement for the SVM `svm1.example.com` and `bucket1` which specifies allowed access to all objects for object store server group `group1`.

```
cluster1::> vservers 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"
```

Create or modify an object store server policy

You can create policies that can apply to one or more buckets in an object store. Object store server policies can be attached to groups of users, thereby simplifying the management of resource access across multiple buckets.

What you'll need

An S3-enabled SVM containing an S3 server and a bucket must already exist.

About this task

You can enable access policies at the SVM level by specifying a default or custom policy in an object storage server group. The policies do not take effect until they are specified in the group definition.



When you use object storage server policies, you specify principals (that is, users and groups) in the group definition, not in the policy itself.

There are three read-only default policies for access to ONTAP S3 resources:

- FullAccess
- NoS3Access
- ReadOnlyAccess

You can also create new custom policies, then add new statements for new users and groups, or you can modify the attributes of existing statements. For more options, see the `vserver object-store-server policy man` pages.

Steps

1. Create an object storage server policy:

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

2. Create a statement for the policy:

```
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]
```

The following parameters define access permissions:

| | |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -effect | The statement may allow or deny access |
| -action | You can specify * to mean all actions, or a list of one or more of the following: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads, and ListMultipartUploadParts. |
| -resource | The bucket and any object it contains. The wildcard characters * and ? can be used to form a regular expression for specifying a resource. |

You can optionally specify a text string as comment with the `-sid` option.

By default, new statements are added to the end of the list of statements, which are processed in order. When you add or modify statements later, you have the option to modify the statement's `-index` setting to change the processing order.

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.