



# VAST Cluster 5.3 CLI Command Reference

18 June 2025

Always check [support.vastdata.com](https://support.vastdata.com) for the latest

# Contents

<b>About this Guide.</b>	<b>14</b>
About this VAST CLI Command Reference.	14
Typographic Conventions in this Guide.	14
<b>activedirectory commands</b>	<b>16</b>
activedirectory change_machine_account_password.	16
activedirectory create	16
activedirectory delete	25
activedirectory list	25
activedirectory modify	27
activedirectory remove	37
activedirectory show	37
activedirectory show_ad_domains	38
activedirectory show_ad_gcs	39
activedirectory show_joined_domain_dcs.	40
<b>alarm commands</b>	<b>42</b>
alarm clear.	42
alarm delete.	42
alarm list	42
alarm show	44
<b>apitoken commands.</b>	<b>45</b>
apitoken create	45
apitoken list	46
apitoken modify	47
apitoken revoke	48
apitoken show	49
<b>blockhost commands.</b>	<b>51</b>
blockhost create	51
blockhost delete	51
blockhost list	52
blockhost modify	53
blockhost show	54
<b>blockmapping commands</b>	<b>56</b>
blockmapping list.	56
blockmapping map_host_to_volumes.	56
blockmapping map_volume_path	57

blockmapping map_volume_to_hosts . . . . .	58
blockmapping show . . . . .	59
blockmapping unmap_host_volumes . . . . .	60
blockmapping unmap_volume_hosts . . . . .	60
<b>callhomeconfig commands . . . . .</b>	<b>62</b>
callhomeconfig list . . . . .	62
callhomeconfig modify . . . . .	62
callhomeconfig register-cluster . . . . .	67
callhomeconfig send . . . . .	68
callhomeconfig show . . . . .	68
<b>carrier commands . . . . .</b>	<b>70</b>
carrier activate . . . . .	70
carrier deactivate . . . . .	70
<b>cbox commands . . . . .</b>	<b>71</b>
cbox led . . . . .	71
cbox list . . . . .	71
cbox modify . . . . .	72
cbox refresh_uid . . . . .	72
cbox show . . . . .	73
<b>cluster commands . . . . .</b>	<b>74</b>
cluster close-protocol-handle . . . . .	74
cluster list-locks . . . . .	75
cluster list-snapshotted-paths-remote . . . . .	76
cluster list-clone-snapshotted-paths-remote . . . . .	76
cluster list-tenants-remote . . . . .	77
cluster list-open-protocol-handles . . . . .	77
cluster modify . . . . .	79
cluster release-lock . . . . .	88
cluster rotate-master-encryption-group-key . . . . .	89
cluster run-upgrade-validations . . . . .	90
cluster set-password . . . . .	90
cluster show . . . . .	91
cluster stat . . . . .	96
cluster upgrade . . . . .	96
cluster vast-db-configure . . . . .	98
cluster vast-db-show-config . . . . .	99
<b>cnode commands . . . . .</b>	<b>100</b>
cnode activate . . . . .	100

cnode add . . . . .	100
cnode deactivate . . . . .	101
cnode highlight . . . . .	102
cnode led . . . . .	102
cnode list . . . . .	103
cnode remove . . . . .	104
cnode rename . . . . .	104
cnode show . . . . .	105
<b>column commands . . . . .</b>	<b>107</b>
column delete . . . . .	107
column list . . . . .	108
column show . . . . .	109
column rename . . . . .	110
<b>dnode commands . . . . .</b>	<b>112</b>
dnode activate . . . . .	112
dnode deactivate . . . . .	112
dnode highlight . . . . .	113
dnode led . . . . .	113
dnode list . . . . .	114
dnode rename . . . . .	115
dnode show . . . . .	116
<b>dns commands . . . . .</b>	<b>117</b>
dns create . . . . .	117
dns delete . . . . .	118
dns list . . . . .	119
dns modify . . . . .	119
dns show . . . . .	120
<b>dtray commands . . . . .</b>	<b>122</b>
dtray deactivate . . . . .	122
dtray activate . . . . .	122
dtray led . . . . .	123
dtray list . . . . .	124
dtray rename . . . . .	124
dtray show . . . . .	125
<b>encryptiongroup commands . . . . .</b>	<b>126</b>
encryptiongroup deactivate-encryption-group . . . . .	126
encryptiongroup list . . . . .	126
encryptiongroup reinstate-encryption-group . . . . .	127

encryptiongroup revoke-encryption-group . . . . .	127
encryptiongroup rotate-encryption-group-key . . . . .	127
<b>encryptedpath commands . . . . .</b>	<b>129</b>
encryptedpath create . . . . .	129
encryptedpath delete . . . . .	129
encryptedpath list . . . . .	130
encryptedpath modify . . . . .	130
encryptedpath reinstate-encryption-group . . . . .	131
encryptedpath revoke-encryption-group . . . . .	131
encryptedpath rotate-encryption-group-key . . . . .	131
encryptedpath show . . . . .	132
<b>event commands . . . . .</b>	<b>133</b>
event list . . . . .	133
event show . . . . .	135
<b>eventdefinition commands . . . . .</b>	<b>137</b>
eventdefinition list . . . . .	137
eventdefinition modify . . . . .	143
eventdefinition show . . . . .	147
eventdefinition test . . . . .	147
<b>eventdefinitionconfig commands . . . . .</b>	<b>149</b>
eventdefinitionconfig list . . . . .	149
eventdefinitionconfig modify . . . . .	149
eventdefinitionconfig show . . . . .	153
<b>eventnotification commands . . . . .</b>	<b>155</b>
eventnotification create . . . . .	155
eventnotification delete . . . . .	156
eventnotification list . . . . .	157
eventnotification modify . . . . .	157
eventnotification show . . . . .	159
<b>globalsnapshotclone commands . . . . .</b>	<b>160</b>
globalsnapshotclone create . . . . .	160
globalsnapshotclone list . . . . .	161
globalsnapshotclone modify . . . . .	162
globalsnapshotclone pause . . . . .	162
globalsnapshotclone remove . . . . .	163
globalsnapshotclone resume . . . . .	163
globalsnapshotclone show . . . . .	164
globalsnapshotclone stop . . . . .	164

<b>group commands</b>	<b>166</b>
group create	166
group delete	166
group list	167
group modify	167
group query	168
group query-by-prefix	170
group show	171
<b>indestructibility commands</b>	<b>173</b>
indestructibility generate-token	173
indestructibility list	173
indestructibility modify	173
indestructibility reset-passwd	175
indestructibility show	175
indestructibility unlock	175
<b>kafkabroker commands</b>	<b>177</b>
kafkabroker create	177
kafkabroker modify	178
kafkabroker delete	179
kafkabroker list	179
kafkabroker show	179
kafkabroker list-topics	180
<b>ldap commands</b>	<b>181</b>
ldap create	181
ldap delete	187
ldap list	187
ldap modify	188
ldap set_primary_provider	195
ldap show	195
<b>license commands</b>	<b>197</b>
license add	197
license delete	197
license list	197
license show	198
<b>lifecyclerule commands</b>	<b>200</b>
lifecyclerule create	200
lifecyclerule delete	203
lifecyclerule get-object-expiration	203

lifecyclerule list . . . . .	203
lifecyclerule modify . . . . .	204
lifecyclerule show . . . . .	206
<b>localprovider commands . . . . .</b>	<b>208</b>
localprovider create . . . . .	208
object delete . . . . .	208
localprovider list . . . . .	209
localprovider modify . . . . .	209
localprovider show . . . . .	210
<b>manager commands . . . . .</b>	<b>212</b>
manager assign . . . . .	212
manager create . . . . .	213
manager delete . . . . .	214
manager join . . . . .	215
manager leave . . . . .	216
manager list . . . . .	216
manager modify . . . . .	217
manager show . . . . .	218
manager unassign . . . . .	219
manager unlock . . . . .	220
<b>nis commands . . . . .</b>	<b>222</b>
nis create . . . . .	222
nis delete . . . . .	222
nis list . . . . .	223
nis modify . . . . .	223
nis refresh . . . . .	224
nis set_primary_provider . . . . .	224
nis show . . . . .	224
<b>nvram commands . . . . .</b>	<b>226</b>
nvram activate . . . . .	226
nvram deactivate . . . . .	226
nvram list . . . . .	227
<b>projection commands . . . . .</b>	<b>229</b>
projection create . . . . .	229
projection delete . . . . .	230
projection list . . . . .	231
projection rename . . . . .	232
projection show . . . . .	233

<b>projectioncolumn commands</b> .....	<b>235</b>
projectioncolumn list .....	235
projectioncolumn show .....	236
<b>protectedpath commands</b> .....	<b>238</b>
protectedpath add-stream .....	238
protectedpath commit .....	239
protectedpath create .....	240
protectedpath delete .....	242
protectedpath delete-prefetch .....	242
protectedpath force-failover .....	243
protectedpath get-prefetch-status .....	243
protectedpath list .....	244
protectedpath modify .....	245
protected path modify-member .....	247
protectedpath pause .....	248
protectedpath reattach-stream .....	249
protectedpath remove-stream .....	249
protectedpath replicate-now .....	250
protectedpath restore .....	250
protectedpath resume .....	251
protectedpath show .....	251
protectedpath start-prefetch .....	253
globalsnapshotclone stop .....	254
<b>protectionpolicy commands</b> .....	<b>255</b>
protectionpolicy create .....	255
protectionpolicy delete .....	257
protectionpolicy list .....	258
protectionpolicy modify .....	259
protectionpolicy show .....	261
<b>realm commands</b> .....	<b>263</b>
realm assign .....	263
realm create .....	263
realm delete .....	264
realm list .....	264
realm show .....	265
realm unassign .....	265
<b>qospolicy commands</b> .....	<b>267</b>
qospolicy attach-user .....	267



qospolicy create . . . . .	268
qospolicy detach-user . . . . .	271
qospolicy delete . . . . .	272
qospolicy list . . . . .	273
qospolicy modify . . . . .	274
qospolicy show . . . . .	278
<b>quota commands . . . . .</b>	<b>279</b>
quota create . . . . .	279
quota delete . . . . .	281
quota list . . . . .	281
quota modify . . . . .	282
quota reset-grace-period . . . . .	284
quota show . . . . .	284
<b>replicationpeer commands . . . . .</b>	<b>286</b>
replicationpeer create . . . . .	286
replicationpeer delete . . . . .	287
replicationpeer list . . . . .	287
replicationpeer modify . . . . .	288
replicationpeer show . . . . .	288
<b>replicationstream commands . . . . .</b>	<b>290</b>
replicationstream list . . . . .	290
replicationstream modify . . . . .	291
replicationstream show . . . . .	292
<b>restorepoint commands . . . . .</b>	<b>293</b>
restorepoint list . . . . .	293
restorepoint show . . . . .	294
<b>role commands . . . . .</b>	<b>295</b>
role assign . . . . .	295
role create . . . . .	297
role delete . . . . .	298
role list . . . . .	298
role show . . . . .	299
role unassign . . . . .	299
<b>schema commands . . . . .</b>	<b>302</b>
schema create . . . . .	302
schema delete . . . . .	302
schema list . . . . .	303
schema rename . . . . .	305

schema show . . . . .	306
<b>snapshot commands . . . . .</b>	<b>308</b>
snapshot clone . . . . .	308
snapshot create . . . . .	309
snapshot delete . . . . .	309
snapshot list . . . . .	310
snapshot modify . . . . .	311
snapshot show . . . . .	312
<b>ssd commands . . . . .</b>	<b>313</b>
ssd activate . . . . .	313
ssd deactivate . . . . .	313
ssd list . . . . .	314
<b>s3replicationpeer commands . . . . .</b>	<b>318</b>
s3replicationpeer create . . . . .	318
s3replicationpeer delete . . . . .	319
s3replicationpeer list . . . . .	320
s3replicationpeer modify . . . . .	321
s3replicationpeer show . . . . .	322
<b>S3policy commands . . . . .</b>	<b>324</b>
identitypolicy create . . . . .	324
identitypolicy delete . . . . .	325
identitypolicy list . . . . .	325
identitypolicy modify . . . . .	326
identitypolicy show . . . . .	327
<b>supportbundle commands . . . . .</b>	<b>328</b>
supportbundle create . . . . .	328
supportbundle delete . . . . .	331
supportbundle list . . . . .	332
supportbundle show . . . . .	332
supportbundle upload . . . . .	332
<b>table commands . . . . .</b>	<b>334</b>
table add-columns . . . . .	334
table create . . . . .	335
table delete . . . . .	336
table list . . . . .	337
table rename . . . . .	338
table show . . . . .	339
<b>tenant commands . . . . .</b>	<b>341</b>

tenant alter-client-ip-ranges . . . . .	341
tenant alter-encryption-group-state . . . . .	342
tenant create . . . . .	343
tenant delete . . . . .	348
tenant list . . . . .	348
tenant list-remote . . . . .	349
tenant modify . . . . .	350
tenant rotate-encryption-group-key . . . . .	354
tenant show . . . . .	355
<b>topic commands . . . . .</b>	<b>357</b>
topic create . . . . .	357
topic modify . . . . .	358
topic delete . . . . .	359
topic list . . . . .	360
topic show . . . . .	360
<b>user commands . . . . .</b>	<b>361</b>
user add . . . . .	361
user copy . . . . .	362
user generate-key . . . . .	363
user list . . . . .	364
user modify . . . . .	365
user modify-key . . . . .	366
user query . . . . .	367
user query-by-prefix . . . . .	371
user refresh . . . . .	372
user remove-key . . . . .	373
<b>userquota commands . . . . .</b>	<b>375</b>
userquota create . . . . .	375
userquota list . . . . .	376
userquota modify . . . . .	377
userquota show . . . . .	378
<b>vastcatalogconfig commands . . . . .</b>	<b>379</b>
vastcatalogconfig columns . . . . .	379
vastcatalogconfig create . . . . .	379
vastcatalogconfig delete . . . . .	380
vastcatalogconfig list . . . . .	380
vastcatalogconfig modify . . . . .	381
vastcatalogconfig show . . . . .	382

<b>vastcatalogindexedcolumn commands</b> .....	<b>383</b>
vastcatalogindexedcolumn add .....	383
vastcatalogindexedcolumn list .....	383
vastcatalogindexedcolumn remove .....	384
<b>view commands</b> .....	<b>385</b>
view bulk-permission-update .....	385
view create .....	386
view delete .....	397
view list .....	397
view modify .....	400
view show .....	411
view stop-bulk-permission-update .....	413
<b>viewpolicy commands</b> .....	<b>415</b>
viewpolicy create .....	415
viewpolicy delete .....	435
viewpolicy list .....	435
viewpolicy modify .....	437
viewpolicy refresh-netgroups .....	454
viewpolicy show .....	455
<b>vippool commands</b> .....	<b>457</b>
vippool create .....	457
vippool delete .....	460
vippool list .....	460
vippool modify .....	461
vippool show .....	465
<b>vms commands</b> .....	<b>466</b>
vms delete_saml_idp_configuration .....	466
vms list .....	466
vms modify .....	467
vms modify_pwd_settings .....	470
vms modify_saml .....	473
vms remove_client_certificate .....	475
vms remove_saml_signed_cert .....	475
vms reset_certificate .....	475
vms reset_ssl_ciphers .....	476
vms set_certificate .....	476
vms set_client_certificate .....	477
vms set_max_api_tokens_per_user .....	477

vms set_ssl_ciphers . . . . .	478
vms set_ssl_port . . . . .	479
vms show. . . . .	479
vms show_saml_config . . . . .	480
vms show_saml_configured_idps . . . . .	481
<b>volume commands . . . . .</b>	<b>483</b>
volume create . . . . .	483
volume delete . . . . .	484
volume fetch-capacity . . . . .	484
volume get_snapshots . . . . .	485
volume list . . . . .	485
volume modify . . . . .	487
volume show . . . . .	488

# About this Guide

## About this VAST CLI Command Reference


This command reference contains reference pages that describe the usage syntax and supported parameters for many, although not all, commands in the VAST CLI.

For additional general information about VAST CLI usage, see [The VAST CLI](#).

## Typographic Conventions in this Guide

Each command reference includes a *Usage* section that shows the syntax for the command. The Usage section is followed by a *Required Parameters* section and an *Options* section. These sections describe each required and optional parameter shown in the syntax and provide additional details such as valid values.

To enter a command into the command line, copy the syntax shown in the *Usage* section at the prompt, except where the following symbols and formats appear in the syntax, in which case, follow the convention described here:

Symbol or Format	Meaning
[ ]	<p>These square brackets denote optional parameter(s) and/or argument(s). When you see these square brackets, any parameters and/or arguments within the brackets are optional and the command is valid without them. You can and should include them if they are needed for your use case.</p> <p>Do not type the square bracket symbols into the command line.</p>
	<p>This bar symbol separates mutually exclusive options. When you see this bar symbol, enter only one of the options that are separated by the bar.</p> <p>Do not type the bar symbol into the command line.</p> <div><b>Note</b><p>If there is a very large array of values, you will not see them all in the command syntax. Instead, you will see a single uppercase text value that represents the argument. The valid values are provided in the parameter description in the <i>Required Parameters</i> or the <i>Options</i> section for the valid values.</p></div>
UPPERCASE	<p>Uppercase text represents an argument that you supply.</p> <p>When you see uppercase text outside of an array of options, replace the uppercase text by a value appropriate to your use case.</p> <p>For an explanation of valid format and range, see the relevant parameter description in the <i>Required</i></p>

Symbol or Format	Meaning
	<p><i>Parameters</i> or the <i>Options</i> section.</p> <p>If you see an array of mutually exclusive options in uppercase text, the uppercase text is usually the value itself that you can enter as it is in uppercase and not a value that should be replaced with a string or integer of your own choice. For clarity in a specific case, see the parameter description in the <i>Required Parameters</i> or the <i>Options</i> section.</p>
{ }	<p>These curly brackets group together expressions in order to prevent ambiguity.</p> <p>Do not type the curly bracket symbols into the command line.</p>

# activedirectory commands

## activedirectory change\_machine\_account\_password

This command triggers a password change for the cluster's Active Directory machine account.

## Usage

```
activedirectory change_machine_account_password --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies the ID of the Active Directory configuration
----------------------	--

## Example

```
vccli: admin> activedirectory change_machine_account_password --id 1
```

## activedirectory create

This command creates an Active Directory (AD) configuration record. After running this command, run [activedirectory list](#) to obtain the ID of the configuration record, and then run [activedirectory modify](#) to make the cluster join the Active Directory domain using the Active Directory configuration record ID you obtained.



### Important

Ensure that your installation meets the prerequisites and requirements listed in [Active Directory Overview](#).

You can create multiple Active Directory configurations. Note that VAST Cluster does not allow adding two different Active Directory configuration records that have:

- The same domain name but different settings for multi-forest authentication and/or auto-discovery.
- The same domain name and the same machine account name.

## Usage

```
activedirectory create --machine-account-name MACHINE_NAME
                        --port PORT
                        --bindpw BIND_PASSWORD
                        --method anonymous|simple|sasl
                        [--organizational-unit OU]
                        [--allow-smb|--disallow-smb]
                        [--enable-ntlm|--disable-ntlm]
```



```

[--abac-read-only-value-name KEYWORD]
[--abac-read-write-value-name KEYWORD]
[--enable-scheduled-ma-pwd-change|--disable-scheduled-ma-pwd-change]
[--ma-pwd-change-frequency FREQUENCY]
[--ma-pwd-update_time TIME]
[--urls URI_LIST]
[--basedn BASE_DN]
[--domain-name DOMAIN_NAME]
[--binddn BIND_DN]
[--group-basedn GROUP_BASE_DN]
[--query-groups-mode COMPATIBLE|RFC2307BIS_ONLY|RFC2307_ONLY|NONE]
[--use-tls|--no-tls]
[--vms-auth|--no-vms-auth]
[--reverse-lookup|--no-reverse-lookup]
[--gid-number ATTRIBUTE_NAME]
[--uid ATTRIBUTE_NAME]
[--uid-number ATTRIBUTE_NAME]
[--member-uid ATTRIBUTE_NAME]
[--posix-account ATTRIBUTE_NAME]
[--posix-group ATTRIBUTE_NAME]
[--match-user ATTRIBUTE_NAME]
[--username-property-name ATTRIBUTE_NAME]
[--user-login-name ATTRIBUTE_NAME]
[--group-login-name ATTRIBUTE_NAME]
[--mail-property-name ATTRIBUTE_NAME]
[--uid-member-value-property-name ATTRIBUTE_NAME]
[--enable-auto-discovery|--disable-auto-discovery]
[--enable-use-ldaps|--disable-use-ldaps]
[--posix-attributes-source JOINED_DOMAIN|ALL_DOMAINS|SPECIFIC_DOMAIN

S|GC]

[--domains-with-posix-attributes DOMAINS]
[--enable-multi-forest|--disable-multi-forest]
[--super-admin-groups GROUPS]
[--monitor-action PING|BIND]


```

## Required Parameters

<code>--machine-account-name MACHINE_NAME</code>	Specifies a name for the machine object that will be created for the cluster within Active Directory, inside the Organizational Unit (see <code>--organizational-unit</code> ). It is recommended to name the machine name the same as the cluster name for simplicity.
<code>--port PORT</code>	Sets the port of the remote LDAP server. Recommended values: 389 for LDAP (with or without TLS), 636 for LDAPS.
<code>--bindpw BIND_PASSWORD</code> (required if <code>--method simple</code> or <code>--method sasl</code> is specified)	Sets the password used with the bind DN to authenticate to the LDAP server.
<code>--method anonymous simple sasl</code>	The authentication method the LDAP server uses to authenticate VAST Cluster as a client querying the LDAP database.  When <a href="#">multi-forest authentication</a> is enabled, VAST Cluster uses SASL for the LDAP bind to

	<p>domain controllers in other trusted forests, and this setting is only honored for the LDAP bind to domain controllers in the forest of the cluster's joined domain.</p> <p>Set the method according to how the LDAP server is configured to authenticate clients:</p> <ul style="list-style-type: none"> <li>• <code>anonymous</code>. The LDAP server accepts queries without any authentication.</li> <li>• <code>simple</code>. The LDAP server attempts to bind a specified user name to a matching LDAP user. If the LDAP bind succeeds, VAST Cluster is allowed to perform the query. If this method is specified, you have to set the bind DN on <code>--binddn</code> and password on <code>--bindpw</code>.</li> <li>• <code>sasl</code>. The LDAP server performs the Simple Authentication and Security Layer (SASL) authentication process. If the SASL bind succeeds, VAST Cluster is allowed to perform the query. If this method is specified, you have to set the bind DN on <code>--binddn</code> and password on <code>--bindpw</code>, with the bind DN in the <code>username@domain</code> or <code>DOMAIN\username</code> format.</li> </ul>
--	--

## Options

<code>--organizational-unit OU</code>	<p>The organizational unit (OU) in the Active Directory domain in which to create the machine object. The name of an organizational unit (OU) in the Active Directory domain.</p> <p>If unspecified, the machine object is created in the Computers OU.</p> <p>Specify as a Distinguished Name (DN).</p> <p>For example: <i>OU=Computers,DC=company-ad,DC=com</i></p>
<code>--allow-smb</code>	<p>When this option is specified, VAST Cluster can use this Active Directory provider to authenticate and authorize clients accessing the cluster via the SMB storage protocol. (Enabled by default).</p>
<code>--disallow-smb</code>	<p>Disables use of this Active Directory provider for SMB client access.</p>
<code>--enable-ntlm</code>	<p>When this option is specified, SMB clients accessing the cluster are allowed to use NTLM authentication to get authenticated via this Active Directory provider. This is the default behavior.</p> <div>  <p><b>Note</b></p> <p>NTLM authentication is not FIPS-compliant.</p> </div>

<code>--disable-ntlm</code>	Prohibits use of NTLM authentication on this Active Directory provider. SMB clients are expected to use Kerberos authentication, which requires an SPN to be <a href="#">configured</a> for each virtual IP pool.
<code>--abac-read-only-value-name KEYWORD</code>	Sets the <a href="#">ABAC attribute value</a> that grants read-only access to a view tagged with this ABAC attribute.  The default is <code>ro</code> .
<code>--abac-read-write-value-name KEYWORD</code>	Sets the <a href="#">ABAC attribute value</a> that grants read/write access to a view tagged with this ABAC attribute.  The default is <code>rw</code> .
<code>--enable-scheduled-ma-pwd-change</code>	Enables scheduled password change for the cluster's machine account on Active Directory. (Disabled by default).
<code>--disable-scheduled-ma-pwd-change</code>	Disables scheduled password change for the cluster's machine account on Active Directory. (Disabled by default).
<code>--ma-pwd-change-frequency FREQUENCY</code>	Sets the frequency, in days, for scheduled password change for the cluster's machine account on Active Directory. Default: 90
<code>--ma-pwd-update_time TIME</code>	The time of day at which scheduled password change for the cluster's Active Directory machine account should take place.  Specify <code>TIME</code> in the format <code>HH:mm</code> where <code>HH</code> is the number of hours and <code>mm</code> is the number of minutes.  Default: 20:00
<code>--use-tls</code>	<p>Enables TLS (StartTLS) to secure communication between VAST Cluster and the LDAP server.</p> <p>When enabled, VAST Cluster connects to the standard port (port 389 for the domain controller, port 3268 for the Global Catalog) and performs a StartTLS operation as defined in RFC 4513.</p> <div>  <p><b>Important</b></p> <p>Use VAST Web UI to <a href="#">provide</a> a TLS certificate.</p> </div>

<code>--no-tls</code>	Disables TLS (STARTTLS) secure communication between VAST Cluster and the LDAP server.
<code>--vms-auth</code>	If this option is specified, the LDAP configuration being created will be the one used for VMS authentication.
<code>--no-vms-auth</code>	If this option is specified, the LDAP configuration being created will not be used for VMS authentication. This is the default setting.
<code>--reverse-lookup</code>	Enables use of DNS reverse lookup for the translation of a client IP address to a host name. When this option is specified, the server compares the host name to host names in netgroup entries. If not specified, the server queries DNS for each host name found in the netgroup entries.
<code>--no-reverse-lookup</code>	Disables use of reverse DNS lookup. This is the default setting.
<code>--enable-auto-discovery</code>	<p>Enables <a href="#">Active Directory domain auto-discovery</a>. (Enabled by default).</p> <p>When auto-discovery is enabled, VAST Cluster automatically discovers and queries all domains and domain controllers in the forest of the cluster's joined domain and, if <a href="#">multi-forest authentication</a> is enabled by the <code>--enable-multi-forest</code> flag, in other trusted forests.</p>
<code>--disable-auto-discovery</code>	<p>Disables <a href="#">Active Directory domain auto-discovery</a>.</p> <p>When auto-discovery is disabled, the LDAP URI (<code>--urls</code>) and search base DN (<code>--basedn</code>) must be specified manually. VAST Cluster contacts only the domain controller configured using the <code>--urls</code> option and does not process requests from users in other domains, neither in the forest of the cluster's joined domain nor in other trusted forests.</p>
<code>--enable-multi-forest</code>	<p>When this option is specified, VAST Cluster automatically discovers all domains in other trusted forests, in addition to domains in the forest of the cluster's joined domain. For more information, see <a href="#">Active Directory Overview</a>.</p> <p>This option can only be specified when <a href="#">Active Directory domain auto-discovery</a> is enabled (<code>--enable-auto-discovery</code>).</p>
<code>--disable-multi-forest</code>	Disables multi-forest authentication on the cluster.

<code>--enable-use-ldaps</code>	<p>Enables use of LDAPS for Active Directory domain auto-discovery.</p> <p>When enabled, VAST Cluster connects to an alternative port (port 636 for the domain controller, port 3269 for the Global Catalog) and initiates a TLS handshake immediately afterwards.</p>
<code>--disable-use-ldaps</code>	<p>Disables use of LDAPS for Active Directory domain auto-discovery.</p>
<code>--posix-attributes-source</code> <code>JOINED_DOMAIN ALL_DOMAINS </code> <code>SPECIFIC_DOMAINS GC</code>	<p>Determines domains from which VAST Cluster queries POSIX attributes. Options include:</p> <ul style="list-style-type: none"> <li>• <code>JOINED_DOMAIN</code>. The domain which VAST Cluster has joined.</li> <li>• <code>ALL_DOMAINS</code>. All domains in the Active Directory forest of the cluster's joined domain and, if <a href="#">multi-forest authentication</a> is enabled, from other trusted forests.</li> <li>• <code>SPECIFIC_DOMAINS</code>. One or more domains specified on the <code>--domains-with-posix-attributes</code> option.</li> <li>• <code>GC</code>. All domains included in the Active Directory global catalog of the cluster's joined domain forest. When this option is specified, the global catalog must be configured with POSIX attributes.</li> </ul>
<code>--domains-with-posix-attributes DOMAINS</code>	<p>Provides a comma-separated list of the specific domains when <code>--posix-attributes-source SPECIFIC_DOMAINS</code> is specified. The domains can be in the forest of the cluster's joined domain, or in other trusted forests.</p> <p>For example: <code>ad.example.com, domain.com</code></p>
<code>--urls URI_LIST</code>	<p>Enter URIs of LDAP servers (domain controllers in the Active Directory joined domain). The order of listing defines the priority order. The URI with highest priority that has a good health status is used.</p> <p>If you are going to use <a href="#">Active Directory domain auto-discovery</a>, specify <code>URI_LIST</code> as a single URI and then run <code>ldap modify</code> to enable Active Directory domain auto-discovery. For a detailed procedure, see <a href="#">Creating Active Directory Configuration and Joining Active Directory from the VAST CLI</a>.</p> <p>Otherwise, specify <code>URI_LIST</code> as a comma-separated list of URIs in the format <code>&lt;scheme&gt;://&lt;address&gt;</code>.</p> <p>The domain controllers should all be in the same Active Directory domain which VAST Cluster joins.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• <code>--urls ldap://company-ad.com</code></li> </ul>

	<ul style="list-style-type: none"> <li>• <code>--urls ldaps://company-ad.com</code></li> <li>• <code>--urls ldap://company-ad.com,ldap://company-ad2.com</code></li> <li>• <code>--urls ldap://192.0.2.0,ldap://192.0.2.1,ldap://192.0.2.2</code></li> </ul>
<code>--binddn BIND_DN (required if --method simple or --method sasl is specified)</code>	<p>Sets the bind DN for authenticating to the LDAP server. The bind DN specifies the user with which VAST Cluster authenticates to the LDAP directory.</p> <p>Enter the bind DN for authenticating to the LDAP domain. The bind DN specifies the user with which VAST Cluster authenticates to the LDAP directory. You can specify any user account that has read access to the domain.</p> <p>The format is a comma separated list of components. Each component is an <i>attribute=value</i> pair defining an object in the directory tree. The first component is a <i>cn</i> attribute component specifying the user object, the next component is its container and so on up the tree, with the last component representing the top level domain.</p> <p>The following attributes can be specified:</p> <ul style="list-style-type: none"> <li>• <i>cn</i>: common name</li> <li>• <i>ou</i>: organizational unit</li> <li>• <i>o</i>: organization</li> <li>• <i>c</i>: country</li> <li>• <i>dc</i>: domain</li> </ul> <p>For example, <code>cn=admin,ou=users,dc=mydomain,dc=local</code> specifies user 'admin' located in the 'users' container under the domain 'mydomain.local'.</p> <p>If <a href="#">multi-forest authentication</a> is enabled and/or SASL authentication method is used, specify the bind DN in one of the following formats:</p> <ul style="list-style-type: none"> <li>• <code>username@domain</code></li> <li>• <code>DOMAIN\username</code></li> </ul>
<code>--group-basedn GROUP_BASE_DN</code>	<p>Sets the entry in the LDAP directory tree to use as a starting point for group queries. If not specified, the base DN is used.</p>
<code>--query-groups-mode</code> <code>COMPATIBLE RFC2307BIS_ONLY RFC2307_ONLY NONE</code>	<p>The mode for querying a user's auxiliary group memberships, when the auth provider is set as the source for group membership in the view policy:</p>

	<ul style="list-style-type: none"> <li>• <b>COMPATIBLE</b> (default). Groups are queried using an aggregate of the RFC2307BIS and RFC2307 compliant group membership queries (see the other options). You can use this default option unless you are using an authentication provider which is incompatible with this aggregated query mode.</li> <li>• <b>RFC2307BIS_ONLY</b>. Auxiliary group memberships are queried according to the RFC2307BIS standard, in which the group has a <i>members</i> attribute that contains the Distinguished Name (DN) of the member user and the user has a <i>memberOf</i> attribute which contains the DNs of the groups to which the user belongs. This standard is used by Active Directory and may be used with other LDAP-based authorization providers with LDAP schema extensions.</li> <li>• <b>RFC2307_ONLY</b>. Auxiliary group memberships are queried according to the RFC2307 standard, in which the group object has a <i>memberUid</i> attribute for each user object that is a member of the group, specifying the name of the user object. This standard may be used by openLDAP, freeIPA and other LDAP-based authorization providers.</li> <li>• <b>NONE</b>. If this option is selected, auxiliary group memberships are not queried at all. In the event that the relevant view's view policy cites the authorization provider as the group membership source and the user tries to access a file or directory within that view to which the user only has permission as a member of a the owning user's group, permission will not be granted.</li> </ul>
<code>--super-admin-groups GROUPS</code>	Grants members of specified groups on the provider <i>cluster admin</i> manager access to VMS. Users in these groups can log into VMS. To grant permissions to these users, add the group name to roles. By default, they are assigned a read-only role.
<code>--monitor-action PING BIND</code>	<p>Determines the type of periodic health check that VAST cluster performs for an Active Directory provider configured for the cluster:</p> <ul style="list-style-type: none"> <li>• <b>PING</b> (default): Ping the provider. This option creates less overhead and reduces impact on the provider.</li> <li>• <b>BIND</b>: Bind to the provider.</li> </ul>

## Attribute Mapping Options

If your Active Directory server uses attributes that differ from the default RFC2307BIS attribute set that is used for LDAP queries, these options map those attributes to the attribute names used on the server you are connecting the cluster to.

Example: `uid=cn --posix-account user --posix-group group`

<code>--gid-number ATTRIBUTE_NAME</code>	<p>The attribute of a group entry that contains the GID number of a group.</p> <p>Default: <i>gidNumber</i></p>
<code>--uid ATTRIBUTE_NAME</code>	<p>The attribute of a user entry that contains the user name.</p> <p>Default: <i>uid</i></p>
<code>--uid-number ATTRIBUTE_NAME</code>	<p>The attribute of a user entry that contains the UID number.</p> <p>Default: <i>uidNumber</i></p>
<code>--member-uid ATTRIBUTE_NAME</code>	<p>The attribute of the group entry that contains names of group members.</p> <p>Default: <i>member</i></p>
<code>--posix-account ATTRIBUTE_NAME</code>	<p>The object class that defines a user entry.</p> <p>Default: <i>user</i></p>
<code>--posix-group ATTRIBUTE_NAME</code>	<p>The object class that defines a group entry.</p> <p>Default: <i>group</i></p>
<code>--match-user ATTRIBUTE_NAME</code>	<p>Use this option to specify which attribute to use for matching users across providers during user refresh and user authentication. When querying a provider for a user that matches a user that was already retrieved from another provider, a user entry that contains a matching value in this attribute will be considered the same user as the user previously retrieved.</p> <p>Default: <i>sAMAccountName</i></p>
<code>--username-property-name ATTRIBUTE_NAME</code>	<p>Overrides 'name' as the attribute to use for querying users in VMS user-initiated user queries.</p> <p>Default: <i>name</i></p>
<code>--user-login-name ATTRIBUTE_NAME</code>	<p>Specifies the attribute used to query Active Directory for the user login name in NFS ID mapping. Applicable only with Active Directory and NFSv4.1.</p> <p>Default: <i>sAMAccountName</i></p>
<code>--group-login-name ATTRIBUTE_NAME</code>	<p>Specifies the attribute used to query Active Directory for the group login name in NFS ID mapping. Applicable only with Active Directory and NFSv4.1.</p>



	Default: <i>sAMAccountName</i>
<code>--mail-property-name ATTRIBUTE_NAME</code>	Specifies the attribute to use for the user's email address.  Default: <i>mail</i>
<code>--uid-member-value-property-name ATTRIBUTE_NAME</code>	Specifies the attribute which represents the value of the LDAP group's <i>member</i> property.  Default: <i>sAMAccountName</i>

## Example

```

vcli: admin> activedirectory create --machine-account-name cluster1 --organizational-unit O
U=Computers,DC=company,DC=com --port 389 --binddn admin@mydomain.local --bindpw !@WE56yt --me
thod simple --domain-name company-ad.com --uid=distinguishedName --member-uid member --posix-
account user --posix-group group --use-tls

```

### activedirectory delete

This command deletes an Active Directory configuration record.

## Usage

```
activedirectory delete --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies the Active Directory configuration to delete.
----------------------	---

## Example

```
vcli: admin> activedirectory delete --id 1
```

### activedirectory list

This command lists Active Directory configuration records with their IDs. It can be used to retrieve the record ID so that you can run [activedirectory modify](#) to join the Active Directory domain.

## Usage

```
activedirectory list
```

## Example

```
vcli: admin> activedirectory list
```

```

+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
| ID | Domain Name | Machine Account Name | Organizational Unit | State
| Smb-allowed | Ldap-state | Port | Method | Searchbase | Group-searchbase
| Use-tls | Use-ldaps | Ntlm-enabled | Scheduled Machine Account password change enabled | Ma
chine Account password change frequency | Machine Account password update time | Last Machin
e Account password renewal status |
+---+---+---+---+---+---+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
| 2 | dom.pvt | vast1 | | | JOINED
D | True | None | 389 | simple | |
| False | False | True | False | | | 0d
| 00:00:00 | {'is_during_change': False, | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| 1 | vast.lab | vast1 | | | JOINED
D | True | None | 389 | simple | |
| False | False | True | False | | | 0d
| 00:00:00 | {'is_during_change': False, | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| 5 | aws-dom01.dev | vast2 | | | NO
T_A_MEMBER | True | None | 389 | simple | CN=Users,DC=aws-dom01,DC=dev | CN=Use
rs,DC=aws-dom01,DC=dev | False | False | True | False
| 3M | 20:00:00 | {'is_du
ring change': False, |

```



```

[--domains-with-posix-attributes DOMAINS]
[--abac-read-only-value-name KEYWORD]
[--abac-read-write-value-name KEYWORD]
[--reverse-lookup|--no-reverse-lookup]
[--enable-multi-forest|--disable-multi-forest]
[--super-admin-groups GROUPS]
[--monitor-action PING|BIND]

```

## Usage (Joining and Leaving)

```



activedirectory modify --id ID
                        [--admin-username USERNAME]
                        [--admin-passwd PASSWORD]
                        [--join|--leave]




```

## Required Parameters

--id ID	Identifies the Active Directory configuration. To obtain the ID of an Active Directory configuration record, run <a href="#">activedirectory list</a> .
------------	---

## Options (Configuration)

--allow-smb	<p>Allows VAST Cluster to use this Active Directory provider to authenticate and authorize clients accessing the cluster via the SMB storage protocol.</p> <div>  <b>Tip</b> <p>Before allowing use of this Active Directory provider for SMB access, leave the cluster's joined Active Directory domain. After SMB is allowed, rejoin the domain.</p> </div>
--disallow-smb	<p>Disables use of this Active Directory provider for SMB client access.</p> <div>  <b>Tip</b> <p>Before disabling use of this Active Directory provider for SMB access, leave the cluster's joined Active Directory domain. After SMB is disallowed, rejoin the domain.</p> </div>

<pre>--enable-ntlm</pre>	<p>When this option is specified, SMB clients accessing the cluster are allowed to use NTLM authentication to get authenticated via this Active Directory provider. This is the default behavior.</p> <div data-bbox="812 304 1555 520">  <p><b>Note</b></p> <p>NTLM authentication is not FIPS-compliant.</p> </div> <div data-bbox="812 541 1555 814">  <p><b>Tip</b></p> <p>Before enabling NTLM, leave the cluster's joined Active Directory domain. After NTLM is enabled, rejoin the domain.</p> </div>
<pre>--disable-ntlm</pre>	<p>Prohibits use of NTLM authentication on this Active Directory provider.</p> <div data-bbox="812 945 1555 1218">  <p><b>Tip</b></p> <p>Before disabling NTLM, leave the cluster's joined Active Directory domain. After NTLM is disabled, rejoin the domain.</p> </div>
<pre>--enable-auto-discovery</pre>	<p>Enables <a href="#">Active Directory domain auto-discovery</a>. (Enabled by default).</p> <p>When auto-discovery is enabled, VAST Cluster automatically discovers and queries all domains and domain controllers in the forest of the cluster's joined domain and, if <a href="#">multi-forest authentication</a> is enabled by the <code>--enable-multi-forest</code> flag, in other trusted forests.</p>
<pre>--disable-auto-discovery</pre>	<p>Disables <a href="#">Active Directory domain auto-discovery</a>.</p> <p>When auto-discovery is disabled, the LDAP URI (<code>--urls</code>) and search base DN (<code>--basedn</code>) must be specified manually. VAST Cluster contacts only the domain controller configured using the <code>--urls</code> option and does not process requests from users in other domains, neither in the forest of the cluster's joined domain nor in other trusted forests.</p>


<code>--enable-use-ldaps</code>	<p>Enables use of LDAPS for Active Directory domain auto-discovery.</p> <p>When enabled, VAST Cluster connects to an alternative port (port 636 for the domain controller, port 3269 for the Global Catalog) and initiates a TLS handshake immediately afterwards.</p>
<code>--disable-use-ldaps</code>	<p>Disables use of LDAPS for Active Directory domain auto-discovery.</p>
<code>--urls URI_LIST</code>	<p>Use this option only if you choose to disable auto discovery (see <code>--disable-auto-discovery</code>). Enter URIs of LDAP servers (domain controllers in the Active Directory joined domain). The order of listing defines the priority order. The URI with highest priority that has a good health status is used.</p> <p>Specify <code>URI_LIST</code> as a comma-separated list of URIs in the format <code>&lt;scheme&gt;://&lt;address&gt;</code>.</p> <p>The domain controllers should all be in the same Active Directory domain which VAST Cluster joins.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li><code>--urls ldap://company-ad.com</code></li> <li><code>--urls ldaps://company-ad.com</code></li> <li><code>--urls ldap://company-ad.com,ldap://company-ad2.com</code></li> <li><code>--urls ldap://192.0.2.0,ldap://192.0.2.1,ldap://192.0.2.2</code></li> </ul>
<code>--port PORT</code>	<p>Sets the port of the remote LDAP server. Recommended values: 389 for LDAP (with or without TLS), 636 for LDAPS.</p>
<code>--binddn BIND_DN</code> (required if <code>--method simple</code> or <code>--method sasl</code> is specified)	<p>Sets the bind DN for authenticating to the LDAP server. The bind DN specifies the user with which VAST Cluster authenticates to the LDAP directory.</p> <p>Enter the bind DN for authenticating to the LDAP domain. The bind DN specifies the user with which VAST Cluster authenticates to the LDAP directory. You can specify any user account that has read access to the domain.</p> <p>The format is a comma separated list of components. Each component is an <i>attribute=value</i> pair defining an object in the directory tree. The first component is a <i>cn</i> attribute component specifying the user object, the next component is its container and so on up the tree, with the last component representing the top level domain.</p>

	<p>The following attributes can be specified:</p> <ul style="list-style-type: none"> <li>• cn: common name</li> <li>• ou: organizational unit</li> <li>• o: organization</li> <li>• c: country</li> <li>• dc: domain</li> </ul> <p>For example, <code>cn=admin,ou=users,dc=mydomain,dc=local</code> specifies user 'admin' located in the 'users' container under the domain 'mydomain.local'.</p> <p>If <a href="#">multi-forest authentication</a> is enabled and/or SASL authentication method is used, specify the bind DN in one of the following formats:</p> <ul style="list-style-type: none"> <li>• <code>username@domain</code></li> <li>• <code>DOMAIN\username</code></li> </ul>
<code>--bindpw BIND_PASSWORD (required if --method simple or --method sasl is specified)</code>	Sets the password used with the bind DN to authenticate to the LDAP server.
<code>--basedn BASE_DN</code>	<p>Specifies the entry in the LDAP directory tree to use as a starting point for user queries. By default, this is also used as the starting point for group queries. Optionally, you can specify a different entry as the group base DN on <code>--group-searchbase</code>.</p> <p>To maximize the speed of authentication queries, start the search in the lowest branch of the tree under which all users can be found. For example, if the entire directory must be queried, the search base must specify the root of the tree. However, if the search can be restricted to a specific organizational unit (OU), queries may be faster.</p> <p>Specify <code>BASE_DN</code> as a comma separated list of components. Each component is an <i>attribute=value</i> pair defining an object in the directory tree. The first component defines the object at the lowest part of the tree that you want to use as the starting point of the search, the next component is its container and so on up the tree, with the last component representing the top level domain.</p> <p>The following attributes can be specified:</p> <ul style="list-style-type: none"> <li>• cn: common name</li> <li>• ou: organizational unit</li> <li>• o: organization</li> <li>• c: country</li> </ul>

	<ul style="list-style-type: none"> <li>• <code>dc: domain</code></li> </ul>
<code>--group-basedn GROUP_BASE_DN</code>	Sets the entry in the LDAP directory tree to use as a starting point for group queries. If not specified, the base DN is used.
<code>--method anonymous simple sasl</code>	<p>The authentication method the LDAP server uses to authenticate VAST Cluster as a client querying the LDAP database.</p> <p>When <a href="#">multi-forest authentication</a> is enabled, VAST Cluster uses SASL for the LDAP bind to domain controllers in other trusted forests, and this setting is only honored for the LDAP bind to domain controllers in the forest of the cluster's joined domain.</p> <p>Set the method according to how the LDAP server is configured to authenticate clients:</p> <ul style="list-style-type: none"> <li>• <code>anonymous</code>. The LDAP server accepts queries without any authentication.</li> <li>• <code>simple</code>. The LDAP server attempts to bind a specified user name to a matching LDAP user. If the LDAP bind succeeds, VAST Cluster is allowed to perform the query. If this method is specified, you have to set the bind DN on <code>--binddn</code> and password on <code>--bindpw</code>.</li> <li>• <code>sasl</code>. The LDAP server performs the Simple Authentication and Security Layer (SASL) authentication process. If the SASL bind succeeds, VAST Cluster is allowed to perform the query. If this method is specified, you have to set the bind DN on <code>--binddn</code> and password on <code>--bindpw</code>, with the bind DN in the <code>username@domain</code> or <code>DOMAIN\username</code> format.</li> </ul>
<code>--enable-scheduled-ma-pwd-change</code>	Enables scheduled password change for the cluster's machine account on Active Directory. (Disabled by default)
<code>--disable-scheduled-ma-pwd-change</code>	Disables scheduled password change for the cluster's machine account on Active Directory. (Disabled by default)
<code>--ma-pwd-change-frequency FREQUENCY</code>	Sets the frequency, in days, for scheduled password change for the cluster's machine account on Active Directory. Default: 90
<code>--ma-pwd-update_time TIME</code>	<p>The time of day, according to the UTC time zone, at which scheduled password change for the cluster's Active Directory machine account should take place.</p> <p>Default: 20:00</p>




<code>--gid-number ATTRIBUTE_NAME</code>	<p>The attribute of a group entry that contains the GID number of a group.</p> <p>Default: <i>gidNumber</i></p>
<code>--uid ATTRIBUTE_NAME</code>	<p>The attribute of a user entry that contains the user name.</p> <p>Default: <i>uid</i></p>
<code>--uid-number ATTRIBUTE_NAME</code>	<p>The attribute of a user entry that contains the UID number.</p> <p>Default: <i>uidNumber</i></p>
<code>--member-uid ATTRIBUTE_NAME</code>	<p>The attribute of the group entry that contains names of group members.</p> <p>Default: <i>member</i></p>
<code>--posix-account ATTRIBUTE_NAME</code>	<p>The object class that defines a user entry.</p> <p>Default: <i>user</i></p>
<code>--posix-group ATTRIBUTE_NAME</code>	<p>The object class that defines a group entry.</p> <p>Default: <i>group</i></p>
<code>--match-user ATTRIBUTE_NAME</code>	<p>Use this option to specify which attribute to use for matching users across providers during user refresh and user authentication. When querying a provider for a user that matches a user that was already retrieved from another provider, a user entry that contains a matching value in this attribute will be considered the same user as the user previously retrieved.</p> <p>Default: <i>sAMAccountName</i></p>
<code>--uid-member-value-property-name ATTRIBUTE_NAME</code>	<p>Specifies the attribute which represents the value of the LDAP group's <i>member</i> property.</p> <p>Default: <i>sAMAccountName</i></p>
<code>--query-groups-mode COMPATIBLE RFC2307BIS_ONLY RFC2307_ONLY NONE</code>	<p>The mode for querying a user's auxiliary group memberships, when the auth provider is set as the source for group membership in the view policy:</p> <ul style="list-style-type: none"> <li>COMPATIBLE (default). Groups are queried using an aggregate of the RFC2307BIS and RFC2307 compliant group membership</li> </ul>

	<p>queries (see the other options). You can use this default option unless you are using an authentication provider which is incompatible with this aggregated query mode.</p> <ul style="list-style-type: none"> <li>• <b>RFC2307BIS_ONLY.</b> Auxiliary group memberships are queried according to the RFC2307BIS standard, in which the group has a <i>members</i> attribute that contains the Distinguished Name (DN) of the member user and the user has a <i>memberOf</i> attribute which contains the DNs of the groups to which the user belongs. This standard is used by Active Directory and may be used with other LDAP-based authorization providers with LDAP schema extensions.</li> <li>• <b>RFC2307_ONLY.</b> Auxiliary group memberships are queried according to the RFC2307 standard, in which the group object has a <i>memberUid</i> attribute for each user object that is a member of the group, specifying the name of the user object. This standard may be used by openLDAP, freeIPA and other LDAP-based authorization providers.</li> <li>• <b>NONE.</b> If this option is selected, auxiliary group memberships are not queried at all. In the event that the relevant view's view policy cites the authorization provider as the group membership source and the user tries to access a file or directory within that view to which the user only has permission as a member of a the owning user's group, permission will not be granted.</li> </ul>
<code>--username-property-name ATTRIBUTE_NAME</code>	<p>Overrides 'name' as the attribute to use for querying users in VMS user-initiated user queries.</p> <p>Default: <i>name</i></p>
<code>--use-tls</code>	<p>Enables TLS (StartTLS) to secure communication between VAST Cluster and the LDAP server.</p> <p>When enabled, VAST Cluster connects to the standard port (port 389 for the domain controller, port 3268 for the Global Catalog) and performs a StartTLS operation as defined in RFC 4513.</p> <div>  <p><b>Important</b></p> <p>Use VAST Web UI to <a href="#">provide</a> a TLS certificate.</p> </div>
<code>--no-tls</code>	<p>Disables TLS (STARTTLS) secure communication between VAST Cluster and the LDAP server.</p>

<code>--domain-name DOMAIN_NAME</code>	<p>Sets the fully qualified domain name (FQDN) of the domain to join.</p> <p>For example: <code>--domain-name company-ad.com</code></p>
<code>--user-login-name ATTRIBUTE_NAME</code>	<p>Specifies the attribute used to query Active Directory for the user login name in NFS ID mapping. Applicable only with Active Directory and NFSv4.1.</p> <p>Default: <i>sAMAccountName</i></p>
<code>--group-login-name ATTRIBUTE_NAME</code>	<p>Specifies the attribute used to query Active Directory for the group login name in NFS ID mapping. Applicable only with Active Directory and NFSv4.1.</p> <p>Default: <i>sAMAccountName</i></p>
<code>--mail-property-name ATTRIBUTE_NAME</code>	<p>Specifies the attribute to use for the user's email address.</p> <p>Default: <i>mail</i></p>
<code>--vms-auth</code>	<p>If this option is specified, the LDAP configuration being created will be the one used for VMS authentication.</p>
<code>--no-vms-auth</code>	<p>If this option is specified, the LDAP configuration being created will not be used for VMS authentication. This is the default setting.</p>
<code>--posix-attributes-source</code> <code>JOINED_DOMAIN ALL_DOMAINS </code> <code>SPECIFIC_DOMAINS GC</code>	<p>Determines domains from which VAST Cluster queries POSIX attributes. Options include:</p> <ul style="list-style-type: none"> <li>• <code>JOINED_DOMAIN</code>. The domain which VAST Cluster has joined.</li> <li>• <code>ALL_DOMAINS</code>. All domains in the Active Directory forest of the cluster's joined domain and, if <a href="#">multi-forest authentication</a> is enabled, from other trusted forests.</li> <li>• <code>SPECIFIC_DOMAINS</code>. One or more domains specified on the <code>--domains-with-posix-attributes</code> option.</li> <li>• <code>GC</code>. All domains included in the Active Directory global catalog of the cluster's joined domain forest. When this option is specified, the global catalog must be configured with POSIX attributes.</li> </ul>
<code>--domains-with-posix-attributes DOMAINS</code>	<p>Provides a comma-separated list of the specific domains when <code>--posix-attributes-source SPECIFIC_DOMAINS</code> is specified. The domains can be in the forest of the cluster's joined domain, or in</p>

	<p>other trusted forests.</p> <p>For example: <code>ad.example.com, domain.com</code></p>
<code>--abac-read-only-value-name KEYWORD</code>	<p>Sets the <b>ABAC attribute value</b> that grants read-only access to a view tagged with this ABAC attribute.</p> <p>The default is <code>ro</code>.</p>
<code>--abac-read-write-value-name KEYWORD</code>	<p>Sets the <b>ABAC attribute value</b> that grants read/write access to a view tagged with this ABAC attribute.</p> <p>The default is <code>rw</code>.</p>
<code>--super-admin-groups GROUPS</code>	<p>Grants members of specified groups on the provider <i>cluster admin</i> manager access to VMS. Users in these groups can log into VMS. To grant permissions to these users, add the group name to roles. By default, they are assigned a read-only role.</p>
<code>--monitor-action PING BIND</code>	<p>Determines the type of periodic health check that VAST cluster performs for an Active Directory provider configured for the cluster:</p> <ul style="list-style-type: none"> <li>• <b>PING</b> (default): Ping the provider. This option creates less overhead and reduces impact on the provider.</li> <li>• <b>BIND</b>: Bind to the provider.</li> </ul>

## Options (Joining and Leaving)

<code>--admin-username</code> <b>USERNAME</b>	<p>Specify an Active Directory admin user with permission to join the Active Directory domain.</p>
<code>--admin-passwd PASSWORD</code>	<p>Specify the password for the specified user. If not supplied, you are prompted for the password.</p> <div>  <div> <p><b>Note</b></p> <p>VAST Cluster does not store this password.</p> </div> </div>

<code>--join</code>	Include this option to join the Active Directory domain.
<code>--leave</code>	Include this option to leave the Active Directory domain.

## Example

This example shows the cluster joining to an Active Directory domain.

```
vcli: admin> activedirectory modify --id 1 --join --admin-username myuser
Are you sure you want to modify the Active directory? [y/N] y
Enter admin password:
Password:

Waiting ...

[2020-03-31 10:18:39] waiting for active directory AD enabled state to change to True ...\
[2020-03-31 10:19:45] modify active directory completed successfully .../
```

### activedirectory remove

This command removes an Active Directory configuration.

## Usage

```
activedirectory remove --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which Active Directory configuration to remove.
----------------------	---

## Example

```
vcli: admin> activedirectory remove --id 4
```

### activedirectory show

This command displays details of a specific Active Directory configuration.

## Usage

```
activedirectory show --id ID
```

# Required Parameters

<code>--id ID</code>	Specifies which Active Directory configuration to show.
----------------------	---

## Example

```
vcli: admin> activedirectory show --id 2
+-----+
+-----+
+
| ID | 2 |
| Domain Name | dom.pvt |
| Machine Account Name | vast1 |
| Organizational Unit | |
| State | JOINED |
| Smb-allowed | True |
| Ldap-state | None |
| Port | 389 |
| Method | simple |
| Searchbase | |
| Group-searchbase | |
| Use-tls | False |
| Use-ldaps | False |
| Ntlm-enabled | True |
| Scheduled Machine Account password change enabled | False |
| Machine Account password change frequency | 0d |
| Machine Account password update time | 00:00:00 |
| Last Machine Account password renewal status | {'is_during_change': False, 'last_chan |
ge_attempt': None, 'last_successful_change': None, 'message': '', |
| 'next_scheduled_change': None} |
+-----+
+-----+
+
```


## activedirectory show\_ad\_domains

This command shows automatically discovered Active Directory domains for the specified Active Directory configuration.

The display lists each of the discovered Active Directory domains in the cluster's joined domain forest with indication of the

domain's fully qualified domain name (FQDN), search base DN, and security identifier (SID).

If [multi-forest authentication](#) is enabled, the display also includes domains from other trusted forests.



**Note**

When Active Directory domain auto-discovery is disabled or Active Directory information is not available, no domains are displayed.

# Usage

```
activedirectory show_ad_domains --id ID
```

# Required Parameters

<code>--id ID</code>	Specifies which Active Directory configuration to show.
----------------------	---

# Example


```
vccli: admin> activedirectory show_ad_domains --id 7
+-----+-----+-----+
| BASE DN | FQDN | SID |
+-----+-----+-----+
| DC=Dep,DC=co-ad,DC=com | dep.co-ad.com | S-1-6-21-3652124371-3558378908-1704889498 |
| DC=co-ad,DC=com | co-ad.com | S-1-6-21-473129083-4162203952-513326743 |
+-----+-----+-----+
```

## activedirectory show\_ad\_gcs

This command shows automatically discovered Active Directory global catalog servers.

The display shows the URI of the Active Directory global catalog (GC) server that is currently used by the cluster and the time to the next global catalog refresh (in seconds). Following is a list of other discovered GC servers, each with indication of its URI, status (such as HEALTHY or FAILED), and whether it is on the same Active Directory site as the cluster.

The display does not include GC servers from other trusted forests (even when [multi-forest authentication](#) is enabled).



**Note**

When Active Directory domain auto-discovery is disabled or Active Directory information is not available, no data is displayed.

# Usage

```
activedirectory show_ad_gcs --id ID
```

## Required Parameters

--id ID	Specifies which Active Directory configuration to show.
---------	---


## Example

```
vcli: admin> activedirectory show_ad_gcs --id 7
Current Global Catalog Details:
  URI: ldap://abc.company-ad.com
  Next global catalog refresh (sec): 3049
+-----+-----+-----+
| URI                                | STATE | ON SITE |
+-----+-----+-----+
| ldap://abc.company-ad.com          | HEALTHY | True    |
| ldap://def.company-ad.com          | HEALTHY | False   |
+-----+-----+-----+
```

### activedirectory show\_joined\_domain\_dcs

This command shows automatically discovered Active Directory domain controllers of the cluster's joined Active Directory domain.

The display lists all DCs from all domains in the discovered forest of the cluster's joined domain. For each DC, it shows its URI, status (such as HEALTHY or FAILED), and whether it is on the same Active Directory site as the cluster.



**Note**

When Active Directory domain auto-discovery is disabled or Active Directory information is not available, no DCs are displayed.

# Usage

```
activedirectory show_joined_domain_dcs --id ID
```

## Required Parameters

--id ID	Specifies which Active Directory configuration to show.
---------	---



## Example

```
vcli: admin> activedirectory show_joined_domain_dcs --id 7
+-----+-----+-----+
| URI                                | STATE  | ON SITE |
+-----+-----+-----+
| ldap://abc.company-ad.com          | HEALTHY | True    |
| ldap://def.company-ad.com          | UNKNOWN | False   |
+-----+-----+-----+
```

# alarm commands

## alarm clear

This command clears all alarms.

## Usage

```
alarm clear
```

## Example

This example clears all alarms.

```
vcli: admin> alarm clear
```

## alarm delete

This command clears a specified alarm.

## Usage

```
alarm delete --id ID
```

## Required Parameters

<code>--id <i>id</i></code>	Specifies the alarm to delete by its ID.
-----------------------------	--

## Example

```
vcli: admin> alarm delete --id 2
```

## alarm list

This command lists alarms.

## Usage

```
alarm list [--start-time START-TIME]
           [--end-time END-TIME]
           [--object-type TYPE]
           [--object-id OBJECT_ID]
           [--message TEXT]
           [--severity CRITICAL|MAJOR|MINOR]
```

[--page PAGE\_NUMBER]  
[--page-size NUMBER\_ON\_PAGE]

## Options

<code>--start-time START-TIME</code>	<p>Starts listing from a specified alarm time.</p> <p>Specify START-TIME in the format <code>YYYY-MM-DD HH:MM:SS</code>. For example: 2017-10-19 10:31:47</p>
<code>--end-time END-TIME</code>	<p>Ends listing by a specified alarm time.</p> <p>Specify END-TIME in the format <code>YYYY-MM-DD HH:MM:SS</code>. For example: 2017-10-19 10:31:47</p>
<code>--object-type TYPE</code>	<p>Filters the list by object type.</p> <p>For example: <code>--object-type Cluster</code></p> <p>Valid types include:</p> <p>Vms   Cluster   BMC   CNode   DNode   ReplicationTarget   ReplicationStream   SSD   NVRAM   NIC   Carrier   Quota   Fan   PSU   DBox   CBox   Switch   Port   Ldap   NIS   Task   Host   SupportBundle   ActiveDirectory   License</p>
<code>--object-id OBJECT_ID</code>	<p>Filters the list by object ID.</p> <p>For example: <code>--object-id 23</code></p>
<code>--message TEXT</code>	<p>Filters the list by alarm message text. Specify any text to search for as TEXT. The search is case sensitive.</p> <p>For example: <code>--message DEGRADED</code></p>
<code>--severity CRITICAL   MAJOR   MINOR</code>	<p>Filters the list by alarm severity.</p>
<code>--page PAGE_NUMBER</code>	<p>Displays a specified page if <code>--page-size</code> is set.</p> <p>Defaults to the first page.</p>
<code>--page-size NUMBER_ON_PAGE</code>	<p>Sets the maximum number of alarms to display on a page.</p>

## Example

```
vccli: admin> alarm list --severity CRITICAL
```

```
+-----+-----+-----+-----+-----+-----+
| ID | Timestamp           | Object-type | Object-id | Cluster  | Severity | Alarm-message |
+-----+-----+-----+-----+-----+-----+
| 4  | 2020-08-19 12:09:27 | CNode      | 3         | vast2    | CRITICAL | CNode cnode-3  
(203.0.113.7) [ac1n3] file server access changed from True to False |
| 3  | 2020-08-19 12:09:27 | CNode      | 2         | vast2    | CRITICAL | CNode cnode-2  
(203.0.113.6) [ac1n2] file server access changed from True to False |
| 2  | 2020-08-19 12:09:27 | CNode      | 1         | vast2    | CRITICAL | CNode cnode-1  
(203.0.113.5) [ac1n1] file server access changed from True to False |
+-----+-----+-----+-----+-----+-----+
```

### alarm show

This command displays details of a specific alarm.

## Usage

```
alarm show --id ID
```

## Required Parameters

## Options

<code>--id ID</code>	Specifies the alarm to display.
----------------------	---------------------------------

## Example

```
vccli: admin> alarm show --id 12
```

```
+-----+
| ID          | 12 |
+-----+
| Timestamp   | 2020-10-19 08:54:56 |
+-----+
| Object-type | SSD |
+-----+
| Object-id   | 6   |
+-----+
| Cluster     | vast11 |
+-----+
| Severity    | MAJOR  |
+-----+
| Alarm-message | SSD Ejected-dbox-A50056-REAR-17-1 serial: S3X3NF0JC00468B detached from DNode 2 |
+-----+
```

# apitoken commands

## apitoken create

This command creates an API token, which can be used to securely authenticate calls to the VMS REST API.

The token is displayed in the command output and cannot be displayed again.

The number of tokens per user is limited to five by default and configurable using [vms set\\_max\\_api\\_tokens\\_per\\_user](#).

The command enables you to create a token for yourself or for another user.



### Note

Creating a token for another user requires *Create* permission for the *Security* realm.

## Usage

```
apitoken create [--name TOKEN_NAME]
                [--expiry-date EXPIRATION_TIME]
                [--owner OWNER]
```

## Options

<code>--name</code> <code>TOKEN_NAME</code>	<p>Customizes the name of the API token.</p> <p>If not specified, the token is named <code>OWNER_api_token</code>, where <code>OWNER</code> is the user name of the token owner.</p>
<code>--expiry-date</code> <code>EXPIRATION_TIME</code>	<p>Sets the token's expiration date by specifying an amount of time from token creation until the token should expire. The expiration date is equal to the token creation date in UTC + the specified time period.</p> <p>Specify <code>EXPIRATION_TIME</code> as a whole integer followed by a unit of time: 'Y' for (365 day) years, 'M' for (30 day) months, 'w' or 'W' for weeks, 'd' or 'D' for days, 'h' or 'H' for hours, 'm' for minutes, 's' or 'S' for seconds.</p> <p>The maximum and default expiration time is the password expiration timeout, which is set by the <code>--pwd-expiration-timeout</code> parameter of the <a href="#">vms modify_pwd_settings</a> command. If password expiration is not enabled, tokens do not expire unless <code>--expiry-date</code> is set.</p> <p>Example: To set the token to expire after 180 days: <code>--expiry-date 180D</code></p>
<code>--owner</code> <code>OWNER</code>	<p>Sets the owner of the token. Use this parameter to create a token for another user.</p>

If not specified, the token is owned by the requesting user.



### Note

Creating a token for another user requires *Create* permission for the *Security* realm.

## Examples

This example creates a token for the `admin` user, named `admin_api_token`:

```
vccli: admin> apitoken create
ApiToken with id: JhxND7ci has been created, your token is: JhxND7ci.AWrRmHXRTbcjUSCANl9KLrxR
T6sMquesu please keep it safe
```

This example creates a token for the user `admin_jb`, named `AWS_TOKEN` that will expire in one day:

```
vccli: admin> apitoken create --name AWS_TOKEN --expiry-date 1D --owner adminjb
ApiToken with id: L7k8ljIC has been created, your token is: L7k8ljIC.jm1P5Y0ONaJfUJhs1JbAjRAY
r9jcy89X please keep it safe
```

### apitoken list

This command displays API tokens and their details.

## Usage

```
apitoken list [--archived]
               [--owner OWNER]
```

## Options

<code>--archived</code>	Includes archived tokens in the list. Tokens are archived when they are revoked.
<code>--owner OWNER</code>	Displays tokens owned by a specific manager user. Specify <code>OWNER</code> as a string, the user name of a manager.

## Example

```
vccli: admin> apitoken list
+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+
| ID      | Name                  | Owner | Expiry-date           | Last-used           | Revoke
d | Revocation-time |
+-----+-----+-----+-----+-----+
```

```

+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+
| c6UmISHU | example_api_token | admin | 2025-06-18 11:59:00 | None | False
| None |
| RWDLagfI | example2_api_token | admin2 | 2025-05-19 12:00:00 | 2025-02-19 11:30:04 | False
| None |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+

```

## Command Output

ID	Token ID
Name	Token name
Owner	Token owner
Expiry-date	The token's expiration date.
Last-used	The time when the token was last used to authenticate to the VMS REST API.
Revoked	True if the token has been revoked. False otherwise.
Revocation-time	The time at which the token was revoked, if applicable.

### apitoken modify

This command modifies an API token.

## Usage

```

apitoken modify --id ID
                  [--name NAME]
                  [--expiry-date EXPIRATION_TIME]

```

## Required Parameters

--id ID	Specifies the API token to modify.
---------	------------------------------------

## Options

<code>--name NAME</code>	<p>Customizes the name of the API token.</p> <p>If not specified, the token is named <code>OWNER_api_token</code>, where <code>OWNER</code> is the user name of the token owner.</p>
<code>--expiry-date EXPIRATION_TIME</code>	<p>Sets the token's expiration date by specifying an amount of time from token creation until the token should expire. The expiration date is equal to the token creation date in UTC + the specified time period.</p> <p>Specify <code>EXPIRATION_TIME</code> as a whole integer followed by a unit of time: 'Y' for (365 day) years, 'M' for (30 day) months, 'w' or 'W' for weeks, 'd' or 'D' for days, 'h' or 'H' for hours, 'm' for minutes, 's' or 'S' for seconds. For example: to set the expiration date to be six months after creating the token: <code>--expiry-date 6M</code></p> <p>The maximum and default expiration time is the password expiration timeout, which is set by the <code>--pwd-expiration-timeout</code> parameter of the <a href="#">vms modify_pwd_settings</a> command. If password expiration is not enabled, tokens do not expire unless <code>--expiry-date</code> is set.</p> <p>Example: To set the token to expire after 180 days: <code>--expiry-date 180D</code></p>

## Example

```
vcli: admin> apitoken modify --id SwpND4dt --name manager1token2 --expiry-date 24M
```

### apitoken revoke

This command revokes an API token.

## Usage

```
apitoken revoke --id ID
```

## Required Parameters

<code>id ID</code>	Specifies the token to revoke.
--------------------	--------------------------------

## Example

```
vcli: admin> apitoken revoke --id swdfos3d
```



## apitoken show

This command displays details of a specific API token.

## Usage

```
apitoken show --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies the token to display.
----------------------	---------------------------------

## Example

```
vcli: admin> apitoken show --id 0MivGn7o
+-----+-----+
| ID           | 0MivGn7o           |
| Name         | admin_api_token     |
| Owner        | admin               |
| Expiry-date   | 2024-10-15 12:40:42 |
| Last-used    | 2024-10-12 18:34:19 |
| Revoked      | True                |
| Revocation-time | 2024-10-14 16:00:20 |
+-----+-----+
```

## Command Output

ID	Token ID
Name	Token name
Owner	Token owner
Expiry-date	The token's expiration date.
Last-used	The time when the token was last used to authenticate to the VMS REST API.
Revoked	True if the token has been revoked. False otherwise.

Revocation-time	The time at which the token was revoked, if applicable.
-----------------	---

# blockhost commands

## blockhost create

This command adds a block client host to VMS, enabling the host to be identified and associated with block storage volumes created on the cluster. The host must first be configured as an NVMe-over-TCP client.

## Usage

```
blockhost create --tenant-id ID
                  --name NAME
                  --nqn NQN
                  [--tags TAGS]
```

## Required Parameters

<code>--tenant-id ID</code>	Specifies on which tenant to create the host definition.  Specify <code>ID</code> as an integer.
<code>--name NAME</code>	Specifies the host name.
<code>--nqn NQN</code>	Specifies the host's NVMe Express Qualified Name (NQN).  The NQN is a unique identifier string that you can retrieve from the host.

## Options

<code>--tags TAGS</code>	Adds specified key-value pairs to tag the host, for the purpose of categorizing and organizing block hosts.  Specify <code>TAGS</code> as a comma separated list of pairs of strings in the format <code>KEY=VALUE</code> .  For example: <code>--tags owner=John,department=research</code>
--------------------------	--

## Example

```
vcli: admin> blockhost create --tenant-id 1 --name h11 --nqn nqn.2015-18.org.nvmexpress:uid:3c4c4545-004e-3210-804d-c6c04f4b3234
```

## blockhost delete

This command deletes a block host. Block hosts cannot be deleted while they are mapped to volumes.

## Usage

```
blockhost delete --id ID
                  [--force]
```

## Required Parameters

<code>--id ID</code>	Specifies which block host to delete.
----------------------	---------------------------------------

## Options

<code>--force</code>	Forces unmapping to enable deletion.
----------------------	--------------------------------------

## Examples

```
vcli: admin> blockhost delete --id 1
Are you sure you want to delete the volume? [y/N] y
vcli: admin> blockhost delete --id 2
Are you sure you want to delete the blockhost? [y/N] y
Command REST Error: {"detail":"Host is mapped to volumes"}
vcli: admin> blockhost delete --id 2 --force
Are you sure you want to delete the blockhost? [y/N] y
vcli: admin>
```

### blockhost list

This command displays all block hosts and their properties.

## Usage

```
blockhost list [--tenant-id ID]
```

## Options

<code>--tenant-id ID</code>	Displays only block hosts on a specified tenant.
-----------------------------	--

## Example

```
vcli: admin> blockhost list
+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
| Id | Tenant-id | Name | Nqn |
```

```
| Tags | Tenant-name |
+-----+-----+
| 2 | 1 | blockhost1 | nqn.2014-08.org.nvmexpress:uuid:4c4c4544-004e-3310-804d-c6c04f4b3234 | {} | default |
+-----+-----+
+-----+-----+
+-----+-----+
```

## blockhost modify

This command modifies a block host.

## Usage

```
blockhost modify --id ID
                  [--name NAME]
                  [--tags TAGS]
```

## Required Parameters

<code>--id ID</code>	Specifies which block host to modify.
----------------------	---------------------------------------

## Options

<code>--name NAME</code>	Specifies the host name.
<code>--tags TAGS</code>	<p>Adds specified key-value pairs to tag the host, for the purpose of categorizing and organizing block hosts.</p> <p>Specify <b>TAGS</b> as a comma separated list of pairs of strings in the format <b>KEY=VALUE</b>.</p> <p>Specifies the host's NQN (NVM Express Qualified Name).</p> <p>For example: <code>--tags owner=John,department=research</code></p>

## Example

```
vccli: admin> blockhost modify --id 2 --tags team=coolguys,owner=bg
vccli: admin> blockhost show --id 2
+-----+-----+
| Id      | 2 |
| Tenant-id | 1 |
| Name     | blockhost1 |
| Nqn      | nqn.2014-08.org.nvmexpress:uuid:4c4c4544-004e-3310-804d-c6c04f4b3234 |
| Tags     | {} |
| Tenant-name | default |
+-----+-----+
vccli: admin> blockhost modify --id 2 --tags "team=coolguys,owner=bg"
vccli: admin> blockhost show --id 2
```

```
+-----+-----+
| Id      | 2      |
| Tenant-id | 1      |
| Name     | blockhost1 |
| Nqn      | nqn.2014-08.org.nvmexpress:uuid:4c4c4544-004e-3310-804d-c6c04f4b3234 |
| Tags     | {'team': 'coolguys', 'owner': 'bg'} |
| Tenant-name | default |
+-----+-----+
```

## blockhost show

This command displays properties of a block host.

## Usage

```
blockhost show --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which block host to display.
----------------------	--

## Example

```
vccli: admin> blockhost show --id 2
```

```
+-----+-----+
| Id      | 2      |
| Tenant-id | 1      |
| Name     | blockhost1 |
| Nqn      | nqn.2014-08.org.nvmexpress:uuid:4c4c4544-004e-3310-804d-c6c04f4b3234 |
| Tags     | {}      |
| Tenant-name | default |
+-----+-----+
```

## Command Output

Id	The VMS identifier for the host definition.
Tenant-id	The identifier of the tenant on which the host is defined.
Name	The name of the host.
Nqn	The host's NQN (NVM Express Qualified Name), a unique identifier string configured on the host.

Tags	Descriptive tags that were added to the host definition.
Tenant-name	The name of the tenant on which the host is defined.

# blockmapping commands

## blockmapping list

This command displays mappings of block volumes to hosts.

## Usage

```
blockmapping list [--tenant-id ID]
```

## Options

<code>--tenant-id ID</code>	Specifies for which tenant to display block mappings. Defaults to the default tenant.
-----------------------------	---

## Example

```
vcli: admin> blockmapping list
+-----+-----+-----+-----+
| Id | Volume id | BlockHost id | Snapshot-data |
+-----+-----+-----+-----+
| 1 | 3 | 1 | {'id': None, 'name': 'N/A'} |
| 3 | 8 | 1 | {'id': 1, 'name': 'VollSnap'} |
| 4 | 9 | 1 | {'id': 5, 'name': 'CatsSnap'} |
| 5 | 7 | 1 | {'id': None, 'name': 'N/A'} |
+-----+-----+-----+-----+
```

## Command Output

Id	The identifier of the mapping.
Volume id	The identifier of a block volume.
BlockHost id	The identifier of a block host that is mapped to the volume specified in the Volume id column.
Snapshot-data	The ID and name of a snapshot of the mapped volume that is mapped to the specified host.

## blockmapping map\_host\_to\_volumes

This command creates a mapping of a single block storage host to one or more block storage volumes.



# Usage

```
blockmapping map_host_to_volumes --blockhost-id ID
                                   --volume-ids IDS
```

## Required Parameters

<code>--blockhost-id ID</code>	Specifies the block host to map to volumes.
<code>--volume-ids IDS</code>	Specifies one or more volumes to map to the host. Specify <code>IDS</code> as a comma separated list of volume IDs.

## Examples

```
vcli: admin> blockmapping map_host_to_volumes --blockhost-id 2 --volume-ids 1

Waiting ...
Waiting ... \
[2025-02-26 17:42:57] mapping host blockhost1 to volume dev/platform, clone_id=None in subsystem blocktarget1
[2025-02-26 17:42:58] mapping host blockhost1 to volume dev/platform finished,remote_mapping_object_id=1, remote_volume_object_id=1
[2025-02-26 17:42:58] bulk mapping finished successfully ... |

Completed
vcli: admin>

vcli: admin> blockmapping map_host_to_volumes --blockhost-id 1 --volume-ids 1 --snapshot-id 2

Waiting ...
Waiting ... \
[2025-04-06 14:59:40] mapping host Host to volume vol1, clone_id=1000000001 in subsystem Subsystem
[2025-04-06 14:59:40] mapping host Host to volume vol1 finished,remote_mapping_object_id=7, remote_volume_object_id=15
[2025-04-06 14:59:41] bulk mapping finished successfully ... |

Completed
```

### blockmapping map\_volume\_path

This command creates a block volume of a volume snapshot and assigns it to block hosts.

## Usage

```
blockmapping map_volume_path --volume-full-path PATH
                              --blockhost-ids IDS
                              --snapshot-id ID
```

## Required Parameters

<code>--volume-full-path PATH</code>	Specifies the full path to the volume. For example, if the volume is provisioned on a view of the path <code>/subsystem1</code> , and the volume name is <code>a/b/c</code> , then specify <code>PATH</code> as <code>/subsystem1/a/b/c/</code> .
<code>--blockhost-ids IDS</code>	Specifies one or more block host(s) to assign to the snapshot volume. Separate multiple host IDs with commas.
<code>--snapshot-id ID</code>	Specifies the snapshot of the specified volume path that you want to make accessible to the block hosts.

## Example

```
vccli: admin> blockmapping map_volume_path --volume-full-path /myblocksubsystem/myvolume --snapshot-id 81 --blockhost-ids 2,3,4
```

### blockmapping map\_volume\_to\_hosts

This command creates a mapping of a single block volume to one or more block hosts.

## Usage

```
blockmapping map_volume_to_hosts --volume-id  
                                --blockhost-ids IDS
```

## Required Parameters

<code>--volume-id</code>	Specifies the block volume to map to hosts.
<code>--blockhost-ids IDS</code>	Specifies block hosts to map to the specified volume.

## Example

```
vccli: admin> blockmapping map_host_to_volumes --volume-id 5 --blockhost-ids 1 --snapshot-id 122
```

```
Waiting ...  
Waiting ... \  
[2025-02-27 22:50:59] mapping host Host1 to volume sub1block5, clone_id=1000000123 in subsystem Block1
```

```
[2025-02-27 22:50:59] mapping host Host1 to volume subblock5 finished,remote_mapping_object_id=5, remote_volume_object_id=7
[2025-02-27 22:50:59] bulk mapping finished successfully ... |
```

Completed

blockmapping show

This command displays details of a mapping of a block host to a volume. The mapping can be a read-write volume mapping that enables the block host to access the data on the volume, or a read-only snapshot volume that enables the block host to access a specific snapshot of the volume.

Usage

```
blockmapping show --id ID
```

Required Parameters

--id ID	Specifies which block mapping to display.
---------	---

Example

```
vcli: admin> blockmapping show --id 113
+-----+-----+
| Id      | 113      |
| Volume id | 119      |
| BlockHost id | 1      |
| Snapshot-data | {'id': 1, 'name': 'Vol1Snap'}|
+-----+-----+
```

Command Output

Id	The mapping ID.
Volume id	The ID of the volume mapped, by the mapping, to the specified host.
BlockHost id	The ID of the block host mapped, by the mapping, to the specified volume.
Snapshot-data	For a snapshot volume mapping, this shows the name and ID of which snapshot of the volume is mapped by the mapping.

## blockmapping unmap\_host\_volumes

This command unmaps one or more volumes from a host.

## Usage

```
blockmapping unmap_host_volumes --blockhost-id ID
                                --volume-ids IDS
```

## Required Parameters

<code>--blockhost-id</code> ID	Specifies the block host.
<code>--volume-ids</code> IDS	Specifies the volumes to unmap from the specified host. Specify IDS as a comma separated list of volume IDs.

## Example

```
vcli: admin> blockmapping unmap_host_volumes --blockhost-id 1 --volume-ids 2
```

```
Waiting ...
Waiting ... \
[2025-02-27 22:07:06] un-mapping host Host1 to volume sub1block2
[2025-02-27 22:07:06] un-mapping host Host1 to volume sub1block2 finished
[2025-02-27 22:07:06] bulk mapping finished successfully ... |
```

```
Completed
vcli: admin>
```

## blockmapping unmap\_volume\_hosts

This command removes mappings between a block volume and specified block hosts.

## Usage

```
blockmapping unmap_volume_hosts --volume-id ID
                                --blockhost-ids IDS
```

## Required Parameters

<code>--volume-id</code> ID	Specifies the volume.
-----------------------------	-----------------------

--blockhost-ids IDS	Specifies the block hosts to unmap from the specified volume. Specify IDS as a comma separated list of block host IDs.
------------------------	--

## Example

```
vcli: admin> blockmapping unmap_volume_hosts --volume-id 2 --blockhost-ids 1

Waiting ...
Waiting ... \
[2025-03-02 14:43:02] un-mapping host Host1 to volume BlockTeam1Vol2
[2025-03-02 14:43:02] un-mapping host Host1 to volume BlockTeam1Vol2 finished
[2025-03-02 14:43:02] bulk mapping finished successfully ... |

Completed
vcli: admin>
```

# callhomeconfig commands

## callhomeconfig list

This command lists all call home configurations.

## Usage

```
callhomeconfig list
```

## Example

```
vcli: admin> callhomeconfig list
+---+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Bundle-enabled | Bundle-interval(Minutes) | Log-enabled | Proxy-scheme | Proxy-host |
Proxy-port | Proxy-username | Log-interval(Minutes) | Customer | Site | Location | Test-mode |
| Callhome-upload-destination | Verify-ssl | Support-channel | Max-upload-concurrency | Max-u
pload-bandwidth | Cloud-enabled | Cloud-api-domain | Cloud-api-key
| Cloud-registered | Cloud-subdomain | Obfuscated | Compress-method | Aggregated | Upload-vi
a-vms | Luna-on-alarm-enabled | Luna-on-alarm-interval(Hours) | Luna-analyze-period |
+---+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | False | 60 | True | http | | False |
3128 | | 30 | | customA | | | False |
| On-Prem | True | True | None | None
| False | api.cloud.vastdata.com | ***** | True
| vastcs | False | zstd | False | False | False
| 24 | 5 | |
+---+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

## callhomeconfig modify

This command modifies the call home configuration. The call home feature sends non-sensitive information to VAST support to provide proactive analysis and fast response on critical issues.

## Usage

```
callhomeconfig modify --id ID
```

```

[--enable]
[--disable]
[--bundle-interval INTERVAL]
[--log-interval INTERVAL]
[--luna-on-alarm-interval INTERVAL]
[--luna-analyze-period INTERVAL]
[--customer CUSTOMER_NAME]
[--site SITE_NAME]
[--location LOCATION]
[--proxy-scheme PROXY_SCHEME]
[--proxy-host PROXY_HOST]
[--proxy-port PROXY_PORT]
[--proxy-username PROXY_USER]
[--proxy-password PROXY_PWD]
[--test-mode]
[--prod-mode]
[--verify-ssl-enable]
[--verify-ssl-disable]
[--support-channel-enable]
[--support-channel-disable]
[--max-upload-concurrency MAX_UPLOAD_CONCURRENCY]
[--max-upload-bandwidth MAX_UPLOAD_BW]
[--cloud-enable]
[--cloud-disable]
[--cloud-api-key CLOUD_API_KEY ]
[--cloud-api-domain CLOUD_DOMAIN]
[--cloud-subdomain CLOUD_SUBDOMAIN]
[--aws-s3-bucket-subdir ]
[--aws-s3-ak S3_ACCESS_KEY]
[--aws-s3-sk S3_SECRET_KEY]
[--aws-s3-bucket-name S3_BUCKET]
[--compress-method COMPRESS_METHOD ]
[--obfuscated-enable]
[--obfuscated-disable]
[--upload-via-vms-enable]
[--upload-via-vms-disable]
[--alt-s3-host-port PORT]

```


## Options

<code>--id ID</code>	The call home configuration to modify. This is assumed to be 1.
<code>--enable</code>	When enabled, VAST Cluster sends logs to the support server.
<code>--disable</code>	Disables the call home configuration.
<code>--bundle-interval INTERVAL</code>	The interval (in minutes) to send VMS metadata and metrics to the support server. If disabled, no VMS metadata and metrics is not sent.
<code>--log-interval INTERVAL</code>	The interval (in minutes) to send system state data to the support server. If disabled, no system state data is sent.

<code>--luna-on-alarm-interval INTERVAL</code>	<p>The interval (in hours) to send Luna results to the support server. If disabled, no Luna data is sent.</p> <p>Specify INTERVAL in hours.</p>
<code>--luna-analyze-period INTERVAL</code>	<p>Sets the period for Luna analysis.</p> <p>Specify INTERNAL in hours.</p>
<code>--customer CUSTOMER_NAME</code>	<p>Your customer name.</p> <p>Specify CUSTOMER_NAME as a string</p>
<code>--site SITE_NAME</code>	<p>The name of the site where the cluster is installed.</p> <p>Specify SITE_NAME as a string</p>
<code>--location LOCATION</code>	<p>The location of the site.</p> <p>Specify LOCATION as a string</p>
<code>--proxy-scheme PROXY_SCHEME</code>	<p>Specifies the proxy scheme. Relevant only if a proxy host is used.</p> <p>Specify PROXY_SCHEME as a string</p>
<code>--proxy-host PROXY_HOST</code>	<p>Specifies the proxy host. Relevant only if a proxy host is used.</p> <p>Specify PROXY_HOST as a string</p>
<code>--proxy-port PROXY_PORT</code>	<p>Specifies the proxy port. Relevant only if a proxy host is used.</p> <p>Specify PROXY_PORT as an integer</p>
<code>--proxy-username PROXY_USER</code>	<p>Specifies the proxy username. Relevant only if a proxy host is used.</p> <p>Specify PROXY_USER as a string</p>
<code>--proxy-password PROXY_PWD</code>	<p>Specifies the proxy password. Relevant only if a proxy host is used.</p> <p>Specify PROXY_PASSWD as a string</p>
<code>--test-mode</code>	<p>Enables test mode. This is only used by VAST Support personnel, for testing.</p>



<code>--prod-mode</code>	Sets the production support server as the destination for call home bundles. For normal use, this should be enabled.
<code>--verify-ssl-enable</code>	Enables SSL verification. Disable if, for example, you are sending the call home data through a proxy server that does not have an SSL certificate recognized by VAST Cluster. VAST Cluster recognizes SSL certificates from a large range of widely recognized certificate authorities (CAs). VAST Cluster may not recognize an SSL certificate signed by your own in-house CA.
<code>--verify-ssl-disable</code>	Disables SSL verification.
<code>--support-channel-enable</code>	Enables the support channel.
<code>--support-channel-disable</code>	Disables the support channel.
<code>--max-upload-concurrency</code> <code>MAX_UPLOAD_CONCURRENCY</code>	Sets the maximum number of concurrent threads. Specify <code>MAX_UPLOAD_CONCURRENCY</code> as an integer
<code>--max-upload-bandwidth</code> <code>MAX_UPLOAD_BW</code>	Sets the maximum upload bandwidth (in bytes/sec) Specify <code>MAX_UPLOAD_BW</code> as an integer
<code>--cloud-enable</code>	Enables reporting call home data to VAST Cloud Call Home service
<code>--cloud-disable</code>	Disables reporting to VAST Cloud services
<code>--cloud-api-key</code> <code>CLOUD_API_KEY</code>	Overrides the Cloud services API key. Specify <code>CLOUD_API_KEY</code> as a string
<code>--cloud-api-domain</code> <code>CLOUD_API_DOMAIN</code>	Overrides the Cloud services API domain name Specify <code>CLOUD_API_DOMAIN</code> as a string
<code>--cloud-subdomain</code> <code>CLOUD_SUBDOMAIN</code>	Specifies the unique subdomain for the customer in the VAST Cloud call home service.

	Specify CLOUD_SUBDOMAIN as a string
<code>--aws-s3-bucket-subdir</code>	Specifies the S3 bucket prefix for the bundle upload.
<code>--aws-s3-ak</code> <code>S3_ACCESS_KEY</code>	<p>Sets the S3 access key to upload the bundle to an S3 bucket.</p> <div>  <p><b>Note</b></p> <p>When configuring call home, leave this field empty. This setting is used for support bundle uploads.</p> </div> <p>Specify S3_ACCESS_KEY as a string</p>
<code>--aws-s3-sk</code> <code>S3_SECRET_KEY</code>	<p>Sets the S3 secret key to upload the bundle to an S3 bucket.</p> <p>Specify S3_SECRET_KEY as a string</p>
<code>--aws-s3-bucket-name</code> <code>S3_BUCKET</code>	<p>Specifies the name of the S3 bucket to which to upload the bundle.</p> <p>Specify S3_BUCKET as a valid S3 bucket name (string)</p>
<code>--compress-method</code> <code>COMPRESS_METHOD</code>	<p>Sets the compression method used to compress call home bundles:</p> <ul style="list-style-type: none"> <li>• zstd (default)</li> <li>• gzip</li> </ul> <p>Specify COMPRESS_METHOD as a string</p>
<code>--obfuscated-enable</code>	Enables obfuscation of data in call home bundles, metrics and heartbeats. These details are replaced with a non-reversible hash: file and directory names, IP addresses, host names, user names, passwords, MAC addresses.
<code>--obfuscated-disable</code>	Disables data obfuscation.
<code>--upload-via-vms-enable</code>	Uploads a call home bundle via VMS. Otherwise, the upload is done from each node.
<code>--upload-via-vms-</code>	Disables upload via VMS.

disable	
<code>--alt-s3-host-port</code> <code>HOST_PORT</code>	<p>Specifies an alternate S3 endpoint on a VAST cluster.</p> <p>Use this as an alternative to the VAST Cloud Call Home Service (so, <code>--cloud-disable</code> is asserted). If used, use also <code>--aws-s3-ak</code> and <code>--aws-s3-sk</code> to indicate the access keys to the S3 bucket on the VAST cluster.</p> <p>Specify <code>HOST_PORT</code> as a string in the form <code>host:port</code>.</p>

## Example

This example configures call home to the VAST Cloud Call Home service

```
vcli: admin> callhomeconfig modify --id 1 --cloud-enable --prod-mode
```

This must be followed by

```
vcli: admin> callhomeconfig register-cluster --id 1 --email myemail@mydomain.com
```

This example configures call home to an alternate S3 bucket on a VAST Cluster (and disables access to the Cloud Call Home service).

```
vcli: admin> callhomeconfig modify --id 1 --cloud-disable --prod-mode --alt_s3_host_port myhost:myport --aws-s3-ak < S3_ACCESS_KEY> --aws-s3-sk <S3_SECRET_KEY>
```

### callhomeconfig register-cluster

This command registers the cluster to VAST Cloud Services. This enables call home data to be collected by VAST.

You must enable VAST Cloud Services (`callhomeconfig modify --id ID --cloud-enable`) before using the `register-cluster` command.

## Usage

```
callhomeconfig register-cluster --id ID --email --EMAIL
```

## Required Parameters

<code>--id ID</code>	Specifies the configuration to register.
<code>--email EMAIL</code>	The email of the VAST Cloud Services super user.

## Example

```
vccli: admin> register-cluster --id 1 --email myemail@mydomain.com
```

### callhomeconfig send

This command sends a test message to VAST Support, to test the call home configuration.

## Usage

```
callhomeconfig send --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies the id of the configuration
----------------------	---------------------------------------

## Example

```
vccli: admin> callhomeconfig send --id 1
```

### callhomeconfig show

This command displays details of a specific call home configuration.

## Usage

```
object show --id ID
```

## Optional Parameters

<code>--id ID</code>	Specifies which configuration to display. This is assumed to be 1.
----------------------	--

## Example

```
vccli: admin> callhomeconfig show --id 1
```

```
+-----+-----+
| ID                | 1 |
| Bundle-enabled    | False |
| Bundle-interval (Minutes) | 60 |
| Log-enabled       | False |
| Proxy-scheme      | http |
| Proxy-host        |      |
| Proxy-port        | 3128 |
| Proxy-username    |      |
+-----+-----+
```

Log-interval (Minutes)	60	
Customer		
Site		
Location		
Test-mode	True	
Callhome-upload-destination	Matar	
Verify-ssl	True	
Support-channel	False	
Max-upload-concurrency	None	
Max-upload-bandwidth	None	
Cloud-enabled	False	
Cloud-api-domain	api.cloud.vastdata.com	
Cloud-api-key	*****	
Cloud-registered	False	
Cloud-subdomain	None	
Obfuscated	False	
Compress-method	zstd	
Aggregated	False	
Upload-via-vms	False	
Luna-on-alarm-enabled	False	
Luna-on-alarm-interval (Hours)	24	
Luna-analyze-period	5	
+-----+-----+		

# carrier commands

## carrier activate

This command activates a device carrier slot.

## Usage

```
carrier activate --id ID
```

## Required Parameters

<code>--id ID</code>	Specify the slot ID.
----------------------	----------------------

## Example

This example shows activation of slot 2:

```
vcli: admin> carrier activate --id 2
```

## carrier deactivate

This command deactivates a device carrier slot.

## Usage

```
carrier deactivate --id ID
```

## Required Parameters

<code>--id ID</code>	Specify the slot ID.
----------------------	----------------------

## Example

This example shows deactivation of slot 2:

```
vcli: admin> carrier deactivate --id 2
```

# cbox commands

## cbox led

This command makes a CBox's ID LED blink or turn off.

## Usage

```
cbox led --id ID
          --on|--off
```

## Required Parameters

<code>--id ID</code>	Specify the CBox ID.
<code>--on --off</code>	Sets the state of CBox LEDs: <ul style="list-style-type: none"><li>• <code>on</code>. The LEDs start blinking.</li><li>• <code>off</code>. The LEDs go off.</li></ul>

## Example

This example shows turning off the LEDs on CBox 1:

```
vcli: admin> cbox led --id 1 --off
```

## cbox list

This command displays all CBoxes and their details.

## Usage

```
cbox list
```

## Example

```
vcli: admin> cbox list
+-----+-----+-----+-----+-----+-----+
| ID | Name          | Cluster  | Uid      | Description | Rack-id |
+-----+-----+-----+-----+-----+-----+
| 1  | cbox-62ZGX04 | myvast   | 62ZGX04  | None        | None     |
+-----+-----+-----+-----+-----+-----+
```

## cbox modify

This command adds or modifies a CBox description.

## Usage

```
cbox modify [--id ID]|[--uid UID]
            --description DESCRIPTION
```

## Required Parameters

<code>{--id ID} [--uid UID]</code>	Identify the CBox to be modified by specifying its ID or UID.
<code>--description DESCRIPTION</code>	Specify a description for the CBox. For example, you can add a data center name, rack location, and so on.

## Example

This example shows adding a description to CBox 1:

```
vccli: admin> cbox modify --id 1 --description mynewcbox
```

## cbox refresh\_uid

This command refreshes the CBox UID.

## Usage

```
cbox refresh_uid --id ID
```

## Required Parameters

<code>--id ID</code>	Specify the CBox ID.
----------------------	----------------------

## Example

This example shows refreshing the UID for CBox 1:

```
vccli: admin> cbox refresh_uid --id 1
```



## cbox show

This command displays details of a specific CBox.

## Usage

```
cbox show --id ID
```

## Required Parameters

<code>--id ID</code>	Specify a CBox ID.
----------------------	--------------------

## Example

```
vcli: admin> cbox show --id 1
+-----+-----+
| ID      | 1      |
| Name    | cbox-62ZGX04 |
| Cluster | myvast |
| Uid     | 62ZGX04 |
| Description | None  |
| Rack-id | None   |
+-----+-----+
```

# cluster commands

## cluster close-protocol-handle

This command closes open filehandles. To list open filehandles, run [cluster list-open-protocol-handles](#).

## Usage

```
cluster close-protocol-handle --file-path FILE_PATH
                             --session-id SESSION_ID
                             --session-handle-unique-id SESSION_HANDLE_UNIQUE_ID
                             [--share SHARE]
                             [--cluster-id ID]
                             [--tenant-name TENANT_NAME]
```

## Required Parameters

<code>--file-path FILE_PATH</code>	Specify the full file path without providing <code>--share</code> or the path to the file within the share if you do provide <code>--share</code> .
<code>--session-id SESSION_ID</code>	Specifies the session ID. This is listed as <i>session_id</i> in the output of <a href="#">cluster list-open-protocol-handles</a> .
<code>--session-handle-unique-id SESSION_HANDLE_UNIQUE_ID</code>	Specifies the unique ID of the session handle you want to close. This is listed as <i>unique_id</i> in the output of <a href="#">cluster list-open-protocol-handles</a> .

## Options

<code>--share SHARE</code>	Use this option to specify the share name. See <i>--file-path</i> in <i>Required Parameters</i> .
<code>--cluster-id ID</code>	This value defaults to 1. If your cluster ID is not 1, use this option to specify the cluster ID. If you are not sure, you can check the cluster ID by running <code>cluster list</code> .
<code>--tenant-name TENANT_NAME</code>	<p>Specifies the tenant under which the file resides.</p> <p>Specify <code>TENANT_NAME</code> as the name of the tenant.</p> <p>Defaults to the default tenant.</p>

# Example

```
vccli: admin> cluster close-protocol-handle --file-path test.txt --share test2 --session-id 0x1c00200000002 --session-handle-unique-id 0x1c0020000000b
Filehandle was closed successfully
```

## cluster list-locks

This command lists open byte range locks.

# Usage

```
cluster list-locks --path FILE_PATH
                    [--tenant-id TENANT_ID]
                    [--direction prev|next]
```

# Required Parameters

<code>--path FILE_PATH</code>	Specifies the file path.  Specify <code>FILE_PATH</code> as the full file path relative to the tenant.
-------------------------------	--

# Options

<code>--tenant-id TENANT_ID</code>	Specifies the tenant under which the file resides.  Defaults to the default tenant.
<code>--direction prev next</code>	Specifies pagination direction.

# Example

```
vccli: admin> cluster list-locks --path /open.txt
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
| Type | Create-Time | Caller | Owner | Exclusive | Offset | Length | Svid | State | Lock-pat
h | Tenant-name | Open-id | Lock-id | Lock-granted-type | Client-id | Create-time-seconds |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
```

## cluster list-snapshoted-paths-remote

This command lists paths on a remote replication peer that are protected by snapshots. Snapshots can be manual snapshots or snapshots created by protected paths.

## Usage

```
cluster list-snapshoted-paths-remote --peer-id ID
                                     --tenant TENANT_NAME
```

## Required Parameters

<code>--peer-id ID</code>	Specifies which replication peer for which to list paths that have snapshots.
<code>--tenant TENANT_NAME</code>	Specifies the name of the tenant on the remote peer for which to return paths.

## Example

```
vcli: admin> cluster list-snapshoted-paths-remote --peer-id 1 --tenant default
+-----+
| Name |
+-----+
| /a/  |
+-----+
```

## cluster list-clone-snapshoted-paths-remote

This command lists snapshots on a specified path on a remote replication peer.

## Usage

```
cluster list-clone-snapshoted-paths-remote --peer-id ID
                                           --path ID
                                           --tenant TENANT_NAME
```

## Required Parameters

<code>--peer-id ID</code>	Specifies the replication peer by its ID.
<code>--path PATH</code>	Specifies the path on the remote peer. To retrieve paths for a given remote peer, run the <a href="#">cluster list-clone-snapshoted-paths-remote</a> command.

<pre>--tenant TENANT_NAME</pre>	Specifies the name of the tenant on the remote peer to which the path belongs.
---------------------------------	--

## Example

```
vcli: admin> cluster list-clone-snapshotted-paths-remote --peer-id 1 --path /a/ --tenant default
+-----+
| Name |
+-----+
| a-1 |
| a-2 |
+-----+
```

### cluster list-tenants-remote

This command lists tenants on a remote replication peer.

## Usage

```
cluster list-tenants-remote --peer-id ID
```

## Required Parameters

<pre>--peer-id ID</pre>	Specifies the ID of the remote replication peer for which to display tenants.
-------------------------	---

## Example

```
vcli: admin> cluster list-tenants-remote --peer-id 3
```

### cluster list-open-protocol-handles

This command lists open file handles.

## Usage

```
cluster list-open-protocol-handles --file-path FILE_PATH
                                   [--share SHARE]
                                   [--tenant-name TENANT_NAME]
                                   [--cluster-id ID]
                                   [--show-nfs4.1-only-handles]
```

## Required Parameters

<code>--file-path</code> <code>FILE_PATH</code>	<p>Specifies the file path.</p> <p>Specify <code>FILE_PATH</code> as the full file path without providing <code>--share</code> or the path to the file within the share if you do provide <code>--share</code>.</p>
--	---

## Options

<code>--share SHARE</code>	Specifies the name of the share in which the file resides.
<code>--tenant-name TENANT_NAME</code>	<p>Specifies the tenant under which the file resides.</p> <p>Specify <code>TENANT_NAME</code> as the name of the tenant.</p> <p>Defaults to the default tenant.</p>
<code>--cluster-id ID</code>	<p>Specifies the cluster ID.</p> <p>You can verify the cluster ID by running <code>cluster list</code>.</p> <p>Default: 1.</p>
<code>--show-nfsv.1-only-handles</code>	Filters the display to include only handles that can be used by NFSv4.1 clients.

## Example

```
vccli: admin> cluster list-open-protocol-handles --file-path /run_bg_many_mercuries/p_smb-f_SM
B-windows--saucy-woodpecker
```

File handle

```
+-----+-----+-----+-----+-----+
+-----+
|          ehandle | clone_id | delete_pending | has_any_lease | lease_break_in_progress |
number_open_protocol_handles |
+-----+-----+-----+-----+-----+
+-----+
| 0xec4b600e1132e090 |      0x0 | False          | False          | False          |
1 |
+-----+-----+-----+-----+-----+
+-----+
```

Open protocol handles

```
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+
| session_id | unique_id | client_ip      | share_access | access_mask | has_lease |
| is_durable | username  | proto_type    | nfs4_seqid  | is_nfs_expirable | nfs_expiration_time |
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
```

0x350a200000003	0x350a200000534	172.19.222.78	R+W+D		0x100081	False
False	UNKNOWN	SMB	N/A	N/A	N/A	

## cluster modify

This command modifies various cluster settings.

## Usage

```
cluster modify [--id ID]
               [--name]
               [--psnt PSNT]
               [--motd MOTD]
               [--motd-append-to-default]
               [--auto-logout-timeout AUTO_LOGOUT_TIMEOUT]
               [--auth-provider-refresh-interval AUTH_PROVIDER_REFRESH_INTERVAL]
               [--enable-metrics|--disable-metrics]
               [--enable-module-metrics|--disable-module-metrics]
               [--enable-trash|--disable-trash]
               [--trash-gid TRASH_GID]
               [--enable-suppressed-showmount|--disable-suppressed-showmount]
               [--enable-showmount-hide-slash|--disable-showmount-hide-slash]
               [--smb-privileged-user-name SMB_PRIVILEGED_USER_NAME]
               [--enable-smb-privileged-user|--disable-smb-privileged-user]
               [--smb-privileged-group-sid SMB_PRIVILEGED_GROUP_SID]
               [--enable-smb-privileged-group|--disable-smb-privileged-group]
               [--smb-read-write-privileged-group-access]
               [--smb-read-only-privileged-group-access]
               [--default-others-share-level-perm FULL|CHANGE|READ]
               [--audit-dir-name AUDIT_DIR_NAME]
               [--read-access-users]
               [--read-access-users-groups]
               [--max-file-size MAX_FILE_SIZE]
               [--max-retention-period PERIOD]
               [--max-retention-timeunit UNIT]
               [--enable-vast-db-audit]
               [--disable-vast-db-audit]
               [--enable-json-audit]
               [--disable-json-audit]
               [--max-audit-dir-size MAX_DIR_SIZE]
               [--keep-forever]
               {
               {
                 [--audit-protocols PROTOCOLS]
                 [--audit-operations OPERATIONS]
                 [--audit-options OPTIONS]
                 [--enable-audit-settings|--disable-audit-settings]
               }
               |
                 [--disable-audit]
               }
               [--enable-similarity|--disable-similarity]
               [--cluster-certificate mTLS_CERT]
               [--cluster-private-key mTLS_KEY]
               [--root-certificate ROOT_CERT]
               [--remove-mtls-certificates]
               [--remove_nfs4_certificate]
               [--enable-use-flash-write-buffers]
               [--disable-use-flash-write-buffers]
               [--enable-bucket-replication]
```

[--enable-bucket-db-replication]  
[--max-cluster-write-bw-mb BW]

## General Options

<code>--id ID</code>	The ID of the cluster.
<code>--name NAME</code>	Modifies the cluster name.
<code>--psnt PSNT</code>	Changes the PSNT of the cluster.
<code>--motd MOTD</code>	Specify a custom Message of the Day (MOTD) text. VAST OS displays this text on login.
<code>--motd-append-to-default</code>	Specify to append a custom message of the day set by <code>--motd</code> to the default. If this parameter is not specified, and a custom message is set using <code>--motd</code> , the custom message replaces the default message.
<code>--auto-logout-timeout</code> <code>AUTO_LOGOUT_TIMEOUT</code>	Sets the inactivity period for auto logout for VAST OS on all nodes (seconds).
<code>--auth-provider-refresh-interval</code> <code>AUTH_PROVIDER_REFRESH_INTERVAL</code>	Sets the Auth Provider Refresh Interval (in seconds).

## NFS Options

<code>--enable-trash</code>	Enables the trash folder feature. Once enabled, trash folder access permission can be given to NFSv3 client hosts per view policy.
<code>--disable-trash</code>	Disables the trash folder feature.
<code>--trash-gid</code>	Specify the GID of a group of non-root users to allow them access to the trash folder.
<code>--enable-suppressed-showmount</code>	Enables <a href="#">suppression</a> of the output of the <code>showmount</code> command for Linux NFSv3 clients.



<code>--disable-suppressed-showmount</code>	Disables suppression of <code>showmount</code> command output.
<code>--enable-showmount-hide-slash</code>	When specified, the response to the <code>showmount</code> command does not show the root export ("/").
<code>--disable-showmount-hide-slash</code>	When specified, the response to the <code>showmount</code> command includes the root export ("/"):  <code>'/' everyone(rw)</code>



## SMB Options

<code>--smb-privileged-user-name</code> <code>SMB_PRIVILEGED_USER_NAME</code>	Specify a custom username for the privileged SMB user. If not specified, the user name of the SMB privileged user is 'vastadmin'.
<code>--enable-smb-privileged-user</code>	Enables the privileged SMB user.
<code>--disable-smb-privileged-user</code>	Disables the privileged SMB user.
<code>--smb-privileged-group-sid</code> <code>SMB_PRIVILEGED_GROUP_SID</code>	Specify a custom SID for the privileged SMB group. If not specified, the privileged SMB group SID is the Backup Operators domain group SID (S-1-5-32-551).
<code>--enable-smb-privileged-group</code>	Enables the privileged SMB group.
<code>--disable-smb-privileged-group</code>	Disables the privileged SMB group.
<code>--smb-read-write-privileged-group-access</code>	Grants read and write control access to the privileged SMB group. Members of the group can perform backup and restore operations on all files and directories, without requiring read or write access to the specific files and directories.
<code>--smb-read-only-</code>	Grants only read-only access control to the privileged SMB group. Members of the group


privileged-group-access	can perform backup operations on all files and directories without requiring read access to the specific files and directories. They cannot perform restore operations without write access to the specific files and directories.
<pre>--default-others-share-level-perm FULL READ CHANGE</pre>	<p>Sets the default 'Everyone' Group SMB share-level permission for the cluster. This default permission affects all views in which share-level ACL is disabled.</p> <p>For more information about SMB share-level permissions, see <a href="#">Share-Level ACLs</a>.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li><code>FULL</code> (default). Grants all SMB users <i>full control</i> share-level access to views that have <i>Share-level ACL</i> disabled.</li> <li><code>READ</code>. Grants all SMB users <i>read</i> share-level access to views that have <i>Share-level ACL</i> disabled.</li> <li><code>CHANGE</code>. Grants all SMB users <i>change</i> share-level access to views that have <i>Share-level ACL</i> disabled.</li> </ul>


## S3 Options

<pre>--remove-s3-key-pair</pre>	Removes the current SSL server certificate key pair for the S3 service.
<pre>--s3-certificate S3_CERTIFICATE</pre>	Specify content of SSL server certificate file, to install SSL certificate for the S3 service, to enable S3 clients to connect to the S3 service over HTTPS. Include also the <code>--s3-private-key</code> parameter to complete the certificate installation.
<pre>--s3-private-key S3_PRIVATE_KEY</pre>	Specify content of SSL server key file, to install SSL certificate for the S3 service, to enable S3 clients to connect to the S3 service over HTTPS. Include also the <code>--s3-certificate</code> parameter to complete the certificate installation.
<pre>--enable-bucket-replication</pre>	<p>Enables bucket replication on the cluster.</p> <p>If enabled, any S3 buckets on or under replicated protected paths are automatically recreated at the replication target(s), provided they are configured on the local cluster (the replication source peer) with the <i>S3 default</i> view policy. They also receive the following properties of the source bucket:</p> <ul style="list-style-type: none"> <li>Object versioning status</li> <li>s3 lock enablement status</li> <li>object ownership rule</li> <li><i>allow anonymous access</i> status</li> </ul>


	<ul style="list-style-type: none"> <li>• <i>has db</i> status</li> <li>• The bucket policy</li> </ul> <p>If a bucket was created manually on the target with the same name as the equivalent bucket on the source peer, the source bucket's properties are applied to the manually created bucket.</p> <p>If this feature is not enabled, buckets must be created on the target paths in order to enable S3 access to the replicated data.</p> <div>  <p><b>Note</b></p> <p>You cannot disable this feature.</p> </div>
<pre>--enable- bucket-db- replication</pre>	<p>When this option is specified, VAST Cluster automatically creates configuration for the replicated VAST Database bucket on the destination replication peer. If disabled, the configuration needs to be created manually.</p> <div>  <p><b>Note</b></p> <p>Once enabled, this capability cannot be disabled.</p> </div>

## Protocol Auditing Options

<pre>--audit-dir- name AUDIT_DIR_NAME</pre>	<p>Sets a name for the audit directory. A directory of this name will be created directly under the root directory of the default tenant in the Element Store. Protocol audit records are written to this directory.</p> <p>The default is <code>.vast_audit_dir</code>.</p>
<pre>--read-access- users</pre>	<p>Identifies users to grant them read access to all files in the audit directory.</p> <p>Specify users as a comma-separated list of user names.</p> <div>  <p><b>Tip</b></p> <p>To make the audit directory accessible to clients, create a view on the directory.</p> </div>

<pre>--read-access- users-groups</pre>	<p>Identifies user groups to grant users in those groups read access to all files in the audit directory.</p> <p>Specify groups as a comma-separated list of user names.</p> <div>  <div> <p><b>Tip</b></p> <p>To make the audit directory accessible to clients, create a view on the directory.</p> </div> </div>
<pre>--max-file- size MAX_FILE_SIZE</pre>	<p>Sets the maximum size of each file of audit records in the audit directory. Audit records are written to subdirectories of the audit directory per CNode core. Records written to each directory roll over to a new file when the file reaches this size.</p> <p>This setting limits the size of each audit file, but it does not limit the total size of all audit files.</p> <p>Specify <code>MAX_FILE_SIZE</code> with units of MB, GB, TB and so on.</p> <p>Default: <i>1024MB</i></p> <p>For example: <code>--max-file-size 2GB</code></p>
<pre>--max- retention- period PERIOD</pre>	<p>Sets the maximum period for which the audit files are kept. The period is defined in units of measurements that you specify in the <code>--max-retention-timeunit</code> parameter.</p> <p>Specify an integer. The default value is 1.</p> <p>This option cannot be specified together with <code>--keep-forever</code>.</p>
<pre>--max- retention- timeunit UNIT</pre>	<p>Sets the unit of measurement for the period specified in <code>--max-retention-period</code>.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> <li>• <code>h</code> for hours (default)</li> <li>• <code>D</code> for days</li> <li>• <code>W</code> for weeks</li> <li>• <code>M</code> for months</li> <li>• <code>y</code> for years</li> </ul>
<pre>--max-audit- dir-size MAX_DIR_SIZE</pre>	<p>Sets a maximum size for the audit directory. No limit is set by default.</p> <p>Specify <code>MAX_DIR_SIZE</code> with units of MB, GB, TB and so on.</p> <p>Example: <code>--max-audit-dir-size 200 GB</code></p>

<pre>--keep-forever</pre>	<p>When this option is specified, audit files are kept for an unlimited period of time. By default, this setting is disabled.</p> <p>This option cannot be specified together with <code>--max-retention-period</code>.</p>
<pre>--audit-protocols PROTOCOLS</pre>	<p>Lists access protocols for which you are enabling or disabling protocol auditing.</p> <p>Use this parameter together with <code>--enable-audit-settings</code> or <code>--disable-audit-settings</code> to enable or disable auditing of the specified protocols.</p> <p>When specifying <code>--audit-protocols</code>, you must also specify <code>--audit-operations</code> and/or <code>--audit-options</code>.</p> <p>Specify <code>PROTOCOLS</code> as a comma-separated list of values. Valid values:</p> <ul style="list-style-type: none"> <li>• NFSv3</li> <li>• NFSv4.1</li> <li>• SMB</li> <li>• S3</li> <li>• NDB (VAST DataBase)</li> </ul>
<pre>--audit-operations OPERATIONS</pre>	<p>Lists categories of protocol operations for which you are enabling or disabling protocol auditing.</p> <p>Use this parameter together with <code>--audit-protocols</code> and either <code>--enable-audit-settings</code> or <code>--disable-audit-settings</code> to enable or disable auditing of the specified protocol operations.</p> <p>Specify <code>OPERATIONS</code> as a comma-separated list of values, each of which specifies a <a href="#">category of operations</a> being audited. Valid values:</p> <ul style="list-style-type: none"> <li>• <code>create_delete_files_dirs_objects</code>. Operations that create or delete files, directories or objects.</li> <li>• <code>modify_data</code>. Operations that modify data.</li> <li>• <code>modify_data_md</code>. Operations that modify metadata.</li> <li>• <code>read_data</code>. Operations that read data.</li> <li>• <code>read_data_md</code>. Operations that read metadata.</li> <li>• <code>session_create_close</code>. Session creation and closing operations for sessions that use Kerberos 5 authentication (<code>krb5</code>, <code>krb5i</code>, or <code>krb5p</code>).</li> </ul>
<pre>--audit-options OPTIONS</pre>	<p>Lists audit options to enable or disable.</p> <p>Use this parameter together with <code>--audit-protocols</code> and either <code>--enable-audit-settings</code> or <code>--disable-audit-settings</code> to enable or disable the specified options for the specified protocols.</p>

	<p>Specify <code>OPTIONS</code> as a comma-separated list of values. Valid values:</p> <ul style="list-style-type: none"> <li><code>log_full_path</code>. If enabled (default for all protocols), audit records contain the full Element Store path to the requested resource. This may affect performance. When disabled, the view path is recorded.</li> <li><code>log_username</code>. Disabled by default. If enabled, audit records contain the username (if a username can be retrieved from the auth provider).</li> </ul>
<code>--enable-audit-settings</code>	<p>Enables audit settings specified in the same command line by the <code>--audit-protocols</code>, <code>--audit-operations</code> and <code>--audit-options</code> parameters.</p> <p>Any previously enabled audit settings (protocols, operations or options) remain enabled.</p>
<code>--enable-json-audit</code>	<p>Enables saving audit logs to a JSON file.</p>
<code>--enable-vast-db-audit</code>	<p>Enables saving audit logs to a VAST DataBase table</p>
<code>--disable-audit-settings</code>	<p>Disables audit settings specified in the same command line by the <code>--audit-protocols</code>, <code>--audit-operations</code> and <code>--audit-options</code> parameters.</p> <p>Any previously enabled audit settings (protocols, operations or options) that you do not specify in the same command line remain enabled.</p>
<code>--disable-audit</code>	<p>Disables protocol auditing.</p> <div>  <p><b>Tip</b></p> <p>To enable protocol auditing, run <code>cluster modify</code> with the <code>--audit-protocols</code> options specified, as well as <code>--audit-options</code> and/or <code>--audit-operations</code>.</p> </div>
<code>--disable-json-audit</code>	<p>Disables saving audit logs to a JSON file. Existing records are not deleted until the <code>--max-retention-period</code> elapses.</p>
<code>--disable-vast-db-audit</code>	<p>Disables saving audit logs to a VAST DataBase table. Existing records are not deleted until the <code>--max-retention-period</code> elapses.</p>

## Similarity Options

<code>--enable-similarity</code>	Enables similarity-based data reduction.
<code>--disable-similarity</code>	Disables similarity-based data reduction (enabled by default).

## mTLS Options

<code>--cluster-certificate</code> <code>mTLS_CERT</code>	<p>Uploads the certificate (public key) file content of a CA signed certificate for mTLS encryption.</p> <p>Replace each new line in the file content with <code>\n</code> and paste the file content into the command line between single quotes as <code>mTLS_CERT</code>.</p> <p>For example:</p> <pre>cluster modify --cluster-certificate '-----BEGIN CERTIFICATE-----&lt;certificate_text&gt;-----END CERTIFICATE-----'</pre>
<code>--cluster-private-key</code> <code>mTLS_KEY</code>	<p>Uploads the private key file content of a CA signed certificate for mTLS encryption.</p> <p>Replace each new line in the file content with <code>\n</code> and paste the file content into the command line between single quotes as <code>mTLS_KEY</code>.</p>
<code>--root-certificate</code> <code>ROOT_CERT</code>	<p>Uploads the CA's root certificate for mTLS encryption.</p> <p>Replace each new line in the file content with <code>\n</code> and paste the file content into the command line between single quotes as <code>ROOT_CERT</code>.</p>
<code>--remove-mtls-certificates</code>	Removes mTLS certificates from the cluster.

## Flash Write Buffer Options

<code>--enable-use-flash-write-buffers</code>	Enables the use of flash memory devices to store write buffers. This allows the total available write buffer size on the cluster to be increased.
<code>--disable-use-flash-write-buffers</code>	Disable use of flash memory devices to store write buffers. When disabled, all write buffers are flushed and allocated buffer space is returned.

## QoS Options

<code>--max-cluster-write-bw-mb BW</code>	<p>Sets the cluster-wide write bandwidth limit to help prevent situations where workloads controlled with prioritized QoS policies are not served at the expected QoS because of extensive media consumption by non-prioritized workloads. For more information, see <a href="#">QoS Overview</a>.</p> <p>Specify <code>BW</code> in MB/s. '0' (zero) means no limit is set, which is the default value.</p> <p>The recommended cluster-wide maximum is 70% of the cluster's total write bandwidth.</p>
---	---

## Example

This example changes the SMB privileged user name to 'vast\_backup\_user'.

```
vcli: admin> cluster modify --smb-privileged-user-name vast_backup_user
```

### cluster release-lock

This command releases locks on a specified file path.

## Usage

```
cluster release-lock --path PATH
                        [--cluster-id ID]
                        [--tenant-id TENANT_ID]
                        [--recursively]
                        [--unlock-type TYPE]
                        [--unlock-id ID]
                        [--lock-type TYPE]
```

## Required Parameters

<code>--path PATH</code>	Specifies a path to a file, relative to the default tenant or to the specified tenant (if specified).
--------------------------	---

## Options

<code>--cluster-id ID</code>	<p>Specifies the cluster ID.</p> <p>You can verify the cluster ID by running <code>cluster list</code>.</p> <p>Default: 1.</p>
<code>--tenant-id</code>	Specifies a non default tenant by ID. The specified file path is relative to the tenant. If not specified,



TENANT_ID	the default tenant is assumed.
--recursively	Deletes all locks on the file recursively.
--unlock-type TYPE	<p>The type of unlock operation to perform:</p> <ul style="list-style-type: none"> <li>• ALL. To unlock all locks on the specified file.</li> <li>• SINGLE. To unlock a single lock on the specified file.</li> </ul>
--unlock-id ID	If unlock-type is <i>SINGLE</i> , include this option to specify the unlock ID for the specific lock that you want to unlock.
--lock-type TYPE	<p>If unlock-type is <i>SINGLE</i>, include this lock to specify type of lock:</p> <ul style="list-style-type: none"> <li>• NLM4. An NLM4 lock taken by an NFSv3 client.</li> <li>• NFSv4. An NFSv4 lock.</li> <li>• SMB. An SMB lock.</li> </ul>

## Example

```
vcli: admin> cluster release-lock --path /dev/test.txt --unlock-type ALL
```

### cluster rotate-master-encryption-group-key

If encryption is enabled with encryption type *CIPHER\_TRUST\_KMIP* (where encryption keys are managed externally on Thales Group CipherTrust Data Security Platform), this command generates a new version of the master key. The master key is used by the cluster to encrypt the data encryption keys when they are retrieved from the EKM and distributed by the cluster node that hosts the encryption service client to other cluster nodes.

The master key is generated by the cluster and should not be rotated from the EKM itself.

## Usage

```
cluster rotate-master-encryption-group-key
```

## Example

```
vcli: admin> cluster rotate-master-encryption-group-key
Are you sure you want to rotate Master encryption group key? [y/N] y
Master encryption group key was rotated successfully.
```

## cluster run-upgrade-validations

This command performs pre-upgrade validations without performing an upgrade on the VAST Cluster core platform and VMS software. The upgrade validations performed with this command are also performed as part of the upgrade process. Running them alone before initiating the upgrade can help you identify an issue that may require fixing so that the upgrade will be successful or to decide to skip hardware validations when actually upgrading.

## Usage

```
cluster run-upgrade-validations [--skip-os-upgrade-validations]
                                [--skip-hardware-validations]
                                [--force]
```

## Options

<code>--skip-os-upgrade-validations</code>	<p>Skips validations that are needed for OS upgrades, including:</p> <ul style="list-style-type: none"><li>• Unmounting certain mountpoints on the hosts if they are found.</li><li>• Validating free space</li><li>• Validating the presence and correct configuration of pre-requisite files on the hosts.</li><li>• Verifying supported ssd models in DBoxes.</li><li>• Verifying host-to-switch connectivity.</li><li>• Checking every DBox FPGA is responsive.</li></ul>
<code>--skip-hardware-validations</code>	<p>Skips validation of hardware component health. Use with caution since component redundancy is important in NDU. The following validations are skipped with this option selected:</p> <ul style="list-style-type: none"><li>• Verification that the MTU of each NIC is correctly configured.</li><li>• Verifying that all DNodes are active.</li><li>• Verifying SSH connectivity to all hosts.</li></ul>
<code>--force</code>	<p>Skips validation of the NVRAM RAID state, which should not be disabled for upgrade.</p>

## cluster set-password

This command sets passwords for the OS and IPMI admin users on all CNodes and DNodes in the cluster. Servers that are added to the cluster or re-activated after the command is run receive the same passwords.

## Usage

```
cluster set-password [--root]
```

[--vastdata]  
[--ipmi]

## Options

<code>--root</code>	<p>Sets the password of the Linux OS superuser on all CNodes and DNodes in the cluster. The user name is (and remains) <i>root</i>.</p> <p>After you enter the command, you are prompted to enter the new password and subsequently to re-enter the new password. The VAST CLI then informs you when the password change is finished.</p>
<code>--vastdata</code>	<p>Sets the password of the Linux OS user <i>vastdata</i> on all CNodes and DNodes in the cluster. The user name is (and remains) <i>vastdata</i>.</p> <p>After you enter the command, you are prompted to enter the new password and subsequently to re-enter the new password. The VAST CLI then informs you when the password change is finished.</p>
<code>--ipmi</code>	<p>Sets the password of the IPMI admin user on all CNodes and DNodes in the cluster. The user name is (and remains) <i>admin</i>.</p> <p>After you enter the command, you are prompted to enter the new password and subsequently to re-enter the new password. The VAST CLI then informs you when the password change is finished.</p>

## Example

This example changes the IPMI password for all CNodes and DNodes to *admin1212*:

```
vcli: admin> cluster set-password --ipmi
Enter new password:
Password: admin1212
Re-enter new password:
Password: admin1212
Setting new password for user ipmi
```

Waiting ...

```
[2019-12-23 11:04:27] mycluster: changing password for all hosts ... \
[2019-12-23 11:04:36] finished changing password ... |
```

Completed

### cluster show

This command displays cluster settings and metrics. With each option the cluster displays different information. With no options, the default output does not include all of the details that you can display with the options.

## Usage

```
cluster show --id ID [--advanced]
                  [--audit]
```

```

[--auto-logout-timeout]
[--capacity]
[--motd]
[--notified-version]
[--performance]
[--raid-state]
[--space-health]
[--tech-details]
[--last-imported-build]
[--gn]
[--shard-expansion-status]
[--turbo-boost-flag]

```

## Options

<code>--id ID</code>	Specifies which cluster to display. This is usually not needed.
<code>--advanced</code>	Displays advanced metrics.
<code>--audit</code>	Displays protocol auditing configuration.
<code>--auto-logout-timeout</code>	Displays the current inactivity period after which VAST OS automatically logs out, in seconds.
<code>--capacity</code>	Displays capacity metrics.
<code>--motd</code>	Displays a customized Message of the Day text, if set, which is displayed by VAST OS on login.
<code>--notified-version</code>	Displays details of an available upgrade version that has been made available by notification.
<code>--performance</code>	Displays performance metrics.
<code>--raid-state</code>	Displays the state of the cluster's RAID striping across SSDs and related statuses and details.
<code>--space-health</code>	Displays health status of stripes and metadata on the cluster.
<code>--tech-details</code>	Displays a selection of settings and metrics.

--last-imported-build	Displays details of the last upgrade version that has been uploaded to the cluster.
--gn	Displays information about the Global Namespace

## Examples

```
vcli: admin> cluster show
```

+-----+-----+		
ID	1	
Name	Bonzo-02	
State	ONLINE	
Enabled	True	
Build	release-4-4-0-704763	
Total-Space (TB)	620.333	
Free-Physical-Space (TB)	330.139	
Physical-Space-In-use (TB)	290.195	
Physical-Aux-Space-In-Use (TB)	0.0	
Enable-encryption	False	
Free-physical-space-wo-overhead-tb	N/A	
Free-Usable-Capacity-TB (TB)	292.752	
Usable-Capacity-TB (TB)	555.366	
User-Space (TB)	1124.713	
Free-Logical-Space (TB)	592.874	
Logical-Space-In-Use (TB)	977.146	
Logical-Aux-Space-In-Use (TB)	0.0	
SMB-privileged-group-sid		
DRR	2.0:1	
Enable-dr	True	
Enable-similarity	False	
Use-smb-privileged-user	True	
Use-smb-privileged-group	True	
Smb-privileged-group-full-access	True	
Smb-user-logon-name		
Smb-administrators-group-name		
Block All External Providers	True	
Rewrite-phase	NONE	
Rewrite-progress	0	
Rewrite-type	[]	
+-----+-----+		

```
vcli: admin> cluster show --audit
```

+-----+-----+		
ID	1	
Name	vast146-av	
Audit-dir-name		
Read-access-users	[]	
Read-access-users-groups	[]	
Max-file-size (GB)	1.024	
Max-retention-period	1	
Max-retention-timeunit	h	
Protocols	[]	
Enable-json-audit	False	
Enable-vast-db-audit	False	
Max-audit-dir-size	None	
+-----+-----+		

```
Operations to audit
```

+-----+-----+	
Operation	Enabled

Create/Delete Files/Dirs/Objects	True
Modify Data	True
Modify Metadata	True
Read Data	True
Read Metadata	True
Session create/close	False

Audit record options

Audit record option	Enabled
Log full path	True
Log username	False

vccli: admin> cluster show --motd

motd	None
------	------

vccli: admin> cluster show --last-imported-build

build	704763
sys_version	4.4.0.26
os_version	12.7.14
ssd_version	8DV10510
nvrnram_version	E2010485
bmc_fw_versions	{'x86_64': {'file': 'bmc/x86_64/rom-Maverick-12.21.1.ima', 'version': '12.21.1'}, 'aarch64': {'file': 'bmc/aarch64/rom-ceres-0.45.2.ima', 'version': '0.45.2', 'mcu_file': 'bmc/aarch64/Ceres_MC_U_v0.0.4.1.hex', 'mcu_version': '0.0.4.1', 'pci_switch_file': 'bmc/aarch64/pcie_v1.4.4.3_mfg_v1.4.0.2.fw', 'pci_switch_version': '1.4.4.3'}}

vccli: admin> cluster show --auto-logout-timeout

auto_logout_timeout	0
---------------------	---

vccli: admin> cluster show --capacity

ID	1
Name	Bonzo-02
Total-Space(TB)	620.333
Free-Physical-Space(TB)	330.165
Physical-Space-In-use(TB)	290.169
Physical-Aux-Space-In-Use(TB)	0.0
User-Space(TB)	1124.795
Free-Logical-Space(TB)	592.982
Logical-Space-In-Use(TB)	977.119
Usable-Auxiliary-Space-In-Use(TB)	0.000
Usable-Capacity(TB)	555.349
Free-Usable-Capacity(TB)	292.775
Usable-Capacity-TB(TB)	555.349
Free-Usable-Capacity-TB(TB)	292.775
Logical-Aux-Space-In-Use(TB)	0.0

Used handles percent	4.65	
DRR	2.0:1	

+-----+

vccli: admin> cluster show --raid-state

ID	1	
Name	Bonzo-02	
SSD-RAID-state	HEALTHY	
NVRAM-RAID-state	HEALTHY	
Memory-RAID-state	HEALTHY	
RAID-rebuild-progress	SSD 0 NVRAM 0 Memory 0	
RAID-drives-can-fail	0	

+-----+

vccli: admin> cluster show --performance

ID	1	
Name	Bonzo-02	
R-IOPS	93	
W-IOPS	933	
R-MD-IOPS	2353	
W-MD-IOPS	8	
R-BW(MB/s)	92.39	
W-BW(MB/s)	698	
R-Latency(msec)	2.723	
W-Latency(msec)	8.059	

+-----+

vccli: admin> cluster show --tech-details

ID	1	
Name	Bonzo-02	
Leader IP	172.16.3.52	
Leader-cnode	cnode-3-52	
Micro-shards	512	
Micro-stripe-groups	64	
Mega-shards	512	
Mega-stripe-groups	64	
CNode-Cores	14	
Max-NVRAM-Replication-Factor	2	
Max-SSD-Capacity-Percent	100	
Max-NVRM-Capacity-Percent	100	
PSNT	Bonzo-02	
GUID	decd8b71-aa6f-56a2-8430-75f736285572	
Online-start-time	None	
Deployment-time	2021-04-06T10:29:20.699575Z	
Uptime		
DBox HA support	False	
Upgrade-phase	NONE	
Mgmt-vip	10.27.200.60	
Mgmt-CNode	cnode-3-51	
VMS-Inner-VIP	172.16.4.60	
VMS-Inner-VIP-CNode	cnode-3-53	
Use-smb-privileged-user	True	
Use-smb-privileged-group	True	
Smb-privileged-group-full-access	True	
Smb-user-logon-name		
SMB-privileged-group-sid		

+-----+

vccli: admin> cluster show --space-health

ID	1	
Name	Bonzo-02	
Stripes-health	HEALTHY	
Metadata-health	HEALTHY	

```
+-----+-----+
```

```
vccli: admin> cluster show --notified-version
++
++
```

## cluster stat

This command shows statistics for a certain path and, optionally, a tenant.

## Usage

```
cluster stats --path PATH
               [--tenant-id ID]
```

## Required Parameters

<code>--path PATH</code>	Specifies the path for which to display the details.
--------------------------	--

## Options

<code>--tenant-id ID</code>	Specifies the tenant for which to display the details.
-----------------------------	--

## Example

```
vccli: admin> cluster stat --path /dir1/dir2 --tenant-id 3
+-----+-----+
| owning_user   | user1@example.com |
| owning_uid    | 10001              |
| owning_group  |                     |
| owning_gid    | 20002              |
| has_default_acl | True               |
| is_directory  | True               |
| children      | 0                  |
| abac_tags     | ['red', 'blue']    |
+-----+-----+
```

## cluster upgrade

This command upgrades the VAST Cluster core platform and VMS software. It can also upgrade the CNode OS along with the VAST Clustersoftware.

All upgrades are performed from a package file per target release. The single package file per release includes the image files for all upgradable components, including CNode OS and NVRAM as well as the core platform software image and the VMS image.

Before running the command, download the package file to the `/vast/bundles` directory on the management CNode. For download details, see the target version's release notes or request them from support.



# Usage

```
cluster upgrade --build-package PACKAGE_FILE_PATH
               [--enable-dr]
               [--force]
               [--os-upgrade]
               [--skip-hw-check]
               [--cnodes-batch-size-percentage]
               [--dnodes-batch-size-percentage]
               [--isolcpus]
               [--vms-only-upgrade]
               [--skip-sw-validations]
               [--fw-upgrade]
               [--bmc-upgrade]
```

## Required Parameters

<code>--build-package</code> <code>PACKAGE_FILE_PATH</code>	<p>Specifies the full path to the package file for the target release. The package file must be located in the <code>/vast/bundles</code> directory on the management CNode.</p> <p>For example: <code>--build-package /vast/bundles/release-3.6.0-123450.vast.tar.gz</code></p>
--	--

## Options

<code>--enable-dr</code>	For a cluster that does not have data reduction enabled before upgrade, this option enables data reduction along with the upgrade.
<code>--force</code>	Forces upgrade regardless of version or upgrade state. Use this option if you need to upgrade to the same version as already installed or if a previous upgrade failed without the upgrade state clearing.
<code>--os-upgrade</code>	Upgrades the OS on the CNodes and DNodes in addition to the core platform and VMS software.
<code>--skip-hw-check</code>	<p>Skips those pre-upgrade validations that are related to hardware when pre-upgrade validations are run after bundle upload.</p> <p>Use with caution since component redundancy is important in NDU.</p> <p>Do not use with OS upgrade.</p>
<code>--skip-sw-validations</code>	Include this option to proceed even if there is a deny list or if NVRAM RAID state is degraded.

<code>--cnodes-batch-size-percentage PERCENTAGE</code>	<p>Overrides the default percentage of CNodes to upgrade in parallel in one batch. The default batch size is 10%.</p> <p>Maximum: 50</p> <p>Example: <code>--cnodes-batch-size-percentage 20</code></p>
<code>--dnodes-batch-size-percentage PERCENTAGE</code>	<p>Overrides the default percentage of DNodes to upgrade in parallel in one batch.</p> <p>The default batch size is 20%.</p> <p>Maximum: 37.5</p> <p>Example: <code>--dnodes-batch-size-percentage 25</code></p>
<code>--isolcpus</code>	Resets the configuration of isolated CPUs according to a formula.
<code>--vms-only-upgrade</code>	Upgrades VMS version only.
<code>--fw-upgrade</code>	For CERES, upgrades firmware for BMC, MCU, PCI and Bluefield.
<code>--bmc-upgrade</code>	Upgrades BMC and all relevant components (FPGA, BIOS, UBM, CPLD and so on).

## Example

```
vcli: admin> cluster upgrade --build-package /vast/bundles/release-3.6.0-123450.vast.tar.gz
```

## cluster vast-db-configure

This command sets configuration parameters for VAST Database and VAST Catalog, such as the number of splits and subsplits. Fine-tuning the splits helps improve VAST Catalog performance for queries that require scanning a large amount of table rows.

## Usage

```
cluster vast-db-configure {--splits COUNT | --subsplits COUNT}
```

## Options

<code>--splits COUNT</code>	Sets the number of splits (concurrent threads) used when processing VAST Database and VAST Catalog queries.
-----------------------------	---

	Valid values are from 1 to 256. The default value is 8.
<code>--subsplits</code> COUNT	Sets the number of subsplits for VAST Database and VAST Catalog queries.  Valid values are from 1 to 64. The default value is 8.

## Example

```
vcli: admin> cluster vast-db-configure --splits 16
```

### cluster vast-db-show-config

This command displays configuration parameters for VAST Database and VAST Catalog, such as the number of splits and subsplits.

## Usage

```
cluster vast-db-show-config
```

# cnode commands

## cnode activate

This command activates a CNode.

## Usage

```
cnode activate [--id ID]{--name NAME}  
               [--replace]  
               [--power-on]  
               [--skip-network-validation]
```

## Required Parameters

<code>{--id ID}{--name NAME}</code>	Identify the CNode to be activated by specifying the CNode ID or name.
-------------------------------------	--

## Options

<code>--replace</code>	Activates a replacement CNode.
<code>--power-on</code>	Activates the CNode and powers it on.
<code>--skip-network-validation</code>	Skips internal network validation before CNode activation.

## Example

This example shows activation of CNode `cnode-1`:

```
vccli: admin> cnode activate --name cnode-1
```

## cnode add

This command adds a CNode to a cluster.

## Usage

```
cnode add --ip IP  
          [--cluster-id ID]  
          [--force]
```

## Required Parameters

<code>--ip IP</code>	Specifies the IP address to be assigned to the CNode.
----------------------	---

## Options

<code>--cluster-id ID</code>	Specifies the ID of the cluster to which to add the CNode.
<code>--force</code>	Lets you add a CNode whose CPU isolation ( <code>isolcpus</code> ) settings are not aligned with other CNodes in the same CBox.

## Example

This example shows adding a CNode with IP 203.0.13.43 to cluster 2:

```
vccli: admin> cnode add --ip 203.0.13.43 --cluster-id 2
```

### **cnode deactivate**

This command deactivates a CNode.

## Usage

```
cnode deactivate [--id ID]|[--name NAME]
                [--power-off]
```

## Required Parameters

<code>{--id ID} [--name NAME]</code>	Identify the CNode to deactivate by specifying its CNode ID or name.
--------------------------------------	--

## Options

<code>--power-off</code>	Deactivates the CNode and powers it off.
--------------------------	--

## Example

This example shows deactivation of CNode `cnode-3` :

```
vcli: admin> cnode deactivate --name cnode-3
```

### cnode highlight

This command highlights a CNode.

When you *highlight* a CNode, its power LED goes off while LEDs on other CNodes are turned on, enabling you to easily identify the CNode specified in the command.

## Usage

```
cnode highlight [--id ID]|[--name NAME]
```

## Required Parameters

<code>{--id ID} [--name NAME]</code>	Identify the CNode to be highlighted by specifying the CNode ID or name.
--------------------------------------	--

## Example

This example shows highlighting of CNode 2:

```
vcli: admin> cnode highlight --id 2
```

### cnode led

This command makes the CNode LED blink or turns it off.

## Usage

```
cnode led [--id ID]|[--name NAME]
          --blink|--off
```

## Required Parameters

<code>{--id ID} [--name NAME]</code>	Specifies the ID or the name of the CNode to manage the LED state.
<code>--blink --off</code>	Sets the LED state: <ul style="list-style-type: none"><li>• <code>blink</code>. The LED starts blinking.</li></ul>

	<ul style="list-style-type: none"> <li>• <code>off</code>. The LED goes off.</li> </ul>
--	---

# Example

This example shows turning off the LED on CNode 1:

```
vcli: admin> cnode led --id 1 --off
```

## cnode list

This command displays all CNodes and their details.

# Usage

```
cnode list [--ip IP]
           [--state STATE]
           [--name NAME]
           [--enabled]
           [--vipool-id ID]
```

# Options

<code>--ip IP</code>	Filters the list by CNode IP address.
<code>--state STATE</code>	<p>Filters the list by CNode state.</p> <p>Specify one of the following values for STATE:</p> <ul style="list-style-type: none"> <li>• INIT</li> <li>• ACTIVATING</li> <li>• ACTIVE</li> <li>• DEACTIVATING</li> <li>• INACTIVE</li> <li>• FAILING</li> <li>• FAILED</li> </ul>
<code>--name NAME</code>	Filters the list by CNode name.
<code>--enabled</code>	If specified, only enabled CNodes are displayed.

<code>--vippool-id ID</code>	Filters the list by VIP pool ID.
------------------------------	----------------------------------

## Example

```

vcli: admin> cnode list
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
| ID | Name          | IP          | Mgmt-ip      | Host Name | State  | Enabled | Build
| Management | Cluster    | OS-Version | CBox         | Cores | Serial          | LED Status
| BMC-FW-Version |
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
| 7 | cnode-3-177 | 203.0.13.177 | 198.51.100.101 | myhost    | ACTIVE | True    | releas
e-4-5-0-776058 | Yes      | mycluster  | 12.8.10      | cbbox-200051 | 14     | a4:bf:01:7c:d
1:1b | off        | 1.93.240    |
| 2 | cnode-3-178 | 203.0.13.178 | 198.51.100.103 | myhost    | ACTIVE | True    | releas
e-4-5-0-776058 | No       | mycluster  | 12.8.10      | cbbox-200051 | 14     | a4:bf:01:7c:c
1:da | off        | 1.93.240    |
| 6 | cnode-3-179 | 203.0.13.179 | 198.51.100.105 | myhost    | ACTIVE | True    | releas
e-4-5-0-776058 | No       | mycluster  | 12.8.10      | cbbox-200051 | 14     | a4:bf:01:7c:c
8:1a | off        | 1.93.240    |
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+

```

## cnode remove

This command removes a CNode.

## Usage

```
cnode remove [--id ID]{--name NAME}
```

## Required Parameters

<code>{--id ID}{--name NAME}</code>	Identify a CNode to display by specifying the CNode ID or name.
-------------------------------------	---

## Example

This example shows removing CNode 3:

```
vcli: admin> cnode remove --id 3
```

## cnode rename

This command renames a CNode.



## Usage

```
cnode rename --id ID --name NEWNAME
```

## Required Parameters

<code>--id ID</code>	Specify the CNode ID.
<code>--name NEWNAME</code>	Specify a new name for the CNode.

## Example

This example shows renaming CNode 4 to `cnode-g`:

```
vccli: admin> cnode rename --id 4 --name cnode-g
```

### cnode show

This command displays details of a specific CNode.

## Usage

```
cnode show [--id ID]{[--name NAME]}
```

## Required Parameters

<code>{--id ID}{[--name NAME]}</code>	Identify a CNode to display by specifying the CNode ID or name.
---------------------------------------	---

## Example

```
vccli: admin> cnode show --id 2
```

```
+-----+-----+
| ID      | 2      |
| Name    | cnode-3|
| IP      | 203.0.113.178 |
| Mgmt-ip | 192.88.99.3 |
| Host Name | myhost |
| State   | ACTIVE  |
| Enabled  | True    |
| Build    | release-4-5-0-776058 |
| Management | No    |
| Cluster  | mycluster |
| OS-Version | 12.8.10 |
| CBox     | cbox-200051 |
| Cores    | 14      |
+-----+-----+
```

Serial	a4:bf:01:7c:c1:da	
LED Status	off	
BMC-FW-Version	1.93.240	
+-----+-----+		

# column commands


## column delete

This command deletes one or more columns from a VAST database table.

## Usage

```
column delete --table-name TABLE
              --schema-name SCHEMA
              --arrow-schema COLUMNS_TO_DELETE
              --database-name DATABASE
              [--tenant-id TENANT]
```

## Required Parameters

<code>--table-name TABLE</code>	Enter the name of the table that contains the column or columns to be deleted.
<code>--schema-name SCHEMA</code>	Enter the name of the schema where the table resides.
<code>--arrow-schema COLUMNS</code>	<div>Enter a comma-separated list of columns to be deleted.</div> <div>The columns are specified using the Arrow format, for example:</div> <div><code>col1-int8,col2-string,col3-int8</code></div> <div> <b>Note</b></div> <div>Complex data types are not supported on this command. To delete a column with a complex data type, <a href="#">use</a> VAST Web UI.</div>
<code>--database-name DATABASE</code>	Enter the name of the database where the table resides.

## Options

<code>--tenant-id TENANT</code>	Enter the ID of the tenant where the database resides.
---------------------------------	--

	If omitted, the default tenant is assumed.
--	--

## Example

This example shows deleting the column `age` from the table named `cats` :

```
vccli: admin> column delete --table-name cats --schema-name schemal --arrow-schema age-int8 --
database_name vastdb
```

### column list

This command lists columns in a VAST Database table.

## Usage

```
column list --database-name DATABASE
            --schema-name SCHEMA
            --table-name TABLE
            [--page PAGE]
            [--page-size PAGE_SIZE]
            [--name COLUMN_NAME]
            [--name-startswith PREFIX]
            [--tenant-id TENANT]
```

## Required Parameters

<code>--database-name DATABASE</code>	Specifies the name of the database containing the table.
<code>--schema-name SCHEMA</code>	Specifies the name of the schema containing the table.
<code>--table-name TABLE</code>	Specifies the name of the table containing the columns.

## Options

<code>--page PAGE</code>	Specifies the specific page in the output list, by its number. This parameter is used only if <code>page-size</code> is set. Default is the first page.
<code>--page-size PAGE_SIZE</code>	Specifies the maximum number of columns to list per output page. Default: 100.

--name COLUMN_NAME	Specifies the name of a specific column.
--name-startswith PREFIX	Specifies a prefix to filter the column names.
--tenant-id TENANT	Enter the ID of the tenant where the database resides  If omitted, the default tenant is assumed.

## Example

```

vcli: admin> column list --database-name table-1 --schema-name schema_jypxvnuobg --table-name
table_jypxvnuobg
+-----+-----+-----+-----+
| Name          | Raw-field          | Database-name      | Schema-name        | T
able-name      |                    |                    |                    |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| theage        | int8               | table-1            | schema_jypxvnuobg | t
able_jypxvnuobg |                    |                    |                    |
| thestate      | string             | table-1            | schema_jypxvnuobg | t
able_jypxvnuobg |                    |                    |                    |
| thedate       | date32[day]        | table-1            | schema_jypxvnuobg | t
able_jypxvnuobg |                    |                    |                    |
| thetinyint    | int8               | table-1            | schema_jypxvnuobg | t
able_jypxvnuobg |                    |                    |                    |
| theint        | int32              | table-1            | schema_jypxvnuobg | t
able_jypxvnuobg |                    |                    |                    |
| thebigint     | int64              | table-1            | schema_jypxvnuobg | t
able_jypxvnuobg |                    |                    |                    |
| thetime       | time32[ms]         | table-1            | schema_jypxvnuobg | t
able_jypxvnuobg |                    |                    |                    |
| thetimestamp  | timestamp[ms]      | table-1            | schema_jypxvnuobg | t
able_jypxvnuobg |                    |                    |                    |
| thevarchar    | string             | table-1            | schema_jypxvnuobg | t
able_jypxvnuobg |                    |                    |                    |
| thebool       | bool               | table-1            | schema_jypxvnuobg | t
able_jypxvnuobg |                    |                    |                    |
| thereal       | float              | table-1            | schema_jypxvnuobg | t
able_jypxvnuobg |                    |                    |                    |
| thedouble     | double             | table-1            | schema_jypxvnuobg | t
able_jypxvnuobg |                    |                    |                    |
| thedecimal    | decimal128(38, 0) | table-1            | schema_jypxvnuobg | t
able_jypxvnuobg |                    |                    |                    |
+-----+-----+-----+-----+
+-----+-----+

```

## column show

This command shows details for a specific column in a VAST Database table.

# Usage

```
column show --database-name DATABASE
            --schema-name SCHEMA
            --table-name TABLE
            --name COLUMN
            [--tenant-id TENANT]
```

## Required Parameters

<code>--database-name DATABASE</code>	Specifies the name of the database containing the table.
<code>--schema-name SCHEMA</code>	Specifies the name of the schema containing the table.
<code>--table-name TABLE</code>	Specifies the name of the table containing the columns.
<code>--name COLUMN</code>	Specifies the name of a specific column.

## Options

<code>--tenant-id TENANT</code>	Specifies the ID of the tenant where the database resides  If omitted, the default tenant is assumed.
---------------------------------	---

## Example

```
vccli: admin> column show --database-name tabular-1 --schema-name schema_jypxvnuobg --table-name table_jypxvnuobg --name theage
```

```
+-----+-----+
| Name      | theage |
| Raw-field | int8   |
| Database-name | tabular-1 |
| Schema-name | schema_jypxvnuobg |
| Table-name | table_jypxvnuobg |
+-----+-----+
```

### column rename

This command renames a table column.

## Usage

```
column rename --name OLD_COLUMN_NAME
```

```

--owner-name OWNER
--table-name TABLE
--schema-name SCHEMA
--database-name DATABASE
--new-column-name NEW_COLUMN_NAME
[--tenant-id TENANT]

```

## Required Parameters

--name OLD_COLUMN_NAME	Enter the name of the column to be renamed.  If the column to be renamed is a nested column, use the dotted format a.b.c to specify the parent column(s) (a, b) and the nested column (c).
--owner-name OWNER	Enter the user name of the VAST database owner.
--table-name TABLE	Enter the name of the table that contains the column.
--schema-name SCHEMA	Enter the name of the schema where the table resides.
--database-name DATABASE	Enter the name of the database where the table resides.
--new-column-name name	Enter a new name for the column. The name must meet the requirements for S3 object names.

## Options

--tenant-id TENANT	Enter the ID of the tenant where the database resides  If omitted, the default tenant is assumed.
--------------------	---

## Example

The following example shows renaming a column named `abc` into `xyz`:

```

vcli: admin> column rename --name abc --owner-name ed --table-name customer --schema-name sch
emal --database-name vastdb --new-column-name xyz

```

# dnode commands

## dnode activate

This command activates a DNode.

## Usage

```
dnode activate --id ID
                [--replace]
                [--power-on]
                [--skip-network-validation]
```

## Required Parameters

<code>--id ID</code>	Specify the DNode ID.
----------------------	-----------------------

## Options

<code>--replace</code>	Activates a replacement DNode.
<code>--power-on</code>	Activates the DNode and powers it on.
<code>--skip-network-validation</code>	Skips internal network validation before DNode activation.

## Example

This example shows activation of DNode 2:

```
vccli: admin> dnode activate --id 2
```

## dnode deactivate

This command deactivates a DNode.

## Usage

```
dnode deactivate --id ID
                  [--power-off]
```



## Required Parameters

<code>--id ID</code>	Specify the DNode ID.
----------------------	-----------------------

## Options

<code>--power-off</code>	Deactivates the DNode and powers it off.
--------------------------	--

## Example

This example shows deactivation of DNode 2:

```
vcli: admin> dnode deactivate --id 2
```

### **dnode highlight**

This command highlights a DNode.

When you *highlight* a DNode, its power LED goes off while LEDs on other DNodes are turned on, enabling you to easily identify the DNode specified in the command.

## Usage

```
dnode highlight --id ID
```

## Required Parameters

<code>--id ID</code>	Specify the DNode ID.
----------------------	-----------------------

## Example

This example shows highlighting of DNode 2:

```
vcli: admin> dnode highlight --id 2
```

### **dnode led**

This command makes the DNode LED blink or turns it off.

## Usage

```
dnode led --id ID
          --on|--off
```

## Required Parameters

<code>--id ID</code>	Specify the DNode ID.
<code>--on --off</code>	Sets the LED state: <ul style="list-style-type: none"><li>• <code>on</code>. The LED starts blinking.</li><li>• <code>off</code>. The LED goes off.</li></ul>

## Example

This example shows turning off the LED on DNode 1:

```
vcli: admin> dnode led --id 1 --off
```

### dnode list

This command displays all DNodes and their details.

## Usage

```
dnode list [--ip IP]
           [--state STATE]
           [--enabled]
```

## Options

<code>--ip IP</code>	Filters the list by DNode IP address.
<code>--state STATE</code>	Filters the list by DNode state. Specify one of the following values for STATE: <ul style="list-style-type: none"><li>• <code>INIT</code></li><li>• <code>ACTIVATING</code></li><li>• <code>ACTIVE</code></li></ul>

	<ul style="list-style-type: none"> <li>• DEACTIVATING</li> <li>• INACTIVE</li> <li>• FAILING</li> <li>• FAILED</li> </ul>
--enabled	If specified, only enabled DNodes are displayed.

## Example

```

vcli: admin> dnode list
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name      | IP          | IPv6          | MGMT IP      | Hostname | State |
| Enabled | Build      | DBox        | DTray | Cluster  | OS      | Serial |
| LED Status | BMC FW version | Primary | BIOS   | Position |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | dnode-3-10 | 172.16.3.10 | fe80::bcef:19ff:fe0b:ff1e | 192.88.99.1 | v112dn2 | ACTIVE | | | | | |
| True | release-4-6-0-918031 | dbx-APF00E | None | vast112-az | 12.8.21 | 00:09:3d:07:75:a7 | off | 12.21.1 | False | V11.05 | top |
| 2 | dnode-3-9 | 172.16.3.9 | fe80::bcef:e9ff:febb:fb6 | 192.88.99.3 | v112dn1 | ACTIVE |
| True | release-4-6-0-918031 | dbx-APF00E | None | vast112-az | 12.8.21 | 00:09:3d:07:78:4a | off | 12.21.1 | True | V11.05 | bottom |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+

```

### dnode rename

This command renames a DNode.

## Usage

```
dnode rename --id ID --name NEWNAME
```

## Required Parameters

--id ID	Specify the DNode ID.
--name NEWNAME	Specify a new name for the DNode.

## Example

This example shows renaming DNode 9 to dnode-j:

```
vccli: admin> dnode rename --id 9 --name dnode-j
```

### dnode show

This command displays details of a specific DNode.

## Usage

```
dnode show --id ID
```

## Required Parameters

<code>--id ID</code>	Specify a DNode ID.
----------------------	---------------------

## Example

```
vccli: admin> dnode show --id 1
```

ID	1	
Name	dnode-3-10	
IP	172.16.3.10	
IPv6	fe80::bcef:19ff:fe0b:ff1e	
MGMT IP	192.88.99.1	
Hostname	v112dn2	
State	ACTIVE	
Enabled	True	
Build	release-4-6-0-918031	
DBox	dbox-APF00E	
DTray	None	
Cluster	vast112-az	
OS	12.8.21	
Serial	00:09:3d:07:75:a7	
LED Status	off	
BMC FW version	12.21.1	
Primary	False	
BIOS	V11.05	
Position	top	

# dns commands

## dns create

This command creates a DNS server configuration. For more information, see [DNS-Based Virtual IP Distribution](#).

## Usage

```
dns create --name NAME
           --ip IP
           [--domain-suffix DOMAIN_SUFFIX]
           [--gateway GATEWAY_IP]
           [--enable|--disable]
           [--net-type NET-TYPE]
           [--subnet-cidr CIDR]
           [--vlan VLAN]
```

## Required Parameters

<code>--name</code> NAME	Specifies a name for the DNS service configuration.
<code>--ip</code> IP	Assigns an IP address to the DNS service. DNS requests from your external DNS server must be delegated to this IP.

## Options

<code>--domain-suffix</code> DOMAIN_SUFFIX	<p>Specifies a suffix to append to domain names of each VIP pool. The suffix should complete each domain name to form a valid FQDN for DNS requests to target.</p> <p>For example, if you have two VIP pools <i>pool1</i> and <i>pool2</i>, you can set the domain name <i>domain1</i> on pool1 and domain name <i>domain2</i> on pool2 and the domain suffix to <i>.vastdata.ourcorp.com</i>. Requests for <i>domain1.vastdata.ourcorp.com</i> will be distributed among the VIPs in pool1 while requests for <i>domain2.vastdata.ourcorp.com</i> will be distributed among the VIPs in pool2.</p>
<code>--gateway</code> GATEWAY_IP	If the external DNS server doesn't reside on the same subnet as the DNS service IP address, include this option to specify the IP address of a gateway through which to connect to the DNS server. The gateway IP address must be on same subnet as the DNS service IP address.
<code>--enable --disable</code>	The DNS service is disabled by default. Include the <code>--enable</code> option to enable the service when you create it.

<pre>--net-type NET-TYPE</pre>	<p>Specifies which interface listens for DNS service delegation requests:</p> <ul style="list-style-type: none"> <li>EXTERNAL_PORT (default). The on-board server management interface.</li> <li>NORTH_PORT. The client-facing network interface.</li> <li>SOUTH_PORT. The internal network interface.</li> </ul>
<pre>--subnet-cidr CIDR</pre>	<p>Specifies the IP subnet, in CIDR format, on which the DNS service IP address resides.</p> <p>In CIDR notation, the subnet is expressed as the number of bits of each IP address that represent the subnet address.</p> <p>For example, the subnet mask 255.255.0.0 is expressed as <i>16</i> in CIDR notation.</p> <p>Specify only the trailing CIDR decimal number that indicates the subnet mask. For example, if the DNS service IP is <i>192.0.2.3</i> and the CIDR subnet is <i>24</i>, specify <i>24</i>.</p>
<pre>--vlan VLAN</pre>	<p>Specifies a VLAN. If your external DNS server is only exposed to a specific VLAN, include this option and specify the DNS server's VLAN to enable communication with the DNS service.</p>

## Example

```
vcli: admin> dns create --name vast_dns --ip 192.0.2.0 --domain-suffix vastdata.ourcorp.com
--gateway 192.0.4.0 --enable --subnet-cidr 16
```

### dns delete

This command deletes a DNS server configuration.

## Usage

```
dns delete --id ID
```

## Required Parameters

<pre>--id ID</pre>	<p>Specifies which DNS server configuration to delete.</p>
--------------------	--

## Example

```
vcli: admin> dns delete --id 1
```



<pre>--domain- suffix DOMAIN_SUFFIX</pre>	<p>Specifies a suffix to append to domain names of each VIP pool. The suffix should complete each domain name to form a valid FQDN for DNS requests to target.</p> <p>For example, if you have two VIP pools <i>pool1</i> and <i>pool2</i>, you can set the domain name <i>domain1</i> on pool1 and domain name <i>domain2</i> on pool2 and the domain suffix to <i>.vastdata.ourcorp.com</i>. Requests for <i>domain1.vastdata.ourcorp.com</i> will be distributed among the VIPs in pool1 while requests for <i>domain2.vastdata.ourcorp.com</i> will be distributed among the VIPs in pool2.</p>
<pre>--gateway GATEWAY_IP</pre>	<p>If the external DNS server doesn't reside on the same subnet as the DNS service IP address, include this option to specify the IP address of a gateway through which to connect to the DNS service. The gateway IP address must be on same subnet as the DNS service IP address.</p>
<pre>--enable -- disable</pre>	<p>Enable or disable the DNS service.</p>
<pre>--net-type NET-TYPE</pre>	<p>Specifies which interface listens for DNS service delegation requests:</p> <ul style="list-style-type: none"> <li>• <code>EXTERNAL_PORT</code> (default). The on-board server management interface.</li> <li>• <code>NORTH_PORT</code>. The client-facing network interface.</li> <li>• <code>SOUTH_PORT</code>. The internal network interface.</li> </ul>
<pre>--subnet-cidr CIDR</pre>	<p>Specifies the IP subnet, in CIDR format, on which the DNS service IP address resides.</p> <p>In CIDR notation, the subnet is expressed as the number of bits of each IP address that represent the subnet address.</p> <p>For example, the subnet mask 255.255.0.0 is expressed as <i>16</i> in CIDR notation.</p> <p>Specify only the trailing CIDR decimal number that indicates the subnet mask. For example, if the DNS service IP is <i>192.0.2.3</i> and the CIDR subnet is <i>24</i>, specify <i>24</i>.</p>
<pre>--vlan VLAN</pre>	<p>Specifies a VLAN. If your external DNS server is only exposed to a specific VLAN, include this option and specify the DNS server's VLAN to enable communication with the DNS service.</p>

## Example

```
vccli: admin> dns modify --enable
```

### dns show

This command displays details of a specific DNS server configuration.



# Usage

dns show --id ID

## Required Parameters

--id ID	Specifies which DNS server configuration to display.
---------	--

## Example

```
vcli: admin> dns show --id 1
```

```
+-----+-----+
| ID           | 1           |
| Name         | dns1        |
| DNS Service IP | 192.0.2.0   |
| DNS Service Gateway |           |
| DNS Service Suffix | mydns      |
| DNS Service Subnet | 24          |
| DNS Service VLAN | 0           |
| Net-type     | EXTERNAL_PORT |
| Enabled      | True         |
+-----+-----+
```

# dtray commands

## dtray deactivate

This command deactivates a DTray.

## Usage

```
dtray deactivate [--id ID|--name NAME]
                [--power-off]
```

## Required Parameters

<code>--id ID</code>	Specify the DTray ID.
<code>--name NAME</code>	Specify the DTray name.

## Options

<code>--power-off</code>	Deactivates the DTray and powers it off.
--------------------------	--

## Example

This example shows deactivation of DTray 2:

```
vcli: admin> dtray deactivate --id 2
```

## dtray activate

This command activates a DTray.

## Usage

```
dtray activate [--id ID|--name NAME]
               [--replace]
               [--power-on]
               [--skip-network-validation]
```

## Required Parameters

<code>--id ID</code>	Specify the DTray ID.
<code>--name NAME</code>	Specify the DTray name.

## Options

<code>--replace</code>	Activates a replacement DTray.
<code>--power-on</code>	Activates the DTray and powers it on.
<code>--skip-network-validation</code>	Skips internal network validation before DTray activation.

## Example

This example shows activation of DTray 2:

```
vcli: admin> dtray activate --id 2
```

### dtray led

This command makes all the DTray LEDs blink or turn them off.

## Usage

```
dtray led --id ID  
          {--on|--off}
```

## Required Parameters

<code>--id ID</code>	Specify the DTray ID.
<code>--on --off</code>	Sets the state of DTray LEDs: <ul style="list-style-type: none"><li>• <code>on</code>. The LEDs start blinking.</li></ul>

- off. The LEDs go off.

## Example

This example shows turning off the LEDs on DTray 1:

```
vccli: admin> dtray led --id 1 --off
```

### dtray list

This command displays all DTrays and their details.

## Usage

```
dtray list
```

## Example

```
vccli: admin> dtray list
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name | Position | State | Enabled | DBox | Cluster |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 2 | DTray-dbox-515-22070500100015-left | left | ACTIVE | True | dbox-100015 | vast
194-av | 0.51.2 | 192.88.99.4 | standby | 0.0.4.5 | C15-22070500100024 |
| 1 | DTray-dbox-515-22070500100015-right | right | ACTIVE | True | dbox-100015 | vast
194-av | 0.51.2 | 192.88.99.6 | active | 0.0.4.5 | C15-22070500100023 |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
```

### dtray rename

This command renames a DTray.

## Usage

```
dtray rename --id ID --name NEWNAME
```

## Required Parameters

<code>--id ID</code>	Specify the DTray ID.
<code>--name NEWNAME</code>	Specify a new name for the DTray.

# Example

This example shows renaming DTray 1 to newdtray:

```
vccli: admin> dnode rename --id 1 --name newdtray
```

## dtray show

This command displays details of a specific DTray.

# Usage

```
dtray show --id ID
```

# Required Parameters

<code>--id ID</code>	Specify a DTray ID.
----------------------	---------------------

# Example

```
vccli: admin> dtray show --id 2
+-----+-----+
| ID      | 2      |
| Name    | DTray-dbox-515-22070500100015-left |
| Position | left   |
| State   | ACTIVE |
| Enabled | True   |
| DBox    | dbox-100015 |
| Cluster | vast194-av |
| BMC-FW-Version | 0.51.2 |
| BMC IP  | 192.88.99.5 |
| MCU state | standby |
| MCU version | 0.0.4.5 |
| Serial Number | C15-22070500100024 |
+-----+-----+
```

# encryptiongroup commands

## encryptiongroup deactivate-encryption-group

This command deactivates an encryption group's encryption key. The key can be reinstated using `encryptiongroup reinstate-encryption-group`.

## Usage

```
encryptiongroup deactivate-encryption-group --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies the encryption group to deactivate.
----------------------	---

## Example

```
vccli: admin> encryptiongroup deactivate-encryption-group --id 6
```

## encryptiongroup list

This command displays all encryption groups and their details.

## Usage

```
encryptiongroup list
```

## Example

```
vccli: admin> encryptiongroup list
+-----+-----+-----+
+-----+
| Id | Name | Crn
| State |
+-----+-----+-----+
+-----+
| 4 | N/A | T_c4c5d91c-acfc-4e2e-bd6e-6406ef0fef2a_EP_c5c12fa2-61cf-4b83-9d2c-032b745bf5c2
| ACTIVE |
| 5 | N/A | T_207e8d20-809c-46b7-8847-5094f9554de4_EP_423c1f0e-bdba-44f7-a964-148c2ed4a1eb
| ACTIVE |
| 3 | N/A | asdfghj_1
| ACTIVE |
| 2 | N/A | INTERNAL_ENCRYPTION_GROUP_CRN
| ACTIVE |
+-----+-----+-----+
+-----+
```

## encryptiongroup reinstate-encryption-group

This command reinstates an encryption group that was deactivated.

### Usage

```
encryptiongroup reinstate-encryption-group --id ID
```

### Required Parameters

<code>--id ID</code>	Specifies which encryption group to reinstate.
----------------------	--

### Example

```
vccli: admin> encryptiongroup reinstate-encryption-group --id 5
```

## encryptiongroup revoke-encryption-group

This command revokes and destroys an encryption group's encryption key. It is irreversible. Data encrypted by the encryption group can no longer be accessed after this command is executed.

### Usage

```
encryptiongroup revoke-encryption-group --id ID
```

### Required Parameters

<code>--id ID</code>	Specifies which encryption group to revoke.
----------------------	---

### Example

```
vccli: admin> encryptiongroup revoke-encryption-group --id 4
```

## encryptiongroup rotate-encryption-group-key

This command rotates an encryption group key.

### Usage

```
encryptiongroup rotate-encryption-group-key --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which encryption group for which to rotate the key.
----------------------	---

## Example

```
vcli: admin> encryptiongroup rotate-encryption-group-key --id 3
```



# encryptedpath commands

## encryptedpath create

This command creates a new path that is encrypted with a dedicated encryption key. See [Encryption of Data at Rest](#) for more details.

To make the encrypted path accessible to clients, create a view on the path after the encrypted path is created.

## Usage

```
encryptedpath create --name NAME
                    --path PATH
                    [--tenant-id TENANT_ID]
```

## Required Parameters

<code>--name NAME</code>	Sets the name of the encrypted path.
<code>--path PATH</code>	Specifies the path to encrypt. The specified path must not be a pre-existing path.

## Options

<code>--tenant-id TENANT_ID</code>	<p>Specifies the tenant on which the path resides. In case not specified, the default tenant is used.</p> <p>Provide <code>TENANT_ID</code> as the integer ID value of the tenant.</p>
------------------------------------	--

## Example

```
vccli: admin> encryptedpath create --name epath1 --path /epath1 --tenant-id 2
```

## encryptedpath delete

This command deletes an encrypted path. Deleting an encrypted path deletes the directory and the encryption group associated with the encrypted path.

## Usage

```
encryptedpath delete --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which encrypted path to delete.
----------------------	---

## Example

```
vccli: admin> encryptedpath delete --id 5
```

### encryptedpath list

This command displays all encrypted paths and their details.

## Usage

```
encryptedpath list
```

## Example

```
vccli: admin> encryptedpath list
```

ID	Name	Path	Tenant-id	Tenant-name	Encryption-group
1	epath1	/epath1	1	default	4
2	epath2	/epath2	3	tenant1	5

### encryptedpath modify

This command changes the name of an encrypted path.

## Usage

```
encryptedpath modify --id ID
                    --name NAME
```

## Required Parameters

<code>--id ID</code>	Specifies which encrypted path to modify.  Provide <code>ID</code> as the integer ID value of the encrypted path.
<code>--name NAME</code>	Sets the name of the encrypted path.

## Example

```
vccli: admin> encryptedpath modify --id 3 --name epath3
```

### **encryptedpath reinstate-encryption-group**

This command reinstates a revoked encryption group associated with an encrypted path.

## Usage

```
encryptedpath reinstate-encryption-group --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies the encrypted path by its ID.
----------------------	---

## Example

```
vccli: admin> encryptedpath reinstate-encryption-group --id 3
```

### **encryptedpath revoke-encryption-group**

This command revokes the encryption group associated with an encrypted path.

It takes some time for a key to be revoked. Once the key is revoked, the path is no longer accessible to clients and remains inaccessible until the key is reinstated.

## Usage

```
encryptedpath revoke-encryption-group --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies the encrypted path by its ID.
----------------------	---

## Example

```
vccli: admin> encryptedpath revoke-encryption-group --id 3
```

### **encryptedpath rotate-encryption-group-key**

This command rotates an encryption group key associated with an encrypted path.

# Usage

```
encryptedpath rotate-encryption-group-key --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies the encrypted path by its ID.
----------------------	---

## Example

```
vcli: admin> encryptedpath rotate-encryption-group-key --id 3
```

### encryptedpath show

This command displays details of a specific encrypted path.

## Usage

```
encryptedpath show --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which encrypted path to display.
----------------------	--

## Example

```
vcli: admin> encryptedpath show --id 2
```

```
+-----+-----+
| ID      | 2      |
| Name    | EPath  |
| Path    | /epath |
| Tenant-id | 1      |
| Tenant-name | default |
| Encryption-group | 4      |
+-----+-----+
```

# event commands

## event list

This command lists all events on the VAST Cluster.

## Usage

```
event list [--start-time START-TIME]
           [--end-time END-TIME]
           [--object-type TYPE]
           [--object-id OBJECT_ID]
           [--message TEXT]
           [--event-type AUDIT|ERROR|GENERAL|OBJECT_CREATED|DELETED|OBJECT_MODIFIED|THRESHOLD]
           [--severity CRITICAL|MAJOR|MINOR|INFO]
           [--event-origin CLUSTER|MANAGEMENT|SECURITY|USER]
           [--page PAGE_NUMBER]
           [--page-size NUMBER_ON_PAGE]
```

## Options

<code>--start-time START-TIME</code>	<p>Starts listing from a specified event time.</p> <p>Specify START-TIME in the format <b>YYYY-MM-DD HH:MM:SS</b>. For example: 2017-10-19 10:31:47</p>
<code>--end-time END-TIME</code>	<p>Ends listing by a specified event time.</p> <p>Specify END-TIME in the format <b>YYYY-MM-DD HH:MM:SS</b>. For example: 2017-10-19 10:31:47</p>
<code>--object-type TYPE</code>	<p>Filters the list by object type.</p> <p>For example: <code>--object-type Cluster</code></p> <p>Valid types:</p> <p>Vms   Cluster   BMC   CNode   DNode   ReplicationTarget   ReplicationStream   SSD   NVRAM   NIC   Carrier   Qu</p>

	ota  Fan PSU DBox CBox Switch Port Ldap License NIS  Task Host SupportBundle ActiveDirectory
--object-id OBJECT_ID	Filters the list by object ID.  For example: --object-id 23
--message TEXT	Filters the list by event message text. Specify any text to search for as TEXT. The search is case sensitive.  For example: --message DEGRADED
--event-type AUDIT ERROR GENERAL OBJECT_CREATED DELETED OBJECT_MODIFIED THRESHOLD	
--severity CRITICAL MAJOR MINOR INFO	Filters the list by severity.
--event-origin CLUSTER MANAGEMENT SECURITY USER	
--page PAGE_NUMBER	Displays a specified page if --page-size is set.  Defaults to the first page.
--page-size NUMBER_ON_PAGE	Sets the maximum number of alarms to display on a page.

## Example

```
vcli: admin> event list
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+
| ID   | Timestamp           | Object-type | Object-id | Cluster | Event-message | Eve
nt-type   | Event-origin | Severity | Event-message |
|
```

```

+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+
| 154 | 2020-10-21 10:35:27 | Vms          | 1          | cluster1 | AUDIT          | USER
| INFO      | Manager: admin, modify eventdefinitionconfig
|
| 152 | 2020-10-21 10:10:43 | CNode          | 1          | cluster1 | OBJECT_MODIFIED | CLUSTER
| INFO      | CNode cnode-1 (10.0.1.23) [centos-7.7-test-new-vm-clean-v1] state changed from A
CTIVATING to ACTIVE |
| 151 | 2020-10-21 10:10:33 | CNode          | 1          | cluster1 | OBJECT_MODIFIED | CLUSTER
| INFO      | CNode cnode-1 (10.0.1.23) [centos-7.7-test-new-vm-clean-v1] state changed from F
AILED to ACTIVATING |
| 150 | 2020-10-21 10:10:18 | CNode          | 1          | cluster1 | OBJECT_MODIFIED | CLUSTER
| CRITICAL  | CNode cnode-1 (10.0.1.23) [centos-7.7-test-new-vm-clean-v1] state changed from A
CTIVE to FAILED |
| 149 | 2020-10-21 09:53:38 | Vms          | 1          | cluster1 | AUDIT          | USER
| INFO      | Manager: admin, modify eventdefinitionconfig
|
| 148 | 2020-10-21 09:30:48 | Vms          | 1          | cluster1 | AUDIT          | USER
| INFO      | Manager: admin, modify eventdefinitionconfig
|
| 147 | 2020-10-21 09:30:40 | Vms          | 1          | cluster1 | ERROR          | USER
| INFO      | Bad Request (400)
|
| 146 | 2020-10-21 09:30:40 | Vms          | 1          | cluster1 | AUDIT          | USER
| INFO      | Manager: admin, modify eventdefinitionconfig
|
| 145 | 2020-10-21 09:30:35 | Vms          | 1          | cluster1 | AUDIT          | USER
| INFO      | Manager: admin, modify eventdefinitionconfig
|
| 144 | 2020-10-21 08:54:05 | Carrier       | 23         | cluster1 | OBJECT_MODIFIED | CLUSTER
| INFO      | Carrier dbx-6390c3-FRONT-4-SSD state changed from UNKNOWN to ACTIVE
|
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+

```

## event show

This command displays details of a specific event.

## Usage

```
event show --id ID
```

## Options

--id ID	Specifies which event to display. Required if there is more than one event.
---------	---

## Example

This example...

```
vccli: admin> event show --id 152
```

```
+-----+
+-----+
+
| ID          | 152
|
| Timestamp   | 2020-10-21 10:10:43
|
| Object-type | CNode
|
| Object-id   | 1
|
| Cluster     | cluster1
|
| Event-type  | OBJECT_MODIFIED
|
| Event-origin | CLUSTER
|
| Severity    | INFO
|
| Event-message | CNode cnode-1 (10.0.1.23) [centos-7.7-test-new-vm-clean-v1] state changed f
rom ACTIVATING to ACTIVE |
+-----+
+-----+
+
```





```

d}%
ne      | None      | None      | None      | None      | MAJOR      | None      | No
| None      | None      | None      | None      | False      |      | ['ge', 95]
| 10 | Cluster      | THRESHOLD      | Cluster {obj} metadata in use reached {threshold}%
d}%
ne      | None      | None      | None      | None      | False      |      | ['ge', 96]
| None      | None      | None      | None      | False      | N/A      | True      |
| 11 | Cluster      | THRESHOLD      | Cluster {obj} reached maximum snapshots capacity of {threshold}
ne      | None      | None      | None      | None      | False      | N/A      | True      |
| None      | None      | None      | None      | False      | N/A      | True      |
| 14 | Cluster      | OBJECT_MODIFIED | Cluster {obj} {property} changed from {old_value} to {new_value}
ne      | None      | None      | None      | None      | CRITICAL | None      | No
| ['DONE']      | None      | None      | None      | False      | N/A      | False      |
| 15 | Cluster      | OBJECT_MODIFIED | Cluster {obj} {property} changed from {old_value} to {new_value}
ne      | None      | None      | None      | None      | CRITICAL | None      | No
| None      | None      | None      | None      | False      |      | ['FAILED', 'DEGRADED']
| ['HEALTHY']      | None      | None      | None      | False      | N/A      | True      |
| 16 | Cluster      | OBJECT_MODIFIED | Cluster {obj} {property} changed from {old_value} to {new_value}
ne      | None      | None      | None      | None      | CRITICAL | None      | No
| None      | None      | None      | None      | False      |      | ['FAILED', 'DEGRADED', 'REBUILD', 'REBALANCE']
| ['HEALTHY']      | None      | None      | None      | False      | N/A      | True      |
| 17 | Cluster      | OBJECT_MODIFIED | Cluster {obj} {property} changed from {old_value} to {new_value}
ne      | None      | None      | None      | None      | CRITICAL | None      | No
| None      | None      | None      | None      | False      |      | ['FAILED', 'DEGRADED']
| ['HEALTHY']      | None      | None      | None      | False      | N/A      | True      |
| 18 | Cluster      | OBJECT_MODIFIED | Cluster {obj} {property} changed from {old_value} to {new_value}
ne      | None      | None      | None      | None      | None      | None      | No
| None      | None      | None      | None      | False      | N/A      | True      |
| 19 | Cluster      | OBJECT_MODIFIED | Cluster {obj} {property} changed from {old_value} to {new_value}
ne      | None      | None      | None      | None      | CRITICAL | None      | No
| None      | None      | None      | None      | False      |      | ['GEN_FAILURE', 'DNODE_INIT_FAILURE', 'DNODE_ACTIVATION_FAILURE', 'NVRAM_DISCOVERY_FAILURE', 'NVRAMS_ACTIVATION_FAILURE', 'ACTIVATE_MEM_REGIONS_FAILURE'] | ['SUCCESS', 'NONE']
| False      | N/A      | True      |
| 20 | Cluster      | OBJECT_MODIFIED | Cluster {obj} {property} changed from {old_value} to {new_value}
ne      | None      | None      | None      | None      | None      | None      | No
| None      | None      | None      | None      | False      | N/A      | True      |
| 21 | Cluster      | OBJECT_MODIFIED | Cluster {obj} {property} changed from {old_value} to {new_value}
ne      | None      | None      | None      | None      | None      | None      | No
| None      | None      | None      | None      | False      | N/A      | True      |
| 44 | BMC      | OBJECT_MODIFIED | {obj} {property} changed from {old_value} to {new_value}. Reason: {obj.state_reason}
ne      | None      | None      | None      | None      | CRITICAL | None      | No
| ['UNKNOWN', 'PASSED']      | None      | None      | None      | False      | N/A      | True      |
| 45 | CNode      | OBJECT_MODIFIED | CNode {obj} {property} changed from {old_value} to {new_value}
ne      | None      | None      | None      | None      | CRITICAL | None      | Non
| None      | None      | None      | None      | False      |      | ['FAILED', 'FAILING']
| ['ACTIVE']      | None      | None      | None      | False      | N/A      | True      |
| 48 | CNode      | OBJECT_MODIFIED | CNode {obj} {property}: {new_value}
| None      | None      | None      | None      | None      | None      | None
| False      | None
| None      | None      | None      | None      | False      | N/A      | True      |
| 49 | CNode      | THRESHOLD      | CNode {obj} temperature {threshold} exceeded threshold 70
ne      | None      | None      | None      | None      | CRITICAL | None      | No
| None      | None      | None      | None      | False      |      | ['gt', 70]
| None      | None      | None      | None      | False      | N/A      | True      |
| 50 | CNode      | RATE      | CNode {obj} pci errors rate exceeded 50 in the past {time_frame}
ne      | None      | None      | None      | None      | CRITICAL | None      | No

```

ne	None	None	None	False	['gt', 100]
None	None	None	None	False	N/A
51   CNode	RATE	CNode {obj}	correctable memory errors exceeded	CRITICAL	None
threshold 100 in the past 24h	None	None	None	False	['gt', 100]
ne	None	None	None	False	N/A
None	None	None	None	False	N/A
53   CNode	THRESHOLD	CNode {obj}	memory usage reached to {threshold}%.	MAJOR	None
None	None	None	None	False	['ge', 97.5]
None	None	None	None	False	N/A
54   CNode	THRESHOLD	CNode {obj}	/ partition used space {threshold}% exceeded threshold of 95%	MAJOR	None
e	None	None	None	False	['gt', 95]
None	None	None	None	False	N/A
55   CNode	THRESHOLD	CNode {obj}	/vast partition used space {threshold}% exceeded threshold of 95%	MAJOR	None
ne	None	None	None	False	['gt', 95]
None	None	None	None	False	N/A
56   CNode	THRESHOLD	CNode {obj}	/userdata partition used space {threshold}% exceeded threshold of 95%	MAJOR	None
ne	None	None	None	False	['gt', 95]
None	None	None	None	False	N/A
57   CNode	RATE	CNode {obj}	memory usage rose by {rate}% within {time_frame}.	CRITICAL	None
e	None	None	None	False	['gt', 15]
None	None	None	None	False	N/A
58   CNode	OBJECT_MODIFIED	CNode {obj}	detected slow CPU speed	None	None
MAJOR	None	None	None	None	None
False	[True]	None	None	None	None
[False]	None	None	None	False	N/A
59   CNode	OBJECT_MODIFIED	CNode {obj}	file server access changed from {old_value} to {new_value}	CRITICAL	None
ne	None	None	None	False	[False]
[True]	None	None	None	False	N/A
60   DNode	OBJECT_MODIFIED	DNode {obj}	{property} changed from {old_value} to {new_value}	CRITICAL	None
e	None	None	None	False	['FAILED', 'FAILING']
['ACTIVE']	None	None	None	False	N/A
63   DNode	OBJECT_MODIFIED	DNode {obj}	{property}: {new_value}	None	None
None	None	None	None	None	None
False	None	None	None	None	None
None	None	None	None	False	N/A
64   DNode	THRESHOLD	DNode {obj}	temperature {threshold} exceeded threshold 70	CRITICAL	None
ne	None	None	None	False	['gt', 70]
None	None	None	None	False	N/A
65   DNode	RATE	DNode {obj}	pci errors rate exceeded 50 in the past {time_frame}	CRITICAL	None
ne	None	None	None	False	['gt', 100]
None	None	None	None	False	N/A
66   DNode	RATE	DNode {obj}	correctable memory errors exceeded threshold 100 in the past 24h	CRITICAL	None
ne	None	None	None	False	['gt', 100]
None	None	None	None	False	N/A
68   DNode	THRESHOLD	DNode {obj}	memory usage reached to {threshold}%.	MAJOR	None
None	None	None	None	False	['ge', 97.5]
None	None	None	None	False	N/A
69   DNode	THRESHOLD	DNode {obj}	/ partition used space {threshold}% exceeded threshold of 95%	MAJOR	None
e	None	None	None	False	['gt', 95]
None	None	None	None	False	N/A
70   DNode	THRESHOLD	DNode {obj}	/vast partition used space {threshold}% exceeded threshold of 95%	MAJOR	None
ne	None	None	None	False	['gt', 95]
None	None	None	None	False	N/A

```

| 71 | DNode | THRESHOLD | DNode {obj} /userdata partition used space {thr
eshold}% exceeded threshold of 95% | MAJOR | None | No
ne | None | None | None | False | ['gt', 95]
| None | False | N/A | True |
| 72 | DNode | RATE | DNode {obj} memory usage rose by {rate}% within
{time_frame}. | CRITICAL | None | Non
e | None | None | None | False | False | ['gt', 10]
| None | False | N/A | True |
| 73 | DNode | OBJECT_MODIFIED | DNode {obj} slow CPU detected
| None | None | None | None | None | None | None
| False | [True]
| [False] | False | N/A | True |
| 74 | ReplicationTarget | OBJECT_MODIFIED | ReplicationTarget {obj} {property} changed from
{old_value} to {new_value}. {obj.state_description} | CRITICAL | None | Non
e | None | None | None | False | False | ['ERROR']
| ['ACTIVE', 'INIT'] | False | N/A | True |
| 75 | ReplicationStream | OBJECT_MODIFIED | ReplicationStream {obj} {property} changed from
{old_value} to {new_value}. {obj.state_description} | CRITICAL | None | Non
e | None | None | None | False | False | ['ERROR']
| ['INIT', 'INITIAL_SYNC', 'INCREMENTAL_SYNC'] | False | N/A | True |
| 76 | ReplicationStream | THRESHOLD | ReplicationStream {obj} missed it's RPO target
by {threshold} seconds | MAJOR | None | No
ne | None | None | None | False | False | ['gt', 120]
| None | False | N/A | True |
| 77 | ReplicationStream | THRESHOLD | ReplicationStream {obj} missed it's RPO target
by {threshold} seconds | CRITICAL | None | No
ne | None | None | None | False | False | ['gt', 300]
| None | False | N/A | True |
| 78 | SSD | OBJECT_MODIFIED | SSD {obj} serial: {obj.sn} {property} changed f
rom {old_value} to {new_value} | CRITICAL | None | No
ne | None | None | None | False | False | ['FAILED', 'FA
ILING', 'INACTIVE']
| ['ACTIVE'] | False | N/A | True |
| 79 | SSD | OBJECT_MODIFIED | SSD {obj} serial: {obj.sn} {property} changed f
rom {old_value} to {new_value} | MAJOR | None | No
ne | None | None | None | False | False | [False]
| [True] | False | N/A | True |
| 80 | SSD | OBJECT_MODIFIED | SSD {obj} serial: {obj.sn} {property} changed f
rom {old_value} to {new_value} | MAJOR | None | No
ne | None | None | None | False | False | [False]
| [None, True] | False | N/A | True |
| 81 | SSD | OBJECT_MODIFIED | SSD {obj} serial: {obj.sn} {property} changed f
rom {old_value} to {new_value} | MAJOR | None | No
ne | None | None | None | False | False | [False]
| [None, True] | False | N/A | True |
| 82 | SSD | THRESHOLD | SSD {obj} serial: {obj.sn} temperature {thresho
ld} exceeded threshold 70 | CRITICAL | None | No
ne | None | None | None | False | False | ['gt', 70]
| None | False | N/A | True |
| 83 | SSD | THRESHOLD | SSD {obj} serial: {obj.sn} have {threshold} med
ia errors | CRITICAL | None | No
ne | None | None | None | False | False | ['ge', 100]
| None | False | N/A | True |
| 91 | NVRAM | OBJECT_MODIFIED | NVRAM {obj} serial: {obj.sn} {property} changed
from {old_value} to {new_value} | MAJOR | None | Non
e | None | None | None | False | False | ['FAILED', 'FAI
LING', 'INACTIVE']
| ['ACTIVE'] | False | N/A | True |
| 92 | NVRAM | OBJECT_MODIFIED | NVRAM {obj} serial: {obj.sn} {property} changed
from {old_value} to {new_value} | MAJOR | None | Non
e | None | None | None | False | False | [False]
| [True] | False | N/A | True |
| 93 | NVRAM | THRESHOLD | NVRAM {obj} serial: {obj.sn} have {threshold} m
edia errors | CRITICAL | None | No
ne | None | None | None | False | False | ['ge', 100]
| None | False | N/A | True |
| 101 | NIC | OBJECT_MODIFIED | NIC {obj} {property} changed from {old_value} t

```

```

o {new_value}
ne | None | None | None | None | MAJOR | None | No
| [False] | None | None | False | [True]
| 102 | NIC | OBJECT_MODIFIED | NIC {obj} flow is balanced: {new_value}
| CRITICAL | None | None | None | None | None
| False | [False]
| [True] | None | False | N/A | True |
| 103 | NIC | OBJECT_MODIFIED | NIC {obj} {property} changed from {old_value} t
o {new_value} | CRITICAL | None | No
ne | None | None | None | False | ['down']
| ['up'] | None | False | N/A | True |
| 104 | NIC | OBJECT_MODIFIED | NIC {obj} {property} changed from {old_value} t
o {new_value} | CRITICAL | None | No
ne | None | None | None | False | ['down']
| ['up'] | None | False | N/A | True |
| 105 | NIC | THRESHOLD | NIC {obj} rx_wqe_err error
| MAJOR | None | None | None | None | None
| False | ['gt', 0]
| None | False | N/A | True |
| 106 | NIC | THRESHOLD | NIC {obj} rx_buff_alloc_err error
| MAJOR | None | None | None | None | None
| False | ['gt', 0]
| None | False | N/A | True |
| 107 | NIC | RATE | NIC {obj} rx_crc_errors_phy rose by {rate} over
{time_frame} | MAJOR | None | Non
e | None | None | None | False | ['ge', 10]
| None | False | N/A | True |
| 108 | NIC | THRESHOLD | NIC {obj} rx_in_range_len_errors_phy error
| MAJOR | None | None | None | None | None
| False | ['gt', 0]
| None | False | N/A | True |
| 109 | NIC | RATE | NIC {obj} rx_symbol_err_phy rose by {rate} over
{time_frame} | MAJOR | None | Non
e | None | None | None | False | ['ge', 10]
| None | False | N/A | True |
| 110 | NIC | THRESHOLD | NIC {obj} tx_errors_phy error
| MAJOR | None | None | None | None | None
| False | ['gt', 0]
| None | False | N/A | True |
| 113 | Carrier | OBJECT_MODIFIED | Carrier {obj} {property} changed from {old_valu
e} to {new_value} | MAJOR | None | No
ne | None | None | None | False | ['FAILED', 'FA
ILING', 'INACTIVE']
| ['ACTIVE'] | None | False | N/A | True |
| 114 | Carrier | OBJECT_MODIFIED | Carrier {obj} {property} changed from {old_valu
e} to {new_value} | None | None | No
ne | None | None | None | False | None
| None | False | N/A | True |
| 115 | Carrier | OBJECT_MODIFIED | {obj} {property} changed from {old_value} to {n
ew_value} | None | None | No
ne | None | None | None | False | None
| None | False | N/A | True |
| 116 | Quota | OBJECT_MODIFIED | Quota {obj} {property} changed from {old_value}
to {new_value} | MAJOR | None | Non
e | None | None | None | False | ['SOFT_EXCEEDE
D', 'HARD_EXCEEDED', 'GRACE_EXPIRED', 'INODE_SOFT_EXCEEDED', 'INODE_HARD_EXCEEDED', 'SOFT_BOT
H_EXCEEDED', 'HARD_BOTH_EXCEEDED'] | ['OK']
| False | N/A | True |
| 117 | Quota | OBJECT_MODIFIED | Quota {obj} soft limit changed from {old_value}
to {new_value} | MAJOR | None | Non
e | None | None | None | False | [True]
| [False] | None | False | N/A | True |
| 118 | Quota | OBJECT_MODIFIED | Quota {obj} hard limit changed from {old_value}
to {new_value} | MAJOR | None | Non
e | None | None | None | False | [True]
| [False] | None | False | N/A | True |
| 119 | Quota | OBJECT_MODIFIED | Quota {obj} state changed from {old_value} to

```

```

{new_value}. {obj.failure_reason}
one | None | None | None | None | False | None | None | None | N/A | True | ['FAILED']
| ['SYNCHRONIZED'] | False | N/A | True |
| 120 | Fan | OBJECT_MODIFIED | FAN {obj.name} in {obj.location} state changed
from {old_value} to {new_value} | MAJOR | None | No
ne | None | None | None | False | ['LOWER_NON_RE
COVERABLE', 'LOWER_CRITICAL', 'LOWER_NON_CRITICAL']
| ['OK'] | False | N/A | True |
| 121 | PSU | OBJECT_MODIFIED | PSU {obj} in {obj.box} {property} changed from
{old_value} to {new_value} | CRITICAL | None | No
ne | None | None | None | False | ['down', 'disc
onnected_cable', 'psu_out']
| ['up'] | False | N/A | True |
| 122 | PSU | THRESHOLD | PSU {obj} in {obj.box} lost AC power (voltage
{threshold} is less than 80 Volts) | CRITICAL | None | No
one | None | None | None | False | ['lt', 80]
| None | False | N/A | True |
| 123 | PSU | THRESHOLD | PSU {obj} in {obj.box} lost AC power (power inp
ut is 0 Watts) | CRITICAL | None | No
ne | None | None | None | False | ['eq', 0]
| None | False | N/A | True |
| 124 | DBox | OBJECT_MODIFIED | {obj} voltage sensor state changed from {old_va
lue} to {new_value}. {obj.voltage_sensor_err_info} | MAJOR | None | No
ne | None | None | None | False | [True]
| [False] | False | N/A | True |
| 125 | DBox | OBJECT_MODIFIED | {obj} temperature sensor state changed from {ol
d_value} to {new_value}. {obj.temperature_sensor_err_info} | MAJOR | None | No
ne | None | None | None | False | [True]
| [False] | False | N/A | True |
| 126 | DBox | OBJECT_MODIFIED | {obj} {property} changed from {old_value} to {n
ew_value} | CRITICAL | None | No
ne | None | None | None | False | ['FAILED']
| ['ACTIVE'] | False | N/A | True |
| 127 | DBox | THRESHOLD | {obj} ambient temperature is {threshold}
| MAJOR | None | None | None | None | None
| False | ['gt', 50]
| None | False | N/A | True |
| 128 | DBox | THRESHOLD | {obj} ambient temperature is {threshold}
| CRITICAL | None | None | None | None | None
| False | ['gt', 55]
| None | False | N/A | True |
| 129 | CBox | OBJECT_MODIFIED | {obj} voltage sensor state changed from {old_va
lue} to {new_value}. {obj.voltage_sensor_err_info} | MAJOR | None | No
ne | None | None | None | False | [True]
| [False] | False | N/A | True |
| 130 | CBox | OBJECT_MODIFIED | {obj} temperature sensor state changed from {ol
d_value} to {new_value}. {obj.temperature_sensor_err_info} | MAJOR | None | No
ne | None | None | None | False | [True]
| [False] | False | N/A | True |
| 131 | CBox | THRESHOLD | {obj} ambient temperature is {threshold}
| MAJOR | None | None | None | None | None
| False | ['gt', 50]
| None | False | N/A | True |
| 132 | CBox | THRESHOLD | {obj} ambient temperature is {threshold}
| CRITICAL | None | None | None | None | None
| False | ['gt', 55]
| None | False | N/A | True |
| 133 | Switch | OBJECT_MODIFIED | {obj} {property} changed from {old_value} to {n
ew_value} | MAJOR | None | No
ne | None | None | None | False | ['FAILED', 'ER
ROR']
| ['OK'] | False | N/A | True |
| 134 | Port | OBJECT_MODIFIED | {obj} {property} changed from {old_value} to {n
ew_value} | None | None | No
ne | None | None | None | False | None
| None | False | N/A | True |
| 135 | Port | OBJECT_MODIFIED | {obj} {property} changed from {old_value} to {n

```

```

ew_value}
ne | None | None | None | None | False | None | No
| None | None | None | None | False | N/A | True |
| 136 | Ldap | OBJECT_MODIFIED | {obj} {property} changed from {old_value} to {n
ew_value}. {obj.error_string} | None | None | No
ne | None | None | None | None | False | None
| None | None | None | None | False | N/A | True |
| 137 | Ldap | OBJECT_MODIFIED | {obj} disconnected: {new_value}. {obj.error_str
ing} | CRITICAL | None | No
ne | None | None | None | None | False | [True]
| None | None | None | None | False | N/A | True |
| 138 | Ldap | OBJECT_MODIFIED | {obj} degraded: {new_value}. {obj.error_string}
| MINOR | None | None | None | None | None | None
| False | [True]
| None | None | None | None | False | N/A | True |
| 139 | Ldap | OBJECT_CREATED | LDAP configuration created
| None | None | None | None | None | None | None
| False | None
| None | None | None | None | False | N/A | True |
| 140 | Ldap | OBJECT_DELETED | LDAP configuration deleted
| None | None | None | None | None | None | None
| False | None
| None | None | None | None | False | N/A | True |
| 141 | NIS | OBJECT_MODIFIED | {obj} {property} changed from {old_value} to {n
ew_value}. {obj.error_string} | CRITICAL | None | No
ne | None | None | None | None | False | ['FAILED']
| ['CONNECTED']
| None | None | None | None | False | N/A | True |
| 142 | NIS | OBJECT_CREATED | NIS configuration created
| None | None | None | None | None | None | None
| False | None
| None | None | None | None | False | N/A | True |
| 143 | NIS | OBJECT_DELETED | NIS configuration deleted
| None | None | None | None | None | None | None
| False | None
| None | None | None | None | False | N/A | True |
| 144 | Task | OBJECT_MODIFIED | {obj} activity {property} changed from {old_val
ue} to {new_value} | MAJOR | None | No
ne | None | None | None | None | False | ['FAILED', 'TI
MEOUT']
| None | None | None | None | False | N/A | True |
| 145 | Host | OBJECT_MODIFIED | {obj} {property} changed from {old_value} to {n
ew_value} | None | None | No
ne | None | None | None | None | False | None
| None | None | None | None | False | N/A | True |
| 146 | SupportBundle | OBJECT_MODIFIED | SupportBundle {obj} {property} changed from {ol
d_value} to {new_value} | None | None | No
ne | None | None | None | None | False | None
| None | None | None | None | False | N/A | True |
| 147 | ActiveDirectory | OBJECT_MODIFIED | {obj} {property} changed from {old_value} to {n
ew_value}. {obj.error_string} | CRITICAL | None | No
ne | None | None | None | None | False | ['JOINED_FAILE
D', 'LEAVE_FAILED']
| ['NOT_A_MEMBER', 'JOINED'] | False | N/A | True |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
+-----+-----+-----+-----+
+-----+-----+-----+-----+
+-----+-----+-----+-----+
+-----+-----+-----+-----+

```

## eventdefinition modify

This command modifies an event definition. The event definition includes actions that can be triggered when an event occurs that matches the definition. These actions override the global actions that you can define for all events using

# Usage

```
eventdefinition modify --id ID
                        [--email-recipients RECIPIENTS]
                        [--webhook-url URL]
                        [--webhook-method POST|GET|DELETE|PUT|PATCH]
                        [--webhook-data PAYLOAD]
                        [--webhook-params key1=value1,key2=value2,...]
                        [--cooldown SECONDS]
                        [--raise-at-count COUNT]
                        [--severity CRITICAL|MAJOR|MINOR|INFO]
                        [--trigger-on TRIGGER_ON]
                        [--trigger-off TRIGGER_OFF]
                        [--time-frame TIMEFRAME]
                        [--disable-actions]
                        [--enable-actions]
                        [--disable]
                        [--enable]
                        [--disable-alarm-only]
                        [--enable-alarm-only]
```

# Required Parameters

<code>--id ID</code>	Specifies the event definition to modify.
----------------------	---

# Options

<code>--email-recipients</code> <code>RECIPIENTS</code>	<p>Configures email recipients to be notified on events and/or alarms of this definition.</p> <p>Specify RECIPIENTS as a comma separated list of email addresses (no spaces).</p> <p>Example: <code>--email-recipients storage_admin@company.com,bsmith@company.com,abrown@company.com</code></p>
<code>--webhook-url URL</code>	<p>Include this option to configure a webhook to be triggered by events of this specific type. A webhook contacts an external application and invokes an HTTP method in the external application. This feature requires the external application to support webhooks.</p> <p>This option specifies the webhook URL of the external application that you want to trigger. Obtain the webhook URL from the external application.</p> <p>You may want to append custom parameters to the URL. To specify the custom parameters, use also <code>--webhook-params</code>.</p> <p>See also <code>--webhook-method</code>.</p>



<pre>--webhook-method POST   GET   PUT   PATCH   DELETE</pre>	<p>Include this option if you are configuring a webhook for the event definition. See <code>--webhook-url</code>.</p> <p>This option specifies which HTTP method to invoke when the webhook is triggered. If the method sends a payload, use <code>--webhook-data</code> to specify the payload.</p>
<pre>--webhook-data PAYLOAD</pre>	<p>Include this option to specify a payload to send if you are configuring a webhook for the event definition. Relevant depending on the webhook method. See first <code>--webhook-url</code> and <code>--webhook-method</code>.</p> <p>Specify the <code>PAYLOAD</code> in JSON format encapsulated with ". Use the data structure supported by the external application. You can include the event message in a text string by specifying the <code>\$event</code> variable.</p> <p>For example: <code>--webhook-data '"text": "\$event"'</code></p>
<pre>--webhook-params PARAMS</pre>	<p>Specifies custom parameters to append to the webhook URL if configured. See <code>--webhook-url</code>.</p> <p>Specify <code>PARAMS</code> as a comma separated set of key value pairs in the format <i>key=value</i>.</p> <p>For example: <code>myparam1=x,myparam2=y</code></p>
<pre>--cooldown SECONDS</pre>	<p>Sets a minimum number of seconds to wait between two consecutive events.</p>
<pre>--raise-at-count COUNT</pre>	<p>Sets the number of event occurrences after which the alarm is raised.</p>
<pre>--severity CRITICAL   MAJOR   MINOR   INFO</pre>	<p>Changes the severity of events with this definition.</p>
<pre>--trigger-on TRIGGER_ON</pre>	<p>Sets the value at which an alarm is triggered on.</p> <p>Relevant to the following event types: <i>OBJECT_MODIFIED</i> , <i>THRESHOLD</i> , <i>RATE</i>.</p> <p>For <i>OBJECT_MODIFIED</i> type events, specify one or more valid values for the property in the definition of the event. Separate the values with a comma.</p> <p>For example: <code>--trigger-on FAILED, TIMEOUT</code></p> <p>For <i>THRESHOLD</i> and <i>RATE</i> type events, specify an operator and a numeric value in the format: '<i>&lt;operator&gt;</i>', <i>&lt;value&gt;</i></p> <p><i>&lt;operator&gt;</i> can be:</p> <ul style="list-style-type: none"> <li>• <i>gt</i>. Greater than</li> <li>• <i>ge</i>. Greater than or equal to</li> </ul>

	<ul style="list-style-type: none"> <li>lt. Lower than</li> <li>eq. Equal to</li> </ul> <p>&lt;value&gt; is the numeric value.</p> <p>For example: <code>--trigger-on 'gt', 50</code></p>
<code>--trigger-off TRIGGER_OFF</code>	<p>Sets the value at which an alarm is triggered off.</p> <p>Relevant to the following event types: <i>OBJECT_MODIFIED</i> and <i>THRESHOLD</i>.</p> <p>Input format as for <code>--trigger-on</code>.</p>
<code>--time-frame TIMEFRAME</code>	<p>Sets the time frame for a <i>RATE</i> type event, in which an alarm is triggered if a property exceeds a threshold value within the configured time frame.</p> <p>For example: <code>--time-frame 12h</code></p>
<code>--disable-actions</code>	Disables any configured email recipients and webhook for the event definition.
<code>--enable-actions</code>	Reenables email recipients and webhook for the event definition, if disabled.
<code>--disable</code>	Disables the event definition, which stops events of the given definition being logged as events, or triggering call home, alarms or actions such as email, webhook or syslogs.
<code>--enable</code>	Re-enables a disabled event definition. See <code>--disable</code> .
<code>--disable-alarm-only</code>	If specified, email recipients and webhooks (if configured) are initiated by all events of this definition and not only by alarms. For example, if the object type is <i>CNode</i> , and the Property is <i>state</i> , then if <code>--disable-alarm-only</code> is specified, any change in state of a <i>CNode</i> will initiate the actions you configured for this event.
<code>--enable-alarm-only</code>	If specified, email recipients and webhooks (if configured) are initiated only by alarms and not by any and every event of this definition.

## Example

This example configures a webhook for a specific event definition. The webhook triggers a POST request on an external application, sending the event message in the payload. Since `--disable-alarm-only` is specified, the webhook will be triggered by all events of this definition, rather than only by alarms.

```
vcli: admin> eventdefinition modify --id 117 --disable-alarm-only --webhook-url https://hook
```

```
s.slack.com/services/T1D8BH5KR/B01CGURPR0F/MpoEdsAs9EzXkOsJyLuTidgG --webhook-method POST --webhook-data {"text": "$event"}
```

## eventdefinition show

This command shows a specified event definition.

## Usage

```
eventdefinition show --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies the ID of the event definition that you want to show.
----------------------	---

## Example

```
vccli: admin> eventdefinition show --id 12
```

ID	12
Object-type	Cluster
Event-type	THRESHOLD
Event-message	Cluster {obj} metadata in use reached {threshold}%
Severity	MINOR
Email-recipients	[]
Webhook-url	None
Webhook-data	None
Webhook-method	
Webhook-params	None
Disable-actions	False
Trigger-on	['ge', 94]
Trigger-off	None
User-modified	False
Enabled	N/A
Alarm-only	True

## eventdefinition test

This command sends a test notification for a specific event definition to any configured email recipients, webhook and syslog server.

## Usage

```
eventdefinition test --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which event definition to test.
----------------------	---

## Example

```
vcli: admin> eventdefinition test --id 144
```

## eventdefinitionconfig commands

## eventdefinitionconfig list

This command displays global settings for **default notification actions** that VAST Cluster performs when a defined event occurs on the cluster.

## Usage

```
eventdefinitionconfig list
```

## Example

```
vcli: admin> eventdefinitionconfig list
```

[illegible]

## eventdefinitionconfig modify

This command configures **default and global action settings** for events. To override actions for a specific event definition, use **eventdefinition modify**.

## Usage

```
eventdefinitionconfig modify [--smtp-host SMTP HOST]
```

```

[--smtp-port SMTP_PORT]
[--smtp-user SMTP_USER]
[--smtp-password SMTP_PASSWORD]
[--smtp-enable-tls|--smtp-disable-tls]
[--email-sender SENDER]
[--email-subject SUBJECT]
[--email-recipients RECIPIENTS]
[--webhook-url URL]
[--webhook-data PAYLOAD]
[--webhook-method POST|GET|PUT|PATCH|DELETE]
[--syslog-host SYSLOG_HOST]
[--syslog-port PORT]
[--syslog-protocol udp|tcp]
[--syslog-enable-vms-audit|--syslog-disable-vms-audit]
[--syslog-enable-shell-audit|--syslog-disable-shell-audit]
[--syslog-enable-ipmi-audit|--syslog-disable-ipmi-audit]
[--audit-logs-retention DAYS]
[--disable-actions|--enable-actions]
[--quota-email-suffix SUFFIX]
[--quota-email-provider aggregated|ldap|ad]
[--quota-email-interval INTERVAL]
[--quota-email-hourly-limit LIMIT]

```

## Options

<code>--smtp-host SMTP_HOST</code>	<p>Sets the host name of the SMTP server from which to send alarm notification emails.</p> <p>Example: <code>--smtp-host mail.company.com</code></p>
<code>--smtp-port SMTP_PORT</code>	<p>Sets the port used by the SMTP server to send outgoing emails.</p>
<code>--smtp-user SMTP_USER</code>	<p>Sets a user for SMTP host authentication.</p>
<code>--smtp-password SMTP_PASSWORD</code>	<p>Sets the password for the SMTP user.</p>
<code>--smtp-enable-tls</code>	<p>Enables sending alarm notification emails over a TLS connection.</p>
<code>--smtp-disable-tls</code>	<p>Disables TLS for sending alarm notification emails (default).</p>
<code>--email-subject SUBJECT</code>	<p>Optionally specifies a string that is used globally as the subject for all notification emails.</p> <p>By default, alarm info appears in the subject.</p> <p>Example: <code>--email-subject VAST Alarm</code></p>
<code>--email-sender SENDER</code>	<p>Specifies the sender email that appears in alarm notification emails. It is global for all</p>

	<p>alarm notification emails.</p> <p>Example: <code>--email-sender do_not_reply@company.com</code></p>
<pre>--email-recipients RECIPIENTS</pre>	<p>Sets default email recipients. These recipients receive notifications of all alarms except those triggered by events that have a different list of email recipients specified in the event definition or for which actions are disabled.</p> <p>Specify RECIPIENTS as a comma separated list of email addresses (no spaces).</p> <p>Example: <code>--email-recipients storage_admin@company.com,bsmith@company.com,abrown@company.com</code></p>
<pre>--syslog-host SYSLOG_HOST</pre>	<p>To send alarms to a syslog server, use this option to specify a remote syslog server's IP address.</p> <p>For example: <code>--syslog-host 192.0.2.0</code></p>
<pre>--syslog-port PORT</pre>	<p>Sets the syslog port number. Default: <b>514</b></p>
<pre>--syslog-protocol udp tcp</pre>	<p>If <code>--syslog-host</code> is set, use this option to set which protocol to use to communicate with the syslog server.</p> <p>Default: <i>udp</i>.</p>
<pre>--syslog-enable-vms-audit</pre>	<p>Enables auditing of VMS operations.</p>
<pre>--syslog-disable-vms-audit</pre>	<p>Disables auditing of VMS operations.</p>
<pre>--syslog-enable-shell-audit</pre>	<p>Enables auditing of CNode and DNode shell commands.</p>
<pre>--syslog-disable-shell-audit</pre>	<p>Disables auditing of CNode and DNode shell commands.</p>
<pre>--syslog-enable-ipmi-audit</pre>	<p>Enables auditing of CNode and DNode IPMI commands.</p>
<pre>--syslog-disable-ipmi-</pre>	<p>Disables auditing of CNode and DNode IPMI commands.</p>

audit	
--audit-logs-retention DAYS	Sets the number of days to store audit logs on the syslog server.
--webhook-url URL	<p>Include this option to configure a webhook to be triggered by default by all types of events.</p> <p>A webhook contacts an external application and invokes an HTTP method in the external application. This feature requires the external application to support webhooks.</p> <p>This option specifies the webhook URL of the external application that you want to trigger. Obtain the webhook URL from the external application.</p> <p>See also --webhook-method.</p>
--webhook-method POST   GET   PUT   PATCH   DELETE	<p>Include this option if you are configuring a webhook. See --webhook-url.</p> <p>This option specifies which HTTP method to invoke when the webhook is triggered. If the method sends a payload, use --webhook-data to specify the payload.</p>
--webhook-data PAYLOAD	<p>Include this option to specify a payload to send if you are configuring a webhook. Relevant depending on the webhook method. See first --webhook-url and --webhook-method.</p> <p>Specify the PAYLOAD in JSON format encapsulated with ". Use the data structure supported by the external application. You can include the event message in a text string by specifying the \$event variable.</p> <p>For example: --webhook-data '"text": "\$event"'</p>
--disable-actions	Disables any configured email recipients, webhook and syslog server.
--enable-actions	Enables any configured email recipients, webhook and syslog server (default).
--quota-email-suffix SUFFIX	Specifies a suffix to append to user names to form an email address. This is used as the email recipient address for sending a user an email if they exceed a user quota limit. It is used if an email address is not found for the user on a provider.
--quota-email-provider aggregated   ldap   ad	<p>Specifies the query context to used when querying providers for user email addresses in order to send users notifications of exceeding user quotas.</p> <p>Possible values:</p>



	<ul style="list-style-type: none"> <li>• aggregated. Performs an aggregated query of all providers,</li> <li>• ldap. Queries an LDAP server for user quota notification email addresses.</li> <li>• ad. Queries Active Directory for user quota notification email addresses.</li> </ul>
<pre>--quota-email-interval INTERVAL</pre>	<p>Specifies the minimal interval time between quota notification emails sent to a user.</p> <p>Format: &lt;days&gt; &lt;hours&gt;:&lt;minutes&gt;:&lt;seconds&gt;</p> <p>For example, if you specify <i>1 00:00:00</i>, a user will not receive more than one email each day.</p> <p>Example: <code>--quota-email-interval '1 06:30:00'</code></p>
<pre>--quota-email-hourly- limit LIMIT</pre>	<p>Sets the maximum allowable number of all the quota notification emails sent to all the users, per hour.</p>

## Example

```

vcli: admin> eventdefinitionconfig modify --smtp-host mail.company.com --smtp-port 587 --smtp-user smtp-admin --smtp-password wh2tever --smtp-enable-tls --email-sender do_not_reply@company.com --email-recipients storage_admin@company.com,bsmith@company.com,abrown@company.com --syslog-host 192.0.2.0

```

### eventdefinitionconfig show

This command displays global settings for [default notification actions](#) that VAST Cluster performs when a defined event occurs on the cluster.

## Usage

```
eventdefinitionconfig show
```

## Example

```

vcli: admin> eventdefinitionconfig show
+-----+
+-----+-----+
| Smtphost          | mail.company.com |
+-----+-----+
| Smtpport          | 587              |
+-----+-----+
| Smtputer          | smtp-admin       |
+-----+-----+
| Smtppassword       | *****         |
+-----+-----+
| Smtputse-tls       | True             |
+-----+-----+
| Emailsubject       |                  |
+-----+-----+

```

```

|
| Email-sender                | do_not_reply@company.com
|
| Email-recipients            | ['storage_admin@company.com', 'bsmith@company.com', 'abrown@comp
any.com'] |
| Webhook-url                 |
|
| Webhook-data                 |
|
| Webhook-method              | GET
|
| Syslog-host                 | 192.0.2.0
|
| Syslog-port                 | 514
|
| Syslog-protocol              | tcp
|
| Quota-email-suffix          |
|
| Quota-email-provider         | aggregated
|
| Quota-email-interval         | 1 00:00:00
|
| Quota-email-hourly-limit     | 100
|
| Syslog-vms-audit             | True
|
| Syslog-shell-audit           | True
|
| Syslog-ipmi-audit            | True
|
| Audit-logs-retention         | 10
|
+-----+
+-----+

```

# eventnotification commands

## eventnotification create

This command creates a definition of an event notification to [publish](#) events to an event broker.

## Usage

```
eventnotification create --name NAME
                        --view-id ID
                        --broker-id ID
                        --topic TOPIC
                        --triggers EVENTS
                        [--prefix-filter FILTER_STRING]
                        [--suffix-filter FILTER_STRING]
```

## Required Parameters

<code>--name NAME</code>	A unique name for the new event notification.
<code>--view-id ID</code>	The ID of the view for which event will be published. The view must have S3 protocol enabled and be controlled with <i>S3 Native</i> security flavor.
<code>--broker-id ID</code>	The ID of the event broker to which events will be published. The event broker must be <a href="#">defined</a> on the VAST cluster.
<code>--topic TOPIC</code>	The name of the topic to which to publish events.
<code>--triggers EVENTS</code>	<p>Specify a comma-separated list of events for which you want to send notifications. Valid keywords for <code>EVENTS</code> include:</p> <ul style="list-style-type: none"><li>Object creation events:<ul style="list-style-type: none"><li><code>S3_OBJECT_CREATED_PUT</code> - Creation of an S3 object by a PUT request.</li><li><code>S3_OBJECT_CREATED_POST</code> - Creation of an S3 object by a POST request.</li><li><code>S3_OBJECT_CREATED_COPY</code> - Creation of an S3 object by copying an existing object.</li><li><code>S3_OBJECT_CREATED_COMPLETE_MULTIPART_UPLOAD</code> - Creation of an S3 object as a result of a multi-part upload.</li><li><code>S3_OBJECT_CREATED_ALL</code> - Any S3 object creation.</li></ul></li><li>Object tagging events:</li></ul>

	<ul style="list-style-type: none"> <li>◦ S3_OBJECT_TAGGING_PUT - Adding an S3 tag to an object.</li> <li>◦ S3_OBJECT_TAGGING_DELETE - Removing an S3 tag from an object.</li> <li>◦ S3_OBJECT_TAGGING_ALL - Any S3 object tagging operation.</li> </ul> <ul style="list-style-type: none"> <li>• Object deletion events: <ul style="list-style-type: none"> <li>◦ S3_OBJECT_REMOVED_DELETE - Deletion of an S3 object by the S3 DELETE operation.</li> <li>◦ S3_OBJECT_REMOVED_DELETE_MARKER_CREATED - Creation of a delete marker for a versioned S3 object.</li> <li>◦ S3_OBJECT_REMOVED_ALL - Any S3 object deletion.</li> </ul> </li> </ul> <p>For example: <code>--triggers S3_OBJECT_CREATED_PUT,S3-OBJECT_REMOVED_ALL</code></p>
--	---

## Options

<pre>--prefix-filter FILTER_STRING</pre>	<p>Sends notifications only for those events that have an object key prefix matching the filter string.</p> <p>For example: <code>--prefix-filter mydocs/</code></p>
<pre>--suffix-filter FILTER_STRING</pre>	<p>Sends notifications only for those events that have an object key prefix matching the filter string.</p> <p>For example: <code>--suffix-filter .txt</code></p>

## Example

To send an event notification each time when a new object is created in the ABC folder on view 12:

```
vccli: admin> eventnotification create --name ev --view-id 12 --kafka-broker 1 --triggers S3_O
BJECT_CREATED_ALL
```

### eventnotification delete

This command deletes an event notification definition.

## Usage

```
eventnotification delete --name NAME
                        --view-id ID
```

## Required Parameters

<code>--name NAME</code>	The name of the event notification definition that you want to delete.
<code>--view-id ID</code>	The ID of the view to which the event notification configuration applies.

## Example

To delete event notification named EV configured for view 34:

```
vccli: admin> eventnotification delete --name ev --view-id 34
```

### eventnotification list

This command lists event notifications defined on the VAST cluster.

## Usage

```
eventnotification list
```

### eventnotification modify

This command modifies an event notification definition.

## Usage

```
eventnotification modify --name NAME
                        --view-id ID
                        [--broker-id ID]
                        [--topic TOPIC]
                        [--triggers EVENTS]
                        [--prefix-filter FILTER_STRING]
                        [--suffix-filter FILTER_STRING]
```

## Required Parameters

<code>--name NAME</code>	The name of the event notification definition that you want to edit.
<code>--view-id ID</code>	The ID of the view to which the event notification definition applies.

# Options

<code>--broker-id ID</code>	The ID of the event broker to which events will be published. The event broker must be <a href="#">defined</a> on the VAST cluster.
<code>--topic TOPIC</code>	The name of the topic to which to publish events.
<code>--triggers EVENTS</code>	<p>Specify a comma-separated list of events for which you want to send notifications. Valid keywords for <code>EVENTS</code> include:</p> <ul style="list-style-type: none"> <li>• Object creation events: <ul style="list-style-type: none"> <li>◦ <code>S3_OBJECT_CREATED_PUT</code> - Creation of an S3 object by a PUT request.</li> <li>◦ <code>S3_OBJECT_CREATED_POST</code> - Creation of an S3 object by a POST request.</li> <li>◦ <code>S3_OBJECT_CREATED_COPY</code> - Creation of an S3 object by copying an existing object.</li> <li>◦ <code>S3_OBJECT_CREATED_COMPLETE_MULTIPART_UPLOAD</code> - Creation of an S3 object as a result of a multi-part upload.</li> <li>◦ <code>S3_OBJECT_CREATED_ALL</code> - Any S3 object creation.</li> </ul> </li> <li>• Object tagging events: <ul style="list-style-type: none"> <li>◦ <code>S3_OBJECT_TAGGING_PUT</code> - Adding an S3 tag to an object.</li> <li>◦ <code>S3_OBJECT_TAGGING_DELETE</code> - Removing an S3 tag from an object.</li> <li>◦ <code>S3_OBJECT_TAGGING_ALL</code> - Any S3 object tagging operation.</li> </ul> </li> <li>• Object deletion events: <ul style="list-style-type: none"> <li>◦ <code>S3_OBJECT_REMOVED_DELETE</code> - Deletion of an S3 object by the S3 DELETE operation.</li> <li>◦ <code>S3_OBJECT_REMOVED_DELETE_MARKER_CREATED</code> - Creation of a delete marker for a versioned S3 object.</li> <li>◦ <code>S3_OBJECT_REMOVED_ALL</code> - Any S3 object deletion.</li> </ul> </li> </ul> <p>For example: <code>--triggers S3_OBJECT_CREATED_PUT,S3-OBJECT_REMOVED_ALL</code></p>
<code>--prefix-filter FILTER_STRING</code>	<p>Sends notifications only for those events that have an object key prefix matching the filter string.</p> <p>For example: <code>--prefix-filter mydocs/</code></p>
<code>--suffix-filter</code>	Sends notifications only for those events that have an object key prefix matching the filter

<code>FILTER_STRING</code>	<p>string.</p> <p>For example: <code>--suffix-filter .txt</code></p>
----------------------------	--

## Example

To modify an existing definition so that it sends event notifications to event broker 2:

```
vcli: admin> eventnotification modify --name ev --view-id 12 --kafka-broker 2
```

### eventnotification show

This command displays details of an event notification configuration.

## Usage

```
eventnotification show --name NAME
                      --view-id ID
```

## Required Parameters

<code>--name NAME</code>	The name of the event notification that you want to display.
<code>--view-id ID</code>	The ID of the view to which the event notification configuration applies.

## Example

To view event notification configuration named EV configured for view 34:

```
vcli: admin> eventnotification show --name ev --view-id 34
```

# globalsnapshotclone commands

## globalsnapshotclone create

This command creates either

- a directory on the local cluster cloned from a snapshot on a remote replication peer, or
- a cloned directory of a local snapshot, effectively restoring the snapshot data to the cluster.

The directory is instantly writable upon creation, and requests to read data from the directory can be read. Optionally, the clone can be *background synced* to the snapshot, which means that the data is fully copied to the cloned directory as a background task afterwards, such that when the copy is complete, read requests are all directed to the directory itself and are not dependent on the cloned snapshot.

## Usage

```
globalsnapshotclone create --name NAME
                             --target-path PATH
                             --target-tenant-id ID
                             [--source-cluster-id ID]
                             [--source-path PATH]
                             [--source-tenant TENANT_NAME]
                             [--remote-source-snapshot name NAME]
                             [--local-snapshot-id ID]
                             [--background-sync]
```

## Required Parameters

<code>--name NAME</code>	Specifies a name for the global snapshot clone.
<code>--target-path PATH</code>	Specifies a local path on the target tenant where you want the clone to reside.
<code>--target-tenant-id ID</code>	Specifies which tenant on the local cluster to which you want to clone the snapshot.

## Options

<code>--source-cluster-id ID</code>	Specifies a remote replication peer from which to clone a snapshot. Specify the ID of the peer, as listed by <a href="#">replicationpeer list</a> .
<code>--source-path PATH</code>	Specifies a path on the source cluster that you want to clone. The path must be protected by a snapshot. To retrieve paths on the remote peer that are protected by protected paths or by manual snapshots, run



	the <a href="#">cluster list-clone-snapshotted-paths-remote</a> command.
<code>--source-tenant</code> <code>TENANT_NAME</code>	Specifies to which tenant on the source cluster the source path belongs.
<code>--remote-source-snapshot</code> <code>name NAME</code>	<p>Use this option when cloning a snapshot on a remote peer, to specify the name of the snapshot of the source path you want to use to create the clone.</p> <p>To retrieve names of all available snapshots for a given source path on a given remote peer, run the <a href="#">cluster list-snapshotted-paths-remote</a> command.</p>
<code>--local-snapshot-id</code> <code>ID</code>	<p>Use this option when cloning a snapshot on the local peer, to specify which snapshot to use to create the clone.</p> <p>To retrieve snapshot IDs, run the <a href="#">snapshot list</a> command.</p>
<code>--background-sync</code>	<p>Causes the snapshot data to be copied from the source to the destination after the clone is created. During the copying stage, read requests are directed to the source if the requested data is not yet copied. When the copying is complete, the clone becomes a local directory.</p> <p>If not specified, this setting is disabled, in which case the snapshot data is only copied to the destination for requests to read data from the cloned directory.</p>

## Example

The following example clones a remote snapshot to a local directory:

```
vcli: admin> globalsnapshotclone create --name remote-gss --target-path /a-remote --target-tenant-id 1 --source-cluster-id 1 --remote-source-snapshot a-1 --source-path /a/ --source-tenant default
```

The following example restores a local snapshot:

```
vcli: admin> globalsnapshotclone create --name local-gss --target-path /local-gss --target-tenant-id 1 --local-snapshot-id 29
```

### globalsnapshotclone list

This command displays all global snapshot clones and their details.

## Usage

```
globalsnapshotclone list
```

# Example

```

vcli: admin> globalsnapshotclone list
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
| ID | Name          | Direction | Target-cluster | Target path | Target-tenant | Source-cluster |
| Source-path | Source-snapshot | Status      | Sync-progress | Bw   | Eta   |
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
| 1  | remote-clo   | N/A        | clusterA      | /a-remote/  | default       | clusterB      |
| None | N/A          | IN_PROGRESS | 0             | N/A  | None  |
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+

```

## globalsnapshotclone modify

This command change the name of a global snapshot clone.

# Usage

```
globalsnapshotclone modify --id ID
                             [--name NAME]
```

# Required Parameters

--id ID	Specifies which object to modify.
---------	-----------------------------------

# Options

--name NAME	Specifies a new name for the global snapshot clone.
-------------	---

# Example

```
vcli: admin> globalsnapshotclone modify --id 12 --name gsc-newer
```

## globalsnapshotclone pause

This command pauses the background sync of a global snapshot clone. Data continues to be available to user requests on the clone.

# Usage

```
globalsnapshotclone pause --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which global snapshot clone to pause.
----------------------	---

## Example

```
vcli: admin> globalsnapshotclone pause --id 3
```

### globalsnapshotclone remove

This command removes a global snapshot clone. This command is available for global snapshot clones that have the state *finished*.

## Usage

```
globalsnapshotclone remove --id ID  
                        [--remove-cloned-dir]
```

## Required Parameters

<code>--id ID</code>	Specifies which global snapshot clone to remove.
----------------------	--

## Options

<code>--remove-cloned-dir</code>	Include this option to remove the cloned directory. Otherwise, the directory is not removed.
----------------------------------	--

## Example

```
vcli: admin> globalsnapshotclone remove --id 4
```

### globalsnapshotclone resume

This command resumes the pausing of background sync of a global snapshot clone.

## Usage

```
globalsnapshotclone resume --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which global snapshot clone to resume.
----------------------	--

## Example

```
vccli: admin> globalsnapshotclone resume --id 4
```

### **globalsnapshotclone show**

This command displays details of a global snapshot clone.

## Usage

```
globalsnapshotclone show --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which global snapshot clone to display.
----------------------	---

## Example

```
vccli: admin> globalsnapshotclone show --id 2
```

```
+-----+-----+
| ID      | 2      |
| Name    | local-gss |
| Direction | N/A    |
| Target-cluster | loopA  |
| Target path | /local-gss/ |
| Target-tenant | default |
| Source-cluster | loopA  |
| Source-path | /loc/    |
| Source-snapshot | loc-1  |
| Status   | IN_PROGRESS |
| Sync-progress | 0      |
| Bw       | N/A      |
| Eta      | None     |
+-----+-----+
```

### **globalsnapshotclone stop**

This command stops and removes a global snapshot clone that was in progress.

## Usage

```
globalsnapshotclone stop --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which global snapshot clone to stop.
----------------------	--

## Example

```
vcli: admin> globalsnapshotclone stop --id 4
```

# group commands

## group create

This command creates a group on the local provider.

## Usage

```
group add --name NAME
          --gid GID
          [--identity-policies IDs]
          [--local-provider-id ID]
```

## Required Parameters

<code>--name NAME</code>	Sets the group's name.
<code>--gid GID</code>	Specifies the group's POSIX (NFS) GID attribute.

## Options

<code>--local-provider-id ID</code>	Specifies a local provider with which the group is associated.
<code>--identity-policy-ids</code>	Specifies identity policies with which the group is associated, as a comma-separated list.

## Examples

```
vccli: admin> group create --name mygroup --gid 1000 --local-provider-id 1
```

## group delete

This command deletes a group from the local provider.

## Usage

```
group delete --id ID
```

## Required Parameters

<code>--id ID</code>	Specify the VAST ID of the group to be deleted.
----------------------	---

## Example

```
vcli: admin> group delete --id 69
```

### group list

This command lists groups on the local provider.

## Usage

```
group list [--page-size SIZE [--page PAGE_NUMBER]]
```

## Options

<code>--page-size SIZE</code>	Sets the maximum number of groups per page. The default value is 200.
<code>--page PAGE_NUMBER</code>	Shows the page with the specified page number. The default value is 1.

## Example

```
vcli: admin> group list
+-----+-----+-----+-----+-----+
| ID | Name          | GID | SID |
+-----+-----+-----+-----+
| 1  | group-1000    | 1000 | S-1-111-1624147990-1599182510-3870292919-110815442-1 |
+-----+-----+-----+-----+-----+
```

### group modify

This command modifies a group.

## Usage

```
group modify --id ID
              [--name NAME]
              [--gid GID]
              [--identity-policies IDs]
              [--local-provider-id ID]
```

## Required Parameters

<code>--id ID</code>	Specifies the group.
----------------------	----------------------

## Options

<code>--name NAME</code>	Specifies the group's name.
<code>--gid GID</code>	Specifies the group's POSIX (NFS) GID attribute.
<code>--local-provider-id ID</code>	Specifies a local provider with which the group is associated.
<code>--identity-policy-ids</code>	Specifies identity policies with which the group is associated, as a comma-separated list.

## Examples

```
vccli: admin> group modify --id 1000 --name mynewgroup --local-provider-id 1
```

### group query

This command queries providers and the user database for a group. A provider query can be aggregated across providers to yield a merged result or it can be provider-specific.

You can also use this command to attach S3 identity policies to groups and to remove S3 identity policies from groups.

## Usage for Retrieving a Group

```
group query {--gid GID | --groupname GROUPNAME | --sid SID | --vaid VID}  
            [--context local|udb|ad|ldap|nis|aggregated]  
            [--tenant-id ID]
```

## Usage for Setting S3 Permissions

```
group query {--gid GID | --groupname GROUPNAME | --sid SID | --vaid VID}  
            [--identity-policies-ids [IDs]]  
            [--tenant-id ID]
```



## Required Parameters

<code>--gid GID</code>	Identifies a group by POSIX (NFS) group ID.
<code>--groupname GROUPNAME</code>	identifies a group by group name.
<code>--sid SID</code>	Identifies a group by Security Identifier (SID).
<code>--vaid VID</code>	Identifies a group by VAST ID.

## Options

<code>--context</code> <code>local udb ad ldap nis aggregated</code>	<p>Specify one of the following contexts:</p> <ul style="list-style-type: none"><li>• <b>local.</b> Restricts the search to local provider groups.</li><li>• <b>udb.</b> Searches the UDB for the group. The output in this case includes the VAID (VAST ID) for the group, which can be used to specify the group as a grantee in S3 ACLs.</li><li>• <b>aggregated (default).</b> Searches all providers and returns a merged entry. In case of conflicts between providers, attributes are resolved according to the following rules:<ul style="list-style-type: none"><li>◦ In case of conflict between local and non local providers, the local provider's attributes override those of the other providers.</li><li>◦ In case of conflicting POSIX attributes on external providers, the POSIX primary provider overrules the other external provider.</li><li>◦ Groups are merged if they match according to a non-configurable group name attribute.</li></ul></li><li>• <b>ad, nis or ldap.</b> Searches the specific provider only. (Each of these options appears only if a provider of that type is connected to the cluster.)</li></ul>
<code>--identity-policies-ids [IDS]</code>	<p>Assigns one or more S3 identity policies to the group.</p> <p>Specify <b>IDS</b> as a comma-separated list of S3 identity policy IDs.</p> <p>Each time you run the command with this option, the list overrides the entire previous list of S3 identity policies that were attached to the group. To remove a policy from a group, specify a list that does not include the policy you wish to remove. To remove all policies from the group, do not specify a list of IDs.</p>


<code>--tenant-id ID</code>	Specify the ID of the tenant with which the group is associated.
-----------------------------	--

# Example

```
vcli: admin> group query --gid 1000
+-----+-----+
| gid      | 1000 |
| sid      | S-1-5-21-927172180-3694312366-24219317-41086 |
| name     | group_gid_1000 |
| provider_type | NONE |
| s3_policies | [] |
| s3_policies_ids | [] |
+-----+-----+
```

## group query-by-prefix

This command queries Active Directory domains for groups by name prefix. It returns identifiers for groups whose names share a specified prefix.



**Tip**

The identifier for a given group can be provided in a [view modify](#) command as `--share-ace-identifier` in order to configure an share-level ACE for the group.

## Usage

```
group query-by-prefix --fqdn FQDN|ALL
                      --prefix PREFIX
                      [--active-directory-id ID]
                      [--tenant-id ID]
```

## Required Parameters

<code>--fqdn FQDN ALL</code>	Specifies either a specific fully qualified domain name of a joined Active Directory domain or 'ALL' to query all AD domains to which the cluster is joined.
<code>--prefix PREFIX</code>	Specifies a string prefix to query for groups on the specified domain.

## Options

<code>--active-directory-id ID</code>	Specifies the ID of Active Directory configuration under which user domains are searched for.
<code>--tenant-id ID</code>	Limits the search to the tenant specified with the tenant ID.

## Example

```
vcli: admin> group query-by-prefix --fqdn ad.arandomorg.com --prefix com
+-----+-----+-----+
| Name                | FQDN                  | Identifier type | Identifier          |
+-----+-----+-----+
| Compliance          | ad.arandomorg.com    | sid_str        | S-x-x-xx-xxxxxxxxx-xxxxxxxxxxx-xxxxxxx-xxxxxx |
| common_group_01     | ad.arandomorg.com    | sid_str        | S-x-x-xx-xxxxxxxxx-xxxxxxxxxxx-xxxxxxx-xxxxxx |
+-----+-----+-----+
```

## Command Output

Name	Name of a group.
FQDN	Fully qualified domain name of a joined Active Directory domain.
Identifier type	<p>Identifier attribute. Can be either:</p> <ul style="list-style-type: none"> <li>• <code>sid_str</code>. Group's SID attribute.</li> <li>• <code>uid_or_gid</code>. Group's GID attribute.</li> </ul>
Identifier	Identifier of type specified as <code>Identifier type</code> .

**group show**

This command displays detailed information for a group on the local provider.

# Usage

```
group show --id ID
```

# Required Parameters

--id ID	Specify the VAST ID of the group to be displayed.
---------	---

# Example

```
vcli: admin> group show --id 1
+-----+-----+
| ID    | 1      |
| Name  | group-1000 |
| GID   | 1000   |
| SID   | S-1-111-1624147990-1599182510-3870292919-110815442-1 |
+-----+-----+
```

# indestructibility commands

## indestructibility generate-token

This command generates a VMS token for unlocking the cluster's indestructibility mechanism. This command is intended for users who are authorized to unlock the cluster's indestructibility mechanism and requires a dedicated password.

Before running this command, open a support request for a challenge token. Support will verify that you are authorized to unlock the indestructibility mechanism. Run the command to generate the token and then provide the token to Support. Support will provide you with a challenge token. You can then run the [indestructibility unlock](#) command with the challenge token to unlock.

For more information about indestructibility, see [Indestructible Backups](#).

## Usage

```
indestructibility generate-token --indestructibility-passwd PASSWORD
```

## Required Parameters

<code>--indestructibility-passwd PASSWORD</code>	Specifies the indestructibility password, required to generate the token.
--	---

## Example

```
vccli: admin> indestructibility generate-token --indestructibility-passwd *****
```

## indestructibility list

This command displays details of the indestructibility configuration and status.

## Usage

```
indestructibility list
```

## Example

```
vccli: admin> indestructibility list
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name | Token | Token-time | Passwd-delay | Passwd-delay-eta | Unlock-system-time |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | N/A | None | None | 1 00:00:00 | None | None |
+-----+-----+-----+-----+-----+-----+-----+-----+
```

## indestructibility modify

This command modifies the indestructibility password and/or the indestructibility password restore delay. The password

restore delay postpones the effect of a user initiated reset of the indestructibility password.

You can use this command to change the default settings for the first time. After the default settings are changed, this command can only be used when the system is unlocked.

For more information about indestructibility, see [Indestructible Backups](#).

## Usage

```
indestructibility modify --indestructibility-passwd INDESTRUCTIBILITY_PASSWD
                        [--new-indestructibility-passwd NEW_INDESTRUCTIBILITY_PASSWD]
                        [--passwd-delay PASSWD_DELAY]
```

## Required Parameters

<code>--indestructibility-passwd</code> <code>INDESTRUCTIBILITY_PASSWD</code>	Specify the existing indestructibility password.  For first time password change, specify the default password, which is <code>LockPasswd</code> .
--	--

## Options

<code>--new-indestructibility-passwd</code> <code>NEW_INDESTRUCTIBILITY_PASSWD</code>	Specify a new indestructibility password. The password must have at least eight characters.  For example: <code>--new-indestructibility-passwd Yrt%587H9</code>
<code>--passwd-delay</code> <code>PASSWD_DELAY</code>	Changes the password reset delay.  Specify <code>PASSWD_DELAY</code> as an integer followed by <i>m</i> for minutes, <i>h</i> for hours or <i>d</i> for days.  For example: <code>--passwd-delay 5d</code> sets the password reset delay to five days.  Default: 1d (one day)  Minimum: 1m (one minute).

## Example

```
vccli: admin> indestructibility modify --indestructibility-passwd ***** --new-indestructibility-passwd *****
Indestructibility modified successfully
```

## indestructibility reset-passwd

This command restores the indestructibility password to its default value. There is a delay until the password restore takes effect. The delay provides additional security in case of a rogue admin using VMS to reset the password. The delay is one day, by default and can be changed using [indestructibility modify](#) while the indestructibility mechanism is unlocked.

For more information about indestructibility, see [Indestructible Backups](#).

## Usage

```
indestructibility reset-passwd
```

## Example

```
vcli: admin> indestructibility reset-passwd
Are you sure you want to reset Indestructibility passwd? Y
Indestructibility password will change in an passwd delay time
```

## indestructibility show

This command displays details of the indestructibility configuration and status.

For more information about indestructibility, see [Indestructible Backups](#).

## Usage

```
indestructibility show
```

## Example

This example

```
vcli: admin> indestructibility show
+-----+-----+
| ID          | 1          |
| Name        | N/A        |
| Token       | None       |
| Token-time  | None       |
| Passwd-delay | 1 00:00:00 |
| Passwd-delay-eta | None     |
| Unlock-system-time | None     |
+-----+-----+
```

## indestructibility unlock

This command unlocks the indestructibility mechanism, using a challenge token obtained from VAST Data Support.

Before running this command, run [indestructibility generate-token](#) to obtain a VMS token and provide the token returned by that command to VAST Data Support in a request for a challenge token.

The unlock procedure can only be performed by specially authorized personnel. For more details about the procedure for unlocking indestructibility, see [Indestructible Backups](#).

## Usage

```
indestructibility unlock --challenge-token CHALLENGE-TOKEN
```

## Required Parameters

<code>--challenge-token CHALLENGE-TOKEN</code>	Specifies a challenge token supplied on authorized request by VAST Data Support.
--	--

## Example

```
vcli: admin> indestructibility unlock --challenge-token *****  
System unlocked
```



# kafkabroker commands


## kafkabroker create

This command creates a Kafka [event broker configuration](#) on the VAST cluster.

## Usage

```
kafkabroker create --name NAME
                  --addresses ADDRESSES
                  [--tenant-ID TENANT_ID]
```

## Required Parameters

<code>--name NAME</code>	The name for the new Kafka broker configuration.
<code>--addresses ADDRESSES</code>	<p>Enter one or more Kafka broker bootstrap URLs.</p> <p>Specify <code>ADDRESSES</code> as a comma-separated list of <code>&lt;host&gt;:&lt;port&gt;</code> pairs, where:</p> <ul style="list-style-type: none"><li>• <code>&lt;host&gt;</code> is an IP address or FQDN of the Kafka broker server.</li><li>• <code>&lt;port&gt;</code> is the port number.</li></ul> <p>You can specify up to five <code>&lt;host&gt;:&lt;port&gt;</code> pairs.</p> <p>For example: <code>192.168.1.1:9092,192.168.1.2:9092</code></p> <div><b>Tip</b><p>Ensure that the hosts are accessible from the VAST cluster's management interface at the specified ports.</p></div>

## Options

<code>--tenant-id TENANT_ID</code>	<p>Add this option if you want to restrict use of this Kafka broker to a particular tenant.</p> <p>If this option is not specified, the Kafka broker will be available for all tenants.</p>
------------------------------------	---

# Example

To create setup to connect to a Kafka broker at 192.168.1.4 that will be used to publish events from tenant 3 only:

```
vcli: admin> kafkabroker create --name mybroker --addresses 192.168.1.4:9092 --tenant-id 3
```

## kafkabroker modify

This command modifies a Kafka [event broker configuration](#) on the VAST cluster.


# Usage

```
kafkabroker modify --id ID
                    [--name NAME]
                    [--addresses ADDRESSES]
                    [--tenant-ID TENANT_ID]
                    [--serve-all-tenants]
```

# Required Parameters

<code>--id ID</code>	The ID of the Kafka broker configuration that you want to change.
----------------------	---

# Options

<code>--addresses</code> ADDRESSES	<p>Kafka broker connection details.</p> <p>Specify ADDRESSES as a comma-separated list of &lt;host&gt;:&lt;port&gt; pairs, where:</p> <ul style="list-style-type: none"><li>• &lt;host&gt; is an IP address or FQDN of the Kafka broker server.</li><li>• &lt;port&gt; is the port number.</li></ul> <p>You can specify up to five &lt;host&gt;:&lt;port&gt; pairs.</p> <p>For example: 192.168.1.1:9092,192.168.1.2:9092</p> <div><b>Tip</b><p>Ensure that the hosts are accessible from the VAST cluster's management interface at the specified ports.</p></div>
<code>--tenant-id</code> TENANT_ID	Add this option if you want to restrict use of this Kafka broker to a particular tenant.

<code>--serve-all-tenants</code>	Lifts any existing tenant restrictions so that the Kafka broker can be used for all tenants.
----------------------------------	--

## Example

To make Kafka broker 2 available for tenant 5 only:

```
vcli: admin> kafkabroker modify --id 2 --tenant-id 5
```

### kafkabroker delete

This command deletes a Kafka [event broker configuration](#) from the VAST cluster.

## Usage

```
kafkabroker delete --id ID
```

## Required Parameters

<code>--id ID</code>	The ID of the Kafka broker configuration that you want to delete.
----------------------	---

## Example

To delete Kafka broker 2:

```
vcli: admin> kafkabroker delete --id 2
```

### kafkabroker list

This command lists Kafka brokers defined on the VAST cluster.

## Usage

```
kafkabroker list
```

### kafkabroker show

This command shows details of a Kafka [event broker configuration](#).

## Usage

```
kafkabroker show --id ID
```

## Required Parameters

<code>--id ID</code>	The ID of the Kafka broker configuration that you want to view.
----------------------	---

### kafkabroker list-topics

This command lists topics that exist on a particular Kafka event broker.

## Usage

```
kafkabroker list-topics --id ID  
                        [--topic-name-filter FILTER]
```

## Required Parameters

<code>--id ID</code>	The ID of the Kafka broker configuration for which you want to list topics.
----------------------	---

## Options

<code>--topic-name-filter FILTER</code>	A string to filter topic names.
---	---------------------------------

# Idap commands

## Idap create

This command configures a connection to an LDAP-based directory server.

## Usage

```
ldap create --urls URI_LIST
            --port PORT
            --basedn BASE_DN
            --method anonymous|simple|sasl
            --domain-name DOMAIN_NAME
            [--binddn BIND_DN]
            [--bindpw BIND_PASSWORD]
            [--group-basedn GROUP_BASE_DN]
            [--advanced-filter FILTER_STRING]
            [--query-groups-mode COMPATIBLE|RFC2307BIS_ONLY|RFC2307_ONLY|NONE]
            [--use-tls|--no-tls]
            [--vms-auth|--no-vms-auth]
            [--reverse-lookup|--no-reverse-lookup]
            [--gid-number ATTRIBUTE_NAME]
            [--uid ATTRIBUTE_NAME]
            [--uid-number ATTRIBUTE_NAME]
            [--member-uid ATTRIBUTE_NAME]
            [--posix-account ATTRIBUTE_NAME]
            [--posix-group ATTRIBUTE_NAME]
            [--match-user ATTRIBUTE_NAME]
            [--username-property-name ATTRIBUTE_NAME]
            [--user-login-name ATTRIBUTE_NAME]
            [--group-login-name ATTRIBUTE_NAME]
            [--mail-property-name ATTRIBUTE_NAME]
            [--uid-member-value-property-name ATTRIBUTE_NAME]
            [--super-admin-groups GROUPS]
            [--monitor-action PING|BIND]
```


## Required Parameters

<code>--urls URI_LIST</code>	<p>Enter URIs of LDAP servers. The order of listing defines the priority order. The URI with highest priority that has a good health status is used.</p> <p>Specify <code>URI_LIST</code> as a comma-separated list of URIs in the format <code>&lt;scheme&gt;://&lt;address&gt;</code>.</p> <p>Example: <code>--urls ldap://192.0.2.0,ldap://192.0.2.1,ldap://192.0.2.2</code></p>
<code>--port PORT</code>	<p>Sets the port of the remote LDAP server. Recommended values: 389 for LDAP (with or without TLS), 636 for LDAPS.</p>
<code>--basedn BASE_DN</code>	<p>Specifies the entry in the LDAP directory tree to use as a starting point for user queries. By default, this is also used as the starting point for group queries. Optionally, you can specify a</p>

	<p>different entry as the group base DN on <code>--group-searchbase</code>.</p> <p>To maximize the speed of authentication queries, start the search in the lowest branch of the tree under which all users can be found. For example, if the entire directory must be queried, the search base must specify the root of the tree. However, if the search can be restricted to a specific organizational unit (OU), queries may be faster.</p> <p>Specify <code>BASE_DN</code> as a comma separated list of components. Each component is an <i>attribute=value</i> pair defining an object in the directory tree. The first component defines the object at the lowest part of the tree that you want to use as the starting point of the search, the next component is its container and so on up the tree, with the last component representing the top level domain.</p> <p>The following attributes can be specified:</p> <ul style="list-style-type: none"> <li>• <code>cn</code>: common name</li> <li>• <code>ou</code>: organizational unit</li> <li>• <code>o</code>: organization</li> <li>• <code>c</code>: country</li> <li>• <code>dc</code>: domain</li> </ul>
<pre>--method anonymous simple sasl</pre>	<p>The authentication method the LDAP server uses to authenticate VAST Cluster as a client querying the LDAP database.</p> <p>Set the method according to how the LDAP server is configured to authenticate clients:</p> <ul style="list-style-type: none"> <li>• <code>anonymous</code>. The LDAP server accepts queries without any authentication.</li> <li>• <code>simple</code>. The LDAP server attempts to bind a specified user name to a matching LDAP user. If the LDAP bind succeeds, VAST Cluster is allowed to perform the query. If this method is specified, you have to set the bind DN on <code>--binddn</code> and password on <code>--bindpw</code>.</li> <li>• <code>sasl</code>. The LDAP server performs the Simple Authentication and Security Layer (SASL) authentication process. If the SASL bind succeeds, VAST Cluster is allowed to perform the query. If this method is specified, you have to set the bind DN on <code>--binddn</code> and password on <code>--bindpw</code>, with the bind DN in the <code>username@domain</code> or <code>DOMAIN\username</code> format.</li> </ul>
<pre>--domain-name DOMAIN_NAME</pre>	<p>Sets the fully qualified domain name (FQDN) of the domain to join.</p> <p>For example: <code>--domain-name company-ad.com</code></p>

# Options

<pre>--binddn BIND_DN (required if --method simple or --method sasl is specified)</pre>	<p>Sets the bind DN for authenticating to the LDAP server. The bind DN specifies the user with which VAST Cluster authenticates to the LDAP directory.</p> <p>Enter the bind DN for authenticating to the LDAP domain. The bind DN specifies the user with which VAST Cluster authenticates to the LDAP directory. You can specify any user account that has read access to the domain.</p> <p>The format is a comma separated list of components. Each component is an <i>attribute=value</i> pair defining an object in the directory tree. The first component is a <i>cn</i> attribute component specifying the user object, the next component is its container and so on up the tree, with the last component representing the top level domain.</p> <p>The following attributes can be specified:</p> <ul style="list-style-type: none"> <li>• cn: common name</li> <li>• ou: organizational unit</li> <li>• o: organization</li> <li>• c: country</li> <li>• dc: domain</li> </ul> <p>For example,  cn=admin,ou=users,dc=mydomain,dc=local specifies user 'admin' located in the 'users' container under the domain 'mydomain.local'.</p>
<pre>--bindpw BIND_PASSWORD (required if --method simple or --method sasl is specified)</pre>	<p>Sets the password used with the bind DN to authenticate to the LDAP server.</p>
<pre>--group-basedn GROUP_BASE_DN</pre>	<p>Sets the entry in the LDAP directory tree to use as a starting point for group queries. If not specified, the base DN is used.</p>
<pre>--advanced-filter FILTER_STRING</pre>	<p>Specify a search filter string to be to be appended to the search base DN in all user queries that VAST Cluster makes to this provider. Entries that do not match the filter string are filtered out from the query results.</p>
<pre>--query-groups-mode COMPATIBLE RFC2307BIS_ONLY RFC2307_ONLY NONE</pre>	<p>The mode for querying a user's auxiliary group memberships, when the auth provider is set as the source for group membership in the view policy:</p>

	<ul style="list-style-type: none"> <li>• <b>COMPATIBLE</b> (default). Groups are queried using an aggregate of the RFC2307BIS and RFC2307 compliant group membership queries (see the other options). You can use this default option unless you are using an authentication provider which is incompatible with this aggregated query mode.</li> <li>• <b>RFC2307BIS_ONLY</b>. Auxiliary group memberships are queried according to the RFC2307BIS standard, in which the group has a <i>members</i> attribute that contains the Distinguished Name (DN) of the member user and the user has a <i>memberOf</i> attribute which contains the DN's of the groups to which the user belongs. This standard is used by Active Directory and may be used with other LDAP-based authorization providers with LDAP schema extensions.</li> <li>• <b>RFC2307_ONLY</b>. Auxiliary group memberships are queried according to the RFC2307 standard, in which the group object has a <i>memberUid</i> attribute for each user object that is a member of the group, specifying the name of the user object. This standard may be used by openLDAP, freeIPA and other LDAP-based authorization providers.</li> <li>• <b>NONE</b>. If this option is selected, auxiliary group memberships are not queried at all. In the event that the relevant view's view policy cites the authorization provider as the group membership source and the user tries to access a file or directory within that view to which the user only has permission as a member of a the owning user's group, permission will not be granted.</li> </ul>
<pre>--use-tls</pre>	<p>Enables TLS (StartTLS) to secure communication between VAST Cluster and the LDAP server.</p> <p>When enabled, VAST Cluster connects to the standard port (port 389 for the domain controller, port 3268 for the Global Catalog) and performs a StartTLS operation as defined in RFC 4513.</p> <div>  <p><b>Important</b></p> <p>Use VAST Web UI to <a href="#">provide</a> a TLS certificate.</p> </div>
<pre>--no-tls</pre>	<p>Disables TLS (STARTTLS) secure communication between VAST Cluster and the LDAP server.</p>



<code>--vms-auth</code>	If this option is specified, the LDAP configuration being created will be the one used for VMS authentication.
<code>--no-vms-auth</code>	If this option is specified, the LDAP configuration being created will not be used for VMS authentication. This is the default setting.
<code>--reverse-lookup</code>	Enables use of DNS reverse lookup for the translation of a client IP address to a host name. When this option is specified, the server compares the host name to host names in netgroup entries. If not specified, the server queries DNS for each host name found in the netgroup entries.
<code>--no-reverse-lookup</code>	Disables use of reverse DNS lookup. This is the default setting.
<code>--super-admin-groups GROUPS</code>	Grants members of specified groups on the provider <i>cluster admin</i> manager access to VMS. Users in these groups can log into VMS. To grant permissions to these users, add the group name to roles. By default, they are assigned a read-only role.
<code>--monitor-action PING BIND</code>	<p>Determines the type of periodic health check that VAST cluster performs for an Active Directory provider configured for the cluster:</p> <ul style="list-style-type: none"> <li><code>PING</code> (default): Ping the provider. This option creates less overhead and reduces impact on the provider.</li> <li><code>BIND</code>: Bind to the provider.</li> </ul>

## Attribute Mapping Options

If your LDAP server uses attributes that differ from the default RFC2307-compliant attribute set that is used to query the LDAP server, these options map those attributes to the attribute names used on the server you are connecting the cluster to. This is typically needed for Active Directory.

Example: `uid=cn --posix-account user --posix-group group`

<code>--gid-number ATTRIBUTE_NAME</code>	<p>The attribute of a group entry that contains the GID number of a group.</p> <p>Default: <i>gidNumber</i></p> <p>Example for Active Directory: <code>--gid-number gidNumber</code></p>
--	--

<code>--uid ATTRIBUTE_NAME</code>	<p>The attribute of a user entry that contains the user name.</p> <p>Default: <i>uid</i></p> <p>Example for Active Directory: <code>--uid sAMAccountName</code></p>
<code>--uid-number ATTRIBUTE_NAME</code>	<p>The attribute of a user entry that contains the UID number.</p> <p>Default: <i>uidNumber</i></p>
<code>--member-uid ATTRIBUTE_NAME</code>	<p>The attribute of the group entry that contains names of group members.</p> <p>Example for Active Directory: <code>--member-uid member</code></p>
<code>--posix-account ATTRIBUTE_NAME</code>	<p>The object class that defines a user entry.</p>
<code>--posix-group ATTRIBUTE_NAME</code>	<p>The object class that defines a group entry.</p>
<code>--match-user ATTRIBUTE_NAME</code>	<p>Use this option to specify which attribute to use for matching users across providers during user refresh and user authentication. When querying a provider for a user that matches a user that was already retrieved from another provider, a user entry that contains a matching value in this attribute will be considered the same user as the user previously retrieved.</p> <p>Example: <code>--match-user sAMAccountName</code></p>
<code>--username-property-name ATTRIBUTE_NAME</code>	<p>Overrides 'name' as the attribute to use for querying users in VMS user-initiated user queries.</p>
<code>--user-login-name ATTRIBUTE_NAME</code>	<p>Specifies the attribute used to query the provider for the user's login name.</p> <p>For example: <code>--user-login-name sAMAccountName</code></p>
<code>--group-login-name ATTRIBUTE_NAME</code>	<p>Specifies the attribute used to query the provider for the group's login name.</p> <p>For most environments, it is recommended to use the default value of <code>cn</code>.</p>
<code>--mail-property-name ATTRIBUTE_NAME</code>	<p>Specifies the attribute to use for the user's email address.</p>

<pre>--uid-member-value- property-name ATTRIBUTE_NAME</pre>	Specifies the attribute which represents the value of the LDAP group's <code>member</code> property.
---	--

## Example

```
vcli: admin> ldap create --url ldap://mydomain.local --port 389 --binddn admin@mydomain.local
--bindpw !@WE56yt -group searchbase ou=groups,dc=mydomain,dc=local --method simple --domain-n
ame company-ad.com --uid=distinguishedName --member-uid member --posix-account user --posix-g
roup group --use-tls
```

### ldap delete

This command deletes and LDAP configuration record.

## Usage

```
ldap delete --id ID
```

## Required Parameters

<pre>--id ID</pre>	Specifies the LDAP configuration to delete.
--------------------	---

## Example

```
vcli: admin> ldap delete --id 1
```

### ldap list

This command displays LDAP configuration and connection details.

## Usage

```
ldap list
```

## Example

```
vcli: admin> ldap list
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

```

+-----+
| ID | URLs | Port | Bind-DN | Search-Base | Group-Search-Base | Me
thod | State | gidNumber | uid | uidNumber | memberUid | PosixAccount | Uid-me
mber-value-property-name | PosixGroup | Use TLS | POSIX Primary Provider | Match-user | Q
uery-groups-mode | Username-property-name | Domain Name | User-login-name | Group-login-name
| TLS-certificate | Mail-property-name | Use-auto-discovery | Use-ldaps | Is-vms-auth-provide
r | Posix-attributes-source | Domains-with-posix-attributes | Read-Only-Value | Read-Write-Va
lue | Resolve-Hostnames | Enable trusted domains on other forests |
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
| 1 | ['ldap://my.co-ad.com'] | 389 | COMP\adm | dc=co-ad,dc=com | dc=co-ad,dc=lab | si
mple | CONNECTED | gidNumber | sAMAccountName | uidNumber | member | user | uid
| group | False | False | sAMAccountName | COMPATIBLE | name
| COMP.com | sAMAccountName | sAMAccountName | | | F
alse | False | False | JOINED_DOMAIN | []
| ro | rw | False | False
|
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
+-----+

```

## ldap modify

This command modifies an existing LDAP configuration.

## Usage

```

ldap modify --id ID
    [--urls URI_LIST]
    [--enable-use-ldaps|--disable-use-ldaps]
    [--port PORT]
    [--binddn BIND_DN]
    [--bindpw BIND_PASSWORD]
    [--basedn BASE_DN]
    [--group-basedn GROUP_BASE_DN]
    [--advanced-filter FILTER_STRING]
    [--query-groups-mode COMPATIBLE|RFC2307BIS_ONLY|RFC2307_ONLY|NONE]
    [--method anonymous|simple|sasl]
    [--domain-name DOMAIN_NAME]
    [--use-tls|--no-tls]
    [--vms-auth|--no-vms-auth]
    [--reverse-lookup|--no-reverse-lookup]
    [--gid-number ATTRIBUTE_NAME]
    [--uid ATTRIBUTE_NAME]
    [--uid-number ATTRIBUTE_NAME]
    [--member-uid ATTRIBUTE_NAME]
    [--posix-account ATTRIBUTE_NAME]
    [--posix-group ATTRIBUTE_NAME]
    [--match-user ATTRIBUTE_NAME]
    [--username-property-name ATTRIBUTE_NAME]
    [--user-login-name ATTRIBUTE_NAME]
    [--group-login-name ATTRIBUTE_NAME]

```

```
[--mail-property-name ATTRIBUTE_NAME]
[--uid-member-value-property-name ATTRIBUTE_NAME]
[--super-admin-groups GROUPS]
[--monitor-action PING|BIND]
```

## Required Parameters

<code>--id ID</code>	Identifies the LDAP configuration record to modify.
----------------------	---

## Options


<code>--urls URI_LIST</code>	<p>If Active Directory domain auto-discovery is disabled, enter URIs of LDAP servers (domain controllers in the Active Directory joined domain). The order of listing defines the priority order. The URI with highest priority that has a good health status is used.</p> <p>The domain controllers should all be in the same Active Directory domain which VAST Cluster joins.</p> <p>Specify <code>URI_LIST</code> as a comma-separated list of URIs in the format <code>&lt;scheme&gt;://&lt;address&gt;</code>.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li><code>--urls ldap://company-ad.com</code></li> <li><code>--urls ldaps://company-ad.com</code></li> <li><code>--urls ldap://company-ad.com,ldap://company-ad2.com</code></li> <li><code>--urls ldap://192.0.2.0,ldap://192.0.2.1,ldap://192.0.2.2</code></li> </ul>
<code>--enable-use-ldaps</code>	<p>Enables use of LDAPS for Active Directory domain auto-discovery.</p> <p>When enabled, VAST Cluster connects to an alternative port (port 636 for the domain controller, port 3269 for the Global Catalog) and initiates a TLS handshake immediately afterwards.</p>
<code>--disable-use-ldaps</code>	Disables use of LDAPS for Active Directory domain auto-discovery.
<code>--port PORT</code>	Sets the port of the remote LDAP server. Recommended values: 389 for LDAP (with or without TLS), 636 for LDAPS.

<pre>--binddn BIND_DN</pre>	<p>Sets the bind DN for authenticating to the LDAP server. The bind DN specifies the user with which VAST Cluster authenticates to the LDAP directory.</p> <p>You can specify any user account that has read access to the domain.</p> <p>This bind DN must be set if <code>--method simple</code> is specified.</p> <p>The format is a comma separated list of components. Each component is an <i>attribute=value</i> pair defining an object in the directory tree. The first component is a <i>cn</i> attribute component specifying the user object, the next component is its container and so on up the tree, with the last component representing the top level domain.</p> <p>The following attributes can be specified:</p> <ul style="list-style-type: none"> <li>• <i>cn</i>: common name</li> <li>• <i>ou</i>: organizational unit</li> <li>• <i>o</i>: organization</li> <li>• <i>c</i>: country</li> <li>• <i>dc</i>: domain</li> </ul> <p>For example, <code>cn=admin,ou=users,dc=mydomain,dc=local</code> specifies user 'admin' located in the 'users' container under the domain 'mydomain.local'.</p> <p>If <a href="#">multi-forest authentication</a> is enabled and/or SASL authentication method is used, specify the bind DN in one of the following formats:</p> <ul style="list-style-type: none"> <li>• <code>username@domain</code></li> <li>• <code>DOMAIN\username</code></li> </ul>
<pre>--bindpw BIND_PASSWORD</pre>	<p>Sets the password used with the bind DN to authenticate to the LDAP server.</p> <p>This password must be set if <code>--method simple</code> is specified.</p>
<pre>--basedn BASE_DN</pre>	<p>If Active Directory domain auto-discovery is disabled, specifies the entry in the LDAP directory tree to use as a starting point for user queries. By default, this is also used as the starting point for group queries. Optionally, you can specify a different entry as the group base DN on <code>--group-searchbase</code>.</p> <p>To maximize the speed of authentication queries, start the search in the lowest branch of the tree under which all users can be found. For example, if the entire directory must be queried, the search base must specify the root of the tree. However, if the search can be restricted to a specific organizational unit (OU), queries may be faster.</p>

	<p>Specify <code>BASE_DN</code> as a comma separated list of components. Each component is an <i>attribute=value</i> pair defining an object in the directory tree. The first component defines the object at the lowest part of the tree that you want to use as the starting point of the search, the next component is its container and so on up the tree, with the last component representing the top level domain.</p> <p>The following attributes can be specified:</p> <ul style="list-style-type: none"> <li>• <code>cn</code>: common name</li> <li>• <code>ou</code>: organizational unit</li> <li>• <code>o</code>: organization</li> <li>• <code>c</code>: country</li> <li>• <code>dc</code>: domain</li> </ul> <p>For example, supposing your user accounts are all located in a container called 'users' under a domain 'mydomain.local'. If you want to set the users container as the starting point for search queries, you would enter: <code>--basedn ou=users,dc=mydomain,dc=local</code></p>
<code>--group-basedn GROUP_BASE_DN</code>	Sets the entry in the LDAP directory tree to use as a starting point for group queries. If not specified, the base DN is used.
<code>--advanced-filter FILTER_STRING</code>	Specify a search filter string to be to be appended to the search base DN in all user queries that VAST Cluster makes to this provider. Entries that do not match the filter string are filtered out from the query results.
<code>--query-groups-mode</code> <code>COMPATIBLE RFC2307BIS_ONLY RFC2307_ONLY NONE</code>	<p>The mode for querying a user's auxiliary group memberships, when the auth provider is set as the source for group membership in the view policy:</p> <ul style="list-style-type: none"> <li>• <b>COMPATIBLE</b> (default). Groups are queried using an aggregate of the RFC2307BIS and RFC2307 compliant group membership queries (see the other options). You can use this default option unless you are using an authentication provider which is incompatible with this aggregated query mode.</li> <li>• <b>RFC2307BIS only</b>. Auxiliary group memberships are queried according to the RFC2307BIS standard, in which the group has a <i>members</i> attribute that contains the Distinguished Name (DN) of the member user and the user has a <i>memberOf</i> attribute which contains the DNs of the groups to which the user belongs. This standard is used by Active Directory and may be used with other LDAP-based authorization providers with LDAP schema extensions.</li> </ul>

	<ul style="list-style-type: none"> <li>• RFC2307 only. Auxiliary group memberships are queried according to the RFC2307 standard, in which the group object has a <i>memberUid</i> attribute for each user object that is a member of the group, specifying the name of the user object. This standard may be used by openLDAP, freeIPA and other LDAP-based authorization providers.</li> <li>• NONE. If this option is selected, auxiliary group memberships are not queried at all. In the event that the relevant view's view policy cites the authorization provider as the group membership source and the user tries to access a file or directory within that view to which the user only has permission as a member of a the owning user's group, permission will not be granted.</li> </ul>
<pre>--method simple anonymous sasl</pre>	<p>The authentication method the LDAP server uses to authenticate VAST Cluster as a client querying the LDAP database.</p> <p>When <a href="#">multi-forest authentication</a> is enabled, VAST Cluster uses SASL for the LDAP bind to domain controllers in other trusted forests, and this setting is only honored for the LDAP bind to domain controllers in the forest of the cluster's joined domain.</p> <p>Set the method according to how the LDAP server is configured to authenticate clients:</p> <ul style="list-style-type: none"> <li>• <i>anonymous</i>. The LDAP server accepts queries without any authentication.</li> <li>• <i>simple</i>. The LDAP server attempts to bind a specified user name to a matching LDAP user. If the LDAP bind succeeds, VAST Cluster is allowed access to perform the query. If this method is specified, you have to set the bind DN on <code>--binddn</code> and password on <code>--bindpw</code>.</li> <li>• <i>sasl</i>. The LDAP server performs the Simple Authentication and Security Layer (SASL) authentication process. If the SASL bind succeeds, VAST Cluster is allowed to perform the query. If this method is specified, you have to set the bind DN on <code>--binddn</code> and password on <code>--bindpw</code>, with the bind DN in the <code>username@domain</code> or <code>DOMAIN\username</code> format.</li> </ul>
<pre>--domain-name DOMAIN_NAME</pre>	<p>Sets the fully qualified domain name (FQDN) of the domain to join.</p> <p>For example: <code>--domain-name company-ad.com</code></p>
<pre>--use-tls</pre>	<p>Enables TLS (StartTLS) to secure communication between VAST Cluster and the LDAP server.</p> <p>When enabled, VAST Cluster connects to the standard port (port 389 for the domain controller, port 3268 for the Global Catalog) and performs a StartTLS operation as defined in RFC 4513.</p>



	 <b>Important</b>  Use VAST Web UI to <a href="#">provide</a> a TLS certificate.
<code>--no-tls</code>	Disables TLS (STARTTLS) secure communication between VAST Cluster and the LDAP server.
<code>--vms-auth</code>	If this option is specified, the LDAP configuration being created will be the one used for VMS authentication.
<code>--no-vms-auth</code>	If this option is specified, the LDAP configuration being created will not be used for VMS authentication. This is the default setting.
<code>--reverse-lookup</code>	Enables use of DNS reverse lookup for the translation of a client IP address to a host name. When this option is specified, the server compares the host name to host names in netgroup entries. If not specified, the server queries DNS for each host name found in the netgroup entries.
<code>--no-reverse-lookup</code>	Disables use of reverse DNS lookup. This is the default setting.
<code>--super-admin-groups GROUPS</code>	Grants members of specified groups on the provider <i>cluster admin</i> manager access to VMS. Users in these groups can log into VMS. To grant permissions to these users, add the group name to roles. By default, they are assigned a read-only role.
<code>--monitor-action PING BIND</code>	Determines the type of periodic health check that VAST cluster performs for an Active Directory provider configured for the cluster: <ul style="list-style-type: none"> <li><code>PING</code> (default): Ping the provider. This option creates less overhead and reduces impact on the provider.</li> <li><code>BIND</code>: Bind to the provider.</li> </ul>

## Attribute Mapping Options

If your LDAP server uses attributes that differ from the default RFC2307-compliant attribute set that is used to query the LDAP server, these options map those attributes to the attribute names used on the server you are connecting the cluster to. This is typically needed for Active Directory.

**Example:** `uid=cn --posix-account user --posix-group group`

<code>--gid-number ATTRIBUTE_NAME</code>	<p>The attribute of a group entry that contains the GID number of a group.</p> <p>Default: <i>gidNumber</i></p>
<code>--uid ATTRIBUTE_NAME</code>	<p>The attribute of a user entry that contains the user name.</p> <p>Default: <i>uid</i></p>
<code>--uid-number ATTRIBUTE_NAME</code>	<p>The attribute of a user entry that contains the UID number.</p> <p>Default: <i>uidNumber</i></p>
<code>--member-uid ATTRIBUTE_NAME</code>	<p>The attribute of the group entry that contains names of group members.</p>
<code>--posix-account ATTRIBUTE_NAME</code>	<p>The object class that defines a user entry.</p>
<code>--posix-group ATTRIBUTE_NAME</code>	<p>The object class that defines a group entry.</p>
<code>--match-user ATTRIBUTE_NAME</code>	<p>Use this option to specify which attribute to use for matching users across providers during user refresh and user authentication. When querying a provider for a user that matches a user that was already retrieved from another provider, a user entry that contains a matching value in this attribute will be considered the same user as the user previously retrieved.</p> <p>Example: <code>--match-user sAMAccountName</code></p>
<code>--username-property-name ATTRIBUTE_NAME</code>	<p>Overrides 'name' as the attribute to use for querying users in VMS user-initiated user queries.</p>
<code>--user-login-name ATTRIBUTE_NAME</code>	<p>Specifies the attribute used to query the provider for the user's login name.</p> <p>For example: <code>--user-login-name sAMAccountName</code></p>
<code>--group-login-name ATTRIBUTE_NAME</code>	<p>Specifies the attribute used to query the provider for the group login name.</p> <p>For most environments, it is recommended to use the default value of <code>cn</code>.</p>

<code>--mail-property-name ATTRIBUTE_NAME</code>	Specifies the attribute to use for the user's email address.
<code>--uid-member-value-property-name ATTRIBUTE_NAME</code>	Specifies the attribute which represents the value of the LDAP group's <code>member</code> property.

## Example

```
vcli: admin> ldap modify --no-tls
```

### ldap set\_primary\_provider

This command sets an LDAP provider to be the POSIX primary provider.

## Usage

```
ldap set_primary_provider --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies the LDAP provider configuration.
----------------------	--

## Example

```
vcli: admin> ldap set_primary_provider --id 1
```

### ldap show

This command displays details of a configured LDAP connection.

## Usage

```
ldap show --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies the LDAP connection to display.
----------------------	---

	<p>Specify <code>ID</code> as an integer value.</p> <p>To retrieve an LDAP connection ID, run <code>ldap list</code>.</p>
--	---

## Example

```
vccli: admin> ldap show --id 1
```

+-----+-----+		
ID	1	
URLs	['ldap://my.co-ad.com']	
Port	389	
Bind-DN	COMP\adm	
Search-Base	dc=co-ad,dc=com	
Group-Search-Base	dc=co-ad,dc=com	
Method	simple	
State	CONNECTED	
gidNumber	gidNumber	
uid	SAMAccountName	
uidNumber	uidNumber	
memberUid	member	
PosixAccount	user	
PosixGroup	group	
Use TLS	False	
POSIX Primary Provider	False	
Match-user	SAMAccountName	
Query-groups-mode	COMPATIBLE	
Username-property-name	name	
Domain Name	COMP.com	
User-login-name	SAMAccountName	
Group-login-name	SAMAccountName	
TLS-certificate		
Mail-property-name	mail	
Use-auto-discovery	False	
Use-ldaps	False	
Is-vms-auth-provider	True	
Posix-attributes-source	JOINED_DOMAIN	
Domains-with-posix-attributes	[]	
Read-Only-Value	ro	
Read-Write-Value	rw	
Resolve-Hostnames	False	
Enable trusted domains on other forests	False	
+-----+-----+		

# license commands

## license add

This command installs a license key on the cluster.

## Usage

```
license add --license-key LICENSE_KEY
```

## Required Parameters

<code>--license-key LICENSE_KEY</code>	Specifies the license key to install.
--	---------------------------------------

## Example

```
vccli: admin> license add --license-key gAAAAABgRHciUs9Mu-y0rTS7grA0Kt-pm852jwMdDlyAqZFxUNDEWH  
sdmbVA83vbPbS0nyz9bchFWJECWZYyOejzX4dVoXxuvlMj3bl5NbN6qD6CVjtFKA6ITFKocEic-lcY_3dw1063
```

## license delete

This command deletes a license.

## Usage

```
license delete --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which license to delete.
----------------------	------------------------------------

## Example

```
vccli: admin> license delete --id 1
```

## license list

This command displays all licenses and their details.

# Usage

license list [--vertical]

## Options

--vertical	Displays the list vertically.
------------	-------------------------------

## Example

```
vcli: admin> license list
+-----+-----+-----+-----+-----+-----+-----+
+
+ | ID | State | Start-date | Expiration-date | Period [months] | Capacity [TB] | License-key |
+ |-----+-----+-----+-----+-----+-----+-----+
+ | 1 | ACTIVE | 2021-05-23 | UNLIMITED | UNLIMITED | 674.276 | gAAAAABgRHciUs9Mu-y0rTS7grA0Kt-pm852jwMdDlyAqZFxUNDEWHsdmbVA83vbPbS0nyz9bchFWJECWZYyOejzX4dVoXxuvlMj3bl5NbN6qD6CVjtFKA6ITFKocEic-1cY_3dw1063 |
+ |-----+-----+-----+-----+-----+-----+-----+
+
+
```

### license show

This command displays details of a specific license.

## Usage

license show --id ID

## Required Parameters

--id ID	Specifies which license to display.
---------	-------------------------------------

## Example

```
vcli: admin> license show --id 2
+-----+-----+-----+-----+
+ | ID | State | Start-date | Expiration-date |
+ |-----+-----+-----+-----+
+ | 2 | ACTIVE | 2021-05-23 | UNLIMITED |
+ |-----+-----+-----+-----+
+
```

Period [months]	UNLIMITED	
Capacity [TB]	674.276	
License-key	gBBBBGBrRFciUr9Hr-y0tEHG7grA0Kt-pm852jwMdDlyAqZFxUNEWFs...	
+-----+-----+-----+-----+-----+-----+-----+-----+-----+		

# lifecycle rule commands

## lifecycle rule create

This command creates an S3 lifecycle rule.

## Usage

```
lifecycle rule create --name NAME
                      --view-id ID
                      --enable|--disable
                      [--prefix PREFIX]
                      [--min-size SIZE]
                      [--max-size SIZE]
                      [--expiration-days DAYS]
                      [--enable-expired-obj-delete-marker|--disable-expired-obj-delete-marker]
                      [--noncurrent-days DAYS]
                      [--newer-noncurrent-versions VERSIONS]
                      [--abort-mpu-days-after-initiation DAYS]
                      [--object-age-attr MODIFICATION_TIME|ACCESS_TIME|CREATION_TIME]
```

## Required Parameters

<code>--name NAME</code>	Specifies a name for the rule.
<code>--view-id ID</code>	Specifies the ID of the view to which the rule applies.

## Options

<code>--enable</code>	Enables the rule immediately upon its creation.
<code>--disable</code>	Specify this option to create a rule without enabling it immediately
<code>--prefix PREFIX</code>	<p>Defines a prefix to limit the object scope by object prefix.</p> <p>In S3 terms, this is a prefix that may be common to multiple object keys (names). Specifying a prefix defines a scope of objects to which the rule applies. For example, if you specify <i>sales/jan</i>, all objects in the view that have object keys that begin with <i>sales/jan</i> will fall into the scope.</p> <p>In terms of file and directory nomenclature, a prefix is a file and/or directory path within the view that can include part of the file</p>



	<p>or directory name. It can be common to multiple items in order to catch them all within the scope.</p> <p>For example, if you want to specify all files under a directory called <i>sales</i> that resides under the view, you can specify <i>salessales/</i>. This prefix will exclude the directory itself from the scope. If you were to specify <i>sales</i> that would include the directory as well as all the files under the directory. If you were to specify <i>sales/j</i> that would include all files under the directory with names that begin with 'j'.</p> <p>For example: <code>--prefix logs/</code></p>
<code>--min-size SIZE</code>	<p>Specifies a minimum object size to limit the scope by size.</p> <p>Specify SIZE as an integer followed by MB, GB, TB, etc.</p> <p>For example: <code>--min-size 2GB</code></p>
<code>--max-size SIZE</code>	<p>Specifies a maximum object size to limit the scope by size.</p> <p>Specify SIZE as an integer followed by MB, GB, TB, etc.</p> <p>For example: <code>--max-size 1TB</code></p>
<code>--expiration-days DAYS</code>	<p>Specifies a number of days after objects are created that they expire.</p> <p>In a non versioned bucket view, expiration means that the object is permanently removed.</p> <p>In a versioned bucket view, where the objects are versioned:</p> <ul style="list-style-type: none"> <li>• if the current version is not a delete marker, a delete marker is created and that becomes the current version. The existing current version is retained as a non current version. When the delete marker reaches this same number of days, it is deleted.</li> <li>• If there are one or more object versions and the delete marker is the current version, no action is taken.</li> <li>• If the current object version is the only object version and it is also a delete marker, it is removed. That is, all object versions were deleted and there is only a delete marker remaining. This is called an expired object delete marker and it is removed.</li> </ul>
<code>--enable-expired-obj-delete-marker</code>	<p>Relevant only for versioned buckets.</p>

	<p>Enables deletion of <i>expired object delete markers</i> when they become expired object delete markers.</p> <p>An expired object delete marker is an object version that is the only version of an object and is also a delete marker.</p> <p>This parameter is mutually exclusive with <code>--expiration-days DAYS</code>, which deletes expired object delete markers when they satisfy the specified age criteria. If you want to expire objects using <code>--expiration-days DAYS</code> and also clean up expired object delete markers as soon as they are created as such, create two separate rules.</p>
<code>--disable-expired-obj-delete-marker</code>	<p>Relevant only for versioned buckets.</p> <p>Disables deletion of <i>expired object delete markers</i> when they become expired object delete markers.</p>
<code>--noncurrent-days DAYS</code>	<p>Relevant only for versioned buckets. If provided, noncurrent versions of objects are deleted after the specified number of days, provided they are not the newest noncurrent versions up to the number set to be retained, if that number is provided with <code>--newer-noncurrent-versions VERSIONS</code>.</p>
<code>--newer-noncurrent-versions VERSIONS</code>	<p>Relevant only for versioned buckets. Use this parameter to specify a number of noncurrent versions of objects to retain. The newest non current versions up to this number will not expire even if they exceed <code>--noncurrent-days</code>.</p>
<code>--abort-mpu-days-after-initiation DAYS</code>	<p>Specifies to remove incomplete multipart uploads, which are not removed through <code>--expiration-days</code>. The value is the number of days after multipart uploads are started when they should be aborted and removed if they are incomplete.</p>
<code>--object-age-attr</code> <code>MODIFICATION_TIME ACCESS_TIME CREATION_TIME</code>	<p>Determines which timestamp to use as the time from which to count expiration days, if <code>--expiration-days</code> is set.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li><code>MODIFICATION_TIME</code> (default). The time the object was last modified.</li> <li><code>ACCESS_TIME</code>. The time the object content was last accessed.</li> <li><code>CREATION_TIME</code>. The time the object was created (or if different, the time the object's metadata was last modified.)</li> </ul>

## Example

```
vccli: admin> lifecyclerule create --name expirelogsrule --view-id 11 --enable --prefix /logs
--expiration-days 60
```

### lifecycle rule delete

This command deletes an S3 lifecycle rule.

## Usage

```
lifecycle rule delete --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which S3 lifecycle rule to delete.
----------------------	--

### lifecycle rule get-object-expiration

This command retrieves the expiration date for an object in a bucket governed by S3 lifecycle rules.

## Usage

```
lifecycle rule get-object-expiration --bucket-name BUCKET_NAME
--object-name OBJECT_NAME
```

## Required Parameters

<code>--bucket-name BUCKET_NAME</code>	Specifies a bucket name.
<code>--object-name OBJECT_NAME</code>	Specifies the name of an object in the specified bucket.

### lifecycle rule list

This command lists S3 lifecycle rules for a specified view.

## Usage

```
lifecycle rule list --view-id ID
                    [--page PAGE]
                    [--page-size SIZE]
```

## Required Parameters

<code>--view-id ID</code>	Specifies a view by its ID.
---------------------------	-----------------------------

## Options

<code>--page PAGE</code>	Display specified page (by #) if page size limit is set.
<code>--page-size SIZE</code>	Maximum number of rules per page.  Default: 20  Limit: 500

### lifecycle rule modify

This command modifies an S3 lifecycle rule.

## Usage

```
lifecycle rule modify --name NAME
                        [--enable|--disable]
                        [--prefix PREFIX]
                        [--min-size SIZE]
                        [--max-size SIZE]
                        [--expiration-days DAYS]
                        [--enable-expired-obj-delete-marker|--disable-expired-obj-delete-marker]
                        [--noncurrent-days DAYS]
                        [--newer-noncurrent-versions VERSIONS]
                        [--abort-mpu-days-after-initiation DAYS]
                        [--object-age-attr MODIFICATION_TIME|ACCESS_TIME|CREATION_TIME]
```

## Required Parameters

<code>--name NAME</code>	Identifies a rule to modify.
--------------------------	------------------------------

## Options

<code>--enable</code>	Enables the rule.
-----------------------	-------------------

<code>--disable</code>	Disables the rule.
<code>--prefix PREFIX</code>	Specifies a prefix common to limit the object scope by object prefix.  For example: <code>--prefix logs/</code>
<code>--min-size SIZE</code>	Specifies a minimum object size to limit the scope by size.  Specify SIZE as an integer followed by MB, GB, TB, etc.  For example: <code>--min-size 2GB</code>
<code>--max-size SIZE</code>	Specifies a maximum object size to limit the scope by size.  Specify SIZE as an integer followed by MB, GB, TB, etc.  For example: <code>--max-size 1TB</code>
<code>--expiration-days DAYS</code>	Specifies a number of days after objects are created that they expire.  In a non versioned bucket view, expiration means that the object is permanently removed.  In a versioned bucket view, where the objects are versioned: <ul style="list-style-type: none"> <li>• if the current version is not a delete marker, a delete marker is created and that becomes the current version. The existing current version is retained as a non current version. When the delete marker reaches this same number of days, it is deleted.</li> <li>• If there are one or more object versions and the delete marker is the current version, no action is taken.</li> <li>• If the current object version is the only object version and it is also a delete marker, it is removed. That is, all object versions were deleted and there is only a delete marker remaining. This is called an expired object delete marker and it is removed.</li> </ul>
<code>--enable-expired-obj-delete-marker</code>	Relevant only for versioned buckets.  Enables deletion of <i>expired object delete markers</i> when they become expired object delete markers.  An expired object delete marker is an object version that is the only version of an object and is also a delete marker.

	<p>This parameter is mutually exclusive with <code>--expiration-days DAYS</code>, which deletes expired object delete markers when they satisfy the specified age criteria. If you want to expire objects using <code>--expiration-days DAYS</code> and also clean up expired object delete markers as soon as they are created as such, create two separate rules.</p>
<code>--disable-expired-obj-delete-marker</code>	<p>Relevant only for versioned buckets.</p> <p>Disables deletion of <i>expired object delete markers</i> when they become expired object delete markers.</p>
<code>--noncurrent-days DAYS</code>	<p>Relevant only for versioned buckets. If provided, noncurrent versions of objects are deleted after the specified number of days, provided they are not the newest noncurrent versions up to the number set to be retained, if that number is provided with <code>--newer-noncurrent-versions VERSIONS</code>.</p>
<code>--newer-noncurrent-versions VERSIONS</code>	<p>Relevant only for versioned buckets. Use this parameter to specify a number of noncurrent versions of objects to retain. The newest non current versions up to this number will not expire even if they exceed <code>--noncurrent-days</code>.</p>
<code>--abort-mpu-days-after-initiation DAYS</code>	<p>Specifies to remove incomplete multipart uploads, which are not removed through <code>--expiration-days</code>. The value is the number of days after multipart uploads are started when they should be aborted and removed if they are incomplete.</p>
<code>--object-age-attr</code> <code>MODIFICATION_TIME ACCESS_TIME CREATION_TIME</code>	<p>Determines which timestamp to use as the time from which to count expiration days, if <code>--expiration-days</code> is set.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li><code>MODIFICATION_TIME</code> (default). The time the object was last modified.</li> <li><code>ACCESS_TIME</code>. The time the object content was last accessed.</li> <li><code>CREATION_TIME</code>. The time the object was created (or if different, the time the object's metadata was last modified.)</li> </ul>

## lifecycle rule show

This command displays details of a specific S3 lifecycle rule.

# Usage

```
lifecyclerule show --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which S3 lifecycle rule to display.
----------------------	---

# localprovider commands

## localprovider create

This command creates a local provider.

## Usage

```
localprovider create --name NAME
                    --managed-by SUPER_ADMIN | TENANT_ADMIN
                    [--description DESC]
```

## Required Parameters

<code>--name NAME</code>	Specifies the name of the provider
<code>--managed-by SUPER_ADMIN   TENANT_ADMIN</code>	<p>Determines whether users defined for the provider are managed by cluster admins and/or tenant admins.</p> <p>If set to <code>SUPER_ADMIN</code>, only cluster admins can define and view and manage users and groups for the provider. Tenant admins for the tenant associated with the provider cannot view or manage these users or groups.</p> <p>If set to <code>TENANT_ADMIN</code>, only the tenant admin for the tenant associated with the provider can view and manage users and groups. Cluster admins have no visibility about these users or groups.</p> <p>If set to both, then both types of admins have visibility about users and groups defined in the provider.</p>

## Options

<code>--description DESC</code>	Add a description for the provider.
---------------------------------	-------------------------------------

## Example

This example...

```
vccli: admin> localprovider create --name myLocalProvider --managed_by TENANT_ADMIN
```

## object delete

This command deletes a local provider.



## Usage

```
localprovider delete --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which local provider to delete. You can find out the ID using the <code>localprovider list</code> command.
----------------------	--

## Example

```
vccli: admin> localprovider delete --id 1
```

### localprovider list

This command displays all local providers and their details.

## Usage

```
localprovider list
```

## Example

```
vccli: admin> localprovider list
+-----+-----+-----+-----+-----+
| ID | Name      | Description | Managed By      | Assigned Tenants Preview |
+-----+-----+-----+-----+-----+
| 1  | default  |              | ['SUPER_ADMIN'] | default, mgmt             |
+-----+-----+-----+-----+-----+
```

### localprovider modify

This command modifies a local provider.

## Usage

```
localprovider modify --id ID
                      [--name NAME]
                      [--managed-by SUPER_ADMIN | TENANT_ADMIN]
                      [--description DESC]
```

## Required Parameters

<code>--id</code>	Specifies which local provider to modify. You can determine the ID using the <code>localprovider show</code> or
-------------------	---

ID	<code>localprovider list</code> command.
----	--

## Options

<code>--name NAME</code>	Specifies the name of the provider.
<code>--managed-by SUPER_ADMIN   TENANT_ADMIN</code>	<p>Determines whether users and groups defined for the provider are managed by cluster admins and/or tenant admins.</p> <p>If set to <code>SUPER_ADMIN</code>, only cluster admins can define and view and manage users and groups for the provider. Tenant admins for the tenant associated with the provider cannot view or manage these users or groups.</p> <p>If set to <code>TENANT_ADMIN</code>, only the tenant admin for the tenant associated with the provider can view and manage users and groups. Cluster admins have no visibility about these users or groups.</p> <p>If set to both, then both types of admins have visibility about users and groups defined in the provider.</p>
<code>description DESC</code>	Specifies a description for the provider.

## Example

This example changes the name and managed-by settings for a provider.

```
vccli: admin> localprovider modify --id 1 --name myLocalProvider --managed-by TENANT_ADMIN
```

### localprovider show

This command displays details of a specific local provider.

## Usage

```
localprovider show --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which local provider to display. You can find out the ID of the local provider using the <code>localprovider list</code> command.
--------------------------	---

## Example

```
vccli: admin> localprovider show --id 1
```

+-----+-----+	
ID	1
Name	default
Description	
Managed By	['SUPER_ADMIN']
Assigned Tenants Preview	default, mgmt
+-----+-----+	

# manager commands

## manager assign

This command assigns management functions to a VMS manager user.

## Usage

```
manager assign --id ID
                [--realm events|hardware|logical|monitoring|security|settings|support]
                [--permissions create|view|edit|delete]
                [--object-type TYPE]
                [--object-id ID]
```

## Required Parameters

<code>--id ID</code>	Identifies the manager for which to assign permissions for management functions.
----------------------	--

## Options

<code>--realm events hardware logical monitoring security settings support</code>	Specifies a realm of management functions for which to assign permissions to the manager.
<code>--permissions create view edit delete</code>	Grants the specified permissions for the realm set with <code>--realm</code> .
<code>--object-type TYPE and</code>	<p>This option is used together with <code>--object-id</code> to grant permissions set with <code>--permissions</code> for a certain object.</p> <p>Use <code>--object-type</code> to supply the type of the object and then further limit the scope by specifying the <code>--object-id</code>.</p> <p>Specify one of the following object types as <code>TYPE</code>:</p> <ul style="list-style-type: none"><li>• cluster</li><li>• cnode</li><li>• dnode</li><li>• dbox</li><li>• cbox</li></ul>

	<ul style="list-style-type: none"> <li>• view</li> <li>• viewpolicy</li> <li>• quota</li> <li>• vipppool</li> <li>• eventdefinition</li> <li>• ldap</li> </ul>
<code>---object-id ID</code>	Grants permissions set with <code>--permissions</code> for the object identified with <code>--object-id</code> of the object type specified with <code>--object-type</code> .

## Example

To allow a manager with ID 6 to edit events:

```
vccli: admin> manager assign --id 6 --realm events --permissions edit
```

### manager create

This command creates a [VMS manager user](#).

## Usage

```
manager create --username NAME
               --role-id ID
               [--password PASSWORD]
               [--prompt-password]
               [--first-name NAME]
               [--last-name NAME]
               [--enable-is-temporary-password]
               [--disable-is-temporary-password]
               [--enable-password-expiration]
               [--disable-password-expiration]
```

## Required Parameters

<code>--username NAME</code>	The manager's user name.
<code>--role-id ID</code>	The ID of the role to assign to the manager.

# Options

<code>--password</code> PASSWORD	The manager password.
<code>--prompt-password</code>	If specified, the manager is prompted for the password.
<code>--first-name</code> NAME	The manager's first name.
<code>--last-name</code> NAME	The manager's last name.
<code>--enable-is-temporary-password</code>	Sets the password as temporary, which means that VMS allows the manager to log in with the temporary password within seven days. The only action available to the user after logging in with a temporary password is to change the password.
<code>--disable-is-temporary-password</code>	Disables temporary password setting.
<code>--enable-password-expiration</code>	Enables the password to expire according to the password expiration period set by <a href="#">vms modify</a> .
<code>--disable-password-expiration</code>	Prevents the manager's password from expiring.

## Example

To create a manager named John Smith with a username of *jsmith* and role ID 12:

```
vccli: admin> manager create --username jsmith --first-name John --last-name Smith --role-id 12
```


### manager delete

This command deletes a VMS manager user.

# Usage

`manager delete --id ID`

## Required Parameters

<code>--id ID</code>	<div>Identifies the manager user to be deleted.</div> <div> <b>Tip</b> Run <code>manager list</code> to obtain IDs of VMS managers.</div>
----------------------	--

## Example

To delete a manager user with ID 14:

```
vccli: admin> manager delete --id 14
```

### manager join

This command assigns a certain role to a VMS manager user.

## Usage

`manager join --id ID`  
`--role-id ID`

## Required Parameters

<code>--id ID</code>	Identifies the manager to which to assign a role.
<code>--role-id ID</code>	Identifies the role to be assigned to the manager.

## Example

To assign role 8 to manager 3:

```
vccli: admin> manager join --id 3 --role-id 8
```

## manager leave

This command removes a certain role from a VMS manager user.

## Usage

```
manager leave --id ID
              --role-id ID
```

## Required Parameters

<code>--id ID</code>	Identifies the manager from which to remove a role.
<code>--role-id ID</code>	Identifies the role to be removed from the manager.

## Example

To remove role 2 from manager 4:

```
vccli: admin> manager join --id 4 --role-id 2
```

## manager list

This command shows all managers and their details.

## Usage

```
manager list
```

## Example

```
vccli: admin> manager list
+---+-----+-----+-----+-----+
+-----+
+-----+
| ID | Username           | First-name | Last-name | Roles
| Default |
+---+-----+-----+-----+
+-----+
| 4 | S3_keys_manager |           |           | [{'id': 2, 'name': 'read_only'}]
| True |
| 2 | admin           |           |           | [{'id': 1, 'name': 'administrators'}, {'i
d': 5, 'name': 'csi'}] | True |
| 1 | root            |           |           | [{'id': 1, 'name': 'administrators'}, {'i
d': 4, 'name': 'debug_metrics'}, {'id': 5, 'name': 'csi'}] | True |
| 3 | support         |           |           | [{'id': 1, 'name': 'administrators'}, {'i
d': 4, 'name': 'debug_metrics'}, {'id': 5, 'name': 'csi'}] | True |
+---+-----+-----+-----+-----+
+-----+
```



+-----+  
+-----+

## manager modify

This command modifies a VMS manager user.

## Usage

```
manager modify [--id ID|--username NAME]
               [--password PASSWORD]
               [--prompt-password]
               [--first-name NAME]
               [--last-name NAME]
               [--enable-is-temporary-password]
               [--disable-is-temporary-password]
               [--enable-password-expiration]
               [--disable-password-expiration]
```

## Required Parameters

<code>--id ID</code>	Identifies the manager with the manager ID.
<code>--username NAME</code>	Identifies the manager with the manager's username ID.

## Options

<code>--password</code> PASSWORD	The manager password.
<code>--prompt-</code> password	If specified, the manager is prompted for the password.
<code>--first-name</code> NAME	The manager's first name.
<code>--last-name</code> NAME	The manager's last name.
<code>--enable-is-</code> temporary-	Sets the password as temporary, which means that VMS allows the manager to log in with the temporary password within seven days. The only action available to the user after logging in with a temporary

password	password is to change the password.
--disable-is-temporary-password	Disables temporary password setting.
--enable-password-expiration	Enables the password to expire according to the password expiration period set by <a href="#">vms modify</a> .
--disable-password-expiration	Prevents the manager's password from expiring.

## Example

To change the last name of a manager with username *jsmith*:

```
vcli: admin> manager modify --username jsmith --last-name Gale
```

### manager show

This command displays details of a VMS manager user.

## Usage

```
manager show --id ID
```

## Required Parameters

--id ID	Identifies the manager to display.
---------	------------------------------------

## Example

```
vcli: admin> manager show --id 4
```

```
+-----+
| ID      | 4 |
| Username | S3_keys_manager |
| First-name |  |
| Last-name  |  |
| Roles     | [{'id': 2, 'name': 'read_only'}] |
| Default   | True |
+-----+
```

## manager unassign

## Usage

```
manager assign --id ID
               [--realm events|hardware|logical|monitoring|security|settings|support]
               [--permissions create|view|edit|delete]
               [--object-type TYPE]
               [--object-id ID]
               [--ldap-groups]
               [--tenant-ids]
```

## Required Parameters

<code>--id ID</code>	Identifies the manager from which to remove permissions for management functions.
----------------------	---

# Options

<pre>--realm events hardware  logical monitoring  security settings support</pre>	<p>Specifies a realm of management functions for which to remove permissions from the manager.</p>
<pre>--permissions create view edit delete</pre>	<p>Removes the specified permissions for the realm set with <code>--realm</code>.</p>
<pre>--object-type TYPE and</pre>	<p>This option is used together with <code>--object-id</code> to remove permissions set with <code>--permissions</code> for a certain object.</p> <p>Use <code>--object-type</code> to supply the type of the object and then further limit the scope by specifying the <code>--object-id</code>.</p> <p>Specify one of the following object types as <code>TYPE</code>:</p> <ul style="list-style-type: none"> <li>• cluster</li> <li>• cnode</li> <li>• dnode</li> <li>• dbx</li> <li>• cbx</li> </ul>

	<ul style="list-style-type: none"> <li>• view</li> <li>• viewpolicy</li> <li>• quota</li> <li>• vipool</li> <li>• eventdefinition</li> <li>• ldap</li> </ul>
<code>---object-id ID</code>	Removes permissions set with <code>--permissions</code> for the object identified with <code>--object-id</code> of the object type specified with <code>--object-type</code> .
<code>--ldap-groups GROUPS</code>	Specify a LDAP group name or a comma-separated list of LDAP group names.
<code>--tenant-id ID</code>	Specify a tenant ID or a comma-separated list of tenant IDs.

# Example

To prohibit editing events by a manager with ID 6:

```
vcli: admin> manager unassign --id 6 --realm events --permissions edit
```

## manager unlock

This command unlocks a VMS manager user that was locked out after exceeding the maximum number of failed login attempts.

# Usage

```
manager unlock --id ID
                [--password PASSWORD]
                [--enable-is-temporary-password]
                [--disable-is-temporary-password]
```

# Required Parameters

<code>--id ID</code>	Identifies the manager with the manager ID.
----------------------	---

## Options

<code>--password PASSWORD</code>	Sets a new password.
<code>--enable-is- temporary- password</code>	Sets the password as temporary, which means that VMS allows the manager to log in with the temporary password within seven days. The only action available to the user after logging in with a temporary password is to change the password.
<code>--disable- is- temporary- password</code>	Disables temporary password setting.

## Example

```
vcli: admin> manager unlock --id 14 --password 85tRuFYu --enable-is-temporary-password
```

# nis commands

## nis create

This command adds a new NIS configuration.

## Usage

```
nis create --domain-name DOMAIN_NAME
           --servers SERVERS
```

## Required Parameters

<code>--domain-name</code> <code>DOMAIN_NAME</code>	Specifies the NIS domain name shared by all the NIS servers and clients on your network.  Example: <code>--domain-name NIS.companyname.com</code>
<code>--servers</code> <code>SERVERS</code>	A comma-separated list of NIS servers. You can specify up to ten servers.  Specify each server by its IP or host name, up to 48 characters. You can specify up to ten servers.  Example: <code>--servers</code> <code>NISmaster.companyname.com,192.0.2.200,NISslave2.companyname.com</code>

## Example

```
vccli: admin> nis create --domain-name NIS.companyname.com --servers NISmaster.companyname.co  
m,192.0.2.200,NISslave2.companyname.com
```

## nis delete

This command deletes a NIS configuration.

## Usage

```
nis delete --id ID
```

## Required Parameters

<code>--id</code> <code>ID</code>	Identifies the NIS configuration to delete.
-----------------------------------	---

# Example

```
vcli: admin> nis delete --id 1
```

## nis list

This command shows the NIS configuration details.

# Usage

```
nis list
```

# Example

```
vcli: admin> nis list
+-----+-----+-----+-----+-----+
| ID | Servers           | Domain Name | State      | POSIX Primary |
+-----+-----+-----+-----+-----+
| 2  | ['192.0.2.200'] | domain.com  | CONNECTED | True           |
+-----+-----+-----+-----+-----+
```

## nis modify

This command modifies an existing NIS configuration.

# Usage

```
nis modify --id ID
            [--domain-name DOMAIN_NAME]
            [--servers SERVERS]
```

# Required Parameters

<code>--id ID</code>	Identifies the NIS configuration to modify.
----------------------	---

# Options

<code>--domain-name</code> <code>DOMAIN_NAME</code>	Specifies the NIS domain name shared by all the NIS servers and clients on your network.  Example: <code>--domain-name NIS.companyname.com</code>
<code>--servers</code> <code>SERVERS</code>	A comma-separated list of NIS servers. You can specify up to ten servers.

	<p>Specify each server by its IP or host name, up to 48 characters. You can specify up to ten servers.</p> <p>Example: <code>--servers NISmaster.companyname.com,192.0.2.200,NISslave2.companyname.com</code></p>
--	---

## Example

To change the domain name to *my.domain.com*:

```
vcli: admin> nis modify --id 1 --domain-name my.domain.com
```

### nis refresh

This command refreshes NIS cache.

## Usage

```
nis refresh
```

## Example

```
vcli: admin> nis refresh
```

### nis set\_primary\_provider

This command sets NIS as the primary POSIX provider.

## Usage

```
nis set_primary_provider --id ID
```

## Required Parameters

<code>--id ID</code>	Identifies the NIS configuration to be used as the primary POSIX provider.
----------------------	--

## Example

```
vcli: admin> nis set_primary_provider --id 1
```

### nis show

This command displays details of a NIS configuration.



# Usage

```
nis show --id ID
```

## Required Parameters

<code>--id ID</code>	Identifies the NIS configuration to display.
----------------------	--

## Example

```
vcli: admin> nis show --id 2
+-----+-----+
| ID      | 2      |
| Servers | ['192.0.2.200'] |
| Domain Name | domain.com |
| State   | CONNECTED |
| POSIX Primary | True    |
+-----+-----+
```

# nvrām commands

## nvrām activate

This command activates an NVRAM device.

## Usage

```
nvrām activate --id ID
```

## Required Parameters

<code>--id ID</code>	Specify the NVRAM ID.  To list NVRAM IDs, use the <a href="#">nvrām list</a> command.
----------------------	---

## Example

This example shows activation of NVRAM 2:

```
vcli: admin> nvrām activate --id 2
```

## nvrām deactivate

This command deactivates an NVRAM device.

## Usage

```
nvrām deactivate --id ID
```

## Required Parameters

<code>--id ID</code>	Specify the NVRAM ID.  To list NVRAM IDs, use the <a href="#">nvrām list</a> command.
----------------------	---

## Example

This example shows deactivation of NVRAM 2:

```
vcli: admin> nvrām deactivate --id 2
```

# **nvramp list**

This command displays all NVRAMs and their details.

## **Usage**

```
nvramp list [--state STATE]
            [--sn SN]
            [--dbox-name DBOX_NAME]
            [--dbox-id DBOX_ID]
            [--fw-version FIRMWARE_VERSION]
```

## **Options**

<code>--state STATE</code>	<p>Filters the list by NVRAM state, which can be one of the following:</p> <ul style="list-style-type: none"><li>• ACTIVATING</li><li>• ACTIVE</li><li>• DEACTIVATING</li><li>• INACTIVE</li><li>• FAILING</li><li>• FAILED</li><li>• PHASING_OUT</li><li>• ENTER_PHASING_OUT</li><li>• EXIT_PHASING_OUT</li><li>• UNKNOWN</li></ul>
<code>--dbox-name DBOX_NAME</code>	<p>Filters the list by the name of the DBox to which the NVRAMs belong.</p> <p>Specify <code>DBOX_NAME</code> as a string value.</p>
<code>--dbox-id DBOX_ID</code>	<p>Filters the list by the ID of the DBox to which the NVRAMs belong..</p> <p>Specify <code>DBOX_ID</code> as an integer value.</p>
<code>--fw-version FIRMWARE_VERSION</code>	<p>Filters the list by firmware version.</p>
<code>--sn SN</code>	<p>Filters the list by serial number.</p>

For example: nvram list --sn PHKE931600ZA1P5CGN

## Example

```
vccli: admin> nvram list
```

```
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
| ID | Name | State | Serial-Number | Model | Total-Space(TB) | DBox
| Slot | Shelf | Attached-dnode-names | Firmware-Version | Enabled | Failure-Reason |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
| 1 | | ACTIVE | PHKE931600ZA1P5CGN | INTEL SSDPE21K015TA | 1.500 | | dbx-0A7P
F016 | 53 | LEFT | dnode-105 | E2010485 | True | NONE | |
| 2 | | ACTIVE | PHKE932000QZ1P5CGN | INTEL SSDPE21K015TA | 1.500 | | dbx-0A7P
F016 | 49 | LEFT | dnode-105 | E2010485 | True | NONE | |
| 3 | | ACTIVE | PHKE9320004D1P5CGN | INTEL SSDPE21K015TA | 1.500 | | dbx-0A7P
F016 | 45 | LEFT | dnode-105 | E2010485 | True | NONE | |
| 4 | | ACTIVE | PHKE931600WD1P5CGN | INTEL SSDPE21K015TA | 1.500 | | dbx-0A7P
F016 | 25 | RIGHT | dnode-105 | E2010485 | True | NONE | |
| 5 | | ACTIVE | PHKE932000PY1P5CGN | INTEL SSDPE21K015TA | 1.500 | | dbx-0A7P
F016 | 21 | RIGHT | dnode-105 | E2010485 | True | NONE | |
| 6 | | ACTIVE | PHKE931601191P5CGN | INTEL SSDPE21K015TA | 1.500 | | dbx-0A7P
F016 | 17 | RIGHT | dnode-105 | E2010485 | True | NONE | |
| 7 | | ACTIVE | PHKE931600YP1P5CGN | INTEL SSDPE21K015TA | 1.500 | | dbx-0A7P
F016 | 41 | LEFT | dnode-104 | E2010485 | True | NONE | |
| 8 | | ACTIVE | PHKE931600WW1P5CGN | INTEL SSDPE21K015TA | 1.500 | | dbx-0A7P
F016 | 37 | LEFT | dnode-104 | E2010485 | True | NONE | |
| 9 | | ACTIVE | PHKE932000PX1P5CGN | INTEL SSDPE21K015TA | 1.500 | | dbx-0A7P
F016 | 33 | LEFT | dnode-104 | E2010485 | True | NONE | |
| 10 | | ACTIVE | PHKE931600VK1P5CGN | INTEL SSDPE21K015TA | 1.500 | | dbx-0A7P
F016 | 13 | RIGHT | dnode-104 | E2010485 | True | NONE | |
| 11 | | ACTIVE | PHKE932000591P5CGN | INTEL SSDPE21K015TA | 1.500 | | dbx-0A7P
F016 | 9 | RIGHT | dnode-104 | E2010485 | True | NONE | |
| 12 | | ACTIVE | PHKE9320005Q1P5CGN | INTEL SSDPE21K015TA | 1.500 | | dbx-0A7P
F016 | 5 | RIGHT | dnode-104 | E2010485 | True | NONE | |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
```

# projection commands

## projection create

This command creates a projection in a VAST Database table. A projection is a set of selected columns in a table. You can specify columns in the projection that are used to sort the rows of the projection.

Up to 64 projections can be created in a single table.

## Usage

```
projection create --database-name DATABASE
                 --schema-name SCHEMA
                 --table-name TABLE
                 --name PROJECTION
                 --sorted-columns SORTED_COLUMNS
                 [--unsorted-columns UNSORTED_COLUMNS]
                 [--tenant-id TENANT]
```

## Required Parameters

<code>--database-name DATABASE</code>	Specifies the name of the database containing the table.
<code>--schema-name SCHEMA</code>	Specifies the name of the schema containing the table.
<code>--table-name TABLE</code>	Specifies the name of the table containing the columns.
<code>--name PROJECTION</code>	Specifies the name of the projection. This is used to refer to the projection in other commands, such as <a href="#">projection show</a> .
<code>--sorted-columns SORTED_COLUMNS</code>	<p>Specifies the columns in the projection (from the table) that are used to sort the projection. The rows of the projection are sorted by these columns, in the order they appear in the list.</p> <p>For example, for <i>--sorted-columns a,b,c,d</i>, the rows in the projection are sorted first by the value in column <i>a</i>, then <i>b</i>, then <i>c</i>, and, finally, by <i>d</i>. Any other columns in the projection (from the <i>unsorted-columns</i> list) would not be used for sorting.</p> <p>Specify SORTED_COLUMNS as a comma-separated list of column names, with no spaces.</p> <p>You can specify up to four columns to sort the projection by.</p>

# Options

<pre>--unsorted-columns UNSORTED_COLUMNS</pre>	<p>Specifies additional columns in the projection (from the table) that are not used to sort the projection.</p> <p>Specify the columns as a comma-separated list, with no spaces.</p> <p>You can specify any number of unsorted columns for the projection, but they cannot include columns included in the sorted-columns list.</p> <p>Columns that are not in the sorted or unsorted list are not included in the projection (and cannot, therefore, be included in queries on the projection).</p>
<pre>--tenant-id TENANT</pre>	<p>Specifies the ID of the tenant where the database resides</p> <p>If omitted, the default tenant is assumed.</p>

## Examples

This example includes a list of sorted columns only. The projection includes only these columns, and is sorted according to all of them in the order they appear in the list.

```
vccli: admin> projection create --database-name tabular --schema-name vast --table-name tab  
l--name myProj --sorted-columns id,logtime,user_id,currency  
Projection has been created
```

This example includes a list of unsorted columns as well. The projection includes the sorted and unsorted columns, but is sorted only according to the sorted list.

```
vccli: admin> projection create --database-name tabular --schema-name vast --table-name tab1  
--name myProj2 --sorted-columns id,logtime,user_id,currency --unsorted-columns session_id,i  
s_nha,language,member_id  
Projection has been created
```

### projection delete

This command deletes a projection.

## Usage

```
projection delete --database-name DATABASE  
                  --schema-name SCHEMA  
                  --table-name TABLE  
                  --name PROJECTION  
                  [--tenant-id TENANT]
```

## Required Parameters

<code>--database-name DATABASE</code>	Specifies the name of the database containing the table.
<code>--schema-name SCHEMA</code>	Specifies the name of the schema containing the table.
<code>--table-name TABLE</code>	Specifies the name of the table.
<code>--name PROJECTION</code>	Specifies the name of the projection to be deleted.

## Options

<code>--tenant-id TENANT</code>	Enter the ID of the tenant where the database resides  If omitted, the default tenant is assumed.
---------------------------------	---

## Example

```
vcli: admin> projection delete --database-name tabular --schema-name vastagoda --table-name a  
goda --name newProj  
Projection has been deleted
```

### projection list

This command shows the projections for a specific VAST Database table.

## Usage

```
projection list --database-name DATABASE  
                --schema-name SCHEMA  
                --table-name TABLE  
                [--page PAGE]  
                [--page-size PAGE_SIZE]  
                [--name PROJECTION]  
                [--name-startswith PREFIX]  
                [--tenant-id TENANT]
```

## Required Parameters

<code>--database-name DATABASE</code>	Specifies the name of the database containing the table.
---------------------------------------	--

<code>--schema-name SCHEMA</code>	Specifies the name of the schema containing the table.
<code>--table-name TABLE</code>	Specifies the name of the table.

## Options

<code>--page PAGE</code>	Specifies the specific page in the output list, by its number. This parameter is used only if <code>page-size</code> is set. Default is the first page.
<code>--page-size PAGE_SIZE</code>	Specifies the maximum number of projections to list per output page. Default: 100.
<code>--name PROJECTION</code>	Specifies the name of a projection.
<code>--name-startswith PREFIX</code>	Specifies a prefix to filter the projection names.
<code>--tenant-id TENANT</code>	Enter the ID of the tenant where the database resides  If omitted, the default tenant is assumed.

## Examples

```

vcli: admin> projection list --database-name tabular --schema-name vastagoda --table-name agoda
+-----+-----+-----+-----+-----+-----+
+-----+
| Name      | Database-name | Schema-name | Table-name | Properties | Num-rows  | Size
|
+-----+-----+-----+-----+-----+-----+
+-----+
| agodaproj | tabular      | vastagoda  | agoda      | None       | 9569577211 | 2077351076
539 |
| myProj    | tabular      | vastagoda  | agoda      | None       | 9377687803 | 9366255280
87 |
| myProj2   | tabular      | vastagoda  | agoda      | None       | 9377687803 | 1364574579
040 |
+-----+-----+-----+-----+-----+-----+
+-----+

```

### projection rename

This command renames a projection.



# Usage

```
projection rename --database-name DATABASE
                  --schema-name SCHEMA
                  --table-name TABLE
                  --name PROJECTION
                  --new-name NEW_PROJECTION_NAME
                  [--tenant-id TENANT]
```

## Required Parameters

<code>--database-name DATABASE</code>	Specifies the name of the database containing the table.
<code>--schema-name SCHEMA</code>	Specifies the name of the schema containing the table.
<code>--table-name TABLE</code>	Specifies the name of the table.
<code>--name PROJECTION</code>	Specifies the name of the projection to be renamed.
<code>--new-name NEW_PROJECTION_NAME</code>	Specifies the new name of the renamed projection

## Options

<code>--tenant-id TENANT</code>	Enter the ID of the tenant where the database resides  If omitted, the default tenant is assumed.
---------------------------------	---

## Example

```
vccli: admin> projection rename --database-name tabular --schema-name vastagoda --table-name a
goda --name myProj --new-name newProj
Projection has been renamed
```

### projection show

Shows details for a specific projection.

## Usage

```
projection show --database-name DATABASE
                --schema-name SCHEMA
```

```
--table-name TABLE
--name PROJECTION
[--tenant-id TENANT]
```

## Required Parameters

<code>--database-name DATABASE</code>	Specifies the name of the database containing the table.
<code>--schema-name SCHEMA</code>	Specifies the name of the schema containing the table.
<code>--table-name TABLE</code>	Specifies the name of the table.
<code>--name PROJECTION</code>	Specifies the name of the projection.

## Options

<code>--tenant-id TENANT</code>	Specifies the ID of the tenant where the database resides  If omitted, the default tenant is assumed.
---------------------------------	---

## Example

```
vcli: admin> projection show --database-name tabular --schema-name vastagoda --table-name agoda --name myProj
```

```
+-----+-----+
| Name           | myProj      |
| Database-name  | tabular     |
| Schema-name    | vastagoda   |
| Table-name     | agoda       |
| Properties     | None        |
| Num-rows       | 9377687803  |
| Size           | 936625528087 |
| Initial-sync-progress(%) | 100.0      |
+-----+-----+
```

# projectioncolumn commands

## projectioncolumn list

This command lists the columns in a VAST Database table projection.

## Usage

```
projectioncolumn list --database-name DATABASE
                    --schema-name SCHEMA
                    --table-name TABLE
                    [--name PROJECTION]
                    [--page PAGE]
                    [--page-size PAGE_SIZE]
                    [--name-startswith PREFIX]
                    [--tenant-id TENANT]
```

## Required Parameters

<code>--database-name DATABASE</code>	Specifies the name of the database containing the table.
<code>--schema-name SCHEMA</code>	Specifies the name of the schema containing the table.
<code>--table-name TABLE</code>	Specifies the name of the table containing the columns.

## Options

<code>--page PAGE</code>	Specifies the specific page in the output list, by its number. This parameter is used only if <code>page-size</code> is set. Default is the first page.
<code>--page-size PAGE_SIZE</code>	Specifies the maximum number of columns to list per output page. Default: 100.
<code>--name COLUMN_NAME</code>	Specifies the name of a specific column.
<code>--name-startswith PREFIX</code>	Specifies a prefix to filter the column names.

--tenant-id TENANT	Specifies the ID of the tenant where the database resides  If omitted, the default tenant is assumed.
-----------------------	---

## Example

```
vcli: admin> projectioncolumn list --database-name tabular --schema-name vastagoda --table-name agoda --projection-name myProj2
+-----+-----+-----+-----+-----+-----+
| Name      | Raw-field | Is-sorted | Database-name | Schema-name | Table-name | Projection-name |
+-----+-----+-----+-----+-----+-----+
| id        | string    | True      | tabular       | vastagoda   | agoda      | myProj2        |
| logtime   | timestamp[ns] | True      | tabular       | vastagoda   | agoda      | myProj2        |
| user_id   | string    | True      | tabular       | vastagoda   | agoda      | myProj2        |
| currency  | string    | True      | tabular       | vastagoda   | agoda      | myProj2        |
| session_id | string    | False     | tabular       | vastagoda   | agoda      | myProj2        |
| is_nha    | bool      | False     | tabular       | vastagoda   | agoda      | myProj2        |
| language  | string    | False     | tabular       | vastagoda   | agoda      | myProj2        |
| member_id | int64     | False     | tabular       | vastagoda   | agoda      | myProj2        |
+-----+-----+-----+-----+-----+-----+
```

### projectioncolumn show

This command shows details for a specific projection column in a VAST Database table projection.

## Usage

```
projectioncolumn show --database-name DATABASE
                     --schema-name SCHEMA
                     --table-name TABLE
                     --projection-name PROJECTION
                     --name COLUMN
                     [--tenant-id TENANT]
```

## Required Parameters

--database-name DATABASE	Specifies the name of the database containing the table.
--schema-name SCHEMA	Specifies the name of the schema containing the table.

<code>--table-name TABLE</code>	Specifies the name of the table.
<code>--projection-name PROJECTION</code>	Specifies the name of the projection in the table.
<code>--name COLUMN</code>	Specifies the name of a column in the projection.

## Options

<code>--tenant-id TENANT</code>	<p>Specifies the ID of the tenant where the database resides</p> <p>If omitted, the default tenant is assumed.</p>
---------------------------------	--

## Example

```
vcli: admin> projectioncolumn show --database-name tabular --schema-name vastagoda --table-name agoda -projection-name myProj2 --name id
```

```
+-----+-----+
| Name           | id           |
| Raw-field      | string       |
| Is-sorted      | True         |
| Database-name  | tabular      |
| Schema-name    | vastagoda    |
| Table-name     | agoda        |
| Projection-name | myProj2      |
+-----+-----+
```

# protectedpath commands

## protectedpath add-stream

This command adds a destination to a replication protected path or to a global access protected path.

### Usage - Async Replication

```
protectedpath add-stream --id ID
                          --name NAME
                          --capabilities ASYNC_REPLICATION
                          [--protection-policy-id ID]
                          [--target-exported-dir]
                          [--remote-tenant-name TENANT_NAME]
```

### Usage - Global Access

```
protectedpath add-stream --id ID
                          --name NAME
                          --capabilities STARED_GLOBAL_NAMESPACE
                          [--target-exported-dir PATH]
                          [--remote-tenant-name TENANT_NAME]
                          [--remote-target-id PEER_ID]
```

### Required Parameters

<code>--id ID</code>	Specifies the protected path by its ID.
<code>--name NAME</code>	A name for the destination.
<code>--capabilities</code> <code>ASYNC_REPLICATION STARED_GLOBAL_NAMESPACE</code>	Specifies if the destination is for replication (ASYNC_REPLICATION) or for global access (STARED_GLOBAL_NAMESPACE).

### Replication Options

<code>--protection-policy-id ID</code>	The ID of the protection policy that specifies the destination peer and other parameters for replicating to the destination, such as the replication schedule.
<code>--target-exported-dir PATH</code>	Specifies the path on the destination peer to which the protected path should replicate data.

<pre>--remote-tenant- name TENANT_NAME</pre>	<p>Specifies the name of the remote tenant on which you want to create the target directory.</p> <p>By default, the target directory is created on the default tenant.</p>
--	--

## Global Access Options

<pre>--target-exported- dir PATH</pre>	<p>Specifies the path on the destination peer to be shared for global access. This must be a directory that does not yet exist on the remote peer.</p>
<pre>--remote-tenant-name TENANT_NAME</pre>	<p>Specifies the name of the remote tenant on which you want to create the directory specified by <code>--target-exported-dir</code>.</p> <p>By default, the directory is created on the default tenant.</p>
<pre>--remote-target-id PEER_ID</pre>	<p>Specifies a destination peer for the global access path.</p> <p>Specify <code>PEER_ID</code> as an integer ID of a <i>replicationpeer</i> object (to list replication peers, run <code>replicationpeer list</code>).</p>

## Example

```
vcli: admin> protectedpath add-stream --id 6 --name vcli-stream-b-c --protection-policy-id 7
```

### protectedpath commit

This command commits a [protected path restore](#).

Before running this command, run the [protectedpath restore](#) command to restore the path to a specific snapshot, and use the [globalsnapshotclone list](#) command to verify that a global snapshot clone for the path is complete.

After running this command, restore cannot be stopped or reverted.

## Usage

```
protectedpath commit --id ID
```

## Required Parameters

<pre>--id ID</pre>	<p>Specifies the protected path for which to commit a restore.</p>
--------------------	--

# Example

```
vccli: admin> protectedpath commit --id 23
```

## protectedpath create

This command creates a protected path.

# Usage


```
protectedpath create --name NAME
                    --protection-policy-id PROTECTION_POLICY_ID
                    --source-dir SOURCE_DIR
                    --local-tenant-id ID
                    [--target-exported-dir PATH_ON_PEER]
                    [--remote-tenant-name NAME]
                    [--sync-interval SYNC_INTERVAL]
                    [--capabilities ASYNC_REPLICATION | STARED_GLOBAL_NAMESPACE | REPLICATIO
N_AND_GN | SYNC_REPLICATION]
                    [--sync-disconnect-time TIME]
                    [--lease-expiry-time TIME]
```

# Required Parameters

<code>--name NAME</code>	Sets a name for the protected path.
<code>--protection-policy-id ID</code>	<div>Specifies which protection policy to apply to the protected path.</div> <div><b>Warning</b>  After creating the protected path, it is not possible to change which policy is associated with the protected path. All changes to a protected path's snapshot schedule, replication schedule, and snapshot expiration must be done by modifying the protection policy. Those modifications affect all protected paths that use the same protection policy. To work around this limitation, create a protection policy per protected path.</div>
<code>--source-dir SOURCE-DIR</code>	<div>Specifies the path to a directory to back up. A snapshot of this directory will be taken periodically on the schedule configured in the protection policy.</div> <div>For example: <code>--source-dir /</code></div>
<code>--local-tenant-id ID</code>	Specifies to which local tenant the path belongs.



# Options

<pre>--target-exported-dir PATH_ON_PEER</pre>	<p>For asynchronous replication or global access, specify the path on the destination peer where the data should be replicated. This must be a directory that does not yet exist on the destination peer.</p> <div>  <p><b>Tip</b></p> <p>You cannot use "/" as path on peer because that always exists already. Therefore if you would like to replicate all data under the root directory, you will need to replicate this to a subdirectory. e.g. path on peer = "mirror/"</p> </div>
<pre>--remote-tenant-name NAME</pre>	<p>If <code>--target-exported-dir</code> is specified, this option specifies which tenant on the destination peer <code>--target-exported-dir</code> belongs to.</p>
<pre>--sync-interval SYNC_INTERVAL</pre>	<p>For asynchronous replication, the maximum duration gap between restore points of members in the replication group, in seconds. Guarantees that a common restore point exists between group members within the specified duration.</p> <p>Default value: 86400 seconds (1 day)</p>
<pre>--capabilities ASYNC_REPLICATION   STARED_GLOBAL_NAMESPACE   REPLICATION_AND_GN   SYNC_REPLICATION</pre>	<p>The mode or purpose of the protected path:</p> <ul style="list-style-type: none"> <li>• <code>ASYNC_REPLICATION</code>. The path is used for Asynchronous Replication</li> <li>• <code>STARED_GLOBAL_NAMESPACE</code>. The path is used for Global Access</li> <li>• <code>REPLICATION_AND_GN</code>. The path is used for Global Access and Asynchronous Replication. This configures the path for Global Access, but also captures snapshots as with Asynchronous Replication, that can be used if the Global Access connection drops on the replication group.</li> <li>• <code>SYNC_REPLICATION</code>. The path is used for Synchronous Replication.</li> </ul> <p>If <code>SYNC_REPLICATION</code> is specified, <code>--sync-disconnect-time</code> must also be specified.</p> <p>If not specified, <code>ASYNC_REPLICATION</code> is assumed.</p>
<pre>--sync-disconnect-time TIME</pre>	<p>The period of time, in seconds, after which a primary and secondary cluster, configured for synchronous replication, will revert to standalone clusters (and no longer replicate data) if communication between them is lost.</p> <p>Default value: 45 seconds</p>

<code>--lease-expiry-time TIME</code>	For global access, the duration for which data that was already requested at the destination path can be read locally from cache without the destination peer requesting it from the source peer. When the lease expires, the cache is invalidated and the next read request for the data is requested again from the source peer.
---------------------------------------	--

## Example

```
vccli: admin> protectedpath create --name stream1 --protection-policy-id 1 --source-dir /
```

### protectedpath delete

This command deletes a protected path.

## Usage

```
protectedpath delete --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies the protected path to delete by its ID.
----------------------	---

## Example

This example deletes the protected path with ID 1.

```
vccli: admin> protectedpath delete --id 6
Are you sure you want to delete the Protected Path? [y/N] y
```

### protectedpath delete-prefetch

This command is used to delete a prefetch task with various options.

## Usage

```
vccli: admin> protectedpath delete-prefetch --id ID
                                           --task-id TASK
                                           [--stop-running-prefetch]
```

## Required Parameters

<code>--id ID</code>	The Protected Path ID.
----------------------	------------------------

<code>--task-id</code>	The prefetch task ID.
------------------------	-----------------------

## Optional Parameters

<code>--stop-running-prefetch</code>	If true, stops the prefetch task (if running), in addition to deleting the record from the prefetch history.
--------------------------------------	--

## Example

This example deletes a prefetch task from the prefetch history, while stopping the prefetch task (if it is still running):

```
vcli: admin> protectedpath delete-prefetch --id 123 --task-id 456 --stop-running-prefetch
```

### protectedpath force-failover

This command forces the local cluster to become the source of replication on a group protected path without asking the current source peer. It can be used to perform an ungraceful failover in the event that the source peer becomes unavailable.

## Usage

```
protectedpath force-failover --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies the protected path by its ID
----------------------	--

## Example

```
vcli: admin> protectedpath force-failover --id 2
```

### protectedpath get-prefetch-status

This command retrieves the status of a prefetch task.

## Usage

```
vcli: admin> protectedpath get-prefetch-status --id ID
--task-id TASK
```

## Required Parameters

<code>--id ID</code>	The Protected Path ID.
<code>--task-id TASK</code>	The Prefetch task ID.

## Example

This example retrieves the status of the specified prefetch folder operation:

```
vccli: admin> protectedpath get-prefetch-status --id 123 --task-id 456
```

Paths for prefetch tasks [1] were removed.

Tenant default:

```
+-----+-----+-----+-----+-----+-----+
| Path      | Code    | Prefetch-type | Inodes-retrieved | Size-retrieved | Task-id |
+-----+-----+-----+-----+-----+-----+
| /b-rem/b1/ | SUCCESS | META_DATA_ONLY | 1                | 0              | 2       |
+-----+-----+-----+-----+-----+-----+
```

Tenant test:

```
+-----+-----+-----+-----+-----+-----+
| Path      | Code    | Prefetch-type | Inodes-retrieved | Size-retrieved | Task-id |
+-----+-----+-----+-----+-----+-----+
| /c-rem/   | SUCCESS | FULL          | 1                | 0              | 3       |
+-----+-----+-----+-----+-----+-----+
```

### protectedpath list

This command lists protected paths.

## Usage

```
protectedpath list [--protection-policy-name NAME]
                  [--state INITIAL_SYNC|INIT|INCREMENTAL_SYNC|SUSPENDED|ERROR|DETACHED]
                  [--name NAME]
                  [--progress]
```

## Options

<code>--protection-policy-name NAME</code>	Filters the list by protection policy name.
<code>--state INITIAL_SYNC INIT INCREMENTAL_SYNC SUSPENDED ERROR</code>	Filters the list by the specified state.
<code>--name NAME</code>	Filters the list by protected path name

<code>--progress</code>	Displays progress details.
-------------------------	----------------------------

## Example

```
vcli: admin> protectedpath list
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
| ID | Name | Role | State | PATH | Path On Remote | Peer-cluster-name |
| Protection-policy-name | Is-local | Bandwidth(MB/s) | Health | Aggregated Usage(GB) | Tenan
t-name | Remote-tenant-name | Replication-streams | Sync-interval |
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
| 5 | protected_cucumber | Source | Active | /plz1zgl | /plz1zgl | vast_enough
| flashy-chat | N/A | None | OK | None | default
| 138 | protected_elephant | Source | Active | /cucXN77 | /cucXN77 | vast_enough
| flashy-chat | N/A | None | OK | None | default
| 139 | protected_cheese | Source | Active | /wpAaQn7 | /wpAaQn7 | vast_enough
| flashy-chat | N/A | None | OK | None | default
| 140 | protected_banana | Source | Active | /wpAaQn7 | /wpAaQn7 | vast_enough
| flashy-chat | N/A | None | OK | None | default
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
```

## protectedpath modify

This command can be used to:

- Deactivate a [protected path](#). This pauses snapshots and replication according to the [protection policy](#) associated with the protected path.
- Activate a protected path if it was previously deactivated. This resumes snapshots and replication according to the protection policy associated with the protected path.
- Initiate a failover in an async replication scenario. This must be done from the destination peer's VMS.
- Abort a graceful failover during the first phase of the failover when the protected data is read-only on both peers.
- Change the name of a protected path.
- Change the lease expiration time of a global access protected path.

In async replication, where the protected path is mirrored on the destination peer, activation/deactivation can be done from either peer. Failover is initiated from the destination peer.

## Usage

```
protectedpath modify --id ID
                    [--name NAME]
                    [--activate]
                    [--deactivate]
                    [--modify-replication-state]
                    [--abort-modify-replication-state]
```

```

[--graceful]
[--ungraceful]
[--sync-interval SYNC_INTERVAL]
[--capabilities ASYNC_REPLICATION | STARED_GLOBAL_NAMESPACE | REPLICATIO
N_AND_GN | SYNC_REPLICATION]
[--sync-disconnect-time TIME]
[--lease-expiry-time TIME]

```

## Required Parameters

<code>--id ID</code>	Specify the protected path by its ID.
----------------------	---------------------------------------

## Options

<code>--name NAME</code>	Changes the name of the protected path.
<code>--activate</code>	Activates a protected path if previously deactivated.
<code>--deactivate</code>	Deactivates a protected path.
<code>--modify-replication-state</code>	<p>Initiates an asynchronous replication failover or synchronous turnover.</p> <p>Must be run from the destination peer and used with either <code>--graceful</code> or <code>--ungraceful</code> to specify the type of failover/turnover.</p>
<code>--abort-modify-replication-state</code>	Aborts a failover. Must be run from the destination peer. The abort operation is supported for graceful failovers during the read-only phase.
<code>--graceful</code>	Specifies failover type as <a href="#">graceful</a> . Use in addition to <code>--modify-replication-state</code> to initiate failover/turnover.
<code>--ungraceful</code>	Specifies failover type as <a href="#">ungraceful</a> . Use in addition to <code>--modify-replication-state</code> to initiate failover/turnover.
<code>--sync-interval SYNC_INTERVAL</code>	<p>The maximum duration gap between restore points of members in the replication group, in seconds. Guarantees that a common restore point exists between group members within the specified duration.</p> <p>Default value: 86400 seconds (1 day)</p>

<pre>--capabilities ASYNC_REPLICATION   STARED_GLOBAL_NAMESPACE   REPLICATION_AND_GN   SYNC_REPLICATION</pre>	<p>The mode or purpose of the protected path:</p> <ul style="list-style-type: none"> <li>• <b>ASYNC_REPLICATION.</b> The path is used for Asynchronous Replication</li> <li>• <b>STARED_GLOBAL_NAMESPACE.</b> The path is used for Global Access</li> <li>• <b>REPLICATION_AND_GN.</b> The path is used for Global Access and Asynchronous Replication. This configures the path for Global Access, but also captures snapshots as with Asynchronous Replication, that can be used if the Global Access connection drops on the replication group.</li> <li>• <b>SYNC_REPLICATION.</b> The path is used for Synchronous Replication.</li> </ul> <p>If <b>SYNC_REPLICATION</b> is specified, <code>--sync-disconnect-time</code> must also be specified.</p>
<pre>--sync-disconnect-time TIME</pre>	<p>The period of time, in seconds, after which a primary and secondary cluster, configured for synchronous replication, will revert to standalone clusters (and no longer replicate data) if communication between them is lost.</p> <p>Default value: 45 seconds</p>
<pre>--lease-expiry-time TIME</pre>	<p>For global access, the duration for which data that was already requested at the destination path can be read locally from cache without the destination peer requesting it from the source peer. When the lease expires, the cache is invalidated and the next read request for the data is requested again from the source peer.</p>

## Example

This example suspends a protected path whose ID is 1.

```
vcli: admin> protectedpath modify --id 1 --deactivate
```

This example starts a graceful failover on protected path with ID 3.

```
vcli: admin> protectedpath modify --id 3 --modify-replication-state --graceful
```

### protected path modify-member

This command modifies the capabilities for a protectedpath stream.

## Usage

```
protectedpath modify-member --id ID
                             --stream-id ID
                             --capabilities ASYNC_REPLICATION | STARED_GLOBAL_NAMESPACE | REPL
ICATION_AND_GN | SYNC_REPLICATION]
```

## Required Parameters

<code>--id ID</code>	The protected path ID.
<code>--stream-id ID</code>	The replication stream by its ID.
<code>--capabilities</code> <code>ASYNC_REPLICATION  </code> <code>STARED_GLOBAL_NAMESPACE  </code> <code>REPLICATION_AND_GN  </code> <code>SYNC_REPLICATION</code>	<p>The mode or purpose of the protected path:</p> <ul style="list-style-type: none"><li>• <code>ASYNC_REPLICATION</code>. The path is used for Asynchronous Replication</li><li>• <code>STARED_GLOBAL_NAMESPACE</code>. The path is used for Global Access</li><li>• <code>REPLICATION_AND_GN</code>. The path is used for Global Access and Asynchronous Replication. This configures the path for Global Access, but also captures snapshots as with Asynchronous Replication, that can be used if the Global Access connection drops on the replication group.</li><li>• <code>SYNC_REPLICATION</code>. The path is used for Synchronous Replication.</li></ul> <p>If <code>SYNC_REPLICATION</code> is specified, <code>--sync-disconnect-time</code> must also be specified.</p> <p>If not specified, <code>ASYNC_REPLICATION</code> is assumed.</p>

## Example

This example changes a stream to Synchronous replication.

```
vccli: admin> protectedpath modify-member --id 1 --stream-id 2 --capabilities SYNC_REPLICATION
```

### protectedpath pause

This command pauses a protected path restore in process.

## Usage

```
protectedpath pause --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies the protected path for which to pause restore.
----------------------	--



## Example

```
vccli: admin> protectedpath pause --id 3
```

### protectedpath reattach-stream

This command reattaches a replication stream to a protected path.

## Usage

```
protectedpath reattach-stream --id ID
                               --stream-id ID
```

## Required Parameters

<code>--id ID</code>	Specifies the protected path by its ID.
<code>--stream-id ID</code>	Specifies the replication stream by its ID.

## Example

```
vccli: admin> protectedpath reattach-stream --id 5 --stream-id 2
```

### protectedpath remove-stream

This command removes a replication stream from a protected path.

## Usage

```
protectedpath remove-stream --id ID --stream-id ID
```

## Required Parameters

<code>--id ID</code>	Specifies the protected path by its ID.
<code>--stream-id ID</code>	Sets the replication stream by its ID.

## Example

```
vccli: admin> protectedpath remove-stream --id 43 --stream-id 41
```

## protectedpath replicate-now

This command takes a snapshot of a configured remote protected path and replicates it to the destination peer(s) defined in the configuration of the protected path. The command enables replication on demand at any time outside of the scheduled snapshots.

## Usage

```
protected path replicate-now --id ID
                             --time-expires-local LOCAL_EXPIRATION_TIME
                             --time-expires-target TARGET_EXPIRATION_TIME
```

## Required Parameters

<code>--id ID</code>	Specifies which protected path to replicate.
<code>--time-expires-local</code> <code>LOCAL_EXPIRATION_TIME</code>	Sets the time for the local snapshot to expire.  Specify <code>LOCAL_EXPIRATION_TIME</code> in the format <code>YYYY-mm-ddTHH:MM:SS</code> .
<code>--time-expires-target</code> <code>TARGET_EXPIRATION_TIME</code>	Specify <code>TARGET_EXPIRATION_TIME</code> in the format <code>YYYY-mm-ddTHH:MM:SS</code> ,

## Example

```
vcli: admin> protectedpath replicate-now --id 12 --time-expires-local 2024-09-15T13:30:00 --time-expires-target 2024-09-16T18:00:00
```

## protectedpath restore

This command restores a protected path to a specified snapshot.

## Usage

```
protectedpath restore --id ID
                     --local-snapshot-id ID
```

## Required Parameters

<code>--id ID</code>	Specifies protected path ID
----------------------	-----------------------------

<code>--local-snapshot-id ID</code>	Specifies which snapshot to use to restore the path.
-------------------------------------	--

## Example

```
vcli: admin> protectedpath restore --id 14 --local-snapshot-id 51234
```

### protectedpath resume

This command resumes a protected path restore that was paused in process.

## Usage

```
protectedpath resume --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which protected path to resume restore for.
----------------------	---

## Example

```
vcli: admin> protectedpath resume --id 14
```

### protectedpath show

This command displays details of a specific protected path.

## Usage

```
protectedpath show --id ID
                  [--progress]
```

## Required Parameters

<code>--id ID</code>	Specifies the ID of the protected path to show.
----------------------	---

# Options

--progress	Displays progress details. Without this option, the command displays the path's configured properties, state, bandwidth and health.
------------	---

## Examples

The following example displays details of a protected path that has no replication streams:

```
vcli: admin> protectedpath show --id 37
+-----+
| ID          | 37          |
| Name        | vcli-path-without-streams |
| Role        | Standalone  |
| State       | Local       |
| PATH        | /b          |
| Path On Remote | None        |
| Peer-cluster-name |           |
| Protection-policy-name |           |
| Is-local    | N/A         |
| Bandwidth (MB/s) | None        |
| Health      | Ok          |
| Aggregated Usage (GB) | 0.0        |
| Tenant-name | default     |
| Remote-tenant-name | None        |
| Replication-streams | []          |
| Sync-interval | None        |
+-----+
```

This example shows details of a protected path that has one replication stream:

```
vcli: root> protectedpath show --id 43
+-----+
| ID          | 43          |
| Name        | vcli-path-e |
| Role        | Source      |
| State       | Active      |
| PATH        | /e          |
| Path On Remote | /e          |
| Peer-cluster-name | loopB       |
| Protection-policy-name | policyAB    |
| Is-local    | N/A         |
| Bandwidth (MB/s) | None        |
| Health      | OK          |
| Aggregated Usage (GB) | 0.0        |
| Tenant-name | default     |
| Remote-tenant-name | default     |
| Replication-streams | ['vcli-path-e'] |
| Sync-interval | 86400       |
+-----+
```

This example shows details of a protected path that has two replication streams:

```
vcli: root> protectedpath show --id 43
+-----+
| ID          | 43          |
| Name        | vcli-path-e |
| Role        | Source      |
| State       | Active      |
+-----+
```

PATH	/e
Path On Remote	/e
Peer-cluster-name	loopB
Protection-policy-name	policyAB
Is-local	N/A
Bandwidth (MB/s)	None
Health	Ok
Aggregated Usage (GB)	0.0
Tenant-name	default
Remote-tenant-name	default
Replication-streams	['vcli-stream-A-C', 'vcli-path-e']
Sync-interval	86400

This example shows the progress of a protected path:

```
vcli: admin> protectedpath show --id 17 --progress
```

ID	17
Name	__ignore_stream_9_qXPAWnS
Last Restore Point Creation Time	2023-06-22T21:44:18Z
Last Uploading Restore Point State	IN_PROGRESS
Last Uploading Restore Point Physical Size	0
Last Uploading Restore Point Logical Size	0
Eta	None
Inode Count	1
Progress	0.0

## protectedpath start-prefetch

This command is used to prefetch a folder to the cache on a cluster. The cluster must be the destination cluster for a Global Access share of a protected path on a source cluster.

## Usage

```
vcli: admin> protectedpath start-prefetch --id ID
--path PATH
--prefetch-type TYPE
```

## Required Parameters

--id ID	The Protected Path ID.
--path PATH	<p>The path (file or folder) to prefetch. Example: /test or /test/file.dat</p> <p>The path on the source cluster is fetched. If the path does not exist on the source, the command fails.</p>
--prefetch-type TYPE	<p>The type of prefetch to perform.</p> <p>Options:</p>

	<ul style="list-style-type: none"> <li>• <b>META_DATA_ONLY.</b> Prefetches only the metadata for the folder and subfolders</li> <li>• <b>FULL.</b> Prefetches the metadata and file data in the folder and subfolders</li> </ul>
--	--

## Example

This example prefetches a folder (all the files) to the cache.

```
vcli: admin> protectedpath start-prefetch --id 123 --path /test --prefetch-type FULL
```

### globalsnapshotclone stop

This command stops and removes a global snapshot clone.

## Usage

```
globalsnapshotclone stop --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which global snapshot clone to stop.
----------------------	--

## Example

```
vcli: admin> globalsnapshotclone stop --id 4
```

# protectionpolicy commands

## protectionpolicy create




This command creates a protection policy.

## Usage

```
protectionpolicy create --clone-type CLOUD_REPLICATION|LOCAL|NATIVE_REPLICATION
                        --name POLICY_NAME
                        --schedule SCHEDULE
                        --snapshot-prefix PREFIX
                        [--peer-id PEER_ID]
                        [--enable-lock]
```

## Required Parameters

<code>--clone-type</code> CLOUD_REPLICATION NATIVE_REPLICATION LOCAL	<p>Specifies what type of protection to configure on the path:</p> <ul style="list-style-type: none"><li>• CLOUD_REPLICATION. Take local snapshots and replicate them to an S3 replication peer.</li><li>• NATIVE_REPLICATION. Take local snapshots and replicate them to an async replication peer.</li><li>• LOCAL. Take snapshots on the local cluster only.</li></ul>
<code>--name POLICY_NAME</code>	<p>Specifies a name for the protection policy.</p>
<code>--schedule SCHEDULE</code>	<p>Defines the schedule for snapshots and replication.</p> <p>The schedule includes a period defined as a number of time units, a start date and time, a retention time limit for local snapshots and, for async replication, a retention time for remote snapshots.</p> <p>Specify SCHEDULE in the following format:</p> <pre>every &lt;number&gt;&lt;time units&gt; start at YYYY-MM-DD H H:MM:SS keep-local &lt;number&gt;&lt;time units&gt; keep-rem ote &lt;number&gt;&lt;time units&gt;</pre> <p>Where:</p> <ul style="list-style-type: none"><li>• &lt;time units&gt; can be any of the following:<ul style="list-style-type: none"><li>◦ s - seconds</li><li>◦ m - minutes</li></ul></li></ul>

	<ul style="list-style-type: none"> <li>◦ h - hours</li> <li>◦ d - days</li> <li>◦ W - weeks</li> <li>◦ M - months</li> <li>◦ Y - years</li> </ul> <div>  <b>Notice</b> <p>The W, M and Y options are available starting with VAST Cluster 4.6.0-SP22.</p> </div> <ul style="list-style-type: none"> <li>• <code>keep-local</code> sets the amount of time to retain each local snapshot on the cluster.</li> </ul> <div>  <b>Note</b> <p>If <code>--clone-type</code> is set to <code>CLOUD_REPLICATION</code>, then the minimum supported period is 6 hours, which can be specified as <code>6h</code>.</p> </div> <ul style="list-style-type: none"> <li>• <code>keep-remote</code> sets the amount of time to retain each snapshot on an async replication remote peer.</li> </ul> <div>  <b>Note</b> <p>S3 backups do not expire and do not have a retention period.</p> </div> <p><b>Example:</b> <code>--schedule every 90m start-at 2025-07-27 20:10:35 keep-local 10h keep-remote 7d</code></p>
<pre>--snapshot-prefix PREFIX</pre>	<p>Specifies the prefix to use in the names of snapshots.</p> <p>The name of each snapshot will be <code>&lt;prefix&gt;_&lt;timestamp&gt;</code>, where <code>&lt;prefix&gt;</code> is the prefix specified here and <code>&lt;timestamp&gt;</code> is the time the snapshot is created, in the format <code>yyyy-mm-ddTHH:MM:SS.SSSSSSzzz</code> (T denotes time and doesn't represent a value, <code>zzz</code> is the timezone, and the time is accurate</p>



	to the microsecond). For example, if the prefix is <i>dev</i> , a snapshot taken at 8:15 pm UTC on 20th November 2024 would be named <i>dev_2024-11-20T20:15:06.144783UTC</i> .
<code>--enable-lock</code>	Makes the policy indestructible. Once this setting is enabled, deleting or modifying the protection policy requires unlocking the cluster's indestructibility mechanism.

# Options

<code>--peer-id</code> <code>PEER_ID</code>	<p>Specifies the replication peer if <code>--clone-type</code> is either <code>CLOUD_REPLICATION</code> or <code>NATIVE_REPLICATION</code>.</p> <p>If <code>--clone-type</code> is <code>CLOUD_REPLICATION</code>, specify the ID of an S3 replication peer.</p> <p>If <code>--clone-type</code> is <code>NATIVE_REPLICATION</code>, specify the ID of an async replication peer.</p> <p>Specify the ID as an integer.</p>
--	--

# Example

```

vcli: admin> protectionpolicy create --schedule every 90m start at 2025-07-27 20:10:35 keep-l
ocal 10h keep-remote 10d --prefix Snapdir1 --clone-type NATIVE_REPLICATION --name protect-po
ll --peer-id 1

```

## protectionpolicy delete

This command deletes a protection policy.

# Usage

```

protectionpolicy delete --id ID

```

# Required Parameters

<code>--id ID</code>	<p>Specifies which protection policy to delete.</p> <p>To retrieve protection policy IDs, use <a href="#">protectionpolicy list</a>.</p>
----------------------	--

# Example

```

vcli: admin> protectionpolicy delete --id 2

```

Are you sure you want to delete the protection Policy? [y/N] y

## protectionpolicy list

This command lists protection policies and their details.

## Usage

protectionpolicy list

## Required Parameters

None

## Example

In this example, there is one protection policy configured to create local snapshots with no remote replication. The snapshots are taken every 20 seconds and each snapshot expires after one minute.

```
vcli: admin> protectionpolicy list
+-----+-----+
+-----+-----+-----+
+-----+-----+-----+
| ID | Name          | Schedule
| Replication Peer | Snapshot Prefix | Clone Type | Indestructible |
+-----+-----+-----+
+-----+-----+-----+
| 1  | AlwaysBackUpData | [{'every': '20s', 'start-at': '2021-02-08 09:25:24', 'keep-local':
'1m'}] | | ABD          | LOCAL      | False      |
+-----+-----+-----+
+-----+-----+-----+
+-----+-----+-----+
```

In this example, there are three async replication policies. For one of them, local snapshots are kept for ten minutes. For the other two, they are discarded after replication:

```
vcli: admin> protectionpolicy list
+-----+-----+
+-----+-----+-----+
+-----+-----+-----+
| ID | Name          | Schedule
| Replication Peer | Snapshot Prefix | Clone Type          | Indestructible |
+-----+-----+-----+
+-----+-----+-----+
+-----+-----+-----+
| 4  | Every10miN    | [{'every': '10m', 'start-at': '2021-06-03 11:30:00', 'keep-local': '10
m', 'keep-remote': '1h'}] | 28-54-gogogogo | PREF              | NATIVE_REPLICATION | False
|
| 7  | Every15Sec    | [{'every': '15s', 'start-at': '2021-06-21 08:08:17', 'keep-local': '0d',
'keep-remote': '5m'}] | 28-54-gogogogo | Every15Sec        | NATIVE_REPLICATION | False
|
| 3  | hourly       | [{'every': '1h', 'start-at': '2021-06-03 09:34:28', 'keep-local': '0d',
'keep-remote': '6h'}] | 28-54-gogogogo | hourly            | NATIVE_REPLICATION | False
|
+-----+-----+
+-----+-----+-----+
```

+-----+-----+-----+-----+

## protectionpolicy modify

This command modifies a protection policy.


## Usage




```
protectionpolicy modify --id ID
                        [--name POLICY_NAME]
                        [--peer-id PEER_ID]
                        [--schedule SCHEDULE]
                        [--snapshot-prefix SNAPSHOT_PREFIX]
                        [--enable-lock]
```

## Required Parameters

<code>--id ID</code>	Specifies the protection policy to modify.
----------------------	--

## Options

<code>--name</code> <code>POLICY_NAME</code>	Modifies the name of the protection policy.
<code>--peer-id</code> <code>PEER_ID</code>	<p>Specifies the replication peer if <code>--clone-type</code> is either <code>CLOUD_REPLICATION</code> or <code>NATIVE_REPLICATION</code>.</p> <p>If <code>--clone-type</code> is <code>CLOUD_REPLICATION</code>, specify the ID of an S3 replication peer.</p> <p>If <code>--clone-type</code> is <code>NATIVE_REPLICATION</code>, specify the ID of an async replication peer.</p> <p>Specify the ID as an integer.</p> <div><b>Note</b> You cannot add an async replication peer to an existing local snapshot policy.</div>
<code>--schedule</code> <code>SCHEDULE</code>	<p>Modifies the schedule for snapshots and replication.</p> <p>The schedule includes a period defined as a number of time units, a start date and time, a retention time limit for local snapshots and, for async replication, a retention time for remote snapshots.</p>

	<p>Specify <code>SCHEDULE</code> in the following format:</p> <pre>every &lt;number&gt;&lt;time units&gt; start at YYYY-MM-DD HH:MM:SS keep-local &lt;number&gt;&lt;time units&gt; keep-remote &lt;number&gt;&lt;time units&gt;</pre> <p>Where:</p> <ul style="list-style-type: none"> <li>• <code>&lt;time units&gt;</code> can be any of the following: <ul style="list-style-type: none"> <li>◦ s - seconds</li> <li>◦ m - minutes</li> <li>◦ h - hours</li> <li>◦ d - days</li> <li>◦ W - weeks</li> <li>◦ M - months</li> <li>◦ Y - years</li> </ul> </li> </ul> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;">  <p><b>Notice</b></p> <p>The W, M and Y options are available starting with VAST Cluster 4.6.0-SP22.</p> </div> <ul style="list-style-type: none"> <li>• <code>keep-local</code> sets the amount of time to retain each local snapshot on the cluster.</li> </ul> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;">  <p><b>Note</b></p> <p>If <code>--clone-type</code> is set to <code>CLOUD_REPLICATION</code>, then the minimum supported period is 6 hours, which can be specified as <code>6h</code>.</p> </div> <ul style="list-style-type: none"> <li>• <code>keep-remote</code> sets the amount of time to retain each snapshot on an async replication remote peer.</li> </ul> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;">  <p><b>Note</b></p> <p>S3 backups do not expire and do not have a retention period.</p> </div>
<pre>--snapshot-prefix SNAPSHOT_PREFIX</pre>	<p>Modifies the prefix to use in the names of snapshots.</p> <p>The name of each snapshot will be <code>&lt;prefix&gt;_&lt;timestamp&gt;</code>, where <code>&lt;prefix&gt;</code> is the prefix specified here</p>

	and <i>&lt;timestamp&gt;</i> is the time the snapshot is created, in the format <code>yyyy-mm-ddTHH:MM:SS.SSSSSSzzz</code> (T denotes time and doesn't represent a value, zzz is the timezone, and the time is accurate to the microsecond). For example, if the prefix is <i>dev</i> , a snapshot taken at 8:15 pm UTC on 20th November 2024 would be named <i>dev_2024-11-20T20:15:06.144783UTC</i> .
<code>--enable-lock</code>	Makes the policy indestructible. Once this setting is enabled, deleting or modifying the protection policy requires unlocking the cluster's indestructibility mechanism.

## Example

This example changes the snapshot prefix of replication policy 1 to "vast".

```
vcli: admin> protectionpolicy modify --id 1 --snapshot-prefix vast
```

## protectionpolicy show

This command displays the configuration of a specified protection policy.

# Usage

```
protectionpolicy show --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which protection policy to show, by its ID (integer).
----------------------	---

## Example

```
vcli: admin> protectionpolicy show --id 6
+-----+
+-----+
+
| ID           | 6
|
| Name         | HourlyPolicy
|
| Schedule     | [{'every': '90m', 'start-at': '2025-07-27 20:10:35', 'keep-local': '10
h', 'keep-remote': '0m'}] |
| Replication Peer | N/A
|
| Snapshot Prefix | VastData_
|
| Clone Type    | LOCAL
|
| Indestructible | False
|
+-----+
+-----+
```

+

# realm commands

## realm assign

This command assigns an object type to a user defined realm.

## Usage

```
realm assign --id ID
              --object-type OBJECT_TYPE
```

## Required Parameters

<code>--id ID</code>	Specifies a user defined realm.
<code>--object-type OBJECT_TYPE</code>	Specifies an object type to assign to the specified realm.  For possible values to specify for <code>OBJECT_TYPE</code> , see <a href="#">Managing User-Defined Permission Realms</a> .

## Example

```
vccli: admin> realm assign --id 18 -object-type qospolicy
```

## realm create

This command creates a security realm.

## Usage

```
realm create --name NAME
              [--object-types OBJECT_TYPES]
```

## Required Parameters

<code>name NAME</code>	Assigns a name to the realm.  Specify <code>NAME</code> as a string.
------------------------	--

## Options

<code>--object-types</code> <code>OBJECT_TYPES</code>	<p>Specifies a list of object types to include in the realm.</p> <p>Specify <code>OBJECT_TYPES</code> as a comma separated list.</p> <p>For possible values to specify for <code>OBJECT_TYPE</code>, see <a href="#">Managing User-Defined Permission Realms</a>.</p>
--	---

## Example

```
vcli: admin> realm create --name dataprotectionrealm --object-types snapshot,protectionpolicy,
```

### realm delete

This command deletes a user defined realm.

## Usage

```
realm delete --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which realm to delete. To retrieve a realm ID, use the <a href="#">realm list</a> command.
----------------------	--

## Example

```
vcli: admin> realm delete --id 8
```

### realm list

This command displays all user defined realms and their details.

## Usage

```
realm list
```

## Example

```
vcli: admin> realm list
+----+-----+
+-----+
```



```

+
| ID | Name          | Object-types
|
+-----+-----+
+
| 1 | replication | ['snapshot', 'protectionpolicy', 'replicationstream', 'protectedpath',
'nativereplicationremotetargets'] |
+-----+-----+
+
+

```

## realm show

This command displays details of a specific user defined realm.

## Usage

```
realm show --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which realm to display details for.
----------------------	---

## Example

```

vcli: admin> realm show --id 1
+-----+-----+
| ID      | 1 |
| Name    | end user admin |
| Object-types | ['s3policy', 'group', 'user', 'nis', 'activedirectory', 'ldap',] |
|
+-----+-----+

```

## realm unassign

This command removes an object type from a user defined realm.

## Usage

```

realm unassign --id ID
               --object-type OBJECT_TYPE

```

## Required Parameters

<code>--id ID</code>	Specifies a user defined realm.
----------------------	---------------------------------

<code>--object-type OBJECT_TYPE</code>	Specifies an object type to remove from the specified realm.
--	--

## Example

```
vcli: admin> realm unassign --id 2 --object-type tenant
```

# qospolicy commands

## qospolicy attach-user

This command assigns a [user QoS policy](#) to a user.

## Usage

```
qospolicy attach-user --id POLICY_ID
                        --name USER_NAME
                        --fqdn USER_FQDN
                        --identifier-type USERID_TYPE
                        --identifier-value USERID_VALUE
```

## Required Parameters

<code>--id POLICY_ID</code>	An ID of the QoS policy.
<code>--name USER_NAME</code>	The name of the user for which the QoS policy will provision VAST Cluster performance.
<code>--fqdn USER_FQDN</code>	The Fully Qualified Domain Name (FQDN) of the user's domain.
<code>--identifier-type</code> <code>USERID_TYPE</code>	<p>The type of a user identifier that you are going to enter in <code>--identifier-value</code> to identify the user.</p> <p>Valid values:</p> <ul style="list-style-type: none"><li>• <code>sid_str</code> for user's Security ID (SID).</li><li>• <code>uid</code> for user's POSIX UID attribute.</li><li>• <code>vid</code> for user's VAST ID.</li></ul>
<code>--identifier-value</code> <code>USERID_VALUE</code>	The user identifier. Enter an identifier of the type specified in <code>--identifier-type</code> .

## Example

```
vccli: admin> qospolicy attach-user --id 4 --name mytestuser --fqdn example.com --identifier-t
ype sid_str --identifier-value <user's SID>
```

## qospolicy create

This command creates a QoS policy.

## Usage




```
qospolicy create --name
                  [--policy-type VIEW|USER]
                  [--is-default]
                  [--tenant-id ID]
                  [--use-total-limits]
                  [--limit-by BW_IOPS|BW|IOPS]
                  [--static-total-limits STATIC_TOTAL_LIMITS]
                  [--static-limits STATIC_LIMITS]
                  [--mode STATIC|USED_CAPACITY|PROVISIONED_CAPACITY]
                  [--capacity-total-limits CAPACITY_TOTAL_LIMITS]
                  [--capacity-limits CAPACITY_LIMITS]
                  [--is-gold]
```

## Required Parameters

<code>--name</code>	Specifies a name for the policy.
---------------------	----------------------------------

## Options

<code>--policy-type VIEW USER</code>	Determines whether the QoS policy provisions performance for a view ( <code>VIEW</code> ) or for one or more users ( <code>USER</code> ).
<code>--is-default</code>	<p>When specified, the policy is used as the default user QoS policy for all users under the tenant specified in <code>--tenant-id</code>.</p> <div><b>Caution</b> Specifying this option resets the list of users assigned to this policy.</div>
<code>--tenant-id ID</code>	If the QoS policy is to be used for one or more users ( <code>--policy-type USER</code> ), specify the ID of the tenant whose users can be assigned this QoS policy.

	 <b>Tip</b> To assign users to a user QoS policy, run the <code>qospolicy attach-user</code> command.
<code>--use-total-limits</code>	If specified, enables you to set limits that cap the total amount of read, write and metadata operations (see <code>--static-total-limits</code> and <code>--capacity-total-limits</code> ).
<code>--limit-by BW_IOPS BW IOPS</code>	<p>Sets performance characteristic(s) by which to limit service:</p> <ul style="list-style-type: none"> <li>• <code>BW_IOPS</code>. Lets you set limits on both bandwidth (BW) and I/O per second (IOPS).</li> <li>• <code>BW</code>. Lets you set limits on bandwidth only.</li> </ul> <div>  <b>Note</b>          When this option is specified, the options for setting IOPS limits are not used.       </div> <ul style="list-style-type: none"> <li>• <code>IOPS</code>. Lets you set limits on IOPS only.</li> </ul> <div>  <b>Note</b>          When this option is specified, the options for setting bandwidth limits are not used.       </div>
<code>--static-total-limits</code> <code>STATIC_TOTAL_LIMITS</code>	<p>Enables and sets static QoS limits that cap the total amount of read, write and metadata operations.</p> <p>Specify <code>STATIC_LIMITS</code> as a comma-separated list of <i>key=value</i> pairs.</p> <p>The following keys can be used, depending on the <code>--limit-by</code> setting:</p> <ul style="list-style-type: none"> <li>• <code>max_bw_mbps</code>. Maximum read bandwidth to provision, in MB/s.</li> <li>• <code>max_iops</code>. Maximum read IOPS to provision.</li> <li>• <code>burst_bw_mb</code>. Burst bandwidth for read operations, in MB/s.</li> <li>• <code>burst_iops</code>. Burst IOPS for read operations.</li> <li>• <code>burst_loan_mb</code>. Maximum credit bandwidth for read operations, in MB/s.</li> <li>• <code>burst_loan_iops</code>. Maximum credit IOPS for read operations.</li> </ul>

	<p>For example: <code>min_bw_mbps=1024,max_iops=2048</code></p>
<pre>--static-limits STATIC_LIMITS</pre>	<p>Enables and sets static QoS limits.</p> <div>  <p><b>Tip</b></p> <p>Minimum limits can only be set when <code>--mode STATIC</code> is specified.</p> </div> <p>Specify <code>STATIC_LIMITS</code> as a comma-separated list of <i>key=value</i> pairs.</p> <p>The following keys can be used, depending on the <code>--limit-by</code> setting:</p> <ul style="list-style-type: none"> <li>• <code>max_reads_bw_mbps</code>. Maximum read bandwidth to provision, in MB/s.</li> <li>• <code>max_reads_iops</code>. Maximum read IOPS to provision.</li> <li>• <code>max_writes_bw_mbps</code>. Maximum write bandwidth to provision, in MB/s.</li> <li>• <code>max_writes_iops</code>. Maximum write IOPS to provision.</li> <li>• <code>burst_reads_bw_mb</code>. Burst bandwidth for read operations, in MB/s.</li> <li>• <code>burst_reads_iops</code>. Burst IOPS for read operations.</li> <li>• <code>burst_reads_loan_mb</code>. Maximum credit bandwidth for read operations, in MB/s.</li> <li>• <code>burst_reads_loan_iops</code>. Maximum credit IOPS for read operations.</li> <li>• <code>burst_writes_bw_mb</code>. Burst bandwidth for write operations, in MB/s.</li> <li>• <code>burst_writes_iops</code>. Burst IOPS for write operations.</li> <li>• <code>burst_writes_loan_mb</code>. Maximum credit bandwidth for write operations, in MB/s.</li> <li>• <code>burst_writes_loan_iops</code>. Maximum credit IOPS for write operations.</li> </ul> <p>For example:</p> <pre>max_reads_bw_mbps=1024,max_writes_iops=2048</pre>
<pre>-- mode STATIC USED_CAPACITY  PROVISIONED_CAPACITY</pre>	<p>Determines how capacity-based limits are set:</p> <ul style="list-style-type: none"> <li>• <code>STATIC</code>. No capacity-based limits are set.</li> <li>• <code>USED_CAPACITY</code>. Capacity-based limits are set based on used capacity.</li> <li>• <code>PROVISIONED_CAPACITY</code>. Capacity-based limits are set based on provisioned capacity.</li> </ul>

<pre>--capacity-total-limits CAPACITY_TOTAL_LIMITS</pre>	<p>Enables and sets QoS limits per unit of used or provisioned logical capacity, depending on the provisioning mode (see <code>--mode</code>), that cap the total amount of read, write and metadata operations.</p> <p>Specify <code>CAPACITY_TOTAL_LIMITS</code> as a comma-separated list of <i>key=value</i> pairs, where the following keys can be used, depending on the <code>--limit-by</code> setting:</p> <ul style="list-style-type: none"> <li><code>max_bw_mbps_per_gb_capacity</code>. Maximum bandwidth to provision per GB of used logical or provisioned logical capacity, depending on the provisioning mode (set by <code>--mode</code>).</li> <li><code>max_iops_per_gb_capacity</code>. Maximum IOPS to provision per GB of used logical or provisioned logical capacity, depending on the provisioning mode (set by <code>--mode</code>).</li> </ul> <p>For example: <code>max_bw_mbps_per_gb_capacity=1024,max_iops_per_gb_capacity=2048</code></p>
<pre>--capacity- limits CAPACITY_LIMITS</pre>	<p>Enables and sets QoS limits per unit of used or provisioned logical capacity, depending on the provisioning mode (see <code>--mode</code>).</p> <p>Specify <code>CAPACITY_LIMITS</code> as a comma-separated list of <i>key=value</i> pairs, where the following keys can be used, depending on the <code>--limit-by</code> setting:</p> <ul style="list-style-type: none"> <li><code>max_reads_bw_mbps_per_gb_capacity</code>. Maximum read bandwidth to provision per GB of used logical or provisioned logical capacity, depending on the provisioning mode (set by <code>--mode</code>).</li> <li><code>max_reads_iops_per_gb_capacity</code>. Maximum read IOPS to provision per GB of used logical or provisioned logical capacity, depending on the provisioning mode (set by <code>--mode</code>).</li> <li><code>max_writes_bw_mbps_per_gb_capacity</code>. Maximum write bandwidth to provision per GB of used logical or provisioned logical capacity, depending on the provisioning mode (set by <code>--mode</code>).</li> <li><code>max_writes_iops_per_gb_capacity</code>. Maximum write IOPS to provision per GB of used logical or provisioned logical capacity, depending on the provisioning mode (set by <code>--mode</code>).</li> </ul> <p>For example:</p> <p><code>max_reads_bw_mbps_per_gb_capacity=1024,max_writes_iops_per_gb_capacity=2048</code></p>
<pre>--is-gold</pre>	<p>Sets a prioritization flag for the QoS policy so that the workloads have higher priority in contention for CPU and memory resources. This option applies to view QoS policies only. For more information, see <a href="#">QoS Overview</a>.</p>

## Example

```
vccli: admin> qospolicy create --name QoSpoll --mode USED_CAPACITY
--capacity-limits max_reads_bw_mbps_per_gb_capacity=1024,max_writes_bw_mbps_per_gb_capacit
y=2048
--limit-by BW
```

### qospolicy detach-user

This command unassigns a user from a [user QoS policy](#).

# Usage

```
gospolicy detach-user --id POLICY_ID
                        --identifier-type USERID_TYPE
                        --identifier-value USERID_VALUE
```

## Required Parameters

<code>--id POLICY_ID</code>	An ID of the QoS policy from which to unassign a user.
<code>--identifier-type</code> <code>USERID_TYPE</code>	The type of a user identifier that you are going to enter in <code>--identifier-value</code> to identify the user.  Valid values: <ul style="list-style-type: none"><li>• <code>sid_str</code> for user's Security ID (SID).</li><li>• <code>uid</code> for user's POSIX UID attribute.</li><li>• <code>vid</code> for user's VAST ID.</li></ul>
<code>--identifier-value</code> <code>USERID_VALUE</code>	The user identifier. Enter an identifier of the type specified in <code>--identifier-type</code> .

## Example

```
vccli: admin> gospolicy attach-user --id 4 --identifier-type sid-str --identifier-value <user's SID>
```

### gospolicy delete

This command deletes a QoS policy.

# Usage

```
gospolicy delete --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which QoS policy to delete.
----------------------	---------------------------------------



## Example

```
vcli: admin> qospolicy delete --id 1
Are you sure you want to delete the QoS Policy? [y/N] y
```

## qospolicy list

This command displays all QoS policies and their configurations.

## Usage

qospolicy list

## Example

[illegible]

# qospolicy modify

This command modifies a QoS policy.

## Usage




```
qospolicy modify --id ID
                    [--policy-type VIEW|USER]
                    [--is-default]
                    [--tenant-id ID]
                    [--use-total-limits|--use-separate-limits]
                    [--limit-by BW_IOPS|BW|IOPS]
                    [--static-total-limits STATIC_TOTAL_LIMITS]
                    [--static-limits STATIC_LIMITS]
                    [--mode STATIC|USED_CAPACITY|PROVISIONED_CAPACITY]
                    [--capacity-total-limits CAPACITY_TOTAL_LIMITS]
                    [--capacity-limits CAPACITY_LIMITS]
                    [--is-gold|--disable-gold]
```



## Required Parameters

<code>--id ID</code>	Specifies which QoS policy to modify.
----------------------	---------------------------------------

## Options

<code>--policy-type VIEW USER</code>	Determines whether the QoS policy provisions performance for a view ( <code>VIEW</code> ) or for one or more users ( <code>USER</code> ).
<code>--is-default</code>	<div>When specified, the policy is used as the default user QoS policy for all users under the tenant specified in <code>--tenant-id</code>.</div> <div><b>Caution</b> Specifying this option resets the list of users assigned to this policy.</div>
<code>--tenant-id ID</code>	If the QoS policy is to be used for one or more users ( <code>--policy-type USER</code> ), specify the ID of the tenant whose users can be assigned this QoS policy.

	 <b>Tip</b> To assign users to a user QoS policy, run the <code>qospolicy attach-user</code> command.
<code>--use-total-limits</code>	If specified, enables you to set limits that cap the total amount of read, write and metadata operations (see <code>--static-total-limits</code> and <code>--capacity-total-limits</code> ).
<code>--use-separate-limits</code>	Disables total QoS limits.
<code>--limit-by BW_IOPS BW IOPS</code>	<p>Sets performance characteristic(s) by which to limit service:</p> <ul style="list-style-type: none"> <li>• <code>BW_IOPS</code>. Lets you set limits on both bandwidth (BW) and I/O per second (IOPS).</li> <li>• <code>BW</code>. Lets you set limits on bandwidth only.</li> </ul> <div>  <b>Note</b>            When this option is specified, the options for setting IOPS limits are not used.         </div> <ul style="list-style-type: none"> <li>• <code>IOPS</code>. Lets you set limits on IOPS only.</li> </ul> <div>  <b>Note</b>            When this option is specified, the options for setting bandwidth limits are not used.         </div>
<code>--static-total-limits</code> <code>STATIC_TOTAL_LIMITS</code>	<p>Enables and sets static QoS limits that cap the total amount of read, write and metadata operations.</p> <p>Specify <code>STATIC_LIMITS</code> as a comma-separated list of <i>key=value</i> pairs.</p> <p>The following keys can be used, depending on the <code>--limit-by</code> setting:</p> <ul style="list-style-type: none"> <li>• <code>max_bw_mbps</code>. Maximum read bandwidth to provision, in MB/s.</li> <li>• <code>max_iops</code>. Maximum read IOPS to provision.</li> <li>• <code>burst_bw_mb</code>. Burst bandwidth for read operations, in MB/s.</li> <li>• <code>burst_iops</code>. Burst IOPS for read operations.</li> </ul>

	<ul style="list-style-type: none"> <li>• <code>burst_loan_mb</code>. Maximum credit bandwidth for read operations, in MB/s.</li> <li>• <code>burst_loan_iops</code>. Maximum credit IOPS for read operations.</li> </ul> <p>For example: <code>min_bw_mbps=1024,max_iops=2048</code></p>
<pre>--static-limits STATIC_LIMITS</pre>	<p>Enables and sets static QoS limits.</p> <div>  <div> <p><b>Tip</b></p> <p>Minimum limits can only be set when <code>--mode STATIC</code> is specified.</p> </div> </div> <p>Specify <code>STATIC_LIMITS</code> as a comma-separated list of <i>key=value</i> pairs.</p> <p>The following keys can be used, depending on the <code>--limit-by</code> setting:</p> <div>  <div> <p><b>Note</b></p> <p>The limits starting with <code>min_</code> can be applied to user QoS policies only.</p> </div> </div> <ul style="list-style-type: none"> <li>• <code>max_reads_bw_mbps</code>. Maximum read bandwidth to provision, in MB/s.</li> <li>• <code>max_reads_iops</code>. Maximum read IOPS to provision.</li> <li>• <code>max_writes_bw_mbps</code>. Maximum write bandwidth to provision, in MB/s.</li> <li>• <code>max_writes_iops</code>. Maximum write IOPS to provision.</li> <li>• <code>burst_reads_bw_mb</code>. Burst bandwidth for read operations, in MB/s.</li> <li>• <code>burst_reads_iops</code>. Burst IOPS for read operations.</li> <li>• <code>burst_reads_loan_mb</code>. Maximum credit bandwidth for read operations, in MB/s.</li> <li>• <code>burst_reads_loan_iops</code>. Maximum credit IOPS for read operations.</li> <li>• <code>burst_writes_bw_mb</code>. Burst bandwidth for write operations, in MB/s.</li> <li>• <code>burst_writes_iops</code>. Burst IOPS for write operations.</li> <li>• <code>burst_writes_loan_mb</code>. Maximum credit bandwidth for write operations, in MB/s.</li> <li>• <code>burst_writes_loan_iops</code>. Maximum credit IOPS for write operations.</li> </ul> <p>For example:</p> <pre>max_reads_bw_mbps=1024,max_writes_iops=2048</pre>

<pre>-- mode STATIC USED_CAPACITY  PROVISIONED_CAPACITY</pre>	<p>Determines how capacity-based limits are set:</p> <ul style="list-style-type: none"> <li>• <b>STATIC.</b> No capacity-based limits are set.</li> <li>• <b>USED_CAPACITY.</b> Capacity-based limits are set based on used capacity.</li> <li>• <b>PROVISIONED_CAPACITY.</b> Capacity-based limits are set based on provisioned capacity.</li> </ul>
<pre>--capacity-total-limits CAPACITY_TOTAL_LIMITS</pre>	<p>Enables and sets QoS limits per unit of used or provisioned logical capacity, depending on the provisioning mode (see <code>--mode</code>), that cap the total amount of read, write and metadata operations.</p> <p>Specify <code>CAPACITY_TOTAL_LIMITS</code> as a comma-separated list of <i>key=value</i> pairs, where the following keys can be used, depending on the <code>--limit-by</code> setting:</p> <ul style="list-style-type: none"> <li>• <code>max_bw_mbps_per_gb_capacity</code>. Maximum bandwidth to provision per GB of used logical or provisioned logical capacity, depending on the provisioning mode (set by <code>--mode</code>).</li> <li>• <code>max_iops_per_gb_capacity</code>. Maximum IOPS to provision per GB of used logical or provisioned logical capacity, depending on the provisioning mode (set by <code>--mode</code>).</li> </ul> <p>For example: <code>max_bw_mbps_per_gb_capacity=1024,max_iops_per_gb_capacity=2048</code></p>
<pre>--capacity- limits CAPACITY_LIMITS</pre>	<p>Enables and sets QoS limits per unit of used or provisioned logical capacity, depending on the provisioning mode (see <code>--mode</code>).</p> <p>Specify <code>CAPACITY_LIMITS</code> as a comma-separated list of <i>key=value</i> pairs, where the following keys can be used, depending on the <code>--limit-by</code> setting:</p> <ul style="list-style-type: none"> <li>• <code>max_reads_bw_mbps_per_gb_capacity</code>. Maximum read bandwidth to provision per GB of used logical or provisioned logical capacity, depending on the provisioning mode (set by <code>--mode</code>).</li> <li>• <code>max_reads_iops_per_gb_capacity</code>. Maximum read IOPS to provision per GB of used logical or provisioned logical capacity, depending on the provisioning mode (set by <code>--mode</code>).</li> <li>• <code>max_writes_bw_mbps_per_gb_capacity</code>. Maximum write bandwidth to provision per GB of used logical or provisioned logical capacity, depending on the provisioning mode (set by <code>--mode</code>).</li> <li>• <code>max_writes_iops_per_gb_capacity</code>. Maximum write IOPS to provision per GB of used logical or provisioned logical capacity, depending on the provisioning mode (set by <code>--mode</code>).</li> </ul> <p>For example:</p> <p><code>max_reads_bw_mbps_per_gb_capacity=1024,max_writes_iops_per_gb_capacity=2048</code></p>
<pre>--is-gold</pre>	<p>Sets a prioritization flag for the QoS policy so that the workloads have higher priority in contention for CPU and memory resources. This option applies to view QoS policies only. For more information, see <a href="#">QoS Overview</a>.</p>
<pre>--disable-gold</pre>	<p>Removes the prioritization flag from the QoS policy.</p>

# Example

```
vccli: admin> qospolicy modify --id 3 --mode STATIC --limit-by BW_IOPS
--static-limits max_reads_bw_mbps=1024,max_reads_iops=1024,max_writes_iops=2048
```

## qospolicy show

This command displays details of a specific QoS policy.

# Usage

```
qospolicy show --id ID
```

# Required Parameters

--id ID	Specifies which QoS policy to display.
---------	--

# Example

```
vccli: admin> qospolicy show --id 2
+-----+
+-----+-----+
+
+ ID                | 2
+
+ Name              | qos_capacity
+
+ Mode              | PROVISIONED_CAPACITY
+
+ Static-limits     | {'burst_reads_bw_mb': 0, 'burst_reads_iops': 0, 'burst_reads_loan_iop
s': 0, 'burst_reads_loan_mb': 0,
+                        |
+                        | 'burst_writes_bw_mb': 0, 'burst_writes_iops': 0, 'burst_writes_loan_iop
s': 0, 'burst_writes_loan_mb': 0,
+                        |
+                        | 'max_reads_bw_mbps': 0, 'max_reads_iops': 0, 'max_writes_bw_mbps': 0,
'max_writes_iops': 0, 'min_reads_bw_mbps': 0,
+                        |
+                        | 'min_reads_iops': 0, 'min_writes_bw_mbps': 0, 'min_writes_iops': 0}
+
+ Capacity-limits   | {'max_reads_bw_mbps_per_gb_capacity': 0, 'max_reads_iops_per_gb_capacit
y': 150, 'max_writes_bw_mbps_per_gb_capacity':
+                        |
+                        | 0, 'max_writes_iops_per_gb_capacity': 150}
+
+ Limit-by          | IOPS
+
+ Policy-type       | VIEW
+
+ Attached-users    | []
+
+ Tenant-name       | None
+
+ Is-default        | False
+-----+-----+
+-----+
+
```

# quota commands

## quota create

This command creates a quota.

## Usage

```
quota create --name NAME
              --path PATH
              [--grace-period GRACE-PERIOD]
              [--soft-limit SOFT-LIMIT]
              [--hard-limit HARD-LIMIT]
              [--create-dir]
              [--hard-limit-inodes HARD-LIMIT-INODES]
              [--soft-limit-inodes SOFT-LIMIT-INODES]
              [--is-user-quota]
              [--enable-email-providers]
              [--disable-email-providers]
              [--default-user-quota DEFAULT_USER_QUOTA]
              [--default-group-quota DEFAULT_GROUP_QUOTA]
```

## Required Parameters

<code>--name</code> NAME	Specifies the name of the quota.
<code>--path</code> PATH	<p>Specifies a path to a directory in the element store to which the quota applies.</p> <p>The quota applies to the entire directory, including all subdirectories. If a quota configured on a subdirectory is bigger than the quota on its parent directory, the more restrictive quota applies.</p> <p>You can specify a non existent directory if you add the <code>--create-dir</code> option to create the directory.</p>

## Options

<code>--grace-period</code> GRACE-PERIOD	<p>Triggers an alarm and blocks write operations to the directory if the storage usage continues to exceed the soft specified time period.</p> <p>If no grace period is set, the directory is only blocked if and when usage reaches the hard limit.</p> <p>Specify GRACE_PERIOD in the format: [DD] [HH:[MM:]]ss or as an integer followed by d for days, h for hours, minutes, or s for seconds. Examples:</p> <ul style="list-style-type: none"><li>To specify 30 days, 20 hours, 15 minutes and 10 seconds: <code>--grace-period 30 20:15:10</code>.</li><li>To specify 18 hours: <code>--grace-period 18:00</code>.</li></ul>
---	--

	<ul style="list-style-type: none"> <li>To specify 7 days: <code>--grace-period 7d</code></li> </ul>
<code>--soft-limit SOFT-LIMIT</code>	<p>Sets a storage usage soft limit. Warnings of exceeding the quota are issued when this limit is reached.</p> <p>If not specified, no soft limit is applied.</p>
<code>--hard-limit HARD-LIMIT</code>	<p>Sets a storage usage limit. No writes are allowed beyond this limit.</p> <p>When the hard limit is reached, the <code>HARD_EXCEEDED</code> alarm is triggered.</p> <p>The value must be a complete integer and must be specified with a unit of measurement. Do not insert a space between the value and the unit of measurements. Valid units are:</p> <ul style="list-style-type: none"> <li>Base 10: <i>KB, MB, GB, TB, PB, EB</i>,</li> <li>Base 2: <i>KiB, MiB, GiB, TiB, PiB, EiB</i></li> </ul> <p>The units are case-insensitive. For example: <code>4gb</code> is valid.</p> <p>If not specified, no hard limit is applied.</p>
<code>--create-dir</code>	<p>Creates the directory if the directory does not exist.</p> <p>Required if the directory doesn't exist.</p>
<code>--hard-limit-inodes HARD-LIMIT-INODES</code>	<p>Sets a limit on the number of directories and unique files under the path. No writes are allowed beyond this limit with multiple hardlinks is counted only once.</p>
<code>--soft-limit-inodes SOFT-LIMIT-INODES</code>	<p>Sets a soft limit on the number of directories and unique files under the path. Warnings of exceeding the quota are issued when the limit is reached. A file with multiple hardlinks is counted only once.</p>
<code>--is-user-quota</code>	<p>Enables the ability to configure user and/or group quotas on the quota directory,</p>
<code>--enable-email-providers</code>	<p>Relevant for user quotas, enables querying of providers for user email addresses used to send email notifications when they exceed user quotas. (Enabled by default.)</p>
<code>--disable-email-providers</code>	<p>Relevant for user quotas, disables querying of providers for user addresses used to send email notifications to users when they exceed user quotas.</p>
<code>--default-user-quota DEFAULT_USER_QUOTA</code>	<p>Specifies the configuration of a default user quota. If configured, the default user quota is applied to users without individual quotas.</p>



	<p>For example: <code>--default-user-quota 'soft_limit=4,hard_limit=20,soft_limit_inodes=6,hard_limit_inodes=9,grace_period=0</code></p>
<code>--default-group-quota DEFAULT_GROUP_QUOTA</code>	<p>Specifies the configuration of a default group quota. If configured, the default group quota is applied to groups w individual quotas.</p> <p>For example: <code>--default-group-quota 'soft_limit=4,hard_limit=20,soft_limit_inodes=6,hard_limit_inodes=9,grace_period=0</code></p>

## Example

```

vcli: admin> quota create --name quotal --path /dev --grace-period 30 20:15:10 --soft-limit 1
tb --hard-limit 2tb --create-dir --hard-limit-inodes 5000 --soft-limit-inodes 4800

```

### quota delete

This command deletes a quota .

## Usage

```

quota delete --id ID

```

## Required Parameters

<code>--id ID</code>	Specifies which quota to delete.
----------------------	----------------------------------

## Example

```

vcli: admin> quota delete --id 1

```

### quota list

This command displays all quotas and their details.

## Usage

```

quota list

```

## Example

```

vcli: admin> quota list
+---+-----+-----+-----+-----+-----+-----+-----+

```

ID	Name	State	Path	Grace-period	Soft-limit (TB)	Hard-limit (TB)	Used-Effective-Capacity(TB)	Soft limit Files/Directories	Hard limit Files/Directories	Used Files/Directories	Grace Period Expiration	Is-user-quota	Enable-email-providers
1	quota1	OK	/dev	30 00:00:00	1.0000	2.0000	0.0000	4800	5000	1			
3	quota2	OK	/whatever	None	None	None	0.0000	None	None	2			
4	quota3	OK	/whatever/other	00:08:00	1.0000	2.0000	0.0000	None	None	1			

quota modify

This command modifies a quota.

Usage

```
quota modify --id ID
               [--name NAME]
               [--grace-period GRACE-PERIOD]
               [--soft-limit SOFT-LIMIT]
               [--hard-limit HARD-LIMIT]
               [--hard-limit-inodes HARD-LIMIT-INODES]
               [--soft-limit-inodes SOFT-LIMIT-INODES]
               [--enable-email-providers]
               [--disable-email-providers]
               [--default-user-quota DEFAULT_USER_QUOTA]
               [--default-group-quota DEFAULT_GROUP_QUOTA]
```

Required Parameters

--id ID	Specifies which quota to modify.
---------	----------------------------------

Options

--name NAME	Changes the name of the quota.
--grace-period GRACE-PERIOD	Sets or modifies a grace period. If the storage usage continues to exceed the soft limit for the period of time set grace period, an alarm is triggered and write operations to the directory are blocked.

	<p>If no grace period is set, the directory is only blocked if and when usage reaches the hard limit.</p> <p>Specify <code>GRACE_PERIOD</code> in the format: <code>[DD] [HH: [MM: ] ]ss</code> or as an integer followed by <code>d</code> for days, <code>h</code> for hours, <code>m</code> for minutes, or <code>s</code> for seconds. Examples:</p> <ul style="list-style-type: none"> <li>To specify 30 days, 20 hours, 15 minutes and 10 seconds: <code>--grace-period 30 20:15:10</code>.</li> <li>To specify 18 hours: <code>--grace-period 18:00</code>.</li> <li>To specify 7 days: <code>--grace-period 7d</code></li> </ul>
<code>--soft-limit SOFT-LIMIT</code>	<p>Sets or modifies a storage usage soft limit. Warnings of exceeding the quota are issued when this limit is reached.</p> <p>If not specified, no soft limit is applied.</p>
<code>--hard-limit HARD-LIMIT</code>	<p>Sets or modifies a storage usage limit. No writes are allowed beyond this limit.</p> <p>When the hard limit is reached, the <code>HARD_EXCEEDED</code> alarm is triggered.</p> <p>The value must be a complete integer and must be specified with a unit of measurement. Do not insert a space between the value and the unit of measurements. Valid units are:</p> <ul style="list-style-type: none"> <li>Base 10: <i>KB, MB, GB, TB, PB, EB</i>,</li> <li>Base 2: <i>KiB, MiB, GiB, TiB, PiB, EiB</i></li> </ul> <p>The units are case-insensitive. For example: <code>4gb</code> is valid.</p> <p>If not specified, no hard limit is applied.</p>
<code>--hard-limit-inodes HARD-LIMIT-INODES</code>	<p>Sets or modifies a limit on the number of directories and unique files under the path. No writes are allowed beyond the limit. A file with multiple hardlinks is counted only once.</p>
<code>--soft-limit-inodes SOFT-LIMIT-INODES</code>	<p>Sets or modifies a soft limit on the number of directories and unique files under the path. Warnings of exceeding the limit are issued when the limit is reached. A file with multiple hardlinks is counted only once.</p>
<code>--enable-email-providers</code>	<p>Relevant for user quotas, enables querying of providers for user email addresses used to send email notifications when they exceed user quotas.</p>
<code>--disable-email-providers</code>	<p>Relevant for user quotas, disables querying of providers for user addresses used to send email notifications to users when they exceed user quotas.</p>
<code>--default-user-quota DEFAULT_USER_QUOTA</code>	<p>Specifies the configuration of a default user quota. If configured, the default user quota is applied to users without individual quotas.</p> <p>For example: <code>--default-user-quota</code></p>

	'soft_limit=4,hard_limit=20,soft_limit_inodes=6,hard_limit_inodes=9,grace_period=0
--default-group-quota DEFAULT_GROUP_QUOTA	Specifies the configuration of a default group quota. If configured, the default group quota is applied to groups without individual quotas.  For example: --default-group-quota 'soft_limit=4,hard_limit=20,soft_limit_inodes=6,hard_limit_inodes=9,grace_period=0

## Example

```
vcli: admin> quota modify --id 4 --grace-period 8h
Are you sure you want to modify the quota? [y/N] y
```

### quota reset-grace-period

This command resets the quota grace period.

## Usage

```
quota reset-grace-period --id ID
```

## Required Parameters

--id ID	Specify the ID of the quota for which to reset the grace period.
---------	--

## Example

```
vcli: admin> quota reset-grace-period --id 1
```

### quota show

This command displays details of a specific quota.

## Usage

```
quota show --id ID
           [--user-rules]
```

## Required Parameters

<code>--id ID</code>	Specifies which quota to display.
<code>--user-rules</code>	Displays the quota's user rules.

## Example

```
vccli: admin> quota show --id 1
```

```
+-----+-----+
| ID           | 1           |
| Name         | quota1      |
| Pretty-state | OK          |
| Sync-state   | SYNCHRONIZED |
| Path         | /dev        |
| Grace-period | 30 00:00:00 |
| Soft-limit   | 1.0000      |
| Hard-limit   | 2.0000      |
| Used-Capacity | 0.0000      |
| Soft limit Files/Directories | 4800      |
| Hard limit Files/Directories | 5000      |
| Used Files/Directories | 1          |
+-----+-----+
```

# replicationpeer commands

## replicationpeer create

This command creates a replication peer.

## Usage

```
replicationpeer create --name NAME
                        --remote-leading-vip REMOTE_LEADING_VIP
                        --local-vip-pool-id LOCAL_VIP_POOL_ID
                        --secure-mode NONE|SECURE
                        [--mss MSS]
[
```

## Required Parameters

<code>--name NAME</code>	Specifies the name of the replication peer.
<code>--remote-leading-vip REMOTE_LEADING_VIP</code>	Specifies any one of the VIPs in the remote peer's replication <a href="#">virtual IP pool</a> to use as the remote leading virtual IP. The remote leading VIP is used to establish an initial connection between the peers. Once the connection is established, the peers share their external network topology and form multiple connections between the virtual IPs.
<code>--local-vip-pool-id LOCAL_VIP_POOL_ID</code>	<p>Specifies the ID of the replication virtual IP pool on the local cluster.</p> <p>To create the replication virtual IP pool, use <a href="#">vipool create</a> and specify <code>--role REPLICATION</code>.</p>
<code>--secure-mode NONE SECURE</code>	<p>Set the secure mode for the replication peer configuration:</p> <ul style="list-style-type: none"><li><code>SECURE</code>. Replication to this peer will be encrypted over the wire with mTLS.</li></ul> <p>Secure mode requires a certificate, key and root certificate to be <a href="#">uploaded to VMS</a> for mTLS encryption.</p> <ul style="list-style-type: none"><li><code>NONE</code>. Replication to this peer will not be encrypted over the wire.</li></ul> <div><h3>Caution</h3><p>This setting cannot be changed after creating the replication peer.</p></div>

## Options

<code>--mss MSS</code>	Maximum segment size (MSS), in bytes, that the peer can receive in a single TCP segment.
------------------------	--

## Example

```
vccli: admin> replicationpeer create --name vastnativebackup --remote-leading-vip 198.51.100.200 --local-vip-pool-id 3
```

### replicationpeer delete

This command deletes an async replication peer.

## Usage

```
replicationpeer delete --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which replication peer to delete.
----------------------	---

## Example

```
vccli: admin> replicationpeer delete --id 1
```

### replicationpeer list

This command displays all async replication peers and their details.

## Usage

```
replicationpeer list
```

## Example

```
vccli: admin> replicationpeer list
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
| ID | Name of native replication peer configuration | State      | Remote-Leading-VIP | Loca
l-VIP-Pool-ID | Remote-version | Last-heart-beat      | Remote-Space-Left | Remote-Peer-Name
| Health | Mss   | Remote-VIP-Range      | Secure-mode |
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
```

```

+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | main-remote-go | CONNECTED | 172.16.10.10 | 4 |
| 3.6.0.71 | 2021-06-28T08:58:27Z | 657394355548252 | vast_remote | OK | 140 |
0 | 198.168.100.200 - 198.168.100.203 | NONE |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+

```

## replicationpeer modify

This command modifies a replication peer.

## Usage

```

replicationpeer modify --id ID
                        [--name NAME]
                        [--remote-leading-vip REMOTE_LEADING_VIP]
                        [--mss MSS]

```

## Required Parameters

<code>--id ID</code>	Specifies which replication peer to modify.
----------------------	---

## Options

<code>--name NAME</code>	Specifies the name of the replication peer.
<code>--remote-leading-vip REMOTE_LEADING_VIP</code>	A virtual IP in the remote peer's replication <a href="#">virtual IP pool</a> to use as the leading virtual IP. This needs to be updated if the replication virtual IP pool on the remote peer was changed to an IP range that does not overlap with the previous IP range.
<code>--mss MSS</code>	Maximum segment size (MSS), in bytes, that the peer can receive in a single TCP segment.

## Example

```
vcli: admin> replicationpeer modify --id --remote-leading-vip 198.168.100.200
```

## replicationpeer show

This command displays details of an async replication peer.



# Usage

```
replicationpeer show --id ID
```

## Required Parameters

--id ID	Specifies which replication peer to display.
---------	--

## Example

```
vcli: admin> replicationpeer show --id 10
+-----+-----+
| ID | 10 |
| Name of native replication peer configuration | assertive-gibbon |
| State | CONNECTED |
| Remote-Leading-VIP | 198.168.100.200 |
| Local-VIP-Pool-ID | 3 |
| Remote-version | 4.6.0 |
| Last-heart-beat | 2023-03-15T19:05:51Z |
| Remote-Space-Left | 1126135934703643 |
| Remote-Peer-Name | vasterthanever |
| Health | OK |
| Mss | 1400 |
| Remote-VIP-Range | 198.168.100.200 - 198.168.100.203 |
| Secure-mode | NONE |
+-----+-----+
```

# replicationstream commands

## replicationstream list

This command displays all replication streams and their details.

## Usage

```
replicationstream list
    [--page PAGE]
    [--page-size PAGE_SIZE]
    [--state STATE]
    [--name NAME]
    [--order-by-priority-number asc|desc]
```

## Options

<code>--page PAGE</code>	Shows specified page of results only.  Specify <code>PAGE</code> as an integer.  Use <code>--page-size</code> to configure number of results per page.
<code>--page-size PAGE_SIZE</code>	Sets number of output results per page.  Specify <code>PAGE_SIZE</code> as an integer.
<code>--state STATE</code>	Filters the list by state.  Specify <code>STATE</code> as a string value.  For example, enter <code>--state Active</code> to display only active streams.
<code>--order-by-priority-number asc desc</code>	Orders the results by replication QoS priority number. Possible values: <ul style="list-style-type: none"><li>• <code>asc</code>. Lists results in ascending order of replication priority.</li><li>• <code>desc</code>. Lists results in descending order of replication priority</li></ul>

## Example

This example lists all active replication streams.

```
vcli: admin> replicationstream list --state Active
+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+
```

ID	Name	Role	State	Source-dir
Protected-path-id	Bandwidth(MB/s)	Remote-tenant-name	Priority-score	Priority-number
Is-manual-priority-score				
5479	S3 replication path 448	Destination	Active	/s3_replication/sources/bland
5478	None	mgmt	0.0	3
False				
5475	S3 replication path 5475	Source	Active	/s3_replication/targets/beefy
5474	0.000	mgmt	0.756	5
False				
5476	VMS configuration path 447	Destination	Active	/vmsmgmt/replicated_configurati
on/miaow   5477	None	mgmt	0.0	2
False				
5474	VMS configuration path 5474	Source	Active	/vmsmgmt/replicated_configurati
on/moo   5473	0.000	mgmt	0.706	4
False				
5487	rep-ute	Destination	Active	/a
5486	None	rep-ute	0.0	1
False				

## replicationstream modify

This command modifies the QoS priority of a replication stream. By default, the relative priority of replication streams is set automatically. It is possible to set a manual priority score.

## Usage

```
replicationstream modify --id ID
                        [--priority-score SCORE],
                        [--auto-calculate-priority-score]
```

## Required Parameters

--id ID	Specifies which replication stream to modify.
---------	---

## Options

--priority-score SCORE	<p>Sets a score to manually adjust stream's priority for replication jobs. A lower score means a higher priority.</p> <p>Specify SCORE as a float value.</p> <p>For example, --priority-score 2.5</p>
--auto-calculate-	Resets priority score to be calculated automatically.

priority-score	
----------------	--

## Example

This example resets priority score of a replication stream to be automatically calculated.

```
vccli: admin> replicationstream modify --id 23 --auto-calculate-priority-score
```

### replicationstream show

This command displays details of a specific replication stream.

## Usage

```
replicationstream show --id ID
```

## Required Parameters

--id ID	Specifies which replication stream to display.
---------	--

## Example

This example shows a (source) stream waiting for a standby:

```
vccli: admin> replicationstream show --id 48
```

+-----+-----+		
ID	48	
Name	vcli-stream-A-C	
Role	Source	
State	Waiting for a standby stream	
Source-dir	/e	
Protected-path-id	43	
Bandwidth (MB/s)	0.000	
Remote-tenant-name	default	
Priority-score	1.967	
Priority-number	14	
Is-manual-priority-score	False	
+-----+-----+		

# restorepoint commands

## restorepoint list

This command displays replication restore points. Restore points are created for protected paths on which either S3 replication or native replication is configured.

## Usage

```
replicationrestorepoint list
```

## Example

```
vccli: admin> restorepoint list
```

ID	Name	State	Bandwidth(MB/s)	Physical Size(TB)	Logical Size(TB)	Creation Time	Target Name	Stream Name
274226	Rep_path1 (point 481)	COMPLETE	0	96	0			
2021-06-28 08:20:00+00:00	Main-to-remote	Rep_path1						
274443	Rep_path1 (point 482)	COMPLETE	0	96	0			
2021-06-28 08:30:00+00:00	Main-to-remote	Rep_path1						
274685	Rep_path1 (point 483)	COMPLETE	0	96	0			
2021-06-28 08:40:00+00:00	Main-to-remote	Rep_path1						
274921	Rep_path1 (point 484)	COMPLETE	0	96	0			
2021-06-28 08:50:00+00:00	Main-to-remote	Rep_path1						
275133	Rep_path1 (point 485)	COMPLETE	0	96	0			
2021-06-28 09:00:00+00:00	Main-to-remote	Rep_path1						
275361	Rep_path1 (point 486)	COMPLETE	0	96	0			
2021-06-28 09:10:00+00:00	Main-to-remote	Rep_path1						
275459	Dir4 (point 18929)	COMPLETE	0	0	0			
2021-06-28 09:14:02+00:00	Main-to-remote	Dir4						
275463	Dir4 (point 18930)	COMPLETE	0	0	0			
2021-06-28 09:14:32+00:00	Main-to-remote	Dir4						
275477	Dir4 (point 18931)	COMPLETE	0	0	0			
2021-06-28 09:15:02+00:00	Main-to-remote	Dir4						
275482	Dir4 (point 18932)	COMPLETE	0	0	0			
2021-06-28 09:15:17+00:00	Main-to-remote	Dir4						
275494	Dir4 (point 18933)	COMPLETE	0	0	0			
2021-06-28 09:15:47+00:00	Main-to-remote	Dir4						
275502	Dir4 (point 18934)	COMPLETE	0	0	0			
2021-06-28 09:16:02+00:00	Main-to-remote	Dir4						
275509	Dir4 (point 18935)	COMPLETE	0	0	0			
2021-06-28 09:16:32+00:00	Main-to-remote	Dir4						
275523	Dir4 (point 18936)	COMPLETE	0	0	0			
2021-06-28 09:17:02+00:00	Main-to-remote	Dir4						
275525	Dir4 (point 18937)	COMPLETE	0	0	0			
2021-06-28 09:17:32+00:00	Main-to-remote	Dir4						
275548	Dir4 (point 18938)	COMPLETE	0	0	0			
2021-06-28 09:17:47+00:00	Main-to-remote	Dir4						
275556	Dir4 (point 18939)	COMPLETE	0	0	0			
2021-06-28 09:18:17+00:00	Main-to-remote	Dir4						
275563	Dir4 (point 18940)	COMPLETE	0	0	0			
2021-06-28 09:18:47+00:00	Main-to-remote	Dir4						
275577	Dir4 (point 18941)	COMPLETE	0	0	0			
2021-06-28 09:19:17+00:00	Main-to-remote	Dir4						
275586	Dir4 (point 18942)	IN_PROGRESS	0	0	0			

```
| 2021-06-28 09:19:32+00:00 | Main-to-remote | Dir4 |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

## restorepoint show

This command displays details of a specified native/s3 replication restore point.

## Usage

```
restorepoint show --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies by ID which restore point to show.
----------------------	--

## Example

```
vcli: admin> restorepoint show --id 10
+-----+-----+-----+-----+
| ID      | 10      |
| Name    | stream-comet-2020-07-13-144234-921633 (point 10) |
| State   | COMPLETE |
| Bandwidth | 0.000   |
| Physical Size | 0.000   |
| Logical Size | 0.000   |
| Creation Time | 2020-07-13 15:35:40 |
| Target Name | target-comet-2020-07-13-144234-921633 |
| Stream Name | stream-comet-2020-07-13-144234-921633 |
+-----+-----+-----+-----+
```

# role commands

## role assign

This command assigns a permission and/or LDAP groups to a role. To add multiple permissions to a role, run the command once for each permission.



### Tip

Use the VAST Web UI to see which permissions are assigned to a role.

Go to Roles tab of the Administrators page, and choose the Edit option from the Actions menu for the role. The Update Roles dialog shows which permissions are currently assigned to the role.

## Usage

```
role assign --id ID [--realm REALM | {--object-type OBJECT_TYPE --object-id OBJECT_ID}]
               [--permissions create|view|edit|delete]
               [--ldap-groups GROUPS]
               [--tenant-ids IDs]
```

## Required Parameters

<code>--id ID</code>	Specifies the role by its ID.
----------------------	-------------------------------

## Options

<code>--realm REALM</code>	<p>Specify a realm of VMS objects. Possible values:</p> <ul style="list-style-type: none"><li>• <code>events</code>. This realm includes alarms, events, event definitions and global event definition settings.</li><li>• <code>hardware</code>. This realm includes the cluster object and all infrastructure components.</li><li>• <code>logical</code>. This realm includes virtual IPs for network access, DNS service, Element Store views for protocol access, directory and user quotas, data protection features except for indestructibility, and S3 life cycle rules.</li><li>• <code>monitoring</code>. This realm includes analytics reports, capacity usage estimations, data flow analytics.</li><li>• <code>security</code>. This realm includes users and groups for data client access, authentication providers, VMS Role Based Access Control (RBAC), indestructibility for snapshots and protection policies, S3 identity policies, and VAST Data Support tunnels for remote</li></ul>
----------------------------	---

	<p>support access.</p> <ul style="list-style-type: none"> <li>• <code>settings</code>. This realm includes VMS settings.</li> <li>• <code>support</code>. This realm includes Call Home configuration, support bundles, licenses, envs, and modules.</li> </ul>
<code>--object-type OBJECT</code>	<p>Use this parameter together with <code>--object-id</code> to specify an object. In this case, the command will grant the role permission to access a specific object.</p> <p>Examples of objects are:</p> <ul style="list-style-type: none"> <li>• <code>cluster</code></li> <li>• <code>cnode</code></li> <li>• <code>dnode</code></li> <li>• <code>dbox</code></li> <li>• <code>cbox</code></li> <li>• <code>view</code></li> <li>• <code>viewpolicy</code></li> <li>• <code>quota</code></li> <li>• <code>vippool</code></li> <li>• <code>eventdefinition</code></li> <li>• <code>ldap</code></li> </ul> <p>For example, if you want to grant permission on a given view, you would specify <code>--object-type view</code> and then provide the view's view ID as <code>--object-id</code>.</p>
<code>--object-id OBJECT_ID</code>	<p>Specify an object ID to assign permission to access a specific object.</p> <p>For example: <code>--object-id 3</code></p>
<code>--permissions create view edit delete</code>	<p>Include this parameter to specify a specific type of permission. Omit this parameter to grant all types.</p>
<code>--ldap-groups GROUPS</code>	<p>Specifies one or more groups to associate the group(s) with the role. Users who belong to groups that are associated with the role will be able to log into VMS using their LDAP user name and password. They will be authorized based on the role(s) associated with their group. Each group can be any group on any connected LDAP-based provider, including Active Directory. Groups can be associated with multiple roles and vice versa.</p>



<code>--tenant-ids IDs</code>	<p>Determines the tenant(s) for the role.</p> <p>You can specify one tenant ID or a comma-separated list of tenant IDs.</p>
-------------------------------	---

## Example

This example assigns to role 2 create permission for the logical realm on tenant 2:

```
vcli: admin> role assign --id 2 --realm logical --permissions create --tenant-ids 2
```

### role create

This command creates a role.

## Usage

```
role create --name NAME
            [--ldap-groups GROUPS]
            [--tenant-ids IDs]
```

## Required Parameters

<code>--name NAME</code>	Specifies the name of the role.
--------------------------	---------------------------------

## Options

<code>--ldap-groups GROUPS</code>	Specifies one or more groups to associate the group(s) with the role. Users who belong to groups that are associated with the role will be able to log into VMS using their LDAP user name and password. They will be authorized based on the role(s) associated with their group. Each group can be any group on any connected LDAP-based provider, including Active Directory. Groups can be associated with multiple roles and vice versa.
<code>--tenant-ids IDs</code>	<p>Determines the tenant(s) for the role.</p> <p>You can specify one tenant ID or a comma-separated list of tenant IDs.</p>

## Example

This example creates a role named *mynewrole* on tenant 2:

```
vcli: admin> role create --name mynewrole --tenant-ids 2
```

## role delete

This command deletes a role.

## Usage

```
role delete --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which role to delete.
----------------------	---------------------------------

## Example

This example deletes the role with id 5.

```
vccli: admin> role delete --id 5
```

## role list

This command displays all roles. The output shows which managers and LDAP groups are assigned to each role.

Managers are locally defined VMS users, while LDAP groups are groups of users on a connected LDAP server, which may be Active Directory or any other LDAP-based authorization provider.

## Usage

```
role list
```

## Example

```
vccli: admin> role list
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
| ID | Name          | Managers          | Ldap-groups | Tenants | Default | Is A
dmin | Tenant-id | Tenant name |
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
| 1 | administrators | ['root', 'admin', 'support'] | []          | []      | True   | True
| None | None          |
| 3 | configuration | []                  | []          | []      | True   | Fals
e   | None         | None              |
| 5 | csi           | ['root', 'support', 'admin'] | []          | []      | True   | Fals
e   | None         | None              |
| 4 | debug_metrics | ['root', 'support']         | []          | []      | True   | Fals
e   | None         | None              |
| 2 | read_only    | []                    | []          | []      | True   | Fals
e   | None         | None              |
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
```

## role show

This command displays a role. The output shows which managers and have a given role and which LDAP groups are mapped to the role. Managers are locally defined VMS users, while LDAP groups are groups of users on a connected LDAP server, which may be Active Directory or any other LDAP-based authorization provider.



### Tip

Use the VAST Web UI to see which permissions are assigned to a role.

Go to Roles tab of the Administrators page, and choose the Edit option from the Actions menu for the role. The Update Roles dialog shows which permissions are currently assigned to the role.

## Usage

```
role show --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which role to display.
----------------------	----------------------------------

## Example

```
vcli: admin> role show --id 1
+-----+-----+
| ID      | 1      |
| Name    | administrators |
| Managers | ['root', 'admin', 'support'] |
| Ldap-groups | []    |
| Tenants | []    |
| Default | True   |
| Is Admin | True   |
| Tenant-id | None  |
| Tenant name | None |
+-----+-----+
```

## role unassign

This command removes permissions from a role.

## Usage

```
role unassign --id ID
  [--realm REALM] [--object-type OBJECT_TYPE --object-id OBJECT_ID]}
  [--permissions create|view|edit|delete]
  [--tenant-ids IDs]
```

# Required Parameters

<code>--id</code>	Specifies the role.
-------------------	---------------------

## Options

<code>--realm REALM</code>	<p>Specify a realm of VMS objects. Possible values:</p> <ul style="list-style-type: none"><li>• <code>events</code>. This realm includes alarms, events, event definitions and global event definition settings.</li><li>• <code>hardware</code>. This realm includes the cluster object and all infrastructure components.</li><li>• <code>logical</code>. This realm includes virtual IPs for network access, DNS service, Element Store views for protocol access, directory and user quotas, data protection features except for indestructibility, and S3 life cycle rules.</li><li>• <code>monitoring</code>. This realm includes analytics reports, capacity usage estimations, data flow analytics.</li><li>• <code>security</code>. This realm includes users and groups for data client access, authentication providers, VMS Role Based Access Control (RBAC), indestructibility for snapshots and protection policies, S3 identity policies, and VAST Data Support tunnels for remote support access.</li><li>• <code>settings</code>. This realm includes VMS settings.</li><li>• <code>support</code>. This realm includes Call Home configuration, support bundles, licenses, envs, and modules.</li></ul>
<code>--object-type OBJECT</code>	<p>Use this parameter together with <code>--object-id</code> to specify an object. In this case, the command will remove permission to access a specific object.</p> <p>Examples of objects are:</p> <ul style="list-style-type: none"><li>• <code>cluster</code></li><li>• <code>cnode</code></li><li>• <code>dnode</code></li><li>• <code>dbox</code></li><li>• <code>cbox</code></li><li>• <code>view</code></li><li>• <code>viewpolicy</code></li><li>• <code>quota</code></li></ul>

	<ul style="list-style-type: none"> <li>• vippool</li> <li>• eventdefinition</li> <li>• ldap</li> </ul> <p>For example, if you want to remove permission to access a given view, you would specify <code>--object-type view</code> and then provide the view's view ID as <code>--object-id</code>.</p>
<code>--object-id OBJECT_ID</code>	<p>Specify an object ID of the type specified by <code>--object-type</code>.</p> <p>For example: <code>--object-id 3</code></p>
<code>--permissions</code> <code>create view edit delete</code>	<p>Include this parameter to specify a specific type of permission. Omit this parameter to remove all types.</p>
<code>--tenant-ids IDs</code>	<p>Determines the tenant(s) for the role.</p> <p>You can specify one tenant ID or a comma-separated list of tenant IDs.</p>

## Example

The following example removes all permissions to the security realm on tenant 2:

```
vcli: admin> role unassign --id 2 --realm security --tenant-ids 2
```

# schema commands

## schema create

This command creates a VAST database schema.

## Usage

```
schema create --name SCHEMA
              --database-name DATABASE
              [--tenant-id TENANT]
```

## Required Parameters

<code>--name SCHEMA</code>	Enter a name for the schema being created. The name must meet the requirements for S3 object names.
<code>--database-name DATABASE</code>	Enter the name of the database where the schema is created.  A database can contain one or more schemas. The database name must meet the requirements for S3 bucket names.

## Options

<code>--tenant-id TENANT</code>	Enter the ID of the tenant where the database resides  If omitted, the default tenant is assumed.
---------------------------------	---

## Example

This example shows adding a schema named `schema1` to database `vastdb`:

```
vccli: admin> schema create --name schema1 --database-name vastdb
```

## schema delete

This command deletes a VAST database schema.

## Usage

```
schema create --name SCHEMA
              --database-name DATABASE
              [--tenant-id TENANT]
```

## Required Parameters

<code>--name SCHEMA</code>	Enter the name for the schema being deleted.
<code>--database-name DATABASE</code>	Enter the name of the database that contains the schema.

## Options

<code>--tenant-id TENANT</code>	Enter the ID of the tenant where the database resides  If omitted, the default tenant is assumed.
---------------------------------	---

## Example

This example shows deleting a schema named `schema1` from database `vastdb`:

```
vccli: admin> schema delete --name schema1 --database_name vastdb
```

### schema list

This command displays VAST Databases and schemas. You can filter for a specific database and schema, or show schemas for all databases.

## Usage

```
schema list [--database-name DATABASE]
            [--schema-name PARENT_SCHEMA]
            [--name SCHEMA]
            [--by-level LEVEL]
            [--page PAGE]
            [--page-size PAGE_SIZE]
            [--name-startswith PREFIX]
            [--tenant-id TENANT]
```

## Options

<code>--database-name DATABASE</code>	Specifies the name of the database containing the schema.
<code>--schema-name PARENT_SCHEMA</code>	Specifies the name of a parent schema in the database. A parent schema has nested schemas within it.

<pre>--name SCHEMA</pre>	<p>Specifies the name of a specific schema in the database. If <i>--schema-name</i> is also specified, this filters for nested schemas within the parent schema</p> <p>For example, for a database containing these schemas:</p> <pre>a a/b a/b/c a/b/d</pre> <p>then the combination of <i>--schema-name b --name c</i> will return <i>c</i>, while <i>--schema-name b</i> returns <i>c,d</i>.</p>
<pre>--by-level</pre>	<p>If present, the output list shows schemas at a single level of nesting only.</p> <p>For example, for the following schemas:</p> <pre>schema1 schema1/schema2 schema1/schema2/schema3</pre> <p>the command <code>schema list --schema-name schema1</code> shows</p> <pre>schema1/schema2 schema1/schema2/schema3</pre> <p>while <code>schema list --schema-name schema1 --by level</code> shows only</p> <pre>schema1/schema2</pre> <p>and <code>schema list --schema-name schema1/schema2 --by-level</code> shows</p> <pre>schema1/schema2/schema3</pre>
<pre>--page PAGE</pre>	<p>Specifies the specific page in the output list, by its number. This parameter is used only if <code>page-size</code> is set. Default is the first page.</p>
<pre>--page-size PAGE_SIZE</pre>	<p>Specifies the maximum number of schema to list per output page. Default: 100.</p>
<pre>--name-startswith PREFIX</pre>	<p>Specifies a prefix to filter the schema names.</p>



--tenant-id TENANT	Specifies the ID of the tenant where the database resides
-----------------------	---

## Example

This example returns all the schemas in a specific database, *db1*:

```
vcli: root> schema list --database-name db1
+-----+-----+-----+
| Name           | Database-name | Properties |
+-----+-----+-----+
| schema_1       | db1           |            |
| schema_1/nested_schema_1 | db1           |            |
| schema_2       | db1           |            |
+-----+-----+-----+
```

This example shows the schemas in a specific parent schema, *schema\_1*:

```
vcli: root> schema list --database-name db1 --schema-name schema_1
+-----+-----+-----+
| Name           | Database-name | Properties |
+-----+-----+-----+
| schema_1/nested_schema_1 | db1           |            |
+-----+-----+-----+
```

This example shows a list filtered with the `name-startswith` parameter:

```
vcli: root> schema list --database-name db1 --name-startswith schema
+-----+-----+-----+
| Name          | Database-name | Properties |
+-----+-----+-----+
| schema_1      | db1           |            |
| schema_2      | db1           |            |
+-----+-----+-----+
```

## schema rename

This command renames a VAST Database schema.

## Usage

```
schema rename --database-name DATABASE
              --name OLD_SCHEMA_NAME
              --new-name NEW_SCHEMA_NAME
              [--tenant-id TENANT]
```

## Required Parameters

--database-name DATABASE	Specifies the name of the database that contains the schema.
-----------------------------	--

<code>--name OLD_SCHEMA_NAME</code>	Specifies the name of the schema to be renamed.
<code>--new-name NEW_SCHEMA_NAME</code>	Specifies the new name for the schema. The name must meet the requirements for S3 object names.

## Options

<code>--tenant-id TENANT</code>	Specifies the ID of the tenant where the database resides  If omitted, the default tenant is assumed.
---------------------------------	---

## Example

This example shows renaming a schema named `schema1` into `abcd`:

```
vccli: admin> schema rename --name schema1 --database_name vastdb --new-name abcd
```

### schema show

This command shows details for a specific schema in a VAST Database.

## Usage

```
schema show --database-name DATABASE
            --name SCHEMA
            [--tenant-id TENANT]
```

## Required Parameters

<code>--database-name DATABASE</code>	Specifies the name of the database that contains the schema.
<code>--name SCHEMA_NAME</code>	Specifies the name of the schema.

## Options

<code>--tenant-id TENANT</code>	Specifies the ID of the tenant where the database resides  If omitted, the default tenant is assumed.
---------------------------------	---

## Example

```
vccli: admin> schema show --database-name tabular-1 --name schema_jypxvnuobg
```

+-----+-----+	
Name	schema_jypxvnuobg
Database-name	tabular-1
Properties	{}
+-----+-----+	

# snapshot commands

## snapshot clone

This command creates a cloned directory of a local snapshot, effectively restoring the snapshot data to the cluster.

The directory is instantly writable upon creation, and requests to read data from the directory can be read. Optionally, the clone can be *background synced* to the snapshot, which means that the data is fully copied to the cloned directory as a background task afterwards, such that when the copy is complete, read requests are all directed to the directory itself and are not dependent on the cloned snapshot.

## Usage

```
snapshot clone --id ID
               --name NAME
               --target-path PATH
               --target-tenant-id ID
               [--background-sync]
```

## Required Parameters

<code>--id ID</code>	Specifies the ID of the snapshot to use to create the clone.  To retrieve snapshot IDs, run the <a href="#">snapshot list</a> command.
<code>--name NAME</code>	Specifies a name for the snapshot clone.
<code>--target-path PATH</code>	Specifies a local path on the target tenant where you want the clone to reside.
<code>--target-tenant-id ID</code>	Specifies the tenant on the local cluster to which you want to clone the snapshot.

## Options

<code>--background-sync</code>	Causes the snapshot data to be copied from the source to the destination after the clone is created. During the copying stage, read requests are directed to the source if the requested data is not yet copied. When the copying is complete, the clone becomes a local directory.  If not specified, this setting is disabled, in which case the snapshot data is not copied to the destination. Requests to read data from the cloned directory continue to read data from the cloned source on the remote peer.
--------------------------------	---

## Example

```
vccli: admin> snapshot clone --id 230 --name local-ss --target-path /local-gss --target-tenant-id 1
```

### snapshot create

This command creates a [snapshot](#).

## Usage

```
snapshot create --path PATH
                 --name NAME
                 [--expiration-time EXPIRATION_TIME]
                 [--enable-lock]
```

## Required Parameters

<code>--path</code> PATH	Specifies the path to a directory. The snapshot will include all files and folders under the specified directory at the time of taking the snapshot.
<code>--name</code> NAME	Sets the name of the snapshot.

## Options

<code>--expiration-time</code> EXPIRATION_TIME	<p>Specifies a time in the future at which the snapshot should expire.</p> <p>Specify EXPIRATION_TIME in the format <i>YYYY-mm-ddTHH:MM:SS</i>.</p> <p>Example: <code>--expiration-time 2019-09-25T22:30:00</code></p>
<code>--enable-lock</code>	Renders the snapshot indestructible. Once this setting is enabled, deleting the snapshot or shortening its expiration time requires unlocking the cluster's indestructibility mechanism.

## Example

```
vccli: admin> snapshot create --path /dev --name snap1 --expiration-time 2020-10-26T21:30:00
```

### snapshot delete

This command deletes a [snapshot](#).

# Usage

```
snapshot delete --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which snapshot to delete.
----------------------	-------------------------------------

## Example

```
vcli: admin> snapshot delete --id 1
Are you sure you want to delete the snapshot? [y/N] y
```

### snapshot list

This command displays all [snapshots](#) and their details.

## Usage

```
snapshot list [--name NAME_CONTAINS]
               [--path PATH]
               [--expiration-time EXPIRATION_TIME]
               [--policy POLICY__NAME]
               [--state STATE]
               [--tenant-name NAME]
               [--tenant-id ID]
```

## Options

<code>--name NAME_CONTAINS</code>	Filters the list by snapshot name or part of the snapshot name.
<code>--path PATH</code>	Filters the list by path.
<code>--expiration-time EXPIRATION_TIME</code>	Filters the list by expiration time .
<code>--policy POLICY__NAME</code>	Filters the list to display snapshots created by a specified snapshot policy. Specify POLICY_NAME as the name of a snapshot policy.
<code>--state STATE</code>	Filters the list by state.

<code>--tenant-name NAME</code>	Filters the list by tenant.
<code>--tenant-id ID</code>	Filters the list by tenant.

## Example

```

vcli: admin> snapshot list
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
| ID | Name | Path | Policy |
Type | Indestructible | Created | Expiration-time | Aggregated Usage(GB) | Unique Usage(GB) | Tenant-id |
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
| 16 | default_protection_policy_2023-03-29_14_55_24 UTC | / | None |
local | False | 2023-03-29T14:55:24.005000Z | Never | 0.0 |
| 0.0 | 1 |
| 26 | big_catalog_2023-03-29_15_40_00 UTC | / | Big catalog policy |
local | False | 2023-03-29T15:40:00.005000Z | 2023-03-29T16:00:00Z | 0.2 |
| 0.0 | None |
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+

```

## snapshot modify

This command modifies a [snapshot](#).

## Usage

```

snapshot modify --id ID
                [--name NAME]
                [--expiration-time EXPIRATION_TIME]
                [--enable-lock]

```

## Required Parameters

<code>--id ID</code>	Specifies which snapshot to modify.
----------------------	-------------------------------------

## Options

<code>--name NAME</code>	Changes the name of the snapshot.
--------------------------	-----------------------------------

<pre>--expiration-time EXPIRATION_TIME</pre>	<p>Sets or modifies a time in the future at which the snapshot should expire.</p> <p>Specify EXPIRATION_TIME in the format <code>YYYY-mm-ddTHH:MM:SS</code>.</p> <p>Example: <code>--expiration-time 2019-09-25T22:30:00</code></p>
<pre>--enable-lock</pre>	<p>Renders the snapshot indestructible. Once this setting is enabled, deleting the snapshot or shortening its expiration time requires unlocking the cluster's indestructibility mechanism.</p>

## Example

```
vccli: admin> snapshot modify --id 971306 --name s3mainsnap
```

### snapshot show

This command displays details of a specific [snapshot](#).

## Usage

```
snapshot show --id ID
```

## Required Parameters

<pre>--id ID</pre>	<p>Specifies which snapshot to display.</p>
--------------------	---

## Example

```
vccli: admin> snapshot show --id 35
```

```
+-----+-----+
| ID          | 35 |
| Name        | bc_table_2023-03-29_15_55_00 |
| Path        | /  |
| Policy       | Big catalog policy |
| Type         | local |
| Indestructible | False |
| Created      | 2023-03-29T15:55:14.660000Z |
| Expiration-time | 2023-03-29T16:15:00Z |
| Aggregated Usage (GB) | 0.0 |
| Unique Usage (GB) | 0.0 |
| Tenant-id    | None |
+-----+-----+
```



# ssd commands

## ssd activate

This command activates an SSD.

## Usage

```
ssd activate --id ID
```

## Required Parameters

<code>--id ID</code>	Specify the SSD ID.  To list SSD IDs, use the <a href="#">ssd list</a> command.
----------------------	---

## Example

This example shows activation of SSD 2:

```
vcli: admin> ssd activate --id 2
```

## ssd deactivate

This command deactivates an SSD.

## Usage

```
ssd deactivate --id ID
```

## Required Parameters

<code>--id ID</code>	Specify the SSD ID.  To list SSD IDs, use the <a href="#">ssd list</a> command.
----------------------	---

## Example

This example shows deactivation of SSD 2:

```
vcli: admin> ssd deactivate --id 2
```

# ssd list

This command displays all SSDs and their details.

## Usage

```
ssd list [--state STATE]
         [--dbox-name DBOX_NAME]
         [--dbox-id DBOX_ID]
         [--fw-version FIRMWARE_VERSION]
         [--page PAGE]
         [--page-size PAGE_SIZE]
```

## Options

<code>--state STATE</code>	<p>Filters the list by SSD state, which can be one of the following:</p> <ul style="list-style-type: none"><li>• ACTIVATING</li><li>• ACTIVE</li><li>• DEACTIVATING</li><li>• INACTIVE</li><li>• FAILING</li><li>• FAILED</li><li>• PHASING_OUT</li><li>• ENTER_PHASING_OUT</li><li>• EXIT_PHASING_OUT</li><li>• UNKNOWN</li></ul>
<code>--dbox-name DBOX_NAME</code>	<p>Filters the list by the name of the DBox to which the SSDs belong.</p> <p>Specify <code>DBOX_NAME</code> as a string value.</p>
<code>--dbox-id DBOX_ID</code>	<p>Filters the list by the ID of the DBox to which the SSDs belong..</p> <p>Specify <code>DBOX_ID</code> as an integer value.</p>
<code>--fw-version FIRMWARE_VERSION</code>	<p>Filters the list by firmware version.</p>
<code>--page PAGE</code>	<p>Specifies which page of the list to list, where default page size is 50 listings.</p>

	See also <code>--page-size</code> .
<code>--page-size PAGE_SIZE</code>	<p>The maximum number of SSDs to list per page in the command output.</p> <p>Default: 50</p> <p>Maximum: 500</p>

## Example

```
vcli: admin> ssd list
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name | State | Serial-Number | Model | Total-Space(TB) | DBox
| Shelf | Carrier-Index | Index-In-Carrier | Attached-dnode-names | Firmware-Version | Enable
d | Failure-Reason |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | | ACTIVE | PHLL0304003415PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | RIGHT | 7 | | 1 | | dnode-105 | 8DV10510 | T
rue | NONE |
| 2 | | ACTIVE | PHLL0305009Q15PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | RIGHT | 12 | | 1 | | dnode-105 | 8DV10510 | T
rue | NONE |
| 3 | | ACTIVE | PHLL030500E415PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | LEFT | 35 | | 1 | | dnode-105 | 8DV10510 | T
rue | NONE |
| 4 | | ACTIVE | PHLL030500BP15PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | LEFT | 39 | | 1 | | dnode-105 | 8DV10510 | T
rue | NONE |
| 5 | | ACTIVE | PHLL0314000X15PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | LEFT | 40 | | 1 | | dnode-105 | 8DV10510 | T
rue | NONE |
| 6 | | ACTIVE | PHLL030400C115PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | RIGHT | 8 | | 1 | | dnode-105 | 8DV10510 | T
rue | NONE |
| 7 | | ACTIVE | PHLL0341008415PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | LEFT | 36 | | 1 | | dnode-105 | 8DV10510 | T
rue | NONE |
| 8 | | ACTIVE | PHLL034100AK15PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | LEFT | 44 | | 1 | | dnode-105 | 8DV10510 | T
rue | NONE |
| 9 | | ACTIVE | PHLL030500FF15PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | RIGHT | 20 | | 1 | | dnode-105 | 8DV10510 | T
rue | NONE |
| 10 | | ACTIVE | PHLL0341005Y15PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | RIGHT | 28 | | 1 | | dnode-105 | 8DV10510 | T
rue | NONE |
| 11 | | ACTIVE | PHLL0305009E15PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | RIGHT | 11 | | 1 | | dnode-105 | 8DV10510 | T
rue | NONE |
| 12 | | ACTIVE | PHLL0305000Z15PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | RIGHT | 15 | | 1 | | dnode-105 | 8DV10510 | T
rue | NONE |
| 13 | | ACTIVE | PHLL0304009H15PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | RIGHT | 3 | | 1 | | dnode-105 | 8DV10510 | T
rue | NONE |
```

F016	14	RIGHT	ACTIVE	PHLL0305003K15PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	15	RIGHT	ACTIVE	PHLL030500G015PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	16	RIGHT	ACTIVE	PHLL034100D415PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	17	LEFT	ACTIVE	PHLL034100BT15PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	18	LEFT	ACTIVE	PHLL034100CD15PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	19	LEFT	ACTIVE	PHLL030400E015PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	20	LEFT	ACTIVE	PHLL0305009D15PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	21	LEFT	ACTIVE	PHLL034100A515PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	22	LEFT	ACTIVE	PHLL0313009C15PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	23	RIGHT	ACTIVE	PHLL0305008V15PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	24	RIGHT	ACTIVE	PHLL0341002T15PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	25	LEFT	ACTIVE	PHLL0305009N15PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	26	RIGHT	ACTIVE	PHLL0313001N15PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	27	RIGHT	ACTIVE	PHLL034100BV15PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	28	RIGHT	ACTIVE	PHLL0305009H15PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	29	LEFT	ACTIVE	PHLL030500FQ15PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	30	LEFT	ACTIVE	PHLL0341001115PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	31	LEFT	ACTIVE	PHLL030400CU15PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	32	RIGHT	ACTIVE	PHLL034100A815PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	33	RIGHT	ACTIVE	PHLL0305007G15PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	34	RIGHT	ACTIVE	PHLL0313005F15PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	35	LEFT	ACTIVE	PHLL0341003715PDGN	INTEL	SSDPE2NV153T8	15.363	8DV10510	dbbox-0A7P	T
rue		NONE								
F016	36		ACTIVE	PHLL0313005315PDGN	INTEL	SSDPE2NV153T8	15.363		dbbox-0A7P	

```

F016 | LEFT | 51 | 1 | dnode-104 | 8DV10510 | T
rue | NONE |
| 37 | | ACTIVE | PHLL0305007J15PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | LEFT | 42 | 1 | dnode-104 | 8DV10510 | T
rue | NONE |
| 38 | | ACTIVE | PHLL030400GX15PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | RIGHT | 10 | 1 | dnode-104 | 8DV10510 | T
rue | NONE |
| 39 | | ACTIVE | PHLL0304009V15PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | RIGHT | 27 | 1 | dnode-104 | 8DV10510 | T
rue | NONE |
| 40 | | ACTIVE | PHLL034100AN15PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | LEFT | 29 | 1 | dnode-104 | 8DV10510 | T
rue | NONE |
| 41 | | ACTIVE | PHLL034100CH15PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | LEFT | 50 | 1 | dnode-104 | 8DV10510 | T
rue | NONE |
| 42 | | ACTIVE | PHLL030400BW15PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | LEFT | 46 | 1 | dnode-104 | 8DV10510 | T
rue | NONE |
| 43 | | ACTIVE | PHLL030500FN15PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | RIGHT | 18 | 1 | dnode-104 | 8DV10510 | T
rue | NONE |
| 44 | | ACTIVE | PHLL0341003415PDGN | INTEL SSDPE2NV153T8 | 15.363 | dbx-0A7P
F016 | LEFT | 55 | 1 | dnode-104 | 8DV10510 | T
rue | NONE |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

# s3replicationpeer commands

## s3replicationpeer create

This command adds a cloud destination for replication. The destination must be an AWS S3 bucket or a custom destination that supports S3 access.

## Usage - AWS S3 Bucket

```
s3replicationpeer create --name NAME
                        --bucket-name BUCKET_NAME
                        --type AWS_S3
                        --access-key ACCESS_KEY
                        --secret-key SECRET_KEY
                        --aws-region AWS_REGION
                        [--proxies PROXIES]
```

## Usage - Custom S3 Bucket

```
s3replicationpeer create --name NAME
                        --bucket-name BUCKET_NAME
                        --http-protocol http|https
                        --type CUSTOM_S3
                        --access-key ACCESS_KEY
                        --secret-key SECRET_KEY
                        --custom-bucket-url CUSTOM_BUCKET_URL
                        [--proxies PROXIES]
```

## Required Parameters

<code>--name NAME</code>	Sets the name of the target.
<code>--bucket-name BUCKET_NAME</code>	Sets the bucket name of the S3 bucket to which you are replicating the cluster's data (up to 63 characters).
<code>--http-protocol http https</code>	Required only if type is set to custom_s3. Specifies which HTTP protocol over which to access the target.
<code>--type AWS_S3 CUSTOM_S3</code>	Specify whether the target is an AWS bucket (AWS_S3) or a custom S3 destination (Custom_S3).
<code>--access-key ACCESS_KEY</code>	Specifies the access key of a key pair for accessing the bucket.

<pre>--secret-key SECRET_KEY</pre>	Specifies the access key of a key pair for accessing the bucket.
------------------------------------	--

## Options

<pre>--custom-bucket- url CUSTOM_BUCKET_URL</pre>	For a custom S3 target, include this option and specify the URL of the custom bucket.
<pre>--aws-region AWS_REGION</pre>	For an AWS S3 target, include this option to specify the AWS region where the bucket resides. <i>AWS-REGION</i> is the
<pre>--proxies PROXIES</pre>	<p>Specifies proxies. If proxies are specified, replication traffic is routed via the proxies to and from the replication target.</p> <p>Proxies can either be external to the cluster or they can run on a subset of the cluster's CNodes.</p> <p>To use a CNode as a proxy, first install third party proxy software on the CNode and then enter the proxy here.</p> <p>You can specify up to eight proxies. Traffic is load balanced between the specified proxies, excluding any inactive proxies.</p> <p>Specify each proxy using the format <code>http://&lt;username&gt;:&lt;password&gt;@&lt;proxy IP&gt;:&lt;proxy port&gt;</code>, in which <code>&lt;password&gt;</code> or the user name and password for authenticating to the proxy, <code>&lt;proxy IP&gt;</code> is the proxy's IP address, and <code>&lt;proxy port&gt;</code> is the proxy port.</p> <p>To specify multiple proxies, separate the proxies by commas.</p> <p>For example: <code>--proxies http://admin:admin@192.0.2.0:8080,http://admin:admin@192.0.2.1:8080,http://admin:admin@192.0.2.2:8080</code></p>

## Example

```
vcli: admin> s3replicationpeer create --name MY-S3-BACKUP-TARGET --type AWS_S3 --access-key A
KIARTN2ZMSYQSD5CW45 --secret-key ON/mupAUNe4DdWR5/thZxfoY2xjLLzLCb0SHqQ8n --bucket-name my-s
3-bucket --aws-region us-east-1
```

### s3replicationpeer delete

This command deletes an S3 replication peer.

## Usage

```
s3replicationpeer delete --id ID
```

# Required Parameters

<code>--id ID</code>	Specifies the S3 replication peer to delete by its ID.
----------------------	--

## Example

`vccli: admin> s3replicationpeer delete --id 2`

### s3replicationpeer list

This command lists s3 replication peers.

## Usage

```
s3replicationpeer list [--aws-region AWS_REGION]
                      [--bucket-name BUCKET_NAME]
                      [--custom-bucket-url CUSTOM_BUCKET_URL]
                      [--http-protocol http|https]
                      [--id ID]
                      [--name NAME]
```

## Options

<code>--aws-region AWS_REGION</code>	Filters the list by AWS region.
<code>--bucket-name BUCKET_NAME</code>	Filters the list by bucket name.
<code>--custom-bucket-url CUSTOM_BUCKET_URL</code>	Filters the list by custom bucket URL.
<code>--http-protocol http https</code>	Filters the list by HTTP protocol.
<code>--id ID</code>	Filters the list by ID.
<code>--name NAME</code>	Filters the list by target name.

## Example

This command lists S3 replication peers with the name *AWS-S3\_TARGET*.



```
vcli: admin> s3replicationpeer list --name AWS-S3-TARGET
+-----+-----+-----+-----+-----+-----+
+-----+
| ID | Name           | State   | Bucket-name | Http-protocol | Custom-bucket-url | Aws-region |
+-----+-----+-----+-----+-----+-----+
| 5  | AWS-S3-TARGET | ACTIVE  | my-s3-bucket| https         | None              | us-east-1  |
+-----+-----+-----+-----+-----+-----+
+-----+
```

## s3replicationpeer modify

This command modifies an S3 replication peer.

## Usage

```
s3replicationpeer modify --id ID
                        [--access-key ACCESS_KEY]
                        [--secret-key SECRET_KEY]
                        [--bucket-name BUCKET_NAME]
                        [--http-protocol http|https]
                        [--custom-bucket-url CUSTOM_BUCKET_URL]
                        [--aws-region AWS_REGION]
                        [--name NAME]
                        [--proxies PROXIES]
```

## Required Parameters

<code>--id ID</code>	Specifies which S3 replication peer to modify, by its ID (integer).
----------------------	---

## Options

<code>--access-key ACCESS_KEY</code>	Specifies the access key of a key pair for accessing the bucket.
<code>--secret-key SECRET_KEY</code>	Specifies the access key of a key pair for accessing the bucket.
<code>--bucket-name BUCKET_NAME</code>	Sets the bucket name of the S3 bucket to which you are replicating the cluster's data (up to 63 characters).
<code>--http-protocol http https</code>	For custom S3 targets, specifies which HTTP protocol over which to access the target.

<pre>--custom-bucket-url CUSTOM_BUCKET_URL</pre>	For a custom S3 target, specifies the URL of the custom bucket.
<pre>--aws-region AWS_REGION</pre>	For an AWS S3 target, specifies the AWS region where the bucket resides. <i>AWS-REGION</i> is the <a href="#">region code</a> .
<pre>--name NAME</pre>	Sets the name of the target.
<pre>--proxies PROXIES</pre>	<p>Specifies proxies. If proxies are specified, replication traffic is routed via the proxies to and from the replication target.</p> <p>Proxies can either be external to the cluster or they can run on a subset of the cluster's CNodes.</p> <p>To use a CNode as a proxy, first install third party proxy software on the CNode and then enter the proxy here.</p> <p>You can specify up to eight proxies. Traffic is load balanced between the specified proxies, excluding any inactive proxies.</p> <p>Specify each proxy using the format <code>http://&lt;username&gt;:&lt;password&gt;@&lt;proxy IP&gt;:&lt;proxy port&gt;</code>, in which <code>&lt;password&gt;</code> or the user name and password for authenticating to the proxy, <code>&lt;proxy IP&gt;</code> is the proxy's IP address, and <code>&lt;proxy port&gt;</code> is the proxy port.</p> <p>To specify multiple proxies, separate the proxies by commas.</p> <p>For example: <code>--proxies http://admin:admin@192.0.2.0:8080,http://admin:admin@192.0.2.1:8080,http://admin:admin@192.0.2.2:8080</code></p>

## Example

This example changes the name of the S3 replication peer with ID 1 to "AWS-S3-REPLICATION-TARGET".

```
vcli: admin> s3replicationpeer modify --id 1 --name AWS-S3-REPLICATION-TARGET
```

### s3replicationpeer show

This command displays the configuration of a specified S3 replication peer.

## Usage

```
s3replicationpeer show --id ID
```

## Required Parameters

<pre>--id ID</pre>	Specifies which S3 replication peer to show, by its ID (integer).
--------------------	---

## Example

This example displays the configuration of the S3 replication peer with ID 1.

```
vcli: admin> s3replicationpeer show --id 1
```

+-----+-----+		
ID	1	
Name	AWS-S3-REPLICATION-TARGET	
State	INIT	
Proxies	[]	
Bucket-name	bucket-1	
Http-protocol	https	
Custom-bucket-url	None	
Aws-region	None	
Aws-role	None	
+-----+-----+		

# S3policy commands

## identitypolicy create

This command creates an identity policy.



### Note

This command requires you to enter policy content in the command line. Since the policy content is multi-line, you may find that your SSH terminal does not succeed in creating the policies.

In case of difficulty, we recommend you use the VAST Web UI to [add identity policies to VMS](#).

## Usage

```
identitypolicy create --name NAME
                    --policy POLICY
                    --tenant-id ID
```

## Required Parameters

<code>--name NAME</code>	Specifies a name for the identity policy.
<code>--policy POLICY</code>	Enter the identity policy content in JSON format. For information about how to write identity policies, see <a href="#">Creating Identity Policies</a> .
<code>--tenant-id ID</code>	Identifies the tenant associated with this identity policy.

## Example

This example creates an identity policy that allows any user on tenant 2 to which the identity policy is attached to perform all actions on all resources:

```
vcli: admin> identitypolicy create --name allow_all --tenant-id 2 --policy '    {
    "Version": "2012-10-17",
    "Statement": [{
    "Sid": "AllowAllActionsAllResources",
    "Action":
    "*",
    "Effect": "Allow",
    "Resource":
    "*"
    }
```

```
}  
  ]  
}'
```

## identitypolicy delete

This command deletes an identity policy.



### Note

You cannot delete an identity policy that was replicated from an async replication peer.

## Usage

```
identitypolicy delete --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which identity policy to delete. To retrieve policy ID numbers, run <a href="#">identitypolicy list</a> .
----------------------	---

## Example

```
vccli: admin> identitypolicy delete --id 10
```

## identitypolicy list

This command displays the details of all identity policies managed by VMS.

## Usage

```
identitypolicy list
```

## Example

```
vccli: admin> identitypolicy list
```

ID	Name	Users	Groups	Policy
10	allow_all	[]	[]	{ "Version": "2012-10-17", "Statement": [{ "Sid": "AllActionsAndResources", "Action": "**", "Effect": "Allow", "Resource": "**"

```

| | | | | }
| | | | | ]
| | | | | }
+-----+

```

## identitypolicy modify

This command modifies an identity policy and can be used to enable or disable an identity policy, such as an identity policy that was replicated from an async replication peer.

## Usage

```

identitypolicy modify --id ID
                        [--name NAME]
                        [--policy POLICY]
                        [--tenant-id ID]
                        [--enable|--disable]

```

## Required Parameters

--id ID	Specifies which identity policy to modify.
---------	--

## Options

--name NAME	Changes the name of the identity policy.
--policy POLICY	Replaces the policy content with a new policy content. For information about how to write identity policies, see <a href="#">Creating Identity Policies</a> .
--tenant-id ID	Identifies the tenant associated with this identity policy.
--enable	Enables a policy that was disabled or was replicated to the cluster from an async replication peer, in which case, it is disabled by default.
--disable	Disables the policy.

## Example

```

vcli: admin> identitypolicy modify --id 10 --name allow_all

```

# identitypolicy show

This command displays details of a specific identity policy.

## Usage

```
identitypolicy show --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which identity policy to display.
----------------------	---

## Example

```
vccli: admin> identitypolicy show --id 10
+-----+
+-----+-----+
+
| ID      | 10
|
| Name    | AllowAll
|
| Users   | []
|
| Groups  | []
|
| Policy  | {      "Version": "2012-10-17",      "Statement": [{      "Sid": "AllowActi
onsAllResources",      "Action": |
|      | "*",      "Effect": "Allow",      "Resource":      ""      }      ]
}
+-----+
+-----+-----+
+
```

# supportbundle commands

## supportbundle create

This command creates a [support bundle](#).

## Usage

```
supportbundle create --prefix PREFIX
                        [--preset PRESET]
                        [--start-time TIME]
                        [--end-time TIME]
                        [--obfuscated]
                        [--cnodes-only] | [dnodes-only]
                        [--cnode-ids CNODE_IDS]
                        [--dnode-ids DNODE_IDS]
                        [--vipool-ids POOL_IDS]
                        [--hubble-args ARGS]
                        [--astron-args ARGS]
                        [--max-size SIZE]
                        [--text]
                        [--send-now]
                        [--upload-via-vms]
                        [--bucket-name NAME]
                        [--access-key KEY]
                        [--secret-key KEY]
                        [--bucket-subdir DIR]
                        [--delete-after-send]
```

## Required Parameters


<code>--prefix</code> PREFIX	<p>Enter an identifying label to include in the bundle file name.</p> <p>The prefix can contain up to 64 characters. Special characters are not allowed.</p> <p>The name of the bundle will be <i>bundle-&lt;preset&gt;-&lt;cluster name&gt;-&lt;prefix&gt;-&lt;timestamp&gt;.tar</i>, where <i>&lt;prefix&gt;</i> is the prefix specified here.</p> <p>For example, if the prefix is <i>MyUrgentIssue</i>, a bundle using the <i>mini</i> preset created at exactly 7:45 am UTC on September 3rd, 2020 on a cluster called <i>cluster1</i> would be named <i>bundle-mini-cluster1-MyUrgentIssue-2020-09-03-074500.tar</i>.</p>
---------------------------------	---

## Options

<code>--preset</code> PRESET	<p>Specify a category (or categories) that best suits the issue for which you are creating the support bundle.</p> <p>Each category includes a predefined set of data objects in the support bundle. Verify with your support engineer which category is suitable for your needs.</p> <p>If no categories are specified, only management logs are collected.</p>
---------------------------------	--



	<p>Specify one or more of the following categories as PRESET:</p> <ul style="list-style-type: none"> <li>• standard (default)</li> <li>• debug</li> <li>• mini</li> <li>• management</li> <li>• performance</li> <li>• traces_and_metrics</li> <li>• nfs</li> <li>• nfs4</li> <li>• smb</li> <li>• s3</li> <li>• estore</li> <li>• raid</li> <li>• hardware</li> <li>• permission_issues</li> <li>• rca</li> <li>• dr</li> <li>• metadata</li> </ul>
<code>--start-time TIME</code>	<p>Sets the start time from which to collect information.</p> <p>Specify TIME in UTC+0 in the format <i>YYYY-MM-DD hh:mm:ss</i>.</p>
<code>--end-time TIME</code>	<p>Sets the end time for the period to collect information.</p> <p>Specify TIME in UTC+0 in the format <i>YYYY-MM-DD hh:mm:ss</i>.</p> <p>It's usually advisable to consult with the support engineer on the time frame so that you can make it as short as possible and minimize the size of the bundle.</p>
<code>--obfuscated</code>	<p>Converts all bundled objects to text and obfuscates them. Any data that cannot be converted to text is not included in the bundle. The following types of information are replaced with a non-reversible hash: file and directory names, IP addresses, host names, user names, passwords, MAC addresses.</p> <p>If this option is not specified (default), the information is not obfuscated.</p>

<code>--cnodes-only</code>	Specify this option to collect data from CNodes only.
<code>--dnodes-only</code>	Specify this option to collect data from DNodes only.
<code>--cnode-ids</code> <code>CNODE_IDS</code>	<p>Specify a comma-separated list of CNode IDs to collect data from.</p> <p>By default, all CNodes are included.</p> <p>This option cannot be used together with <code>--dnodes-only</code>.</p> <div>  <p><b>Note</b></p> <p>If you specified the <code>metadata</code> preset, you can specify only one CNode.</p> </div>
<code>--dnode-ids</code> <code>DNODE_IDS</code>	<p>Specify a comma-separated list of DNode IDs to collect data from.</p> <p>By default, all DNodes are included.</p> <p>This option cannot be used together with <code>--cnodes-only</code>.</p>
<code>--vipool-ids</code> <code>POOL_IDS</code>	Specify a comma-separated list of virtual IP pools to collect data only from CNodes that are included in these virtual IP pools.
<code>--hubble-args ARGS</code>	Enter any arguments to pass to <i>Hubble</i> , per instructions from the support engineer.
<code>--astron-args ARGS</code>	Enter any arguments to pass to <i>Astron</i> , per instructions from the support engineer.
<code>--max-size SIZE</code>	Enter a maximum data limit to apply to the collection of binary trace files, in GB. You can use this option to limit the overall size of the support bundle.
<code>--text</code>	<p>Converts all bundled objects to a text format. Any data that cannot be converted to text is not included in the bundle.</p> <p>This setting is enabled automatically if <code>--obfuscated</code> is specified.</p>

<code>--send-now</code>	Sends the support bundle immediately.
<code>--upload-via-vms</code>	Uploads a support bundle via VMS. Otherwise, the upload is done from each node. This option is available only if <code>--send-now</code> is specified.
<code>--bucket-name NAME</code>	Specifies the S3 bucket name of the destination S3 bucket.
<code>--access-key KEY</code>	Specifies the access key of a valid key pair to access the destination S3 bucket.
<code>--secret-key KEY</code>	Specifies the secret key of a valid key pair to access the destination S3 bucket.
<code>--bucket-subdir DIR</code>	Specifies the subdirectory in the destination S3 bucket to which to upload the support bundle.
<code>--delete-after-send</code>	Deletes the support bundle immediately after it has been sent successfully.

## Example

This example shows creating a standard support bundle on CNodes 5 and 6:

```

vcli: admin> supportbundle create --prefix SB --preset standard --start-time "2022-04-18 03:00:00" --end-time "2022-04-18 03:15:00" --cnode-ids 5,6

```

### supportbundle delete

This command deletes a support bundle.

## Usage

```
supportbundle delete --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which support bundle to delete.
----------------------	---

## Example

```
vccli: admin> supportbundle delete --id 1
```

### supportbundle list

This command displays all support bundles and their details.

## Usage

```
supportbundle list
```

## Example

This example

```
vccli: admin> supportbundle list
```

### supportbundle show

This command displays details of a support bundle.

## Usage

```
supportbundle show --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which support bundle to display.
----------------------	--

## Example

```
vccli: admin> supportbundle show --id 1
```

### supportbundle upload

This command uploads a support bundle.

## Usage

```
supportbundle upload --id ID
                        [--upload-via-vms]
                        [--bucket-name NAME]
                        [--access-key KEY]
                        [--secret-key KEY]
```

[--bucket-subdir DIR]

## Required Parameters

<code>--id ID</code>	Specifies the support bundle to upload.
----------------------	---

## Options

<code>--upload-via-vms</code>	Uploads a support bundle via VMS. Otherwise, the upload is done from each node.  This option is available only if <code>--send-now</code> is specified.
<code>--bucket-name NAME</code>	Specifies the S3 bucket name of the destination S3 bucket.
<code>--access-key KEY</code>	Specifies the access key of a valid key pair to access the destination S3 bucket.
<code>--secret-key KEY</code>	Specifies the secret key of a valid key pair to access the destination S3 bucket.
<code>--bucket-subdir DIR</code>	Specifies the subdirectory in the destination S3 bucket to which to upload the support bundle.

## Example

This example shows uploading support bundle 1 to the S3 bucket named "my-bucket":

```
vcli: admin> supportbundle upload --id 1 --bucket-name vast-bucket
```

# table commands


## table add-columns

This command creates a VAST database table.

## Usage

```
table create --name TABLE
             --schema-name SCHEMA
             --arrow-schema COLUMNS
             --database-name DATABASE
             [--tenant-id TENANT]
```

## Required Parameters

<code>--name TABLE</code>	Enter the name of the table where you want to add more columns.
<code>--schema-name SCHEMA</code>	Enter the name of the schema where the table resides.
<code>--arrow-schema COLUMNS</code>	<div>Enter a comma-separated list of columns to be added.</div> <div>The columns are specified using the Arrow format, for example:</div> <div><code>col1-int8,col2-string,col3-int8</code></div> <div> <b>Note</b></div> <div>Complex data types are not supported on this command. To add a column with a complex data type, <a href="#">use</a> VAST Web UI.</div>
<code>--database-name DATABASE</code>	Enter the name of the database where the table resides.

## Options

<code>--tenant-id TENANT</code>	Enter the ID of the tenant where the database resides
---------------------------------	---

	If omitted, the default tenant is assumed.
--	--

# Example

This example shows adding a column named `age` to table `cats`:

```

vcli: admin> table create --name cats --schema-name schema1 --arrow-schema age-int8 --database_name vastdb

```

## table create

This command creates a VAST database table.


# Usage

```

table create --name TABLE
             --schema-name SCHEMA
             --arrow-schema COLUMNS
             --database-name DATABASE
             [--tenant-id TENANT]

```

# Required Parameters

<code>--name TABLE</code>	Enter a name for the table being created. The name must meet the requirements for S3 object names.
<code>--schema-name SCHEMA</code>	Enter the name of the schema where the table is to be created.
<code>--arrow-schema COLUMNS</code>	<p>Enter a comma-separated list of columns for the new table.</p> <p>The columns are specified using the Arrow format, for example:</p> <pre>col1-int8,col2-string,col3-int8</pre> <div>  <div> <p><b>Note</b></p> <p>Complex data types are not supported on this command. To add a column with a complex data type, <a href="#">use VAST Web UI</a>.</p> </div> </div>
<code>--database-name</code>	Enter the name of the database where the table's schema is created.

DATABASE	
----------	--

## Options

--tenant-id TENANT	Specifies the ID of the tenant where the database resides  If omitted, the default tenant is assumed.
--------------------	---

## Example

This example shows adding a table named `cats` to schema `schema1` in database `vastdb`:

```
vcli: admin> table create --name cats --schema-name schema1 --arrow-schema name-string,age-in
t8 --database_name vastdb
```

### table delete

This command deletes a VAST database table.

## Usage

```
table create --name TABLE
             --schema-name SCHEMA
             --database-name DATABASE
             [--tenant-id TENANT]
```

## Required Parameters

--name TABLE	Enter the name of the table to be deleted.
--schema-name SCHEMA	Enter the name of the schema where the table resides.
--database-name DATABASE	Enter the name of the database where the table resides.

## Options

--tenant-id TENANT	Specifies the ID of the tenant where the database resides
--------------------	---



	If omitted, the default tenant is assumed.
--	--

## Example

This example shows deleting a table named `cats` :

```
vccli: admin> table delete --name cats --schema-name schema1 --database_name vastdb
```

### table list

This command lists tables in a VAST Database.

## Usage

```
table list --database-name DATABASE
           --schema-name SCHEMA
           [--name TABLE]
           [--page PAGE_NUMBER]
           [--page-size PAGE_SIZE]
           [--name-startswith PREFIX]
           [--tenant-id TENANT]
```

## Required Parameters

<code>--database-name DATABASE</code>	Specifies the name of the database that contains the schema.
<code>--name SCHEMA_NAME</code>	Specifies the name of the schema containing the table.

## Options

<code>--page PAGE</code>	Specifies the specific page in the output list, by its number. This parameter is used only if <code>page-size</code> is set. Default is the first page.
<code>--page-size PAGE_SIZE</code>	Specifies the maximum number of tables to list per output page. Default: 100.
<code>--name TABLE</code>	Specifies the name of a specific table. If included, only this table is shown.
<code>--name-startswith</code>	Specifies a prefix to filter the table names.

PREFIX	
--tenant-id TENANT	Specifies the ID of the tenant where the database resides  If omitted, the default tenant is assumed.

## Example

```
vcli: admin> table list --database-name tabular-industrious --schema-name schema_abc
+-----+-----+-----+-----+
+-----+
| Name           | Database-name           | Schema-name           | Num-rows | Siz
e           |
+-----+-----+-----+-----+
+-----+
| table_mdihlhrzdy | tabular-industrious     | schema_abc           | 6400000  | 704
00000 |
+-----+-----+-----+-----+
+-----+
```

### table rename

This command renames a VAST Database table.

## Usage

```
table rename --database-name DATABASE
             --schema-name SCHEMA
             --name OLD_TABLE_NAME
             --new-name NEW_TABLE_NAME
             [--tenant-id TENANT]
```

## Required Parameters

--database-name DATABASE	Specifies the name of the database containing the schema.
--schema-name SCHEMA	Specifies the name of the schema containing the table.
--name OLD_TABLE_NAME	Specifies the name of the table being renamed.
--new-name NEW_TABLE_NAME	Specifies the new name for the table. The name must meet the requirements for S3 object names.

# Options

<code>--tenant-id TENANT</code>	Specifies the ID of the tenant where the database resides  If omitted, the default tenant is assumed.
---------------------------------	---

# Example

This example shows renaming a table named `cats` into `dogs`:

```
vcli: admin> table rename --name cats --schema-name schema1 --database_name vastdb --new-name dogs
```

## table show

This command shows details of a specific table in a VAST Database.

# Usage

```
table show --database-name DATABASE
           --schema-name SCHEMA
           --name TABLE
           [--tenant-id TENANT]
```

# Required Parameters

<code>--database-name DATABASE</code>	Specifies the name of the database containing the schema.
<code>--schema-name SCHEMA</code>	Specifies the name of the schema containing the table.
<code>--name NAME</code>	Specifies the name of a specific table.

# Options

<code>--tenant-id TENANT</code>	Specifies the ID of the tenant where the database resides  If omitted, the default tenant is assumed.
---------------------------------	---

## Example

```
vccli: admin> table show --database-name tabular --schema-name schema_jypxvnuobg --name table_jypxvnuobg
```

Name	table_jypxvnuobg
Database-name	tabular
Schema-name	schema_jypxvnuobg
Num-rows	10485760
Size	963000624

# tenant commands

## tenant alter-client-ip-ranges

This command adds or removes one or more client IP ranges for a tenant.

## Usage

```
tenant alter-client-ip-ranges --id TENANT_ID
                                [--client-ip-ranges-to-add IP_RANGES]
                                [--client-ip-ranges-to-remove IP_RANGES]
```

## Required Parameters

<code>--id TENANT_ID</code>	Specifies the tenant for which you want to add or remove client IP addresses.
-----------------------------	---

## Options

<code>--client-ip-ranges-to-add IP_RANGES</code>	<p>Adds one or more client IP ranges to the tenant configuration so that VAST Cluster allows access to tenant data from these IPs.</p> <p>Specify <code>IP_RANGES</code> as an array where ranges are separated by spaces and the start and end IP of each range is separated by a comma, for example:</p> <pre>192.0.2.0,192.0.2.2 2001:db8::69:1337:420:8153,2001:db8::69:1337:420:8200</pre>
<code>--client-ip-ranges-to-remove IP_RANGES</code>	<p>Removes one or more IPs from the tenant configuration so that VAST Cluster does not allow access to tenant data from these IPs.</p> <p>Specify <code>IP_RANGES</code> as an array where ranges are separated by spaces and the start and end IP of each range is separated by a comma, for example:</p> <pre>192.0.2.0,192.0.2.2 2001:db8::69:1337:420:8153,2001:db8::69:1337:420:8200</pre>

## Example

To allow access from IP range 2001:db8::69:1337:420:8153,2001:db8::69:1337:420:8200:

```
vcli: admin> tenant --alter-client-ip-ranges --id=3
               --client-ip-ranges-to-add 2001:db8::69:1337:420:8153,2001:db8::69:1337:420:8200
```

# tenant alter-encryption-group-state

If encryption is enabled with an external Encryption Key Manager (Thales Group CipherTrust Data Security Platform, Fortanix DSM, or HashiCorp Vault Enterprise), this command can deactivate, or reinstate, or irreversibly revoke and destroy, all encryption keys for an encryption group on an EKM.

When running this command, you specify one tenant. Keys are deactivated/reinstated/revoked for all tenants that share the same encryption group as the specified tenant. The encryption group to which each tenant belongs is identified by an identifier called the encryption CRN. You can display the encryption CRN per tenant with the [tenant list](#) command.

## Usage

```
tenant alter-encryption-group-state --id ID
                                   [--deactivate] | [--reinstall]
                                   [--revoke]
```

## Required Parameters

--id ID	Specifies a tenant.
---------	---------------------

## Options

-- deactivate	Deactivates all keys for the specified tenant's encryption group. When the keys are deactivated, data encrypted with those keys is no longer accessible.  After running the command with this option, the keys can be reinstated by running the command again with the --reinstall option.
-- reinstall	Reinstates keys deactivated by the --deactivate option for the specified tenant's encryption group.
--revoke	Revokes and irreversibly destroys all keys for the specified tenant's encryption group. Data encrypted with the revoked keys is no longer accessible.

## Examples

```
vccli: admin> tenant alter-encryption-group-state --id 4 --revoke

vccli: admin> tenant alter-encryption-group-state --deactivate --id 3
Tenants using this encryption group: tenant1.
Are you sure you want to deactivate tenant's encryption group? [y/N]
```

## tenant create

This command creates a tenant.

## Usage

```
tenant create --name NAME
               [--enable-privileged-domain-user-restore-access] | [--disable-privileged-domain-user-restore-access]
               [--enable-privileged-domain-group-backup-access] | [--disable-privileged-domain-group-backup-access]
               [--enable-privileged-domain-group-restore-access] | [--disable-privileged-domain-group-restore-access]
               [--privileged-domain-user-logon-name]
               [--privileged-domain-group-sid SID]
               [--local-administrators-group-name NAME]
               [--default-others-share-level-perm FULL|READ|CHANGE]
               [--encryption-group ENCRYPTION_GROUP]
               [--trash-gid TRASH_GID]
               [--client-ip-ranges IP_RANGES]
               [--posix-primary-provider AD|LDAP|NIS]
               [--login-name-primary-provider AD|LDAP|NIS]
               [--ad-provider-id ID]
               [--ldap-provider-id ID]
               [--nis-provider-id ID]
               [--enable-use-smb-native] | [--disable-use-smb-native]
               [--enable-require-smb-signing] | [--disable-require-smb-signing]
               [--allow-disabled-users] | [--prohibit-disabled-users]
               [--allow-locked-users] | [--prohibit-locked-users]
               [--enable-nfs-v4.2] | [--disable-nfs-v4.2]
               [--local-provider-id ID]
               [--preferred-owning-group PROTOCOL_BASED|POSIX_GID]
```

## Required Parameters

<code>--name NAME</code>	Specifies a name for the tenant.
--------------------------	----------------------------------


## Options


<code>--enable-privileged-domain-user-restore-access</code>	Enables the privileged SMB user.
<code>--disable-privileged-domain-user-restore-access</code>	Disables the privileged SMB user.
<code>--enable-privileged-domain-group-backup-access</code>	Enables the privileged SMB group.

<code>--disable-privileged-domain-group-backup-access</code>	Disables the privileged SMB group.
<code>--enable-privileged-domain-group-restore-access</code>	Enables read and write control access for the privileged SMB user group. Members of the group can perform backup and restore operations on all files and directories, without requiring read or write access to the specific files and directories.
<code>--disable-privileged-domain-group-restore-access</code>	Disables write control access for the SMB privileged user group. If enabled (see <code>--enable-privileged-domain-group-backup-access</code> ), the group has read control access. Members of the group can perform backup operations on all files and directories without requiring read access to the specific files and directories. They cannot perform restore operations without write access to the specific files and directories.
<code>--privileged-domain-user-login-name PRIVILEGED_USER_NAME</code>	An optional custom user name for the SMB or NFSv4.1 privileged user. If not set, the user name is 'vastadmin' in the cluster's joined domain.
<code>--privileged-domain-group-sid PRIVILEGED_DOMAIN_GROUP_SID</code>	Specify a custom group SID in order to have a working SMB or NFSv4.1 privileged group with backup operator privileges. If not set, the SMB privileged group is set to the Backup Operators domain group (S-1-5-32-551), which, due to a known issue, does not receive backup operator privileges.
<code>--local-administrators-group-name GROUP_NAME</code>	Specify a custom name for the privileged SMB group. If not specified, the privileged SMB group name is <i>Backup Operators</i> .
<code>--default-others-share-level-perm FULL READ CHANGE</code>	<p>Sets the default 'Everyone' Group SMB share-level permission for the tenant. This default permission affects all views in which share-level ACL is disabled.</p> <p>For more information about SMB share-level permissions, see <a href="#">Share-Level ACLs</a>.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li><code>FULL</code> (default). Grants all SMB users <i>full control</i> share-level access to views that have <i>Share-level ACL</i> disabled.</li> <li><code>READ</code>. Grants all SMB users <i>read</i> share-level access to views that have <i>Share-level ACL</i> disabled.</li> <li><code>CHANGE</code>. Grants all SMB users <i>change</i> share-level access to views that have <i>Share-level ACL</i> disabled.</li> </ul>
<code>--encryption-group</code>	If encryption is enabled on the cluster with external key management (EKM),



<p>ENCRYPTION_GROUP</p>	<p>enter a string identifier for the tenant's encryption group for encryption group management.</p> <p>You can optionally provide the same group for more than one tenant if you want to join multiple tenants to the same encryption group on the EKM. Tenants that belong to the same group will be managed by the same encryption key.</p> <p>Supply the group's Cloud Resource Name (CRN) identifier as ENCRYPTION_GROUP.</p> <p>Valid format: string, up to 128 characters</p> <p>An encryption group is required for tenant creation if EKM encryption is enabled.</p> <p>The encryption group cannot be changed after creating the tenant.</p> <p>For more information about EKM encryption, see <a href="#">Encryption of Data at Rest</a>.</p>
<p>--trash-gid TRASH_GID</p>	<p>If you want to allow access to the <a href="#">trash folder</a> for non-root NFSv3 users serviced by the tenant, specify this option and provide the GID of the user group that you want to use for this purpose as TRASH_GID. Users who belong to this group will have permission to move files into the trash folder.</p> <p>By default, the operation of moving files into the trash folder is supported for the root user only.</p>
<p>--client-ip-ranges IP_RANGES</p>	<p>Specifies an array of ranges of client IPs to be served by the tenant. Specify IP_RANGES as an array where ranges are separated by spaces and the start and end IP of each range is separated by a comma.</p> <p>For example: 10.10.10.2,10.10.10.4 2022:3::69:1337:420:8153,2022:3::69:1337:420:8200</p> <p>See <a href="#">Overview of Tenants</a> for more information about dedicating virtual IP pools to tenants and associating client IPs to a tenant.</p>
<p>--posix-primary-provider AD LDAP NIS</p>	<p>Specifies one provider to take precedence over other providers in case of any conflicts between attribute values when user information is retrieved from the providers.</p> <p>Applicable if more than one provider is enabled (see --ad-provider-id, --ldap-provider-id, nis-provider-id).</p>
<p>--login-name-primary-provider AD LDAP NIS</p>	<p>Determines which authorization provider is the primary provider for the user's login name.</p> <p>Applicable if more than one provider is enabled (see --ad-provider-id, --ldap-provider-id, nis-provider-id).</p>

<code>--ad-provider-id ID</code>	<p>Select which external authorization providers should be enabled for the tenant. Providers configured on the cluster are available for you to select up to one of each type (Active Directory, LDAP and NIS), subject to combination restrictions per tenant described in <a href="#">Authorization Providers in VAST Cluster</a>.</p> <p>Providers configured on the cluster are available for you to select up to one of each type (Active Directory, LDAP and NIS), subject to combination restrictions per tenant described in</p>
<code>--ldap-provider-id ID</code>	<p>Specify up to one LDAP server configuration by its ID in order to enable it for the tenant.</p> <p>Providers configured on the cluster are available for you to select up to one of each type (Active Directory, LDAP and NIS), subject to combination restrictions per tenant described in <a href="#">Authorization Providers in VAST Cluster</a>.</p>
<code>--nis-provider-id ID</code>	<p>Specify up to one NIS configuration by its ID in order to enable it for the tenant.</p> <p>Providers configured on the cluster are available for you to select up to one of each type (Active Directory, LDAP and NIS), subject to combination restrictions per tenant described in <a href="#">Authorization Providers in VAST Cluster</a>.</p>
<code>--enable-use-smb-native</code>	<p>When this option is specified, VAST Cluster authorizes client access by using user and group information supplied via Kerberos or NTLM authentication, rather than by querying that user in Active Directory. For more information, see <a href="#">Authentication for SMB Access</a>.</p>
<code>--disable-use-smb-native</code>	<p>Disables use of Kerberos or NTLM authentication to authorize SMB client access. This is the default setting.</p> <div>  <p><b>Note</b></p> <p>After you disable use of Kerberos/NTLM Authentication to authorize users from non-trusting domains, users that previously had access, would still have access although the feature is now disabled.</p> </div>
<code>--enable-require-smb-signing</code>	<p>When specified, SMB clients are required to sign SMB requests. SMB requests with missing or invalid signatures are not accepted.</p>
<code>--disable-require-smb-signing</code>	<p>When specified, SMB clients are not required to sign SMB requests.</p>

<code>--allow-disabled-users</code>	<p>Allows IO to be performed on the cluster by users whose accounts are disabled in Active Directory.</p> <p>By default, if the user's account is disabled in Active Directory by an administrator, the user is blocked from performing IO on the cluster. This setting overrides the default behavior.</p>
<code>--prohibit-disabled-users</code>	<p>Restores default behavior, where users whose accounts are disabled in Active Directory are blocked from performing IO on the cluster.</p>
<code>--allow-locked-users</code>	<p>Allows IO to be performed on the cluster by users whose accounts are automatically locked out in Active Directory by account lockout policies. Active Directory account lockout policies determine when and for how long users are automatically locked out after invalid login attempts.</p> <p>By default, if the user's account is locked out by Active Directory lockout policies, the user is blocked from performing IO on the cluster. This setting overrides the default behavior.</p>
<code>--prohibit-locked-users</code>	<p>Restores default behavior, where users whose accounts are locked out by Active Directory lockout policies are blocked from performing IO on the cluster.</p>
<code>--enable-nfs-v4.2</code>	<p>Enables support of NFS version 4.2 for this tenant.</p> <div>  <p><b>Tip</b></p> <p>Specify this option if you want to let your clients use the <a href="#">NFSv4.2 Security Labels</a> capability.</p> </div>
<code>--disable-nfs-v4.2</code>	<p>Disables support of NFS version 4.2 for this tenant.</p>
<code>--local-provider-id ID</code>	<p>Specifies a local provider with which the tenant is associated. If not specified, the default tenant is used.</p>
<code>--preferred-owning-group PROTOCOL_BASED POSIX_GID</code>	<p>Controls the way VAST Cluster sets the owning group when creating files on a view controlled with the SMB and Mixed Last Wins security flavor:</p> <ul style="list-style-type: none"> <li>• <b>PROTOCOL_BASED (default):</b> The owning group is determined based on the access protocol: <ul style="list-style-type: none"> <li>◦ For SMB, the <code>primaryGroupID</code> of the user</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>◦ For NFS, the POSIX GID of the user</li> <li>• <code>POSIX_GID</code>: The owning group is determined based on the POSIX GID of the user.</li> </ul>
--	--

## Example

```

vcli: admin> tenant create --name Tenant1 --client-ip-ranges 10.10.10.2,10.10.10.4 11.11.11.2,11.11.11.4
--posix-primary-provider AD --ad-provider-id 1 --nis-provider-id 1 --localprovider 1

```

### tenant delete

This command deletes a tenant. When a tenant is deleted, the tenant's directory is deleted. If the directory contains data, the tenant cannot be deleted, unless the `--force` flag is supplied with the command.

## Usage

```

tenant delete --id ID
               [--force]

```

## Required Parameters

<code>--id ID</code>	Specifies which tenant to delete.
----------------------	-----------------------------------

## Options

<code>--force</code>	Forces deletion of the tenant, even if files exist in the tenant directory.
----------------------	---

## Example

```

vcli: admin> tenant delete --id 1
Are you sure you want to delete the Tenant? [y/N] y

```

### tenant list

This command displays all tenants and their configurations.

## Usage

```

tenant list [--name NAME]

```

# Example

```

vcli: admin> tenant list
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name      | Enable privileged domain user restore access | Logon name of the privileged
domain user | Enable privileged domain group backup access | Enable privileged domain group r
estore access | SID of the privileged domain group | Local administrators group name | Defaul
t others share level ACL | Trash folder GID | AD provider ID | Open LDAP provider ID | NIS pr
ovider ID | Encryption CRN | Posix Primary Provider | Login Name Primary Provider | Client IP
ranges | VIP Pools                                     | Use native SMB authentication
|
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 3 | bgio      | True                                         |                               |                               |
| True                                         |                               |                               |                               |
| 0                                           | None                         | None                         | None                         | None                         | FULL
| NONE                                         | NONE                         |                               | []                           | ['bgio-non-rdma',
'bgio-rdma']
| 1 | default  | True                                         |                               |                               |
| True                                         |                               | True                         |                               |                               |
| 0                                           | 1                           | None                         | None                         | None                         | FULL
| AD                                           | NONE                         |                               | []                           | ['vipool-1', 'vi
ppool-comet', 'vipool-comet-rdma'] | False
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

## tenant list-remote

This command displays a list of remote tenants.

## Usage

```

tenant list--remote [--name NAME]
                    [--peer-id ID]

```

## Options

--name NAME	Filters the list of remote tenants by tenant name.
-------------	--

<code>--peer-id ID</code>	Filters the list of remote tenants by peer ID.
---------------------------	--

## tenant modify

This command modifies a tenant.

## Usage

```
tenant modify --id ID
                [--enable-privileged-domain-user-restore-access] [--disable-privileged-domain-user-restore-access]
                [--enable-privileged-domain-group-backup-access] [--disable-privileged-domain-group-backup-access]
                [--enable-privileged-domain-group-restore-access] [--disable-privileged-domain-group-restore-access]
                [--privileged-domain-user-logon-name]
                [--privileged-domain-user-logon-name]
                [--privileged-domain-group-sid SID]
                [--local-administrators-group-name NAME]
                [--default-others-share-level-perm FULL|READ|CHANGE]
                [--trash-gid TRASH_GID]
                [--client-ip-ranges IP_RANGES]
                [--posix-primary-provider AD|LDAP|NIS]
                [--login-name-primary-provider AD|LDAP|NIS]
                [--ad-provider-id ID]
                [--detach-ad-provider]
                [--ldap-provider-id ID]
                [--detach-ldap-provider]
                [--nis-provider-id ID]
                [--detach-nis-provider]
                [--enable-use-smb-native|--disable-use-smb-native]
                [--enable-require-smb-signing|--disable-require-smb-signing]
                [--enable-nfs-v4.2] [--disable-nfs-v4.2]
                [--local-provider-id ID]
                [--preferred-owning-group PROTOCOL_BASED|POSIX_GID]
```

## Required Parameters

<code>--id ID</code>	Specifies which tenant to modify.
----------------------	-----------------------------------


## Options


<code>--enable-privileged-domain-user-restore-access</code>	Enables the privileged SMB user.
<code>--disable-privileged-domain-user-restore-access</code>	Disables the privileged SMB user.

<code>--enable-privileged-domain-group-backup-access</code>	Enables the privileged SMB group.
<code>--disable-privileged-domain-group-backup-access</code>	Disables the privileged SMB group.
<code>--enable-privileged-domain-group-restore-access</code>	Enables read and write control access for the privileged SMB user group. Members of the group can perform backup and restore operations on all files and directories, without requiring read or write access to the specific files and directories.
<code>--disable-privileged-domain-group-restore-access</code>	Disables write control access for the SMB privileged user group. If enabled (see <code>--enable-privileged-domain-group-backup-access</code> ), the group has read control access. Members of the group can perform backup operations on all files and directories without requiring read access to the specific files and directories. They cannot perform restore operations without write access to the specific files and directories.
<code>--privileged-domain-user-logon-name PRIVILEGED_USER_NAME</code>	An optional custom user name for the SMB or NFSv4.1 privileged user. If not set, the user name is 'vastadmin' in the cluster's joined domain'.
<code>--privileged-domain-group-sid PRIVILEGED_DOMAIN_GROUP_SID</code>	Specify a custom group SID in order to have a working SMB or NFSv4.1 privileged group with backup operator privileges. If not set, the SMB privileged group is set to the Backup Operators domain group (S-1-5-32-551), which, due to a known issue, does not receive backup operator privileges.
<code>--local-administrators-group-name GROUP_NAME</code>	Specify a custom name for the privileged SMB group. If not specified, the privileged SMB group name is <i>Backup Operators</i> .
<code>--default-others-share-level-perm FULL READ CHANGE</code>	<p>Sets the default 'Everyone' Group SMB share-level permission for the tenant. This default permission affects all views in which share-level ACL is disabled.</p> <p>For more information about SMB share-level permissions, see <a href="#">Share-Level ACLs</a>.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li><code>FULL</code> (default). Grants all SMB users <i>full control</i> share-level access to views that have <i>Share-level ACL</i> disabled.</li> <li><code>READ</code>. Grants all SMB users <i>read</i> share-level access to views that have <i>Share-level ACL</i> disabled.</li> <li><code>CHANGE</code>. Grants all SMB users <i>change</i> share-level access to views that have</li> </ul>

	<i>Share-level ACL disabled.</i>
<code>--trash-gid TRASH_GID</code>	<p>If you want to allow access to the <a href="#">trash folder</a> for non-root NFSv3 users serviced by the tenant, specify this option and provide the GID of the user group that you want to use for this purpose as <code>TRASH_GID</code>. Users who belong to this group will have permission to move files into the trash folder.</p> <p>By default, the operation of moving files into the trash folder is supported for the root user only.</p>
<code>--client-ip-ranges IP_RANGES</code>	<p>Specifies an array of ranges of client IPs to be served by the tenant. Specify <code>IP_RANGES</code> as an array where ranges are separated by spaces and the start and end IP of each range is separated by a comma.</p> <p>For example: <code>10.10.10.2,10.10.10.4</code>  <code>2022:3::69:1337:420:8153,2022:3::69:1337:420:8200</code></p> <p>See <a href="#">Overview of Tenants</a> for more information about dedicating virtual IP pools to tenants and associating client IPs to a tenant.</p>
<code>--posix-primary-provider</code> <code>AD LDAP NIS</code>	<p>Specifies one provider to take precedence over other providers in case of any conflicts between attribute values when user information is retrieved from the providers.</p> <p>Applicable if more than one provider is enabled (see <code>--ad-provider-id</code>, <code>--ldap-provider-id</code>, <code>nis-provider-id</code>)</p>
<code>--login-name-primary-provider</code> <code>AD LDAP NIS</code>	<p>Determines which authorization provider is the primary provider for the user's login name.</p> <p>Applicable if more than one provider is enabled (see <code>--ad-provider-id</code>, <code>--ldap-provider-id</code>, <code>nis-provider-id</code>).</p>
<code>--ad-provider-id ID</code>	<p>Specify up to one Active Directory configuration by its ID in order to enable it for the tenant.</p> <p>Providers configured on the cluster are available for you to select up to one of each type (Active Directory, LDAP and NIS), subject to combination restrictions per tenant described in <a href="#">Authorization Providers in VAST Cluster</a>.</p>
<code>--detach-ad-provider</code>	Detaches a previously connected Active Directory provider from the tenant.
<code>--ldap-provider-id ID</code>	Specify up to one LDAP server configuration by its ID in order to enable it for the tenant.



	Providers configured on the cluster are available for you to select up to one of each type (Active Directory, LDAP and NIS), subject to combination restrictions per tenant described in <a href="#">Authorization Providers in VAST Cluster</a> .
<code>--detach-ldap-provider</code>	Detaches a previously connected LDAP provider from the tenant.
<code>--nis-provider-id ID</code>	Specify up to one NIS configuration by its ID in order to enable it for the tenant.  Providers configured on the cluster are available for you to select up to one of each type (Active Directory, LDAP and NIS), subject to combination restrictions per tenant described in <a href="#">Authorization Providers in VAST Cluster</a> .
<code>--detach-nis-provider</code>	Detaches a previously connected NIS provider from the tenant.
<code>--enable-use-smb-native</code>	When this option is specified, VAST Cluster authorizes client access by using user and group information supplied via Kerberos or NTLM authentication, rather than by querying that user in Active Directory. For more information, see <a href="#">Authentication for SMB Access</a> .
<code>--disable-use-smb-native</code>	Disables use of Kerberos or NTLM authentication to authorize SMB client access. This is the default setting.  <div>  <div> <p><b>Note</b></p> <p>After you disable use of Kerberos/NTLM Authentication to authorize users from non-trusting domains, users that previously had access, would still have access although the feature is now disabled.</p> </div> </div>
<code>--enable-require-smb-signing</code>	When specified, SMB clients are required to sign SMB requests. SMB requests with missing or invalid signatures are not accepted.
<code>--disable-require-smb-signing</code>	When specified, SMB clients are not required to sign SMB requests.
<code>--enable-nfs-v4.2</code>	Enables support of NFS version 4.2 for this tenant.

	 <b>Tip</b> Specify this option if you want to let your clients use the <a href="#">NFSv4.2 Security Labels</a> capability.
<code>--disable-nfs-v4.2</code>	Disables support of NFS version 4.2 for this tenant.
<code>--local-provider-id ID</code>	Specifies a local provider with which the tenant is associated.
<code>--preferred-owning-group PROTOCOL_BASED POSIX_GID</code>	Controls the way VAST Cluster sets the owning group when creating files on a view controlled with the SMB and Mixed Last Wins security flavor: <ul style="list-style-type: none"> <li>• <code>PROTOCOL_BASED</code> (default): The owning group is determined based on the access protocol: <ul style="list-style-type: none"> <li>◦ For SMB, the <code>primaryGroupID</code> of the user</li> <li>◦ For NFS, the POSIX GID of the user</li> </ul> </li> <li>• <code>POSIX_GID</code>: The owning group is determined based on the POSIX GID of the user.</li> </ul>

## Example

```

vcli: admin> tenant modify --id 3
--client-ip-ranges 10.10.10.1,10.10.10.9 10.10.10.200,10.10.10.240

--detach-ad-provider

--ldap-provider-id 2

```

### tenant rotate-encryption-group-key

If encryption is enabled with encryption type `CIPHER_TRUST_KMIP` (where encryption keys are managed externally on Thales Group CipherTrust Data Security Platform), this command rotates the key encryption key for the encryption group to which a given tenant belongs. The key encryption key is used by the cluster to retrieve the data encryption key from the EKM when needed to encrypt data. Rotating the key encryption key generates a new version of the key encryption key, with the same key name and attributes.

## Usage

```
tenant rotate-encryption-group-key --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies a tenant.
----------------------	---------------------

## Example

```
vcli: admin> tenant rotate-encryption-group-key --id 5
Tenants using this encryption group: tenant_1.
Are you sure you want to rotate tenant's encryption group key? [y/N] y
Tenant's encryption group key was rotated successfully.
```

### tenant show

This command displays details of a specific tenant.

## Usage

```
tenant show --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which tenant to display.
----------------------	------------------------------------

## Example

```
vcli: admin> tenant show --id 1
+-----+
+-----+
+
| ID                      | 1
|
| Name                    | default
|
| Enable privileged domain user restore access | True
|
| Logon name of the privileged domain user      |
|
| Enable privileged domain group backup access  | True
|
| Enable privileged domain group restore access | True
|
| SID of the privileged domain group            |
|
| Local administrators group name              |
|
| Default others share level ACL                | FULL
|
| Trash folder GID                            | 0
|
```

AD provider ID	1
Open LDAP provider ID	None
NIS provider ID	None
Encryption CRN	
Posix Primary Provider	AD
Login Name Primary Provider	NONE
Client IP ranges	[]
Use SMB native authentication	False
VIP Pools IP ranges	['172.19.122.232 - 172.19.122.247', '172.19.122.212 - 172.19.122.227', '172.19.122.1 - 172.19.122.16']

-----

+

# topic commands

## topic create

This command creates a topic for event publishing.

## Usage

```
topic create --database-name NAME
             --name NAME
             --topic-partitions COUNT
             [--retention-ms MILLISECONDS]
             [--message-timestamp-type CreateTime|LogAppendTime]
             [--message-timestamp-before-max-ms MILLISECONDS]
             [--message-timestamp-after-max-ms MILLISECONDS]
```

## Required Parameters

<code>--database-name NAME</code>	The name of the database where the topic is to be created.
<code>--name NAME</code>	The name of the topic to be created.
<code>--topic-partitions</code>	The number of partitions in the topic to be created.  Each partition can hold up to 1000 topics. The number of partitions in a topic cannot be changed after the topic has been created.

## Options

<code>--retention-ms MILLISECONDS</code>	The amount of time, in milliseconds, to keep an event record in the topic. When the retention period for a record expires, the records is deleted from the topic.
<code>--message-timestamp-type CreateTime LogAppendTime</code>	Determines how the event timestamp is set: <ul style="list-style-type: none"><li>• <code>CreateTime</code> (default): The timestamp is based on the time when the event was encountered at the event producer.</li><li>• <code>LogAppendTime</code>: The timestamp is based on the time when the event record was added to the log at the event broker.</li></ul>
<code>--message-timestamp-</code>	If the message timestamp type is set to <code>CreateTime</code> , specify this option to determine

before-max-ms MILLISECONDS	how much earlier the message timestamp can be than the broker timestamp. If this value is exceeded, the message is rejected.
--message-timestamp- after-max-ms MILLISECONDS	If the message timestamp type is set to <code>CreateTime</code> , specify this option to determine how much later the message timestamp can be than the broker timestamp. If this value is exceeded, the message is rejected.

## Example

To create a topic named `mytopic` with 30 partitions in the `kafkatopics` database:

```
vcli: admin> topic create --database-name kafkatopics --name mytopic --partitions 30
```

### topic modify

This command modifies a topic.

## Usage

```
topic modify --database-name NAME
             --name NAME
             [--new-name NEW_NAME]
             [--retention-ms MILLISECONDS]
             [--message-timestamp-type CreateTime|LogAppendTime]
             [--message-timestamp-before-max-ms MILLISECONDS]
             [--message-timestamp-after-max-ms MILLISECONDS]
```

## Required Parameters

--database-name NAME	The name of the database where the topic resides.
--name NAME	The name of the topic to be modified.

## Options

--new-name NEW_NAME	This option lets you rename an existing topic.
--retention-ms MILLISECONDS	The amount of time, in milliseconds, to keep an event record in the topic. When the retention period for a record expires, the records is deleted from the topic.

<pre>--message-timestamp-type CreateTime LogAppendTime</pre>	<p>Determines how the event timestamp is set:</p> <ul style="list-style-type: none"> <li>• <b>CreateTime</b> (default): The timestamp is based on the time when the event was encountered at the event producer.</li> <li>• <b>LogAppendTime</b>: The timestamp is based on the time when the event record was added to the log at the event broker.</li> </ul>
<pre>--message-timestamp- before-max-ms MILLISECONDS</pre>	<p>If the message timestamp type is set to <b>CreateTime</b>, specify this option to determine how much earlier the message timestamp can be than the broker timestamp. If this value is exceeded, the message is rejected.</p>
<pre>--message-timestamp- after-max-ms MILLISECONDS</pre>	<p>If the message timestamp type is set to <b>CreateTime</b>, specify this option to determine how much later the message timestamp can be than the broker timestamp. If this value is exceeded, the message is rejected.</p>

## Example

To set the message timestamp type to **LogAppendTime**:

```

vcli: admin> topic modify --database-name kafkatopics --name mytopic --message-timestamp-type
LogAppendTime

```

### topic delete

This command deletes a topic.

## Usage

```

topic delete --database-name NAME
             --name NAME

```

## Required Parameters

<code>--database-name NAME</code>	The name of the database where the topic is to be deleted.
<code>--name NAME</code>	The name of the topic to be deleted.

## Example

To delete a topic named **mytopic** from the **kafkatopics** database:

```
vcli: admin> topic delete --database-name kafkatopics --name mytopic
```

## topic list

This command lists event topics.

## Usage

```
topic list [--database-name NAME]
           [--name NAME]
           [--page-size COUNT]
           [--page PAGE_NO]
```

## Options

<code>--database-name NAME</code>	Filters the output by name of the database where the topic resides.
<code>--name NAME</code>	Filters the output by topic name.
<code>--page-size COUNT</code>	Sets the maximum number of topics per page in the output. The default value is 100.
<code>--page PAGE_NO</code>	If the page size limit is set, displays the page specified by its page number. The default value is 1.

## topic show

This command shows a topic.

## Usage

```
topic show --database-name NAME
           --name NAME
```

## Required Parameters

<code>--database-name NAME</code>	The name of the database where the topic resides.
<code>--name NAME</code>	The name of the topic to be displayed.



# user commands

## user add

This command lets you manually add a user to the local provider and, optionally, grant S3 permissions to the users.



### Tip

The newly created user needs an S3 access key pair to be able to create or access S3 buckets. Run `user generate-key` to generate a key pair. To enable the key pair, run `user modify-key`.

## Usage

```
user add --name NAME
        --uid UID
        [--leading-group-gid LEADING_GID]
        [--groups-gids GIDs]
        [--allow-create-bucket|--disallow-create-bucket]
        [--allow-delete-bucket|--disallow-delete-bucket]
        [--s3-superuser|--not-s3-superuser]
        [--identity-policies-ids IDs]
        [--local-provider-id ID]
```

## Required Parameters

<code>--name NAME</code>	Sets the user's name.
<code>--uid UID</code>	Specifies the user's POSIX (NFS) UID attribute.

## Options

<code>--leading-group-gid LEADING_GID</code>	<p>The group ID (GID) of the user's leading group.</p> <p>The leading group is the owning group of any files created by the user.</p> <p>If no local group with the specified GID exists, it is created.</p> <p>For example: <code>--leading-gid 44</code></p>
<code>--groups-gids GIDs</code>	<p>The group IDs (GIDs) of groups to which the user belongs.</p> <p>Enter the GIDs as a comma-separated list. The first group listed is the default leading group.</p>

	For example: <code>--gids 5,65,102,170</code>
<code>--allow-create-bucket</code>	Allows the user to create buckets when connecting to the cluster via S3.
<code>--disallow-create-bucket</code>	Prohibits the user to create buckets when connecting to the cluster via S3.
<code>--allow-delete-bucket</code>	Allows the user to delete buckets when connecting to the cluster via S3.
<code>--disallow-delete-bucket</code>	Prohibits the user to delete buckets when connecting to the cluster via S3.
<code>--s3-superuser</code>	Grants the user S3 super user permission, which enables the user to override S3 ACLs.
<code>--not-s3-superuser</code>	Removes S3 super user permission from the user.
<code>--identity-policies-ids IDs</code>	Assigns one or more S3 identity policies to the user. Specify a comma-separated list of policy IDs.
<code>--local-provider-id ID</code>	Specifies a local provider with which the tenant is associated. If not specified, the default provider is used.

## user copy

This command copies users from one local provider to another.

## Usage

```
user copy --destination-provider-id ID
          [--tenant-id TENANT]
          [--user-ids USERS]
```

## Required Parameters

<code>--destination-provider-id ID</code>	Specifies the local provider to which the users are copied. Cannot be the default provider.
---	---

## Options

<code>--tenant-id TENANT</code>	Specifies the tenant containing the provider and users. This parameter cannot be included if <code>--user-ids</code> is included. If included, then all users with s3 access keys for this tenant are copied.
<code>--user-ids USERS</code>	Specifies a list of a users to copy. This parameter cannot be included if <code>--tenant-id</code> is included.

## Example

This example copies three users (IDs 10, 11, 12) from one local provider (ID 1) to another (ID 2)

```
vccli: admin> user copy --destination-provider-id 2 --user-ids 10, 11, 12
```

This example copies all users from a tenant (ID 7)

```
vccli: admin> user copy --destination-provider-id 2 --tenant-id 7
```

### user generate-key

This command generates an S3 access key pair for a user. The access key pair comprises an access key and a secret key. The access key and secret key are displayed in the command output. The secret key cannot be displayed again. Copy the secret key and keep it safe for usage.

When enabling, disabling or removing an access key pair, you specify only the access key.

When generating the keys for a local provider user, you can specify the user's ID or another attribute. When generating the keys for an external provider user, specify a UID, SID, username or login name.

## Usage

```
user generate-key [--id ID]|[--uid UID]|[--sid SID]|[--username USERNAME]|[--login-name LOGIN_NAME]
                  [--tenant-id ID]
```

## Required Parameters

<code>--id ID</code>	Identifies a local provider user by VAST ID.
<code>--uid UID</code>	Identifies a user by POSIX (NFS) UID number.
<code>--sid SID</code>	Identifies a user by Security Identifier (SID).

<code>--username USERNAME</code>	Identifies a user by user name.
<code>--login-name LOGIN_NAME</code>	Identifies a user by login name.

## Options

<code>--tenant-id ID</code>	Specify the ID of the tenant with which the user is associated.  The tenant ID is used only to look up the user. The generated key pair enables access to the default tenant only.
-----------------------------	--

## Example

This example shows generating an access key pair for the local provider user with VAST ID 200.

```

vcli: admin> user generate-key --id 200
{'access_key': '2h/MzqtiTQSVl8J/4wsDbg==',
 'secret_key': 'dzd0eX/+d+IqGRHy5EJgoVde656+A1NpHGHHHcL+5mE='}

```

### user list

This command displays all users on the local provider. To retrieve details of other users, use `user query`.

## Usage

```
user list
```

## Example

```

vcli: admin> user list
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+
| ID | Name | UID | SID | Leading-Group | Leading-Group-GID | Groups | Group-count | Access-keys | Create-Bucket | Delete-Bucket | S3-Superuser |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 16 | abcdef | 1133659114 | S-1-111-1624147990-1599182510-3870292919-110815442-17 | None | None | [] | 0 | [] | False | False | False |
| 17 | ghijkl | 997730826 | S-1-111-1624147990-1599182510-3870292919-110815442-18 | None | None | [] | 0 | [] | False | False | False |
| 8 | mnopqr | 702512003 | S-1-111-1624147990-1599182510-3870292919-110815442-9 | None | None | [] | 0 | [] | False | False | False |

```

## user modify



### Note

## Usage

## Required Parameters

## Options



	For example: <code>--leading-gid 44</code>
<code>--groups-gids GIDS</code>	<p>Alters the list of groups to which the user belongs.</p> <p>Enter the groups IDs (GIDs) as a comma-separated list. Include all GIDs that should be associated with the user entry.</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p style="text-align: center;"><b>Caution</b></p> <p>Any GIDs that were defined in the entry previously will be removed if they are not included.</p> </div> <p>For example: <code>--gids 5,65,102,170</code></p>
<code>--allow-create-bucket</code>	Allows the user to create buckets when connecting to the cluster via S3.
<code>--disallow-create-bucket</code>	Prohibits the user to create buckets when connecting to the cluster via S3.
<code>--allow-delete-bucket</code>	Allows the user to delete buckets when connecting to the cluster via S3.
<code>--disallow-delete-bucket</code>	Prohibits the user to delete buckets when connecting to the cluster via S3.
<code>--s3-superuser</code>	Grants the user S3 super user permission, which enables the user to override S3 ACLs.
<code>--not-s3-superuser</code>	Removes S3 super user permission from the user.
<code>--identity-policies-ids IDs</code>	<p>Assigns one or more S3 identity policies to the user.</p> <p>Specify a comma-separated list of policy IDs.</p>
<code>--local-provider-id ID</code>	Specifies a local provider with which the tenant is associated.

## user modify-key

This command enables or disables an S3 access key pair. An access key pair consists of a secret key and an access key. The

access key pair is enabled/disabled by specifying the access key in the pair.

# Usage

```
user modify-key {--id ID | --uid UID | --sid SID}  
               --access-key ACCESS-KEY  
               [--enable|--disable]  
               [--tenant-id ID]
```

# Required Parameters

<code>--id ID</code>	Identifies a local provider user by VAST ID.
<code>--uid UID</code>	Identifies a user by POSIX (NFS) UID number.
<code>--sid SID</code>	Identifies a user by Security Identifier (SID).
<code>--access-key ACCESS-KEY</code>	Specifies an S3 access key to disable or enable the key pair.

# Options

<code>--enable</code>	Enables the S3 access key pair.
<code>--disable</code>	Disables the S3 access key pair.
<code>--tenant-id ID</code>	Specify the ID of the tenant with which the user is associated.

# Example

This example shows disabling an access key pair.

```
vccli: admin> user modify-key --id 4 --access-key NHZ9GBLYS21TST3BGQXO --disable  
Are you sure you want to disable this access key [NHZ9GBLYS21TST3BGQXO]? [y/N] y
```

## user query

This command queries providers and the user database for a user entry. A provider query can be aggregated across providers to yield a merged result, or it can be provider-specific. See [Querying Users](#) for more information.

You can also use this command to:

- Attach S3 identity policies to users or remove S3 identity policies from users, and
- Grant or remove create bucket, delete bucket and super user permissions for users on external providers.



### Note

Permission allowed or denied by identity policies to create or delete buckets overrides explicit create bucket and delete bucket permission settings.



### Note

To grant or remove the explicit create bucket, delete bucket and super user permissions for local provider users, use the [user modify](#) command.

## Usage for Retrieving a User Entry

```
user query {--uid UID | --username USERNAME | --login-name LOGINNAME | --sid SID}
           [--context local|udb|ad|ldap|nis|aggregated]
           [--tenant-id ID]
```

## Usage for Setting S3 Permissions

```
user query {--uid UID | --username USERNAME | --login-name LOGINNAME | --sid SID}
           [--allow-create-bucket|--disallow-create-bucket]
           [--allow-delete-bucket|--disallow-delete-bucket]
           [--s3-superuser|--not-s3-superuser]
           [--identity-policies-ids [IDs]]
           [--tenant-id ID]
```

## Required Parameters

--uid UID	Identifies a user by POSIX (NFS) UID number.
--username USERNAME	identifies a user by user name.
--login-name LOGINNAME	Identifies a user by login name.
--sid SID	Identifies a user by Security Identifier (SID).



## Options

<pre>--context local udb ad ldap nis aggregated</pre>	<p>Specify one of the following contexts:</p> <ul style="list-style-type: none"> <li>• local. Restricts the search to local provider users.</li> <li>• udb. Searches the UDB for the user. The output in this case includes the VAST ID (VID) for the user, which can be used when specifying a grantee in S3 ACLs.</li> <li>• aggregated (default). Searches all providers and returns a merged user entry. In case of conflicts between providers, attributes are resolved according to the following rules: <ul style="list-style-type: none"> <li>◦ In case of conflict between local and non local providers, the local provider's attributes override those of the other providers.</li> <li>◦ In case of conflicting POSIX attributes on external providers, the POSIX primary provider overrules the other external provider.</li> <li>◦ Users are merged if their match user attributes match. The match user attribute is configurable in that you can set which attribute on the POSIX primary provider is used to match the users.</li> <li>◦ All groups found for the user on all providers with distinct group names are treated as distinct groups to which the user belongs. Groups are merged if they match according to a non-configurable group name attribute.</li> </ul> </li> <li>• ad, nis or ldap. Searches the specific provider only. (Each of these options appears only if a provider of that type is connected to the cluster.)</li> </ul>
<pre>--allow-create-bucket</pre>	Allows the user to create buckets when connecting to the cluster via S3.
<pre>--disallow-create-bucket</pre>	Prohibits the user to create buckets when connecting to the cluster via S3.
<pre>--allow-delete-bucket</pre>	Allows the user to delete buckets when connecting to the cluster via S3.
<pre>--disallow-delete-bucket</pre>	Prohibits the user to delete buckets when connecting to the cluster via S3.
<pre>--s3-superuser</pre>	Grants the user S3 super user permission, which enables the user to override S3 ACLs.
<pre>--not-s3-superuser</pre>	Removes S3 super user permission from the user.

<pre>--identity-policies-ids [IDs]</pre>	<p>Assigns one or more S3 identity policies to the user.</p> <p>Specify IDs as a comma-separated list of S3 identity policy IDs.</p> <p>Each time you run the command with this option, the list overrides the entire previous list of S3 identity policies that were attached to the user. To remove a policy from a user, specify a list that does not include the policy you wish to remove. To remove all policies from the user, do not specify a list of IDs.</p>
<pre>--tenant-id ID</pre>	<p>Specify the ID of the tenant with which the user is associated.</p>

## Example

```
vcli: admin> user query --uid 1000
+-----+
+-----+
| uid           | 1000 (LDAP) |
| sid           |              |
| leading_group  | {'gid': 10000, 'sid': -1, 'name': -1} (LDAP) |
| leading_group_name | -1          |
| leading_group_gid | 10000       |
| primary_group_name | -1          |
| primary_group_sid | -1          |
| name           | test-user-1000 (LDAP) |
| login_name      | test-user-1000 |
| historical_sids  | []          |
| groups          | [] ([])     |
| group_count     | 0           |
| allow_create_bucket | True        |
| allow_delete_bucket | True        |
| s3_superuser     | False       |
| s3_policies      | []          |
| s3_policies_ids  | []          |
| s3_remote_policies | []          |
| access_keys      | []          |
| origins          | {'uid': 'LDAP', 'leading_group': 'LDAP', 'name': 'LDAP', 'groups': []} |
| user_qos_policies | []          |
| quotas          | []          |
```


```
|
| s3_vid          | None
|
+-----+
+-----+
```

In the command output:

- The provider from which an attribute was retrieved is indicated in parentheses ( `(LDAP)` in the example).
- *leading group* is the POSIX attribute for the user's group(s). A leading group is identified with its group ID (GID).
- *primary group* is an Active Directory group identified by its security identifier (SID).
- `-1` is returned for fields where an empty string was retrieved from the provider.

user query-by-prefix

This command queries Active Directory domains for users by name prefix. It returns identifiers for users whose names share a specified prefix.



Tip

The identifier for a given user can be provided in a [view modify](#) command as `--share-ace-identifier` in order to configure an share-level ACE for the user.

Usage

```
user  query-by-prefix --fqdn FQDN|ALL
                        --prefix PREFIX
                        [--active-directory-id ID]
                        [--tenant-id ID]
```

Required Parameters

--fqdn FQDN ALL	Specifies either a specific fully qualified domain name of a joined Active Directory domain or 'ALL' to query all AD domains to which the cluster is joined.
--prefix PREFIX	Specifies a string prefix to query for users on the specified domain.

Options

--active-directory-id ID	Specifies the ID of Active Directory configuration under which user domains are searched for.
-----------------------------	---



```
[--username NAME]
[--login-name NAME]
```

## Required Parameters

<code>--uid UID</code>	Queries providers for a user with the specified POSIX (NFS) UID.
<code>--sid SID</code>	Queries providers for a user with the specified Security Identifier (SID).

## Options

<code>--tenant-id ID</code>	Queries providers for a user associated with the specified tenant.
<code>--username NAME</code>	Queries providers for the specified user name.
<code>--login-name NAME</code>	Queries providers for the specified login name.

## Example

```
vccli: admin> user refresh --uid 1000
```

### user remove-key

This command removes an S3 access key pair.

## Usage

```
user remove-key {--id ID | --uid UID | --sid SID}
                --access-key ACCESS-KEY
                [--tenant-id ID]
```

## Required Parameters

<code>--id ID</code>	Identifies a local provider user by VAST ID.
<code>--uid UID</code>	Identifies a user by POSIX (NFS) UID number.

<code>--sid SID</code>	Identifies a user by Security Identifier (SID).
<code>--access-key ACCESS-KEY</code>	Specifies an S3 access key to remove the key pair.

## Options

<code>--tenant-id ID</code>	Specify the ID of the tenant with which the user is associated.
-----------------------------	---

## Example

```
vcli: admin> user remove-key --id 4 --access-key NHZ9GBLYS21TST3BGQXO
Are you sure you want to remove this access key [NHZ9GBLYS21TST3BGQXO]? [y/N] y
```

# userquota commands

## userquota create

This command creates a user or group quota rule for a specific directory quota.

## Usage

```
userquota create --identifier-type username|groupname|uid|gid
                 --identifier IDENTIFIER
                 --quota-id QUOTA_ID
                 --user|--group
                 [--grace-period]
                 [--soft-limit]
                 [--hard-limit]
                 [--hard-limit-inodes]
                 [--soft-limit-inodes]
```

## Required Parameters

<code>--identifier-type</code> <code>username groupname uid gid</code>	Specify how you want to identify the user or group for which a quota is create: <ul style="list-style-type: none"><li>• <code>username</code>. By the name of the user.</li><li>• <code>groupname</code>. By the name of the group.</li><li>• <code>uid</code>, By the user's UID.</li><li>• <code>gid</code>. By the group's GID.</li></ul>
<code>--identifier IDENTIFIER</code>	Specify the identifier of the user or group for which the quota is created. The identifier must be of the type set with <code>--identifier-type</code> .
<code>--quota-id QUOTA_ID</code>	Identifies the directory quota under which the user or group quota is created.
<code>--user --group</code>	Specify <code>--user</code> to configure a user quota rule or <code>--group</code> to configure a group quota.

## Options

<code>--grace-period</code>	<p>Sets a grace period. If the specified user's or group's capacity usage continues to exceed the soft limit for the period of time set as the grace period, the user or group is blocked from writing to the directory.</p> <p>Specify <code>GRACE_PERIOD</code> in the format: <code>[DD] [HH: [MM: ] ]ss</code> or as an integer followed by <code>d</code> for days, <code>h</code> for</p>
-----------------------------	---

	<p>hours, m for minutes, or s for seconds. Examples:</p> <ul style="list-style-type: none"> <li>• To specify 30 days, 20 hours, 15 minutes and 10 seconds: <code>--grace-period 30 20:15:10</code>.</li> <li>• To specify 18 hours: <code>--grace-period 18:00</code>.</li> <li>• To specify 7 days: <code>--grace-period 7d</code></li> </ul>
<code>--soft-limit</code>	Sets a capacity usage soft limit for the specified user/group.
<code>--hard-limit</code>	<p>Sets a storage usage limit. No writes are allowed for the specified user/group beyond this limit.</p> <p>The value must be a complete integer and must be specified with a unit of measurement. Do not insert a space between the value and the unit of measurements. Valid units are:</p> <ul style="list-style-type: none"> <li>• Base 10: <i>KB, MB, GB, TB, PB, EB</i>,</li> <li>• Base 2: <i>KiB, MiB, GiB, TiB, PiB, EiB</i></li> </ul>
<code>--hard-limit-inodes</code>	Sets a limit on the number of directories and unique files the specified user/group can create under the path. A file with multiple hardlinks is counted only once.
<code>--soft-limit-inodes</code>	Sets a soft limit on the number of directories and unique files under the path. Warnings of exceeding the quota are issued when the limit is reached. A file with multiple hardlinks is counted only once.

### userquota list

This command lists user and group quota rules and accounting for a specified directory quota.

### Usage

```
userquota list --quota-id QUOTA_ID
               --user-rules|--group-rules|--user-accounting|--group-accounting
```

### Required Parameters

<code>--quota-id QUOTA_ID</code>	Specifies which directory quota for which to list user and group quota rules.
----------------------------------	---



<pre>--user-rules --group-rules --user-accounting --group-accounting</pre>	<p>Specifies which details to list:</p> <ul style="list-style-type: none"> <li>• <code>--user-rules</code>. View all user quota rules configured for the specified directory quota.</li> <li>• <code>--group-rules</code>. View all group quota rules configured for the specified directory quota.</li> <li>• <code>--user-accounting</code>. Query users that own files in the directory and display their usage details and the status of their quota usage.</li> <li>• <code>--group-accounting</code>. Query groups that own files in the directory and display their usage details and the status of their quota usage.</li> </ul>
--	--

### userquota modify

This command creates a user or group quota rule for a specific directory quota.

## Usage

```
userquota modify --id ID
                  [--grace-period]
                  [--soft-limit]
                  [--hard-limit]
                  [--hard-limit-inodes]
                  [--soft-limit-inodes]
```

## Required Parameters

<code>--id ID</code>	Specifies which to user quota rule to modify.
----------------------	---

## Options

<code>--grace-period</code>	<p>Sets or modifies a grace period. If the specified user's or group's capacity usage continues to exceed the soft limit for the period of time set as the grace period, the user or group is blocked from writing to the directory.</p> <p>Specify <code>GRACE_PERIOD</code> in the format: <code>[DD] [HH:[MM:]]ss</code> or as an integer followed by <code>d</code> for days, <code>h</code> for hours, <code>m</code> for minutes, or <code>s</code> for seconds. Examples:</p> <ul style="list-style-type: none"> <li>• To specify 30 days, 20 hours, 15 minutes and 10 seconds: <code>--grace-period 30 20:15:10</code>.</li> <li>• To specify 18 hours: <code>--grace-period 18:00</code>.</li> <li>• To specify 7 days: <code>--grace-period 7d</code></li> </ul>
-----------------------------	--

<code>--soft-limit</code>	Sets or modifies a capacity usage soft limit for the specified user/group.
<code>--hard-limit</code>	<p>Sets or modifies a storage usage limit. No writes are allowed for the specified user/group beyond this limit.</p> <p>The value must be a complete integer and must be specified with a unit of measurement. Do not insert a space between the value and the unit of measurements. Valid units are:</p> <ul style="list-style-type: none"> <li>• Base 10: <i>KB, MB, GB, TB, PB, EB</i>,</li> <li>• Base 2: <i>KiB, MiB, GiB, TiB, PiB, EiB</i></li> </ul>
<code>--hard-limit-inodes</code>	Sets or modifies a limit on the number of directories and unique files the specified user/group can create under the path. A file with multiple hardlinks is counted only once.
<code>--soft-limit-inodes</code>	Sets or modifies a soft limit on the number of directories and unique files under the path. Warnings of exceeding the quota are issued when the limit is reached. A file with multiple hardlinks is counted only once.

## userquota show

This command displays details of a specific user or group quota rule.

## Usage

```
userquota show --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies which user quota to display.
----------------------	--

# vastcatalogconfig commands

## vastcatalogconfig columns

This command displays the VAST Catalog schema, including column names and the data type of each column.

## Usage

```
vastcatalogconfig columns
```

## Example

```
vccli: admin> vastcatalogconfig columns
```

Name	Raw-field
atime	timestamp[ns]
creation_time	timestamp[ns]
ctime	timestamp[ns]
element_type	string
extension	string
gid	int32
group_owner_name	string
group_owner_sid	string
login_name	string
major_device	int32
minor_device	int32
mtime	timestamp[ns]
name	string
name_aces_exist	bool
nfs_mode_bits	int32
nlinks	int64
owner_name	string
owner_sid	string
parent_path	string
phandle	struct<clone_id: int32, handle_id: int64>
s3_locks_legal_hold	bool
s3_locks_retention	struct<mode: int8, timeout: time64[us]>
search_path	string
size	int64
symlink_path	string
uid	int32
used	int64
user_metadata	map<string, string>
user_tags	map<string, string>
user_tags_count	int16

## vastcatalogconfig create

This command creates a schedule for periodic snapshot creation for VAST Catalog, with retention periods for the periodic snapshots and for the VAST Catalog table.

## Usage

```
vastcatalogconfig create --schedule SCHEDULE
```

## Required Parameters

<code>--schedule SCHEDULE</code>	<p>Specifies a schedule definition in the following format:</p> <pre>every &lt;integer&gt;&lt;time unit&gt; start-at YYYY-MM-DD HH:MM:SS keep-local &lt;integer&gt;&lt;time unit&gt; keep-remote &lt;integer&gt;&lt;time unit&gt;</pre> <p>For example:</p> <pre>--schedule every 90m start-at 2025-07-27 20:10:35 keep-local 10h keep-remote 30d</pre>
--------------------------------------	---

## Example

```
vccli: admin> vastcatalogconfig create --schedule every 90m start-at 2025-07-27 20:10:35 keep-  
local 10h keep-remote 30d
```

## vastcatalogconfig delete

This command deletes a VAST Catalog schedule and configuration.

## Usage

```
vastcatalogconfig delete
```

## Example

```
vcli: admin> vastcatalogconfig delete
```

## vastcatalogconfig list

This command displays the VAST Catalog schedule and status (enabled or disabled).

## Usage

```
vastcatalogconfig list
```

## Example

```
vcli: admin> vastcatalogconfig list
```

+-----+-----  
 +-----+-----

```
+-----+
| Id | Name | Frames
| Enable |
+-----+
+-----+
| 20 | Vast catalog policy | [{"every": "30m", "start-at": "2023-03-06 13:21:03", "keep-local": "1h", "keep-remote": "30m"}] | True |
+-----+
+-----+
```

vastcatalogconfig modify

This command enables or disables VAST Catalog, and also modifies the periodic snapshot schedule for VAST Catalog.

Usage

```
vastcatalogconfig modify --id ID
                        [--schedule SCHEDULE]
                        [--enable|--disable]
                        [--splits COUNT]
```

Required Parameters

--id ID	Specifies the ID of the existing VAST Catalog configuration. To retrieve this ID, use <a href="#">vastcatalogconfig list</a> .
---------	--

Options

--schedule SCHEDULE	<p>Specifies the schedule definition in the following format:</p> <pre>every &lt;integer&gt;&lt;time unit&gt; start-at YYYY-MM-DD HH:MM:SS keep-local &lt;integer&gt;&lt;time unit&gt; keep-remote &lt;integer&gt;&lt;time unit&gt;</pre> <p>For example:</p> <pre>--schedule every 90m start-at 2025-07-27 20:10:35 keep-local 10h keep-remote 30d</pre>
--enable	Enables VAST Catalog.
--disable	Disables VAST Catalog.
--splits COUNT	Specifies the number of splits (concurrent threads) used to scan catalog tables. This option can be used to improve VAST Catalog performance for queries that require scanning a large amount of table rows.

## Example

```
vccli: admin> vastcatalogconfig modify --id 1 --enable
```

### **vastcatalogconfig show**

This command displays details of the VAST Catalog configuration.

## Usage

```
vastcatalogconfig show
```

## Example

```
vccli: admin> vastcatalogconfig show
+-----+
+-----+
+
| Id      | 20
|
| Name    | Vast catalog policy
|
| Frames  | [{'every': '30m', 'start-at': '2023-03-06 13:21:03', 'keep-local': '1h', 'keep-rem
ote': '30m'}] |
| Enable  | True
|
+-----+
+-----+
+
```

# vastcatalogindexedcolumn commands

## vastcatalogindexedcolumn add

This command explicitly adds a column to VAST Catalog for an S3 tag or S3 metadata attribute. The added column for an S3 tag is named `tag_<name>`, where `<name>` is the name you supply for the tag. The add column for an S3 metadata attribute is named `metadata_<name>`, where `<name>` is the name you supply for the metadata attribute.



### Note

VAST Catalog indexes all S3 tags found in objects and buckets as key-pair values in the `user_tags` column, regardless of whether user defined attributes are specified.

## Usage

```
vastcatalogindexedcolumn add --name NAME
                             --column-type tag|metadata
```

## Required Parameters

<code>--name NAME</code>	Specifies the key value of the user defined attribute. For example, if you have S3 objects tagged with <i>department=Sales</i> , <i>department=Marketing</i> , and so on, you would supply the key value "department" as the name of the attribute.
<code>--column-type tag metadata</code>	Specifies if the user defined attribute is an S3 tag ( <i>tag</i> ) or an S3 metadata attribute ( <i>metadata</i> ).

## Example

```
vccli: admin> vastcatalogindexedcolumn add --name department --column-type tag
```

## vastcatalogindexedcolumn list

This command lists columns that were added to VAST Catalog for user defined S3 tags and S3 metadata attributes.

## Usage

```
vastcatalogindexedcolumn list
```

# Example

```
vcli: admin> vastcatalogindexedcolumn list
+-----+-----+
| Name      | Column-type |
+-----+-----+
| department | tag         |
| company    | tag         |
+-----+-----+
```

## vastcatalogindexedcolumn remove

This command removes a column that was added to VAST Catalog for a user-defined S3 tag or S3 metadata attribute.

# Usage

```
vastcatalogindexedcolumn remove --name NAME
                                --column-type tag|metadata
```

# Required Parameters

<code>--name NAME</code>	Specifies the key value of the user-defined attribute that you want to remove from the catalog.
<code>--column-type tag metadata</code>	Specifies if the user-defined attribute that you want to remove is an S3 tag ( <code>tag</code> ) or an S3 metadata attribute ( <code>metadata</code> ).

# Example

```
vcli: admin> vastcatalogindexedcolumn remove --name department --column-type tag
```



# view commands

## view bulk-permission-update

This command lets you set up and run a bulk permission update on a view.

## Usage

```
view bulk-permission-update --id ID
                             --target-path PATH
                             --template-view-id TEMPLATE_ID
                             --template-dir-path TEMPLATE_DIR_PATH
                             [--template-file-path TEMPLATE_FILE_PATH]
```

## Required Parameters

<code>--id ID</code>	Specify the ID of the view that exposes the files and directories for which you want to update permissions.
<code>--target-path PATH</code>	Specify a view path where files and directories for which to update permissions reside.
<code>--template-view-id TEMPLATE_ID</code>	<p>Specify a view that exposes a directory and (optionally) a file from which to copy permissions and ownership attributes.</p> <p>This view should be on the same tenant as the view specified on <code>--target-path</code>.</p> <p>It is strongly recommended that the target view and the template view have view policies with the same security flavor. Running a bulk permission update on a view where the security flavor does not match that of the template view may result in inaccessible or incompatible permissions set.</p>
<code>--template-dir-path TEMPLATE_DIR_PATH</code>	<p>Specify a path to the directory from which to copy permissions and ownership attributes to the directories under <code>--target-path</code>. For more information about choosing a template directory, see <a href="#">Running a Bulk Permission Update on a View</a>.</p>

## Options

<code>--template-file-path TEMPLATE_FILE_PATH</code>	<p>Specify a path to the file from which to copy permissions and ownership attributes to the files under <code>--target-path</code>.</p> <p>If not specified, the attributes are copied from the directory specified on <code>--template-dir-path</code>.</p>
--	---

For more information about choosing a template file, see <a href="#">Running a Bulk Permission Update on a View</a> .
---

## Example

After the following command is run, all directories under `/mydir/test` on view 7 will have permissions and ownership as of `/template` on view 1, and all files under `/mydir/test` on view 7 will have permissions and ownership as of `/template.txt` on view 1:

```
vcli: admin> view bulk-permission-update --id 7 --target-path /mydir/test --template-view-id 1 --template-dir-path /template --template-file-path /template.txt
```

### view create



This command creates a *view*, which exposes a resource location to data clients. A view can expose a path to various different protocols, some in combination with each other, such as NFSv3 and SMB. Protocols include SMB, NFS versions 3 and 4 (including 4.1 and 4.2), S3 object storage, which enables clients to use the view as an S3 bucket, tabular, where the view is exposed to third-party database query engines, block storage where the view allocates a path as a block storage subsystem, and Kafka, which exposes VAST Database tables as topics to publish and consume events.

## Usage

```
view create --path PATH
            --protocols PROTOCOLS
            --policy-id ID
            [--tenant-id TENANT_ID]
            [--alias ALIAS]
            [--bucket BUCKET]
            [--bucket-owner BUCKET_OWNER]
            [--bucket-creators BUCKET_CREATORS]
            [--bucket-creators-groups BUCKET_CREATORS_GROUPS]
            [--create-dir [--inherit-parent-acl]]
            [--enable-global-sync]
            [--enable-live-monitoring]
            [--enable-s3-unverified-lookup]
            [--qos-policy-id QOS_POLICY_ID]
            [--share SHARE]
            [--s3-versioning]
            [--locking]
            [--default-retention-period DEFAULT_RETENTION_PERIOD]
            [--s3-locks-retention-mode NONE|GOVERNANCE|COMPLIANCE]
            [--allow-s3-anonymous-access] [--block-s3-anonymous-access]
            [--enable-acls|--disable-acls]
            [--abe-protocols SMB]
            [--abe-max-depth LEVEL]
            [--files-retention-mode NONE|GOVERNANCE|COMPLIANCE]
            [--max-retention-period MAX_RETENTION_PERIOD]
            [--min-retention-period MIN_RETENTION_PERIOD]
            [--auto-commit AUTO_COMMIT]
            [--abac-tags TAGS]
            [--bucket-logging-destination-id DESTINATION_BUCKET_ID]
            [--bucket-logging-prefix PREFIX]
            [--bucket-logging-key-format SIMPLE_PREFIX|PARTITIONED_PREFIX_EVENT_TIME|PARTITIONED_PREFIX_DELIVERY_TIME]
            [--disable-bucket-logging]
            [--enable-user-impersonation|--disable-user-impersonation]
```

```
[--user-impersonation-identifier-type ID_TYPE]
[--user-impersonation-identifier ID]
[--user-impersonation-username NAME]
[--kafka-vip-pools POOL_ID]
[--name NAME]
[--set-is-default-subsystem]
[--enable-indestructible-object]
[--indestructible-object-duration RETENTION_PERIOD]
```

## Required Parameters

<pre>--path PATH</pre>	<p>Specifies a path to a file system directory to be exposed to clients. It can be a directory that was already created by a client inside an exposed parent directory, or it can be a new directory, in which case you must specify the <code>--create_dir</code> option to create the directory.</p> <div data-bbox="310 653 1463 869">  <p><b>Note</b></p> <p>For block storage subsystem views, there is no need to specify <code>--create_dir</code>.</p> </div> <p>Example:</p> <pre>--path /a/b/c</pre> <p>If you are going to use the path to create an S3 bucket, ensure that none of the subdirectories under the path has a replication protected path defined on it.</p> <div data-bbox="310 1098 1463 1346">  <p><b>Note</b></p> <p>If the path is an encrypted path, the path must be created as an encrypted path before you create the view.</p> </div>
<pre>--policy-id ID</pre>	<p>Specifies which view policy to apply. Specify <code>ID</code> as an integer value. To display view policy configurations with their IDs, use <a href="#">viewpolicy list</a>.</p>
<pre>-- protocols PROTOCOLS</pre>	<p>Specifies the protocol(s) to which the view is exposed.</p> <p>Specify <code>PROTOCOLS</code> as a string value for a single protocol or a comma separated list of strings to enable multiple protocols. Valid string values are:</p> <ul style="list-style-type: none"> <li>• <code>NFS</code>. To expose the view as an NFS export to clients using NFS version 3.</li> <li>• <code>NFS4</code>. To expose the view as an NFS export to clients using NFS version 4.1 or 4.2.</li> <li>• <code>SMB</code> (Not in combination with <code>ENDPOINT</code>). To expose the view as an SMB share to SMB clients.</li> </ul>



## Note

If you want to configure share-level ACL for an SMB-enabled view, see [Share-Level ACLs](#) for the relevant commands to run after the view is created.


- **S3** (Not in combination with **ENDPOINT**). To expose the view as an S3 bucket.
- **ENDPOINT** (Not in combination with **SMB** or **S3**). To create an S3 Endpoint, which is a template for creating buckets via S3 APIs. Whenever a bucket is created using this endpoint, a new view is created under the specified path. See [Managing S3 Request-Initiated Bucket Creation](#) for more information about S3 Endpoint buckets.
- **DATABASE**. To expose the view as a VAST database. This option is used for each view that VAST Cluster creates when a user chooses to create a database on the cluster. For more information, see [Configuring the VAST Cluster for Database Access](#).
- **KAFKA** exposes VAST Database tables that are used as topics to publish and consume events. For more information, see [Publishing Events to VAST Event Broker](#). If you specify **KAFKA**, you also need to specify **DATABASE** and **S3** protocols for the view.
- **BLOCK**. To expose the view as a block storage subsystem. The specified path must be an empty directory. **BLOCK** cannot be specified in combination with any other protocol.


### Examples:

```
--protocols NFS,SMB  
  
--protocols NFS,NFS4,ENDPOINT  
  
--protocols NFS,S3  
  
--protocols SMB  
  
--protocols DATABASE  
  
--protocols KAFKA,DATABASE,S3  
  
--protocols BLOCK
```

## Options

<code>--tenant-id TENANT_ID</code>	Specifies a non-default tenant to associate with the view.
<code>--alias ALIAS</code>	For NFSv3 exports, specifies an alternative shorter name for the path that can be used alternatively when mounting. Optional and relevant only if the view is exposed to NFS. An alias must begin with a forward slash ("/") and must consist of only ASCII

	characters.
<code>--bucket BUCKETNAME</code>	Specifies the name of an S3 bucket. Required if <code>S3</code> is specified in <code>--protocols</code> .
<code>--bucket-owner BUCKET_OWNER</code>	Specifies a user to be the bucket owner. Required if <code>S3</code> is specified in <code>--protocols</code> .
<code>--bucket-creators BUCKET_CREATORS</code>	<p>Relevant if <code>ENDPOINT</code> is specified in <code>--protocols</code>. Specifies users such that any request to create an S3 bucket that is sent by S3 API by a specified user will use this S3 Endpoint view.</p> <p>Specify <code>BUCKET_CREATORS</code> as a comma separated list of user names.</p> <div>  <p><b>Note</b></p> <p>Users should not be specified as bucket creators in more than one S3 Endpoint view.</p> </div>
<code>bucket-creators-groups BUCKET_CREATORS_GROUPS</code>	<p>Relevant if <code>ENDPOINT</code> is specified in <code>--protocols</code>. Specifies groups such that any request to create an S3 bucket that is sent by S3 API by a user who belongs to a specified group will use this S3 Endpoint view.</p> <p>Specify <code>BUCKET_CREATORS_GROUPS</code> as a comma separated list of group names.</p> <div> <p><b>Caution</b></p> <p>Take extra care not to duplicate bucket creators through groups: If you specify a group as a bucket creator group in one view and you also specify a user who belongs to that group as a bucket creator user in another view, view creation will not fail. Yet, there is a conflict between the two configurations and the selection of a view for configuring the user's buckets is not predictable.</p> </div>
<code>--create-dir</code>	Creates a directory at the specified path. Include this option if the directory does not already exist.

	 <p><b>Note</b></p> <p>When creating a view on an encrypted path, do not include this option. The path is created when you create the encrypted path, before you create the view.</p>
<code>--inherit-parent-acl</code>	<p>This option can only be used together with the <code>--create-dir</code> option, when creating a new directory for the view.</p> <p>If specified, the newly created directory will inherit the ACL of the parent directory.</p> <p>If not specified, and also in case the parent directory does not have an inherited ACL, the newly created directory will be assigned an ACL granting POSIX 777 permissions.</p>
<code>--enable-global-sync</code>	<p>Supports seamless failover between replication peers by syncing file handles between the view and remote views on the replicated path on replication peers. This enables NFSv3 client users to retain the same mount point to the view in the event of a failover of the view path to a replication peer. Enabling this option may cause overhead and should only be enabled when the use case is relevant. For more information about seamless replication, see <a href="#">Preparing for Seamless Replication Failover (NFSv3)</a>.</p>
<code>--enable-live-monitoring</code>	<p>Enables <i>live monitoring</i> on the view. Live monitoring can be enabled for up to ten views at one time and can also be enabled any time after view creation using <a href="#">view modify</a>.</p> <p>Analytics data for views is polled every 5 minutes by default and every 10 seconds with live monitoring.</p>
<code>--qos-policy-id</code> <code>QOS_POLICY_ID</code>	<p>Associates a QoS policy with the view. Specify the QoS policy by its ID. To list QoS policy definitions, use <a href="#">qospolicy list</a>.</p>
<code>--share SHARE</code>	<p>Specifies the SMB share name. Required if the view is exposed to SMB. The name cannot include the following characters: <code>\: &lt;&gt;*"?</code></p>
<code>--s3-versioning</code>	<p>Enables object versioning on the bucket if <code>S3</code> is specified in <code>--protocols</code>.</p>
<code>--locking</code>	<p>Enables object locking on the view bucket, if <code>S3</code> is specified in <code>--protocols</code>, or file locking in NFSv3/SMB, if they are selected in <code>--protocols</code>. This setting can't be disabled after the view is created.</p>
<code>--s3-locks-retention-mode</code>	<p>Sets a default retention mode for objects in the bucket.</p>

NONE   GOVERNANCE   COMPLIANCE	<p>Possible values:</p> <ul style="list-style-type: none"> <li><b>NONE</b> (default). Object versions that are placed in the bucket have no automatic protection but can be configured with a retention period or legal hold.</li> <li><b>GOVERNANCE</b>. Object versions that are placed in the bucket are automatically protected with a retention lock with retention mode set to governance.</li> <li><b>COMPLIANCE</b>. Object versions that are placed in the bucket are automatically protected with a retention lock with retention mode set to compliance.</li> </ul>
<code>--allow-anonymous-access</code>	<p>If the view has S3 Bucket or S3 Endpoint enabled, include this option to allow anonymous S3 access to the view's S3 bucket.</p> <p>If allowed, anonymous requests are granted access provided that the object ACL grants access to the <i>All Users</i> group (in S3 Native security flavor) or the permission mode bits on the requested file and directory path grant access permission to "others" (in NFS security flavor). For views with SMB security flavor, anonymous requests are not granted access.</p>
<code>--block-anonymous-access</code>	Blocks anonymous S3 access to the view's S3 bucket, if applicable. This is the default setting.
<code>--enable-acls</code>	<p>When this option is specified, the user which uploads the object, becomes the object owner. Access is authorized based on ACLs and identity or bucket policies.</p> <p>For more information about the <i>ACLs enabled</i> mode, see <a href="#">S3 Object Ownership</a>.</p>
<code>--disable-acls</code>	<p>When this option is specified, the bucket owner has full control over any object in the bucket. Access to objects is controlled based on identity and bucket policies. ACLs are not used.</p> <p>For more information about the <i>ACLs disabled</i> mode, see <a href="#">S3 Object Ownership</a>.</p>
<code>--abe-protocols SMB</code>	<p>Enables <a href="#">Access-Based Enumeration</a> (ABE) for the view, if <code>SMB</code> is specified in <code>--protocols</code>.</p> <p>By default, ABE is disabled.</p>
<code>--abe-max-depth LEVEL</code>	<p>Sets the maximum directory level (depth) at which ABE is enabled. By default, ABE depth is unlimited.</p> <p>Specify <code>LEVELS</code> as an integer, for example: <code>--abe-max-depth 3</code></p>
<code>--files-retention-mode</code>	Sets the retention mode for files saved in the view, if locking ( <code>--locking</code> ) is enabled.

NONE   GOVERNANCE   COMPLIANCE	<p>Possible values:</p> <ul style="list-style-type: none"> <li>• <b>NONE</b> (default). Files that are saved to the view have no automatic protection but can be manually configured with a retention period or legal hold.</li> <li>• <b>GOVERNANCE</b>. Files that are saved in the view are automatically protected with a retention lock with retention mode set to governance. In this mode, the retention period can be lengthened or shortened.</li> <li>• <b>COMPLIANCE</b>. Files that are saved in the view are automatically protected with a retention lock with retention mode set to compliance. In this mode, the retention period can be lengthened, but not shortened.</li> </ul>
<pre>--default-retention-period DEFAULT_RETENTION</pre>	<p>Sets the default retention period for files that are locked in the view to <code>DEFAULT_RETENTION</code>. Files that are locked automatically using <code>auto-commit</code> will be locked for this period of time, after which they will be unlocked.</p> <p>Files that are locked manually (by setting the <i>atime</i> for the file to a future time) do not use the default retention period.</p> <p>The value <code>DEFAULT_RETENTION</code> must be in the range between the <i>min-retention-period</i> and <i>max-retention-period</i>.</p> <p>Set it as an integer value, including units (m - minutes, h - hours, d - days, y - years).</p> <p>Example: 5d (5 days).</p>
<pre>--max-retention-period MAX_RETENTION</pre>	<p>Sets the maximum retention period for files that are locked in the view to <code>MAX_RETENTION</code>. Files cannot be locked for longer than this period, whether they are locked manually (by setting the <i>atime</i>) or automatically, using <i>auto-commit</i>.</p> <p>It must be larger than the <i>min-retention-period</i>.</p> <p>Set it as an integer value, including units (m - minutes, h - hours, d - days, y - years).</p> <p>Example: 2m (2 months).</p>
<pre>--min-retention-period MIN_RETENTION</pre>	<p>Sets the minimum retention period for files that are locked in the view to <code>MIN_RETENTION</code>. Files cannot be locked for less than this period, whether locked manually (by setting the <i>atime</i>) or automatically, using <i>auto-commit</i>.</p> <p>It must be less than the <i>max-retention-period</i>.</p> <p>Set it as an integer value, including units (m - minutes, h - hours, d - days, y - years).</p> <p>Example: 3d (3 days).</p>
<pre>--auto-commit AUTO_COMMIT</pre>	<p>Sets the auto-commit time to <code>AUTO_COMMIT</code> for files that are locked automatically. These files are locked automatically after the <code>AUTO_COMMIT</code> period elapses from the time the file is saved. Files locked automatically are locked for the <i>default-retention-</i></p>



	<p><i>period</i>, after which they are unlocked.</p> <p>If set, then <code>--default-retention-period</code>, <code>--min-retention-period</code>, and <code>--max-retention-period</code> must also be set.</p> <p>Set it as an integer value, including units (m - minutes, h - hours, d - days, y - years).</p> <p>Example: 5m (5 minutes).</p>
<code>--abac-tags TAGS</code>	<p>If you are going to use <a href="#">Attribute-Based Access Control (ABAC)</a>, enter a comma-separated list of ABAC tags.</p> <p>Up to 20 ABAC tags can be defined per view. ABAC tags are case-sensitive and can include alphanumeric characters, a hyphen (-), a colon (:), a plus sign (+), and an underline (_).</p> <p>For example: <code>red,green,yellow</code></p>

## Block Storage Configuration Options

Use the following options with the `--protocol BLOCK` to configure a Block storage subsystem:

<code>--name NAME</code>	A name for the subsystem.
<code>--set-is-default-subsystem</code>	Sets the view to be the default subsystem view from which to provision block volumes.

## S3 Bucket Logging Options

The following options let you configure S3 Bucket Logging for an *S3 Bucket* view:

<code>--bucket-logging-destination-id</code> <code>DESTINATION_BUCKET_ID</code>	<p>Enables S3 bucket logging for the bucket and determines the destination bucket which will be store the logs.</p> <p><code>DESTINATION_BUCKET_ID</code> is an ID of a view that exposes the destination bucket.</p>
<code>--bucket-logging-prefix PREFIX</code>	<p>Optionally, specify a prefix that will be prepended to each key of a log object uploaded to the bucket. This prefix can be used to categorize log objects; for example, if you use the same destination bucket for multiple source buckets.</p> <p>The prefix can be up to 128 characters and must follow <a href="#">S3 object naming rules</a>.</p>
<code>--bucket-logging-key-format</code>	Specify the format for the log object keys:

<p>SIMPLE_PREFIX  PARTITIONED_PREFIX_EVENT_TIME  PARTITIONED_PREFIX_DELIVERY_TIME</p>	<ul style="list-style-type: none"> <li>• <b>SIMPLE_PREFIX</b> adds log object keys in the following format:  [DestinationPrefix] [YYYY] - [MM] - [DD] - [hh] - [mm] - [ss] - [UniqueString]  This is the default format.</li> <li>• <b>PARTITIONED_PREFIX_EVENT_TIME</b> and <b>PARTITIONED_PREFIX_DELIVERY_TIME</b> add log object keys in the following format:  [DestinationPrefix] [SourceUsername] / [SourceBucket] / [YYYY] / [MM] / [DD] - [MM] - [DD] - [hh] - [mm] - [ss] - [UniqueString]  This format enables timestamp-based partitioning of log objects. <ul style="list-style-type: none"> <li>◦ With <b>PARTITIONED_PREFIX_EVENT_TIME</b>, the partitioning is done based on the time of the logged events occurred.</li> <li>◦ With <b>PARTITIONED_PREFIX_DELIVERY_TIME</b>, the partitioning is done based on the time the log object has been delivered to the destination bucket.</li> </ul> </li> </ul> <p>In the formats:</p> <ul style="list-style-type: none"> <li>• [DestinationPrefix] is the optional prefix that prepends keys of log objects uploaded to the destination bucket. You define this prefix with the <code>--bucket-logging-prefix</code> parameter.</li> <li>• [SourceUsername] is the username for the owner of the bucket being logged.</li> <li>• [SourceBucket] is the bucket being logged.</li> <li>• UTC time is used in timestamps.</li> <li>• [UniqueString] is a unique string added to prevent overwriting of objects.</li> </ul>
<code>--disable-bucket-logging</code>	Disables S3 bucket logging configured for the bucket.

## User Impersonation Options


The following options let you configure [user impersonation](#) for a view:

<code>--enable-user-impersonation</code>	Enables user impersonation.
<code>--disable-user-impersonation</code>	Disables user impersonation.
<code>--user-impersonation-identifier</code>	The type of a user identifier that you are going to specify on the <code>--user-impersonation-identifier</code> option to identify the impersonator (the user account to be used instead of the

<pre>identifier-type ID_TYPE</pre>	<p>original user).</p> <p>Valid values for <code>ID_TYPE</code>:</p> <ul style="list-style-type: none"> <li>• <code>username</code> for user's username in format <i>username@domain</i>.</li> <li>• <code>sid_str</code> for user's Security ID (SID).</li> <li>• <code>uid</code> for user's POSIX UID attribute.</li> </ul> <p>This option is required if <code>--enable-user-impersonation</code> is specified on the command.</p>
<pre>--user-impersonation-identifier ID</pre>	<p>The impersonator user ID or name. The ID or name must be of the type specified on the <code>--user-impersonation-identifier-type</code> option (<i>username@domain</i>, SID or UID).</p> <p>This option is required if <code>--enable-user-impersonation</code> is specified on the command.</p>
<pre>--user-impersonation-username NAME</pre>	<p>The impersonator username.</p> <p>If <code>--user-impersonation-identifier ID</code> and <code>--user-impersonation-username NAME</code> point to different users, the user specified with <code>--user-impersonation-identifier ID</code> becomes the impersonator.</p>


## Event Publishing Options

The following options let you configure a view for [VAST Event Broker](#):

<pre>--kafka-vip-pools POOL_ID</pre>	<p>Specifies a virtual IP pool to be used to access event topics exposed by the view.</p> <div>  <div> <p><b>Note</b></p> <p>Only one virtual IP pool can be used per view.</p> </div> </div> <p>The pool must belong to the same VAST tenant as the Kafka-enabled view.</p> <p>If the view is associated with a view policy that includes virtual IP pools, the pool specified as the Kafka pool must be one of the view policy pools.</p>
<pre>--kafka-first-join-group-timeout-sec SECONDS</pre>	<p>Specifies the amount of time to wait for more consumers to join a new group before performing the first rebalance. Valid values are 1-3600. The default value is 60 seconds.</p>


<code>--kafka-rejoin-group-timeout-sec SECONDS</code>	Specifies the maximum allowed session timeout for registered consumers. Valid values are 1-3600. The default value is 60 seconds.
---	---

# Indestructible Object Mode Options



**Note**

These options are not supported by default. To use these options, first enable indestructible object mode on the cluster. For complete feature information, see [Indestructible Object Mode](#).

<code>--enable-indestructible-object</code>	<p>Enables indestructible object mode on the view.</p> <p>See also <code>--indestructible-object-duration RETENTION_PERIOD</code> since this value cannot be changed after creating the view without unlocking the cluster's indestructibility mechanism.</p>
<code>--indestructible-object-duration RETENTION_PERIOD</code>	<p>Sets the number of days for which objects in the bucket should be protected by indestructible object mode.</p> <p>Specify <code>RETENTION_PERIOD</code> as an integer.</p> <p>Default: 8</p> <p>Supported range: 1-400</p> <div>  <div> <p><b>Note</b></p> <p>If you are enabling indestructibility mode, you will not be able to change this retention period after view creation without first <a href="#">unlocking the cluster's indestructibility mechanism</a>, which requires a secure authentication procedure.</p> </div> </div>

## Example

This example creates a view of the pre-existing `/dev` directory, with an NFS export, using the default view policy.

```
vcli: admin> view create --path /dev --protocols NFS
```

This example creates a multiprotocol view of a directory at the `/home/users/devteam` path using a non default view policy.

```
vcli: admin> view create --path /home/users/devteam --protocols NFS,SMB
--alias /devteam --share devteamusers --policy-id 2 --create-dir
```

### view delete

This command deletes a view.

## Usage

```
view delete --id ID
```

## Required Parameters

<code>--id ID</code>	Specifies the view to delete.
----------------------	-------------------------------

## Example

```
vccli: admin> view delete --id 2
```

### view list

This command displays configured views.

## Usage

```
view list [--path PATH]
          [--alias ALIAS]
          [--policy-name VIEW_POLICY_NAME]
          [--policy-id VIEW_POLICY_ID]
          [--cluster-name CLUSTER_NAME]
          [--cluster-id CLUSTER_ID]
          [--tenant-name TENANT_NAME]
          [--tenant-id TENANT_ID]
          [--page PAGE]
          [--page-size PAGE-SIZE]
```

## Options

<code>--name VIEW_NAME</code>	Filters views by view name.
<code>--path PATH</code>	Filters views by directory path.
<code>--alias ALIAS</code>	Filters views by NFS export alias.
<code>--policy-name</code>	Filters views by view policy name.

VIEW_POLICY_NAME	
--policy-id VIEW_POLICY_ID	Filters views by view policy ID.
--cluster-name CLUSTER_NAME	Filters views by cluster name.
--cluster-id CLUSTER_ID	Filters views by cluster ID.
--tenant-name TENANT_NAME	Filters views by tenant name.
--tenant-id TENANT_ID	Filters views by tenant ID.
--page PAGE	Displays a specified page of views, where page size is the maximum number of views to display per page.
--page-size PAGE-SIZE	Sets the number of views per page for displaying by page (using the --page option).  Default: 20  Maximum: 500

## Examples

```

vcli: admin> view list
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Path | Alias | Share | Bucket | Bucket-owner | Policy | Protocols | C
luster | Physical-capacity | Logical-capacity | WORM | Is-remote | Created time
| Live Monitoring | Qos-policy | Tenant-id | Bulk-permission-update-state | Bulk-permission-u
pdate-progress | Files-retention-mode | Abe-protocols | Abe-max-depth | Global Synchronizatio
n | ABAC tags | User-impersonation | Is-default-subsystem | Name | Nqn
|
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+

```



```

+-----+
vcli: admin> view list
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
| ID | Path | Alias | Share | Bucket | Bucket-owner | Policy | Protocols | Cluste
r | Physical-capacity | Logical-capacity | S3-locks | NFS-interop | Is-remote | Created tim
e | Live Monitoring | Qos-policy | Tenant-id | Bulk-permission-update-state | Bulk-per
mission-update-progress | Files-retention-mode | Abe-protocols | Abe-max-depth | Global Synch
ronization | ABAC tags |
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
| 1 | / | / | | | None | default | ['NFS', 'NFS4'] | myclus
ter | 666777066374 | | 2027959133651 | False | Disabled | False | 2023-05-12
05:07:57 | False | None | 1 | N/A | | 0
| NONE | [] | None | False | []
|
| 3 | /io_agent | | | None | default | ['NFS'] | myclus
ter | 161732 | | 293901970596 | False | Disabled | False | 2023-05-12
05:11:22 | False | None | 1 | N/A | | 0
| NONE | [] | None | False |
|
| 4 | /path1 | | | None | default | ['NFS'] | myclus
ter | 23761665568 | | 867598264582 | False | Disabled | False | 2023-05-12
05:11:40 | False | None | 1 | N/A | | 0
| NONE | [] | None | False |
|
| 5 | /path2 | | | None | default | ['NFS'] | myclus
ter | 466004064 | | 15724903967 | False | Disabled | False | 2023-05-12
05:11:45 | False | None | 1 | N/A | | 0
| NONE | [] | None | False |
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+
+-----+

```

[view modify](#)

This command modifies a view.

## General Usage

```
view modify --id VIEW_ID
            [--path PATH]
            [--protocols PROTOCOLS]
            [--alias ALIAS]
            [--share SHARE]
            [--policy-id ID]
            [--cluster-id ID]
            [--create-dir]
            [--enable-live-monitoring|--disable-live-monitoring]
            [--enable-s3-unverified-lookup]|--disable-s3-unverified-lookup
            [--s3-versioning]
            [--locking]
            [--default-retention-period DEFAULT RETENTION PERIOD]
```



```

[--s3-locks-retention-mode NONE|GOVERNANCE|COMPLIANCE]
[--bucket BUCKET]
[--bucket-owner BUCKET_OWNER]
[--bucket-creators BUCKET_CREATORS]
[--bucket-creators-groups BUCKET_CREATORS_GROUPS]
[--allow-s3-anonymous-access] | [--block-s3-anonymous-access]
[--qos-policy-id QOS_POLICY_ID]
[--delete_qos_policy]
[--enable-acls|--disable-acls]
[--enable-share-acl] | [--disable-share-acl]
[--clear-share-acl]
[--share-ace-grantee users|groups]
[--share-ace-permissions FULL|READ|CHANGE]
[--share-ace-identifier IDENTIFIER]
[--remove-share-ace-name NAME --remove-share-ace-fqdn FQDN]
[--abe-protocols [SMB]]
[--abe-max-depth LEVEL]
[--max-retention-period MAX_RETENTION_PERIOD]
[--min-retention-period MIN_RETENTION_PERIOD]
[--auto-commit AUTO_COMMIT]
[--bucket-logging-destination-id DESTINATION_BUCKET_ID]
[--bucket-logging-prefix PREFIX]
[--bucket-logging-key-format SIMPLE_PREFIX|PARTITIONED_PREFIX_EVENT_TIME|PARTITIONED_PREFIX_DELIVERY_TIME]
[--disable-bucket-logging]
[--enable-user-impersonation|--disable-user-impersonation]
[--user-impersonation-identifier-type ID_TYPE]
[--user-impersonation-identifier ID]
[--user-impersonation-username NAME]
[--name NAME]
[--set-is-default-subsystem|--reset-is-default-subsystem]
[--enable-indestructible-object|--disable-indestructible-object]
[--indestructible-object-duration RETENTION_PERIOD]

```

## Share-Level ACL Usage

To enable or disable share-level ACL on the view:

```
view modify --id VIEW_ID --enable-share-acl|--disable-share-acl
```

To add an ACE to the view's share-level ACL:

```
view modify --id VIEW_ID
  --share-ace-grantee users|groups
  --share-ace-identifier IDENTIFIER
  --share-ace-permissions FULL|READ|CHANGE
```

To clear all ACEs from the view's share-level ACL:

```
view modify --id VIEW_ID
  --clear-share-acl
```

To remove an ACE:

```
view modify --id VIEW_ID
  --remove-share-ace-name NAME
  --remove-share-ace-fqdn FQDN
```

# Required Parameters

<code>--id VIEW_ID</code>	Specifies the ID of the view you want to modify.
---------------------------	--


## Options

<code>--path PATH</code>	<p>Modifies the Element Store path to be exposed to clients. It can be a directory that was already created by a client inside an exposed parent directory, or it can be a new directory, in which case you must specify the <code>--create_dir</code> option to create the directory.</p> <p>Example:</p> <pre>--path /a/b/c</pre> <p>If you are going to use the path to create an S3 bucket, ensure that none of the subdirectories under the path has a replication protected path defined on it.</p>
<code>--protocols PROTOCOLS</code>	<p>Specifies which protocol(s) the view will be exposed to.</p> <p>Specify PROTOCOLS as a string value for a single protocol or a comma separated list of strings to enable multiple protocols. Valid string values are:</p> <ul style="list-style-type: none"><li>• <code>NFS</code>. To expose the view as an NFS export to clients using NFS version 3.</li><li>• <code>NFS4</code>. To expose the view as an NFS export to clients using NFS version 4.1 or 4.2.</li><li>• <code>SMB</code> (Not in combination with <code>ENDPOINT</code>). To expose the view as an SMB share to SMB clients.</li><li>• <code>S3</code> (Not in combination with <code>ENDPOINT</code>). To expose the view as an S3 bucket.</li><li>• <code>ENDPOINT</code> (Not in combination with <code>SMB</code> or <code>S3</code>). To create an S3 Endpoint, which is a template for creating buckets via S3 APIs. Whenever a bucket is created using this endpoint, a new view is created under the specified path. See <a href="#">Managing S3 Request-Initiated Bucket Creation</a> for more information about S3 Endpoint buckets.</li><li>• <code>DATABASE</code>. To expose the view as a VAST database. This option is used for each view that VAST Cluster creates when a user chooses to create a database on the cluster. For more information, see <a href="#">Configuring the VAST Cluster for Database Access</a>.</li></ul> <p>Examples:</p> <pre>--protocols NFS,SMB --protocols NFS,NFS4,ENDPOINT --protocols NFS,S3 --protocols SMB</pre>

	<code>--protocols DATABASE</code>
<code>--alias ALIAS</code>	For NFSv3 exports, specifies an alternative shorter name for the path that can be used alternatively when mounting. Optional and relevant only if the view is exposed to NFS. An alias must begin with a forward slash ("/") and must consist of only ASCII characters.
<code>--share SHARE</code>	Specifies the SMB share name. Required if the view is exposed to SMB. The name cannot include the following characters: <code>\: &lt;&gt;*?"</code>
<code>--policy-id ID</code>	Specifies which view policy to apply. If unspecified, the default policy (ID 1) is used.
<code>--create-dir</code>	Creates a directory at the specified path. Include this option if the directory does not already exist.
<code>--enable-live-monitoring</code>	<p>Enables <i>live monitoring</i> on the view. Live monitoring can be enabled for up to ten views at one time.</p> <p>Analytics data for views is polled every 5 minutes by default and every 10 seconds with live monitoring.</p>
<code>--disable-live-monitoring</code>	Disables <i>live monitoring</i> on the view. See also <code>--enable-live-monitoring</code> .
<code>--s3-versioning</code>	Enables object versioning on the bucket if <code>s3</code> is specified in <code>--protocols</code> .
<code>--locking</code>	Enables object locking on the view bucket, if <code>s3</code> is specified in <code>--protocols</code> , or file locking in NFSv3/SMB, if they are selected in <code>--protocols</code> . This setting can't be disabled after the view is created.
<code>--s3-locks-retention-mode</code> NONE   GOVERNANCE   COMPLIANCE	<p>Sets a default retention mode for objects in the bucket.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li><b>NONE (default).</b> Object versions that are placed in the bucket have no automatic protection but can be configured with a retention period or legal hold.</li> <li><b>GOVERNANCE.</b> Object versions that are placed in the bucket are automatically protected with a retention lock with retention mode set to governance.</li> <li><b>COMPLIANCE.</b> Object versions that are placed in the bucket are automatically protected with a retention lock with retention mode set to compliance.</li> </ul>

<code>--bucket BUCKETNAME</code>	Specifies the name of an S3 bucket. Required if <code>S3</code> is specified in <code>--protocols</code> .
<code>--bucket-owner BUCKET_OWNER</code>	Specifies a user to be the bucket owner. Required if <code>S3</code> is specified in <code>--protocols</code> .
<code>--bucket-creators BUCKET_CREATORS</code>	<p>Relevant if <code>ENDPOINT</code> is specified in <code>--protocols</code>. Specifies users such that any request to create an S3 bucket that is sent by S3 API by a specified user will use this S3 Endpoint view.</p> <p>Specify <code>BUCKET_CREATORS</code> as a comma separated list of user names.</p> <div>  <p><b>Note</b></p> <p>Users should not be specified as bucket creators in more than one S3 Endpoint view.</p> </div>
<code>--allow-anonymous-access</code>	<p>If the view has S3 Bucket or S3 Endpoint enabled, include this option to allow anonymous S3 access to the view's S3 bucket.</p> <p>If allowed, anonymous requests are granted provided that the object ACL grants access to the <i>All Users</i> group (in S3 Native security flavor) or the permission mode bits on the requested file and directory path grant access permission to "others" (in NFS security flavor). For views with SMB security flavor, anonymous requests are not granted access.</p>
<code>--block-anonymous-access</code>	Blocks anonymous S3 access to the view's S3 bucket, if applicable. This is the default setting.
<code>--qos-policy-id QOS_POLICY_ID</code>	Associates a QoS policy with the view. Specify the QoS policy by its ID. To list QoS policy definitions, use <a href="#">qospolicy list</a> .
<code>--delete-qos-policy</code>	If a QoS policy is associated with the view, this option removes the QoS policy from the view.
<code>--enable-acls</code>	<p>When this option is specified, access to bucket objects is controlled based on ACLs rather than on the bucket owner's permissions.</p> <p>This option disables <a href="#">S3 Object Ownership</a> for the bucket.</p>
<code>--disable-acls</code>	When this option is specified, the bucket owner has full control over any object in the

	<p>bucket. Access to objects is controlled based on policies configured for the bucket. ACLs are not used.</p> <p>Specifying this option is equivalent to setting the S3 object ownership rule of <i>Bucket Owner Enforced</i>.</p>
<code>--enable-share-acl</code>	<p>Enables share-level ACL on the view.</p> <p>This setting enables share-level ACL on the view, which means that SMB requests to access the view will fail unless permission is granted to the requesting user by an ACE.</p>
<code>--disable-share-acl</code>	<p>Disables a share-level ACL on a view.</p> <p>Share-level ACL is disabled by default.</p>
<code>--clear-share-acl</code>	<p>Removes all ACEs from a share-level ACL if enabled on the view, without disabling share-level ACL.</p>
<code>--share-ace-grantee</code> <code>users groups</code>	<p>Specifies a grantee type when running the command to configure an Access Control Entry (ACE) in a share-level ACL.</p> <p>See also <a href="#">Share-Level ACL Usage</a> .</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <code>users</code>. Specify this option when configuring an ACE for a user.</li> <li>• <code>groups</code>. Specify this option when configuring an ACE for a group.</li> </ul>
<code>--share-ace-permissions</code> <code>READ CHANGE FULL</code>	<p>Specifies the type of permission to grant to a specified grantee when running the command to configure an Access Control Entry (ACE) in a share-level ACL.</p> <p>See also <a href="#">Share-Level ACL Usage</a> .</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <code>FULL</code> (default). Grants the grantee <i>full control</i> share-level access to the view.</li> <li>• <code>READ</code>. Grants the grantee <i>read</i> share-level access to the view.</li> <li>• <code>CHANGE</code>. Grants the grantee <i>change</i> share-level access to the view.</li> </ul>
<code>--share-ace-identifier</code> <code>IDENTIFIER</code>	<p>Specifies a grantee by SID, UID or GID identifier when running the command to configure an Access Control Entry (ACE) in a share-level ACL.</p> <p>See also <a href="#">Share-Level ACL Usage</a> .</p>

	<p>Specify <code>IDENTIFIER</code> as the exact value of the user's or group's SID, UID or GID attribute value on the joined Active Directory domain.</p> <p>To obtain an identifier, run a query by prefix against the Active Directory domain using one of the following commands:</p> <ul style="list-style-type: none"> <li>• <a href="#">user query-by-prefix</a> for a user.</li> <li>• <a href="#">group query-by-prefix</a> for a group.</li> </ul>
<pre>--remove-share-ace-name NAME</pre>	<p>Specifies the grantee name when running the command to remove an ACE from a share-level ACL.</p> <p>See also <a href="#">Share-Level ACL Usage</a>.</p>
<pre>--remove-share-ace-fqdn FQDN</pre>	<p>Specifies the domain when running the command to remove an ACE for a given from a share-level ACL.</p> <p>See also <a href="#">Share-Level ACL Usage</a>.</p>
<pre>--abe-protocols SMB</pre>	<p>Enables <a href="#">Access-Based Enumeration</a> (ABE) for the view, if <code>SMB</code> is specified in <code>--protocols</code>.</p> <div>  <div> <p><b>Note</b></p> <p>To disable ABE, specify the option without the protocol keyword: <code>--abe-protocols</code>.</p> </div> </div>
<pre>--abe-max-depth LEVEL</pre>	<p>Sets the maximum directory level (depth) at which ABE is enabled.</p>
<pre>--files-retention-mode NONE   GOVERNANCE   COMPLIANCE</pre>	<p>Sets the retention mode for files saved in the view, if locking (<code>--locking</code>) is enabled.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <code>NONE</code> (default). Files that are saved to the view have no automatic protection but can be manually configured with a retention period or legal hold.</li> <li>• <code>GOVERNANCE</code>. Files that are saved in the view are automatically protected with a retention lock with retention mode set to governance. In this mode, the retention period can be lengthened or shortened.</li> <li>• <code>COMPLIANCE</code>. Files that are saved in the view are automatically protected with a retention lock with retention mode set to compliance. In this mode, the retention period can be lengthened, but not shortened.</li> </ul>

<pre>--default-retention-period DEFAULT_RETENTION</pre>	<p>Sets the default retention period for files that are locked in the view to <code>DEFAULT_RETENTION</code>. Files that are locked automatically using <i>auto-commit</i> will be locked for this period of time, after which they will be unlocked.</p> <p>Files that are locked manually (by setting the <i>atime</i> for the file to a future time) do not use the default retention period.</p> <p>The value <code>DEFAULT_RETENTION</code> must be in the range between the <i>min-retention-period</i> and <i>max-retention-period</i>.</p> <p>Set it as an integer value, including units (m - minutes, h - hours, d - days, y - years).</p> <p>Example: 5d (5 days).</p>
<pre>--max-retention-period MAX_RETENTION</pre>	<p>Sets the maximum retention period for files that are locked in the view to <code>MAX_RETENTION</code>. Files cannot be locked for longer than this period, whether they are locked manually (by setting the <i>atime</i>) or automatically, using <i>auto-commit</i>.</p> <p>It must be larger than the <i>min-retention-period</i>.</p> <p>Set it as an integer value, including units (m - minutes, h - hours, d - days, y - years).</p> <p>Example: 2m (2 months).</p>
<pre>--min-retention-period MIN_RETENTION</pre>	<p>Sets the minimum retention period for files that are locked in the view to <code>MIN_RETENTION</code>. Files cannot be locked for less than this period, whether locked manually (by setting the <i>atime</i>) or automatically, using <i>auto-commit</i>.</p> <p>It must be less than the <i>max-retention-period</i>.</p> <p>Set it as an integer value, including units (m - minutes, h - hours, d - days, y - years).</p> <p>Example: 3d (3 days).</p>
<pre>--auto-commit AUTO_COMMIT</pre>	<p>Sets the auto-commit time to <code>AUTO_COMMIT</code> for files that are locked automatically. These files are locked automatically after the <code>AUTO_COMMIT</code> period elapses from the time the file is saved. Files locked automatically are locked for the <i>default-retention-period</i>, after which they are unlocked.</p> <p>If set, then <code>--default-retention-period</code>, <code>--min-retention-period</code>, and <code>--max-retention-period</code> must also be set.</p> <p>Set it as an integer value, including units (m - minutes, h - hours, d - days, y - years).</p> <p>Example: 5m (5 minutes).</p>

## Block Options

Use the following options with the `--protocol BLOCK` to modify a block subsystem view:

<code>--name NAME</code>	Modifies the name of the subsystem.
<code>--set-is-default-subsystem</code>	Sets the view to be the default subsystem view from which to provision block volumes.
<code>--reset-is-default-subsystem</code>	Resets the default status of a default subsystem view.

## S3 Bucket Logging Options

The following options let you configure S3 Bucket Logging for an *S3 Bucket* view:

<code>--bucket-logging-destination-id DESTINATION_BUCKET_ID</code>	<p>Enables S3 bucket logging for the bucket and determines the destination bucket which will be store the logs.</p> <p><code>DESTINATION_BUCKET_ID</code> is an ID of a view that exposes the destination bucket.</p>
<code>--bucket-logging-prefix PREFIX</code>	<p>Optionally, specify a prefix that will be prepended to each key of a log object uploaded to the destination bucket. This prefix can be used to categorize log objects; for example, if you use the same destination bucket for multiple source buckets.</p> <p>The prefix can be up to 128 characters and must follow <a href="#">S3 object naming rules</a>.</p>
<code>--bucket-logging-key-format SIMPLE_PREFIX  PARTITIONED_PREFIX_EVENT_TIME  PARTITIONED_PREFIX_DELIVERY_TIME</code>	<p>Specify the format for the log object keys:</p> <ul style="list-style-type: none"> <li><code>SIMPLE_PREFIX</code> adds log object keys in the following format: <p><code>[DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]</code></p> <p>This is the default format.</p> </li> <li><code>PARTITIONED_PREFIX_EVENT_TIME</code> and <code>PARTITIONED_PREFIX_DELIVERY_TIME</code> add log object keys in the following format: <p><code>[DestinationPrefix][SourceUsername]/[SourceBucket]/[YYYY]/[MM]/[DD]/[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]</code></p> <p>This format enables timestamp-based partitioning of log objects.</p> <ul style="list-style-type: none"> <li>With <code>PARTITIONED_PREFIX_EVENT_TIME</code>, the partitioning is done based on the time of the logged events occurred.</li> <li>With <code>PARTITIONED_PREFIX_DELIVERY_TIME</code>, the partitioning is done based on the time the log object has been delivered to the destination bucket.</li> </ul> </li> </ul> <p>In the formats:</p>



	<ul style="list-style-type: none"> <li>• [DestinationPrefix] is the optional prefix that prepends keys of log objects uploaded destination bucket. You define this prefix with the <code>--bucket-logging-prefix</code> parameter.</li> <li>• [SourceUsername] is the username for the owner of the bucket being logged.</li> <li>• [SourceBucket] is the bucket being logged.</li> <li>• UTC time is used in timestamps.</li> <li>• [UniqueString] is a unique string added to prevent overwriting of objects.</li> </ul>
<code>--disable-bucket-logging</code>	Disables S3 bucket logging configured for the bucket.


## User Impersonation Options

The following options let you configure [user impersonation](#) for a view:

<code>--enable-user-impersonation</code>	Enables user impersonation.
<code>--disable-user-impersonation</code>	Disables user impersonation.
<code>--user-impersonation-identifier-type ID_TYPE</code>	<p>The type of a user identifier that you are going to specify on the <code>--user-impersonation-identifier</code> option to identify the impersonator (the user account to be used instead of the original user).</p> <p>Valid values for <code>ID_TYPE</code>:</p> <ul style="list-style-type: none"> <li>• <code>username</code> for user's username in format <i>username@domain</i>.</li> <li>• <code>sid_str</code> for user's Security ID (SID).</li> <li>• <code>uid</code> for user's POSIX UID attribute.</li> </ul> <p>This option is required if <code>--enable-user-impersonation</code> is specified on the command.</p>
<code>--user-impersonation-identifier ID</code>	<p>The impersonator user ID or name. The ID or name must be of the type specified on the <code>--user-impersonation-identifier-type</code> option (<i>username@domain</i>, SID or UID).</p> <p>This option is required if <code>--enable-user-impersonation</code> is specified on the command.</p>
<code>--user-impersonation-</code>	The impersonator username.


username NAME	If <code>--user-impersonation-identifier ID</code> and <code>--user-impersonation-username NAME</code> point to different users, the user specified with <code>--user-impersonation-identifier ID</code> becomes the impersonator.
---------------	--

# Indestructible Object Mode Options



**Note**

These options are not supported by default. To use these options, first enable indestructible object mode on the cluster. For full feature information, see [Indestructible Object Mode](#).

<code>--enable-indestructible-object</code>	Enables indestructible object mode on the view.
<code>--disable-indestructible-object</code>	Disables indestructible object mode on the view. This is only allowed when the cluster's indestructibility mechanism is unlocked.
<code>--indestructible-object-duration</code> RETENTION_PERIOD	<p>Modifies the retention period for indestructible object mode. This is only allowed when the cluster's indestructibility mechanism is unlocked.</p> <p>Specify <code>RETENTION_PERIOD</code> as an integer.</p> <p>Default: 8</p> <p>Supported range: 1-400</p> <div>  <div> <p><b>Note</b></p> <p>If you are enabling indestructibility mode, you will not be able to change this retention period after view creation without first <a href="#">unlocking the cluster's indestructibility mechanism</a>, which requires a secure authentication procedure.</p> </div> </div>

# Example

This example changes the view policy used by the view that exposes the `/dev` path of the element store.

```
vcli: admin> view modify --id 2 --path /dev --policy-id 2
```

This example removes an ACE from a share-level ACL:

```
vcli: admin> view modify --id 101 --remove-share-ace-name joej --remove-share-ace-fqdn ad.ar  
andomorg.com
```

**view show**

This command displays details of a view.

**Usage**

```
view show --id ID  
          [--global-synchronization]  
          [--s3]  
          [--share-level-acl]  
          [--worm]
```

**Required Parameters**

--id ID	Specify the ID of the view you want to view.
---------	--

**Options**

--global-synchronization	<p>If the view supports global synchronization, this option displays details of synchronization between the view and other views that support global synchronization.</p> <p>When a view supports global synchronization, the cluster checks for views on paths protected by the same replication group as the view path and synchronizes file handles with those views. The command output shows you if there is a matching view on each remote peer that has global synchronization enabled, and whether it is synced with this view.</p> <p>The global synchronization feature enables views to support <a href="#">seamless replication failover</a>.</p>
--s3	Displays S3 details.
--share-level-acl	Displays share-level ACL details.
--worm	Display WORM details for the View.

**Example**

```
vcli: admin> view show --id 3
```

```

+-----+
+-----+
+
| ID                      | 3
|
| Path                    | /blockstorage
|
| Alias                   | blocktarget1
|
| Share                   |
|
| Bucket                  |
|
| Bucket-owner            | None
|
| Policy                  | default
|
| Protocols               | ['BLOCK']
|
| Cluster                 | docs-system1-gcp
|
| Physical-capacity       | 0
|
| Logical-capacity        | 0
|
| WORM                    | False
|
| Is-remote               | False
|
| Created time            | 2025-02-26 13:01:36
|
| Live Monitoring         | False
|
| Qos-policy              | None
|
| Tenant-id              | 1
|
| Bulk-permission-update-state | None
|
| Bulk-permission-update-progress | None
|
| Files-retention-mode    | NONE
|
| Abe-protocols           | []
|
| Abe-max-depth           | None
|
| Global Synchronization  | False
|
| ABAC tags               | []
|
| User-impersonation      | {'enabled': False, 'identifier': '', 'identifier_type':
| ', 'login_name': '', 'username': ''} |
| Is-default-subsystem    | False
|
| Name                    | blocktarget1
|
| Nqn                     | nqn.2024-08.com.vastdata:c4d2b679-17c4-5075-b8c2-07941024
6670:default:blocktarget1
+-----+
+-----+
+

```

This example displays S3 details of a view:

```
vccli: admin> view show --id 26 --s3
```

```

+-----+-----+
| Path          | /bucket-jovial-lyrebird |
| Bucket        | bucket-jovial-lyrebird  |
| Bucket-owner  | lean-cerberus           |
| S3-versioning | False                   |
| Allow-s3-anonymous-access | False                 |
| Bucket Creators (Users) | []                     |
| Bucket Creators (Groups) | []                   |
| S3-unverified-lookup | False                  |
+-----+-----+

```

This example shows share-level ACL details for a view.

```

vcli: admin> view show --id 5 --share-level-acl
Share-level ACL is disabled
Share-level ACL is not configured

```

This example shows information about global synchronization for a view that has global synchronization enabled. In this case, there is a view on a remote replicated path on a remote peer but the view does not have global synchronization enabled. In order to complete the configuration of global synchronization for the replication path, a new view must be created on the remote peer with global synchronization enabled.

```

vcli: admin> view show --id 13 --global-synchronization
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| Path      | Cluster name | Peer name | Sync status | Failure-reason |
|           |             |          |            |               |
+-----+-----+-----+-----+
| /rep_dir | ClusterA    | peerAtoB | Error       | Remote view does not support global syn
chronization |
+-----+-----+-----+-----+
+-----+-----+-----+-----+

```

This example shows WORM details for a view.

```

vcli: admin> view show --id 9 --worm
+-----+-----+
| Path          | /inventive-cockatoo-fee5-view-622d |
| WORM          | True                                |
| Files-retention-mode | N/A                                |
| Default-retention-period |                                     |
| Min-retention-period  | N/A                                |
| Max-retention-period  | N/A                                |
| Auto-commit        | N/A                                |
+-----+-----+

```

## view stop-bulk-permission-update

This command stops a bulk permission update task running on a view.

When you stop a running bulk permission update, the changes that the task has already made are not rolled back.

## Usage

```

view stop-bulk-permission-update --id ID

```

## Required Parameters

<code>--id ID</code>	Specify the ID of the view where a bulk permission update task is running.
----------------------	--

## Example

To stop a bulk permission update task on view 3:

```
vcli: admin> view stop-bulk-permission-update --id 3
```

# viewpolicy commands


## viewpolicy create

This command creates a view policy. Every view has a policy. The view policy specifies part of the view's configuration. One view policy can be applied to any number of views.



## Usage

```
viewpolicy create --name NAME
                  --flavor NFS|SMB|MIXED_LAST_WINS|S3_NATIVE
                  --auth-source RPC|PROVIDERS|RPC_AND_PROVIDERS
[--access-flavor NFS4|SMB|ALL]
[--path-length LCD|NPL]
[--allowed-characters LCD|NPL]
[--gid-inheritance linux|bsd]
[--atime-frequency ATIME_FREQUENCY]
[--nfs-read-write [HOSTS]]
[--nfs-read-only [HOSTS]]
[--nfs-no-squash [HOSTS]]
[--nfs-root-squash [HOSTS]]
[--nfs-all-squash [HOSTS]]
[--enable-nfs-return-open-permissions|--disable-nfs-return-open-permissions]
[--enable-nfs-posix-acl|--disable-nfs-posix-acl]
[--enable-32bit-fileid|--disable-32bit-fileid]
[--enable-expose-id-in-fsid|--disable-expose-id-in-fsid]
[--nfs-trash-access [HOSTS]]
[--nfs4-case-sensitive|--nfs4-case-insensitive]
[--enable-nfs4-enforce-tls|--disable-nfs4-enforce-tls]
[--smb-file-mode SMB_FILE_MODE]
[--smb-directory-mode SMB_DIRECTORY_MODE]
[--permission-per-vip-pool <pool ID 1>=RW|RO,<pool ID 2>=RW|RO,...]
[--nfs-minimal-protection-level NONE|SYSTEM|KRB_AUTH_ONLY|KRB_INTEGRITY|KRB_PRIVACY]
[--s3-visibility USERS]
[--s3-visibility-groups GROUPS]
[--enable-s3-default-policy|--disable-s3-default-policy]
[--s3-special-chars|--s3-special-chars-not-supported]
[--s3-read-write [HOSTS]]
[--s3-read-only [HOSTS]]
[--smb-read-write [HOSTS]]
[--smb-read-only [HOSTS]]
[--enable-apple-sid|--disable-apple-sid]
[--smb-is-ca|--smb-is-not-ca]
[--audit-protocols PROTOCOLS]
[--audit-operations OPERATIONS]
[--audit-options OPTIONS]
[--enable-audit-settings|--disable-audit-settings]
[--enable-access-to-snapshot-dir-in-subdirs|--disable-access-to-snapshot-dir-in-subdirs]
[--enable-visibility-of-snapshot-dir|--disable-visibility-of-snapshot-dir]
[--tenant-id ID][--serve-all-tenants]
[--disable-read-leases|--enable-read-leases]
[--disable-write-leases|--enable-write-leases]
[--disable-handle-leases|--enable-handle-leases]
[--s3-flavor-allow-free-listing|--s3-flavor-disallow-free-listing]
[--enable-s3-flavor-detect-full-pathname|--disable-s3-flavor-detect-full-pathname]
[--enable-inherit-parent-mode-bits|--disable-inherit-parent-mode-bits]
```

# Required Parameters

<pre>--name NAME</pre>	<p>Sets a unique name for the view policy.</p>
<pre>--flavor NFS SMB MIXED_LAST_WINS S3_NATIVE</pre>	<p>Sets a security flavor for the view policy:</p> <ul style="list-style-type: none"> <li>• <b>NFS.</b> Treats NFS as a native protocol and other protocols as non-native protocols. Supports NFSv3, SMB and S3. Supports NFSv4.1 without support for NFSv4.1 ACLs.</li> </ul> <p>Files and directories created by SMB clients receive a set of initial permission bits, configurable using the <code>--smb-file-mode</code> and <code>--smb-directory-mode</code> options.</p> <ul style="list-style-type: none"> <li>• <b>SMB.</b> Treats SMB as a native protocol and other protocols as non-native protocols. Supports SMB, NFSv3, NFSv4.1 and S3.</li> <li>• <b>MIXED_LAST_WINS.</b> Allows file and directory permissions to be set and modified by all clients. Includes support for NFSv4.1 clients to set NFSv4.1 ACLs. Supports SMB, NFSv3, NFSv4.1 and S3.</li> </ul> <p>See also <code>--access-flavor</code> for further control.</p> <ul style="list-style-type: none"> <li>• <b>S3_NATIVE.</b> Treats S3 as a native protocol and other protocols as non-native protocols. Supports S3, NFSv3 and SMB. Supports NFSv4.1 without support for NFSv4.1 ACLs.</li> </ul> <p>For more information about security flavors, see <a href="#">Controlling File and Directory Permissions Across Protocols</a>.</p>
<pre>--auth-source RPC PROVIDERS RPC_AND_PROVIDERS</pre>	<p>Specifies which source is trusted for the user's group memberships, when users' access to the view is authorized. Possible values:</p> <ul style="list-style-type: none"> <li>• <b>RPC.</b> For NFSv3 only. The GIDs declared in the NFS request as the user's leading group and auxiliary groups are trusted and provider-sourced groups are not considered.</li> </ul> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;">  <p><b>Note</b></p> <p>This option is not supported for NFSv4.1.</p> </div> <ul style="list-style-type: none"> <li>• <b>PROVIDERS.</b> Group memberships retrieved from authorization providers are considered as the user's group memberships. The GIDs declared in the request are ignored.</li> </ul>



	<div>  <p><b>Note</b></p> <p>This option is required for views that have SMB enabled.</p> <p>Similarly, where NFSv4.1 is enabled in the view, if <i>Kerberos Authentication Minimal protection level</i> is set to Kerberos Auth-only, then this option must be used.</p> </div> <ul style="list-style-type: none"> <li>• <code>RPC_AND_PROVIDERS</code>. Both the GIDs declared in an NFS request and group memberships retrieved from authorization providers are considered. If the GID provided by the client does not match the GID retrieved from the authorization provider, the GID from the client is set.</li> </ul> <div>  <p><b>Note</b></p> <p>If Kerberos authentication is used by NFSv4.1 clients, the groups declared in the RPC are ignored.</p> </div>
--	---

# General Options

<pre>--permission-per-vip-pool &lt;pool ID 1&gt;=RW RO,&lt;pool ID 2&gt;=RW RO,...</pre>	<p>Grants read/write or read-only access to clients from certain virtual IP pools.</p> <p>Specify a comma-separated list of virtual IP pool IDs with indication of the access type (RW for read/write or RO for read-only) for each of the pools, for example:</p> <pre>--permission-per-vip-pool 1=RW,2=RW,3=RO</pre>
<pre>--tenant-id TENANT_ID</pre>	<p>Associates the view policy with a specific tenant.</p>
<pre>--serve-all-tenants</pre>	<p>Sets the view policy to serve all tenants (default setting).</p>

# Protocol Auditing Options



## Note

Any audit settings that are enabled globally for the cluster are enabled for all views. Auditing settings in a view policy can only add more protocols, operations and/or options to the audit performed on views that use this view policy.

<code>--audit-protocols</code> PROTOCOLS	<p>Lists access protocols for which you are enabling or disabling protocol auditing on views that use this view policy.</p> <p>Use this parameter together with <code>--enable-audit-settings</code> or <code>--disable-audit-settings</code> to enable or disable auditing of the specified protocols.</p> <p>When specifying <code>--audit-protocols</code>, you must also specify <code>--audit-operations</code> and/or <code>--audit-options</code>.</p> <p>Specify PROTOCOLS as a comma-separated list of values. Valid values:</p> <ul style="list-style-type: none"><li>• NFSv3</li><li>• NFSv4.1</li><li>• SMB</li><li>• S3</li><li>• NDB (Database)</li></ul>
<code>--audit-operations</code> OPERATIONS	<p>Lists categories of protocol operations for which you are enabling or disabling protocol auditing on views that use this view policy.</p> <p>Use this parameter together with <code>--audit-protocols</code> and either <code>--enable-audit-settings</code> or <code>--disable-audit-settings</code> to enable or disable auditing of the specified protocol operations for views that use this view policy.</p> <p>Specify OPERATIONS as a comma-separated list of values, each of which specifies a <a href="#">category of operations</a> being audited. Valid values:</p> <ul style="list-style-type: none"><li>• <code>create_delete_files_dirs_objects</code>. Operations that create or delete files, directories or objects.</li><li>• <code>modify_data</code>. Operations that modify data.</li><li>• <code>modify_data_md</code>. Operations that modify metadata.</li><li>• <code>read_data</code>. Operations that read data.</li><li>• <code>read_data_md</code>. Operations that read metadata.</li></ul>

	<ul style="list-style-type: none"> <li>• <code>session_create_close</code>. Session creation and closing operations for sessions that use Kerberos 5 authentication (<code>krb5</code>, <code>krb5i</code>, or <code>krb5p</code>).</li> </ul>
<code>--audit-options</code> <code>OPTIONS</code>	<p>Lists audit options to enable or disable on views that use this view policy.</p> <p>Use this parameter together with <code>--audit-protocols</code> and either <code>--enable-audit-settings</code> or <code>--disable-audit-settings</code> to enable or disable the specified options for the specified protocols.</p> <p>Specify <code>OPTIONS</code> as a comma-separated list of values. Valid values:</p> <ul style="list-style-type: none"> <li>• <code>log_full_path</code>. If enabled (default for all protocols), audit records contain the full Element Store path to the requested resource. This may affect performance. When disabled, the view path is recorded.</li> <li>• <code>log_username</code>. Disabled by default. If enabled, audit records contain the username (if a username can be retrieved from the auth provider).</li> </ul>
<code>--enable-audit-settings</code>	<p>Enables audit settings specified in the same command line by the <code>--audit-protocols</code>, <code>--audit-operations</code> and <code>--audit-options</code> parameters.</p> <p>Any auditing protocols, operations options that are already enabled in the policy remain enabled.</p> <p>Any audit settings (protocols, operations or options) that are already enabled in the view policy remain enabled.</p>
<code>--disable-audit-settings</code>	<p>Disables audit settings specified in the same command line by the <code>--audit-protocols</code>, <code>--audit-operations</code> and <code>--audit-options</code> parameters.</p> <p>Any audit settings (protocols, operations or options) that are already enabled in the view policy and that are not specified in the same command line remain enabled.</p>

## NFS Security Flavor Options

<code>--smb-file-mode</code> <code>SMB_FILE_MODE</code>  <code>--smb-directory-mode</code> <code>SMB_DIRECTORY_MODE</code>	<p>For multiprotocol views, if the security flavor is NFS, specify default Unix permission bits for files (<code>--smb-file-mode</code>) and directories (<code>--smb-directory-mode</code>). These are applied as initial permissions to files and directories created by SMB or S3 clients.</p> <p>Specify <b>SMB_FILE_MODE</b> and <b>SMB_DIRECTORY_MODE</b> in three digit numeric notation, in which each digit represents a component of the permissions: user, group and others (in that order). Each digit is the sum of the following component bits:</p> <ul style="list-style-type: none"> <li>• If reading is permitted, the read bit adds 4 to the component.</li> <li>• If writing is permitted, the write bit adds 2 to the component.</li> <li>• If execution is permitted, the execute bit adds 1 to the component</li> </ul>
--	--

	<h2>Example</h2> <p>Supposing you want to set the following permissions for file mode:</p> <table><tr><td></td><td><b>user</b></td><td><b>group</b></td><td><b>others</b></td></tr><tr><td>read</td><td>permitted</td><td>permitted</td><td>permitted</td></tr><tr><td>write</td><td>permitted</td><td>not permitted</td><td>not permitted</td></tr><tr><td>execute</td><td>not permitted</td><td>not permitted</td><td>not permitted</td></tr></table> <p>The user's read bit (4) and a write bit (2) total 6, the group and others each have a read bit only so that is 4 each. Therefore, you set the permission bits to 644:</p> <pre>--smb-file-mode 644</pre> <h2>Defaults</h2> <p>SMB file mode permission bits: 644</p> <p>SMB directory mode permission bits: 755</p>		<b>user</b>	<b>group</b>	<b>others</b>	read	permitted	permitted	permitted	write	permitted	not permitted	not permitted	execute	not permitted	not permitted	not permitted
	<b>user</b>	<b>group</b>	<b>others</b>														
read	permitted	permitted	permitted														
write	permitted	not permitted	not permitted														
execute	not permitted	not permitted	not permitted														
--enable-inherit-parent-mode-bits	If specified, permission mode bits for files/objects and directories/buckets created by protocols other than NFS on a view controlled with the NFS security flavor, inherit their permission mode bites from the parent directory.																
--disable-inherit-parent-mode-bits	If specified, permission mode bits for files/objects and directories/buckets created by protocols other than NFS on a view controlled with the NFS security flavor, are taken from the view policy definition (instead of inheriting them from the parent directory).																

## S3 Options

<pre>-- s3-visibility USERS</pre>	<p>Specify users to enables those users to list buckets that are created using this policy even if they do not have permission to access those buckets.</p> <p>When an S3 user sends a bucket listing request, the command returns a list of all buckets the user owns and all buckets that they have this listing permission for, even if they do not have permission to access those buckets.</p> <p>Specify <code>USERS</code> as a comma separated list of user names.</p>
-----------------------------------	--

	<p>Example: <code>--s3-visibility jsmith,sjobs</code></p>
<p><code>--s3-visibility-groups GROUPS</code></p>	<p>Specify groups to enable members of those groups to list buckets that are created using this policy even if they do not have permission to access those buckets.</p> <p>Specify <b>GROUPS</b> as a comma separated list of group names.</p> <p>Example: <code>--s3-visibility-groups interns,deptheads</code></p>
<p><code>--enable-s3-default-policy</code></p>	<p>Specify this option to use this policy as the default view policy for new buckets created via VAST S3 API, where the user is not associated with an S3 endpoint.</p>
<p><code>--disable-s3-default-policy</code></p>	<p>Specify this option to stop using this policy as the default view policy for new buckets created via VAST S3 API.</p>
<p><code>--s3-special-chars</code></p>	<p>Allows S3 object names containing character combinations that are not compatible with other access protocols, such as names containing <code>//</code> or <code>../</code>.</p>
<p><code>--s3-special-chars-not-supported</code></p>	<p>Prohibits S3 object names containing character combinations that are not compatible with other access protocols.</p>
<p><code>--s3-flavor-allow-free-listing</code></p>	<p>When this option is specified, NFS and SMB clients are allowed or denied access based on the full resource names specified in the identity policies. This means that the identity policy can refer to particular files and directories, rather than to the bucket as a whole.</p>
<p><code>--s3-flavor-disallow-free-listing</code></p>	<p>When this option is specified, NFS and SMB clients are allowed or denied access based on the bucket name in the identity policy, rather than on the full resource names.</p>
<p><code>--enable-s3-flavor-detect-full-pathname</code></p>	<p>When this option is specified, NFS and SMB clients are able to list bucket views and their subdirectories regardless of individual object permissions.</p>
<p><code>--disable-s3-flavor-detect-full-</code></p>	<p>When this option is specified, listing a directory by an NFS or SMB client is allowed or denied based on the identity policies, rather than on individual object permissions.</p>

pathname	
----------	--

# S3 Host Access Options

These options set which S3 client hosts can access the view with which access types.

For each option, `HOSTS` can be specified as a comma separated series of any of the following:

- A single IP.
- A fully qualified domain name (FQDN).



## Note

The following rules apply when specifying FQDNs:

- Maximum total length of an FQDN; 255 characters.
- Each domain name label is limited to 63 characters.
- Allowed characters: a-z, 0-9, hyphen (-).
- A label cannot start with a hyphen.

- A subnet indicated by CIDR notation. For example: 1.1.1.1/24.
- A range of IPs indicated by an IP address with '\*' as a wildcard in place of any of the 8-bit fields in the address. For example, 3.3.3.\*, or 3.3.\*.\*.
- A range of IPs where the starting and ending IPs are separated by a hyphen, for example: 192.0.2.3-22

The access types comprise read/write and read-only access.

If a host is specified with multiple entries in mutually exclusive access types, the conflict is resolved as follows:


- An IP overrides a CIDR, and a CIDR overrides a wildcard expression.
- If a conflict remains after the previous rule is applied, the read-only setting overrides the read/write setting.


On new installations, if a view policy does not have any host-based access rules defined for a specific access protocol, access is denied for all hosts. On upgraded deployments, all hosts are allowed access if no host-based access rules are defined..

<pre>--s3-read-write [HOSTS]</pre>	<p>Controls which S3 client hosts have read/write access to the view.</p> <p>By default, all hosts have read/write access.</p> <p>To remove all hosts from read/write access, include this option without any values.</p> <p>To restrict read/write access to specific hosts, specify <code>HOSTS</code> according to the format description above this table.</p>
------------------------------------	--

	For example: <code>--s3-read-write 98.51.100.1,98.51.100.2</code>
<code>--s3-read-only [HOSTS]</code>	Specifies which S3 client hosts have read-only access to the view. Specify <code>HOSTS</code> according to the format description above this table.

## SMB Options

<code>--enable-apple-sid</code>	For use when connecting from Mac clients to SMB shares, this option enables Security IDs (SIDs) to be returned in Apple compatible representation.
<code>--disable-apple-sid</code>	Disables <code>--enable-apple-sid</code> .
<code>--smb-is-ca</code>	<p>When specified, the SMB share exposed by the view is set as <i>continuously available</i>, which allows SMB3 clients to request use of persistent file handles and keep their connections to this share in case of a failover event.</p> <div>  <p><b>Note</b></p> <p>This option requires that the client uses SMBv3.</p> </div> <p>By default, continuous availability is disabled.</p>
<code>--smb-is-not-ca</code>	Stops exposing the view path as a <i>continuously available</i> SMB3 share.
<code>--disable-read-lease</code>	Disables SMB client read leases so that SMB clients cannot cache data read from the server.
<code>--enable-read-lease</code>	Enables SMB client read leases to let SMB clients cache data read from the server.
<code>--disable-write-lease</code>	Disables SMB client write leases so that SMB clients cannot cache data written to the server or set byte-range locks on files and directories.

<code>--enable-write-lease</code>	Enables SMB client write leases to let SMB clients cache data written to the server and set byte-range locks on files and directories.
<code>--disable-handle-lease</code>	<p>Disables handle leases so that SMB clients cannot delay closing handles on files or directories.</p> <div>  <p><b>Note</b></p> <p>Disabling handle leases may impact client resiliency to network and server failures.</p> </div>
<code>--enable-handle-lease</code>	Enables SMB client handle leases to let SMB clients delay closing of handles files or directories.

## SMB Host Access Options

These options set which SMB client hosts can access the view with which access types.

For each option, `HOSTS` can be specified as a comma separated series of any of the following:

- A single IP.
- A subnet indicated by CIDR notation. For example: 1.1.1.1/24.
- A range of IPs indicated by an IP address with '\*' as a wildcard in place of any of the 8-bit fields in the address. For example, 3.3.3.\*, or 3.3.\*.\*.
- A range of IPs where the starting and ending IPs are separated by a hyphen, for example: 192.0.2.3-22
- A fully qualified domain name (FQDN).



### Note

The following rules apply when specifying FQDNs:

- Maximum total length of an FQDN; 255 characters.
- Each domain name label is limited to 63 characters.
- Allowed characters: a-z, 0-9, hyphen (-).
- A label cannot start with a hyphen.

The access types comprise read/write and read-only access.




If a host is specified with multiple entries in mutually exclusive access types, the conflict is resolved as follows:


- An IP overrides a CIDR, and a CIDR overrides a wildcard expression.
- If a conflict remains after the previous rule is applied, the read-only setting overrides the read/write setting.

On new installations, if a view policy does not have any host-based access rules defined for a specific access protocol, access is denied for all hosts. On upgraded deployments, all hosts are allowed access if no host-based access rules are defined.

<code>--smb-read-write [HOSTS]</code>	<p>Controls which SMB client hosts have read/write access to the view.</p> <p>By default, all hosts have read/write access.</p> <p>To remove all hosts from read/write access, include this option without any values.</p> <p>To restrict read/write access to specific hosts, specify <code>HOSTS</code> according to the format description above this table.</p> <p>For example: <code>--smb-read-write 98.51.100.1,98.51.100.2</code></p>
<code>--smb-read-only [HOSTS]</code>	<p>Specifies which SMB client hosts have read-only access to the view.</p> <p>Specify <code>HOSTS</code> according to the format description above this table.</p>

## Advanced Multi-Protocol Options

<code>--access-flavor NFS4   SMB   ALL</code>	<div><h3>Caution</h3><p>Changing this setting when already in effect on a view that is being used by clients could lead to unexpected behavior and is not advised.</p></div> <p>If <code>--flavor</code> is <code>MIXED_LAST_WINS</code>, this parameter can be used to control which protocols can set file permissions, including Access Control Lists (ACLs) and setting user-owner and group-owner of files.</p> <div><h3>Note</h3><p>NFSv3 is unaffected by this setting. NFSv3 users can set permission mode bits in <i>Mixed Last Wins</i> security flavor regardless of this setting.</p></div> <p>Attempts by the blocked protocol fail silently. See <a href="#">Controlling File and Directory Permissions Across Protocols</a> for details.</p> <p>Possible values:</p>
---	--

	<ul style="list-style-type: none"> <li>• <b>NFS4.</b> Allows NFSv4.1 to set file permissions, and blocks SMB users from setting file permissions.</li> <li>• <b>SMB.</b> Allows SMB users to set file permissions, and blocks NFSv4.1 users from setting file permissions.</li> </ul> <div>  <p><b>Note</b></p> <p>Linux super user cannot bypass this blockage.</p> </div> <ul style="list-style-type: none"> <li>• <b>ALL</b> (default). Allows both NFSv4.1 and SMB to set file permissions, as well as NFSv3.</li> </ul>
<pre>--path-length LCD NPL</pre>	<p>Specifies the policy for limiting file path component name length.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <b>LCD</b> (default) (=Lowest Common Denominator). Imposes the lowest common denominator file path component length limit of all VAST Cluster-supported protocols, regardless of the specific protocol enabled on a specific view.</li> <li>• <b>NPL</b> (=Native Protocol Limit). Imposes no limitation beyond that of the client protocol.</li> </ul> <div> <p><b>Caution</b></p> <p>If you select this mode in a view policy and then in the future expose a view using this policy to a previously not exposed protocol, that view might contain files that won't be accessible by the newly added protocol, due to the limitations of that protocol.</p> </div>
<pre>--allowed-characters LCD NPL</pre>	<p>Specifies the policy for which characters are allowed in file names.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <b>LCD</b> (default). Allows only characters allowed by all VAST Cluster-supported protocols, regardless of the specific protocol enabled on a specific view.</li> <li>• <b>NPL.</b> Imposes no limitation beyond that of the client protocol.</li> </ul> <div> <p><b>Caution</b></p> <p>If you select this mode in a view policy and then in the future expose a view using this policy to a previously not exposed protocol, that view might contain files that won't be accessible by the newly added protocol, due to the limitations of that protocol.</p> </div>

<pre>--gid- inheritance linux bsd</pre>	<p>Specifies how files receive their owning group when they are created.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <b>linux</b> (default). Each new file inherits its owning group from the group ID of the user who creates the file.</li> <li>• <b>bsd</b>. Each new file inherits its owning group from the group ID of the parent directory.</li> </ul>
---	--

## NFS Host Access Options

These options determine which NFS client hosts can access the view with which access types.

The hosts (`HOSTS`) can be specified including any of the following items separated by commas:

- A single IP.
- A fully qualified domain name (FQDN).



### Note

The following rules apply when specifying FQDNs:

- Maximum total length of an FQDN; 255 characters.
- Each domain name label is limited to 63 characters.
- Allowed characters: a-z, 0-9, hyphen (-).
- A label cannot start with a hyphen.

- A subnet indicated by CIDR notation. For example: 1.1.1.1/24.
- A subset of IPs specified as an IP address with '\*' as a wildcard in place of any of the 8-bit fields in the address. For example, 3.3.3.\*, or 3.3.\*.\*.
- A range of IPs where the starting and ending IPs are separated by a hyphen, for example: 192.0.2.3-22
- A netgroup, prefixed with an '@'. For information about using netgroups, see [Using Netgroups to Authorize Hosts](#).

The access types include read/write or read-only access, the squash policy, and trash folder access.


If the configuration specifies that a host has mutually exclusive access types, the conflict is resolved as follows:

- An IP overrides a netgroup, a netgroup overrides a netmask, and a netmask overrides a wildcard expression.
- If a conflict remains after the previous rule is applied, then:
  - `--nfs-read-only` overrides `--nfs-read-write`.
  - `--nfs-all-squash` overrides `--nfs-root-squash`.

- `--nfs-root-squash` overrides `--nfs-no-squash`.

On new installations, if a view policy does not have any host-based access rules defined for a specific access protocol, access is denied for all hosts. On upgraded deployments, all hosts are allowed access if no host-based access rules are defined.

<code>--nfs-read-write</code> <code>[HOSTS]</code>	<p>Determines which NFS client hosts have read/write access to the view.</p> <p>By default, all hosts have read/write access.</p> <p>To restrict read/write access to specific hosts, specify <code>HOSTS</code> as shown above the table. For example: <code>--nfs-read-write 98.51.100.1,98.51.100.2</code></p> <p>To prohibit read/write access for all hosts, specify this option without any values.</p> <p>To create a reversed rule, e.g. a rule that allows read/write access from all IPs except the one specified, prepend the IP address with a tilde, for example: <code>~192.0.2.0</code></p>
<code>--nfs-read-only</code> <code>[HOSTS]</code>	<p>Determines which NFS client hosts have read-only access to the view.</p> <p>Specify <code>HOSTS</code> as shown above the table.</p>
<code>--nfs-no-squash</code> <code>[HOSTS]</code>	<p>Determines which hosts have <i>no squash</i> access. With <i>no squash</i>, all operations are supported. Use this option if you trust the root user not to perform operations that will corrupt data.</p> <p>This option is not relevant for NFSv4.1 users if Kerberos is used, since Active Directory does not include the 'root' user principal by default and since the handling of credentials for the user with UID 0 depends on configuration of the <code>rpc.gssd</code> service.</p> <p>Specify <code>HOSTS</code> as shown above the table.</p>
<code>--nfs-root-squash</code> <code>[HOSTS]</code>	<p>Determines which hosts have <i>root squash</i> access. With <i>root squash</i>, the root user is mapped to nobody for all file and folder management operations on the export. This enables you to prevent the strongest super user from corrupting all user data on the VAST Cluster.</p> <p>This option is not relevant for NFSv4.1 users if Kerberos is used, since Active Directory does not include the 'root' user principal by default and since the handling of credentials for the user with UID 0 depends on configuration of the <code>rpc.gssd</code> service.</p> <p>By default, all hosts have <i>root squash</i> access.</p> <p>To restrict root squash to specific hosts, specify <code>HOSTS</code> according to the format description above this table.</p> <p>To remove root squash access for all hosts, include this option without values.</p>
<code>--nfs-all-squash</code> <code>[HOSTS]</code>	<p>Determines which hosts have <i>all squash</i> access. With <i>all squash</i>, all client users are mapped to nobody for all file and folder management operations on the export.</p> <p>Specify <code>HOSTS</code> as shown above the table.</p>

<pre>--nfs-trash-access [HOSTS]</pre>	<p>Determines which hosts have access to the trash folder, if the trash folder is enabled for the cluster.</p> <p>Granting this permission gives hosts the ability to delete files by moving them into the <a href="#">trash folder</a>, from which they are automatically deleted. Requires that the host is listed as <i>No Squash</i> (<code>--nfs-no-squash</code>).</p> <div>  <div> <p><b>Note</b></p> <p>This option is applicable for NFSv3 only. The <i>Trash folder</i> feature is not supported for NFSv4.1 clients.</p> </div> </div> <p>Specify <code>HOSTS</code> as shown above the table.</p>
---------------------------------------	--

# Advanced NFS Options

<pre>--atime-frequency ATIME_FREQUENCY</pre>	<p><i>atime</i> is a metadata attribute of NFS files that represents the last time the file was updated. <i>atime</i> is updated on read operations if the difference between the current time and the file's atime value is greater than the configured atime frequency. Consider that a very low value might have a performance impact if high numbers of files are being read.</p> <p>Specify <code>ATIME_FREQUENCY</code> as an integer followed by a unit of time (s = seconds, m= minutes, h=hours, d=days).</p> <p>Example: <i>1h</i></p> <p>Default: <i>0</i>, which means no atime updates.</p>
<pre>--nfs-return-open-permissions</pre>	<p>Sets the NFS server to unilaterally return open (777) permission for all files and directories when responding to client side access checks.</p> <p>This setting works around a permissions issue that occurs with Windows clients. Windows clients perform NFSv3 access checks before executing read/write requests. This client side check uses the UID and the primary GID of the user without taking into account secondary GIDs. If the check fails, requests are not executed. This means that some permissions may not be honored as</p>

	<p>they should be, such as those based on secondary groups.</p> <p>When <i>return open permissions</i> is enabled, VAST Cluster returns open permissions for client side access checks, so that the Windows client allows access rights and executes read/write requests. VAST Cluster does a proper permission check when the request is executed.</p> <div> <p><b>Caution</b></p> <p>Use this feature with caution if Windows client systems are shared by more than one user, since the following security breach could occur: While a user is accessing a file with correct permissions and the file is cached in memory on the Windows system, if another user tries to access the same file, access is incorrectly allowed. No proper access check is done for the second user.</p> </div>
<code>--disable-nfs-return-open-permissions</code>	<p>Disables the NFS <i>return open permissions</i> setting. See <code>--nfs-return-open-permissions</code>.</p>
<code>--enable-nfs-posix-acl</code>	<p>Enables full support of extended POSIX Access Control Lists (ACL). By default, VAST Cluster supports the traditional POSIX file system object permission mode bits, (minimal ACL mode) in which each file has three ACL entries defining the permissions for the owner, owning group, and others, respectively. To learn more about POSIX ACL, see <a href="https://linux.die.net/man/5/acl">https://linux.die.net/man/5/acl</a>.</p>



### Note

The Posix ACL setting is relevant for NFSv3 only.



### Note

The Posix ACL setting is supported only with the NFS security flavor.




### Note

The [setfacl Linux command](#) is blocked if this option is not enabled.




### Note

- NFSv4.1 does not support POSIX ACLs.
- If clients have created files and directories with POSIX ACLs using NFSv3 and then they start to access those files and directories via NFSv4.1, the POSIX ACLs will have no effect.
- If this setting is enabled, POSIX ACLs may be used via NFSv3 only. They cannot be used via NFSv4.1.
- Support for NFSv4.1 ACLs requires *Mixed Last Wins* security flavor and is not supported

	 concurrently with POSIX ACLs for NFSv3.
<code>--disable-nfs-posix-acl</code>	Disables support for extended POSIX ACLs, restoring default minimal ACL mode.
<code>--enable-32bit-fileid</code>	Sets the VAST Cluster's NFS server to use 32-bit file IDs. This setting supports legacy 32-bit applications running over NFSv3.
<code>--disable-32bit-fileid</code>	Disables 32-bit file IDs (default).
<code>--nfs-minimal-protection-level NONE SYSTEM KRB_AUTH_ONLY KRB_INTEGRITY KRB_PRIVACY</code>	<p>Set the Kerberos Authentication Minimal protection level to accept from NFSv4.1 client RPCs:</p> <ul style="list-style-type: none"> <li>• <code>KRB_PRIVACY</code>. Allows client mounts only if they use Kerberos 5 authentication with privacy checking (<i>krb5p</i>), the highest level Kerberos security mode.</li> <li>• <code>KRB_INTEGRITY</code>. Allows client mounts only if they use either Kerberos 5 authentication with privacy checking (<i>krb5p</i>) or Kerberos 5 authentication with integrity (<i>krb5i</i>).</li> <li>• <code>KRB_AUTH_ONLY</code>. Allows client mounts with Kerberos authentication only and allows any of the three Kerberos security modes (<i>krb5</i>, <i>krb5i</i>, or <i>krb5p</i>).</li> <li>• <code>SYSTEM</code>. Allows client mounts using either the AUTH_SYS RPC security flavor (the traditional default NFS authentication scheme) or with any of the three Kerberos security modes (<i>krb5</i>, <i>krb5i</i>, or <i>krb5p</i>).</li> <li>• <code>NONE</code>. Allows client mounts with the AUTH_NONE (anonymous access), or AUTH_SYS RPC security flavors, or with any of the three Kerberos security modes (<i>krb5</i>, <i>krb5i</i>, or <i>krb5p</i>).</li> </ul>



<pre>--nfs-case-sensitive</pre>	<p>When this option is specified, VAST Cluster honors case in the names of files or directories accessed through NFSv4.1.</p> <p>This is the default behavior.</p> <div data-bbox="992 361 1464 680"> <p><b>Caution</b></p> <p>Changing the NFSv4.1 case insensitivity setting for an existing view may have unpredictable results.</p> </div>
<pre>--nfs-case-insensitive</pre>	<p>When this option is specified, VAST Cluster does not honor case in the names of files or directories accessed through NFSv4.1.</p> <div data-bbox="992 869 1464 1188"> <p><b>Caution</b></p> <p>Changing the NFSv4.1 case insensitivity setting for an existing view may have unpredictable results.</p> </div>
<pre>--enable-nfs4-enforce-tls</pre>	<p>Enforces TLS encryption between the NFS4.1 client and the cluster. When this setting is enabled, the <i>Kerberos Authentication Minimal protection level</i> must be set to <i>System</i> or <i>None</i>.</p> <div data-bbox="992 1440 1464 1785"> <p> <b>Note</b></p> <p>TLS encryption requires further setup in addition to this view policy setting. For details, see <a href="#">Configuring TLS Encryption with NFSv4.1</a>.</p> </div>
<pre>--disable-nfs4-enforce-tls</pre>	<p>Disables enforcing of TLS encryption between the NFSv4.1 client and the cluster.</p>

# Snapshot Options

<code>--enable-access-to-snapshot-dir-in-subdirs</code>	<p>Enables accessible <i>.snapshot</i> directories under all directories in the view. In subdirectories of protected paths, these <i>.snapshot</i> directories will provide links to any existing snapshots of parent directories even if there is no protected path on the subdirectory itself. This provides easier access from each directory to snapshots of parent directories.</p> <p>This setting is enabled by default.</p>
<code>--disable-access-to-snapshot-dir-in-subdirs</code>	<p>Disables <code>--enable-access-to-snapshot-dir-in-subdirs</code> (enabled by default). Access to a <i>.snapshot</i> directory under each directory is then only enabled if the directory has a protected path on it.</p>
<code>--enable-visibility-of-snapshot-dir</code>	<p>If <code>--enable-access-to-snapshot-dir-in-subdirs</code> is also enabled, this setting enables listing of a snapshot directory in every directory in the view, even if there is no protected path on the specific directory. As with all snapshot directories, these are hidden directories that will appear in directory listings only for SMB clients.</p>
<code>--disable-visibility-of-snapshot-dir</code>	<p>Disables <code>--enable-visibility-of-snapshot-dir</code> if enabled. (Disabled by default).</p>

## Multiprotocol Example

In this example, we create a policy called *multipro1* to attach to multiprotocol views.

In this policy, we choose to set security flavor to NFS. That enables NFS clients to set permissions on files and directories, while SMB clients will not be able to set permissions.

We will set a non-default set of permission mode bits for files and directories to inherit whenever created by SMB clients.

```
vcli: admin> viewpolicy create --name multipro1 --flavor nfs --auth-source PROVIDERS --nfs-read-write 10.0.0.* --nfs-read-only 10.0.0.1 --nfs-all-squash 10.0.0.3 --nfs-trash-access 10.0.0.1,10.0.0.4 --smb-file-mode 664 --smb-directory-mode 775
```

Client 10.0.0.1 has read-only access, will be root squashed and can use the trash folder.

Client 10.0.0.2 has read/write access, will be root squashed and can not use the trash folder.

Client 10.0.0.3 has read/write access, will be all squashed and cannot use the trash folder.

Client 10.0.0.4 has read/write access, will not be squashed and can use the trash folder.

Client 10.0.0.5 has read/write access, will not be squashed and cannot use the trash folder.

# SMB Example

This example simply names a policy for SMB usage and enables auth provider, as required for SMB. No other view policy parameters are relevant for a policy used for views that are only exposed as SMB shares.

```
vcli: admin> viewpolicy create --name smbpolicy --auth-source PROVIDERS
```

# NFS Example

In this example, a view policy intended for NFS-only views is named nfspolicy1 and gives read/write and trash folder access to one specific host while enabling read-only access for all hosts. The host given trash folder access is also not squashed, which is a necessary configuration for trash folder access to work. Remaining hosts are root squashed by default.

```
vcli: admin> viewpolicy create --name nfspolicy1 --auth-source RPC_AND_PROVIDERS --read-write 192.0.2.0 --nfs-read-only * --nfs-no-squash 192.0.2.0 --nfs-trash-access 192.0.2.0
```

## viewpolicy delete

This command deletes a view policy.

# Usage

```
viewpolicy delete --id ID
```

# Required Parameters

--id ID	Specifies the view policy to delete.
---------	--------------------------------------

# Example

This example...

```
vcli: admin> viewpolicy delete --id 3
```

## viewpolicy list

This command displays all view policies.

# Usage

```
viewpolicy list [--name POLICY_NAME]
                [--vertical]
                [--nfs-acl]
                [--smb-acl]
                [--advanced]
                [--s3]
                [--tenant-id ID]
```

# Options

<code>--name POLICY_NAME</code>	Filters the output by view policy name.
<code>--vertical</code>	Displays the list vertically with all fields shown for each view policy.
<code>--nfs-acl</code>	Displays only NFS ACL fields.
<code>--smb-acl</code>	Displays only SMB ACL fields.
<code>--advanced</code>	Displays only advanced settings.
<code>--s3</code>	Displays S3 settings.
<code>--tenant-id ID</code>	Filters the output by tenant.

## Examples

```
vcli: admin> viewpolicy list
```

```
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| ID | Name | Cluster | Flavor | Access-flavor |
Auth-source | Tenant-id |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| 7 | bgio:default | vast1 | NFS | ALL |
RPC | 3 |
| 6 | bgio_policy | vast1 | NFS | ALL |
RPC | 3 |
| 9 | comet-MIXED_LAST_WINS | vast1 | MIXED_LAST_WINS | ALL |
PROVIDERS | 1 |
| 5 | comet-NFS | vast1 | NFS | ALL |
PROVIDERS | 1 |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

```
vcli: admin> viewpolicy list --nfs-acl
```

```
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
| ID | Name | Cluster | Flavor | Access-flavor |
Auth-source | NFS-read-write | NFS-read-only | NFS-trash-access | NFS-no-squash | NFS-root-sq
uash | NFS-all-squash | NFS-case-insensitivity |
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
| 7 | bgio:default | vast1 | NFS | ALL |
RPC | ['*'] | [] | [] | [] | ['*'] |
```

```

| [] | False | | | | | | |
| 6 | bgio_policy | | | | | | |
RPC | ['*'] | [] | ['*'] | ['*'] | [] |
| [] | False | | | | | | |
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+

```

## viewpolicy modify

This command modifies a view policy.

## Usage

```

viewpolicy modify --id ID
                    [--name NAME]
                    [--flavor NFS|SMB|MIXED_LAST_WINS|S3_NATIVE]
                    [--access-flavor NFS4|SMB|ALL]
                    [--auth-source RPC|PROVIDERS|RPC_AND_PROVIDERS]
                    [--path-length LCD|NPL]
                    [--allowed-characters LCD|NPL]
                    [--gid-inheritance linux|bsd]
                    [--atime-frequency ATIME_FREQUENCY]
                    [--nfs-read-write [HOSTS]]
                    [--nfs-read-only [HOSTS]]
                    [--nfs-no-squash [HOSTS]]
                    [--nfs-root-squash [HOSTS]]
                    [--nfs-all-squash [HOSTS]]
                    [--enable-nfs-return-open-permissions|--disable-nfs-return-open-permission]
s]
                    [--enable-nfs-posix-acl|--disable-nfs-posix-acl]
                    [--enable-32bit-fileid|--enable-32bit-fileid]
                    [--enable-expose-id-in-fsid|--disable-expose-id-in-fsid]
                    [--nfs-trash-access [HOSTS]]
                    [--nfs4-case-sensitive|--nfs4-case-insensitive]
                    [--enable-nfs4-enforce-tls|--disable-nfs4-enforce-tls]
                    [--smb-file-mode SMB_FILE_MODE]
                    [--smb-directory-mode SMB_DIRECTORY_MODE]
                    [--permission-per-vip-pool <pool ID 1>=RW|RO,<pool ID 2>=RW|RO,...]
                    [--nfs-minimal-protection-level NONE|SYSTEM|KRB_AUTH_ONLY|KRB_INTEGRITY|KR
B_PRIVACY]
                    [--s3-visibility USERS]
                    [--s3-visibility-groups GROUPS]
                    [--enable-s3-default-policy|--disable-s3-default-policy]
                    [--s3-special-chars|--s3-special-chars-not-supported]
                    [--s3-read-write [HOSTS]]
                    [--s3-read-only [HOSTS]]
                    [--smb-read-write [HOSTS]]
                    [--smb-read-only [HOSTS]]
                    [--enable-apple-sid|--disable-apple-sid]
                    [--smb-is-ca|--smb-is-not-ca]
                    [--audit-protocols PROTOCOLS]
                    [--audit-operations OPERATIONS]
                    [--audit-options OPTIONS]
                    [--enable-audit-settings|--disable-audit-settings]
                    [--enable-access-to-snapshot-dir-in-subdirs|--disable-access-to-snapshot-di
r-in-subdirs]
                    [--enable-visibility-of-snapshot-dir|--disable-visibility-of-snapshot-dir]
                    [--tenant-id ID]|[--serve-all-tenants]
                    [--disable-read-leases|--enable-read-leases]
                    [--disable-write-leases|--enable-write-leases]
                    [--disable-handle-leases|--enable-handle-leases]

```

thname]

[--s3-flavor-allow-free-listing|--s3-flavor-disallow-free-listing]

[--enable-s3-flavor-detect-full-pathname|--disable-s3-flavor-detect-full-pa




[--enable-inherit-parent-mode-bits|--disable-inherit-parent-mode-bits]


## Required Parameters

<code>--id ID</code>	Specifies the view policy to modify.
----------------------	--------------------------------------

## General Options

<code>--name NAME</code>	Sets a unique name for the view policy.
<code>--flavor</code> <code>NFS SMB MIXED_LAST_WINS S3_NATIVE</code>	<p>Sets a security flavor for the view policy:</p> <ul style="list-style-type: none"><li>• <b>NFS</b>. Treats NFS as a native protocol and other protocols as non-native protocols. Supports NFSv3, SMB and S3. Supports NFSv4.1 without support NFSv4.1 ACLs.</li></ul> <p>Files and directories created by SMB clients receive a set of initial permission bits, configurable using the <code>--smb-file-mode</code> and <code>--smb-directory-mode</code> options.</p> <ul style="list-style-type: none"><li>• <b>SMB</b>. Treats SMB as a native protocol and other protocols as non-native protocols. Supports SMB, NFSv3, NFSv4.1 and S3.</li><li>• <b>MIXED_LAST_WINS</b>. Allows file and directory permissions to be set and modified by all clients. Includes support for NFSv4.1 clients to set NFSv4.1 ACLs. Supports SMB, NFSv3, NFSv4.1 and S3.</li></ul> <p>See also <code>--access-flavor</code> for further control.</p> <ul style="list-style-type: none"><li>• <b>S3_NATIVE</b>. Treats S3 as a native protocol and NFS/SMB as a non-native protocol. Supports S3, NFSv3 and SMB. Supports NFSv4.1 without support for NFSv4.1 ACLs.</li></ul> <p>For more information about security flavors, see <a href="#">Controlling File and Directory Permissions Across Protocols</a>.</p>
<code>--access-flavor NFS4 SMB ALL</code>	<div><div><h3>Caution</h3><p>Changing this setting when already in effect on a view that is being used by clients could lead to unexpected behavior and is not advised.</p></div></div>

	<p>If <code>--flavor</code> is <code>MIXED_LAST_WINS</code>, this parameter can be used to control which protocols can set file permissions, including Access Control Lists (ACLs) and setting user-owner and group-owner of files.</p> <p>NFSv3 is unaffected by this setting. NFSv3 users can set permission mode bits in <i>Mixed Last Wins</i> security flavor regardless of this setting.</p> <p>Attempts by the blocked protocol fail silently. See <a href="#">Controlling File and Directory Permissions Across Protocols</a> for details.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <code>NFS4</code>. Allows NFSv4.1 to set file permissions, and blocks SMB users from setting file permissions.</li> <li>• <code>SMB</code>. Allows SMB users to set file permissions, and blocks NFSv4.1 users from setting file permissions.</li> </ul> <div data-bbox="683 730 1464 942">  <p><b>Note</b></p> <p>Linux super user cannot bypass this blockage.</p> </div> <ul style="list-style-type: none"> <li>• <code>ALL</code> (default). Allows both NFSv4.1 and SMB to set file permissions, as well as NFSv3.</li> </ul>
<pre>--auth-source RPC PROVIDERS RPC_AND_PROVIDERS</pre>	<p>Specifies which source is trusted for the user's group memberships, when users' access to the view is authorized. Possible values:</p> <ul style="list-style-type: none"> <li>• <code>RPC</code>. For NFS only. The GIDs declared in the NFS request as the user's leading group and auxiliary groups are trusted and provider-sourced groups are not considered.</li> </ul> <div data-bbox="683 1329 1464 1541">  <p><b>Note</b></p> <p>This option is not supported for NFSv4.1.</p> </div> <ul style="list-style-type: none"> <li>• <code>PROVIDERS</code>. Group memberships retrieved from authorization providers are considered as the user's group memberships. The GIDs declared in the request are ignored.</li> </ul> <div data-bbox="683 1694 1464 1906">  <p><b>Note</b></p> <p>This option is required for views that have SMB enabled.</p> </div>

	<ul style="list-style-type: none"> <li>• <code>RPC_AND_PROVIDERS</code>. Both the GIDs declared in an NFS request and group memberships retrieved from authorization providers are considered. If the GID provided by the client does not match the GID retrieved from the authorization provider, the GID from the client is set.</li> </ul> <div>  <p><b>Note</b></p> <p>If Kerberos authentication is used by NFSv4.1 clients, the groups declared in the RPC are ignored.</p> </div>
<pre>--permission-per-vip-pool &lt;pool ID 1&gt;=RW RO,&lt;pool ID 2&gt;=RW RO,...</pre>	<p>Grants read/write or read-only access to clients from certain virtual IP pools.</p> <p>Specify a comma-separated list of virtual IP pool IDs with indication of the access type (<code>RW</code> for read/write or <code>RO</code> for read-only) for each of the pools, for example:</p> <pre>--permission-per-vip-pool 1=RW,2=RW,3=RO</pre>
<pre>--tenant-id TENANT_ID</pre>	<p>Associates the view policy with a specific tenant.</p>
<pre>--serve-all-tenants</pre>	<p>Sets the view policy to serve all tenants (default setting).</p>

## Protocol Auditing Options



### Note

Any audit settings that are enabled globally for the cluster are enabled for all views. Auditing settings in a view policy can only add more protocols, operations and/or options to the audit performed on views that use this view policy.

<pre>--audit-protocols PROTOCOLS</pre>	<p>Lists access protocols for which you are enabling or disabling protocol auditing on views that use this view policy.</p> <p>Use this parameter together with <code>--enable-audit-settings</code> or <code>--disable-audit-settings</code> to enable or disable auditing of the specified protocols.</p> <p>When specifying <code>--audit-protocols</code>, you must also specify <code>--audit-operations</code> and/or <code>--audit-options</code>.</p> <p>Specify <code>PROTOCOLS</code> as a comma-separated list of values. Valid values:</p>
--	--



	<ul style="list-style-type: none"> <li>• NFSv3</li> <li>• NFSv4.1</li> <li>• SMB</li> <li>• S3</li> <li>• NDB (Database)</li> </ul>
<pre>--audit-operations OPERATIONS</pre>	<p>Lists categories of protocol operations for which you are enabling or disabling protocol auditing on views that use this view policy.</p> <p>Use this parameter together with <code>--audit-protocols</code> and either <code>--enable-audit-settings</code> or <code>--disable-audit-settings</code> to enable or disable auditing of the specified protocol operations for views that use this view policy.</p> <p>Specify <code>OPERATIONS</code> as a comma-separated list of values, each of which specifies a <a href="#">category of operations</a> being audited. Valid values:</p> <ul style="list-style-type: none"> <li>• <code>create_delete_files_dirs_objects</code>. Operations that create or delete files, directories or objects.</li> <li>• <code>modify_data</code>. Operations that modify data.</li> <li>• <code>modify_data_md</code>. Operations that modify metadata.</li> <li>• <code>read_data</code>. Operations that read data.</li> <li>• <code>read_data_md</code>. Operations that read metadata.</li> <li>• <code>session_create_close</code>. Session creation and closing operations for sessions that use Kerberos 5 authentication (<code>krb5</code>, <code>krb5i</code>, or <code>krb5p</code>).</li> </ul>
<pre>--audit-options OPTIONS</pre>	<p>Lists audit options to enable or disable on views that use this view policy.</p> <p>Use this parameter together with <code>--audit-protocols</code> and either <code>--enable-audit-settings</code> or <code>--disable-audit-settings</code> to enable or disable the specified options for the specified protocols.</p> <p>Specify <code>OPTIONS</code> as a comma-separated list of values. Valid values:</p> <ul style="list-style-type: none"> <li>• <code>log_full_path</code>. If enabled (default for all protocols), audit records contain the full Element Store path to the requested resource. This may affect performance. When disabled, the view path is recorded.</li> <li>• <code>log_username</code>. Disabled by default. If enabled, audit records contain the username (if a username can be retrieved from the auth provider).</li> </ul>
<pre>--enable-audit-settings</pre>	<p>Enables audit settings specified in the same command line by the <code>--audit-protocols</code>, <code>--audit-operations</code> and <code>--audit-options</code> parameters.</p>

	<p>Any auditing protocols, operations options that are already enabled in the policy remain enabled.</p> <p>Any audit settings (protocols, operations or options) that are already enabled in the view policy remain enabled.</p>
<pre>--disable-audit-settings</pre>	<p>Disables audit settings specified in the same command line by the <code>--audit-protocols</code>, <code>--audit-operations</code> and <code>--audit-options</code> parameters.</p> <p>Any audit settings (protocols, operations or options) that are already enabled in the view policy and that are not specified in the same command line remain enabled.</p>

## NFS Security Flavor Options

	<p>so that is 4 each. Therefore, you set the permission bits to 644:</p> <pre>--smb-file-mode 644</pre> <p><b>Defaults</b></p> <p>SMB file mode permission bits: 644</p> <p>SMB directory mode permission bits: 755</p>
<code>--enable-inherit-parent-mode-bits</code>	If specified, permission mode bits for files/objects and directories/buckets created by protocols other than NFS on a view controlled with the NFS security flavor, inherit their permission mode bites from the parent directory.
<code>--disable-inherit-parent-mode-bits</code>	If specified, permission mode bits for files/objects and directories/buckets created by protocols other than NFS on a view controlled with the NFS security flavor, are taken from the view policy definition (instead of inheriting them from the parent directory).

## S3 Options

<pre>--s3-visibility USERS</pre>	<p>Specify users to enables those users to list buckets that are created using this policy even if they do not have permission to access those buckets.</p> <p>When an S3 user sends a bucket listing request, the command returns a list of all buckets the user owns and all buckets that they have this listing permission for, even if they do not have permission to access those buckets.</p> <p>Specify <b>USERS</b> as a comma separated list of user names.</p> <p>Example: <code>--s3-visibility jsmith,sjobs</code></p>
<pre>--s3-visibility-groups GROUPS</pre>	<p>Specify groups to enable members of those groups to list buckets that are created using this policy even if they do not have permission to access those buckets.</p> <p>Specify <b>GROUPS</b> as a comma separated list of group names.</p> <p>Example: <code>--s3-visibility-groups interns,deptheads</code></p>
<code>--enable-s3-default-policy</code>	Specify this option to use this policy as the default view policy for new buckets created via VAST S3 API, where the user is not associated with an S3 endpoint.
<code>--disable-s3-default-</code>	Specify this option to stop using this policy as the default view policy for new buckets created via VAST S3 API.

policy	
--s3-special-chars	Allows S3 object names containing character combinations that are not compatible with other access protocols, such as names containing // or / . . /.
--s3-special-chars-not-supported	Prohibits S3 object names containing character combinations that are not compatible with other access protocols.
--s3-flavor-allow-free-listing	When this option is specified, NFS and SMB clients are allowed or denied access based on the full resource names specified in the identity policies. This means that the identity policy can refer to particular files and directories, rather than to the bucket as a whole.
--s3-flavor-disallow-free-listing	When this option is specified, NFS and SMB clients are allowed or denied access based on the bucket name in the identity policy, rather than on the full resource names.
--enable-s3-flavor-detect-full-pathname	When this options is specified, NFS and SMB clients are able to list bucket views and their subdirectories regardless of individual object permissions.
--disable-s3-flavor-detect-full-pathname	When this option is specified, listing a directory by an NFS or SMB client is allowed or denied based on the identity policies, rather than on individual object permissions.

## S3 Host Access Options

These options set which S3 client hosts can access the view with which access types.

For each option, `HOSTS` can be specified as a comma separated series of any of the following:

- A single IP.
- A subnet indicated by CIDR notation. For example: 1.1.1.1/24.
- A range of IPs indicated by an IP address with '\*' as a wildcard in place of any of the 8-bit fields in the address. For example, 3.3.3.\*, or 3.3.\*.\*.
- A range of IPs where the starting and ending IPs are separated by a hyphen, for example: 192.0.2.3-22
- A fully qualified domain name (FQDN).



## Note

The following rules apply when specifying FQDNs:

- Maximum total length of an FQDN; 255 characters.
- Each domain name label is limited to 63 characters.
- Allowed characters: a-z, 0-9, hyphen (-).
- A label cannot start with a hyphen.

The access types comprise read/write and read-only access.

If a host is specified with multiple entries in mutually exclusive access types, the conflict is resolved as follows:



- An IP overrides a CIDR, and a CIDR overrides a wildcard expression.
- If a conflict remains after the previous rule is applied, the read-only setting overrides the read/write setting.

On new installations, if a view policy does not have any host-based access rules defined for a specific access protocol, access is denied for all hosts. On upgraded deployments, all hosts are allowed access if no host-based access rules are defined.

<code>--s3-read-write</code> <code>[HOSTS]</code>	<p>Controls which S3 client hosts have read/write access to the view.</p> <p>By default, all hosts have read/write access.</p> <p>To remove all hosts from read/write access, include this option without any values.</p> <p>To restrict read/write access to specific hosts, specify <code>HOSTS</code> according to the format description above this table.</p> <p>For example: <code>--s3-read-write 98.51.100.1,98.51.100.2</code></p>
<code>--s3-read-only</code> <code>[HOSTS]</code>	<p>Specifies which S3 client hosts have read-only access to the view.</p> <p>Specify <code>HOSTS</code> according to the format description above this table.</p>

## SMB Options

<code>--enable-apple-sid</code>	For use when connecting from Mac clients to SMB shares, this option enables Security IDs (SIDs) to be returned in Apple compatible representation.
<code>--disable-apple-sid</code>	Disables <code>--enable-apple-sid</code> .

<pre>--smb-is-ca</pre>	<p>When specified, the SMB share exposed by the view is set as <i>continuously available</i>, which allows SMB3 clients to request use of persistent file handles and keep their connections to this share in case of a failover event.</p> <div>  <p><b>Note</b></p> <p>This option requires that the client uses SMBv3.</p> </div> <p>By default, continuous availability is disabled.</p>
<pre>--smb-is-not-ca</pre>	<p>Stops exposing the view path as a <i>continuously available</i> SMB3 share.</p>
<pre>--disable-read-lease</pre>	<p>Disables SMB client read leases so that SMB clients cannot cache data read from the server.</p>
<pre>--enable-read-lease</pre>	<p>Enables SMB client read leases to let SMB clients cache data read from the server.</p>
<pre>--disable-write-lease</pre>	<p>Disables SMB client write leases so that SMB clients cannot cache data written to the server or set byte-range locks on files and directories.</p>
<pre>--enable-write-lease</pre>	<p>Enables SMB client write leases to let SMB clients cache data written to the server and set byte-range locks on files and directories.</p>
<pre>--disable-handle-lease</pre>	<p>Disables handle leases so that SMB clients cannot delay closing handles on files or directories.</p> <div>  <p><b>Note</b></p> <p>Disabling handle leases may impact client resiliency to network and server failures.</p> </div>
<pre>--enable-handle-lease</pre>	<p>Enables SMB client handle leases to let SMB clients delay closing of handles files or directories.</p>

# SMB Host Access Options

These options set which SMB client hosts can access the view with which access types.

For each option, `HOSTS` can be specified as a comma separated series of any of the following:

- A single IP.
- A subnet indicated by CIDR notation. For example: 1.1.1.1/24.
- A range of IPs indicated by an IP address with '\*' as a wildcard in place of any of the 8-bit fields in the address. For example, 3.3.3.\*, or 3.3.\*.\*.
- A range of IPs where the starting and ending IPs are separated by a hyphen, for example: 192.0.2.3-22
- A fully qualified domain name (FQDN).



### Note

The following rules apply when specifying FQDNs:

- Maximum total length of an FQDN; 255 characters.
- Each domain name label is limited to 63 characters.
- Allowed characters: a-z, 0-9, hyphen (-).
- A label cannot start with a hyphen.

The access types comprise read/write and read-only access.

If a host is specified with multiple entries in mutually exclusive access types, the conflict is resolved as follows:

- An IP overrides a CIDR, and a CIDR overrides a wildcard expression.
- If a conflict remains after the previous rule is applied, the read-only setting overrides the read/write setting.

On new installations, if a view policy does not have any host-based access rules defined for a specific access protocol, access is denied for all hosts. On upgraded deployments, all hosts are allowed access if no host-based access rules are defined.

<pre>--smb-read-write [HOSTS]</pre>	<p>Controls which SMB client hosts have read/write access to the view.</p> <p>By default, all hosts have read/write access.</p> <p>To remove all hosts from read/write access, include this option without any values.</p> <p>To restrict read/write access to specific hosts, specify <code>HOSTS</code> according to the format description above this table.</p> <p>For example: <code>--smb-read-write 98.51.100.1,98.51.100.2</code></p>
---	---

<pre>--smb-read-only [HOSTS]</pre>	<p>Specifies which SMB client hosts have read-only access to the view.</p> <p>Specify <code>HOSTS</code> according to the format description above this table.</p>
------------------------------------	--

## Advanced Multi-Protocol Options


<pre>--path-length LCD NPL</pre>	<p>Specifies the policy for limiting file path component name length.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <b>LCD</b> (default) (=Lowest Common Denominator). Imposes the lowest common denominator file path component length limit of all VAST Cluster-supported protocols, regardless of the specific protocol enabled on a specific view.</li> <li>• <b>NPL</b>. (=Native Protocol Limit). Imposes no limitation beyond that of the client protocol.</li> </ul> <div> <p><b>Caution</b></p> <p>If you select this mode in a view policy and then in the future expose a view using this policy to a previously not exposed protocol, that view might contain files that won't be accessible by the newly added protocol, due to the limitations of that protocol.</p> </div>
<pre>--allowed-characters LCD NPL</pre>	<p>Specifies the policy for which characters are allowed in file names.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <b>LCD</b> (default). Allows only characters allowed by all VAST Cluster-supported protocols, regardless of the specific protocol enabled on a specific view.</li> <li>• <b>NPL</b>. (=Native Protocol Limit). Imposes no limitation beyond that of the client protocol.</li> </ul> <div> <p><b>Caution</b></p> <p>If you select this mode in a view policy and then in the future expose a view using this policy to a previously not exposed protocol, that view might contain files that won't be accessible by the newly added protocol, due to the limitations of that protocol.</p> </div>
<pre>--gid-inheritance linux bsd</pre>	<p>Specifies how files receive their owning group when they are created.</p> <p>Possible values:</p>




	<ul style="list-style-type: none"> <li>• <b>linux</b> (default). Each new file inherits its owning group from the group ID of the user who creates the file.</li> <li>• <b>bsd</b>. Each new file inherits its owning group from the group ID of the parent directory.</li> </ul>
--	---

## Advanced NFS Options

<pre>--atime-frequency ATIME_FREQUENCY</pre>	<p><i>atime</i> is a metadata attribute of NFS files that represents the last time the file was updated. <i>atime</i> is updated on read operations if the difference between the current time and the file's atime value is greater than the configured atime frequency. Consider that a very low value might have a performance impact if high numbers of files are being read.</p> <p>Specify ATIME_FREQUENCY as an integer followed by a unit of time (s = seconds, m= minutes, h=hours, d=days).</p> <p>Example: <i>1h</i></p>
<pre>--enable-nfs-return-open- permissions</pre>	<p>Sets the NFS server to unilaterally return open (777) permission for all files and directories when responding to client side access checks.</p> <p>This setting works around a permissions issue that occurs with Windows clients. Windows clients perform NFSv3 access checks before executing read/write requests. This client side check uses the UID and the primary GID of the user without taking into account secondary GIDs. If the check fails, requests are not executed. This means that some permissions may not be honored as they should be, such as those based on secondary groups.</p> <p>When <i>return open permissions</i> is enabled, VAST Cluster returns open permissions for client side access checks, so that the Windows client allows access rights and executes read/write requests. VAST Cluster does a proper permission check when the request is executed.</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p style="text-align: center;"><b>Caution</b></p> <p>Use this feature with caution if Windows client systems are shared by more than one user, since the following security breach could occur: While a user is accessing a file with correct permissions and the file is cached in memory on the Windows system, if another user tries to access the same file, access is incorrectly allowed. No proper access check is done for the second user.</p> </div>
<pre>--disable-nfs-return-open- permissions</pre>	<p>Disables the NFS <i>return open permissions</i> setting. See <code>--nfs-return-open-permissions</code>.</p>

<code>--enable-nfs-posix-acl</code>	<p>Enables full support of extended POSIX Access Control Lists (ACL). By default, VAST Cluster supports the traditional POSIX file system object permission mode bits, (minimal ACL mode) in which each file has three ACL entries defining the permissions for the owner, owning group, and others, respectively. To learn more about POSIX ACL, see <a href="https://linux.die.net/man/5/acl">https://linux.die.net/man/5/acl</a>.</p> <div>  <div> <p><b>Note</b></p> <p>The <code>setfacl</code> Linux command is blocked if this option is not enabled.</p> </div> </div>
<code>--disable-nfs-posix-acl</code>	Disables support for extended POSIX ACLs, restoring default minimal ACL mode.
<code>--enable-32bit-fileid</code>	Sets the VAST Cluster's NFS server to use 32-bit file IDs. This setting supports legacy 32-bit applications running over NFS.
<code>--disable-32bit-fileid</code>	Disables 32-bit file IDs (default).
<code>--nfs-minimal-protection-level</code> <code>NONE SYSTEM KRB_AUTH_ONLY </code> <code>KRB_INTEGRITY KRB_PRIVACY</code>	<p>Set the Kerberos Authentication Minimal protection level to accept from NFSv4.1 client RPCs:</p> <ul style="list-style-type: none"> <li>• <code>KRB_PRIVACY</code>. Allows client mounts only if they use Kerberos 5 authentication with privacy checking (<i>krb5p</i>), the highest level Kerberos security mode.</li> <li>• <code>KRB_INTEGRITY</code>. Allows client mounts only if they use either Kerberos 5 authentication with privacy checking (<i>krb5p</i>) or Kerberos 5 authentication with integrity (<i>krb5i</i>).</li> <li>• <code>KRB_AUTH_ONLY</code>. Allows client mounts with Kerberos authentication only and allows any of the three Kerberos security modes (<i>krb5</i>, <i>krb5i</i>, or <i>krb5p</i>).</li> <li>• <code>SYSTEM</code>. Allows client mounts using either the AUTH_SYS RPC security flavor (the traditional default NFS authentication scheme) or with any of the three Kerberos security modes (<i>krb5</i>, <i>krb5i</i>, or <i>krb5p</i>).</li> <li>• <code>NONE</code>. Allows client mounts with the AUTH_NONE (anonymous access), or AUTH_SYS RPC security flavors, or with any of the three Kerberos security modes (<i>krb5</i>, <i>krb5i</i>, or <i>krb5p</i>).</li> </ul>
<code>--nfs-case-sensitive</code>	<p>When this option is specified, VAST Cluster honors case in the names of files or directories accessed through NFSv4.1.</p> <p>This is the default behavior.</p>

	<p><b>Caution</b></p> <p>Changing the NFSv4.1 case insensitivity setting for an existing view may have unpredictable results.</p>
<code>--nfs-case-insensitive</code>	<p>When this option is specified, VAST Cluster does not honor case in the names of files or directories accessed through NFSv4.1.</p> <p><b>Caution</b></p> <p>Changing the NFSv4.1 case insensitivity setting for an existing view may have unpredictable results.</p>
<code>--enable-nfs4-enforce-tls</code>	<p>Enforces TLS encryption between the NFS4.1 client and the cluster. When this setting is enabled, the <i>Kerberos Authentication Minimal protection level</i> must be set to <i>System</i> or <i>None</i>.</p> <p> <b>Note</b></p> <p>TLS encryption requires further setup in addition to this view policy setting. For details, see <a href="#">Configuring TLS Encryption with NFSv4.1</a>.</p>
<code>--disable-nfs4-enforce-tls</code>	<p>Disables enforcing of TLS encryption between the NFSv4.1 client and the cluster.</p>

## NFS Host Access Options

These options determine which NFS client hosts can access the view with which access types.

The hosts (`HOSTS`) can be specified including any of the following items separated by commas:

- A single IP.
- A fully qualified domain name (FQDN).



## Note

The following rules apply when specifying FQDNs:

- Maximum total length of an FQDN; 255 characters.
- Each domain name label is limited to 63 characters.
- Allowed characters: a-z, 0-9, hyphen (-).
- A label cannot start with a hyphen.

- A subnet indicated by CIDR notation. For example: 1.1.1.1/24.
- A subset of IPs specified as an IP address with '\*' as a wildcard in place of any of the 8-bit fields in the address. For example, 3.3.3.\*, or 3.3.\*.\*.
- A range of IPs where the starting and ending IPs are separated by a hyphen, for example: 192.0.2.3-22
- A netgroup, prefixed with an '@'. For information about using netgroups, see [Using Netgroups to Authorize Hosts](#).


The access types include read/write or read-only access, the squash policy, and trash folder access.

If the configuration specifies that a host has mutually exclusive access types, the conflict is resolved as follows:

- An IP overrides a netgroup, a netgroup overrides a netmask, and a netmask overrides a wildcard expression.
- If a conflict remains after the previous rule is applied, then:
  - `--nfs-read-only` overrides `--nfs-read-write`.
  - `--nfs-all-squash` overrides `--nfs-root-squash`.
  - `--nfs-root-squash` overrides `--nfs-no-squash`.

On new installations, if a view policy does not have any host-based access rules defined for a specific access protocol, access is denied for all hosts. On upgraded deployments, all hosts are allowed access if no host-based access rules are defined.

<code>--nfs-read-write</code> <code>[HOSTS]</code>	<p>Determines which NFS client hosts have read/write access to the view.</p> <p>By default, all hosts have read/write access.</p> <p>To restrict read/write access to specific hosts, specify <code>HOSTS</code> as shown above the table. For example: <code>--nfs-read-write 98.51.100.1,98.51.100.2</code></p> <p>To prohibit read/write access for all hosts, specify this option without any values.</p> <p>To create a reversed rule, e.g. a rule that allows read/write access from all IPs except the one specified, prepend the IP address with a tilde, for example: <code>~192.0.2.0</code></p>
<code>--nfs-read-only</code> <code>[HOSTS]</code>	<p>Determines which NFS client hosts have read-only access to the view.</p>

	Specify <code>HOSTS</code> as shown above the table.
<pre>--nfs-no-squash [HOSTS]</pre>	<p>Determines which hosts have <i>no squash</i> access. With <i>no squash</i>, all operations are supported. Use this option if you trust the root user not to perform operations that will corrupt data.</p> <p>This option is not relevant for NFSv4.1 users if Kerberos is used, since Active Directory does not include the 'root' user principal by default and since the handling of credentials for the user with UID 0 depends on configuration of the <code>rpc.gssd</code> service.</p> <p>Specify <code>HOSTS</code> as shown above the table.</p>
<pre>--nfs-root-squash [HOSTS]</pre>	<p>Determines which hosts have <i>root squash</i> access. With <i>root squash</i>, the root user is mapped to nobody for all file and folder management operations on the export. This enables you to prevent the strongest super user from corrupting all user data on the VAST Cluster.</p> <p>This option is not relevant for NFSv4.1 users if Kerberos is used, since Active Directory does not include the 'root' user principal by default and since the handling of credentials for the user with UID 0 depends on configuration of the <code>rpc.gssd</code> service.</p> <p>By default, all hosts have <i>root squash</i> access.</p> <p>To restrict root squash to specific hosts, specify <code>HOSTS</code> according to the format description above this table.</p> <p>To remove root squash access for all hosts, include this option without values.</p>
<pre>--nfs-all-squash [HOSTS]</pre>	<p>Determines which hosts have <i>all squash</i> access. With <i>all squash</i>, all client users are mapped to nobody for all file and folder management operations on the export.</p> <p>Specify <code>HOSTS</code> as shown above the table.</p>
<pre>--nfs-trash-access [HOSTS]</pre>	<p>Determines which hosts have access to the trash folder, if the trash folder is enabled for the cluster.</p> <p>Granting this permission gives hosts the ability to delete files by moving them into the <a href="#">trash folder</a>, from which they are automatically deleted. Requires that the host is listed as <i>No Squash</i> (<code>--nfs-no-squash</code>).</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;">  <p><b>Note</b></p> <p>This option is applicable for NFSv3 only. The <i>Trash folder</i> feature is not supported for NFSv4.1 clients.</p> </div> <p>Specify <code>HOSTS</code> as shown above the table.</p>

# Snapshot Options

<code>--enable-access-to-snapshot-dir-in-subdirs</code>	<p>Enables accessible <i>.snapshot</i> directories under all directories in the view. In subdirectories of protected paths, these <i>.snapshot</i> directories will provide links to any existing snapshots of parent directories even if there is no protected path on the subdirectory itself. This provides easier access from each directory to snapshots of parent directories.</p> <p>This setting is enabled by default.</p>
<code>--disable-access-to-snapshot-dir-in-subdirs</code>	<p>Disables <code>--enable-access-to-snapshot-dir-in-subdirs</code> (enabled by default). Access to a <i>.snapshot</i> directory under each directory is then only enabled if the directory has a protected path on it.</p>
<code>--enable-visibility-of-snapshot-dir</code>	<p>If <code>--enable-access-to-snapshot-dir-in-subdirs</code> is also enabled, this setting enables listing of a snapshot directory in every directory in the view, even if there is no protected path on the specific directory. As with all snapshot directories, these are hidden directories that will appear in directory listings only for SMB clients.</p>
<code>--disable-visibility-of-snapshot-dir</code>	<p>Disables <code>--enable-visibility-of-snapshot-dir</code> if enabled. (Disabled by default).</p>

## Example

This example modifies some of the NFS host access rules of an existing view policy.

```
vcli: admin> viewpolicy modify --id 4 --nfs-read-write 10.0.0.2,10.0.0.3,10.0.0.4 --nfs-read-only 10.0.0.* --nfs-trash-access 10.0.0.4
```

## viewpolicy refresh-netgroups

This command refreshes [netgroups](#) configured for a view policy.

## Usage

```
viewpolicy refresh-netgroups --id ID
```

## Required Parameters

<code>--id ID</code>	Identifies the view policy for which you want to refresh netgroups.
----------------------	---

## Example

To refresh netgroups for view policy 8:

```
vccli: admin> viewpolicy refresh-netgroups --id 8
```

### viewpolicy show

This command displays details of a specific view policy or the protocol auditing configuration in the view policy.

## Usage

```
viewpolicy show --id ID  
                [--audit]
```

## Required Parameters

<code>--id ID</code>	Specifies which view policy to show, by its ID (integer).
----------------------	---

## Options

<code>--audit</code>	Shows the protocol auditing configuration.
----------------------	--

## Example

This example displays details of the default view policy.

```
vccli: admin> viewpolicy show --id 3
```

+-----+-----+		
ID	3	
Name	s3_default_policy	
Cluster	vast-cluster-1	
Atime-frequency	None	
NFS-read-write	['*']	
NFS-read-only	[]	
SMB-read-write	['*']	
SMB-read-only	[]	
S3-read-write	['*']	
S3-read-only	[]	
NFS-trash-access	[]	

Auth-source	RPC	
NFS-POSIX-ACL	No	
NFS-return-open-permissions	False	
NFS-no-squash	[]	
NFS-root-squash	['*']	
NFS-all-squash	[]	
Default file permissions	644	
Default folder permissions	755	
Gid-inheritance	LINUX	
Flavor	S3_NATIVE	
Path-length	NPL	
Allowed-characters	NPL	
Use-32bit-fileid	False	
Expose-id-in-fsid	False	
VIP Pools	[]	
Nfs-minimal-protection-level	SYSTEM	
Apple sid	True	
Remote-mapping	{}	
Created time	2023-01-18 07:54:41	
Accessible .snapshot Folder In Subdirectories	True	
Visible .snapshot Folder In SMB Subdirectories	False	
Tenant-id	1	
Enforce use of TLS certificate	False	
+-----+		



# vippool commands

## vippool create

This command creates a [virtual IP pool](#).

## Usage

```
vippool create --ip-ranges IP_RANGES
               [--subnet-cidr CIDR]
               [--subnet-cidr-ipv6 CIDR]
               [--gw-ip IPV4]
               [--gw-ipv6 IPV6]
               [--vlan VLAN]
               [--cnode-ids CNODE_IDS]
               [--cnode-names CNODE_NAMES]
               [--name NAME]
               [--vast-dns-domain-name DOMAIN_NAME]
               [--role PROTOCOLS|REPLICATION|VAST_CATALOG]
               [--vms-preferred]
               [--not-vms-preferred]
               [--port-membership ALL|RIGHT|LEFT]
               [--tenant-id TENANT_ID]
               [--serve-all-tenants]
               [--enable-weighted-balancing|--disable-weighted-balancing]
```

## Required Parameters

<code>--ip-ranges</code> <code>IP_RANGES</code>	<p>Lists the ranges of IPv4 or IPv6 addresses included in the virtual IP pool.</p> <p>Specify <code>IP_RANGES</code> as a list of IP ranges in the format <i>&lt;start IP&gt;</i>,<i>&lt;end IP&gt;</i>. Separate ranges with a space.</p> <p>For example: <code>--ip-ranges 10.10.10.2,10.10.10.4 10.10.10.8,10.10.10.24</code></p>
--	--

## Options

<code>--subnet-cidr</code> <code>CIDR</code>	<p>Specifies the subnet in Classless Inter-Domain Routing (CIDR) notation for IPv4.</p> <p>In CIDR notation, the subnet is expressed as the number of bits of each IP address that represent the subnet address. For example, the subnet mask 255.255.255.0 is expressed as 24 in CIDR notation.</p> <p>Specify <code>CIDR</code> as an integer.</p> <p>For example: <code>--subnet-cidr 24</code></p>
--	--

<code>--subnet-cidr-ipv6 CIDR</code>	<p>Specifies the subnet in Classless Inter-Domain Routing (CIDR) notation for IPv6.</p> <p>This option is required if IPv6 is used in <code>--ip-ranges</code>.</p> <p>In CIDR notation, the subnet is expressed as the number of bits of each IP address that represent the subnet address. For IPv6, this is known as <i>IPv6 prefix length</i>. For example, the prefix length of /32 in 2001:db8::/32 would include IP addresses from 2001:db8:: to 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff.</p> <p>Specify <code>CIDR</code> as an integer.</p> <p>For example: <code>--subnet-cidr-ipv6 48</code></p>
<code>--gw-ip IPV4</code>	<p>Specifies a gateway IPv4 address. Use this option if your storage clients are on multiple subnets and you are routing your client storage traffic through a local gateway.</p>
<code>--gw-ipv6 IPV6</code>	<p>Specifies a gateway IPv6 address. Use this option if your storage clients are on multiple subnets and you are routing your client storage traffic through a local gateway.</p>
<code>--vlan VLAN</code>	<p>Tags the virtual IP pool with a specific VLAN on the data network. See <a href="#">Tagging Virtual IP Pools with VLANs</a>.</p> <p>Specify <code>VLAN</code> as a VLAN number (0-4096).</p>
<code>--cnode-ids CNODE_IDS</code>	<p>Dedicates a specific group of CNodes to the virtual IP pool. The virtual IPs in this pool will only be distributed among the specified CNodes.</p> <p>Specify <code>CNODE_IDS</code> as a comma separated list of CNode IDs.</p> <p>By default, virtual IP pools are distributed among all active CNodes.</p>
<code>--cnode-names CNODE_NAMES</code>	<p>Dedicates a group of CNodes to the virtual IP pool, specifying CNodes by name. Specify CNode names as a comma separated list.</p> <p>For example: <code>--cnode-names cnode-1,cnode-3,cnode-4</code></p> <p>By default, virtual IP pools are distributed among all active CNodes.</p>
<code>--name NAME</code>	<p>Specifies a name for the virtual IP pool.</p>
<code>--vast-dns-domain-name DOMAIN_NAME</code>	<p>Specifies a domain name to associate with the virtual IP pool for DNS resolution by the VAST Cluster DNS server. If a domain suffix is defined in the <a href="#">DNS server configuration</a>, it is appended to the domain name to form a</p>

	FQDN.
<pre>--role PROTOCOLS REPLICATION VAST_CATALOG</pre>	<p>Determines the usage of the virtual IP pool:</p> <ul style="list-style-type: none"> <li>• <b>PROTOCOLS.</b> The virtual IP pool is used to provide access to the cluster for data network clients.</li> <li>• <b>REPLICATION.</b> The virtual IP pool is used for async replication.</li> <li>• <b>VAST_CATALOG.</b> The virtual IP pool is dedicated to VAST Catalog. If a virtual IP pool with this role exists, the VIPs in this pool are used for VAST Catalog queries run from the VAST Web UI. This pool is not required but creating a pool of this role can improve performance when running VAST Catalog queries.</li> </ul>
<pre>--vms-preferred</pre>	Sets CNodes participating in the virtual IP pool to belong to a preferred domain for VMS failover. For more details, see <a href="#">Configuring Network Access</a> .
<pre>--not-vms-preferred</pre>	Disables <code>--vms-preferred</code> .
<pre>--port-membership ALL RIGHT LEFT</pre>	Determines which port (right or left) in a group of CNodes is allocated to the virtual IP pool. For more information, see <a href="#">Configuring Network Access</a> . By default, all ports on the pool's CNodes are included in the virtual IP pool.
<pre>--tenant-id TENANT_ID</pre>	<p>Specifies a tenant for the virtual IP pool to serve exclusively.</p> <p>If a tenant ID is specified, only this particular tenant is able to access the virtual IP pool. If no tenant ID is set, the pool can be accessed by any tenant.</p>
<pre>--serve-all-tenants</pre>	Detaches a tenant from the virtual IP pool, so that the virtual IP pool serves all tenants.
<pre>--enable-weighted-balancing</pre>	<p>Applicable for combinations of CNodes of different generations. Enables automatic rebalancing of VIPs across CNodes according to the following ratios:</p> <ul style="list-style-type: none"> <li>• Ice Lake CNodes are allocated 50% more VIPs than Cascade Lake CNodes,</li> <li>• Cascade Lake CNodes are allocated 50% more VIPs than Broadwell CNodes.</li> </ul> <p>This feature allows you to leverage the increased CPU capacity of newer</p>

	CNode generations that can handle a higher workload.
<code>--disable-weighted-balancing</code>	Disables CNode VIP rebalancing.

## Example

```

vcli: admin> vipool create --ip-ranges 203.0.113.2,203.0.113.5 203.0.113.8,203.0.113.24 --s
ubnet-cidr 24 --gw-ip 203.0.113.1 --vlan 60 --cnode-ids 1,2,3 --name vipool1

```

### vipool delete

This command deletes a [virtual IP pool](#).

## Usage

```

vipool delete --id ID

```

## Required Parameters

<code>--id ID</code>	Specifies which virtual IP pool to delete.
----------------------	--

## Example

```

vcli: admin> vipool delete --id 1
Are you sure you want to delete the VIP pool? [y/N] y

```

### vipool list

This command displays details of all [virtual IP pools](#) on the VAST Cluster.

## Usage

```

vipool list [--cluster-id CLUSTER_ID]
            [--cluster-name CLUSTER_NAME]
            [--cnode-id CNODE_ID]
            [--port-membership ALL|RIGHT|LEFT]

```

## Options

<code>--cluster-id CLUSTER_ID</code>	Filters virtual IP pools by cluster ID.
--------------------------------------	---

<code>--cluster-name CLUSTER_NAME</code>	Filters virtual IP pools by cluster name.
<code>--cnode-id CNODE_ID</code>	Filters virtual IP pools by CNode ID.
<code>--port-membership</code> <code>ALL RIGHT LEFT</code>	Filters virtual IP pools by CNode port membership. For more information, see <a href="#">Port Affinity</a> .

## Example

```

vcli: admin> vipool list
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name          | IP-ranges                               | Subnet-CIDR | IPv6-Subnet-CIDR | G
W-IP | GW-IPv6 | VLAN | Role          | CNodes | Port-membership | Domain-name | Cluster      | VM
S-preferred | Enabled |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 2  | vipool-2      | [['203.0.113.1', '203.0.113.16']]      | 16          | None             | 
|      | 0          | PROTOCOLS | []          | ALL              | vipool-2    | mycluster   | False
| True |
| 3  | vipool-3      | [['203.0.113.212', '203.0.113.227']]  | 16          | None             | 
|      | 0          | PROTOCOLS | []          | ALL              | vipool-3    | mycluster   | False
| True |
| 4  | vipool-4      | [['203.0.113.232', '203.0.113.247']]  | 16          | None             | 
|      | 0          | PROTOCOLS | []          | ALL              | vipool-4    | mycluster   | False
| True |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

## vipool modify

This command modifies a [virtual IP pool](#).

## Usage

```

vipool modify --id ID
               [--ip-ranges IP_RANGES]
               [--subnet-cidr CIDR]
               [--subnet-cidr-ipv6 CIDR]
               [--cnode-ids CNODE_IDS]
               [--cnode-names CNODE_NAMES]
               [--gw-ip IPV4]
               [--gw-ipv6 IPV6]
               [--name NAME]
               [--vlan VLAN]
               [--vast-dns-domain-name DOMAIN_NAME]
               [--role PROTOCOLS|REPLICATION|VAST_CATALOG]
               [--vms-preferred]
               [--not-vms-preferred]
               [--port-membership ALL|RIGHT|LEFT]
               [--tenant-id TENANT_ID]

```

[--serve-all-tenants]  
[--enable-weighted-balancing|--disable-weighted-balancing]



## Required Parameters

<code>--id ID</code>	Specifies the virtual IP pool to modify.
----------------------	--

## Options

<code>--ip-ranges IP_RANGES</code>	<p>Lists the ranges of IPv4 or IPv6 addresses included in the virtual IP pool.</p> <p>Specify <code>IP_RANGES</code> as a list of IP ranges in the format <code>&lt;start IP&gt;,&lt;end IP&gt;</code>. Separate ranges with a space.</p> <p>For example, <code>--ip-ranges 10.10.10.2,10.10.10.4 10.10.10.8,10.10.10.24</code></p>
<code>--subnet-cidr CIDR</code>	<p>Specifies the subnet in Classless Inter-Domain Routing (CIDR) notation for IPv4.</p> <p>In CIDR notation, the subnet is expressed as the number of bits of each IP address that represent the subnet address. For example, the subnet mask 255.255.255.0 is expressed as 24 in CIDR notation.</p> <p>Specify <code>CIDR</code> as an integer.</p> <p>For example: <code>--subnet-cidr 24</code></p>
<code>--subnet-cidr-ipv6 CIDR</code>	<p>Specifies the subnet in Classless Inter-Domain Routing (CIDR) notation for IPv6.</p> <p>In CIDR notation, the subnet is expressed as the number of bits of each IP address that represent the subnet address. For IPv6, this is known as <i>IPv6 prefix length</i>. For example, the prefix length of /32 in 2001:db8::/32 would include IP addresses from 2001:db8:: to 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff.</p> <p>Specify <code>CIDR</code> as an integer.</p> <p>For example: <code>--subnet-cidr-ipv6 48</code></p>
<code>--cnode-ids CNODE_IDS</code>	<p>Dedicates a specific group of CNodes to the virtual IP pool. The virtual IPs in this pool will only be distributed among the specified CNodes.</p> <p>By default, virtual IP pools are distributed among all active CNodes.</p>

<code>--cnode-names CNODE_NAMES</code>	<p>Dedicates a group of CNodes to the virtual IP pool, specifying CNodes by name. Specify CNode names as a comma separated list.</p> <p>For example: <code>--cnode-names cnode-1,cnode-3,cnode-4</code></p> <p>By default, virtual IP pools are distributed among all active CNodes.</p>
<code>--gw-ip IPV4</code>	<p>Specifies a gateway IPv4 address. Use this option if your storage clients are on multiple subnets and you are routing your client storage traffic through a local gateway.</p>
<code>--gw-ipv6 IPV6</code>	<p>Specifies a gateway IPv6 address. Use this option if your storage clients are on multiple subnets and you are routing your client storage traffic through a local gateway.</p>
<code>--name NAME</code>	<p>Specifies a name for the virtual IP pool.</p>
<code>--vlan VLAN</code>	<p>Tags the virtual IP pool with a specific VLAN on the data network. See <a href="#">Tagging Virtual IP Pools with VLANs</a>.</p> <p>Specify <code>VLAN</code> as a VLAN number (0-4096).</p>
<code>--vast-dns-domain-name DOMAIN_NAME</code>	<p>Specifies a domain name to associate with the virtual IP pool for DNS resolution by the VAST Cluster DNS server. If a domain suffix is defined in the <a href="#">DNS server configuration</a>, it is appended to the domain name to form a FQDN.</p>
<code>--role</code> <code>PROTOCOLS REPLICATION VAST_CATALOG</code>	<p>Determines the usage of the virtual IP pool:</p> <ul style="list-style-type: none"> <li>• <code>PROTOCOLS</code>. The virtual IP pool is used to provide access to the cluster for data network clients.</li> <li>• <code>REPLICATION</code>. The virtual IP pool is used for native replication.</li> <li>• <code>VAST_CATALOG</code>. The virtual IP pool is dedicated to VAST Catalog. If a virtual IP pool with this role exists, the virtual IPs in this pool are used for VAST Catalog queries run from the VAST Web UI. This pool is not required but creating a pool of this role can improve performance when running VAST Catalog queries.</li> </ul>
<code>--vms-preferred</code>	<p>Sets CNodes participating in the virtual IP pool to belong to a preferred domain for VMS failover. For more details, see <a href="#">Configuring Network Access</a>.</p>

<code>--not-vms-preferred</code>	Disables <code>--vms-preferred</code> .
<code>--port-membership ALL RIGHT LEFT</code>	Determines which port (right or left) in a group of CNodes is allocated to the virtual IP pool. For more information, see <a href="#">Configuring Network Access</a> . By default, all ports on the pool's CNodes are included in the virtual IP pool.
<code>--tenant-id TENANT_ID</code>	<p>Specifies a tenant for the virtual IP pool to serve exclusively.</p> <p>If a tenant ID is specified, only this particular tenant is able to access the virtual IP pool. If no tenant ID is set, the pool can be accessed by any tenant.</p> <div>  <p><b>Note</b></p> <p>You cannot detach a tenant from a virtual IP pool as long as there are view policies associated with that tenant. This is in order to avoid a scenario where a client using a virtual IP gets disconnected from the tenant.</p> </div>
<code>--serve-all-tenants</code>	<p>Detaches a tenant from the virtual IP pool, so that the virtual IP pool serves all tenants.</p> <div>  <p><b>Note</b></p> <p>You cannot detach a tenant from a Virtual IP pool as long as there are view policies associated with that tenant. This is in order to avoid a scenario where a client using a virtual IP gets disconnected from the tenant.</p> </div>
<code>--enable-weighted-balancing</code>	<p>Applicable for combinations of CNodes of different generations. Enables automatic rebalancing of VIPs across CNodes according to the following ratios:</p> <ul style="list-style-type: none"> <li>Ice Lake CNodes are allocated 50% more VIPs than Cascade Lake CNodes,</li> <li>Cascade Lake CNodes are allocated 50% more VIPs than Broadwell CNodes.</li> </ul> <p>This feature allows you to leverage the increased CPU capacity of newer CNode generations that can handle a higher workload.</p>



<code>--disable-weighted-balancing</code>	Disables CNode VIP rebalancing.
---	---------------------------------

## Example

This example changes the last IP in the pool's IP range and tags the pool with VLAN 70:

```
vcli: admin> vipool modify --id 1 --vlan 70
```

## vipool show

This command displays details of a specific [virtual IP pool](#).

## Usage

```
vipool show
--id ID
```

## Required Parameters

<code>--id ID</code>	Specifies the virtual IP pool to display.
----------------------	---

## Example

```
vcli: admin> vipool show --id 2
```

```
+-----+-----+
| ID      | 2      |
| Name    | vipool-2 |
| IP-ranges | [['203.0.113.1', '203.0.113.16']] |
| Subnet-CIDR | 16    |
| IPv6-Subnet-CIDR | None |
| GW-IP    |        |
| GW-IPv6  |        |
| VLAN    | 0      |
| Role    | PROTOCOLS |
| CNodes   | []     |
| Port-membership | ALL  |
| Domain-name | vipool-2 |
| Cluster  | mycluster |
| VMS-preferred | False |
| Enabled  | True    |
+-----+-----+
```

# vms commands

## vms delete\_saml\_idp\_configuration

This command deletes the SAML configuration for a specified IDP.

### Usage

```
vms delete_saml_idp_configuration --idp-name IDP_NAME
```

### Required Parameters

<code>--idp-name IDP_NAME</code>	The name of the IdP to be removed.
----------------------------------	------------------------------------

### Example

```
vcli: admin> vms delete_saml_idp_configuration --idp-name Okta
```

## vms list

This command displays the specified object and their details.

### Usage

```
vms list
```

### Example

```
vcli: admin> vms list
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
| Name | Created | SW-Version | Build | Auto-Logout-Timeout |
IP1 | IP2 | MGMT-VIP | Mgmt-CNode | Performance-base-10 | Capacity-bas
e-10 | Login-banner | Access-token-lifetime | Refresh-token-lifetime | MGMT-VIP-IPv6 | Perf-d
ebug-metrics-enabled |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
| VMS | 2021-04-06 09:59:50 | 4.7.0.49 | release-4-7-0-1029112-vms | 600 |
172.16.2.52 | 172.16.1.52 | 198.51.100.10 | cnode-3-52 | True | True
| None | 01:00:00 | 1 00:00:00 | UNKNOWN | N/A
|
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
```

# vms modify

This command modifies VMS settings.

## Usage

```
vms modify [--mgmt-vip MGMT_VIP]
           [--mgmt-inner-vip MGMT_INNER_VIP]
           [--min-tls-version MIN_TLS_VERSION]
           [--access-token-lifetime ACCESS_TOKEN_LIFETIME]
           [--refresh-token-lifetime REFRESH_TOKEN_LIFETIME]
           [--enable-vms-metrics]
           [--disable-vms-metrics]
           [--performance-base-10]
           [--performance-base-2]
           [--capacity-base-10]
           [--capacity-base-2]
           [--login-banner LOGIN_BANNER]
           [--min-pwd-length LENGTH]
           [--preferred-cnode-ids PREFERRED_CNODE_IDS]
           [--enable-vms-perf-debug-metrics]
           [--disable-vms-perf-debug-metrics]
```

## Required Parameters

--id ID	Specifies the ID of the VMS resource.
---------	---------------------------------------

## Options

--mgmt-vip MGMT_VIP	Changes the IP address configured on the management interfaces on all CNodes. VAST Management Service (VMS) listens on this IP. The IP should be on the management subnet.
--mgmt-inner-vip MGMT_INNER_VIP	Changes the management inner VIP, a virtual IP on the cluster's internal network used for mounting the VMS database.
--min-tls-version MIN_TLS_VERSION	Sets minimum supported version of TLS for HTTPS connection to VMS. Possible values: <ul style="list-style-type: none"><li>1.1</li><li>1.2 (default)</li></ul>
--access-token-lifetime ACCESS_TOKEN_LIFETIME	Changes the VMS session access token timeout. See also --refresh-token-lifetime.  When a user logs in to the VMS GUI, two session tokens are issued: an access token and

	<p>a refresh token.</p> <p>The access token is a digitally encoded signature used to authenticate the user and authorize access. Access tokens are designed to have a minimal lifetime, to ensure minimum time for a user's identity to be exploited.</p> <p>The refresh token must have a longer lifetime than the access token. It is used to request a new access token on behalf of the user before the access token expires, without bothering the user for login credentials. When the refresh token expires, the user is logged out.</p> <p>Default: 1 hour</p> <p>Example: <code>--access-token-lifetime 02:00:00</code></p>
<pre>--refresh-token-lifetime REFRESH_TOKEN_LIFETIME</pre>	<p>Changes the VMS session refresh token timeout. See also <code>--access-token-lifetime</code>.</p> <p>When a user logs in to the VMS GUI, two session tokens are issued: an access token and a refresh token.</p> <p>The access token is a digitally encoded signature used to authenticate the user and authorize access. Access tokens are designed to have a minimal lifetime, to ensure minimum time for a user's identity to be exploited.</p> <p>The refresh token must have a longer lifetime than the access token. It is used to request a new access token on behalf of the user before the access token expires, without bothering the user for login credentials. When the refresh token expires, the user is logged out.</p> <p>Default: 1 day</p> <p>Example: <code>--refresh-token-lifetime 12:00:00</code></p>
<pre>--enable-vms-metrics</pre>	Enables VMS metrics collection.
<pre>-disable-vms-metrics</pre>	Disables VMS metrics collection.
<pre>--performance-base-10</pre>	<p>Set units of measurement for performance metrics, displayed on the VAST Web UI dashboard and in VMS analytics reports to base10 units (default setting).</p> <p>Base10 units have the prefixes M, G, T, and so on, representing powers of 10. In base10, 1 TB refers to 1000 GB, which refers to 1000 MB, and so on.</p>
<pre>--performance-base-2</pre>	<p>Set units of measurement for performance metrics, displayed on the VAST Web UI dashboard and in VMS analytics reports to base2 units instead of the default base10 units.</p> <p>Base2 units have the prefixes TiB, GiB, MiB, and so on, in which 1 TiB = 1024 GiB, 1 GiB = 1024 MiB, and so on.</p>

<code>--capacity-base-10</code>	<p>Set units of measurement for capacity metrics, displayed on the VAST Web UI dashboard and in VMS analytics reports to base10 units (default setting).</p> <p>Base10 units have the prefixes M, G, T, and so on, representing powers of 10. In base10, 1 TB refers to 1000 GB, which refers to 1000 MB, and so on.</p>
<code>--capacity-base-2</code>	<p>Set units of measurement for capacity metrics, displayed on the VAST Web UI dashboard and in VMS analytics reports to base2 units instead of the default base10 units.</p> <p>Base2 units have the prefixes TiB, GiB, MiB, and so on, in which 1 TiB = 1024 GiB, 1 GiB = 1024 MiB, and so on.</p>
<code>--login-banner</code> <code>LOGIN_BANNER</code>	<p>Sets a custom login banner or removes a custom login banner.</p> <p>To set a custom login banner, specify a string and enter it in single quotes. Multiple lines are not supported when specifying the banner text via the VAST CLI. However, there is no limit on the line length and the words wrap from one line to the next when displayed.</p> <p>To remove a custom login banner, specify an empty string in single quotes.</p>
<code>--preferred-cnode-ids</code> <code>PREFERRED_CNODE_IDS</code>	Specifies VMS preferred CNodes IDs.
<code>--min-pwd-length</code> <code>LENGTH</code>	<p>Sets the minimum required password length.</p> <p>Specify <code>LENGTH</code> as a number of characters.</p> <p>Default: 8</p>
<code>--enable-vms-perf-debug-metrics</code>	Enables VMS performance debug metrics.
<code>--disable-vms-perf-debug-metrics</code>	Disables VMS performance debug metrics.

## Examples

To specify custom login banner text:

```
vcli: admin> vms modify --id 1 --login-banner 'You are logging into VMS'
```

To remove a custom login banner text:

```
vcli: admin> vms modify --login-banner ''
```

To set the access token lifetime to 2 hours and the refresh token lifetime to 12 hours:

vcli: admin> vms modify --access-token-lifetime 02:00:00 --refresh-token-lifetime 12:00:00

**vms modify\_pwd\_settings**

This command modifies VMS password settings.

**Usage**

```

vms modify_pwd_settings [--id ID]
                        [--min-pwd-length LENGTH]
                        [--enable-pwd-uppercase-validation]
                        [--disable-pwd-uppercase-validation]
                        [--enable-pwd-lowercase-validation]
                        [--disable-pwd-lowercase-validation]
                        [--enable-pwd-numeric-validation]
                        [--disable-pwd-numeric-validation]
                        [--enable-pwd-special-chars-validation]
                        [--disable-pwd-special-chars-validation]
                        [--pwd-change-timeout TIMEOUT]
                        [--pwd-expiration-timeout TIMEOUT]
                        [--tmp-pwd-expiration-timeout TIMEOUT]
                        [--max-failed-login-attempts ATTEMPTS]
                        [--pwd-history-no-reuse-count COUNT]
                        [--enable-pwd-change-timeout]
                        [--disable-pwd-change-timeout]
                        [--enable-pwd-expiration-timeout]
                        [--disable-pwd-expiration-timeout]
                        [--enable-max-failed-login-attempts]
                        [--disable-max-failed-login-attempts]
                        [--enable-pwd-history-no-reuse-count]
                        [--disable-pwd-history-no-reuse-count]

```

**Required Parameters**

--id ID	Specifies the ID of the VMS resource.
---------	---------------------------------------

**Options**

--min-pwd-length LENGTH	Sets the minimum required password length.  Specify LENGTH as a number of characters.  Default: 8
--enable-pwd- uppercase-validation	Enables requirement of at least one uppercase character in VMS passwords.
--disable-pwd-	Disables requirement of at least one uppercase character in VMS passwords.

uppercase-validation	
-enable-pwd-lowercase-validation	Enables requirement of at least one lowercase character in VMS passwords.
--disable-pwd-lowercase-validation	Disables requirement of at least one lowercase character in VMS passwords.
--enable-pwd-numeric-validation	Enables requirement of at least one numeric character in VMS passwords.
--disable-pwd-numeric-validation	Disables requirement of at least one numeric character in VMS passwords.
--enable-pwd-special-chars-validation	Enables requirement of at least one non-alphanumeric character in VMS passwords.
--disable-pwd-special-chars-validation	Disables requirement of at least one non-alphanumeric character in VMS passwords.
--pwd-change-timeout TIMEOUT	<p>Sets the time frame within which VMS managers may not change their passwords again after setting a new password if password change timeout is enabled.</p> <p>Specify <b>TIMEOUT</b> as an integer followed by a prefix for time units. D for days, H for hours, M for months.</p> <p>Default: 24H</p>
--pwd-expiration-timeout TIMEOUT	<p>Sets the password expiration timeout, which applies if password expiration timeout is enabled.</p> <p>Specify <b>TIMEOUT</b> as an integer followed by a prefix for time units: D for days, M for months. The minimum valid value is one day.</p> <p>Default: 180D</p>
--tmp-pwd-expiration-timeout TIMEOUT	<p>Sets the expiration timeout for the new managers' temporary passwords.</p> <p>Specify <b>TIMEOUT</b> as an integer followed by a prefix for time units: H for hours, D for days, M for months. The minimum valid value is one hour.</p>

	Default: 7D
<code>--max-failed-login-attempts ATTEMPTS</code>	Sets the number of failed login attempts after which password lockout occurs if enabled. Specify ATTEMPTS as an integer. Default: 10
<code>--pwd-history-no-reuse-count COUNT</code>	Sets the number of previous passwords that VMS managers may not reuse if prevention of password reuse is enabled. Specify COUNT as an integer. Default: 8
<code>--enable-pwd-change-timeout</code>	Enables prevention of password changes within the time frame set by <code>--pwd-change-timeout</code> .
<code>--disable-pwd-change-timeout</code>	Disables prevention of password changes within the time frame set by <code>--pwd-change-timeout</code> .
<code>--enable-pwd-expiration-timeout</code>	Enables expiration of VMS passwords after the time period set by <code>--pwd-expiration-timeout</code> .
<code>--disable-pwd-expiration-timeout</code>	Disables expiration of VMS passwords.
<code>--enable-max-failed-login-attempts</code>	Enables password lockout after a number of failed login attempts. The number of failed attempts is set by <code>--max-failed-login-attempts</code> .
<code>--disable-max-failed-login-attempts</code>	Disables password lockout after a number of failed login attempts.
<code>--enable-pwd-history-no-reuse-count</code>	Enables prevention of VMS manager users from reusing a number of previous passwords, set by <code>--pwd-history-no-reuse-count</code> .
<code>--disable-pwd-history-no-reuse-count</code>	Disables prevention of VMS manager users from reusing a number of previous passwords.



# Examples

To enable password expiration and set password expiration to 60 days:

```

vcli: admin> vms modify_pwd_settings --enable-pwd-expiration-timeout --pwd-expiration-timeout
60D

```

To enable enforcement of all forms of password complexity and to enforce manager lockout after 5 failed login attempts:

```

vcli: admin> vms modify_pwd_settings --enable-pwd-uppercase-validation --enable-pwd-lowercas
e-validation --enable-pwd-numeric-validation --enable-pwd-special-chars-validation --enable-m
ax-failed-login-attempts --max-failed-login-attempts 5

```

## vms modify\_saml

This command modifies a new or existing Identity Provider (IDP).

# Usage

```

vms modify_saml --idp-name IDP_NAME
                [--idp-entityid ENTITY_ID]
                [--encrypt-assertion]
                [--disable-encrypt-assertion]
                [--want-assertions-or-response-signed]
                [--force-authn]
                [--disable-force-authn]
                [--local-idp-metadata]
                [--idp-metadata-url METADATA_URL]
                [--remove-idp-metadata local|remote]

```

# Required Parameters

<code>--idp-name</code> <code>IDP_NAME</code>	Specifies the name of the new IDP configuration, or the name of a previously configured IDP to modify. This field is used later for the SSO login URL for the SP (VMS).
--	---

# Options

<code>--idp-</code> <code>entityid</code> <code>ENTITY_ID</code>	The unique identifier of the IDP entity.
<code>--encrypt-</code> <code>assertion</code>	This option is required if the IDP encrypts the assertion. If this option is used, you are prompted for the certificate and key.
<code>--disable-</code>	This option removes the certificate used in <code>--encrypt-assertion</code> files and the IDP configuration.

encrypt-assertion	
--want-assertions-or-response-signed	If this option is used the SP (VMS) will accept only a signed response or signed assertion from the IDP. VMS will fail the user authentication if an unsigned response is received. If this option is used, a certificate and key must be provided after executing the command.
--force-authn	Forces authentication with the IDP even if there is an active session with the IdP for the user.
--disable-force-authn	Disable the <code>--force-authn</code> option.
--local-idp-metadata	Use local metadata. If used, you are prompted for the metadata (must be in XML file format).
--idp-metadata-url METADATA_URL	Use metadata located at METADATA_URL. The URL is typically in the format: <https://<YourIDPURL>>/sso/saml/metadata
--remove-idp-metadata local remote	This option will remove either the local or remote IDP metadata file. Specify which file to remove, local or remote.  For example: <b>vms modify_saml --remove-idp-metadata local</b>

## Examples

```
vcli: admin> vms modify_saml --idp-name Okta --force-authn
This action will impact you saml login with Okta.
Are you sure you want to continue? [y/N] y
Saml Config as been changed for Okta
```

```
vcli: admin> vms modify_saml --idp-name Okta --idp-metadata-url https://dev-46872236.okta.com/app/ekxm4bscg4RuruH8C5g7/sso/saml/metadata --idp-entityid http://www.okta.com/ewkh4aftf7NerrH4C5t1
This action will impact you saml login with Okta.
Are you sure you want to continue? [y/N] y
Saml Config as been changed for Okta
```

With encrypted assertions (requires certificate):

```
vms modify_saml --idp-entityid http://www.okta.com/ewkh4aftf7NerrH4C5t1 --idp-metadata-url https://dev-46872236.okta.com/app/ekxm4bscg4RuruH8C5g7/sso/saml/metadata --idp-name Okta --encrypt_assertion
This action will impact your saml login with Okta.
Are you sure you want to continue? [y/N] y
Please enter idp signing certificate (ALT+ENTER/option+ENTER to finish):
```

```
PUT_CERTIFICATE_FILE_CONTENT
Please enter idp signing certificate key (ALT+ENTER/option+ENTER to finish):
PUT_KEY_FILE_CONTENT
```

**vms remove\_client\_certificate**

This command removes an mTLS certificate from VMS.

**Usage**

```
vms remove_client_certificate
```

**Example**

```
vcli: admin> vms remove_client_certificate
This action will remove the client certificate from vms,
vms will no longer verify client requests after that.
Are you sure you want to proceed? [y/N] y
client certificate has been removed, please reconnect.
```

**vms remove\_saml\_signed\_cert**

This command removes all the Security Assertion Markup Language (SAML) signed certificates and keys from the IDP configuration.

**Usage**

```
vms remove_saml_signed_cert --idp-name IDP_NAME
```

**Required Parameters**

<code>--idp-name IDP_NAME</code>	The name of the IdP.
----------------------------------	----------------------

**Example**

```
vcli: admin> vms remove_saml_signed_cert --idp-name Okta
```

**vms reset\_certificate**

This command resets the VMS SSL certificate to the default self signed certificate.

**Usage**

```
vms reset_certificate [--id ID]
```

# Options

<code>--id ID</code>	ID of the VMS.
----------------------	----------------

## Example

```
vcli: admin> Reset vms reset_certificate
Reset VMS SSL certificate to default? [y/N]
```

### vms reset\_ssl\_ciphers

This command resets the SSL ciphers support to default.

## Usage

```
vms reset_ssl_ciphers
```

## Example

```
vcli: admin> vms reset_ssl_ciphers
Reset VMS SSL ciphers to default? [y/N]
```

### vms set\_certificate

This command installs an authority-signed SSL certificate to secure the HTTPS connection between the VAST Web UI and VMS. By default, VMS is pre-installed with a self-signed SSL certificate.

## Usage

```
vms set_certificate [--id ID]
```



#### Note

After you run the command, you are prompted to enter the certificate and private key. Enter the certificate and key content one after the other, including the "BEGIN CERTIFICATE", "END CERTIFICATE", "BEGIN PRIVATE KEY" and "END PRIVATE KEY" lines:

```
-----BEGIN CERTIFICATE-----
<Certificate file content>
-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
<Key file content>
-----END PRIVATE KEY-----
```

## Options

<code>--id ID</code>	ID of the VMS.
----------------------	----------------

## Example

This example

```
vccli: admin> vms set_certificate --id 1
Please enter certificate AND private key (ALT+ENTER/option+ENTER to finish):
```

### **vms set\_client\_certificate**

This command uploads an mTLS to VMS, effectively enabling mTLS authentication for VMS clients. Read more about this feature [here](#).

## Usage

```
vms set_client_certificate --id 1
```



### **Note**

After you run the command, you are prompted to enter the certificate and private key. Enter the certificate and key content one after the other, including the "BEGIN CERTIFICATE", "END CERTIFICATE", "BEGIN PRIVATE KEY" and "END PRIVATE KEY" lines:

```
-----BEGIN CERTIFICATE-----
<Certificate file content>
-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
<Key file content>
-----END PRIVATE KEY-----
```

## Example

```
vccli: admin> vms set_client_certificate --id 1
Please enter certificate AND private key (ALT+ENTER/option+ENTER to finish):
```

### **vms set\_max\_api\_tokens\_per\_user**

This command sets the maximum API tokens per VMS manager user.

## Usage

```
vms set_max_api_tokens_per_user --max-api-tokens-per-user MAX_TOKENS
```

[--id ID]

## Required Parameters

<code>--max-api-tokens-per-user MAX_TOKENS</code>	<p>The number of valid tokens a VMS user can have at one time. When tokens are revoked, they become invalid.</p> <p>Specify <code>MAX_TOKENS</code> as an integer.</p> <p>Default: 5.</p>
---	---

## Options

<code>--id ID</code>	VMS ID
----------------------	--------

## Example

```
vccli: admin> vms set_max_api_tokens_per_user --max-api-tokens-per-user 8
```

### vms set\_ssl\_ciphers

This command restricts the VMS SSL cipher support to a more restricted set of ciphers.

## Usage

```
vms set_ssl_ciphers --ssl-ciphers SSL_CIPHERS  
                    [--id ID]
```

## Required Parameters

<code>--ssl-ciphers SSL_CIPHERS</code>	Specifies the more restricted SSL cipher set.
--	---

## Options

<code>--id ID</code>	ID of the VMS object
----------------------	----------------------

## Example

```
vcli: admin> vms set_ssl_ciphers --ssl-ciphers AES256+EECDH:AES256+EDH:!aNULL:!SHA1:!SHA256:!SHA384
```

### vms set\_ssl\_port

This command changes the VMS SSL port.

## Usage

```
vms set_ssl_port --ssl-port SSL-PORT  
                [--id ID]
```

## Required Parameters

<code>--ssl-port</code>	Specifies the SSL port.  Default: 443
-------------------------	---

## Options

<code>--id</code>	Specifies the VMS ID.
-------------------	-----------------------

## Example

```
vcli: admin> vms set_ssl_port --ssl-port 443
```

### vms show

This command displays details of VMS.

## Usage

```
vms show [--passwords-settings]
```

## Options

<code>--passwords-settings</code>	Shows password complexity requirement settings.
-----------------------------------	---

# Example

```
vcli: admin> vms show
+-----+
| Name           | VMS |
| Created        | 2024-07-22 21:05:36 |
| SW-Version     | 5.1.2.17 |
| Build          | release-5-1-2-1411704-vms |
| Auto-Logout-Timeout | 600 |
| IP1            | 10.10.0.1 |
| IP2            | 10.10.64.1 |
| MGMT-VIP       | 10.131.200.152 |
| Mgmt-CNode     | cnode-128-1 |
| Performance-base-10 | True |
| Capacity-base-10 | True |
| Login-banner   | None |
| Access-token-lifetime | 01:00:00 |
| Refresh-token-lifetime | 1 00:00:00 |
| MGMT-VIP-IPv6  | UNKNOWN |
| Perf-debug-metrics-enabled | N/A |
+-----+

vcli: admin> vms show --passwords-settings
+-----+
| Min-pwd-length | 8 |
| Pwd-requires-uppercase | True |
| Pwd-requires-lowercase | True |
| Pwd-requires-numeric | True |
| Pwd-requires-special-chars | True |
| Pwd-change-timeout | 24H |
| Pwd-expiration-timeout | 180D |
| Tmp-pwd-expiration-timeout | 7D |
| Max-failed-login-attempts | 10 |
| Pwd-history-no-reuse-count | 8 |
| Pwd-change-timeout-enabled | False |
| Pwd-expiration-timeout-enabled | False |
| Max-failed-login-attempts-enabled | False |
| Pwd-history-no-reuse-count-enabled | False |
+-----+
```

## vms show\_saml\_config

This command displays important SAML configuration for a specific IDP. This command also displays the SP SSO login URL to use in the IDP configuration page.

# Usage

```
vms show_saml_config --idp-name IDP_NAME
```

# Required Parameters

<code>--idp-name IDP_NAME</code>	Specifies the name of the IDP configuration to display.
----------------------------------	---



# Command Output

idp	The sso_login to your IDP application.
metadata	Displays the metadata, and shows if it is local or remote.
sp_settings	The SP (VMS) settings for SAML. Some of the values such as sso_url or the required_attributes must to be entered in the IDP.

## Example

```
vcli: admin> vms show_saml_config --idp-name Okta
+-----+
+-----+
+
| idp          | {'http://www.okta.com/<app_id>': {}}
|
| metadata     | {'remote': [{'url': 'https://<idp_app_url>.okta.com/app/<app_id>/sso/saml/met
adata'}}]
|
| sp_settings  | {'entityid': 'https://<mgmt_vip>/api/saml2/metadata/', 'sso_url': ['http
s://<mgmt_vip>/api/saml2/acs/?idp_name=Okta',
|
|               | 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST'], 'single_logout_service':
|
|               | 'https://<mgmt_vip>/saml2/ls/post/',
|
|               | 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST'], 'encrypt_assertion': Fals
e, 'want_assertions_or_response_signed':
|
|               | False, 'force_authn': False, 'required_attributes': ['email', 'username']}
|
+-----+
+-----+
+
```

## vms show\_saml\_configured\_idps

This command displays all the IDP names you configured in VMS, and the IDPs that can be used for user authentication in VMS.

## Usage

```
vms show_saml_configured_idps
```

## Example

```
vcli: admin> vms show_saml_configured_idps
```

## Command Output

idp name	The name of the IDP configured in VMS.
----------	--

## Example

```
vcli: admin> vms show_saml_configured_idps
+-----+
| Okta   |
+-----+
```

# volume commands

## volume create

This command creates a volume of block storage on a block enabled view.

## Usage

```
volume create --view-id ID
               --name
               --size
               [--tags TAGS]
```

## Required Parameters

<code>--view-id ID</code>	Specifies which block subsystem view under which to provision the volume. Specify the integer ID of a view that is configured for block storage (has the block protocol enabled).
<code>--name NAME</code>	<p>Modifies the volume name, which is the path to the volume relative to the subsystem view to which it belongs. The path can include a nesting of subdirectories. Subdirectories that do not yet exist will be created accordingly when the name is configured.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• To place the volume directly under the subsystem view to which it belongs and name it <i>block1</i>: <code>--name block1</code>.</li><li>• To place the volume under a subdirectory called <i>blocks</i> under the subsystem view to which it belongs and name it <i>block1</i>: <code>--name blocks/block1</code>.</li></ul>
<code>--size SIZE</code>	<p>Modifies the capacity of the volume.</p> <p>Specify <i>SIZE</i> as a number followed by GB or TB.</p> <p>For example: <code>--size 500GB</code>.</p>

## Options

<code>--tags TAGS</code>	<p>Adds key-value pairs to tag the volume, for the purpose of categorizing and organizing block volumes.</p> <p>Specify <i>TAGS</i> as a comma separated list of key-value pairs in format <i>&lt;key&gt;=&lt;value&gt;</i>.</p>
--------------------------	--

	For example: <code>--tags team=backend,owner=BG</code>
--	--

## Example

```
vcli: admin> volume create --view-id 3 --name dev/platform --size 100GB --tags owner=DG,team=platform
```

### volume delete

This command deletes a block storage volume.

## Usage

```
volume delete --id ID
                [--force]
```

## Required Parameters

<code>--id ID</code>	Specifies which volume to delete.
----------------------	-----------------------------------

## Options

<code>--force</code>	If hosts are mapped to the volume, this option forces unmapping of the hosts and deletion of the volume.
----------------------	--

## Example

```
vcli: admin> volume delete --id 1
Are you sure you want to delete the volume? [y/N] y
Command REST Error: {"detail":"Volume is mapped to hosts"}
vcli: admin> volume delete --id 1 --force
Are you sure you want to delete the volume? [y/N] y
vcli: admin>
```

### volume fetch-capacity

This command fetches the capacity in use of a volume.

## Usage

```
volume fetch-capacity --id ID
```

# Required Parameters

<code>--id ID</code>	Specifies a volume by its ID.
----------------------	-------------------------------

## Example

```
vccli: admin> volume fetch-capacity --id 1
0.055
```

### volume get\_snapshots

This command lists snapshots of a volume.

## Usage

```
volume get_snapshots --id ID
```

# Required Parameters

<code>--id ID</code>	Specifies the volume.
----------------------	-----------------------

## Example

```
vccli: admin> volume get_snapshots --id 1
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+
| Id | View-id | Name | Size(GB) | Tags | Namespace-id | Nguid | Uuid | Capacity(GB) | Snapsh
ot-id | Tenant-name |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+
| 1 | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A
| N/A |
| 2 | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A
| N/A |
| 3 | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A
| N/A |
| 4 | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A
| N/A |
| 5 | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A
| N/A |
| 6 | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A
| N/A |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+
```

### volume list

This command lists volumes and their properties.

# Usage

volume list [--view-id ID]

## Options

--view-id ID	Filters the list by subsystem. Specify the ID of a subsystem view.
--------------	--

## Example

```
vcli: admin> volume list
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
| Id | View-id | Name          | Size(GB) | Tags          | Namespace-id |
| Nguid          | Uuid          | Capacity(GB) |
| Snapshot-data | Tenant-name | Mapped-block-hosts-preview | Mapped-block-host-count |
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
| 1 | 3 | vol1 | 1.000 | {} | None |
| 066e3181-aa6b-44fe-8c87-26cc28680606 | 066e3181-aa6b-44fe-8956-3ccc28680606 | 0.000 |
| {'id': None, 'name': 'N/A'} | default | | 0 |
|
| 2 | 3 | vol2 | 1000.000 | {} | None |
| 1759cdf8-9f1a-420e-8c87-26ff03f50536 | 1759cdf8-9f1a-420e-9e6c-c7ff03f50536 | 0.000 |
| {'id': None, 'name': 'N/A'} | default | | 0 |
|
| 3 | 3 | cats/tiger | 1.000 | {} | 1 |
| 0f331ba5-8e66-46ed-8c87-26a2c6ad7714 | 0f331ba5-8e66-46ed-a683-6ca2c6ad7714 | 0.000 |
| {'id': None, 'name': 'N/A'} | default | Host | 1 |
|
| 5 | 3 | cats/other | 1.000 | {} | None |
| 6ba2df6a-8804-4b04-8c87-269750455d4e | 6ba2df6a-8804-4b04-9232-ca9750455d4e | 0.000 |
| {'id': None, 'name': 'N/A'} | default | | 0 |
|
| 7 | 3 | cats/lion | 1.000 | {'Team': 'Lions', 'Owner': 'Lioness'} | 5 |
| 6890147a-7d44-48d2-8c87-26568e3a36f8 | 6890147a-7d44-48d2-8a56-c4568e3a36f8 | 0.000 |
| {'id': None, 'name': 'N/A'} | default | Host | 1 |
|
| 8 | 3 | vol1 | 1.000 | {} | 3 |
| a41e00d0-68b1-4900-8c87-26ec9655430e | a41e00d0-68b1-4900-9210-e4ec9655430e | 0.000 |
| {'id': 1, 'name': 'VollSnap'} | default | Host | 1 |
|
| 9 | 3 | cats/lion | 1.000 | {} | 4 |
| b7e73c6d-7be4-4354-8c87-26d663daace6 | b7e73c6d-7be4-4354-9a62-44d663daace6 | 0.000 |
| {'id': 5, 'name': 'CatsSnap'} | default | Host | 1 |
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
```

# Command Output

Id	The VMS ID of the volume.
View-id	The VMS ID of the subsystem view to which the volume belongs.
Name	The name of the volume.
Size (GB)	The amount of capacity allocated to the volume.
Tags	The tags assigned to the volume, if applicable.
Namespace-id	The namespace ID as used by hosts to search the volume within the subsystem. Each namespace ID is unique within the subsystem. If a volume snapshot is mapped to any host(s), a snapshot volume is created with its own namespace ID.
Nguid	The NGUID used by block hosts to access the volume.
Uuid	The UUID, used by hosts to search the volume in the subsystem.
Capacity	The amount of used capacity on the volume.
Snapshot-data	For snapshot volumes, the ID and name of the snapshot from which the volume was mapped.
Tenant-name	The name of the tenant to which the volume belongs.

## volume modify

This command modifies a block storage volume. You can change the name and size, remove tags and add tags.

## Usage

```
volume modify --id ID
               [--name NAME]
               [--size SIZE]
```

[--tags|--tags TAGS]

## Required Parameters

<code>--id ID</code>	Specifies which volume to modify.
----------------------	-----------------------------------

## Options

<code>--name NAME</code>	<p>Modifies the volume name, which is the path to the volume relative to the subsystem view to which it belongs. The path can include a nesting of subdirectories. Subdirectories that do not yet exist will be created accordingly when the name is configured.</p> <p>Examples:</p> <ul style="list-style-type: none"><li>• To place the volume directly under the subsystem view to which it belongs and name it <i>block1</i>: <code>--name block1</code>.</li><li>• To place the volume under a subdirectory called <i>blocks</i> under the subsystem view to which it belongs and name it <i>block1</i>: <code>--name blocks/block1</code>.</li></ul>
<code>--size SIZE</code>	<p>Use this option to expand the capacity of the volume.</p> <p>Specify <i>SIZE</i> as a number followed by GB or TB.</p> <p>For example: <code>--size 500GB</code>.</p>
<code>-- tags -- tags TAGS</code>	<p>Add or remove tags:</p> <ul style="list-style-type: none"><li>• To remove all tags, specify <code>--tags</code> without an argument.</li><li>• To remove all tags and add new ones, provide only the new tags.</li><li>• To add tags without removing the existing tags, provide all old and new tags.</li></ul> <p>Specify <i>TAGS</i> as a comma separated list of key-value pairs in format <i>&lt;key&gt;=&lt;value&gt;</i>. Encapsulate the list with quotation marks. For example: <code>--tags "team=backend,owner=BG"</code></p>

## Example

```
vcli: admin> volume modify --id 1 --size 80GB
```

### volume show

This command displays the properties of a specified volume.



# Usage

volume show --id ID

## Required Parameters

--id ID	Specifies which volume to display.
---------	------------------------------------

## Example

```
vcli: admin> volume show --id 4
+-----+-----+
| Id      | 4      |
| View-id | 12     |
| Name    | vol_2  |
| Size(GB)| 10.000 |
| Tags    | {'team': 'platform', 'owner': 'DG'} |
| Namespace-id | 2      |
| Nguid   | 1533db2e-8c87-26d8-8069-510695bb6e51 |
| Uuid    | 1533db2e-8cd3-45d8-8069-510695bb6e51 |
| Capacity(GB) | 0.055 |
| Snapshot-data | {'id': None, 'name': 'N/A'} |
| Tenant-name | default |
+-----+-----+
```

## Command Output

Id	The VMS ID of the volume.
View-id	The VMS ID of the subsystem view to which the volume belongs.
Name	The name of the volume.
Size (GB)	The amount of capacity allocated to the volume.
Tags	The tags assigned to the volume, if applicable.
Namespace-id	The namespace ID as used by hosts to search the volume within the subsystem. Each namespace ID is unique within the subsystem. If a volume snapshot is mapped to any host(s), a snapshot volume is created with its own namespace ID.

Nguid	The NGUID used by block hosts to access the volume.
Uuid	The UUID, used by hosts to search the volume in the subsystem.
Capacity	The amount of used logical capacity on the volume.
Snapshot- data	For snapshot volumes, the ID and name of the snapshot from which the volume was mapped.
Tenant- name	The name of the tenant to which the volume belongs.

