



# Create or modify access policy statements

## ONTAP 9

NetApp  
July 21, 2023

# 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 ..... 3

# 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.

### Before you begin

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

You must have already created users or groups before granting permissions.

### 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.

User and group permissions can be granted when the bucket is created or as needed later. You can also modify the bucket capacity and QoS policy group assignment.

Beginning with ONTAP 9.9.1 and later releases, if you plan to support AWS client object tagging functionality with the ONTAP S3 server, the actions `GetObjectTagging`, `PutObjectTagging`, and `DeleteObjectTagging` need to be allowed using the bucket or group policies.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

## System Manager

### Steps

1. Edit the bucket: click **Storage > Buckets**, click the desired bucket, and then click **Edit**. When adding or modifying permissions, you can specify the following parameters:

- **Principal**: the user or group to whom access is granted.
- **Effect**: allows or denies access to a user or group.
- **Actions**: permissible actions in the bucket for a given user or group.
- **Resources**: paths and names of objects within the bucket for which access is granted or denied.

The defaults **bucketname** and **bucketname/\*** grant access to all objects in the bucket. You can also grant access to single objects; for example, **bucketname/\*\_readme.txt**.

- **Conditions** (optional): expressions that are evaluated when access is attempted. For example, you can specify a list of IP addresses for which access will be allowed or denied.

### CLI

#### 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.
-principal	A list of one or more S3 users or groups. <ul style="list-style-type: none"><li>• A maximum of 10 users or groups can be specified.</li><li>• If an S3 group is specified, it must be in the form group/group_name.</li><li>• * can be specified to mean public access; that is, access without an access-key and secret-key.</li><li>• If no principal is specified, all S3 users in the SVM are granted access.</li></ul>
-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.

## 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::> 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"
```

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::> 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"
```

## 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.

### Before you begin

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` [command reference](#).


Beginning with ONTAP 9.9.1 and later releases, if you plan to support AWS client object tagging functionality with the ONTAP S3 server, the actions `GetObjectTagging`, `PutObjectTagging`, and `DeleteObjectTagging` need to be allowed using the bucket or group policies.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

## System Manager

### Use System Manager to create or modify an object store server policy

#### Steps

1. Edit the storage VM: click **Storage > storage VMs**, click the storage VM, click **Settings** and then click  under S3.
2. Add a user: click **Policies**, then click **Add**.
  - a. Enter a policy name and select from a list of groups.
  - b. Select an existing default policy or add a new one.

When adding or modifying a group policy, you can specify the following parameters:

- Group: the groups to whom access is granted.
  - Effect: allows or denies access to one or more groups.
  - Actions: permissible actions in one or more buckets for a given group.
  - Resources: paths and names of objects within one or more buckets for which access is granted or denied. For example:
    - \* grants access to all buckets in the storage VM.
    - **bucketname** and **bucketname/\*** grant access to all objects in a specific bucket.
    - **bucketname/readme.txt** grants access to an object in a specific bucket.
- c. If desired, add statements to existing policies.

## CLI

### Use the CLI to create or modify an object store server policy

#### 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
---------	--

<code>-action</code>	You can specify <code>*</code> to mean all actions, or a list of one or more of the following: <code>GetObject</code> , <code>PutObject</code> , <code>DeleteObject</code> , <code>ListBucket</code> , <code>GetBucketAcl</code> , <code>GetObjectAcl</code> , <code>ListAllMyBuckets</code> , <code>ListBucketMultipartUploads</code> , and <code>ListMultipartUploadParts</code> .
<code>-resource</code>	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.

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 © 2023 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## 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.