



vserver object-store-server commands

Command reference

NetApp
July 17, 2026

Table of Contents

vserver object-store-server commands	1
vserver object-store-server create	1
Description	1
Parameters	1
Examples	2
vserver object-store-server delete	2
Description	2
Parameters	2
Examples	2
vserver object-store-server modify	3
Description	3
Parameters	3
Examples	4
vserver object-store-server show-flexcache-bucket	4
Description	4
Parameters	5
Examples	5
vserver object-store-server show	5
Description	5
Parameters	6
Examples	7
vserver object-store-server audit create	8
Description	8
Parameters	9
Examples	10
vserver object-store-server audit delete	10
Description	11
Parameters	11
Examples	11
vserver object-store-server audit disable	11
Description	11
Parameters	11
Examples	11
vserver object-store-server audit enable	11
Description	12
Parameters	12
Examples	12
vserver object-store-server audit modify	12
Description	12
Parameters	12
Examples	13
vserver object-store-server audit rotate-log	14
Description	14

Parameters	14
Examples	14
vserver object-store-server audit show	14
Description	15
Parameters	15
Examples	16
vserver object-store-server audit event-selector create	17
Description	17
Parameters	18
Examples	18
vserver object-store-server audit event-selector delete	18
Description	18
Parameters	18
Examples	19
vserver object-store-server audit event-selector modify	19
Description	19
Parameters	19
Examples	19
vserver object-store-server audit event-selector show	20
Description	20
Parameters	20
Examples	20
vserver object-store-server bucket clear-snapshot-metadata	21
Description	21
Parameters	21
Examples	21
vserver object-store-server bucket create	21
Description	22
Parameters	22
Examples	24
vserver object-store-server bucket delete	24
Description	24
Parameters	24
Examples	24
vserver object-store-server bucket evict-remote-cached-objects	25
Description	25
Parameters	25
Examples	25
vserver object-store-server bucket modify	25
Description	25
Parameters	25
Examples	26
vserver object-store-server bucket show	26
Description	27
Parameters	27

Examples	29
vserver object-store-server bucket cors-rule create	31
Description	31
Parameters	31
Examples	31
vserver object-store-server bucket cors-rule delete	32
Description	32
Parameters	32
Examples	32
vserver object-store-server bucket cors-rule show	32
Description	32
Parameters	33
Examples	34
vserver object-store-server bucket lifecycle-management-rule create	34
Description	34
Parameters	34
Examples	36
vserver object-store-server bucket lifecycle-management-rule delete	36
Description	36
Parameters	36
Examples	37
vserver object-store-server bucket lifecycle-management-rule modify	37
Description	37
Parameters	37
Examples	38
vserver object-store-server bucket lifecycle-management-rule show	38
Description	39
Parameters	39
Examples	41
vserver object-store-server bucket policy-statement-condition create	42
Description	42
Parameters	42
Examples	43
vserver object-store-server bucket policy-statement-condition delete	44
Description	44
Parameters	44
Examples	45
vserver object-store-server bucket policy-statement-condition modify	45
Description	45
Parameters	45
Examples	46
vserver object-store-server bucket policy-statement-condition show	46
Description	46
Parameters	47
Examples	48

vserver object-store-server bucket policy statement create	48
Description	48
Parameters	48
Examples	49
vserver object-store-server bucket policy statement delete	49
Description	50
Parameters	50
Examples	50
vserver object-store-server bucket policy statement modify	50
Description	50
Parameters	50
Examples	51
vserver object-store-server bucket policy statement show	52
Description	52
Parameters	52
Examples	53
vserver object-store-server bucket snapshot create	53
Description	53
Parameters	54
Examples	54
vserver object-store-server bucket snapshot delete	54
Description	54
Parameters	54
Examples	55
vserver object-store-server bucket snapshot show	55
Description	55
Parameters	55
Examples	56
vserver object-store-server bucket snapshot restore show	57
Description	57
Parameters	57
Examples	58
vserver object-store-server bucket snapshot restore start	59
Description	59
Parameters	59
Examples	59
vserver object-store-server group create	60
Description	60
Parameters	60
Examples	60
vserver object-store-server group delete	60
Description	61
Parameters	61
Examples	61
vserver object-store-server group modify	61

Description	61
Parameters	61
Examples	62
vserver object-store-server group show	62
Description	62
Parameters	62
Examples	63
vserver object-store-server policy create	63
Description	63
Parameters	63
Examples	64
vserver object-store-server policy delete	64
Description	64
Parameters	64
Examples	64
vserver object-store-server policy modify	64
Description	64
Parameters	65
Examples	65
vserver object-store-server policy show	65
Description	65
Parameters	65
Examples	66
vserver object-store-server policy statement create	66
Description	66
Parameters	66
Examples	67
vserver object-store-server policy statement delete	68
Description	68
Parameters	68
Examples	68
vserver object-store-server policy statement modify	68
Description	69
Parameters	69
Examples	69
vserver object-store-server policy statement show	70
Description	70
Parameters	70
Examples	71
vserver object-store-server user create	72
Description	72
Parameters	72
Examples	72
Related Links	73
vserver object-store-server user delete-keys	73

Description	74
Parameters	74
Examples	74
Related Links	74
vserver object-store-server user delete	74
Description	74
Parameters	74
Examples	74
vserver object-store-server user modify	75
Description	75
Parameters	75
Examples	75
vserver object-store-server user regenerate-keys	75
Description	75
Parameters	76
Examples	76
Related Links	77
vserver object-store-server user show	77
Description	77
Parameters	77
Examples	78

vserver object-store-server commands

vserver object-store-server create

Create an object store server

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server create` command creates an object store server.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver on which to create the object store server. The Vserver must already exist.

-object-store-server <Object store server name> - Object Store Server Name

This parameter specifies the name of the object store server. Note that the object-store-server name must not begin with a bucket name. For virtual hosted style (VHS) API access, you must use the same hostname as the server name configured here.

[-is-http-enabled {true|false}] - Accept Connections Over HTTP

This optional parameter specifies if server should accept HTTP connections.

[-is-https-enabled {true|false}] - Accept Connections Over HTTPS

This optional parameter specifies if server should accept HTTPS connections.

[-certificate-name <text>] - Name of Certificate Used for HTTPS Connections

Common name of the certificate used for HTTPS connections.

[-listener-port <integer>] - Object Store Server Listener Port

Use this parameter to specify the listener port for the object store server. The default port is *80* .

[-secure-listener-port <integer>] - Object Store Server Listener Port for HTTPS

Use this parameter to specify the secure listener port for the object store server. The default port is *443* .

-status-admin {down|up} - Object Store Server Administrative State

Use this parameter to specify whether the initial administrative status of the object store server is up or down. The default setting is *up* .

[-comment <text>] - Object Store Server Description

This optional parameter specifies a text comment for the object store server.

[-default-unix-user <text>] - Default UNIX User for NAS Access

This optional parameter specifies the default UNIX user for name-mapping from an S3 user to UNIX user during NAS access. The default UNIX user name is *pcuser* .

[`-default-win-user <text>`] - Default Windows User for NAS Access

This optional parameter specifies the default Windows user for name-mapping from an S3 user to Windows user during NAS access.

[`-is-ldap-fastbind-enabled {true|false}`] - Is LDAP FastBind Authentication Enabled? (privilege: advanced)

This parameter specifies whether LDAP FastBind authentication is enabled for the object store server.

[`-max-key-time-to-live {P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P[<integer>W]}`] - Maximum Value for Key TTL

Use this parameter to specify the maximum permissible value for object store user key time-to-live property.

[`-max-lock-retention-period {{<integer> days|years} | none}`] - Maximum Object Lock Retention Period

This parameter specifies the maximum value that can be specified as lock retention period for an object in an object store bucket.

[`-min-lock-retention-period {{<integer> days|years} | none}`] - Minimum Object Lock Retention Period

This parameter specifies the minimum value that can be specified as lock retention period for an object in an object store bucket.

Examples

The following example creates an object store server OSS1 for Vserver vs1.

```
cluster1::> vsserver object-store-server create -vserver vs1 -object-store
-server OSS1
```

vsserver object-store-server delete

Delete an object store server

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vsserver object-store-server delete` command deletes an object store server.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver for the object store server you want to delete.

Examples

The following example deletes an object store server for Vserver vs1.

```
cluster1::> vserver object-store-server delete -vserver vs1
```

vserver object-store-server modify

Modify an object store server

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server modify` command modifies an object store server.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver for the object store server which you want to modify.

[-object-store-server <Object store server name>] - Object Store Server Name

This parameter specifies the name of the object store server. Note that the object-store-server name must not begin with a bucket name.

[-is-http-enabled {true|false}] - Accept Connections Over HTTP

This optional parameter specifies if server should accept HTTP connections. Modifying this field requires setting the `status-admin` of the object store server to *down*.

[-is-https-enabled {true|false}] - Accept Connections Over HTTPS

This optional parameter specifies if server should accept HTTPS connections. Modifying this field requires setting the `status-admin` of the object store server to *down*.

[-certificate-name <text>] - Name of Certificate Used for HTTPS Connections

Common name of the certificate used for HTTPS connections. Modifying this field does not require setting the `status-admin` of the object store server to *down*.

[-listener-port <integer>] - Object Store Server Listener Port

This parameter specifies the listener port for the object store server. Modifying this field requires setting the `status-admin` of the object store server to *down*.

[-secure-listener-port <integer>] - Object Store Server Listener Port for HTTPS

This parameter specifies the secure listener port for the object store server. Modifying this field requires setting the `status-admin` of the object store server to *down*.

[-status-admin {down|up}] - Object Store Server Administrative State

This parameter specifies the administrative status of the object store server.

[-comment <text>] - Object Store Server Description

This parameter specifies the text comment for the object store server. Modifying this field does not require setting the `status-admin` of the object store server to *down*.

[`-default-unix-user <text>`] - Default UNIX User for NAS Access

This optional parameter specifies the default UNIX user used for name-mapping from an S3 user to UNIX user during NAS access. Modifying this field does not require setting the `status-admin` of the object store server to `down`.

[`-default-win-user <text>`] - Default Windows User for NAS Access

This optional parameter specifies the default Windows user used for name-mapping from an S3 user to Windows user during NAS access. Modifying this field does not require setting the `status-admin` of the object store server to `down`.

[`-is-ldap-fastbind-enabled {true|false}`] - Is LDAP FastBind Authentication Enabled? (privilege: advanced)

This parameter specifies whether LDAP FastBind authentication is enabled for the object store server. Modifying this field does not require setting the `status-admin` of the object store server to `down`.

[`-max-key-time-to-live {P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W}`] - Maximum Value for Key TTL

This parameter specifies the maximum permissible value for object store user key time-to-live property. Modifying this field does not require setting the `status-admin` of the object store server to `down`.

[`-max-lock-retention-period {{<integer> days|years} | none}`] - Maximum Object Lock Retention Period

This parameter specifies the maximum value that can be specified as lock retention period for an object in an object store bucket. Modifying this field does not require setting the `status-admin` of the object store server to `down`.

[`-min-lock-retention-period {{<integer> days|years} | none}`] - Minimum Object Lock Retention Period

This parameter specifies the minimum value that can be specified as lock retention period for an object in an object store bucket. Modifying this field does not require setting the `status-admin` of the object store server to `down`.

Examples

The following example modifies the name of the object store server for Vserver vs1.

```
cluster1::> vsserver object-store-server modify -vsserver vs1 -object-store
-server OSS2
```

vsserver object-store-server show-flexcache-bucket

Display NAS buckets which are on FlexCache volumes.

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

The `vsserver object-store-server show-flexcache-bucket` command displays information about

the object store server NAS buckets which are on FlexCache volumes.

Parameters

[`-fields <fieldname>,...`]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

[`-instance`] (privilege: advanced) }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[`-vserver <Vserver Name>`] - Vserver Name (privilege: advanced)

If you specify this parameter, the command displays information only for object store server NAS buckets for the specified SVM.

[`-bucket <TextNoCase>`] - Object Store Server Bucket Name (privilege: advanced)

If you specify this parameter, the command displays information only for object store server NAS buckets that match the specified bucket.

[`-nas-path <text>`] - NAS Path corresponding to the Bucket (privilege: advanced)

If you specify this parameter, the command displays information only for NAS buckets that match the specified `nas-path`. This parameter specifies the path to the NAS directory which the bucket maps to.

[`-cache-volume <volume name>`] - Cache Volume Name (privilege: advanced)

If you specify this parameter, the command displays information only for object store server buckets that match the specified FlexCache volume.

Examples

The following example displays information of all NAS buckets:

```
cluster1::> vsriver object-store-server show-flexcache-bucket
Vserver      Bucket      Volume      Nas Path
-----
vs1          fc-bucket   fcVol       /fcVolPath/subdir
```

vsvrer object-store-server show

Display object store servers

Availability: This command is available to *cluster* and *Vsvrer* administrators at the *admin* privilege level.

Description

The `vsvrer object-store-server show` command displays information about the object store server.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information only about the object store servers for the specified Vserver

[-object-store-server <Object store server name>] - Object Store Server Name

If you specify this parameter, the command displays information only for object store servers that match the specified object store server name.

[-is-http-enabled {true|false}] - Accept Connections Over HTTP

If you specify this parameter, the command displays information only for object store servers that accept HTTP connections.

[-is-https-enabled {true|false}] - Accept Connections Over HTTPS

If you specify this parameter, the command displays information only for object store servers that accept HTTPS connections.

[-certificate-name <text>] - Name of Certificate Used for HTTPS Connections

If you specify this parameter, the command displays information only for object store servers that match specified certificate name.

[-listener-port <integer>] - Object Store Server Listener Port

If you specify this parameter, the command displays information only for object store servers that match the specified listener port.

[-secure-listener-port <integer>] - Object Store Server Listener Port for HTTPS

If you specify this parameter, the command displays information only for object store servers that match the specified secure listener port.

[-status-admin {down|up}] - Object Store Server Administrative State

If you specify this parameter, the command displays information only for object store servers that match the specified administrative status.

[-comment <text>] - Object Store Server Description

If you specify this parameter, the command displays information only for object store servers that match the specified comment field.

[-default-unix-user <text>] - Default UNIX User for NAS Access

If you specify this parameter, the command displays information only for object store servers that match the specified default UNIX user.

[`-default-win-user <text>`] - Default Windows User for NAS Access

If you specify this parameter, the command displays information only for object store servers that match the specified default Windows user.

[`-is-ldap-fastbind-enabled {true|false}`] - Is LDAP FastBind Authentication Enabled? (privilege: advanced)

This parameter specifies whether LDAP FastBind authentication is enabled for the object store server.

[`-max-key-time-to-live {P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P[<integer>W]}`] - Maximum Value for Key TTL

If you specify this parameter, the command displays information only for object store servers that match the specified time-to-live value.

[`-max-lock-retention-period {{<integer> days|years} | none}`] - Maximum Object Lock Retention Period

If you specify this parameter, the command displays information only for object store servers that match the specified maximum lock retention period.

[`-min-lock-retention-period {{<integer> days|years} | none}`] - Minimum Object Lock Retention Period

If you specify this parameter, the command displays information only for object store servers that match the specified minimum lock retention period.

Examples

The following example displays information of all object store servers:

```
cluster1::> vsriver object-store-server show
Vserver: vs3
Object Store Server Name: test.s3.local
      Administrative State: up
      Listener Port For HTTP: 80
      Secure Listener Port For HTTPS: 443
      HTTP Enabled: false
      HTTPS Enabled: true
      Certificate for HTTPS Connections: server_cert
      Default UNIX User: pcuser
      Default Windows User: win_user
      Maximum Object Lock Retention Period: 100 days
      Minimum Object Lock Retention Period: 10 days
      Comment: Server comment
```

The following example displays information about the object store server associated with Vserver vs1:

```
cluster1::> vsriver object-store-server show -vsriver vs1
Vserver: vs1
Object Store Server Name: test.s3.local
      Administrative State: up
      Listener Port For HTTP: 80
      Secure Listener Port For HTTPS: 443
      HTTP Enabled: false
      HTTPS Enabled: true
      Certificate for HTTPS Connections: server_cert
      Default UNIX User: pcuser
      Default Windows User: win_user
Maximum Object Lock Retention Period: 100 days
Minimum Object Lock Retention Period: 10 days
      Comment: Server comment
```

vsvrrer object-store-server audit create

Create an audit configuration

Availability: This command is available to *cluster* and *Vsvrrer* administrators at the *admin* privilege level.

Description

The `vsvrrer object-store-server audit create` command creates an audit configuration for a Vsvrrer.

When you create an object store audit configuration, you can also specify the rotation method. By default, the audit log is rotated based on size.

You can use the time-based rotation parameters in any combination (`-rotate-schedule-month`, `-rotate-schedule-dayofweek`, `-rotate-schedule-day`, `-rotate-schedule-hour`, and `-rotate-schedule-minute`). The `-rotate-schedule-minute` parameter is mandatory. All other time-based rotation parameters are optional.

The rotation schedule is calculated by using all the time-related values. For example, if you specify only the `-rotate-schedule-minute` parameter, the audit log files are rotated based on the minutes specified on all days of the week, during all hours on all months of the year. If you specify only one or two time-based rotation parameters (say `-rotate-schedule-month` and `-rotate-schedule-minutes`), the log files are rotated based on the minute values that you specified on all days of the week, during all hours, but only during the specified months. For example, you can specify that the audit log is to be rotated during the months January, March, and August on all Mondays, Wednesdays, and Saturdays at 10:30.

If you specify values for both `-rotate-schedule-dayofweek` and `-rotate-schedule-day`, they are considered independently. For example if you specify `-rotate-schedule-dayofweek` as Friday and `-rotate-schedule-day` as 13 then the audit logs would be rotated on every Friday and on the 13th day of the specified month, not just on every Friday the 13th.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver on which to create the audit configuration. The Vserver must already exist.

-destination <text> - Log Destination Path

This parameter specifies the audit log destination path where consolidated audit logs are stored. If the path is not valid, the command fails. The path can be up to 864 characters in length and must have read-write permissions.

[-events {data|management}] - Categories of Events to Audit

This parameter specifies the categories of events to be audited. Supported event categories are: data and management events, The corresponding parameter values are: *data* , *management* .

[-format <json>] - Log Format

This parameter specifies the output format of the audit logs. By default, the output format is JSON.

[-rotate-size {<size>|-}] - Log File Size Limit

This parameter specifies the audit log file size limit. By default, the audit log is rotated based on size. The default audit log size is 100 MB.

[-rotate-schedule-month <cron_month>,...] - Log Rotation Schedule: Month

This parameter specifies the monthly schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated during the months January, March, and August, or during all the months. Valid values are January, February, March, April, May, June, July, August, September, October, November, December, and all. Specify "all" to rotate the audit logs every month.

[-rotate-schedule-dayofweek <cron_dayofweek>,...] - Log Rotation Schedule: Day of Week

This parameter specifies the daily (day of the week) schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated on Tuesdays and Fridays, or during all the days of a week. Valid values are Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and all. Specify "all" to rotate the audit logs every day.

[-rotate-schedule-day <cron_dayofmonth>,...] - Log Rotation Schedule: Day

This parameter specifies the day of the month schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated on the 10th and 20th days of a month, or all days of a month. Valid values range from 1 to 31.

[-rotate-schedule-hour <cron_hour>,...] - Log Rotation Schedule: Hour

This parameter specifies the hourly schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated at 6 a.m and 10 a.m. Valid values range from 0 (midnight) to 23 (11:00 p.m.). Specify "all" to rotate the audit logs every hour.

[-rotate-schedule-minute <cron_minute>,...] - Log Rotation Schedule: Minute

This parameter specifies the minute schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated at the 30th minute. Valid values range from 0 to 59.

{ [-rotate-limit <integer>] - Log Files Rotation Limit

This parameter specifies the audit log files rotation limit. A value of 0 indicates that all the log files are retained. The default value is 0. For example, if you enter a value of 5, the last five audit logs are retained.

| [-retention-duration <[<integer>d] [<integer>h] [<integer>m] [<integer>s]>] - Log Retention Duration }

This parameter specifies the audit log files retention duration. A value of 0s indicates that all the log files are retained. The default value is 0s. For example, if you enter a value of 5d0h0m, logs more than 5 days old are deleted.

Examples

The following examples create an audit configuration for Vserver vs1 using size-based rotation.

```
cluster1::> vsserver object-store-server audit create -vserver vs1
-destination /audit_log -rotate-size 10MB -rotate-limit 5
```

+ +

The following example creates an audit configuration for Vserver vs1 using time-based rotation. The audit logs are rotated monthly, all days of the week, at 12:30.

```
cluster1::> vsserver object-store-server audit create -vserver vs1
-destination /audit_log -rotate-schedule-month all -rotate-schedule
-dayofweek all -rotate-schedule-hour 12 -rotate-schedule-minute 30
```

The following example creates an audit configuration for Vserver vs1 using time-based rotation. The audit logs are rotated in January, March, May, July, September, and November on Monday, Wednesday, and Friday, at 6:15, 6:30, 6:45, 12:15, 12:30, 12:45, 18:15, 18:30, and 18:45. The last 6 audit logs are retained.

```
cluster1::> vsserver object-store-server audit create -vserver vs1
-destination /audit_log -rotate-schedule-month
January,March,May,July,September,November -rotate-schedule-dayofweek
Monday,Wednesday,Friday -rotate-schedule-hour 6,12,18 -rotate-schedule
-minute 15,30,45 -rotate-limit 6
```

The following example creates an audit configuration for Vserver vs1 for auditing object store data access events in the output log format Json.

```
cluster1::> vsserver object-store-server audit create -vserver vs1
-destination /audit_log -format json -events data
```

vserver object-store-server audit delete

Delete audit configuration

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server audit delete` command deletes the audit configuration for a Vserver.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver associated with the audit configuration to be deleted.

[-force <true>] - Force Delete (privilege: advanced)

This parameter is used to forcibly delete the audit configuration. By default the setting is `false`.

Examples

The following example deletes the audit configuration for Vserver `vs1`.

```
cluster1::> vserver object-store-server audit delete -vserver vs1
```

vserver object-store-server audit disable

Disable auditing

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server audit disable` command disables auditing for a Vserver.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver for which auditing is to be disabled. The Vserver audit configuration must already exist.

Examples

The following example disables auditing for Vserver `vs1`.

```
cluster1::> vserver object-store-server audit disable -vserver vs1
```

vserver object-store-server audit enable

Enable auditing

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server audit enable` command enables auditing for a Vserver.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver for which auditing is to be enabled. The Vserver audit configuration must already exist.

[-force <true>] - Force Enable (privilege: advanced)

This parameter is used to ignore errors while enabling auditing.

Examples

The following example enables auditing for Vserver vs1:

```
cluster1::> vserver object-store-server audit enable -vserver vs1
```

vserver object-store-server audit modify

Modify the audit configuration

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server audit modify` command modifies an audit configuration for a Vserver.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver for which the audit configuration is to be modified. The Vserver audit configuration must already exist.

If you have configured time-based rotation, modifying one parameter of time-based rotation schedule does not affect the other parameters. For example, if the rotation schedule is set to run at Monday 12:30 a.m., and you modify the `-rotate-schedule-dayofweek` parameter to Monday,Wednesday,Friday, the new rotation-schedule rotates the audit logs on Monday, Wednesday, and Friday at 12:30 a.m. To clear time-based rotation parameters, you must explicitly set that portion to "-". Some time-based parameters can also be set to "all".

[-destination <text>] - Log Destination Path

This parameter specifies the audit log destination path where consolidated audit logs are stored. If the path is not valid, the command fails. The path can be up to 864 characters in length and must have read-write permissions.

[-events {data|management}] - Categories of Events to Audit

This parameter specifies the categories of events to be audited. Supported event categories are: data and management events. The corresponding parameter values are: *data* , *management* . By default, *data* events are enabled

[-format <json>] - Log Format

This parameter specifies the output format of the audit logs. By default, the output format is JSON.

[-rotate-size {<size>|-}] - Log File Size Limit

This parameter specifies the audit log file size limit. By default, the audit log is rotated based on size. The default audit log size is 100 MB.

[-rotate-schedule-month <cron_month>,...] - Log Rotation Schedule: Month

This parameter specifies the monthly schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated during the months January, March, and August, or during all the months. Valid values are January, February, March, April, May, June, July, August, September, October, November, December, and all. Specify "all" to rotate the audit logs every month.

[-rotate-schedule-dayofweek <cron_dayofweek>,...] - Log Rotation Schedule: Day of Week

This parameter specifies the daily (day of the week) schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated on Tuesdays and Fridays, or during all the days of a week. Valid values are Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and all. Specify "all" to rotate the audit logs every day.

[-rotate-schedule-day <cron_dayofmonth>,...] - Log Rotation Schedule: Day

This parameter specifies the day of the month schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated on the 10th and 20th days of a month, or all days of a month. Valid values range from 1 to 31.

[-rotate-schedule-hour <cron_hour>,...] - Log Rotation Schedule: Hour

This parameter specifies the hourly schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated at 6 a.m and 10 a.m. Valid values range from 0 (midnight) to 23 (11:00 p.m.). Specify "all" to rotate the audit logs every hour.

[-rotate-schedule-minute <cron_minute>,...] - Log Rotation Schedule: Minute

This parameter specifies the minute schedule for rotating the audit log. For example, you can specify that the audit log is to be rotated at the 30th minute. Valid values range from 0 to 59.

{ [-rotate-limit <integer>] - Log Files Rotation Limit

This parameter specifies the audit log files rotation limit. A value of 0 indicates that all the log files are retained. The default value is 0.

[-retention-duration <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Log Retention Duration }

This parameter specifies the audit log files retention duration. A value of 0s indicates that all the log files are retained. For example, if you enter a value of 5d0h0m0s, logs more than 5 days old are deleted.

Examples

The following example modifies the rotate-size and rotate-limit field for Vserver vs1.

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

The following example modifies an audit configuration for Vserver vs1 using the time-based rotation method. The audit logs are rotated monthly, all days of the week, at 12:30.

```
cluster1::> vserver object-store-server audit modify -vserver vs1
-destination /audit_log -rotate-schedule-month all -rotate-schedule
-dayofweek all -rotate-schedule-hour 12 -rotate-schedule-minute 30
```

The following example modifies an audit configuration for Vserver vs1 for auditing object store data events in the output log format Json.

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -format
json -events data
```

vserver object-store-server audit rotate-log

Rotate audit log

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server audit rotate-log` command rotates audit logs for a Vserver.

Parameters

-vserver <vserver name> -Vserver

This parameter specifies the name of the Vserver for which audit logs are to be rotated. The Vserver audit configuration must already exist. Auditing must be enabled for the Vserver.

Examples

The following example rotates audit logs for Vserver vs1.

```
cluster1::> vserver object-store-server audit rotate-log -vserver vs1
```

vserver object-store-server audit show

Display the audit configuration

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server audit show` command displays object store audit configuration information about Vservers. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all the Vservers:

- Vserver name
- Audit state
- Target directory

You can specify the `-fields` parameter to specify which audit configuration information to display about Vservers. + You can specify additional parameters to display only information that matches those parameters. For instance, to display information about the log file rotation size of a Vserver whose value matches 10 MB, run the command with the `-rotate-size 10MB` parameter.

You can specify the `-instance` parameter to display audit configuration information for all Vservers in list form.

Parameters

{ [-fields <fieldname>, ...]

If you specify the `-fields <fieldname>, ...` parameter, the command only displays the fields that you specify.

| [-log-save-details]

You can specify the `-log-save-details` parameter to display the following information about all the Vservers:

- Vserver name
- Rotation file size
- Rotation schedules
- Rotation limit

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all entries.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays information about the specified Vserver.

[-state {true|false}] - Auditing State

If you specify this parameter, the command displays information about the Vservers that use the specified audit state value.

[-destination <text>] - Log Destination Path

If you specify this parameter, the command displays information about the Vservers that use the specified destination path.

[-events {data|management}] - Categories of Events to Audit

If you specify this parameter, the command displays information about the Vservers that use the specified

category of events that are audited. Valid values are *file-ops*, *cifs-logon-logoff*, *cap-staging*, *file-share*, *audit-policy-change*, *user-account*, *security-group* and *authorization-policy-change*. *audit-policy-change* will appear only in diag mode.

[-format <json>] - Log Format

If you specify this parameter, the command displays information about the Vservers that use the specified log format.

[-rotate-size {<size>|-}] - Log File Size Limit

If you specify this parameter, the command displays information about the Vservers that use the specified log file rotation size.

[-rotate-schedule-month <cron_month>,...] - Log Rotation Schedule: Month

If you specify this parameter, the command displays information about the Vservers that use the specified month of the time-based log rotation scheme. Valid values are January, February, March, April, May, June, July, August, September, October, November, and December.

[-rotate-schedule-dayofweek <cron_dayofweek>,...] - Log Rotation Schedule: Day of Week

If you specify this parameter, the command displays information about the Vservers that use the specified day of the week of the time-based log rotation scheme. Valid values are Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.

[-rotate-schedule-day <cron_dayofmonth>,...] - Log Rotation Schedule: Day

If you specify this parameter, the command displays information about the Vservers that use the specified day of the month of the time-based log rotation scheme. Valid values range from 1 to 31.

[-rotate-schedule-hour <cron_hour>,...] - Log Rotation Schedule: Hour

If you specify this parameter, the command displays information about the Vservers that use the specified hour of the time-based log rotation scheme. Valid values range from 0 (midnight) to 23 (11:00 p.m.).

[-rotate-schedule-minute <cron_minute>,...] - Log Rotation Schedule: Minute

If you specify this parameter, the command displays information about the Vservers that use the specified minute of the time-based log rotation scheme. Valid values range from 0 to 59.

[-rotate-schedule-description <text>] - Rotation Schedules

If you specify this parameter, the command displays information about the Vservers that use the specified rotation schedules. This field is derived from the rotate-time fields.

[-rotate-limit <integer>] - Log Files Rotation Limit

If you specify this parameter, the command displays information about the Vservers that use the specified rotation limit value.

[-retention-duration [<integer>d] [<integer>h] [<integer>m] [<integer>s]>] - Log Retention Duration

If you specify this parameter, the command displays information about the Vservers audit logs retention duration.

Examples

The following example displays the name, audit state, event types, log format, and target directory for all Vservers.

```
cluster1::> vsriver object-store-server audit show
Vserver      State  Event Types Log Format Target Directory
-----
vs1          false  data      json      /audit_log
```

The following example displays the Vserver names and details about the audit log for all Vservers.

```
cluster1::> vsriver object-store-server audit show -log-save-details
Rotation
Vserver      File Size Rotation Schedule Limit
-----
vs1          100MB      -              0
```

The following example displays in list form all audit configuration information about all Vservers.

```
cluster1::> vsriver object-store-server audit show -instance
Vserver: vs1
      Auditing state: true
      Log Destination Path: /audit_log
      Categories of Events to Audit: data
      Log Format: json
      Log File Size Limit: 100MB
      Log Rotation Schedule: Month: -
      Log Rotation Schedule: Day of Week: -
      Log Rotation Schedule: Day: -
      Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
      Rotation Schedules: -
      Log Files Rotation Limit: 0
      Log Retention Time: 0s
```

vsvrr object-store-server audit event-selector create

Create an object store server audit event-selector

Availability: This command is available to *cluster* and *Vsvrr* administrators at the *admin* privilege level.

Description

The `vsvrr object-store-server audit event-selector create` command creates an audit event selector for the object store server bucket. The audit event selector specifies the types of event access and the types of event permission that are to be audited. S3 auditing configurations are enabled at the Vsvrr level. However, this command must be used to specify the buckets in the Vsvrr that are enabled for audit. If buckets are added to the Vsvrr and need to be audited, they must be added with this command.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver on which the bucket audit event-selector needs to be created for the object store server bucket.

-bucket <TextNoCase> - Object Store Server Bucket Name

This parameter specifies the name of the object store server bucket for which the audit event-selector needs to be created. The object store bucket must already exist.

-access {read-only|write-only|all} - Access type for audit events

Use this parameter to specify which type of event access is being audited. Possible values are: read-only, write-only or all.

-permission {allow-only|deny-only|all} - Permission type for audit events

Use this parameter to specify which type of event permission is being audited. Possible value are: allow-only, deny-only or all.

Examples

The following example displays information on object store server audit event-selector for vs1 and bucket bucket1:

```
cluster1::> vs1 object-store-server audit event-selector create
               -vserver vs1 -bucket bucket1 -access read-only -permission
allow-only
```

vserver object-store-server audit event-selector delete

Delete an object store server audit event-selector

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server audit event-selector delete` command delete an audit event-selector for the object store server bucket.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver on which the bucket audit event-selector needs to be deleted.

-bucket <TextNoCase> - Object Store Server Bucket Name

This parameter specifies the name of the object store server bucket for which the audit event-selector needs to be deleted.

Examples

The following example delete an object store server audit event-selector for Vserver vs1 and bucket1:

```
cluster1::> vserver object-store-server audit event-selector delete
               -vserver vs1 -bucket bucket1
```

vserver object-store-server audit event-selector modify

Modify an object store server audit event-selector

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server audit event-selector modify` command modifies an audit event-selector for the object store server bucket.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver on which the bucket audit event-selector needs to be modified for the object store server bucket.

-bucket <TextNoCase> - Object Store Server Bucket Name

This parameter specifies the name of the object store server bucket for which the audit event-selector needs to be modified.

[-access {read-only|write-only|all}] - Access type for audit events

Use this parameter to specify which type of event access is being audited. Possible values are: read-only, write-only or all.

[-permission {allow-only|deny-only|all}] - Permission type for audit events

Use this parameter to specify which type of event permission is being audited. Possible value are: allow-only, deny-only or all.

Examples

The following example modified an object store server audit event-selector for Vserver vs1 and bucket1 with read-only access to write-only access:

```
cluster1::> vserver object-store-server audit event-selector modify
               -vserver vs1 -bucket bucket1 -access write-only
```

vserver object-store-server audit event-selector show

Display object store server audit event-selector

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server audit event-selector show` command displays information about object store server audit event-selector.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver Name

If you specify this parameter, the command displays information on the object store server audit event-selector for the specified Vserver.

[-bucket <TextNoCase>] - Object Store Server Bucket Name

If you specify this parameter, the command displays information on the object store server audit event-selector for the specified bucket.

[-access {read-only|write-only|all}] - Access type for audit events

If you specify this parameter, the command displays information on the object store server audit event-selector that match the specified access.

[-permission {allow-only|deny-only|all}] - Permission type for audit events

If you specify this parameter, the command displays information on the object store server audit event-selector that match the specified permission.

Examples

The following example displays information on object store server audit event-selector for vs1 and bucket bucket1:

```
cluster1::> vserver object-store-server audit event-selector show
               -vserver vs1 -bucket bucket1
Vserver      Bucket      Access      Permission
-----
vs1
            bucket1      read-only      allow-only
```

The following example displays detailed information of the object server audit event-selector associated with Vserver vs1.

```
cluster1::> vsserver object-store-server audit event-selector show
               -vsserver vs1
```

```
Vserver          :vs1
Bucket           :bucket1
Access           :all
Permission       :all
```

vserver object-store-server bucket clear-snapshot-metadata

Delete all snapshot metadata for the S3 bucket.

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

The `vserver object-store-server bucket clear-snapshot-metadata` command removes all snapshot metadata for a specified S3 bucket. This command is available in advanced privilege.

Parameters

-vsserver <Vserver Name> - Vserver Name (privilege: advanced)

This specifies the name of the Vserver that contains the S3 bucket for which the snapshot metadata will be removed.

-bucket <TextNoCase> - Object Store Server Bucket Name (privilege: advanced)

This specifies the name of the S3 bucket for which the snapshot metadata will be removed.

Examples

The following example removes all snapshot metadata for an S3 bucket bucket-1 on Vserver named vs0.

```
cluster1::> vsserver object-store-server bucket clear-snapshot-metadata
               -vsserver vs0 -bucket bucket-1
```

vserver object-store-server bucket create

Create an object store server bucket

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server bucket create` command creates a bucket for the object store server.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver for the object store server where the bucket needs to be created. The object store server must already exist.

-bucket <TextNoCase> - Object Store Server Bucket Name

This parameter specifies the name of the object store server bucket. Note that the bucket name must not be same as the beginning of the object-store-server name present in the vserver.

[-type {s3|nas}] - Type of bucket

This parameter specifies the type of the bucket. The default value is `s3`.

[-versioning-state {disabled|enabled|suspended}] - Object Store Server Versioning State

Use this parameter to specify the state of versioning on the bucket.

[-comment <text>] - Object Store Server Bucket Comment

This optional parameter specifies a text comment for the object store server bucket.

{ [-aggr-list <aggregate name>, ...] - List of Aggregates for FlexGroup Constituents (privilege: advanced)

Use this parameter to specify the list of aggregates for the FlexGroup constituents on which the bucket needs to be created. Each entry in the list will create a constituent on the specified aggregate. The root constituent will always be placed on the first aggregate in the list, unless `optimize-aggr-list` is specified as `true`. An aggregate may be specified multiple times to have multiple constituents created on it. This parameter only applies to FlexGroup volumes. This parameter is available only in advanced privilege mode.

[-aggr-list-multiplier <integer>] - Aggregate List Repeat Count (privilege: advanced)

Use this parameter to specify the number of FlexGroup constituents to be created. This parameter is available only in advanced privilege mode.

[-optimize-aggr-list {true|false}] - Have the System Optimize the Order of the Aggregate List (privilege: advanced)

Specifies whether to create the constituents of the FlexGroup volume on which the bucket needs to be created, on the aggregates specified in the `aggr-list` in the order they are specified, or whether the system should optimize the ordering of the aggregates. If this value is `true`, the system will optimize the ordering of the aggregates specified in the `aggr-list`. If this value is `false` the order of the `aggr-list` will be unchanged. The default value is `false`. This parameter only applies to FlexGroup volumes. This parameter is available only in advanced privilege mode.

{ [-used-as-capacity-tier {true|false}] - Is Used as Capacity Tier

Use this parameter to specify if the bucket is going to be used for FabricPool capacity tier. This parameter is used for bucket provisioning to strike a balance between low cost and performance.

[`-storage-service-level <text>`] - Storage Service Level of the Bucket }

Use this parameter to specify the storage service level with which the bucket should be created.

[`-size {<integer>[KB|MB|GB|TB|PB]}`] - Size of the Bucket

Use this parameter to specify the size of the FlexGroup volume to be created.

[`-exclude-aggr-list <aggregate name>,...`] - List of Aggregates to Exclude During FlexGroup Create

Use this parameter to specify the list of aggregates to exclude during FlexGroup creation. This parameter is used only when creating bucket for capacity tier use case within the local cluster.

[`-qos-policy-group <text>`] - QoS policy group

A policy group defines measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated. If you do not assign a policy group to a bucket, the system will not monitor and control the traffic to it.

[`-nas-path <text>`] - NAS Path Specified During Bucket Creation

This parameter specifies the path to the NAS directory which the bucket maps to.

[`-is-nas-path-mutable {true|false}`] - Is NAS Path Mutable (privilege: advanced)

This parameter determines if the NAS bucket mapping with a NAS volume can change with the changes in NAS volume `junction-path` due to operations like mount and unmount. If mutable, the NAS bucket will access any path in a NAS volume that matches the specified `nas-path`. If immutable, the NAS bucket will always access the `nas-path` specified during creation, regardless of `junction-path` changes. For example, if a NAS volume 'volA' is mounted at '/data' and a NAS bucket is created with `nas-path` '/data', and later 'volA' is unmounted and 'volB' is mounted at '/data': If mutable, '/data' of 'volB' will be accessible over S3. If immutable, '/data' of 'volA' will be accessible over S3. The default value is *true*.

[`-retention-mode {no-lock|compliance|governance}`] - Bucket Retention Mode

Use this parameter to specify the retention-mode in which objects within the bucket can be locked.

[`-use-mirrored-aggregates {true|false}`] - Use Mirrored Aggregates

Use this parameter to specify whether mirrored aggregates are selected for the FlexGroup on which the bucket will be created. Only mirrored aggregates are used if this parameter is set to *true* and only unmirrored aggregates are used if this parameter is set to *false*. The default value is *true* for a MetroCluster configuration and is *false* for a non-MetroCluster configuration.

[`-default-retention-period {{<integer> days|years} | none}`] - Bucket Default Retention Period

Use this parameter to specify the retention-period to be applied on all unlocked objects inserted into the bucket. The retention period can be in years, or days. A period specified for years and days is represented in the ISO-8601 format as "10 years" and "100 days" respectively, for example "10 years" represents a duration of 10 years. The period string must contain only a single time element that is, either years, or days. A duration which combines different periods is not supported, for example "10 years 12 days" is not supported.

[`-snapshot-policy <snapshot policy>`] - Snapshot Policy

This parameter specifies the snapshot policy for the object store server bucket.

`[-is-consistent-etag {true|false}]` - Return Consistent ETag for NAS Bucket (privilege: advanced)

This parameter specifies whether a consistent entity tag is returned across different S3 requests for the NAS bucket. The default value is *false*.

Examples

The following example creates an object store server bucket for Vserver vs1 of size 1TB.

```
cluster1::> vsriver object-store-server bucket create -vserver vs1 -bucket
testbucket -size 1TB.
```

The following example creates an object store server bucket for Vserver vs1 of size 1TB using aggr-list.

```
cluster1::*> vsriver object-store-server bucket create -vserver vs1
-bucket testbucket -aggr-list aggr1 -size 1TB.
```

The following example creates an object store server NAS bucket for Vserver vs1 with *is-nas-path-mutable* option turned off.

```
cluster1::> vsriver object-store-server bucket create -vserver vs1 -bucket
nasbucket -nas-path /path1 -is-nath-path-mutable false
```

vserver object-store-server bucket delete

Delete an object store bucket

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server bucket delete` command deletes the bucket belonging to the object store server.

Parameters

`-vserver <Vserver Name>` - Vserver Name

This parameter specifies the name of the Vserver for the object store server's bucket you want to delete.

`-bucket <TextNoCase>` - Object Store Server Bucket Name

This parameter specifies the name of the bucket of the object store server you want to delete.

Examples

The following example deletes an object store server bucket for Vserver vs1.

```
cluster1::> vsriver object-store-server delete -vsriver vs1 -bucket  
testbucket
```

vsvriver object-store-server bucket evict-remote-cached-objects

Evict remote read-write cached objects

Availability: This command is available to *cluster* and *Vsvriver* administrators at the *advanced* privilege level.

Description

The `vsvriver object-store-server evict-remote-cached-objects` command will evict read-write dirty cached objects in all constituent volumes of a given object store server bucket. This command will evict only objects that are cached on a different volume than its origin volume. This command requires two parameters - a Vsvriver name and an object store server bucket name.

Parameters

-vsriver <Vsvriver Name> - Vsvriver Name (privilege: advanced)

This specifies the name of the Vsvriver for the object store server.

-bucket <TextNoCase> - Object Store Server Bucket Name (privilege: advanced)

This specifies the name of the object store server bucket.

Examples

The following example starts the command:

```
cluster1::>vsvriver object-store-server bucket evict-remote-cached-objects  
-vsriver my-vsvriver -bucket my-bkt
```

vsvriver object-store-server bucket modify

Modify an object store server bucket

Availability: This command is available to *cluster* and *Vsvriver* administrators at the *admin* privilege level.

Description

The `vsvriver object-store-server bucket modify` command modifies an object store server bucket.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver for the object store server which you want to modify.

-bucket <TextNoCase> - Object Store Server Bucket Name

This parameter specifies the name of the object store server bucket which you want to modify.

[-versioning-state {disabled|enabled|suspended}] - Object Store Server Versioning State

Use this parameter to specify the state of versioning on the bucket. Note that the versioning state cannot be modified to 'disabled' from any other state.

[-comment <text>] - Object Store Server Bucket Comment

This parameter specifies the text comment for the object store server bucket.

[-size {<integer>[KB|MB|GB|TB|PB]}] - Size of the Bucket

This parameter specifies the size of the object store server bucket.

[-qos-policy-group <text>] - QoS policy group

A policy group defines measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated. If you do not assign a policy group to a bucket, the system will not monitor and control the traffic to it.

[-nas-path <text>] - NAS Path Specified During Bucket Creation

This parameter specifies the path to the NAS directory which the bucket maps to.

[-default-retention-period {{<integer> days|years} | none}] - Bucket Default Retention Period

Use this parameter to modify the default-retention-period to be applied on all unlocked objects to be inserted into the bucket.

[-snapshot-policy <snapshot policy>] - Snapshot Policy

This parameter specifies the snapshot policy for the object store server bucket.

[-is-consistent-etag {true|false}] - Return Consistent ETag for NAS Bucket (privilege: advanced)

This parameter specifies whether a consistent entity tag is returned across different S3 requests for the NAS bucket.

Examples

The following example modifies the comment of the object store server bucket for Vserver vs1.

```
cluster1::> vsriver object-store-server bucket modify -vserver vs1 -bucket  
testbucket -comment test
```

vsvrer object-store-server bucket show

Display object store server buckets

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server bucket show` command displays information about the object store server bucket.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver Name

If you specify this parameter, the command displays information only about the object store server buckets for the specified Vserver

[-bucket <TextNoCase>] - Object Store Server Bucket Name

If you specify this parameter, the command displays information only for object store server buckets that match the specified bucket.

[-type {s3|nas}] - Type of bucket

This parameter specifies the type of bucket.

[-versioning-state {disabled|enabled|suspended}] - Object Store Server Versioning State

This parameter specifies the state of the versioning on a bucket.

[-uuid <UUID>] - Object Store Server Bucket UUID

If you specify this parameter, the command displays information only for object store server buckets that match the specified bucket uuid.

[-comment <text>] - Object Store Server Bucket Comment

If you specify this parameter, the command displays information only for object store server buckets that match the specified comment.

[-volume <volume name>] - Hosting Volume Name

If you specify this parameter, the command displays information only for object store server buckets that match the specified volume.

[-size {<integer>[KB|MB|GB|TB|PB]}] - Size of the Bucket

If you specify this parameter, the command displays information only for object store server buckets that match the specified size.

[-logical-used {<integer>[KB|MB|GB|TB|PB]}] - Object Store Server Bucket Logical Used Size

If you specify this parameter, the command displays information only for object store server buckets that match the specified logical used size.

[-object-count <integer>] - Object Store Server Object Count

If you specify this parameter, the command displays information only for object store server buckets that match the specified object-count.

[-incomplete-multipart-uploads-count <integer>] - Count of Incomplete Multipart Uploads

If you specify this parameter, the command displays information only for object store server buckets that match the specified incomplete-multipart-uploads-count.

[-encryption {true|false}] - Is Encryption Enabled on Bucket

If you specify this parameter, the command displays information only for object store server buckets that match the specified encryption field.

[-qos-policy-group <text>] - QoS policy group

A policy group defines measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated. If you do not assign a policy group to a bucket, the system will not monitor and control the traffic to it.

[-is-protected {true|false}] - Is bucket a FabricLink source and protected

This parameter specifies whether a bucket is protected using SnapMirror relationship to another bucket.

[-is-protected-on-ontap {true|false}] - Is bucket protected over ONTAP

This parameter specifies whether a bucket is protected using SnapMirror relationship to another ONTAP bucket.

[-is-protected-on-cloud {true|false}] - Is bucket protected over Cloud

This parameter specifies whether a bucket is protected using SnapMirror relationship to a Cloud bucket.

[-is-protected-on-external-cloud {true|false}] - Is bucket protected on External Cloud

This parameter specifies whether a bucket is protected using S3 SnapMirror relationship to a bucket on an external Cloud provider i.e. excluding providers types ONTAP_S3 and SGWS.

[-nas-path <text>] - NAS Path Specified During Bucket Creation

This parameter specifies the path to the NAS directory which the bucket maps to.

[-nas-path-current <text>] - Current NAS Path corresponding to the Bucket (privilege: advanced)

This parameter specifies the current path to the NAS directory which the bucket maps to.

[-is-nas-path-mutable {true|false}] - Is NAS Path Mutable (privilege: advanced)

If you specify this parameter, the command displays information only for object store server buckets that match the specified value. This parameter specifies whether to use nas-path name or nas-path file handle for data access through NAS bucket.

[-retention-mode {no-lock|compliance|governance}] - Bucket Retention Mode

If you specify this parameter, the command displays information only for object store server buckets that match the specified retention-mode. This parameter specifies the object locking mode of the bucket.

[-default-retention-period {{<integer> days|years} | none}] - Bucket Default Retention Period

If you specify this parameter, the command displays information only for object store server buckets that match the specified default-retention-period field. This parameter specifies the default-retention-period

applied on the bucket.

[`-snapshot-policy <snapshot policy>`] - Snapshot Policy

If you specify this parameter, the command displays information only for object store server buckets that match the specified snapshot-policy field. This parameter specifies the snapshot-policy for the bucket.

[`-is-consistent-etag {true|false}`] - Return Consistent ETag for NAS Bucket (privilege: advanced)

If you specify this parameter, the command displays information only for object store server buckets that match the specified consistent entity tag behavior. This parameter specifies whether a consistent entity tag is returned across different S3 requests for the NAS bucket.

Examples

The following example displays information of all object store servers buckets:

```
cluster1::> vsriver object-store-server bucket show
nsankaracluster-1::*> vsriver object-store-server bucket show
Vserver      Bucket      Type      Volume      Size
Encryption Role      NAS Path
-----
vs1          s3bucket1    nas       s3adapter    -        false
-            /s3adapter
vs1          testbucket1  s3        fg_oss_1654817100 1.56GB   false
standalone -
Comment: test1
vs2          nasbucket1    nas       vol2         -        false
-            /vol2
vs2          nasbucket2    nas       vol2         -        false
-            /vol2
4 entries were displayed.
```

The following example displays information of the object store server bucket associated with Vserver vs1:

```
cluster1::> vsriver object-store-server bucket show -vserver vs1
Vserver      Bucket      Type      Volume      Size
Encryption Role      NAS Path
-----
vs1          s3bucket1    nas       s3adapter    -        false
-            /s3adapter
vs1          testbucket1  s3        fg_oss_1654817100 1.56GB   false
standalone -
Comment: test1
```

The following example displays detailed information of the object store server bucket associated with Vserver vs1:

```
cluster1::> vs1 object-store-server bucket show -vserver vs1 -instance
Vserver Name: vs1
    Object Store Server Bucket Name: s3bucket1
        Type of bucket: nas
    Object Store Server Versioning State: -
    Object Store Server Bucket UUID: c621d53a-ddf0-11ec-958f-
005056bba281
    Object Store Server Bucket Comment:
        Hosting FlexGroup Volume Name: s3adapter
        Size of the Bucket: -
Object Store Server Bucket Logical Used Size: -
    Object Store Server Object Count: -
    Is Encryption Enabled on Bucket: false
        QoS policy group: -
        Role of the Bucket: -
    Is bucket a FabricLink source and protected: -
        Is bucket protected over ONTAP: -
        Is bucket protected over Cloud: -
    Is bucket protected on External Cloud: -
    NAS Path corresponding to the Bucket: /s3adapter
        Current NAS Path: -
        Is Mutable NAS Path: true
Vserver Name: vs1
    Object Store Server Bucket Name: testbucket1
        Type of bucket: s3
    Object Store Server Versioning State: disabled
    Object Store Server Bucket UUID: 6a1fa354-e84b-11ec-adce-
005056bba281
    Object Store Server Bucket Comment:
        Hosting FlexGroup Volume Name: fg_oss_1654817100
        Size of the Bucket: 1.56GB
Object Store Server Bucket Logical Used Size: 0B
    Object Store Server Object Count: 0
    Is Encryption Enabled on Bucket: false
        QoS policy group: -
        Role of the Bucket: standalone
    Is bucket a FabricLink source and protected: false
        Is bucket protected over ONTAP: false
        Is bucket protected over Cloud: false
    Is bucket protected on External Cloud: false
    NAS Path corresponding to the Bucket: -
2 entries were displayed.
```

vserver object-store-server bucket cors-rule create

Create a Cross-Origin rule

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server bucket cors-rule create` command creates a cross-origin resource sharing (CORS) rule for the object store server bucket.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver hosting the object store server bucket for which the CORS rule will to be created.

-bucket <TextNoCase> - Object Store Server Bucket Name

This parameter specifies the name of the object store server bucket for which the CORS rule will to be created.

[-index <integer>] - Cross-Origin Access Rule Index

This parameter specifies the index of the object store server bucket CORS rule. This is an optional parameter. Its value is calculated automatically by the system, if not specified.

[-rule-id <text>] - Cross-Origin Access Rule ID

This parameter specifies the ID of the object store server bucket CORS rule.

-allowed-origins <text>, ... - List of the Origins Allowed for Cross-Origin Requests

This parameter specifies a list of origins from where a cross-origin request is allowed to originate from for the object store bucket.

-allowed-methods <text>, ... - List of HTTP Request Methods Allowed in Cross-Origin Requests

This parameter specifies a list of HTTP methods allowed in the cross-origin requests.

[-allowed-headers <text>, ...] - List of the Headers Allowed in Cross-Origin Requests

This parameter specifies a list of HTTP headers allowed in the cross-origin requests.

[-expose-headers <text>, ...] - Headers that Servers Allow Clients to Access

This parameter specifies a list of extra headers sent in the response that customers can access from their applications.

[-max-age-in-seconds <integer>] - How Long (in Seconds) the Results of a Cross-Origin Pre-Flight Request Can Be Cached?

This optional parameter specifies the time in seconds for your browser to cache the pre-flight response for the specified resource.

Examples

The following example creates an object store server bucket CORS rule for Vserver vs1 and bucket bb1.

```
cluster1::> vsserver object-store-server bucket cors-rule create -vsserver
vs1 -bucket bbl -allowed-origins example.com -allowed-methods POST,DELETE
-allowed-headers x-amz-request-id -max-age-in-seconds 2000 -expose-headers
x-purpose -rule-id rule1
```

vsserver object-store-server bucket cors-rule delete

Delete a Cross-Origin rule

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vsserver object-store-server bucket cors-rule delete` command deletes a cross-origin resource sharing (CORS) rule belonging to the object store server bucket.

Parameters

-vsserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver hosting the object store server bucket for which the CORS rule will be deleted.

-bucket <TextNoCase> - Object Store Server Bucket Name

This parameter specifies the name of the object store server bucket for which the CORS rule will be deleted.

-index <integer> - Cross-Origin Access Rule Index

This parameter specifies the index of the object store server bucket CORS rule.

Examples

The following example deletes an object store server bucket CORS rule with index 1 of Vserver vs1 and bucket bucket1.

```
cluster1::> vsserver object-store-server bucket cors-rule delete -vsserver
vs1 -bucket bucket1 -index 1
```

vsserver object-store-server bucket cors-rule show

Show the Cross-Origin rule

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vsserver object-store-server bucket cors-rule show` command displays information about

the cross-origin resource sharing (CORS) rules for the specified object store server bucket.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver Name

If you specify this parameter, the command displays information on the object store server bucket CORS rules for the specified Vserver.

[-bucket <TextNoCase>] - Object Store Server Bucket Name

If you specify this parameter, the command displays information on the object store server bucket CORS rules for the specified object store server bucket.

[-index <integer>] - Cross-Origin Access Rule Index

If you specify this parameter, the command displays information on the object store server bucket CORS rules that match the specified index.

[-rule-id <text>] - Cross-Origin Access Rule ID

If you specify this parameter, the command displays information on the object store server bucket CORS rules that match the specified rule ID.

[-allowed-origins <text>,...] - List of the Origins Allowed for Cross-Origin Requests

If you specify this parameter, the command displays information on the object store server bucket CORS rules that match the specified allowed origins.

[-allowed-methods <text>,...] - List of HTTP Request Methods Allowed in Cross-Origin Requests

If you specify this parameter, the command displays information on the object store server bucket CORS rules that match the specified allowed methods.

[-allowed-headers <text>,...] - List of the Headers Allowed in Cross-Origin Requests

If you specify this parameter, the command displays information on the object store server bucket CORS rules that match the specified allowed headers.

[-expose-headers <text>,...] - Headers that Servers Allow Clients to Access

If you specify this parameter, the command displays information on the object store server bucket CORS rules that match the specified exposed headers.

[-max-age-in-seconds <integer>] - How Long (in Seconds) the Results of a Cross-Origin Pre-Flight Request Can Be Cached?

If you specify this parameter, the command displays information on the object store server bucket CORS rules that match the specified value for this parameter.

Examples

The following example displays information on object store server bucket CORS rules for vs1 and bucket bucket1:

```
cluster1::> vserver object-store-server bucket cors-rule show -vserver vs1
-bucket bb1
```

Vserver	Bucket	Rule-Index	Origin	Methods
vs1	bb1	1	hello.com	POST
vs1	bb1	2	*	POST
vs1	bb1	5	example.com	POST, DELETE

2 entries were displayed.

The following example displays detailed information of the object store server bucket CORS rule associated with Vserver vs1 and bucket bucket1:

```
cluster1::> vserver object-store-server bucket cors-rule show -vserver vs1
-bucket bb1 -index 5
```

```
-----
                                Vserver: vs1
      Object Store Server Bucket Name: bb1
      Cross-Origin Access Rule Index: 5
      Cross-Origin Access Allowed Origins: example.com
      Cross-Origin Access Allowed Methods: POST, DELETE
      Cross-Origin Access Allowed Headers: x-amz-request-id
      Cross-Origin Access Rule Identifier: rule1
      Cross-Origin Access Exposed Headers: x-purpose
      Time a browser can cache Cross-Origin Response: 2000
```

vserver object-store-server bucket lifecycle-management-rule create

Create a lifecycle management rule

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server bucket lifecycle-management-rule create` command creates a lifecycle management rule for the object store server bucket.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver on which the bucket lifecycle management rule needs to be created for the object store server bucket.

-bucket <TextNoCase> - Object Store Server Bucket Name

This parameter specifies the name of the object store server bucket for which the lifecycle management rule needs to be created. The object store server bucket must already exist.

-rule-id <text> - Lifecycle Management Rule Identifier

This parameter specifies the rule identifier of the lifecycle management rule to be applied on the object store server bucket.

[-index <integer>] - Lifecycle Management Rule Index

This parameter specifies the index of the lifecycle management rule to be applied on the object store server bucket.

[-is-enabled {true|false}] - Is This Rule Enabled?

This parameter specifies whether the configured lifecycle management rule is enabled or disabled on the object store server bucket. If you do not specify this parameter, the default is *true*.

[-prefix <text>] - Prefix to be Matched with Object Names

Use this parameter to specify a prefix that is matched against object-names within a bucket.

[-tags <text>, ...] - Tags in Format <tag> or <tag=value>

Use this parameter to specify a list of key-value paired tags.

[-obj-size-greater-than {<integer>[KB|MB|GB|TB|PB]}] - Min Size of the Object

Use this parameter to specify the minimum size of the object for which the corresponding lifecycle rule is to be applied.

[-obj-size-less-than {<integer>[KB|MB|GB|TB|PB]}] - Max Size of the Object

Use this parameter to specify the maximum size of the object for which the corresponding lifecycle rule is to be applied.

-action

{Expiration|NoncurrentVersionExpiration|AbortIncompleteMultipartUpload|ExpirationInternal} - Lifecycle Management Action

Use this parameter to specify lifecycle management actions. The set of actions that the object store server supports are *Expiration*, *NoncurrentVersionExpiration* and *AbortIncompleteMultipartUpload*.

{ [-obj-age-days <integer>] - Number of Days since Creation, After Which Current Version of Objects Can be Deleted

Minimum lifetime in number of days since creation, after which objects can be deleted. This parameter is available for expiration actions only.

[-obj-exp-date <MM/DD/YYYY HH:MM:SS>] - Specific Date When the Objects Should Expire

Expiration date of an object. This parameter is available for expiration actions only.

[`-expired-obj-del-marker {true|false}`] - Cleanup Object Delete Markers

When set to `true`, an object with a delete marker will be deleted. This parameter is available for expiration actions only.

[`-new-non-curr-versions <integer>`] - Number of Latest Non-current Versions to Be Retained

This parameter specifies the number of latest non-current versions to be retained. This parameter is available for non-current version expiration actions only.

[`-non-curr-days <integer>`] - Number of Days after Which Non-current Versions will Be Deleted

This parameter specifies the number of days after which non-current versions can be deleted. This parameter is available for non-current version expiration actions only.

[`-after-initiation-days <integer>`] - Number of Days of Initiation, After Which Upload Can Be Aborted }

This parameter specifies the number of days of initiation, after which uploads can be aborted. This parameter is required for abort-incomplete multipart upload actions only.

Examples

The following example creates an object store server bucket lifecycle management rule for Vserver `vs1` and bucket `bucket1` which specifies an expiration action on a set of objects.

```
cluster1::> vserver object-store-server bucket lifecycle-management-rule
create -vserver vs1 -bucket bucket1 -rule-id rule1 -prefix obj1/ -action
Expiration -obj-age-days 100"
```

vserver object-store-server bucket lifecycle-management-rule delete

Delete a Lifecycle Management rule

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server bucket lifecycle-management-rule delete` command deletes a lifecycle management rule for the object store server bucket.

Parameters

`-vserver <Vserver Name>` - Vserver Name

This parameter specifies the name of the Vserver on which the bucket lifecycle management rule needs to be deleted for the object store server bucket.

`-bucket <TextNoCase>` - Object Store Server Bucket Name

This parameter specifies the name of the object store server bucket for which the lifecycle management rule needs to be deleted. The object store server bucket must already exist.

-rule-id <text> - Lifecycle Management Rule Identifier

This parameter specifies the rule identifier of the lifecycle management rule to be deleted from the object store server bucket.

-index <integer> - Lifecycle Management Rule Index

This parameter specifies the index of the lifecycle management rule to be deleted from the object store server bucket.

[-force <true>] - Ignore Errors

If this parameter is specified and set to true, the user is not prompted to confirm each deletion operation. In addition, several potential errors are ignored. By default, this setting is *true*.

Examples

The following example deletes an object store server bucket lifecycle management rule for Vserver vs1 and bucket1.

```
cluster1::> vsserver object-store-server bucket lifecycle-management-rule
delete -vsserver vs1 -bucket bucket1 -rule-id rule1 -index 1"
```

vserver object-store-server bucket lifecycle-management-rule modify

Modify a lifecycle management rule

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server bucket lifecycle-management-rule modify` command modifies a lifecycle management rule for the object store server bucket.

Parameters

-vsserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver on which the bucket lifecycle management rule will be modified for the object store server bucket.

-bucket <TextNoCase> - Object Store Server Bucket Name

This parameter specifies the name of the object store server bucket for which the lifecycle management rule will be modified. The object store server bucket must already exist.

-rule-id <text> - Lifecycle Management Rule Identifier

This parameter specifies the rule identifier of the lifecycle management rule to be applied on the object store server bucket.

-index <integer> - Lifecycle Management Rule Index

This parameter specifies the index of the lifecycle management rule to be applied on the object store server bucket.

[-is-enabled {true|false}] - Is This Rule Enabled?

This parameter specifies whether the configured lifecycle management rule is to be enabled or disabled on the object store server bucket. The default value when a rule is created is *true*.

{ [-obj-age-days <integer>] - Number of Days since Creation, After Which Current Version of Objects Can be Deleted

This parameter specifies the minimum lifetime, in days since creation, after which objects can be deleted. This parameter is available for expiration actions only.

[-obj-exp-date <MM/DD/YYYY HH:MM:SS>] - Specific Date When the Objects Should Expire

This parameter specifies the expiration date when an object will expire. This parameter is available for expiration actions only.

[-expired-obj-del-marker {true|false}] - Cleanup Object Delete Markers

This parameter specifies whether to delete an object that has a delete marker or not. When set to *true*, an object with a delete marker will be deleted. This parameter is available for expiration actions only.

[-new-non-curr-versions <integer>] - Number of Latest Non-current Versions to Be Retained

This parameter specifies the number of latest non-current versions to be retained. This parameter is available for non-current version expiration actions only.

[-non-curr-days <integer>] - Number of Days after Which Non-current Versions will Be Deleted

This parameter specifies the number of days after which non-current versions can be deleted. This parameter is available for non-current version expiration actions only.

[-after-initiation-days <integer>] - Number of Days of Initiation, After Which Upload Can Be Aborted }

This parameter specifies the number of days of initiation, after which uploads can be aborted. This parameter is available for abort-incomplete multipart upload actions only.

Examples

The following example modifies an object store server bucket lifecycle management rule for Vserver vs1 and bucket1 which specifies expiration action on a set of objects.

```
cluster1::> vsserver object-store-server bucket lifecycle-management-rule
modify -vsserver vs1 -bucket bucket1 -rule-id rule1 -index 1 -obj-age-days
200"
```

vserver object-store-server bucket lifecycle-management-rule show

Show the lifecycle management rule

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server bucket lifecycle-management-rule show` command displays information about lifecycle management rules. If no parameters are specified, the command displays the following information about all lifecycle management rule:

- Vserver name
- Bucket name
- Lifecycle Management rule identifier
- Lifecycle Management rule index
- Action
- Enabled

To display detailed information about a single lifecycle management rule, run the command with the `-vserver -bucket-rule-id` and `-index` parameters. The detailed view provides all of the information in the default list and the following additional information:

- Link-id
- Prefix to be matched with object names
- Tags
- Minimum size of the object
- Maximum size of the object
- Lifecycle Management Rule Action
- Number of days since creation after which objects can be deleted
- Specific Date when the objects should expire cleanup object delete markers
- Number of latest non-current versions to be retained
- Number of days after which non-current versions will be deleted
- Number of days of initiation after which upload can be aborted

To display detailed information about all lifecycle management rules, run the command with the `-instance` parameter.

You can specify additional parameters to display information that matches only those parameters. For example, to display information only about lifecycle management rules with a specified rule identifier, run the command with the `-rule-id` specified rule identifier parameter.

Parameters

{ [-fields <fieldname>,...]

This specifies the fields that need to be displayed.

| [-instance] }

If this parameter is specified, the command only displays information about all lifecycle management rule entries.

[`-vserver <Vserver Name>`] - Vserver Name

If this parameter is specified, the command only displays information about all lifecycle management rule entries on the specified vservers.

[`-bucket <TextNoCase>`] - Object Store Server Bucket Name

If this parameter is specified, the command only displays information about all lifecycle management rule entries on the specified bucket.

[`-rule-id <text>`] - Lifecycle Management Rule Identifier

If this parameter is specified, the command only displays information about all lifecycle management rule entries with the specified rule identifier.

[`-index <integer>`] - Lifecycle Management Rule Index

If this parameter is specified, the command only displays information about all lifecycle management rule entries with the specified index.

[`-is-enabled {true|false}`] - Is This Rule Enabled?

If this parameter is specified, the command only displays information about lifecycle management rules that are enabled (true) or disabled (false).

[`-prefix <text>`] - Prefix to be Matched with Object Names

If this parameter is specified, the command only displays information about lifecycle management rules with the specified prefix.

[`-tags <text>,...`] - Tags in Format `<tag>` or `<tag=value>`

If this parameter is specified, the command only displays information about lifecycle management rules with the specified tags.

[`-obj-size-greater-than {<integer>[KB|MB|GB|TB|PB]}`] - Min Size of the Object

If this parameter is specified, the command only displays information about lifecycle management rules with the specified object greater than size.

[`-obj-size-less-than {<integer>[KB|MB|GB|TB|PB]}`] - Max Size of the Object

If this parameter is specified, the command only displays information about lifecycle management rules with the specified object lesser than size.

[`-action`

{`Expiration|NoncurrentVersionExpiration|AbortIncompleteMultipartUpload|ExpirationInternal`}] - Lifecycle Management Action

If this parameter is specified, the command only displays information about lifecycle management rules with the specified action.

[`-obj-age-days <integer>`] - Number of Days since Creation, After Which Current Version of Objects Can be Deleted

If this parameter is specified, the command only displays information about lifecycle management rules with the specified number of days since creation, after which objects can be deleted.

[`-obj-exp-date <MM/DD/YYYY HH:MM:SS>`] - Specific Date When the Objects Should Expire

If this parameter is specified, the command only displays information about lifecycle management rules with the specified date from when objects can expire.

[-expired-obj-del-marker {true|false}] - Cleanup Object Delete Markers

If this parameter is specified, the command only displays information about lifecycle management rules that have delete markers enabled (true) or disabled (false).

[-new-non-curr-versions <integer>] - Number of Latest Non-current Versions to Be Retained

If this parameter is specified, the command only displays information about lifecycle management rules with the specified non current versions to be allowed.

[-non-curr-days <integer>] - Number of Days after Which Non-current Versions will Be Deleted

If this parameter is specified, the command only displays information about lifecycle management rules with the specified number of days after which non-current versions can be deleted.

[-after-initiation-days <integer>] - Number of Days of Initiation, After Which Upload Can Be Aborted

If this parameter is specified, the command only displays information about lifecycle management rules with the specified number of days of initiation, after which uploads can be aborted.

Examples

The following example displays object store server bucket lifecycle management rule entries for all Vservers.

```
cluster1::> vservers object-store-server bucket lifecycle-management-rule
show
Vserver  Bucket      Rule-identifier Action-identifier Action
Enabled
-----
vs1      bucket1     rule1          1                Expiration      true
vs1      bucket1     rule2          1                Expiration      true
AbortIncompleteMultipartUpload true
vs1      bucket2     rule1          1                Expiration      true
vs1      bucket2     rule2          1                Expiration      true
AbortIncompleteMultipartUpload true
vs1      bucket3     rule1          1                Expiration      true
vs1      bucket3     rule2          1                Expiration      true
AbortIncompleteMultipartUpload true
vs2      bucket4     rule1          1                Expiration      true
vs2      bucket4     rule2          1                Expiration      true
AbortIncompleteMultipartUpload true
vs2      bucket5     rule1          1                Expiration      true
vs2      bucket5     rule2          1                Expiration      true
AbortIncompleteMultipartUpload true
10 entries were displayed.
```

The following example displays detailed information about a lifecycle management rule on bucket bucket1 on a Vserver named vs1 with rule identifier rule1 and index 1:


```
cluster1::*> vserver object-store-server bucket lifecycle-management-rule
show -vserver vs1 -bucket bucket1 -rule-id rule1 -index 1
-----
                                Vserver: vs1
                                Object Store Server Bucket Name: bucket1
                                Lifecycle Management Rule Identifier: rule1
                                Lifecycle Management Rule Index: 1
                                Link-id from the Fabriclink Links Table: 4
                                Is This Rule Enabled?: true
                                Prefix to Be Matched with Object Names: obj1/
                                Tags in Format: -
                                Minimum Size of the Object: -
                                Maximum Size of the Object: -
                                Lifecycle Management Rule Action: Expiration
                                Number of Days Since Creation After Which
                                Objects Can Be Deleted: 100
                                Specific Date When the Objects Should Expire: -
                                Cleanup Object Delete Markers: -
                                Number of Latest Non-current Versions to be
                                Retained: -
                                Number of Days after Which Non-current
                                Versions will Be Deleted: -
                                Number of Days of Initiation After Which
                                Upload Can Be Aborted: -
```

vserver object-store-server bucket policy-statement-condition create

Create a bucket policy statement condition

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

The `vserver object-store-server bucket policy-statement-condition create` command creates a single condition for a bucket policy statement in an object store server bucket.

Parameters

-vserver <Vserver Name> - Vserver Name (privilege: advanced)

This parameter specifies the name of the Vserver on which the bucket policy statement condition needs to be created for the object store server bucket.

-bucket <TextNoCase> - Object Store Server Bucket Name (privilege: advanced)

This parameter specifies the name of the object store server bucket for which the policy statement condition needs to be created. The object store bucket must already exist.

-index <integer> - Statement Index (privilege: advanced)

This parameter specifies the index of the object store server bucket policy statement in which a condition needs to be created. The index must already exist.

-operator {ip-address|not-ip-address|string-equals|string-not-equals|string-equals-ignore-case|string-not-equals-ignore-case|string-like|string-not-like|numeric-equals|numeric-not-equals|numeric-greater-than|numeric-greater-than-equals|numeric-less-than|numeric-less-than-equals} - Policy Condition Operator (privilege: advanced)

This parameter specifies the condition operator to be applied on the condition keys specified.

[-source-ips <IP Address or Subnet>,...] - List of IP Addresses with Access Allowed or Denied (privilege: advanced)

Use this parameter to specify a list of IP addresses for which the access is allowed or denied based on the operator specified.

[-usernames <text>,...] - List of Usernames with Access Allowed or Denied (privilege: advanced)

Use this parameter to specify a list of object store server users for which the access is allowed or denied based on the operator specified. The user name policy variables '\${aws:username}' can be specified here, serving as placeholders that are dynamically replaced with the actual user name during run time based on the request context.

[-prefixes <text>,...] - List of Prefixes to be Matched (privilege: advanced)

Use this parameter to specify a list of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified. The user name policy variables '\${aws:username}' can be specified here, serving as placeholders that are dynamically replaced with the actual user name during run time based on the request context.

[-max-keys <integer>,...] - List of Maximum Keys Allowed to be Fetched (privilege: advanced)

Use this parameter to specify a list of max-keys values that are allowed or denied retrieval using an S3 list operation, based on the condition operator specified.

[-delimiters <text>,...] - List of Delimiters to be Matched (privilege: advanced)

Use this parameter to specify a list of delimiters that are compared with the input delimiter value specified at the time of execution of an S3-based command, using the condition operator specified. The user name policy variables '\${aws:username}' can be specified here, serving as placeholders that are dynamically replaced with the actual user name during run time based on the request context.

Examples

The following example creates an object store server bucket policy statement condition for storage virtual machine (SVM) vs1, bucket bucket1, index 1 and ip-address as operator.

```
cluster1::*> vsriver object-store-server bucket policy-statement-condition
create -vsriver vs1 -bucket bucket1 -index 1 -operator ip-address -source
-ips 10.1.1.0/24,10.1.1.1
```

The following example creates an object store server bucket policy statement condition for storage virtual machine (SVM) vs1, bucket bucket1, index 1, string-like as operator and prefix with the user name policy variable.

```
cluster1::*> vserver object-store-server bucket policy-statement-condition
create -vserver vs1 -bucket bucket1 -index 1 -operator string-like
-prefixes ${aws:username}/*
```

The following example creates an object store server bucket policy statement condition for storage virtual machine (SVM) vs1, bucket bucket1, index 1, string-like as operator and prefix with a specific folder name policy variable.

```
cluster1::*> vserver object-store-server bucket policy-statement-condition
create -vserver vs1 -bucket bucket1 -index 1 -operator string-like
-prefixes ${aws:username}/folder/*
```

vserver object-store-server bucket policy-statement-condition delete

Delete a bucket policy statement condition

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

The `vserver object-store-server bucket policy-statement-condition delete` command deletes a condition for the specified bucket policy statement belonging to the object store server bucket.

Parameters

-vserver <Vserver Name> - Vserver Name (privilege: advanced)

This parameter specifies the name of the Vserver for which a condition belonging to a particular bucket policy statement (which belongs to the object store server bucket) you want to delete.

-bucket <TextNoCase> - Object Store Server Bucket Name (privilege: advanced)

This parameter specifies the name of the object store server bucket for which a condition belonging to a particular bucket policy statement needs to be deleted.

-index <integer> - Statement Index (privilege: advanced)

This parameter specifies the index of the object store server bucket policy for which a condition needs to be deleted.

-operator {ip-address|not-ip-address|string-equals|string-not-equals|string-equals-ignore-case|string-not-equals-ignore-case|string-like|string-not-like|numeric-equals|numeric-not-equals|numeric-greater-than|numeric-greater-than-equals|numeric-less-than|numeric-less-than-equals} - Policy Condition Operator (privilege: advanced)

This parameter specifies the condition operator of a condition which needs to be deleted.

Examples

The following example deletes an object store server bucket policy statement condition for Vserver vs1, bucket bucket1, index 1 and operator as IpAddress.

```
cluster1::*> vsserver object-store-server bucket policy-statement-condition
delete -vsserver vs1 -bucket bucket1 -index 1 -operator IpAddress
```

vserver object-store-server bucket policy-statement-condition modify

Modify a bucket policy statement condition

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

The `vserver object-store-server bucket policy-statement-condition modify` command modifies a single condition for a bucket policy statement in an object store server bucket.

Parameters

-vsserver <Vserver Name> - Vserver Name (privilege: advanced)

This parameter specifies the name of the Vserver on which the bucket policy statement condition needs to be modified for the object store server bucket.

-bucket <TextNoCase> - Object Store Server Bucket Name (privilege: advanced)

This parameter specifies the name of the object store server bucket for which the policy statement condition needs to be modified.

-index <integer> - Statement Index (privilege: advanced)

This parameter specifies the index of the object store server bucket policy statement in which a condition needs to be modified.

-operator {ip-address|not-ip-address|string-equals|string-not-equals|string-equals-ignore-case|string-not-equals-ignore-case|string-like|string-not-like|numeric-equals|numeric-not-equals|numeric-greater-than|numeric-greater-than-equals|numeric-less-than|numeric-less-than-equals} - Policy Condition Operator (privilege: advanced)

This parameter specifies the condition operator to be applied on the condition keys specified.

[-source-ips <IP Address or Subnet>,...] - List of IP Addresses with Access Allowed or Denied (privilege: advanced)

Use this parameter to specify a list of IP addresses for which the access is allowed or denied based on the operator specified.

[-usernames <text>,...] - List of Usernames with Access Allowed or Denied (privilege: advanced)

Use this parameter to specify a list of object store server users for which the access is allowed or denied based on the operator specified. The user name policy variables '\${aws:username}' can be specified here,

serving as placeholders that are dynamically replaced with the actual user name during run time based on the request context.

[`-prefixes <text>,...`] - List of Prefixes to be Matched (privilege: advanced)

Use this parameter to specify a list of prefixes that are compared with the input prefix value specified at the time of execution of an S3-based command, using the condition operator specified. The user name policy variables '`{aws:username}`' can be specified here, serving as placeholders that are dynamically replaced with the actual user name during run time based on the request context.

[`-max-keys <integer>,...`] - List of Maximum Keys Allowed to be Fetched (privilege: advanced)

Use this parameter to specify a list of max-keys values that are allowed or denied retrieval using an S3 list operation, based on the condition operator specified.

[`-delimiters <text>,...`] - List of Delimiters to be Matched (privilege: advanced)

Use this parameter to specify a list of delimiters that are compared with the input delimiter value specified at the time of execution of an S3-based command, using the condition operator specified. The user name policy variables '`{aws:username}`' can be specified here, serving as placeholders that are dynamically replaced with the actual user name during run time based on the request context.

Examples

The following example modifies an object store server bucket policy statement condition for storage virtual machine (SVM) vs1, bucket bucket1, index 1 and ip-address as operator.

```
cluster1::*> vserver object-store-server bucket policy-statement-condition
modify -vserver vs1 -bucket bucket1 -index 1 -operator ip-address -source
-ips 10.1.0.0/16,10.1.1.1
```

The following example modifies an object store server bucket policy statement condition for storage virtual machine (SVM) vs1, bucket bucket1, index 1, string-like as operator and prefix with the user name policy variable.

```
cluster1::*> vserver object-store-server bucket policy-statement-condition
modify -vserver vs1 -bucket bucket1 -index 1 -operator string-like
-prefixes "${aws:username}/*"
```

vserver object-store-server bucket policy-statement-condition show

Show the bucket policy condition

Availability: This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

Description

The `vserver object-store-server bucket policy-statement-condition show` command displays information about object store server bucket policy condition.

Parameters

`[-fields <fieldname>,...]`

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

`[-instance ] (privilege: advanced) }`

If you specify the `-instance` parameter, the command displays detailed information about all fields.

`[-vserver <Vserver Name>] - Vserver Name (privilege: advanced)`

If you specify this parameter, the command displays information on the object store server bucket policy statement conditions for the specified Vserver.

`[-bucket <TextNoCase>] - Object Store Server Bucket Name (privilege: advanced)`

If you specify this parameter, the command displays information on the object store server bucket policy statement conditions for the specified bucket.

`[-index <integer>] - Statement Index (privilege: advanced)`

If you specify this parameter, the command displays information on the object store server bucket policy statement conditions for the specified bucket policy index.

`[-operator {ip-address|not-ip-address|string-equals|string-not-equals|string-equals-ignore-case|string-not-equals-ignore-case|string-like|string-not-like|numeric-equals|numeric-not-equals|numeric-greater-than|numeric-greater-than-equals|numeric-less-than|numeric-less-than-equals}] - Policy Condition Operator (privilege: advanced)`

If you specify this parameter, the command displays information on the object store server bucket policy statement conditions that match the specified condition operator.

`[-source-ips <IP Address or Subnet>,...] - List of IP Addresses with Access Allowed or Denied (privilege: advanced)`

If you specify this parameter, the command displays information on the object store server bucket policy statement conditions that match the specified bucket policy condition source IP addresses.

`[-usernames <text>,...] - List of Usernames with Access Allowed or Denied (privilege: advanced)`

If you specify this parameter, the command displays information on the object store server bucket policy statement conditions that match the specified usernames.

`[-prefixes <text>,...] - List of Prefixes to be Matched (privilege: advanced)`

If you specify this parameter, the command displays information on the object store server bucket policy statement conditions that match the specified prefixes.

`[-max-keys <integer>,...] - List of Maximum Keys Allowed to be Fetched (privilege: advanced)`

If you specify this parameter, the command displays information on the object store server bucket policy statement conditions that match the specified max-keys.

`[-delimiters <text>,...] - List of Delimiters to be Matched (privilege: advanced)`

If you specify this parameter, the command displays information on the object store server bucket policy statement conditions that match the specified delimiters.

Examples

The following example displays information on object store server bucket policy statement conditions for vs1, bucket bb1 and index 1:

```
cluster1::*> vs1 object-store-server bucket policy-statement-condition
show -vs1 -bucket bb1 -index 1
Vserver: vs1
Bucket: bb1
```

Index	Operator	Source-IPs	Username	Prefixes	Max-Keys
1	ip-address	1.1.1.0/24	-	-	- -
1	string-like	-	user1	pref	- delim1

2 entries were displayed.

vs1 object-store-server bucket policy statement create

Create a bucket policy statement

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vs1 object-store-server bucket policy statement create` command creates a bucket policy statement for the object store server bucket.

Parameters

-vs1 <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver on which the bucket policy statement needs to be created for the object store server bucket.

-bucket <TextNoCase> - Object Store Server Bucket Name

This parameter specifies the name of the object store server bucket for which the policy statement needs to be created. The object store bucket must already exist.

[-index <integer>] - Statement Index

This parameter specifies the index of the object store server bucket policy statement. The allowed range is 1-10. This is an optional parameter.

-effect {deny|allow} - Allow or Deny Access

Use this parameter to specify whether access is allowed or denied when a user requests the specific action.

[-action <Action>,...] - Bucket Policy Action Allowed or Denied

Use this parameter to specify resource operations. The set of resource operations that the object store server supports are GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts, GetObjectTagging, PutObjectTagging, DeleteObjectTagging, PutBucketPolicy, GetBucketPolicy, DeleteBucketPolicy, GetBucketLocation, GetBucketVersioning, PutBucketVersioning, and ListBucketVersions. Wildcards are accepted for this parameter.

[-principal <Objectstore Principal>,...] - List of Users to Be Allowed or Denied Access

Validate the user requesting access against the object store server users or groups or NAS groups specified in this parameter. To gain access, the user in the context should either match one of the users or belong to one of the groups specified in this principle parameter. An object store server group is specified by adding a prefix "group/" to the group name. A NAS group is specified by adding a prefix "nasgroup/" to the group name.

[-resource <text>,...] - Bucket or Objects to Be Allowed or Denied Access

Use this parameter to specify the bucket, folder, or object for which allow or deny permissions are set. The user name policy variables '\${aws:username}' can be specified here, serving as placeholders that are dynamically replaced with the actual user name during run time based on the request context.

[-sid <SID>] - Statement Identifier

This optional parameter specifies a text comment for the object store server bucket policy statement.

Examples

The following example creates an object store server bucket policy statement for storage virtual machine (SVM) vs1 and bucket1 which specifies allowed access to a readme folder for the object store server user user1.

```
cluster1::> vsserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal
user1,group/group1,nasgroup/group2 -resource bucket1/readme/* -sid
"fullAccessToReadmeForUser1"
```

The following example creates an object store server bucket policy statement for storage virtual machine (SVM) vs1 and bucket1 which specifies allowed access to the corresponding user home directory by specifying the user name policy variable in the resource field.

```
cluster1::> vsserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action * -principal *
-resource bucket1,bucket1/${aws:username}/* -sid
"full_Access_To_Users_Home_Directory!"
```

vsserver object-store-server bucket policy statement delete

Delete a bucket policy statement

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server bucket policy statement delete` command deletes the bucket policy statement belonging to the object store server bucket.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver whose bucket policy statement (which belongs to the object store server bucket) you want to delete.

-bucket <TextNoCase> - Object Store Server Bucket Name

This parameter specifies the name of the object store server bucket whose policy needs to be deleted.

-index <integer> - Statement Index

This parameter specifies the index of the object store server bucket policy.

Examples

The following example deletes an object store server bucket policy statement with index 1 of Vserver vs1 and bucket bucket1.

```
cluster1::> vserver object-store-server bucket policy statement delete  
-vserver vs1 -bucket bucket1 -index 1
```

vserver object-store-server bucket policy statement modify

Modify a bucket policy statement

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server bucket policy statement modify` command modifies a bucket policy statement.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver for the object store server bucket for which the bucket policy statement needs to be modified.

-bucket <TextNoCase> - Object Store Server Bucket Name

This parameter specifies the name of the object store server bucket for which policy statement needs to be modified.

-index <integer> - Statement Index

This parameter specifies the index of the object store server bucket policy statement.

[-effect {deny|allow}] - Allow or Deny Access

Use this parameter to specify whether access is allowed or denied when a user requests the specific action.

[-action <Action>,...] - Bucket Policy Action Allowed or Denied

Use this parameter to specify resource operations. The set of resource operations that the object store server supports are GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts, GetObjectTagging, PutObjectTagging, DeleteObjectTagging, GetBucketLocation, PutBucketPolicy, GetBucketPolicy, DeleteBucketPolicy, GetBucketVersioning, PutBucketVersioning, and ListBucketVersions.

[-principal <Objectstore Principal>,...] - List of Users to Be Allowed or Denied Access

Validate the user requesting access against the object store server users or groups or NAS groups specified in this parameter. To gain access, the user in the context should either match one of the users or belong to one of the groups specified in this principle parameter. An object store server group is specified by adding a prefix "group/" to the group name. A NAS group is specified by adding a prefix "nasgroup/" to the group name.

[-resource <text>,...] - Bucket or Objects to Be Allowed or Denied Access

Use this parameter to specify the bucket, folder, or object for which allow or deny permissions are set. The user name policy variables '\${aws:username}' can be specified here, serving as placeholders that are dynamically replaced with the actual user name during run time based on the request context.

[-sid <SID>] - Statement Identifier

This optional parameter specifies a text comment for the object store server bucket policy statement.

Examples

The following example modifies an object store server bucket policy statement for storage virtual machine (SVM) vs1 and bucket1 which specifies allowed access to a readme folder for the object store server user user1.

```
cluster1::> vsserver object-store-server bucket policy statement modify
-vserver vs1 -bucket bucket1 -index 1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "full_Access_To_Readme_For_User1!"
```

The following example modifies an object store server bucket policy statement for storage virtual machine (SVM) and bucket1 which specifies allowed access to the corresponding user home directory by specifying the user name policy variable in the resource field.

```
cluster1::> vsserver object-store-server bucket policy statement modify
-vserver vs1 -bucket bucket1 -index 1 -effect allow -action * -principal *
-resource bucket1,bucket1/${aws:username}/* -sid
"full_Access_To_Users_Home_Directory!"
```

vserver object-store-server bucket policy statement show

Show the bucket policy

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server bucket policy statement show` command displays information about object store server bucket policy.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver Name

If you specify this parameter, the command displays information on the object store server bucket policy statements for the specified Vserver.

[-bucket <TextNoCase>] - Object Store Server Bucket Name

If you specify this parameter, the command displays information on the object store server bucket policy statements for the specified bucket.

[-index <integer>] - Statement Index

If you specify this parameter, the command displays information on the object store server bucket policy statements that match the specified index.

[-effect {deny|allow}] - Allow or Deny Access

If you specify this parameter, the command displays information on the object store server bucket policy statements that match the specified effect.

[-action <Action>,...] - Bucket Policy Action Allowed or Denied

If you specify this parameter, the command displays information on the object store server bucket policy statements that match the specified action.

[-principal <Objectstore Principal>,...] - List of Users to Be Allowed or Denied Access

If you specify this parameter, the command displays information on the object store server bucket policy statements that match the specified bucket principal.

[-resource <text>,...] - Bucket or Objects to Be Allowed or Denied Access

If you specify this parameter, the command displays information on the object store server bucket policy statements that match the specified resource.

[-sid <SID>] - Statement Identifier

If you specify this parameter, the command displays information on the object store server bucket policy statements that match the specified sid.

Examples

The following example displays information on object store server bucket policy statements for vs1 and bucket bucket1:

```
cluster1::> vs1 object-store-server bucket policy show -vs1
-bucket bucket1
Vserver      Bucket      Index Effect Action      Principal      Resource
-----
vs1
      bucket1      1 allow  GetObject,  user1      bucket1/
      PutObject,
      DeleteObject
      , ListBucket
      bucket1      2 allow  GetObject  user2      bucket1/*
2 entries were displayed.
```

The following example displays detailed information of the object store server bucket policy statement associated with Vserver vs1 and bucket bucket1:

```
cluster1::> vs1 object-store-server bucket policy show -vs1
-bucket bucket1 -index 1
Vserver      :vs1
      Bucket      :bucket1
      Index      :1
      Effect      :allow
      Action      :GetObject
      Principal   :user-2
      Resource    :bucket1/readme/*
      Sid         :Allow_Access_To_User_user1_For_GetObject!
```

vs1 object-store-server bucket snapshot create

Create a snapshot for the S3 bucket.

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vs1 object-store-server bucket snapshot create` command creates a snapshot of a specified S3 bucket.

Parameters

-vserver <vserver name> - Vserver

This specifies the name of the Vserver that contains the S3 bucket for which the snapshot is to be created.

-bucket <TextNoCase> - S3 Bucket Name

This specifies the name of the S3 bucket where the snapshot is to be created.

-snapshot <TextNoCase> - Snapshot Name

This specifies the name of the snapshot that is to be created.

[-foreground <true>] - Run Operation in the Foreground

This specifies whether the operation runs in the foreground. The default setting is `true` (the operation runs in the foreground). If `true`, the command will wait until the operation is finished. If `false`, the command will return immediately and the operation will complete in the background.

Examples

The following example creates a snapshot named `bucket-1-snap` on S3 bucket `bucket-1` on Vserver named `vs0`.

```
cluster1::> vsserver object-store-server bucket snapshot create -vserver  
vs0 -bucket bucket-1 -snapshot bucket-1-snap
```

vserver object-store-server bucket snapshot delete

Delete a snapshot for the S3 bucket.

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vsserver object-store-server bucket snapshot delete` command deletes a snapshot from a specified S3 bucket.

Parameters

-vserver <vserver name> - Vserver

This specifies the name of the Vserver that contains the S3 bucket for which the snapshot will be deleted.

-bucket <TextNoCase> - S3 Bucket Name

This specifies the name of the S3 bucket for which the snapshot will be deleted.

-snapshot <TextNoCase> - Snapshot Name

This specifies the name of the snapshot that is to be deleted.

[`-foreground <true>`] - Run Operation in the Foreground

This specifies whether the operation runs in the foreground. The default setting is `true` (the operation runs in the foreground). If `true`, the command will wait until the operation is finished. If `false`, the command will return immediately and the operation will complete in the background.

Examples

The following example deletes a snapshot named `bucket-1-snap` on S3 bucket named `bucket-1` on Vserver named `vs0`.

```
cluster1::> vsserver object-store-server bucket snapshot delete -vserver
vs0 -bucket bucket-1 -snapshot bucket-1-snap
```

vsserver object-store-server bucket snapshot show

Display a list of snapshots associated with the S3 bucket.

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vsserver object-store-server bucket snapshot show` command displays information about snapshots created for S3 buckets.

Parameters

{ [`-fields <fieldname>`,...]

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [`-instance`] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[`-vserver <vserver name>`] - Vserver

If you specify this parameter, the command displays information only about the snapshots located for the specified Vserver.

[`-bucket <TextNoCase>`] - S3 Bucket Name

If you specify this parameter, the command displays information only about the snapshots located for the specified S3 buckets.

[`-snapshot <TextNoCase>`] - Snapshot Name

If you specify this parameter, the command displays information only snapshots matching the specified name.

[`-create-time <Date>`] - Snapshot Creation Time

If this parameter is specified, the command displays information only for the snapshots that match the specified creation time. The create time format is `<day> <month> <day of month> <hour>:<min>:<sec>`

<year>.

[`-instance-uuid <UUID>`] - Snapshot Instance UUID

If this parameter is specified, the command displays information only for the snapshots that have the specified instance UUID.

Examples

The following example displays information for all snapshots associated with Vserver vs0.

```
cluster1::> vsserver object-store-server bucket snapshot show
Vserver   Bucket      Snapshot                                Create Time
-----
vs0       bucket      snap1                                Wed May 15 19:47:04
2024
vs0       bucket      snap2                                Thu May 16 03:21:26
2024
vs0       bucket      snap3                                Thu May 16 17:02:03
2024
3 entries were displayed.
```

The following example displays detailed information of the snapshots associated with Vserver vs0:

```
cluster1::> vsserver object-store-server bucket snapshot show -instance
Vserver Name: vs0
    Bucket Name: bucket
    Snapshot Name: snap1
    Create Time: Wed May 15 19:47:04 2024
    Instance Uuid: 1639d804-5245-4a64-af89-093891b251a1
Vserver Name: vs0
    Bucket Name: bucket
    Snapshot Name: snap2
    Create Time: Thu May 16 03:21:26 2024
    Instance Uuid: dec5daf6-28f8-4eef-89f7-a9256de17d86
Vserver Name: vs0
    Bucket Name: bucket
    Snapshot Name: snap3
    Create Time: Thu May 16 17:02:03 2024
    Instance Uuid: aeed7372-a16f-4aad-8e23-708267a109fb
3 entries were displayed.
```

The following example displays information for all snapshots created at or after "Thu May 16 03:21:26 2024":

```
cluster1::> vservers object-store-server bucket snapshot show -create-time
>="Thu May 16 03:21:26 2024"
Vserver  Bucket      Snapshot              Create Time
-----  -
vs0      bucket      snap2                Thu May 16 03:21:26
2024
vs0      bucket      snap3                Thu May 16 17:02:03
2024
2 entries were displayed.
```

vserver object-store-server bucket snapshot restore show

Displays the progress of ongoing snapshot restore operation of S3 buckets.

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server bucket snapshot restore show` command displays information about the progress of ongoing snapshot restore operations in S3 bucket(s).

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver Name

If you specify this parameter, the command displays information only about the snapshot restore operations for the specified Vserver.

[-bucket <TextNoCase>] - S3 Bucket Name

If you specify this parameter, the command displays information only about the snapshot restore operations for the specified S3 bucket.

[-snapshot <TextNoCase>] - Snapshot Name

If you specify this parameter, the command displays information only about the snapshot restore operation matching the specified snapshot.

[-restore-status <Bucket snapshot restore progress State>] - Restore Progress Status

If you specify this parameter, the command displays information only about the snapshot restore operation matching the specified restore-status.

[-restore-progress <percent>] - Restore Progress

If you specify this parameter, the command displays information only about the snapshot restore operation matching the specified restore-progress.

[-objects-remaining <integer>] - Remaining Objects to be Restored

If you specify this parameter, the command displays information only about the snapshot restore operation matching the specified objects-remaining.

Examples

The following example displays information for all restore operations in the cluster.

```
cluster1::> vservers object-store-server bucket snapshot restore show
Vserver  Bucket      Snapshot      Status      Progress  Objects Remaining
-----
vs0      buck1       snap1         restoring   98%       1092
vs1      buck2       snap2         restoring   47%       19287
vs2      buck3       snap3         preparing   0%        2910
vs3      buck4       snap4         done        100%      0
4 entries were displayed.
```

The following example displays detailed information of snapshot restore for a particular bucket:

```
cluster1::> vservers object-store-server bucket snapshot restore show
-vserver vs0 -bucket buck1
(vservers object-store-server bucket snapshot restore show)
Vserver Name: vs0
      S3 Bucket Name: buck1
      Snapshot Name: snap1
      Restore Progress Status: done
      Restore Progress: 100%
      Remaining Objects to be restored: 0
```

The following example displays information for all restore operations for a particular vservers.

```
cluster1::> vserver object-store-server bucket snapshot restore show
-vserver vs0
```

Vserver	Bucket	Snapshot	Status	Progress	Objects Remaining
vs0	buck1	snap1	restoring	98%	1092
vs0	buck2	snap2	restoring	47%	19287
vs0	buck3	snap3	preparing	0%	2910
vs0	buck4	snap4	done	100%	0

4 entries were displayed.

vserver object-store-server bucket snapshot restore start

Restore a snapshot for the S3 bucket.

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server bucket snapshot restore start` command restores a snapshot for a specified S3 bucket.

Parameters

-vserver <vserver name> - Vserver

This specifies the name of the Vserver that contains the S3 bucket for which the snapshot will be restored.

-bucket <TextNoCase> - S3 Bucket Name

This specifies the name of the S3 bucket for which the snapshot will be restored.

-snapshot <TextNoCase> - Snapshot Name

This specifies the name of the snapshot that is to be restored.

[-foreground <true>] - Run Operation in the Foreground

This specifies whether the operation runs in the foreground. The default setting is `true` (the operation runs in the foreground). If `true`, the command will wait until the operation is finished. If `false`, the command will return immediately and the operation will complete in the background.

Examples

The following example restores a snapshot named `bucket-1-snap` on S3 bucket named `bucket-1` on Vserver named `vs0`.

```
cluster1::> vserver object-store-server bucket snapshot restore start
-vserver vs0 -bucket bucket-1 -snapshot bucket-1-snap
```

vserver object-store-server group create

Create an Object Store Server Group

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server group create` command creates an object store group.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver on which to create the object store group. The Vserver must already exist.

-gid <integer> - Group ID

This parameter specifies a unique ID used to identify a particular object store group.

-name <TextNoCase> - Group Name

This parameter specifies the name of the object store group.

[-users <TextNoCase>, ...] - List of Users Belonging to the Group

Use this parameter to specify the list of object store users who belong to the object store group.

[-policies <TextNoCase>, ...] - List of Policies Attached to the Group

Use this parameter to specify the list of object store policies that are attached to the object store group.

[-comment <text>] - Group Description

This optional parameter specifies a text comment for the object store group.

Examples

The following example creates an object store group named `user_group` for Vserver `vs1`:

```
cluster1:> vserver object-store-server group create -vserver vs1 -name
user_group -users user1,user2 -policies policy1,policy2 -comment
"UserGroup1"
```

vserver object-store-server group delete

Delete an Object Store Server Group

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server group delete` command deletes an object store group.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver for the object store server you want to delete.

-gid <integer> - Group ID

This parameter specifies the ID of the object store group you want to delete.

Examples

The following example deletes an object store group for Vserver vs1:

```
cluster1::> vserver object-store-server group delete -vserver vs1 -gid 1
```

vserver object-store-server group modify

Modify an Object Store Server Group

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server group modify` command modifies an object store group.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver for the object store group which you want to modify.

-gid <integer> - Group ID

This parameter specifies the ID of the object store group.

[-name <TextNoCase>] - Group Name

This parameter specifies the name of the object store group.

[-users <TextNoCase>, ...] - List of Users Belonging to the Group

Use this parameter to specify the list of object store users who belong to the object store group.

[-policies <TextNoCase>, ...] - List of Policies Attached to the Group

Use this parameter to specify the list of object store policies that are attached to the object store group.

[-comment <text>] - Group Description

This parameter specifies the text comment for the object store group.

Examples

The following example modifies the comment of the object store group for Vserver vs1:

```
cluster1::> vsserver object-store-server group modify -vsserver vs1 -gid 3  
-comment "UserGroup"
```

vsserver object-store-server group show

Display Object Store Server Groups

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vsserver object-store-server group show` command displays information about the object store group.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vsserver <Vserver Name>] - Vserver Name

If you specify this parameter, the command displays information on the object store server groups for the specified Vserver.

[-gid <integer>] - Group ID

If you specify this parameter, the command displays information on the object store server group that match the specified group ID.

[-name <TextNoCase>] - Group Name

If you specify this parameter, the command displays information on the object store server groups that match the specified group name.

[-users <TextNoCase>,...] - List of Users Belonging to the Group

If you specify this parameter, the command displays information on the object store server groups that match the specified user.

[-policies <TextNoCase>,...] - List of Policies Attached to the Group

If you specify this parameter, the command displays information on the object store server groups that match the specified policy.

[-comment <text>] - Group Description

If you specify this parameter, the command displays information on the object store server groups that match the specified comment.

Examples

The following example displays information for all object store groups in admin privilege:

```
cluster1::> vsriver object-store-server group show
Vserver      Group ID  Group Name      Users              Policies
-----
vs1          3  UserGroup      user1, user2      policy1, policy2
    Comment: User_Privileges
vs1          4  AdminGroup     admin1, admin2    policy1, policy2
    Comment: Admin_Privileges
    2 entries were displayed.
```

The following example displays information for a particular object store group associated with vsriver vs1:

```
cluster1::> vsriver object-store-server group show -vsriver vs1 -gid 5
Vserver Name      :vs1
    Group ID       :5
    Group Name     :User-Group
    Users          :user_1, user_2
    Policies       :Policy1, Policy2, Policy3
    Comment        :User group
```

vsriver object-store-server policy create

Create a policy

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vsriver object-store-server policy create` command creates an object store policy.

Parameters

-vsriver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver on which to create the object store policy. The Vserver must already exist.

-policy <TextNoCase> - Policy Name

This parameter specifies the name of the object store policy.

[-comment <text>] - Comment

This optional parameter specifies a text comment for the object store policy.

Examples

The following example creates an object store policy named Policy_1 for Vserver vs1:

```
cluster1::> vserver object-store-server policy create -vserver vs1 -policy
Policy_1 -comment "ReadAccessForBucket1"
```

vserver object-store-server policy delete

Delete a policy

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server policy delete` command deletes an object store policy.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver for the object store server you want to delete.

-policy <TextNoCase> - Policy Name

This parameter specifies the name of the object store policy you want to delete.

Examples

The following example deletes an object store policy for Vserver vs1:

```
cluster1::>vserver object-store-server policy delete -vserver vs1 -policy
Policy_2
```

vserver object-store-server policy modify

Modify a policy

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server policy modify` command modifies an object store policy.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver for the object store policy you want to modify.

-policy <TextNoCase> - Policy Name

This parameter specifies the name of the object store policy.

[-comment <text>] - Comment

This parameter specifies the text comment for the object store policy.

Examples

The following example modifies the comment of the object store policy for Vserver vs1:

```
cluster1::> vsriver object-store-server policy modify -policy Policy_1  
-comment "Read_Access_for_Bucket2"
```

vserver object-store-server policy show

Show the policy

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server policy show` command displays information about the object store policy.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver Name

If you specify this parameter, the command displays information on the object store server policies for the specified Vserver.

[-policy <TextNoCase>] - Policy Name

If you specify this parameter, the command displays information on the object store server policies that match the specified policy name.

`[-is-read-only {true|false}] - Is Read-Only?`

If you specify this parameter, the command displays information on the object store server policies that match the specified read only field.

`[-comment <text>] - Comment`

If you specify this parameter, the command displays information on the object store server policies that match the specified comment.

Examples

The following example displays information for all object store policies in admin privilege:

```
cluster1::> vsriver object-store-server policy show
Vserver      Name                Is Read-Only Comment
-----
vs1          FullAccess          true          Read Only Policy: To allow
full access to S3 resources
vs1          NoS3Access          true          Read Only Policy: To deny
access to all S3 resources
vs1          Policy_1            false         Read_access_for_bucket1
vs1          Policy_2            false         Read_access_for_bucket2
vs1          ReadOnlyAccess      true          Read Only Policy: To allow
read-only access to S3 resources
5 entries were displayed.
```

The following example displays information for a particular object store policy associated with Vserver vs1:

```
cluster1::> vsriver object-store-server policy show -policy Policy_1
Vserver      Name                Is Read-Only Comment
-----
vs1          Policy_1            false         Read_access_for_bucket1
```

vsvrer object-store-server policy statement create

Create a Policy Statement

Availability: This command is available to *cluster* and *Vsvrer* administrators at the *admin* privilege level.

Description

The `vsvrer object-store-server policy statement create` command creates a policy statement for the object store server policy.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver on which the policy statement needs to be created for the object store server policy.

-policy <TextNoCase> - Policy Name

This parameter specifies the name of the object store server policy for which the policy statement needs to be created. The object store policy must already exist.

-index <integer> - Statement Index

This parameter specifies the unique index used to identify the particular object store server policy statement.

-effect {deny|allow} - Allow or Deny Access

Use this parameter to specify whether or not access is allowed or denied when a user requests a specific action.

-actions <Action>, ... - Policy Actions

Use this parameter to specify resource operations. The set of resource operations that the object store server supports are GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads, ListMultipartUploadParts, GetObjectTagging, PutObjectTagging, DeleteObjectTagging, CreateBucket, DeleteBucket, GetBucketLocation, GetBucketVersioning, PutBucketVersioning, and ListBucketVersions. Wildcards are accepted for this parameter. If all operations must be specified, then use the wildcard character * to specify it. The default actions are GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts, GetObjectTagging, PutObjectTagging, DeleteObjectTagging, GetBucketLocation, PutBucketPolicy, GetBucketPolicy, DeleteBucketPolicy, GetBucketVersioning, PutBucketVersioning, and ListBucketVersions.

-resource <text>, ... - Buckets or Objects

Use this parameter to specify the bucket, folder, or object for which allow or deny permissions are set. The user name policy variables '\${aws:username}' can be specified here, serving as placeholders that are dynamically replaced with the actual user name during run time based on the request context.

[-sid <SID>] - Statement Identifier

This optional parameter specifies a text comment for the object store server policy statement. The parameter name "sid" refers to statement identifier.

Examples

The following example creates an object store server policy statement for storage virtual machine (SVM) vs1 and Policy_1 which specifies allowed access to bucket1 resources.

```
cluster1::> vsserver object-store-server policy statement create -vserver
vs1 -policy Policy_1 -effect allow -actions
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,List
AllMyBuckets,GetBucketLocation -resource bucket1/* -sid
"FullAccesToBucket1"
```

The following example creates an object store server policy statement for storage virtual machine (SVM) vs1

and Policy_1 which specifies allowed access to the corresponding user home directory by specifying the user name policy variable in the resource field.

```
cluster1::> vsserver object-store-server policy statement create -vsserver
vs1 -policy Policy_1 -effect allow -actions * -resource
bucket1,bucket1/${aws:username}/* -sid "fullAccessToUsersHomeDirectory"
```

vserver object-store-server policy statement delete

Delete a Policy Statement

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vsserver object-store-server policy statement delete` command deletes the policy statement belonging to the object store server policy.

Parameters

-vsserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver whose policy statement you want to delete.

-policy <TextNoCase> - Policy Name

This parameter specifies the name of the object store server policy whose policy statement needs to be deleted.

-index <integer> - Statement Index

This parameter specifies the index of the object store server policy statement.

Examples

The following example deletes an object store server policy statement with index 1 of Vserver vs1 and policy Policy_1.

```
cluster1::> vsserver object-store-server policy statement delete -vsserver
vs1 -policy Policy_1 -index 1
```

vserver object-store-server policy statement modify

Modify a Policy Statement

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server policy statement modify` command modifies a policy statement.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver for the object store server policy for which the policy statement needs to be modified.

-policy <TextNoCase> - Policy Name

This parameter specifies the name of the object store server policy for the policy statement that needs to be modified.

-index <integer> - Statement Index

This parameter specifies the index of the object store server policy statement.

[-effect {deny|allow}] - Allow or Deny Access

Use this parameter to specify whether or not access is allowed or denied when a user requests a specific action.

[-actions <Action>,...] - Policy Actions

Use this parameter to specify resource operations. The set of resource operations that the object store server supports are `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `GetBucketAcl`, `GetObjectAcl`, `ListAllMyBuckets`, `ListBucketMultipartUploads`, `ListMultipartUploadParts`, `GetObjectTagging`, `PutObjectTagging`, `DeleteObjectTagging`, `CreateBucket`, `DeleteBucket`, `GetBucketLocation`, `PutBucketPolicy`, `GetBucketPolicy`, `DeleteBucketPolicy`, `GetBucketVersioning` and `PutBucketVersioning`.

[-resource <text>,...] - Buckets or Objects

Use this parameter to specify the bucket, folder, or object for which allow or deny permissions are set. The user name policy variables `'${aws:username}'` can be specified here, serving as placeholders that are dynamically replaced with the actual user name during run time based on the request context.

[-sid <SID>] - Statement Identifier

This optional parameter specifies a text comment for the object store server policy statement.

Examples

The following example modifies an object store server policy statement for storage virtual machine (SVM) `vs1` and `Policy_1` which specifies allowed access to `bucket1` resources.

```
cluster1::> vserver object-store-server policy statement modify -vserver
vs1 -policy Policy_1 -index 5 -effect allow -actions
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,List
AllMyBuckets,GetBucketLocation -resource bucket1/* -sid
FullAccesToBucket1Resources
```

The following example modifies an object store server policy statement for storage virtual machine (SVM) `vs1`

and Policy_1 which specifies allowed access to the corresponding user home directory by specifying the user name policy variable in the resource field.

```
cluster1::> vsserver object-store-server policy statement modify -vsserver
vs1 -policy Policy_1 -index 5 -effect allow -actions * -resource
bucket1,bucket1/${aws:username}/* -sid "fullAccessToUsersHomeDirectory"
```

vsserver object-store-server policy statement show

Show Policy Statements

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vsserver object-store-server policy statement show` command displays information about object store server policy statements.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vsserver <Vserver Name>] - Vserver Name

If you specify this parameter, the command displays information on the object store server policy statements for the specified Vserver.

[-policy <TextNoCase>] - Policy Name

If you specify this parameter, the command displays information on the object store server policy statements for the specified policy.

[-index <integer>] - Statement Index

If you specify this parameter, the command displays information on the object store server policy statements that match the specified index.

[-effect {deny|allow}] - Allow or Deny Access

If you specify this parameter, the command displays information on the object store server policy statements that match the specified effect.

[-actions <Action>,...] - Policy Actions

If you specify this parameter, the command displays information on the object store server policy statements that match the specified action.

[-resource <text>,...] - Buckets or Objects

If you specify this parameter, the command displays information on the object store server policy statements that match the specified resource.

[-sid <SID>] - Statement Identifier

If you specify this parameter, the command displays information on the object store server policy statements that match the specified sid.

Examples

The following example displays information on object store server policy statements for Vserver vs1 and policy Policy_1:

```
cluster1::> vsriver object-store-server policy statement show -vserver vs1
-policy Policy_1
```

Vserver	Policy	Index	Effect	Actions	Resources
vs1	Policy_1	1	allow	ListBucket	*
	Policy_1	5	allow	GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListAllMyBuckets	bucket1/*

Sid: FullAccesToBucket1
2 entries were displayed.

The following example displays detailed information of the object store server policy statement associated with Vserver vs1 and policy Policy_1:

```
cluster1::> vsriver object-store-server policy statement show -vserver vs1
-policy Policy_1 -index 5
```

Vserver: vs1
Policy: Policy_1
Index: 5
Effect: allow
Actions: GetObject, PutObject, DeleteObject, ListBucket,
GetBucketAcl, GetObjectAcl, ListAllMyBuckets
Resource: bucket1/*
Sid: FullAccesToBucket1

vserver object-store-server user create

Create an object store server user

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server user create` command creates an object store user. This will generate an access-key and a secret-key to be used for aws v4 authentication. The user keys generated will be shown as part of the response of this command. Note that the secret-key is not retrievable and should be noted down. It will not be shown as part of the `vserver object-store-server user show` command. If the secret-key is lost, the user keys will need to be regenerated.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver on which to create the object store user. The Vserver must already exist.

-user <TextNoCase> - Object Store Server User Name

This parameter specifies the name of the object store user. If user is a part of Active Directory, user must be specified in User Principal Name (UPN) format.

[-comment <text>] - Object Store Server User Description

This optional parameter specifies a text comment for the object store user.

[-access-key <text>] - Access Key for the Object Store Server User

This optional parameter specifies the access key for the object store user.

[-secret-key <text>] - Secret Key for the Object Store Server User

This optional parameter specifies the secret key for the object store user.

[-key-time-to-live {P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W}] - Time Period After Which User Keys Expire

This optional parameter specifies a time period after which the object store user keys expire and are no longer valid. If the value specified is zero or no value is specified, then the user keys will not expire.

Examples

The following example creates an object store user `user1` for Vserver `vs1`.

```
cluster1::> vsserver object-store-server user create -vsserver vs1 -user
user1

Vserver: vs1
User: user1
Access Key: DUMMYACCESSKEY123
Secret Key: dummy_secret_key_1234_abcd__lkfj
Warning: The secret key won't be displayed
again. Save this key for future use.
```

The following example creates an object store user user1, with the specified keys, for Vserver vs1.

```
cluster1::> vsserver object-store-server user create -vsserver vs1 -user
user1 -access-key DUMMYACCESSKEY123 -secret-key
dummy_secret_key_1234_abcd__lkfj

Vserver: vs1
User: user1
Access Key: DUMMYACCESSKEY123
Secret Key: dummy_secret_key_1234_abcd__lkfj
Warning: The secret key won't be displayed
again. Save this key for future use.
```

The following example creates an object store user user1, for Vserver vs1, where user1 is a member of active directory.

```
cluster1::> vsserver object-store-server user create -vsserver vs1 -user
user1@domain1.com -access-key DUMMYACCESSKEY123 -secret-key
dummy_secret_key_1234_abcd__lkfj

Vserver: vs1
User: user1@domain1.com
Access Key: DUMMYACCESSKEY123
Secret Key: dummy_secret_key_1234_abcd__lkfj
Warning: The secret key won't be displayed
again. Save this key for future use.
```

Related Links

- [vsserver object-store-server user show](#)

vsserver object-store-server user delete-keys

Delete keys for an object store user

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server user delete-keys` command deletes the access-key and secret-key for an object store user. To regenerate the keys for the user again, use the [vserver object-store-server user regenerate-keys](#) command.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the SVM on which the keys should be deleted for the object store user. The object store user must already exist.

-user <TextNoCase> - Object Store Server User Name

This parameter specifies the name of the object store user.

Examples

The following example deletes the keys for object store user for the SVM vs1.

```
cluster1::> vserver object-store-server user delete-keys -vserver vs1
-user user1
```

Related Links

- [vserver object-store-server user regenerate-keys](#)

vserver object-store-server user delete

Delete an object store server user

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server user delete` command deletes an object store user.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver for the object store server you want to delete.

-user <TextNoCase> - Object Store Server User Name

This parameter specifies the name of the object store user you want to delete.

Examples

The following example deletes an object store user for Vserver vs1.

```
cluster1::> vserver object-store-server user delete -vserver vs1 -user user1
```

vserver object-store-server user modify

Modify an object store server user

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server user modify` command modifies an object store user.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the SVM for the object store user which you want to modify.

-user <TextNoCase> - Object Store Server User Name

This parameter specifies the name of the object store user.

[-comment <text>] - Object Store Server User Description

This parameter specifies the text comment for the object store user.

Examples

The following example modifies the object store user for the SVM vs1:

```
cluster1::> vserver object-store-server user modify -vserver vs1 -user user1 -comment testuser
```

vserver object-store-server user regenerate-keys

Regenerate keys for object store user

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server user regenerate-keys` command regenerates a new access-key and secret-key for an object store user. The user keys generated will be shown as part of the command response. Note that the secret-key is not retrievable and should be noted down. It will not be shown as part of the [vserver object-store-server user show](#) command. If the secret-key is lost, the user keys will need to be regenerated.

Parameters

-vserver <Vserver Name> - Vserver Name

This parameter specifies the name of the Vserver on which the keys should be generated for the object store user. The object store user must already exist.

-user <TextNoCase> - Object Store Server User Name

This parameter specifies the name of the object store user.

[-key-time-to-live {P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P[<integer>W]}] - Time Period after Which User Keys Expire

This optional parameter specifies a time period after which the object store user keys expire and are no longer valid. If the value specified is zero, then the user keys will not expire.

[-access-key <text>] - Access Key for the Object Store User

This optional parameter specifies the access key for the object store user.

[-secret-key <text>] - Secret Key for the Object Store User

This optional parameter specifies the secret key for the object store user.

Examples

The following example regenerates the keys for object store user for Vserver vs1.

```
cluster1::> vsserver object-store-server user regenerate-keys -vserver vs1
-user user1

Vserver: vs1
User: user1
Access Key: DUMMYACCESSKEY123
Secret Key: dummy_secret_key_1234_abcd__lkfj
Warning: The secret key won't be displayed
again. Save this key for future use.
```

The following example sets the new keys, that are passed from the input, for object store user for Vserver vs1.

```
cluster1::> vsserver object-store-server user regenerate-keys -vserver vs1
-user user1 -access-key DUMMYACCESSKEY123 -secret-key
dummy_secret_key_1234_abcd__lkfj

Vserver: vs1
User: user1
Access Key: DUMMYACCESSKEY123
Secret Key: dummy_secret_key_1234_abcd__lkfj
Warning: The secret key won't be displayed
again. Save this key for future use.
```

Related Links

- [vserver object-store-server user show](#)

vserver object-store-server user show

Display object store server users

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `vserver object-store-server user show` command displays information about the object store user. The user secret-key will not be shown as part of the response. It is shown only when user is created or user keys are regenerated.

Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver Name

If you specify this parameter, the command displays information only about the object store users for the specified SVM.

[-user <TextNoCase>] - Object Store Server User Name

If you specify this parameter, the command displays information only for object store users that match the specified object store user name.

[-id <integer>] - Object Store Server User ID

If you specify this parameter, the command displays information only for object store users that match the specified user id.

[-comment <text>] - Object Store Server User Description

If you specify this parameter, the command displays information only for object store users that match the specified comment field.

[-access-key <text>] - Access Key for the Object Store Server User

If you specify this parameter, the command displays information only for object store users that match the specified access key.

[-key-time-to-live {P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W}] - Time Period After Which User Keys Expire

If you specify this parameter, the command displays information only for object store users that match the specified key time to live value.

[-key-expiry-time {MM/DD/YYYY HH:MM:SS [{+|-}hh:mm]}] - Date And Time When User Keys Expire

If you specify this parameter, the command displays information only for object store users that match the specified key expiry date value.

Examples

The following example displays information of all object store users in admin privilege:

```
cluster1::> vsserver object-store-server user show
Vserver      User              ID      Key Time To Live Key Expiry Time
-----
vs1          user1             1       1h              2/6/2023
13:28:50
Comment: testuser
vs1          user2             2       -               -
vs1          user@domain1.com  3       -               -
2 entries were displayed.
```

The following example displays information of a particular object store user associated with the SVM vs1 in admin privilege:

```
cluster1::> vsserver object-store-server user show -vserver vs1 -user user1
Vserver Name: vs1
Object Store Server User Name: user1
Object Store Server User ID: 1
Object Store Server User Description: testuser
Access Key for the Object Store Server User: 5HBRV20PWWX7IIHKYRRN
Time Period After Which User Keys Expire: 1h
Date And Time When User Keys Expire: 2/6/2023 13:28:50
```

The following example displays information of all object store users in advanced privilege:

```
cluster1::*> vsserver object-store-server user show
Vserver      User              ID      Key Time To Live Key Expiry Time
-----
vs1          root              0       -               -
Access Key: -
Comment: Root User
vs1          user2             2       99999h0m0s      7/6/2034 23:40:54
Access Key: 2K4PL22JQV5L2WA564TB
Comment:
2 entries were displayed.
```

The following example displays information of a particular object store user associated with the SVM vs1 in advanced privilege. Note that user secret key is not shown as part of this command:

```
cluster1::*> vserver object-store-server user show -vserver vs1 -user  
user1
```

```
          Vserver Name: vs1
```

```
    Object Store Server User Name: user1
```

```
      Object Store Server User ID: 1
```

```
Object Store Server User Description: testuser
```

```
Access Key for the Object Store Server User: 5HBRV20PWWX7IIHKYRRN
```

```
Time Period After Which User Keys Expire: 1h
```

```
    Date And Time When User Keys Expire: 2/6/2023 13:28:50
```

Copyright information

Copyright © 2026 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.